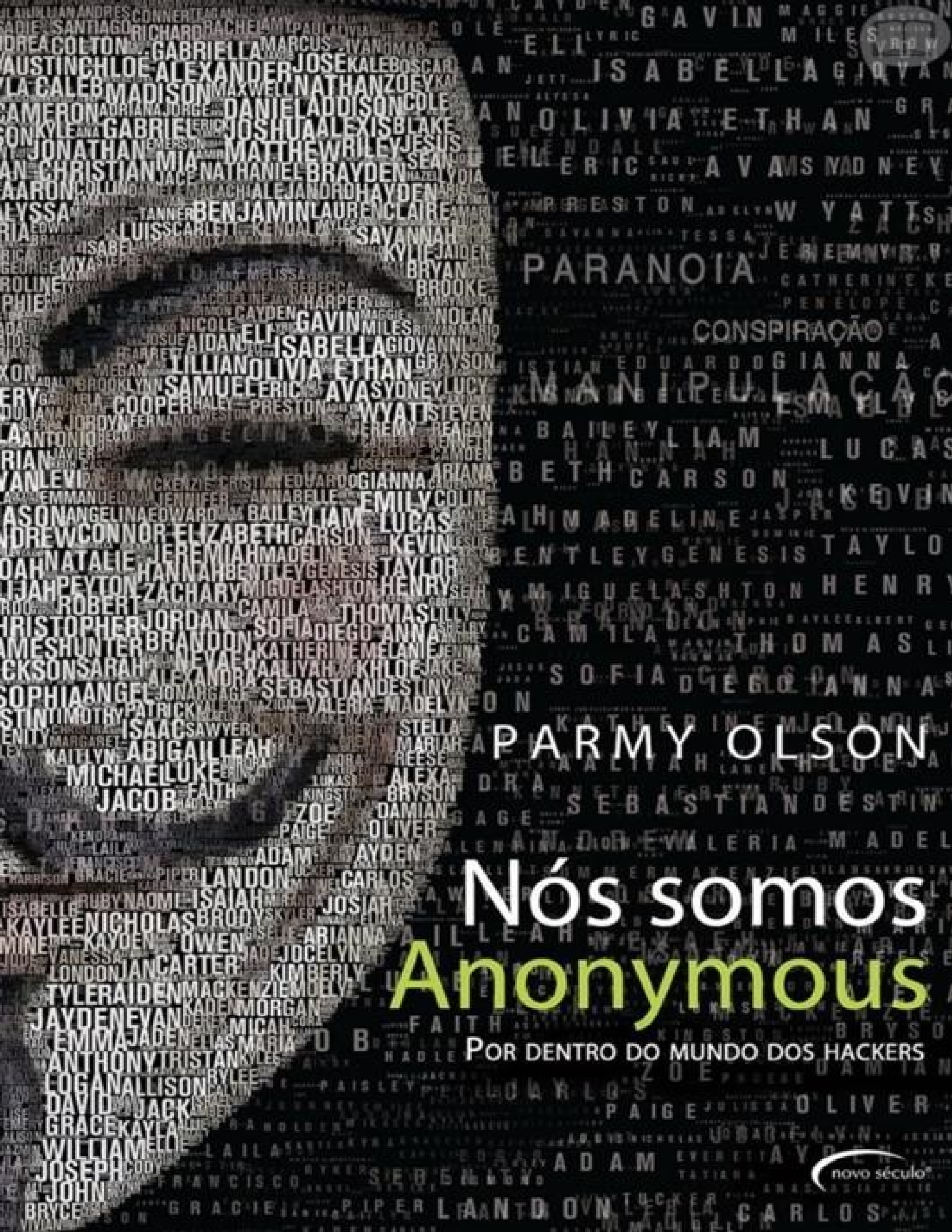
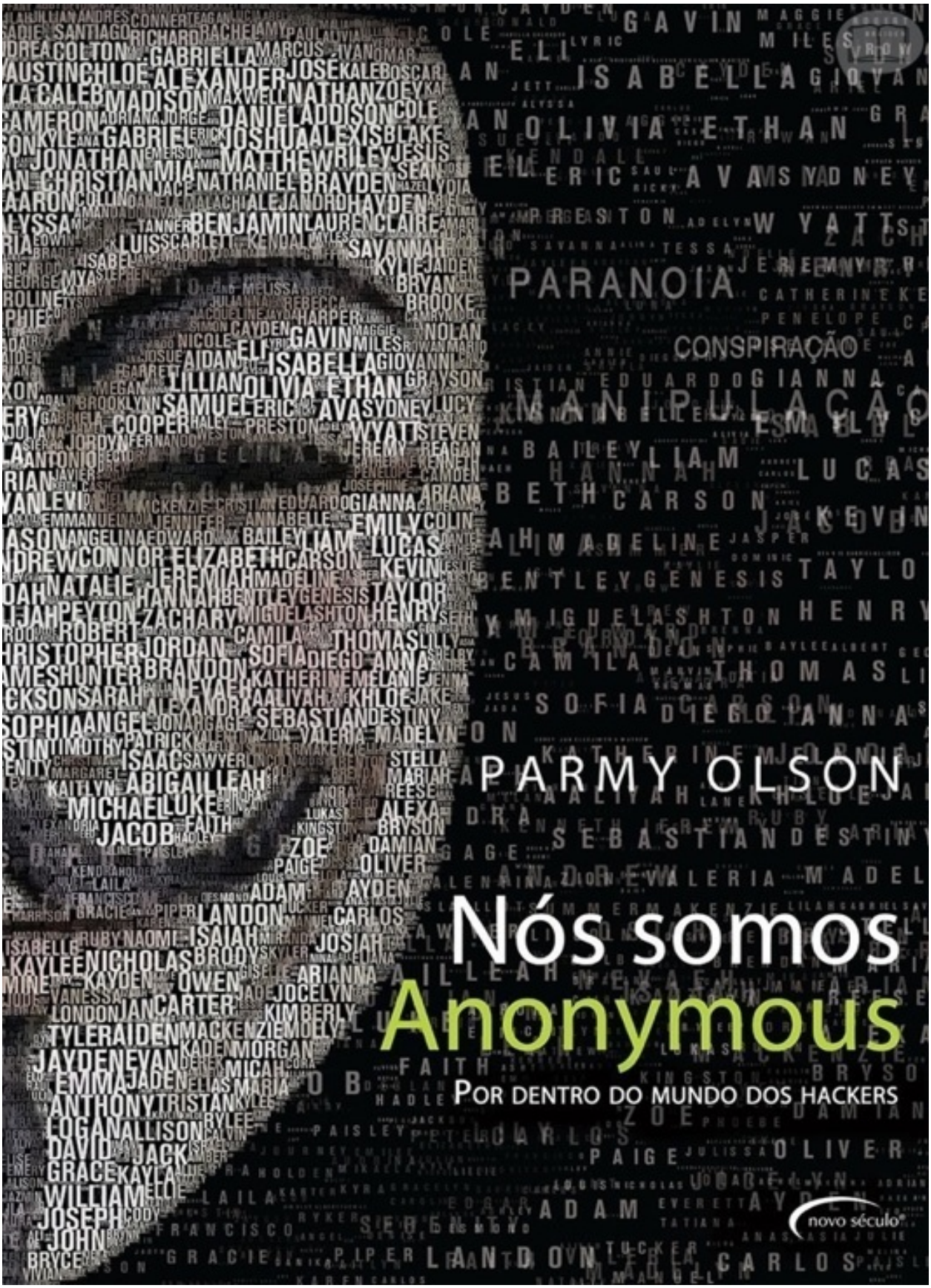


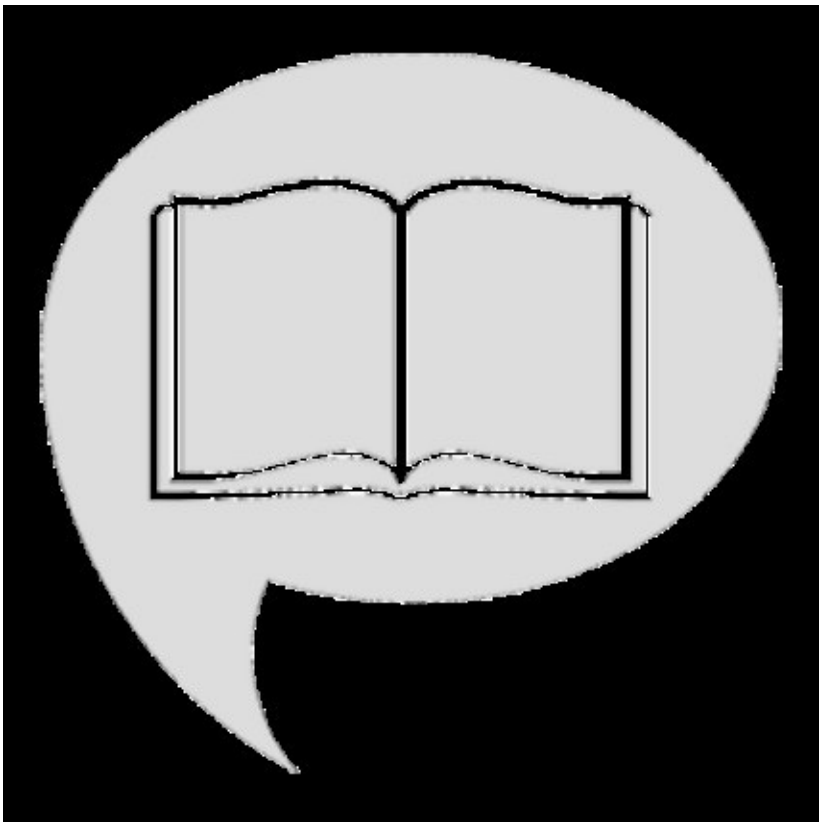
PARMY OLSON

Nós somos Anonymous

Por dentro do mundo dos hackers

novo século


PARMY OLSON
Nós somos
Anonymous
POR DENTRO DO MUNDO DOS HACKERS
novo século



E les acreditavam que toda informação deveria ser livre, e eram capazes de i nvadir seu site se você discordasse disso. Combatiam o sistema e toda forma de g overno imposta. Alegavam que não se tratava apenas de um grupo organizado, m as sim de pessoas dispostas a “tudo ou nada”. A descrição mais próxima seria u ma “marca”, um “símbolo”, um “coletivo”. Suas poucas regras eram como a quelas do “Clube da Luta”: não fale sobre o Anonymous, não revele sua v erdadeira identidade e não ataque a mídia. Naturalmente, o anonimato dava a e les a liberdade de cometer certos delitos, como invadir servidores privados, r oubar dados secretos de uma empresa, derrubar um site e depois devolvê--lo,

c ompletamente desIigurado. Algumas destas ações poderiam, inclusive, ser

consideradas crimes, condenando-os à prisão por dez anos ou mais.

ELOGIOS A *NÓS SOMOS*

ANONYMOUS, DE PARMY OLSON

“Obra dinâmica e estarrecedora que se lê como *A rede social* para grupos de hackers. Semelhante ao que acontece no filme sobre o Facebook, as inovações tecnológicas criadas por algumas pessoas tornam-se uma bola de neve muito além das expectativas, até alcançar efeito generalizado. Mas é o elemento humano – a mescla de deleite, malevolência, aleatoriedade, megalomania e apenas pura traquinagem que ajudou a criar essas mudanças – que Parmy Olson consegue explorar melhor...

Somos Anonymous também captura a vasta gama de motivos pelos quais o Anonymous e o LulzSec atraíram seguidores.”

Janet Maslin, *The New York Times*

“Extraordinário relato sobre as entranhas do movimento hacker.”

Steve Fishman, *New York*

“Uma história incrível.”

Jon Stewart, *The Daily Show*

“Obra-prima do jornalismo investigativo, relato ágil e ricamente detalhado sobre as origens do grupo, suas várias facções e seus ataques mais espetaculares.”

The Daily

“Mulher que se infiltrou numa subcultura essencialmente masculina, Parmy Olson oferece entrevistas notáveis com os anti-heróis do Anonymous.”

Justin Moyer, *Washington Post*

“Olson mantém acelerado o ritmo de *Somos Anonymous*, ao dar saltos cronológicos e utilizar elementos de suspense e drama com o objetivo de amarrar os diferentes fios narrativos e ao mesmo tempo atrair a atenção do leitor... Essencialmente um conto humano.”

Rowan Kaiser, *A.V. Club*

“Os únicos livros novos que li este ano foram sobre a internet. O melhor deles foi *Somos Anonymous: uma incursão ao mundo hacker do Lulzsec, do Anonymous e da insurgência cibernética global*, de Parmy Olson, a jornalista da revista *Forbes*. Tenho lido (e escrito) milhares de palavras sobre o grupo hacktivista Anonymous, mas mesmo assim adorei esse mordaz relato interno acerca dos altos e baixos, das conflagrações e repressões do movimento hacker nos últimos anos. Olson desvela a personalidade de Jake “Topiary” Davis, jovem de dezoito anos, um dos líderes do grupo hacker LulzSec, e utiliza a história dele para transformar o que seria apenas uma insossa repetição de manchetes numa complexa análise de como a internet levou jovens (em sua maioria do sexo masculino) a se envolver em coisas bem maiores que eles próprios. Qualquer um com o mínimo interesse nos assuntos da internet que vá além do Facebook ou do Twitter deve ler este livro.”

Adrian Chen, *Gawker*

“Narrativas midiáticas tendem a pintar esses grupos seja como asquerosos vilões, seja como adolescentes bufões com muito tempo para dispor de suas mãos codificadoras. *Somos Anonymous*, **empolgante espiada nessas organizações misteriosas e complexas e em alguns dos hackers no núcleo delas, fornece uma perspectiva mais cheia de nuanças que as manchetes.”**

Karlin Lillington, *Irish Times*

“*Somos Anonymous* oferece uma brilhante compreensão sobre o mundo dos hacktivistas... Parmy Olson rastreia a emergência e a dominação do LulzSec, seguindo as reviravoltas da história conforme ela aconteceu.”

Carole Cadwalladr, *The Observer (UK)*

“Encantador... Olson recria meticulosa e imparcialmente as operações do Anonymous e do LulzSec.”

Publishers Weekly (resenha com estrela) ANTES DE VOCÊ LER ESTE LIVRO

Nomes

A maioria dos nomes e nicknames on-line utilizados neste livro é verdadeira, à exceção de alguns. Todos os nomes inventados se relacionam com “William”, jovem que mora no Reino Unido e cujas tentativas noturnas de aplicar trotes e atormentar pessoas nos fornecem uma espiada no universo do *b*, o painel de discussões mais popular do 4chan. O nome dele e os das vítimas foram modificados.

Fontes

A maioria das informações e dos relatos deste livro tem como fonte entrevistas diretas com os protagonistas de cada caso, como Hector “Sabu” Monsegur e Jake “Topiary” Davis. Porém, sabe-se que hackers costumam compartilhar nicknames para ajudá-los a ocultar suas identidades ou apenas para mentir descaradamente. Sendo assim, procurei corroborar os relatos das pessoas até onde o tempo me permitiu. Em relatos pessoais – por exemplo, como no caso em que Sabu foi parado e revistado pela polícia de Nova York –, deixo claro que se trata do testemunho do próprio hacker. Durante o ano de pesquisas para escrever este livro, alguns hackers se revelaram mais confiáveis que outros, por isso dediquei mais atenção ao testemunho das fontes que considerei mais seguras. Nos apêndices, encontram-se notas sobre fontes de informações essenciais, notícias divulgadas e estatísticas.

Grafia

Para manter o ritmo da narrativa, limpei a grafia e a gramática de citações extraídas de salas de bate-papo e utilizadas como diálogo entre os personagens. Nos casos em que entrevistei pessoas pelo protocolo interativo de Internet Relay Chat, também limpei a grafia; no entanto, se uma fonte pulava uma ou duas palavras, as que ficaram subentendidas aparecem [entre colchetes].

Gente

Algumas pessoas apresentadas neste livro são pseudolíderes do Anonymous, mas não o representam como um todo. Vale a pena repetir: elas não representam o Anonymous como um todo. Alguns protagonistas, como William ou Sabu, têm personalidades voláteis e, ao conhecer suas histórias extraordinárias, você, leitor ou leitora, passará a entender engenharia social, hackeagem, quebra de senhas e ascensão de perturbadores cibernéticos de modo talvez mais cativante do que se lesse acerca dessas técnicas isoladamente. Muita gente no Anonymous não é alvo das investigações policiais apresentadas neste livro e também procura defender padrões autênticos de legalidade e ativismo político. Para obter outras perspectivas sobre o Anonymous, fique de olho na obra de Gabriella Coleman, acadêmica que há vários anos acompanha as atividades da organização, e no livro sobre o Anonymous escrito por Gregg Housh e Barrett Brown, com lançamento em 2012. O documentário *We Are Legion: The Story of the Hacktivists*, de Brian Knappenberger, também focaliza aspectos do ativismo político do Anonymous.

PARTE 1

Nós Somos Anonymous

CAPÍTULO 1

O Ataque

Por todo o território dos EUA, no dia 6 de fevereiro de 2011, milhões de pessoas se acomodavam em seus sofás, abrindo sacos de salgadinhos e vertendo cerveja em copos de plástico nos preparativos para o maior evento esportivo do ano. Naquele domingo de Super Bowl em que o Green Bay Packers derrotou o Pittsburgh Steelers, um executivo de segurança digital chamado Aaron Barr assistiu de camarote a sete pessoas que ele não conhecia virarem seu mundo de pernas para o ar. O domingo do Super Bowl foi o dia em que ele deparou cara a cara com o Anonymous.

Ao cabo daquele fim de semana, a palavra Anonymous tinha nova acepção. Ampliando a definição do dicionário (algo sem nome identificável), parecia ser um grupo nebuloso e sinistro de hackers empenhado em atacar inimigos do acesso livre a informações, inclusive indivíduos como Barr, cidadão casado, pai de gêmeos, que cometera o engano de tentar vislumbrar quem realmente estava por trás do Anonymous.

O momento realmente decisivo aconteceu na hora do almoço, seis horas antes do início do Super Bowl. Sentado no sofá da sala de sua residência nos subúrbios da capital Washington, numa confortável roupa dominical – camiseta e jeans –, ele percebeu que o iPhone não havia tocado em seu bolso na última meia hora. Em geral, o aparelho o alertava sobre a chegada de um e-mail a cada quinze minutos. Ao pinçá-lo do bolso e apertar um botão para atualizar as mensagens, uma janela azul-escura surgiu.

Mostrava três palavras que mudariam sua vida: *Impossível acessar mensagens*. Em seguida, o programa de leitor de e-mails solicitou que ele verificasse se a senha estava certa. Barr entrou nas configurações da conta e cuidadosamente digitou: “kibafo33”. Não funcionou. Os seus e-mails não estavam aparecendo.

Baixou o olhar e fitou a telinha inexpressivamente. Devagarinho, um calafrio de ansiedade percorreu sua espinha, à medida que percebia o significado daquilo. Desde o bate-papo com um hacker do Anonymous de alcunha Topiary algumas horas antes, ele pensou que havia se safado.

Agora sabia que alguém tinha hackeado sua conta da HBGary Federal, empresa de segurança tecnológica, possivelmente acessando dezenas de milhares de e-

mails internos e depois blindando a sua entrada. Isso significava que alguém, em algum lugar, tinha visto acordos de confidencialidade e documentos sigilosos capazes de comprometer um banco multinacional, uma conceituada agência do governo dos EUA e a sua própria empresa.

Um por um, foi se lembrando de comunicados e documentos secretos, cada qual prenunciando uma nova onda de pavor nauseante. Barr subiu correndo os degraus até seu *home office* e sentou-se diante do laptop.

Tentou entrar em sua conta no Facebook para conversar com um hacker conhecido seu, alguém que pudesse ajudá-lo. Mas essa rede social, com suas poucas centenas de amigos, estava bloqueada. Tentou a conta no Twitter, com poucas centenas de seguidores. Nada. Depois o Yahoo. Mesma coisa. O acesso a quase todas as suas contas na web estava impedido, até mesmo ao jogo de RPG World of Warcraft. Barr silenciosamente se censurou por utilizar a mesma senha em todas as contas. Mirou de relance o roteador Wi-Fi e viu luzes brilhando freneticamente. Agora alguém tentava sobrecarregar o tráfego, com o objetivo de penetrar ainda mais em sua rede doméstica.

Estendeu a mão e desconectou o plugue. As luzes piscantes se apagaram.

***

Aaron Barr havia sido militar. De ombros largos, cabelo preto como breu e sobrancelhas espessas que sugeriam longínquos ancestrais mediterrâneos, ele se alistara na Marinha dos EUA após cursar dois semestres na universidade e se dar conta de que aquilo não era para ele.

Logo se tornou um agente de SIGINT (*signals intelligence* – atividade de colher informações ou inteligência através da interceptação de sinais de comunicações entre pessoas ou máquinas), com especialidade numa rara atribuição: analítica. Barr era enviado ao estrangeiro quando necessário: quatro anos no Japão, três na Espanha, além de transferências temporárias por toda a Europa, desde a Ucrânia até Portugal e Itália. Ficou acantonado em navios de assalto anfíbio e foi ferido em terra firme em Kosovo. A experiência o deixou ressentido pelo modo como a guerra tornava os soldados insensíveis à vida humana.

Após doze anos na Marinha, ele aceitou uma oferta de emprego na empreiteira de segurança Northrop Grummann e resolveu baixar a poeira e formar família, tapando as tatuagens navais e tornando-se um executivo empresarial. Em

novembro de 2009, surgiu uma nova oportunidade, quando um consultor de segurança chamado Greg Hoglund perguntou a Barr se ele queria ajudá-lo a começar uma nova empresa. Hoglund já administrava uma empresa de segurança digital, a HBGary Inc., e, sabendo da experiência militar de Barr e de sua perícia em criptografia, almejava sua ajuda para formar uma empresa irmã especializada em vender serviços ao governo dos EUA. Chamar-se-ia HBGary Federal, e a HBGary seria proprietária de 10% da nova empresa. Com unhas e dentes, Barr agarrou a chance de se tornar chefe de si mesmo e conviver mais com a esposa e as duas crianças pequenas, mantendo um escritório na própria casa.

No começo, ele saboreou o cargo. Em dezembro de 2009, não conseguiu dormir por três noites consecutivas, com a cabeça repleta de ideias sobre novos contratos. Ligava o computador à uma e meia da madrugada e enviava um e-mail a Hoglund com algumas de suas ideias. Menos de um ano depois, porém, nenhuma das ideias de Barr havia resultado em lucros financeiros. Desesperado por novos contratos, Barr mantinha à tona a diminuta empresa de três funcionários ministrando cursos de “treinamento de mídia social” para executivos, obtendo 25 mil dólares em cada edição. As aulas não eram sobre como manter amizades no Facebook, mas sim sobre como lançar mão das redes sociais, Facebook, LinkedIn e Twitter, para obter informações sobre pessoas – como ferramentas de espionagem.

Em outubro de 2010, enfim veio a salvação. Barr começou tratativas com a Hunton & Williams, empresa jurídica cujos clientes – entre eles a Câmara de Comércio dos EUA e o Bank of America – precisavam de ajuda para lidar com adversários. O WikiLeaks, por exemplo, recentemente havia insinuado a aquisição de uma valiosa coleção de dados confidenciais do Bank of America. Barr e duas outras empresas de segurança fizeram apresentações em PowerPoint nas quais propunham, entre outras coisas, campanhas de desinformação para desacreditar jornalistas que apoiavam o WikiLeaks e ataques cibernéticos ao site do WikiLeaks. Desencavou seus perfis falsos no Facebook e mostrou como podia espionar os adversários, “adicionando” os próprios funcionários da Hunton & Williams e coletando informações sobre suas vidas pessoais. A empresa jurídica pareceu interessada, mas em janeiro de 2011 nenhum contrato havia sido lavrado ainda, e a HBGary Federal precisava de dinheiro.

Então Barr teve uma ideia. Estava prestes a acontecer em São Francisco o B-Sides, conceituado simpósio para profissionais do ramo da segurança.

Se ele desse uma palestra revelando como sua espionagem de mídia social descobrira informações sobre um assunto misterioso, alcançaria uma renovada credibilidade, e quem sabe até mesmo fecharia aqueles contratos.

Barr decidiu que não existia alvo melhor que o Anonymous. Cerca de um mês antes, em dezembro de 2010, o noticiário foi inundado por reportagens falando de um grande e misterioso grupo de hackers que tinha começado a atacar os sites das empresas Mastercard, PayPal e Visa, em retaliação ao corte de financiamento ao WikiLeaks por essas empresas. O

WikiLeaks recentemente havia publicado um conjunto de milhares de cabogramas diplomáticos secretos, e o seu fundador e editor-chefe, Julian Assange, fora preso no Reino Unido, aparentemente por comportamento sexual inadequado.

Hacker era uma palavra famosamente vaga. Podia se referir a um programador entusiasmado ou a um criminoso cibernético. Mas os membros do Anonymous, ou Anons, com frequência eram chamados de hacktivistas – hackers com mensagem ativista. A opinião consensual baseava-se no fato de eles acreditarem que todas as informações deveriam ser livres e, caso você discordasse, podiam muito bem invadir o seu site.

Afirmavam não dispor de estrutura nem de líderes, além de não constituírem um grupo, mas sim “tudo e nada”. A descrição mais aproximada parecia ser “marca, estilo” ou “ação coletiva”. Suas poucas regras lembravam as do filme *Clube da luta*: não falar sobre o Anonymous, nunca revelar sua identidade verdadeira e não atacar a mídia, já que ela podia ser fornecedora de uma mensagem. Naturalmente, o anonimato facilitava a realização de atos ilegais, como invadir servidores, roubar dados de clientes de uma empresa ou derrubar um site e em seguida desfigurá-lo. Coisas que podem levar a uma pena de dez anos na cadeia.

Mas o pessoal do Anonymous parecia não se importar. Afinal de contas, contavam com a força e a proteção dos números e postavam seu slogan nefasto em blogs, sites hackeados ou seja lá onde pudessem: Somos Anonymous Somos Legião

Não perdoamos Não esquecemos Esperem por nós.

Seus panfletos e mensagens digitais mostravam o logotipo de um homem sem cabeça trajando terno e cercado por ramos da paz (ao estilo dos ramos de oliveira

do símbolo da ONU), supostamente inspirado na pintura surrealista de René Magritte, aquela com um sujeito de chapéu-coco e a maçã verde. Muitas vezes incluíam a máscara lasciva de Guy Fawkes, o revolucionário londrino adornado no filme *V de vingança* e agora símbolo de uma horda rebelde e sem rosto. Era impossível quantificar os membros do Anonymous, mas não eram apenas dezenas, nem mesmo centenas de pessoas. Em dezembro de 2010, milhares de pessoas do mundo todo tinham visitado suas principais salas de bate-papo para participar dos ataques ao PayPal, e outras milhares visitavam habitualmente os blogs relacionados ao Anonymous e novos sites, como AnonNews.org. Todo mundo no ramo de segurança cibernética comentava sobre o grupo de hacktivistas, mas ninguém parecia saber quem era esse pessoal.

Barr ficou intrigado. Havia observado crescer a atenção mundial em relação a esse grupo misterioso e visto relatórios de dezenas de ataques e detenções nos EUA e pela Europa afora. Mas ninguém fora condenado, e os líderes do grupo não tinham sido rastreados. Barr acreditava que podia fazer melhor que o Federal Bureau of Investigation – talvez inclusive ajudar o FBI – com sua perícia em espionagem via mídia social. Rastrear o Anonymous era arriscado, mas Barr imaginava que, se o grupo se voltasse contra ele, o pior que podiam fazer seria derrubar o site da HBGary Federal por algumas horas – na pior das hipóteses, por alguns dias.

Começou espreitando as salas de bate-papo on-line onde os sectários da organização se reuniam. Criou um nickname para si mesmo, primeiro AnonCog, depois CogAnon. Misturou--se, utilizando o jargão do grupo e fingindo ser um jovem recruta ansioso para atacar uma ou duas empresas.

Paralelamente, em silêncio, tomava nota do nickname dos outros na sala de bate-papo. Havia centenas, mas prestou atenção nos visitantes habituais e naqueles mais participativos. Quando essas pessoas saíam da sala de bate-papo, ele também anotava o horário. Depois entrava no Facebook. A essa altura, Barr já havia criado várias personas falsas no Facebook e “feito amizade” com dezenas de pessoas do mundo real que abertamente declaravam apoiar o Anonymous. Se um desses amigos súbito se tornasse ativo no Facebook logo após a saída de um nickname do bate-papo do Anonymous, Barr calculava que seria a mesma pessoa.

No fim de janeiro, ele dava os retoques em um documento de vinte páginas com nomes, descrições e informações de contato de suspeitos apoiadores e líderes do

grupo Anonymous. Em 22 de janeiro de 2011, Barr enviou um e-mail para Hoglund, endereçado à copresidente da HBGary Inc., Penny Leavy (esposa de Hoglund) e para o vice-presidente da HBGary Federal, Ted Vera, tratando da iminente palestra no simpósio B-Sides sobre o grupo Anonymous. O maior benefício dela seria atrair a atenção da imprensa. Usando falsa identidade, ele também mencionaria a algumas pessoas no Anonymous a pesquisa de um "suposto especialista em segurança cibernética" chamado Aaron Barr.

– Isso vai gerar um grande debate nos canais de bate-papo do Anonymous, que também são frequentados pela imprensa – contou Barr a Hoglund e Leavy.

Portanto, mais cobertura de imprensa sobre a palestra. E acrescentou: – Mas também vai nos tornar um alvo. Ideias?

A resposta de Hoglund foi sucinta: – Bem, não gostaria de ser alvo de um ataque de negação de serviço distribuída. E se a gente for alvo de um ataque desses, o que fazemos?

Como fazer do limão uma limonada?

Hoglund se referia ao DDoS, tipo de ataque no qual um conjunto de computadores era coordenado para dominar um site com tanto tráfego que temporariamente o tirava do ar. Era a modalidade de ataque mais popular do grupo Anonymous. Como acertar um soco no olho de alguém. Você fica de olho roxo e dolorido, mas não morre disso.

Barr decidiu que a melhor coisa a fazer era estabelecer contato direto com a imprensa antes de sua palestra. E procurou Joseph Menn, repórter do *Financial Times* sediado em São Francisco, oferecendo-lhe uma reportagem sobre como os dados obtidos por ele tinham o potencial de conduzir a mais detenções de "protagonistas" do grupo hacktivista.

Forneceu a Menn uma prévia de suas descobertas: das várias centenas de participantes dos ataques cibernéticos do Anonymous, somente por volta de trinta mostravam atividade constante, e apenas dez pessoas mais experientes tomavam a maioria das decisões. Os comentários de Barr e o relato de sua investigação sugeriam pela primeira vez que o grupo possuía uma hierarquia e não era tão "anônimo" quanto se pensava. O jornal publicou a reportagem na sexta-feira, 4 de fevereiro, com a manchete "Ciberativistas ameaçados de prisão", e citou Barr.

Ao ver o artigo publicado, Barr começou a se empolgar e mandou uma mensagem a Hoglund e Leavy com o assunto: “A história está realmente tomando forma”.

– Devemos postar isso na página inicial e enviar alguns tweets – respondeu Hoglund. – “A HBGary Federal aumenta a altura da barra em termos de agência de inteligência privada.” O trocadilho com “barra” não é mera coincidência *lol*.

No finzinho da sexta-feira, inspetores da divisão de crimes eletrônicos do FBI já tinham lido o artigo e entrado em contato com Barr, perguntando se ele não gostaria de compartilhar suas informações. Concordou em se encontrar com eles na segunda-feira, no dia seguinte ao Super Bowl. Mais ou menos no mesmo horário, um pequeno grupo de hackers do Anonymous também havia lido a reportagem.

***

Eles eram três pessoas, em três locais diferentes do mundo, e tinham sido convidadas a participar de um bate-papo on-line. Seus nicknames eram Topiary, Sabu e Kayla, e ao menos dois deles, Sabu e Topiary, se encontravam pela primeira vez. A pessoa que os convidara atendia pelo nickname de Tflow e também estava na sala. Ninguém ali sabia o nome, a idade, o sexo nem o domicílio verdadeiro dos outros. Dois deles, Topiary e Sabu, começaram a utilizar seus nicknames em salas de bate-papo públicas há apenas um ou dois meses. Só conheciam fragmentos de fofoca uns dos outros e sabiam que cada um deles acreditava no grupo Anonymous. Em essência era isso.

A sala de bate-papo estava bloqueada, ou seja, ninguém podia entrar a menos que fosse convidado. A conversa a princípio foi tímida, mas em poucos minutos todo mundo participava. As personalidades começaram a emergir. Audacioso e atrevido, Sabu utilizava gírias como *yo* e *my brother.*

Nenhum dos outros da sala sabia que ele era nascido e criado em Nova York, com raízes em Porto Rico. Aprendera a hackear computadores na adolescência, subvertendo a conexão discada da família para conseguir acesso grátis à internet. Depois, no final dos anos 1990, aprendeu mais truques em fóruns de hackers. Por volta de 2001, o nickname Sabu tinha saído de cena; agora, quase uma década depois, ressurgia. Sabu era o veterano peso-pesado do grupo.

Infantil e cordial, mas arguta como só ela, Kayla afirmava ser do sexo feminino

e, quando lhe perguntavam, declarava ter dezesseis anos. Muitos supunham que ela mentia. Embora houvesse muitos hackers jovens no Anonymous e muitas mulheres que o apoiavam, jovens hackers do sexo feminino eram raras. Ainda assim, se fosse mentira, era bastante elaborada.

Falava pelos cotovelos e fornecia muitos detalhes sobre sua vida pessoal: trabalhava num salão de beleza e nas horas vagas ganhava grana extra como babá. Tirava férias na Espanha. Inclusive declarava que Kayla era seu nome verdadeiro, mantido como forma de desdenhar todos que tentassem identificá-la. Paradoxalmente obsessiva em relação à privacidade de seu computador, ela nunca digitava o nome verdadeiro em seu netbook, no caso de as atividades do teclado serem monitoradas (keylogging), não tinha disco rígido físico e inicializava a partir de um diminuto microcartão SD que ela podia engolir rapidamente se a polícia batesse à sua porta.

Corria o boato de que um dia ela havia esfaqueado a webcam, só para evitar que alguém hackeasse o seu PC e a filmasse sem que ela notasse.

Em se tratando de hackeagem, Topiary era o menos habilidoso do grupo, deficiência compensada por outro talento: a sagacidade.

Autoconfiante e quase sempre fervilhando de ideias, Topiary utilizava a língua afiada e uma rara queda para a promoção pública para lentamente escalar os degraus das salas de planejamento secretas nas redes de bate-papo do Anonymous. Enquanto outros se esforçavam para escutar na porta, Topiary logo era convidado a entrar. Depositavam tanta confiança nele que os operadores da rede lhe pediam que escrevesse as declarações oficiais do Anonymous de cada ataque contra o PayPal e a Mastercard. Escolhera seu nickname por capricho. Cultuava *Primer*, filme de baixo orçamento sobre viagem no tempo, e, quando ficou sabendo que o próximo projeto do diretor seria chamado *A Topiary*, simpatizou com a palavra, alheio a seu significado (poda artística de arbustos).

Programador habilidoso, Tflow, o sujeito que convidou todos a entrar, na maior parte do tempo ficava calado, seguindo rigidamente o costume do Anonymous de nunca falar sobre si mesmo. Estava na organização há pelo menos quatro meses, um bom tempo para entender a cultura e os principais componentes do grupo. Conhecia melhor do que ninguém os canais de comunicação e o elenco de hackers adjuvantes. Como seria de se esperar, foi ele que levantou a lebre: alguém tinha de tomar alguma providência em relação a esse tal de Aaron Barr e

sua “pesquisa”. Barr afirmara que existiam líderes no Anonymous, uma inverdade. Isso significava que a pesquisa dele provavelmente estava errada. Mas havia a citação da reportagem do *Financial Times*, dizendo que Barr havia “coletado informações sobre os líderes principais, inclusive muitos de seus nomes verdadeiros, e que eles podiam ser presos se as autoridades responsáveis pela aplicação da lei conseguissem esses dados”.

Ora, isso representava outro problema: se os dados de Barr realmente estivessem certos, os Anons poderiam correr risco. O grupo começou a urdir planos. Primeiro, tinham de esquadrinhar o servidor que administrava o site da HBGary Federal e verificar qualquer vulnerabilidade.

Com sorte, encontrariam uma brecha para penetrar, e, assim, tomar o controle e substituir a página inicial de Barr por um gigantesco logotipo do Anonymous e um recado avisando que não mexessem com o grupo.

Naquela tarde, alguém pesquisou “Aaron Barr” no Google e descobriu seu retrato corporativo oficial: cabelo penteado para trás, terno e um olhar atento à câmera. O grupo riu quando viu a foto. Ele parecia tão... sério. E

cada vez mais com a aparência de presa fácil. Em seguida, Sabu começou a escrutinar o HBGaryFederal.com para encontrar um ponto de penetração.

Eis que o site de Barr era administrado por um sistema de postagem criado por um desenvolvedor terceirizado, que tinha um bug dos grandes. Sorte é para quem tem.

Embora o seu trabalho fosse ajudar outras empresas a se proteger contra ataques cibernéticos, a própria HBGary Federal mostrou-se vulnerável a um método simples de ataque denominado injeção de SQL, que tinha como alvo as bases de dados, que consistem em uma das muitas tecnologias essenciais que impulsionam a internet. Armazenam senhas, emails corporativos e uma vasta gama de outros tipos de dados. O uso da linguagem de consulta estruturada (SQL, muitas vezes pronunciada erroneamente como “sequel”) era um jeito popular de obter e manipular as informações nas bases de dados. A injeção de SQL funcionava por meio de “injetar” ordens em SQL no servidor anfitrião do site para obter informações que deviam estar ocultas. Em essência, usava a linguagem contra si mesma. Como resultado, o servidor não reconhecia os caracteres digitados como texto apenas, mas também como ordens que deviam

ser executadas. Às vezes isso pode ser alcançado apenas digitando ordens na barra de pesquisa de uma página inicial. A chave era encontrar a barra de pesquisa ou a caixa de texto que representasse um ponto fraco e permitisse a entrada.

Essa ação podia ser devastadora para uma empresa. Se o DDoS

significava um soco no olho, a injeção de SQL secretamente removia os órgãos vitais de alguém durante o sono. A linguagem necessária para isso, uma série de símbolos e palavras--chave como “SELECT”, “NULL” e “UNION”, ainda que obscura para gente como Topiary, para Sabu e Kayla era brincadeira de criança.

Agora que tinham invadido, os hackers precisavam extrair os nomes e as senhas de gente como Barr e Hoglund, que detinha o controle dos servidores do site. Sorte grande outra vez. Encontraram uma lista de nomes de usuários e senhas dos funcionários da HBGary. Mas aqui surgiu um obstáculo. As senhas estavam criptografadas pela técnica MD5. Se todas as senhas administrativas fossem demoradas e complicadas, seria impossível quebrá-las, e a diversão dos hackers teria chegado ao fim.

Sabu escolheu três hashes (extensas séries de números aleatórios) correspondentes às senhas de Aaron Barr, Ted Vera e outro executivo chamado Phil Wallisch. Esperava que os hashes fossem incrivelmente difíceis de decifrar, e, ao mostrá-los à equipe, não ficou surpreso quando ninguém conseguiu desvendá-los. Numa derradeira tentativa, ele os carregou na web, num fórum sobre quebra de senhas popular entre os hackers – o Hashkiller.com. Em duas horas, os três hashes tinham sido decifrados por voluntários anônimos aleatórios. O resultado de um deles tinha exatamente a seguinte aparência: **4036d5fe575fb46f48ffcd5d7aeeb5af:kibafo33**

Ali mesmo no fim da série de letras e números se encontrava a senha de Aaron Barr. Tentaram kibafo33 para acessar os e-mails dele na HBGary Federal hospedados pelo Google Apps, e bingo. O grupo nem acreditou na sorte que teve. Na sexta-feira à noite, assistiam a um despercebido Barr trocar e-mails felizes com seus colegas sobre o artigo do *Financial Times*.

De veneta, um deles resolveu conferir se kibafo33 funcionava em outro lugar além da conta de e-mail de Barr. Valia a pena tentar. De modo inacreditável para um especialista em segurança cibernética investigando os altamente voláteis

Anonymous, Barr utilizava a mesma senha fácil de quebrar em quase todas as suas contas da web, inclusive no Twitter, Yahoo!, Flickr, Facebook, até mesmo no World of Warcraft. Ou seja, agora existia a oportunidade de “lulz” pura e não adulterada.

Lulz era uma variação do termo *lol* (morrer de rir, do inglês *laugh out loud*), que durante anos marcava o fim de declarações espirituosas como “O

trocadilho com ‘barra’ não é mera coincidência *lol*”. Acréscimo mais recente à gíria de internet, *lulz* ampliava esse sentimento e significava em essência diversão à custa dos outros. Dar um trote no FBI era lol. Dar um trote no FBI e conseguir enviar com sucesso uma equipe da SWAT até a casa de Aaron Barr era lulz.

O grupo decidiu não investir contra Barr naquele dia nem mesmo no sábado. Aproveitariam o fim de semana para espioná-lo e baixar todos os emails enviados e recebidos por ele desde o início da HBGary Federal. Mas havia uma sensação de urgência. Enquanto navegava, a equipe percebeu que Barr planejava se encontrar com o FBI na próxima segunda-feira.

Baixaram todas as informações que puderam e decidiram instalar o caos no domingo, antes do pontapé inicial do Super Bowl. Faltavam sessenta horas.

***

O sábado começou como qualquer outro para Barr. Relaxando e passando o tempo com sua família, enviando e recebendo alguns e-mails em seu iPhone durante o café da manhã, ele não tinha ideia de que uma equipe de sete pessoas do Anonymous estava ocupada mergulhando em seus e-mails, nem no quão empolgados eles estavam ao deparar com uma nova descoberta: a pesquisa de Barr sobre o Anonymous. Era um documento em PDF que começava com uma explanação concisa e decente sobre em que consistia o grupo. Listava sites, uma cronologia de recentes ataques cibernéticos e vários nicknames lado a lado com nomes e endereços da vida real. Os nomes Sabu, Topiary e Kayla não apareciam no documento. No final havia observações apressadas como *Mmxanon – states. . ghetto*. Parecia inacabado. Gradativamente, à medida que percebiam o modo com que Barr utilizara o Facebook para tentar identificar pessoas verdadeiras, se deram conta de que ele talvez não tivesse ideia do que fazia. Parecia que Barr realmente podia acusar algumas pessoas inocentes.

Nesse meio-tempo, Tflow havia baixado os e-mails de Barr em seu servidor, depois esperado umas quinze horas enquanto os compilava em um torrent, diminuto arquivo que se conecta a um arquivo maior num computador anfitrião em outro lugar, neste caso o da HBGary. Tratava-se de um processo utilizado todos os dias por milhões de pessoas mundo afora para baixar software, música ou filmes pirateados, e Tflow planejava colocar seu arquivo torrent no mais popular site de torrents: The Pirate Bay. Isso significava que em breve qualquer pessoa poderia baixar e ler mais de 40 mil e-mails de Aaron Barr.

Naquela manhã, faltando umas trinta horas para o pontapé inicial, Barr rodou algumas checagens no HBGaryFederal.com e, exatamente como havia esperado, percebeu que tinha mais tráfego do que de costume. Isso não significava mais visitantes legítimos, mas o começo de um ataque de DDoS feito pelo Anonymous. Não era o fim do mundo, mas ele entrou no Facebook com o perfil falso de Julian Goodspeak para conversar com um de seus contatos no Anon, indivíduo aparentemente mais velho, que utilizava o apelido CommanderX. A pesquisa de Barr e os debates com CommanderX

o levaram a acreditar que seu nome verdadeiro era “Benjamin Spock de Vries”, embora essa informação fosse inexata. CommanderX, por sua vez, não tinha nem ideia de que um grupinho de hackers já havia invadido os emails de Barr. Respondeu à mensagem instantânea de Barr. Polidamente, Barr perguntava se CommanderX podia fazer algo em relação ao tráfego extra que ele estava obtendo.

– Já terminei minha pesquisa. Não estou determinado a desmascarar vocês – explicou Barr. – Meu foco é a vulnerabilidade das mídias sociais.

Barr queria dizer que a pesquisa dele só tentava mostrar como as organizações podiam ser infiltradas por espionagem nos perfis de seus membros no Facebook, no Twitter e no LinkedIn.

– Não é obra minha – disse CommanderX honestamente. Deu uma conferida no site da HBGary Federal e salientou a Barr que, seja como for, parecia vulnerável. – Espero que você esteja sendo bem pago.

***

Na manhã de domingo, faltando onze horas para o pontapé inicial, Tflow acabara de organizar todos os e-mails de Barr com aqueles dos dois outros

executivos, Vera e Wallisch. O arquivo torrent estava pronto para ser publicado. Agora vinha o prazer de contar a Barr o que eles haviam acabado de fazer. Claro, para executar essa parte do plano, os hackers não lhe contariam tudo de imediato. Melhor diversão (lulz) seria alcançada se brincassem com ele primeiro. A essa altura já tinham percebido que Barr utilizava o apelido CogAnon para conversar com as pessoas nas salas de bate-papo do Anonymous, e que ele morava na capital Washington. Sabu revelou aos demais: – Sabemos tudo sobre ele, desde o número de Segurança Social até sua carreira militar, passando por suas licenças. Sabemos até quantas vezes por dia ele senta no vaso.

Por volta das oito da manhã dominical, horário da costa leste dos EUA, o grupo decidiu deixá-lo um pouco paranoico antes do ataque. Quando Barr entrou na rede de bate-papo AnonOps com o codinome CogAnon, Topiary lhe enviou uma mensagem em particular: – Olá – disse Topiary.

– Oi – respondeu CogAnon.

Noutra janela de bate-papo, Topiary falava em tempo real com outros Anons que se divertiam com sua façanha.

– Diga que você está recrutando para uma nova missão – sugeriu Sabu.

– Tenha cuidado – alertou outro. – Ele pode ficar desconfiado num piscar de olhos.

Topiary voltou à sua conversa com o especialista em segurança, ainda fingindo acreditar que CogAnon era um verdadeiro sectário do Anonymous.

– Estamos recrutando para uma nova operação na área de Washington.

Interessado?

Barr fez uma pausa de vinte segundos.

– Potencialmente. Dependendo do que se trata – respondeu ele.

Topiary colou a resposta na outra janela.

– Hahaha – divertiu-se Sabu.

– Olha só aquela bicha tentando extrair informações com táticas de psique – falou Topiary, referindo-se aos métodos militares de guerra psicológica. A palavra *bicha*, usada de modo tão liberal no Anonymous, já não era mais considerada um insulto de verdade.

– Percebi pelo seu host que você está perto de nosso alvo – contou Topiary a Barr.

Lá em Washington, D.C., Barr sustou a respiração.

– É físico ou virtual? – digitou ele, sabendo muito bem que era virtual, mas sem encontrar mais o que dizer. – Ah, sim... estou perto...

Como cargas d'água tinham descoberto que ele morava na capital?

– Virtual – respondeu Topiary. – Já está tudo preparado.

Topiary repassou a mensagem novamente aos Anons.

– Vou rir muito se ele enviar um e-mail sobre isso – contou ele aos amigos.

Eles não acreditavam no que liam.

– ESSE CARA É UM BAITA TROUXA – exclamou Sabu.

– Quero estuprar o rabo dele – comentou Topiary.

"Estuprar" servidores era um modo habitual de descrever uma hackeagem na rede de alguém. Na rede de bate-papos do Anonymous, Tflow criou uma nova sala de bate-papo, #ophbgary, e convidou Topiary para entrar nela.

– Galera – atalhou um hacker chamado AVunit. – Isso está acontecendo mesmo? Porque é incrível.

De volta à conversa, Barr tentou soar solícito: – Posso chegar à cidade em algumas horas... dependendo do trânsito lol.

Topiary decidiu assustá-lo um pouco mais: – O nosso alvo é uma empresa de segurança – disse ele.

O estômago de Barr se revirou. Ok, então isso significava que o Anonymous

definitivamente escolhera a HBGary Federal como alvo. Abriu seu e-mail e com rapidez digitou uma mensagem para os outros gerentes da HBGary, inclusive Hoglund e Penny Leavy.

– Agora estamos sendo diretamente ameaçados – escreveu. – Amanhã vou informar isso ao FBI.

Sabu e os outros assistiram silenciosamente à remessa da mensagem.

Barr voltou à conversa com Topiary e escreveu: – Ok, só me avisa quando. Mas não sei bem como posso ajudar.

– Isso depende – disse Topiary. – Que habilidades você tem? Precisamos de ajuda para reunir informações sobre a empresa de segurança Ligatt.com.

Barr soltou um longo suspiro de alívio. A Ligatt seguia a mesma linha de trabalho da HBGary Federal, por isso parecia (pelo menos por enquanto) que a empresa dele não era o alvo.

– Ahh, ok, deixa comigo – respondeu Barr sem esconder a gratidão. – Já faz um tempo desde que pesquisei sobre eles. Algo específico? – Nesse ponto ele parecia contente em fazer qualquer coisa que impedisse a HBGary de se tornar um alvo, mesmo que não estivesse falando sério.

Não houve resposta.

Ele digitou:

– Eu não sabia que a base deles era aqui.

Pouco depois, acrescentou: – Cara, estou quebrando a cabeça e não consigo me lembrar por que eles se tornaram tão famosos uns tempos atrás. Lembro que haviam *[sic]*

muitas agressões contra eles.

Nada.

– Continua aí? – indagou Barr.

Topiary tinha voltado ao planejamento com os outros. Não havia muito tempo, e ele precisava escrever a mensagem oficial do Anonymous que substituiria a página inicial do HBGaryFederal.com.

Quarenta e cinco minutos depois, enfim Topiary respondeu: – Vai me desculpar... Fique ligado.

– Ok – escreveu Barr.

Algumas horas depois já era o momento do almoço, cerca de seis horas para o pontapé inicial do Super Bowl, com Barr sentado na sala íntima de seu lar e fitando com horrenda fascinação seu iPhone após se dar conta de que não conseguia acessar os e-mails. Quando correu escada acima para tentar novo contato com CommanderX no Facebook, descobriu que o acesso à sua conta na rede social também estava bloqueado. Ao ver que sua conta do Twitter estava sob o controle de outra pessoa, percebeu a gravidade da situação e o quanto ela era potencialmente constrangedora.

Pegou o telefone e ligou para Greg Hoglund e Penny Leavy a fim de informá-los do que acontecia. Em seguida ligou a seus administradores de TI, que disseram que entrariam em contato com o Google para tentar recuperar o controle do HBGaryFederal.com. Mas não havia nada a fazer quanto aos e-mails roubados.

Às 14h45, Barr recebeu nova mensagem de Topiary: – Certo, algo vai acontecer hoje à noite. Qual a sua disponibilidade?

Faltava pouco tempo para a hora marcada, e ele queria que Barr assistisse de camarote ao fim de sua carreira.

***

Enquanto a noite caía na costa leste, os Anons, em suas próprias casas e em seus próprios fusos horários mundo afora, se preparavam para atacar.

O público começou a lotar o Cowboys Stadium, em Arlington, Texas, ao som das músicas do Black Eyed Peas. Na hora do hino nacional, Christina Aguilera se confundiu com a letra. Enfim, o sorteio. Um jogador do Green Bay Packers recuou o pé e com um chute fez a bola de pele de porco atravessar o campo.

Do outro lado do Atlântico, Topiary assistiu em seu laptop à bola de futebol

americano voar no céu. Sentado em sua cadeira destacada para jogos com um par de fones de ouvido gigantes acomodado no cabelo, agilmente abriu outra janela e fez logon na conta de Barr no Twitter. Seis horas antes, havia bloqueado Barr com a senha kibafo33 e, com a bola finalmente em jogo no Super Bowl, começou a fazer postagens. Não sentiu inibição alguma; não sentiu pudor algum em relação ao que ia fazer. Barr bem que merecia.

– Ok, meus camaradas bichas do Anonymous – postou ele na conta de Barr no Twitter –, enquanto a gente conversa, trabalha para fornecer a vocês a melhor lulz. Fiquem ligados!

E depois:

– O que tá pegando, seus energúmenos. Sou o diretor-executivo de uma empresa merreca e um baita puxa-saco da mídia. LOL dá só uma olhada no site de meu parceiro Greg: rootkit.com.

Declarações que Topiary jamais pronunciaria em voz alta ou cara a cara com Barr. Na vida real, ele é quieto, polido e raramente solta uma praga.

O rootkit.com era o site de Hoglund dedicado a ferramentas de programação capazes de obter acesso invisível a um sistema de computador. Ironicamente, Sabu e Kayla agora também tinham acesso ao administrador do sistema, ou o "root" do rootkit.com. Isso porque Barr havia sido um administrador do sistema de e-mails da empresa, ou seja, "kibafo33" permitiu-lhes resetar as senhas de outras caixas de entrada, inclusive a de Hoglund.

Assim que invadiu a caixa de entrada de Hoglund, Sabu enviou um email como se fosse Hoglund para um dos administradores de TI da HBGary, o finlandês especialista em segurança chamado Jussi Jaakonaho. Sabu desejava acesso ao diretório raiz do rootkit.com.

– estou na europa e preciso ssh no servidor – escreveu Sabu no e-mail para Jaakonaho, utilizando letras minúsculas para sugerir pressa.

SSH significa "secure shell" e se refere a uma interface para acessar um servidor a partir de um local remoto. Quando Jaakonaho indagou se Hoglund (Sabu) estava num computador público, Hoglund (Sabu) disse: – Não, no momento eu não tenho o ip público comigo porque estou na corrida para entrar numa reunião. pelo menos altere minha senha para changeme123 e me forneça IP público, daí

eu consigo acesso ssh e altero minha senha.

– Ok – respondeu Jaakonaho. – Sua senha é changeme123.

E acrescentou com uma carinha sorridente: – Na Europa, mas não na Finlândia?

Sabu resolveu brincar: – Se sobrar um tempo talvez a gente possa se ver... vou passar uns dias na alemanha. obrigado.

A senha não funcionou de imediato, e Sabu precisou enviar novos emails a Jaakonaho com perguntas, inclusive se seu próprio nome de usuário era "greg ou?", antes de Jaakonaho explicar que era "hoglund". Sabu entrou.

Esse foi um exemplo primordial de engenharia social, a arte de manipular alguém para divulgar informações secretas ou fazer algo que ele normalmente não faria.

Agora Sabu e Kayla tinham controle integral do rootkit.com. Primeiro, pegaram os nomes de usuários e as senhas de todas as pessoas que já haviam se registrado no site, depois apagaram completamente seu conteúdo. Agora só havia uma página em branco onde se lia: "Greg Hoglund = dominado". Sabu notou que gostava de trabalhar com Kayla. Ela era simpática e tinha notáveis habilidades técnicas. Sabu mais tarde contou aos outros que *ela* havia realizado a engenharia social com Jussi Jaakonaho, parcialmente porque a ideia de ser "dominado" por uma garota de dezesseis anos só aumentaria o constrangimento da HBGary.

Depois Sabu e Kayla voltaram suas atenções para a HBGaryFederal.com, retirando a página inicial e substituindo-a pelo logotipo do Anonymous (homem sem cabeça vestindo terno). No lugar da cabeça, um ponto de interrogação. No rodapé havia um link que mencionava "Baixe e-mails da HBGary" – o arquivo torrent de Tflow. Agora qualquer pessoa podia ler todos os e-mails confidenciais de Barr a seus clientes com a mesma facilidade com que podiam obter uma canção no iTunes, só que de graça.

Na nova página inicial também havia uma mensagem escrita por Topiary: *Este domínio foi tomado pelo Anonymous com base na cláusula 14*

das Regras da Internet. Saudações, HBGary (empresa de "segurança" computacional). Suas afirmações recentes de ter se "infiltrado" no Anonymous são risíveis. Também nos divertem suas tentativas de utilizar o Anonymous como

meio de atrair atenção da mídia para si mesmo. Que tal isto para atrair a atenção? Tentou morder a mão do Anonymous, e agora a mão do Anonymous esbofeteia seu rosto de cadela.

***

Por volta das 18h45 no horário da costa leste dos EUA, aos vinte e quatro minutos de jogo no Super Bowl, a maior parte da "hackeagem" havia acabado. Nada de comemorações e auês pelo jogo de futebol americano oriundos dos vizinhos de Barr, em sua maioria famílias de gente jovem. O

mundo ao seu redor parecia bizarramente silencioso. Com certa palpitação, ele voltou a entrar nas salas de bate-papo do Anonymous para confrontar seus oponentes. Eles estavam prontos e à espera. Barr viu uma mensagem piscar, um convite para uma nova sala de bate-papo chamada #ophbgary.

Logo vislumbrou um grupo de vários nicknames. Alguns ele reconhecia de sua pesquisa e outros não: junto com Topiary, Sabu, Kayla, apareciam outros (Q, Heyguise, BarretBrown e c0s). O último apelido era de Gregg Housh, Anon de longa data na faixa dos 35 anos que em 2008 ajudara a coordenar a primeira onda de maciços ataques de DDoS do Anonymous contra a Igreja da Cientologia.

Topiary não perdeu tempo.

– Agora estão nos ameaçando diretamente – disse ele a Barr, citando o e-mail anterior. – Não estou certo?

Barr não disse nada.

– Curtindo o Super Bowl, imagino? – comentou Q.

– E aí, Sr. Barr – atalhou Tflow. – Sinto muito pelo que está prestes a acontecer com o senhor e sua empresa.

Por fim, Barr se manifestou: – Imaginei que aconteceria algo desse tipo – digitou ele.

– Tsc, tsc, você não vai gostar do que vai acontecer – avisou Topiary.

Barr tentou persuadir o grupo de que no fundo suas intenções eram as melhores possíveis.

– Cara... você não está entendendo – protestou. – Foi só uma pesquisa sobre as vulnerabilidades da mídia social. Eu jamais ia divulgar os nomes.

– MENTIROSO – agora Sabu entrou na conversa. – Não tem uma reunião com o FBI na segunda de manhã?

– Pode apostar, Sabu – interpôs Topiary.

– Tudo bem. Certo... – reconheceu Barr. – Eles me convocaram.

– Ah, pessoal. O que está prestes a acontecer é uma delícia de bolo – disse Topiary.

Coube a Tflow enfim largar a bomba: – Tenho os e-mails de Barr, Ted e Phil – avisou. – Todas as 68 mil mensagens.

– Esses e-mails vão fazer sucesso – comentou Housh.

– Lol – respondeu Barr inexplicavelmente, como se quisesse manter a conversa em tom ameno ou convencer a si mesmo de que a coisa não era tão ruim quanto pensava. – Ok, pessoal – acrescentou ele –, vocês me pegaram de jeito :).

Pegaram-no, sem dúvida. Topiary desferiu o último golpe: – Bem, Aaron, obrigado por participar deste miniteste social para ver se atrairia atenção para sua empresa com “novidades” sobre o Anon. Você atraiu, drenamos seu sangue e caímos na gargalhada. – Fez uma pausa. – Morra nas chamas. Você está acabado.

***

Já em plena madrugada de segunda-feira, defronte ao laptop em sua escrivaninha, Barr via suas esperanças de uma reviravolta minguarem. Na parede à sua frente havia uma foto comprada por ele em Nova York, em outubro de 2011. Os ataques de 11/9 ainda repercutiam e, após visitar o Marco Zero, ele entrou por acaso numa pequena galeria que vendia fotos amadoras tiradas durante os ataques. Uma se destacava. Ao fundo, o caos das torres desabadas: papéis e tijolos espalhados por todos os lados, pessoas a caminho do trabalho atordoadas e cobertas de caliça, e, em primeiro plano, *Double Check*, a famosa

estátua de bronze do escultor John Seward Johnson, que mostrava um homem de negócios de terno num banco do parque, remexendo na valise aberta. Algo na incongruência da imagem lhe fez gostar instantaneamente dela. Agora, Barr era aquele homem, tão absorto em suas ambições que se tornava alheio ao caos à sua volta.

A postagem em seu Twitter, importante ferramenta de reputação com público, clientela e imprensa, agora tinha virado uma confusão obscena.

Topiary havia publicado dezenas de tweets repletos de palavras de baixo calão e comentários racistas. Na biografia de Barr agora se lia: “Diretor-Executivo da HBGary Federal. Especialista em Operações de Cibersegurança e Informações e BICHA LOUCA”. Pichada sobre sua foto, a palavra *CRIOULO* em letras vermelhas. Topiary não se considerava racista – ninguém no grupo dele se considerava. Mas a pichação fazia sentido perfeito com a cultura subterrânea de humor bruto e bullying cibernético que grassava no Anonymous.

Topiary se empolgou ao postar o endereço domiciliar de Barr. Em seguida, tweetou o número de segurança social de Barr, depois o número de seu celular. Qualquer pessoa com conexão à internet podia ler as informações.

– E aí, pessoal, me enviem mensagens de voz!

E depois o número com o recado “#meligue”.

Logo centenas e depois milhares de pessoas que liam atentamente as salas de bate-papo, os blogs e o Twitter do Anonymous já tinham ouvido falar do que acontecia com Aaron Barr. Clicavam em links para o site dele na web, agora uma tela branca com o logotipo e a mensagem do Anonymous. Acompanhavam a postagem no Twitter e ligavam para o número dele. Não foram poucos os que pegaram sua distinta foto corporativa e a desfiguraram, decapitando-a e colando a cabeça num pôster do 007 para caçoar de seus métodos de espionagem. Outro intumesceu o queixo de Barr para fazê-lo se parecer com o grotesco Forever Alone, conhecido personagem de tirinhas da internet.

Barr não conseguia se desconectar das salas de bate-papo do Anonymous, hipnotizado pelo modo com que as pessoas caçoavam da “bicha” e se incitavam mutuamente para ligarem no celular dele. O seu telefone tocou a noite toda. Atendeu uma vez, só para escutar uma voz feminina dizer algo inaudível e desligar. Houve algumas mensagens de voz silenciosas e uma pessoa que parecia

cantarolar “Never Gonna Give You Up”, a canção de Rick Astley lançada em 1987. Homenagem ao trote popular no Anonymous que consistia em “rickrollear” alguém.

Barr havia pedido reforços. Penny Leavy entrou on-line para tentar a sorte e limpar a barra com os perpetradores dos ataques. A princípio, eles foram cordiais e bem-educados com ela, mas suas solicitações foram recebidas com respostas lacônicas.

– Por favor, não liberem os e-mails da HBGary – implorou ela. – Contêm informações particulares da clientela.

– Não devia enviar e-mails que não gostaria que sua mãe lesse – respondeu Heyguise.

E, seja como for, os e-mails já tinham sido publicados como arquivo torrent no The Pirate Bay.

– Muita gente inocente poderia ter sido presa – Sabu retrucou com raiva.

Antes do ataque, seu recém-formado grupinho de Anons, que havia se encontrado em meio a centenas de outros nas redes de bate-papo do Anonymous, não tinha ideia de que a pesquisa de Barr era tão defeituosa, nem que os e-mails dele seriam tão fáceis de hackear. Na realidade, eles ainda não sabiam que Barr estivera propondo uma campanha caluniosa contra sindicatos trabalhistas e o WikiLeaks para uma agência governamental e um importante banco. A motivação do grupo era a vingança e o desejo, intensificado pela psicologia coletiva, de perseguir qualquer um que parecesse merecer. À medida que mais e mais pessoas vasculhavam os e-mails de Barr e descobriam o que ele fizera com a Hunton & Williams, o ataque repentinamente passou a parecer mais do que justificado, quase necessário para eles. Na comunidade do Anonymous, Sabu, Kayla, Topiary e os outros se tornariam heroicos condutores de justiça vigilante. Barr tinha merecido. Provocara um mundo em que insultar, mentir e roubar eram coisas corriqueiras. Um mundo que trazia emoções eufóricas, diversão e realização, sem praticamente quaisquer consequências no mundo real.

No dia seguinte, em meio a telefonemas de jornalistas, Barr tentava desesperadamente juntar os cacos. Enquanto isso, Topiary, Sabu, Kayla e Tflow se encontraram novamente na sala de bate-papo secreta.

Comemoraram as conquistas, reviveram os acontecimentos, riram e sentiram-se invencíveis. Haviam “dominado” uma empresa de segurança.

No fundo, tinham consciência de que agentes do FBI começariam a tentar descobri-los. Mas, com o passar do tempo, os membros da pequena equipe concluiriam que haviam trabalhado tão bem contra Barr que deveriam fazer tudo de novo contra novos alvos, por lulz, pelo Anonymous e por qualquer outra causa que surgisse no caminho. Nenhuma presa seria grande demais: uma famosa instituição midiática, uma gigantesca empresa de entretenimento – e até mesmo o próprio FBI.

CAPÍTULO 2

William e as raízes do Anonymous Aaron Barr jamais teria deparado virtualmente cara a cara com o Anonymous se não fosse por Christopher Poole, garotinho magro e loiro da cidade de Nova York, e a extraordinária contribuição que ele deu para a internet. Sete anos antes, no verão de 2003, Poole, então com catorze anos, surfava na web em seu quarto, em busca de informações sobre animes japoneses. Como milhares de outros adolescentes americanos, ele era um grande fã. Por fim, descobriu um painel japonês de imagens cor de pêssego dedicado a animes chamado 2channel ou 2chan. Poole nunca vira algo parecido. Fundado em 1999 pelo universitário Hiroyuki Nishimura (que completou 35 anos em 2012), trazia debates sobre animes que se atualizavam com a velocidade de um relâmpago. Poole esperava trinta segundos, apertava F5 para dar um refresh, e súbito a página se reabastecia com uma sequência de novos posts que chegavam até mil. Quase todos os postadores eram anônimos. Ao contrário dos fóruns internéticos em língua inglesa, o 2chan não exigia que você registrasse seu nome em algum campo, e dificilmente alguém se identificava.

No Japão, naquele mesmo verão, os noticiários observaram que o 2chan estava se tornando uma janela deveras constrangedora que revelava o ponto nevrálgico da nação. Debates sobre animes extrapolaram para conversas sobre garotos assassinando seus professores, atacando seus chefes ou explodindo um jardim de infância local. O site se tornava uma das páginas da web mais populares do país.

Poole desejava um local para conversar em inglês sobre animes, e o 2chan começou a bloquear os postadores de língua inglesa. Assim, ele resolveu clonar

o 2chan, copiando seu código HTML disponível publicamente, traduzindo-o para o inglês e fazendo adaptações a partir dessa base. Construiu tudo pelo próprio computador de seu quarto e batizou o site de 4chan. Quando um amigo virtual perguntou a Poole, que atendia pelo nickname de moot, qual seria a diferença entre o 4chan e o 2chan, ele respondeu com certa petulância: – É DUAS VEZES O CHAN, SEU IMBECIL.

Em 29 de setembro de 2003, Poole registrou o domínio 4chan.net e o anunciou no Something Awful, fórum da web no qual ele já era figurinha carimbada. O título do novo tópico: “4chan.net – o 2chan.net em inglês!”.

O 4chan possuía quase o mesmo leiaute do 2chan: fundo simples em pêssego, texto em vermelho-escuro, quadros sombreados para novos tópicos de discussão. Até hoje, tanto o 4chan quanto o 2chan pouco modificaram seus designs, apenas acrescentando alguns esquemas de cores. Após o 4chan ser aberto ao público, o Raspberry Heaven – centro de discussão de animes falado em inglês – começou a fazer link com ele, como também o Something Awful. De imediato, as primeiras centenas de visitantes o adotaram. Painéis de discussão eram listados alfabeticamente na parte superior do site: *a* para anime, *f* para fotografia e assim por diante. Poole tinha configurado o *b*, o painel “aleatório” que se tornaria o recurso mais importante do 4chan, logo nos dois primeiros meses. Numa discussão com os primeiros usuários, moot comentou que *b* era “o coração pulsante deste site”, mas acrescentou que se tratava de “um recipiente para retardados”. O painel randômico era livre para todos.

Primeiro, Poole configurou o 4chan de modo a qualquer pessoa conseguir postar um comentário com um nickname. Isso continuou até o começo de 2004, quando um usuário do 4chan e programador de PHP, que atendia pelo nickname de Shii, se irritou com os nicknames obrigatórios.

Naquele ano, Shii publicou um ensaio sobre o valor do anonimato em painéis de imagens, apontando o 2chan do Japão como exemplo de local onde o anonimato combatia a vaidade e impedia que os usuários desenvolvessem panelinhas e status de elite. Quando um site obrigava as pessoas a se registrarem com apelido, também afastava pessoas interessantes com vidas ocupadas, atraindo, em vez disso, aquelas com tempo de sobra e com tendência a fazer comentários asquerosos ou absurdos. “Num fórum anônimo”, escreveu, “a lógica supera a vaidade.”

Poole viu o post, gostou dele e nomeou Shii como moderador e administrador dos painéis do 4chan. Solicitou que outro admin desenvolvesse um novo recurso chamado “Forced_Anon” em diferentes partes do site. Muitos usuários ficaram profundamente aborrecidos quando o Forced_Anon foi adotado em alguns desses painéis, e alguns digitavam em “tripcodes” com o objetivo de driblar o anonimato compulsório e utilizar um nickname. Outros, que abraçaram o recurso do anonimato, caçoaram dos que assinavam e os batizaram de “tripfags”.

Talvez de modo profético, instalou-se o conflito. Apoiadores do anonimato e dos *tripcodes* começaram a criar tópicos separados, convocando todos que apoiavam seu próprio ponto de vista a postar uma mensagem e demonstrar apoio, ou a começar tópicos “tripcode *versus* anon”. Os *tripfags* começaram a caçoar dos usuários anônimos como se fossem uma só pessoa chamada “Anonymous”, ou jocosamente se referindo a eles como “mente colmeia”. Ao longo dos anos seguintes, porém, a brincadeira perderia a graça, e a ideia do Anonymous como entidade única cresceria além de alguns poucos tópicos de discussão. Poole ficaria em segundo plano à medida que o Anonymous ganhava vida própria. Ao longo dos anos, o *b* em específico atrairia uma base fiel de usuários cujas vidas giravam em torno das oportunidades de diversão e aprendizado que o painel lhes fornecia. Esses usuários, em sua maioria, provinham de países onde se falava inglês, tinham entre dezoito e trinta e cinco anos e pertenciam ao sexo masculino. Um deles se chamava William.

***

William entreabriu os olhos e fitou à frente. Naquela gélida tarde de fevereiro de 2011, o assíduo usuário do 4chan avaliou a possibilidade de sair da cama. Noutra parte do mundo, Aaron Barr tentava reparar os danos causados por um grupo de hackers do Anonymous. William também pertencia ao grupo e, às vezes, gostava de atacar pessoas na web. Não possuía as habilidades técnicas de Sabu e Kayla, mas ainda assim seus métodos conseguiam causar impacto.

Preso com tachinhas, um lençol tapava a parede do quarto, desde o teto até o chão. Outros lençóis estavam suspensos no cômodo. Na ponta da cama havia um conjunto de prateleiras baixas, com uma pilha de entulhos à esquerda e uma janela à direita, oculta pela persiana do tipo blecaute. O

quarto era seu casulo invernal; a cama, a rede de segurança. Aos 21, ele se conectava ao 4chan quase todos os dias desde que abandonara o colégio, seis

anos antes, às vezes durante horas a fio. Por vários motivos, ele nunca se mantivera num emprego em tempo integral por um período superior a poucos meses. E bem que queria. Mas profundos conflitos dominavam William. No mundo real, era gentil com a família e leal aos seus amigos.

Como usuário anônimo do painel interativo *b* do 4chan, ele se tornava mais sombrio, até mesmo peçonhento.

O 4chan era mais do que um simples site de visita rápida para diversões aleatórias visitado por milhões de pessoas diariamente. Para William e um fiel núcleo de participantes, tratava-se de uma escolha de vida. Além da pornografia, das piadas e das imagens chocantes, oferecia alvos para brincadeiras. No 4chan, brincar com alguém ou perturbá-lo seriamente era chamado de "arruinar a vida alheia". Lançando mão de muitas das mesmas táticas de investigação na internet utilizadas por Aaron Barr, William encontrava pessoas nos fóruns de discussão do 4chan que estavam sendo ridicularizadas ou mereciam sê-lo. Em seguida, ele as "doxeava", ou seja, descobria suas identidades verdadeiras, enviava-lhes ameaças pelo Facebook ou descobria seus familiares e também os assediava. A sorte grande era conseguir fotos nuas, que podiam ser enviadas a familiares, amigos e colegas de trabalho apenas para constrangê-los, ou até mesmo para chantageá-los.

Arruinar a vida das pessoas dava emoção a William e uma sensação de poder sem paralelos no mundo exterior. A única outra ocasião em que sentia algo parecido era quando escapava de casa na calada da noite, encontrava-se com velhos amigos e espargia grafites coloridos em muros e trens locais. O grafite se tornara sua amante nas noites de verão. No inverno, era o 4chan e agora, às vezes, as atividades mais amplas do Anonymous.

O 4chan oferecia certo conteúdo domesticado e discussões amadurecidas, em meio a uma mixórdia de pornografia, sangue e insultos constantes entre usuários que criavam uma palpitante massa de negatividade. Às vezes provocava assustadores pensamentos suicidas em William. Mas o 4chan também o mantinha vivo. Às vezes, o rapaz sentia a depressão tomar conta e varava a noite acordado, conectado ao site, e no restante do outro dia permanecia insone. Quando pensamentos suicidas o dominavam, ele se escondia no sono, na segurança do leito, embaixo do cobertor, junto à parede coberta pelo lençol.

William foi criado numa residência inglesa de baixa renda. Os pais dele se

conheceram no YMCA, depois que a mãe, imigrante do sudeste asiático, fugira de um casamento infeliz e se tornara temporariamente sem-teto. O

casal se separou quando William tinha sete anos, e ele preferiu morar com o pai. Apresentava mau comportamento na escola, estatisticamente uma das piores do país. Desaforava professores ou simplesmente saía da sala de aula. Depois veio uma interminável sequência de idas à coordenação.

William não era um pária social; simplesmente não entendia por que estudar. Após ser expulso aos catorze anos, recebeu a permissão de voltar, mas no ano seguinte, em outubro de 2004, decidiu abandonar completamente os estudos.

Nessa ocasião, o rapaz já havia criado uma nova vida virtual. Tudo começou quando ele e alguns amigos passaram a visitar sites frequentados por pedófilos, onde se registravam com nomes de usuário como “sexy_baby_girl” para atrair a atenção. Pediam aos homens que ligassem a webcam, e, se eles apareciam pelados, como em geral acontecia, os rapazes caíam na gargalhada. Para aumentar o perigo, colavam um alerta oficial dos Serviços de Proteção à Criança no Messenger MSN, o popular programa de bate-papos da Microsoft, acrescentando que tinham o endereço IP do homem, e a série de números que correspondia ao seu computador, o que eles inventavam. Em geral, o homem simplesmente interrompia a conexão, mas eles se divertiam ao saber que ele estava provavelmente aterrorizado e que, talvez, merecesse isso.

Era sempre William quem incentivava os amigos a prolongar a brincadeira ou deixar o alvo masculino mais excitado sexualmente. Por fim, sem sair de casa, passou a realizar trotes no iSketch.com, TeenChat.net e em viveiros de pervertidos sexuais naquela época. As imagens já não chocavam mais o jovem, que deparara com pornografia pela primeira vez aos onze anos.

Em breve começou a passar muitas horas do dia imerso na denominada Deep Web, composta por mais de um trilhão de páginas da internet que não podem ser indexadas pelos mecanismos de busca tipo Google. Assim como fóruns dinâmicos da web, a maior parte de seu conteúdo é ilegal. William se viu preso numa arapuca diária de imagens sanguinolentas, horrendos acidentes de trânsito e pornografia feita em casa, tudo no computador da família. Se alguma imagem depravada piscava na tela, o menino entrava em pânico e rapidamente fechava a janela do navegador. Mas na mesma noite ele voltaria a deparar com elas. E depois de novo na noite seguinte. Por volta dos quinze anos de idade, enfim

descobriu o 4chan, o site que se tornaria seu mundo nos próximos anos.

***

Muita gente envolvida com o Anonymous afirma ter travado o primeiro contato com o grupo por meio do 4chan. Esse foi o caso de William e Topiary: os dois descobriram o site na mesma época, em 2005. Naquele ano, o lema “Somos Legião” já surgia internet afora. No 4chan, eram raros os usuários tripcode. Um ano após Shii ter escrito seu ensaio, o anonimato obrigatório se tornara amplamente aceito no painel de imagens. Qualquer pessoa considerada tripfag era rapidamente desacreditada e caçoada.

O 4chan estava no auge, poço fértil de imagens depravadas e piadas repulsivas e, ao mesmo tempo, fonte de notável e desenfreada criatividade.

O pessoal começou a criar memes na internet – imagens, vídeos ou expressões que se tornavam piadas internas para milhares de usuários on-line após serem transmitidas para um número suficiente de amigos e outros painéis de imagens. Muitas vezes esses memes eram hilários.

Lado a lado com vídeos de terror e abuso explícitos, imagens de nudez feminina e masculina e personagens de anime, havia fotos intermináveis de gatos domésticos. Em 2005, os usuários do *b* tinham começado a incentivar uns aos outros a colocar legendas engraçadas sob fotos felinas fofas aos sábados (o que ficou conhecido como *Cat* urday). Essas macroimagens, fotografias com letras brancas em cima e comentário espirituoso embaixo, acabaram conduzindo ao meme LOLcats. Foi o primeiro de muitos memes a obter popularidade fora do 4chan, por fim se espalhando em outros sites da web e até mesmo em livros.

Milhares de macroimagens foram feitas e depois postadas no 4chan e noutros painéis de imagens todos os dias. Algumas poucas viralizavam, transformando-se em expressões repetidas por milhões de outras pessoas durante anos a fio. Uma pessoa autora de uma macroimagem que se transformou num meme bastante conhecido foi Andrew “weev”

Auernheimer. Ex-hacker e troll da internet, ele encontrou uma foto de arquivo de um thomem vibrando com o punho em riste diante do computador. Digitou as palavras “Internet é um negócio sério” sobre a foto.

O meme agora já é mais do que um clichê: tornou-se um slogan cibernético.

Weev afirma ter participado da própria discussão on-line na qual o termo *lulz* nasceu. Em 2003, um moderador de fórum de outro site comentava sobre algo engraçado quando de repente digitou “lulz!”. Outros na sala de bate-papo começaram a repetir a interjeição e a partir daí ela se espalhou.

– Era bem superior a lol – lembrou-se Weev mais tarde.

Por fim, “Eu fiz por lulz” ou apenas “por lulz” se tornaria um símbolo de cultura internética e do próprio Anonymous, assim como um slogan sempre popular no 4chan.

Embora o site muitas vezes pareça superficial e obtuso, o 4chan começou a desenvolver uma fiel legião de usuários apaixonados. Tornou-se o maior dos painéis de imagens falado em inglês da web, e seus usuários aceitavam uns aos outros não apesar de seus desejos e humores ofensivos, mas por causa deles. Uma atração do *b* era que, como clube secreto, não podia ser anunciado em lugar algum. As pessoas apareciam por meio do boca a boca ou a partir de links de sites semelhantes e eram instadas a não convidar pessoas que não se enquadrassem naquela cultura, as quais eram chamadas de “câncer de newfags”. Isso explica o fato de as regras número 1

e 2 das famosas 47 Regras da internet, supostamente originadas a partir de debates em 2006 no *b* e em redes de bate-papo em tempo real, serem “Não falar sobre o *b*” e “Não falar sobre o *b*”.

Os componentes do 4chan logo desenvolveram sua linguagem própria, com expressões como “an hero”, que significava cometer suicídio. Essa expressão entrou em uso quando alguns usuários do MySpace fizeram uma página em tributo a um amigo que havia cometido suicídio. Um deles, provavelmente desejando digitar a frase “ele era *a hero* de verdade”, em vez disso escrevera “ele era *an hero* de verdade”. Logo se tornou uma tendência no site descrever alguém como “an hero” – antes de se metamorfosear na forma verbal: “Estou à beira de cometer *an hero*”.

Também havia “u jelly?”, modo de indagar se alguém era jealous (ciumento), e “cheese pizza” (CP, pizza de queijo), gíria para pornografia infantil. Usuários mais argutos do 4chan começavam tópicos sobre pizzas de queijo literais, inclusive com fotos de pizzas, e acrescentavam links a um arquivo de pornografia infantil dentro do código de imagem – acessados apenas ao se

abrirem as imagens de pizza em programas de texto em vez de em visualizadores de imagens.

O painel *r* servia para requerimentos ou solicitações quaisquer, desde fotos até conselhos sobre o que fazer ao levar um fora. Pr0nz, n00dz e regra 34 significavam pornografia. A regra 34 era outra das 47 Regras da internet, que declarava apenas: “Se algo existe, existe pornografia nesse algo”. Assim, fazer uma regra 34 no *r* sobre uma celebridade feminina significava solicitar pornografia, talvez alterada digitalmente, de uma cantora ou atriz. “Moar!” significa more (mais!) e “lulz”, é claro, significava diversão à custa dos outros, geralmente envolvendo constrangimento.

Os postadores originais, ou OPs, de cada tópico eram a única semelhança com hierarquia numa comunidade anárquica sob os demais pontos de vista. Ainda assim, eles podiam apenas esperar respostas irreverentes a seus posts e, muito habitualmente, insultos. “OP é uma bicha” era uma resposta comum, e não havia exceções. Comentários racistas, homofobia e gracejos sobre pessoas com deficiências eram a norma. Costumeiramente os usuários se chamavam uns aos outros de “nigger”, “faggot” ou apenas “fag”. Novos usuários do 4chan eram newfags; os antigos, oldfags; britânicos, britfags; homossexuais, fagfags ou gayfags.

Formavam ali um mundo implacável, mas bizarramente tolerante. Tornou-se um tabu identificar o sexo, a raça ou a idade de alguém. Ao privar os usuários do 4chan das características que os identificavam, todos se sentiam mais parte da coletividade, e por isso muitos voltavam.

Fonte das histórias e imagens menos palatáveis que os usuários podiam encontrar, o *b* foi chamado de “o ânus da internet” pela Encyclopedia Dramatica (ED), depósito satírico on-line dos memes da internet que tinha a aparência do Wikipedia, mas muito mais desbocado. A exemplo do anonimato dos usuários, o *b* era uma tábula rasa sem rótulo – os usuários possuíam liberdade completa para decidir o conteúdo e a direção a seguir.

Ao longo do tempo, frequentadores habituais, que se denominavam *b*rothers ou *b*tards, criaram um mundo próprio. Um dos tópicos mais comuns que as pessoas começaram a postar no *b* (além de pr0nz) intitulava-se “bawww”. Aqui os usuários apelavam para o lado solidário do 4chan, com títulos como “acabo de levar um fora da namorada, tópico bawww, por favor?”, postados com a foto de

um rosto tristonho. Esse era um raro exemplo em que os usuários do *b* ofereciam aconselhamento e solidariedade sinceros ou fotos engraçadas para animar o OP. Não havia como ter certeza, mas as pessoas que visitavam o 4chan aparentavam ser peritas em tecnologia, entediadas e muitas vezes emocionalmente bizarras.

Quando o Anonymous começou a atrair a atenção do mundo em 2008, a maioria das pessoas que o apoiavam tinha passado algum tempo no 4chan, e se considera que em torno de 30% dos usuários do 4chan são visitantes habituais do *b*.

A primeira vez em que William deparou com o 4chan, já vira coisa bem pior em sites como myg0t, Rotten e o YNC. Mas ficava horas no *b*, pois o painel era tão imprevisível, tão dinâmico. Anos mais tarde, dia após dia, William se maravilhava pelo quanto ainda se surpreendia ao abrir o *b*, agora sua página inicial. Navegar era uma loteria – você nunca sabia quando alguma coisa lasciva, sórdida ou engraçada ia surgir. Havia algo unificador nesse completo niilismo. À medida que a mídia e outros observadores externos começaram a criticar as atividades dos usuários do *b*, muitos também foram dominados por um sentimento de honradez.

Ainda havia duas coisas inaceitáveis no *b*. Uma delas era pornografia infantil (embora o fato seja motivo de discussão entre alguns usuários radicais que gostam do modo com que isso afasta os newfags), e a outra, os moralfags. Chamar alguém de “moralfag” no 4chan era o pior insulto possível. Alguns visitantes do *b* discordavam de sua depravação e tentavam mudá-la ou, pior, tentavam fazer com que o *b* atuasse em outro tipo de transgressão. Sabiam que centenas de usuários do *b* em geral concordavam em massa sobre uma questão de um tópico de discussão. E às vezes não só concordavam com a ideia, mas concordavam em tomar alguma medida. Embora o *b* fosse completamente imprevisível, às vezes seus usuários pareciam contribuir para uma espécie de consciência coletiva. Juntos criavam piadas e juntos ridicularizavam OPs de quem eles não gostavam. Querendo ou não, moralfags por fim se aproveitavam dessa habilidade de agir em sincronia, persuadindo o *b* a participar de protestos.

O *b* acabou se tornando famoso pelo modo com que um postador conseguia inspirar outros no painel a se unirem para realizar um trote ou “ataque” em massa. Em geral, alguém começava um tópico sugerindo um assunto sobre o qual o *b* deveria fazer algo a respeito. O melhor jeito de coordenar um ataque nunca era sugeri-lo diretamente. Em vez disso, o ideal era insinuar que um ataque já estava prestes a acontecer. A frase “E aí, galera, que tal fazermos isso?”

quase sempre recebia como resposta um chega para lá: “GTFO” [*get the fuck out*], enquanto a frase “Isso está acontecendo agora, participe” atraía a multidão. Se um postador havia preparado uma imagem com instruções, tipo uma imagem digital com instruções sobre como participar, era mais provável que tivesse força permanente, pois a mensagem podia ser postada infinitas vezes.

Comentar sobre a incrível velocidade do *b* não é exagero algum. A melhor ocasião do dia para conseguir atenção, quando os Estados Unidos acordavam, também era a pior, já que nesse instante seu post poderia se perder no dilúvio de outros posts populares. Você começava um tópico com um post lá em cima, e, ao atualizar a página dez segundos depois, descobria que o tópico já não aparecia na página inicial e sim na página 2. Os tópicos mudavam constantemente de lugar – assim que alguém fazia um comentário, o tópico voltava à página inicial. Quanto mais comentários, maior a probabilidade de o tópico permanecer na página principal e atrair mais comentários, e assim por diante. Um ataque era mais provável de acontecer se muita gente concordasse em participar dele. Mas isso poderia ser manipulado caso um grupinho de quatro ou cinco pessoas sugerisse um ataque e repetidamente fizesse comentários no tópico para simular o funcionamento da mente colmeia. Às vezes, essa tática funcionava; às vezes, não. Nesse jogo, cada segundo contava – se o postador original não conseguia postar durante dois minutos, a oportunidade seria perdida e a mente colmeia perderia o interesse.

Outro motivo para ficar por perto: o *b* era uma fonte inesgotável de aprendizado, seja sobre como atormentar pedófilos ou desencavar dados particulares de alguém. Sem demora, os requerimentos do *r* por pornografia não se restringiam a celebridades, mas também a n00dz de moças da vida real, ex-namoradas ou inimigas dos *b*tards. Enquanto abraçavam o desafio de farejar pornografia feita em casa, os usuários do *b* ensinavam uns aos outros práticas recomendadas – por exemplo, como encontrar uma série exclusiva de números para cada URL de foto no Facebook ou endereço de site e utilizá-la para acessar o perfil de alguém e suas informações. Os métodos eram simples e toscos. Em geral, tornava-se desnecessário o tipo de hackeagem talentosa utilizada por cibercriminosos ou pela turma que atacou a HBGary Federal.

A partir dos dezoito anos, William começou a preencher uma coleção da pastas secretas no computador da família com pornografia caseira e informações sobre pessoas, inclusive suspeitos de serem pedófilos e mulheres que ele conhecia on--line. Logo ele passou a incentivar outros newfags para “lurk moar” ou aprender

mais sobre o 4chan. Criou outra pasta oculta chamada “info”, na qual guardava quaisquer técnicas e métodos novos para sua espionagem, geralmente em forma de capturas de tela, de coisas variadas como hackear máquinas de venda automática para conseguir Coca-Cola grátis – mensagem postada nos tópicos “Real Life Hacking” – até tirar um site do ar. O painel *rs* (*rapid share*, compartilhamento rápido), que compilava links de sites populares de compartilhamento de arquivos, tornou-se uma fonte de programas úteis e livres como o Auto-Clicker, que ajudava a reverter a tendência de pesquisas on-line ou a causar spam em um site. Espreite por tempo suficiente, concluiu ele, e você consegue acesso a quase tudo que deseja.

William primordialmente sentia atração por mulheres. Mas, investigando o 4chan, ele observou outros usuários dizendo que oscilavam rumo à bissexualidade ou até mesmo à homossexualidade. Um tópico recorrente vinha nesta linha: “O quão gay você se tornou desde que começou a navegar no *b*?”. Muitos heterossexuais do sexo masculino que visitavam o *b* descobriram que sua reação à pornografia gay mudava de negativa a indiferente para positiva. William não se sentia tornando-se gay nem bi, mas havia deparado com tanta pornografia masculina ao longo dos anos que já não lhe causava repulsa. Era mais quase fadiga de pênis.

A moral de William tornava-se cada vez mais ambígua, à medida que constantemente ele não só assistia a cenas de violência, estupro, racismo e abuso sexual –, mas ria ao vê-las. Tudo era “cash” ou “win” (bom e aceitável). *b*tards sabiam a diferença entre o certo e o errado – apenas não reconheciam essas designações no 4chan. Todos aceitavam que estavam ali por lulz – e o ato de obter lulz geralmente significava machucar alguém. Não causa surpresa que um slogan futuro do Anonymous seria: “Nenhum de nós é tão cruel quanto todos nós”. A crescente ambivalência de William em relação ao sexo e à moralidade multiplicava-se em larga escala entre os demais usuários do 4chan e se tornaria uma base para a identidade “cult” do Anonymous.

Nesse meio-tempo, o vigilantismo on-line do rapaz se tornou seu emprego em tempo integral. Era recompensador e eficaz. Ele não precisava hackear computadores das pessoas para obter seus dados privados – apenas conversava com elas e em seguida exercia a arte sutil da “engenharia social”, esse modo sofisticado de descrever a mentira.

***

Naquela fria tarde de fevereiro, William saiu debaixo dos cobertores, foi buscar algo para comer e voltou ao computador da família. Como de costume, abriu seu navegador da internet e o painel *b* do 4chan apareceu como página inicial. Clicou em alguns tópicos e após algumas horas deparou com a foto de uma garota. O cabelo preto escondia parcialmente os olhos verdes e um meio sorriso fascinante. A foto havia sido tirada de cima para baixo, o habitual autorretrato de adolescentes do sexo feminino. O

postador original queria que o *b* constrangesse a moça invadindo sua conta no Photobucket, descobrindo várias fotos nuas e enviando-as para os amigos e a família dela. Obviamente havia alguma espécie de ressentimento.

– Seja como for, ela é uma puta – escreveu ele, adicionando um link para o perfil da jovem no Facebook. Esse era o tipo de coisa que William fazia com alguém toda hora, mas o OP parecia não entender o espírito do *b*.

Para começo de conversa, os usuários do *b* queriam mais de seu tempo do que apenas "n00dz", afinal a nudez já era o maior produto do 4chan. Mais relevante que isso: um OP nunca deve acreditar que tem o *b* à sua mercê. Em poucos minutos, o post dele tinha acumulado mais de cem comentários – quase todos dizendo "NYPA" (*not your personal army*, algo como "não somos seu exército pessoal") – junto com outros insultos.

William respondeu a mesma coisa, mas também ficou intrigado. Clicou sobre a foto da garota novamente e decidiu que não tinha nada a perder com uma noite de diversão e justiça. Uma hora da manhã de sábado. Os vizinhos voltavam para casa depois de uns tragos nos bares locais enquanto William, escarrapachado na cozinha de sua família, navegava no velho computador, de vez em quando passando os dedos pelo cabelo desalinhado.

Clicou no link do Facebook e viu outra foto da moça, sentada num muro de tijolos, balançando alegremente as pernas aquecidas por meias-calças de lã colorida, franzindo a testa para a câmera. Chamava-se Jen e morava no Tennessee.

William entrou no Facebook com um de seus vinte perfis fajutos. Quase todos simulavam perfis de mulheres inexistentes. Era muito mais fácil adicionar amigos no Facebook sendo mulher, e amizades tornavam-se cruciais para que um perfil parecesse verdadeiro. Sua principal conta falsa no Facebook tinha uns

130 amigos do mundo real. Para adicioná-los, escolhia um lugar como Chicago e daí adicionava rapazes da região. Se perguntassem quem “ela” era, William afirmava ter se mudado recentemente para lá. A maioria das outras contas falsas eram refugos, no sentido de que a maior parte dos amigos consistia em outros perfis falsos de usuários do *b*. Ele adicionava os amigos no próprio *b* com o tópico ocasional intitulado “Adicione aqui suas contas troll!”. Os usuários falsos se conectavam ao Facebook e deixavam comentários nos perfis do outros para torná-los mais realistas. William acrescentava fotos à página e falsificava “fotos de férias” baixando pastas completas de imagens de uma mulher solteira de repositórios de fotos on-line ou do próprio 4chan, ou coagindo a moça a lhe fornecer os retratos. Às vezes, o Facebook apaga contas “troll”

como essas, em especial se elas têm nomes sem sentido como I. P. Daily.

(William perdia em média duas contas por mês por esse motivo.) Mas contas que pareciam reais poderiam durar anos. Dessa vez, para conversar com Jen, ele utilizava o perfil em nome de Kaylie Harmon, conta frequentada por gente de verdade.

Obteve uma captura de tela do post do 4chan com a foto da moça.

Depois, sob o disfarce de Kaylie, digitou uma mensagem particular no Facebook para Jen. Qualquer pessoa no Facebook pode enviar uma mensagem sigilosa para outro usuário, até mesmo se ambos não estiverem conectados como amigos.

– Olhe o que alguém está tentando fazer com você – avisou anexando a captura de tela do 4chan. Assinou como “Anonymous”, o que costumava fazer para assustar seus alvos.

A resposta de Jen foi quase imediata: – OMG. Quem é você? Como me achou no Facebook?

– Sou um hacker – mentiu William. – Vou hackear seu Facebook e suas fotos no Photobucket. Não importa quantas fotos você tiver on-line, eu vou tornar todas elas públicas.

Ele mantinha suas respostas sucintas e ameaçadoras.

– O que preciso fazer para impedir isso? – indagou, aparentemente desesperada para evitar a publicação das fotos.

William sorriu de si para si. Anos de experiência atacando contas de moças na web lhe ensinaram isto: ela realmente tinha fotos de nudez e estava disposta a fazer concessões.

– Se me fornecer as suas fotos nua, vou impedir o ataque de outros hackers em sua conta – prometeu ele. – Neste exato instante, tem um monte de gente tentando hackear você.

Sem motivos para acreditar que ele estava mentindo, Jen consentiu e lhe enviou os detalhes importantes de login.

– Pegue o que você quiser – disse ela.

Havia talvez trezentas fotos na conta de Jen no Photobucket, a maioria delas em companhia de amigos e familiares, instantâneos de férias na praia, um grupo de membros da família fazendo sinal de positivo num restaurante Ruby Tuesday. E em torno de setenta fotos com ela nua. Uma por uma, William começou a baixá-las em sua coleção particular de pornografia caseira.

– Prontinho – disse William a Jen no recurso de bate-papo do Facebook.

– Fico contente que você tenha concordado. Poderia ter sido bem pior.

Ele lhe avisou que intensificasse as configurações de privacidade no Facebook e se livrar de sua pergunta de segurança. A pergunta de segurança, que os sites utilizam para ajudar o usuário a se lembrar de uma senha esquecida, segue na linha de “Qual o nome de seu primeiro bicho de estimação?”. William só precisaria entabular uma conversinha com ela para descobrir a resposta e, em seguida, descobrir a senha da garota se assim desejasse – mas desta vez ele a alertou sobre o estratagema.

Uma hora depois, Jen já perdoara a William por seus estranhos atos.

Estava intrigada e interessada em conhecer o “hacker” que a salvara de um destino constrangedor. Os dois começaram a falar sobre banalidades como Facebook e amigos. Em seguida, William propôs uma ideia: – Se quiser, descubro o nome da pessoa que postou sua foto no 4chan – sugeriu ele.

Jen concordou.

– Descubra quem é o cara que eu mando outras fotos especialmente para você.

– Quem está na sua lista de pessoas bloqueadas no Facebook? – perguntou William.

– Seis pessoas, acho eu.

William estudou o perfil de cada uma. O dia amanhecia quando, por fim, seus olhos repousaram no Facebook de Joshua Dean Scott; a foto do perfil: barba por fazer, sorriso de escárnio, camisa jeans rasgada e piercings na sobrancelha. Na mesma hora, soube que aquele rapaz devia ser o OP do 4chan. Parecia alguém completamente asqueroso. Em várias fotos aparecia uma mulher sorridente com corte de cabelo punk que aparentava ser a noiva de Josh.

Ainda na conta falsa de Kaylie, completa com a sorridente foto feminina e 130 amigos reais, William digitou uma mensagem a Josh.

– E aí, OP. – E clicou “enviar”.

Em seguida, William enviou mensagens a seis amigos de Josh no Facebook, escolhidos aleatoriamente, indagando se alguém tinha algo a reclamar de Josh e queria o ajudar a puni-lo. Um amigo íntimo de Josh, chamado Anthony, respondeu. William explicou o que havia acontecido no 4chan – que Josh havia tentado se vingar de uma garota transformando o *b* em seu exército pessoal. Eis que o próprio Anthony, usuário do 4chan de longa data, ficou instantaneamente chocado com a falta de etiqueta de Josh no painel de imagens.

– Vou ajudá-lo – disse Anthony. – Ele não devia ter feito isso.

Anthony forneceu a William o nome completo, o número do celular e a área residencial de Josh. Às vezes, na engenharia social, você precisa apenas pedir algo com jeitinho.

William enviou mais algumas mensagens a Josh, a primeira delas postando o endereço residencial dele, na seguinte, o número de seu celular.

Ele assinava as mensagens “Anon” para que Josh pensasse que havia um grupo de pessoas por trás disso. Logo Josh respondeu, implorando misericórdia: – Por favor, pare de me hackear – escreveu ele.

William respondeu com instruções. Josh teria de enviar um foto sua segurando um papel onde se lia: “Jen é dona de meu rabo”. Com a outra mão devia segurar um sapato sobre a cabeça. A pose do sapato sobre a cabeça tinha um simbolismo enorme no 4chan e significava a derradeira admissão de derrota em qualquer tipo de discussão ou ataque on-line.

(Faça uma busca no Google Imagens com *shoe on head* e confira você mesmo. Estranhamente, as pessoas sorriem para a câmera.) Para arrematar, William pediu a Josh que enviasse uma foto da noiva dele, sem roupas, segurando um papel onde se lia apenas “*b*”. Acreditando piamente que William, jovem desempregado no lar de sua família o qual havia varado a noite acordado, era mesmo um exímio grupo de hackers, Josh simplesmente obedeceu. William encaminhou as fotos para Jen. Eram sete horas da manhã, e o resto da vizinhança se preparava para ir ao trabalho. William foi direto para cama.

Nem todo mundo no *b* agia como William, mas ele e muitos outros no 4chan viviam por esse tipo de experiência noturna. Embora não conseguisse se fixar em um emprego por mais de poucos meses, William, às vezes em apenas uma hora, conseguia apavorar e coagir alguém do outro lado do mundo a fazer algo que a maioria de nós jamais sonharia em fazer: tirar a roupa, bater uma foto e enviá-la a um completo estranho. O painel *b* oferecia uma inigualável sensação de poder e imprevisibilidade que atraía muita gente como ele ao Anonymous e os mantinha fisgados. Ao longo do tempo, as pessoas descobriam suas próprias funções na multidão sempre mutante. Para o Anon de língua ferina chamado Topiary, essa função era desempenhar um papel.

CAPÍTULO 3

Todo mundo vem para cá O ataque contra Aaron Barr em fevereiro de 2011 seria emblemático para o Anonymous por vários motivos: mostrava que uma ação coletiva causava grande impacto por meio do roubo de dados, não apenas tirando um site do ar. A publicação on-line dos e-mails de Barr teve importantes repercussões na reputação dele e na de seus sócios. Isso também revelou o incrível potencial de um ataque via Twitter. O processo de entrar na conta do Twitter de Barr tinha sido fácil.

Topiary apenas testara a já conhecida senha “kibafo33” e na primeira tentativa fizera o logon. Mas raptar a conta e enviar uma série de tweets com humor

vulgar se tornaria um dos pontos altos do ataque, na opinião de outros Anons e da imprensa. Esses tweets repentinamente deram nova voz ao Anonymous, mostrando que não se tratava apenas de uma sinistra rede de hackers ansiosa por realizar ataques. Eles também queriam se divertir.

Topiary sempre apreciara mergulhar em novas e empolgantes experiências como o ataque à HBGary. Seu nome verdadeiro, guardado a sete chaves, era Jake Davis. Desde a mais tenra idade demonstrou intensa curiosidade; preferia assistir ao jogo matemático *Countdown* da televisão britânica a ver desenhos animados. Gostava tanto de números que, ao completar dois anos, ganhou da mãe uma calculadora, em cujas teclas apertava os dedinhos frenéticos enquanto a mãe empurrava o carrinho no supermercado. O menino tornou-se um daqueles raros indivíduos simultaneamente criativos e analíticos, com os dois hemisférios cerebrais bem desenvolvidos. Adorava números, mas amava música e, mais tarde, seria atraído por bandas e músicos de vanguarda e os escutava simultaneamente com outros amigos on-line, ritual semelhante a uma experiência religiosa. Jake atribuía cores aos números: por exemplo, sete era laranja, e seis, amarelo. Não era uma visão de cores, apenas a sensação dela, e a condição o ajudou a se destacar em matemática quando criança – lembrar-se da cor amarela como 42 facilitava aprender a tabuada de 6 x 7; 81 era um número azul porque 9 era azul, e assim por diante. Tinha certeza de que todo mundo pensava assim até se dar conta de que portava uma “condição” chamada sinestesia de som para cor.

Nascido em Canterbury, na Inglaterra, aos seis anos se mudou, com a mãe, para um afastado arquipélago ao norte da Escócia, conhecido como as ilhas Shetland. A causa da mudança: a impulsiva aquisição, feita pelo avô Sam Davis, de um hotel dilapidado que se encontrava à venda em uma das ilhas. O idoso ouviu um comentário sobre a oportunidade e embarcou num avião para dar uma olhada. Uma semana depois, mudava-se para lá com a esposa Dot. Durão e espontâneo, Sam Davis gostava de correr riscos. A mãe de Jake, Jennifer Davis, perdera o contato com os pais durante um bom tempo, mas, quando descobriu por acaso onde eles estavam, decidiu ir atrás. Até então, estivera pulando com os dois filhos de uma pensão para outra, em busca de uma residência fixa no sul da Inglaterra. Jennifer e o parceiro, pai de Jake, mantinham um relacionamento instável há seis anos, entre rompimentos e reconciliações. Cada vez mais irresponsável, ele se perdera na bebida, balbuciando sobre encontrar religião e saindo com outras mulheres. Um dia, ela deu uma mochila a cada um dos filhos pequenos, enfiou tudo que pôde em duas malas e embarcou com eles num ônibus

(o trem era muito caro) para uma jornada de dezoito horas até Aberdeen, Escócia, antes de pegarem a balsa rumo às ilhas Shetland.

Foram morar numa ilha chamada Yell, a segunda maior do arquipélago, mas ainda pequenina, com novecentos habitantes. Lúgubre e, sob certos aspectos, uns vinte anos atrasada em relação ao resto do país. Havia eletricidade, mas nada de cadeias de lojas, bares de fast-food ou bons restaurantes. Os adolescentes locais se aventuravam nas drogas como recreação de último recurso. Paisagem gélida, cinzenta e fustigada pelo vento, com raras árvores à vista. Estradinhas de uma só pista se espalhavam pela ilha e casinhas de pedra salpicavam a zona rural.

As pessoas ali estavam isoladas. Quem chegava mal compreendia o complicado dialeto nativo. A maioria nascera e vivera ali a vida toda, nunca se arriscando a sair da ilha ou a ler algo além do jornal local. Apesar da área agrícola, o lugar dependia de remessas diárias de alimento e combustível trazidas de balsa. Quando tempestades escureciam o horizonte, os moradores afluíam ao mercado local com medo de falta de víveres. Os ilhéus não se identificavam com os dois países que os cercavam, a Noruega e o Reino Unido. A coesão da comunidade tinha lá suas vantagens: as pessoas cuidavam umas das outras. Muitas vezes os agricultores e pescadores locais davam o excesso de carne e peixe aos vizinhos. Após alguns anos, a família de Jake tinha três geladeiras cheias de alimentos frescos, desde carne de cordeiro até filés de salmão tão espessos que, servidos no prato, mal eram atravessados pelo garfo. Mas a gente local desconfiava dos forasteiros, e ir à escola seria algo insuportável para o pequeno Jake.

Enquanto os avôs de Jake cuidavam dele e de seu irmão depois da aula, a mãe tinha vários empregos para ajudar a pagar as contas. Por fim, ela acabou conhecendo um novo parceiro, Alexander Spence, o “Allie”. Ela e os garotos se mudaram para a casa de Spence, e Jake começou a tratar Allie como seu padrasto. Na escola, ele sofria bullying. Embora tivesse inteligência aguçada, também tinha ambliopia, condição chamada de “olho preguiçoso”, que lhe afetava a pupila do olho esquerdo. Socializar-se na escola representava um grande esforço, e ele decidiu que era mais fácil nem tentar fazer amigos. Calado, mantinha-se distante da maioria dos colegas.

Se alguém caçoasse dele, defendia-se com um comentário afiado, e se outros meninos caíssem na risada, ele ria junto. Na maior parte do tempo, a falta de amigos na escola não o incomodava.

Mais frustrante era o nível de ensino. Jake percebia que sua minúscula escola de cem alunos ensinava pouca coisa sobre o mundo fora da ilha. Em vez disso, as aulas se centravam nos detalhes da ovinocultura: como identificar ovelhas e como dar banhos de imersão para combater ectoparasitos. Duas vezes por semana havia aula obrigatória de tricô, nas quais Jake produzia brinquedos coloridos (em formato de fantasmas e dinossauros) ou chapéus. Um de seus dinossauros foi premiado no concurso de tricô local, julgado pela "tricotadora mais rápida do mundo", verdadeira heroína da ilha. Um sentimento agridoce o dominou: ele não queria aprender a tricotar; ele queria aprender algo que o desafiasse.

Cada vez mais, a escola e o currículo escolar começaram a parecer sem sentido. Quando começou a frequentar o ensino médio de Yell, tornou-se insolente, questionando abertamente a lógica dos professores, esforçando-se apenas quando um professor afirmava que ele não conseguia fazer o trabalho adequadamente. Tornava a rotina tolerável aplicando trotes. Um dia, disparou o alarme de incêndio da escola e, com a ajuda de colegas, amontoou mobília no corredor, impedindo o acesso de alunos e professores ao salão que servia como ponto de encontro. Não queria impressionar os outros colegas. Só gostava de causar confusão, e ansiava fazer coisas que ninguém fizera antes. Quando entrou na adolescência, os professores alertaram sua mãe de que Jake precisava interagir com um círculo de amigos mais amplo. Na visão deles, o jovem era petulante, frio e calculista.

Em fevereiro de 2004, a tragédia atingiu sua vida: o padrasto, Allie, envolveu-se num acidente de carro em uma das estradinhas da ilha e morreu. Jake tinha treze anos de idade. Para piorar a situação, ele e sua família foram avisados de que não poderiam continuar a morar na casa do padrasto. A ex-mulher de Spence ainda tinha direitos sobre a casa e pediu à família que liberasse o imóvel. Por fim, Jennifer Davis e os dois filhos conseguiram encontrar moradia subsidiada pelo governo – uma casinha marrom com tábuas verticais de madeira no meio de Yell.

A experiência foi demais para Jake, que decidiu não mais voltar à escola.

O melhor lugar para ficar seria em casa, sozinho. Tornou-se um recluso. Em meio à própria dor, a mãe ficou furiosa, dizendo ao filho que ele não poderia desperdiçar a oportunidade de concluir os estudos. Mas ele não queria sentir-se restringido por cronogramas, currículos – nem mesmo por sua própria mãe.

Após abandonar os estudos, Jake dedicava a maior parte do tempo a jogos de vídeo e aprendizado tutorial em meio turno. A essa altura, a mãe instalara uma conexão de internet via linha discada na casa, a fim de enviar e receber e-mails. Jake a convenceu de fazer um upgrade e instalar banda larga e, desde os onze anos, ele se conectava na internet quase todos os dias, explorando um mundo inteiramente novo de aprendizado, socialização e, depois, aprendizado por meio da socialização. Quando começou a praticar jogos de RPG como RuneScape, outros jogadores lhe ensinaram vários truques, desde navegar na web até ocultar o endereço de IP conversando por meio de mensagens instantâneas, sem falar em programação básica. Fazer amizades on-line era fácil. Ninguém notava sua ambliopia, e as pessoas davam muito mais valor à sua inteligência e à sua criatividade. Tornou-se mais audacioso e mais engraçado. Havia uma igualdade jamais experimentada por ele antes, uma facilidade para conversar e uma sensação de identidade compartilhada. Quando o serviço de telefone na internet – o Skype – surgiu, ele o utilizou para conversar de verdade com seus novos amigos pela primeira vez.

Um dia no Skype alguém sugeriu dar um trote e deixar todos os outros escutando. Jake embarcou na oportunidade. Descobriu o número de uma loja aleatória do Walmart nos Estados Unidos e disse à mulher que atendeu que procurava um “helicóptero de controle remoto e em formato de peixe”.

Enquanto implorava à mulher que o ajudasse a encontrar o produto, Jake tinha plena consciência de que os amigos (no mudo) morriam de rir. No dia seguinte, fez um trote para um restaurante da Applebee em San Antonio, no Texas. O gerente se exasperou tanto que Jake decidiu repetir o trote, dessa vez pedindo, em voz de falsetto, para chamarem uma ambulância, alegando estar dando à luz no porão do restaurante. Quando o gerente ameaçou ligar a um inspetor do Departamento de Polícia de San Antonio, Jake e um amigo ligaram ao referido inspetor denunciando que o gerente da Applebee era um terrorista. Os amigos de Jake não se cansavam de ouvir seus trotes.

Ficavam hipnotizados pela imprevisibilidade e pela ousadia de sua voz de barítono. Jamais suspeitariam que, um ano atrás, ele era o garotinho calado e mirrado que sofria bullying numa escola de vilarejo.

Em pouco tempo ele fazia trotes para se exibir aos amigos quase todos os dias. Descobriu um ou dois bons aplicadores de trotes para ajudá-lo, inclusive um sujeito em Londres com quem ele fingia ser um pai aconselhando a filha. Tudo

era improvisado e, às vezes, a ideia lhe vinha quando o telefone estava tocando. Procurava sempre inovar modos ousados de incomodar, assustar ou confundir seus alvos. Era como produzir um show de televisão, mantendo os espectadores felizes com novas ideias e artifícios. Por fim, mudaram-se para um site chamado Tiny Chat, no qual dezenas de usuários podiam ouvir os trotes de Jake no Skype.

Neste ponto ele já era um visitante ocasional do 4chan e do *b*, atraído principalmente pelos trotes e ataques. Observou que poderia conquistar mais ouvintes se fizesse propaganda no 4chan. Começava um tópico no *b* e colava links para a sala de bate-papo em que transmitia o trote, incentivando mais gente a entrar e ouvir algo divertido. Em pouco tempo, ele dava trotes acompanhados por 250 ouvintes cada vez. A Applebee de San Antonio se tornou sua vítima favorita. Ao longo de um ano, ele encomendou rodadas de vinte pizzas de uma só vez e inúmeras caixas grátis da UPS. Noutra ocasião, recebeu (por meio do 4chan) uma dica de um funcionário despedido de uma loja de móveis dos EUA, o qual lhe forneceu o código interno para acessar o sistema de alto-falantes da loja. Quando Jake ligou, forjou um convincente sotaque americano e avisou aos clientes que todos os itens eram grátis pelos próximos vinte minutos. Pouco depois, ligou novamente, e o som ambiente só poderia ser descrito como caótico.

Dois anos nesse ritmo e Jake, aos catorze anos, borboleteava entre seus trotes transmitidos via Skype e ataques perpetrados por *b*tards do 4chan. Ataques bem-sucedidos tinham como alvo qualquer coisa on-line, mas tendiam a apresentar uma característica em comum, algo que pouco mudou até hoje: um surto. Quer seja enviar spam de fotos chocantes ao fórum de alguém, quer seja sobrecarregar de tráfego um site específico, ou até mesmo influenciar os votos para a Pessoa do Ano da revista *Time* ou o personagem favorito de videogame na votação de um site, os ataques do *b* envolviam a formação de um grupo para inundar um alvo até o limite do constrangimento. A união faz a força. Quanto mais pessoas participavam, maior o dilúvio.

Muitos consideram que o primeiro ataque significativo do 4chan foi realizado em 12 de julho de 2006 contra o Habbo Hotel, popular site de jogos e bate-papos em tempo real projetado como distração virtual para adolescentes. Assim que entrava no site, o usuário conseguia ter uma visão panorâmica dos vários quartos do hotel e, na pele de um personagem criado por ele, explorava o local e conversava com os avatares de outras pessoas.

Certo dia alguém no 4chan sugeriu perturbar o ambiente virtual entrando em

massa e inundando o lugar com o mesmo personagem, um homem de ascendência africana de terno cinza e corte de cabelo afro. Em seguida, os homens de cabelo afro tinham de impedir o acesso à piscina e explicar aos outros avatares que ela estava "interditada devido a um defeito e à aids". Quando os usuários habituais do Habbo faziam logon, subitamente deparavam com a área sobrecarregada com o que mais pareciam dançarinos de discoteca vestidos a rigor. O *b* festejou o Grande Ataque ao Habbo de 2006; nascia o meme da "piscina interditada". Durante os anos seguintes, em 12 de julho, grupos de usuários do 4chan retornavam ao Habbo Hotel com seus avatares de cabelo afro, às vezes movimentando seus personagens para criar o formato de uma suástica no hotel.

Ao completar dezesseis anos, há três anos fora da escola, Jake não só participava dos ataques do 4chan: ele os organizava. Em 2008, ajudou a desencadear a Operação Basement Dad. Naquele ano, surgiu a notícia de que o engenheiro austríaco Josef Fritzl havia estuprado e aprisionado sua filha de 45 anos durante os últimos 24 anos, tendo 7 filhos com ela. Os detalhes dos monstruosos crimes de Fritzl chocaram o mundo, e o julgamento dele ganhou manchetes durante semanas a fio. Naturalmente, o 4chan vislumbrou o lado engraçado da coisa. Jake e vários outros usuários do site se encontraram em separado numa sala de bate-papo e decidiram criar uma conta falsa no Twitter para Fritzl. Objetivavam tornar @basementdad a primeira conta do Twitter a alcançar um milhão de seguidores, competição na época disputada entre o ator Ashton Kutcher e a CNN. Menos de vinte e quatro horas após configurarem a conta e anunciá-la no 4chan, no site de compartilhamento de mídia eBaum's World e em outros sites, ela já alcançava quase 300 mil seguidores. Quase meio milhão de pessoas seguia @basementdad antes de o Twitter cancelar a conta; de acordo com os cálculos de Jake, estavam a caminho de vencer a corrida.

Trotes como esse não eram facilmente organizados via 4chan. Agora havia milhões de pessoas utilizando seus fóruns e mais de 200 mil posts diários no *b*. Os tópicos de discussão mudavam com tanta rapidez que era impossível estabelecer uma discussão persuasiva. Por fim, as pessoas se deram conta de que, para organizar um bom ataque, seria necessário lançar mão do Internet Relay Chat (IRC).

O IRC, sistema de bate-papo simples e em tempo real, foi criado em 1988 pelo programador Jarkko "WiZ" Oikarinen (hoje funcionário do Google na Suécia). Por volta de 2008, alguns milhões de pessoas já o utilizavam – não era preciso

ter conta, como no MSN ou no AOL Instant Messenger. Bastava ter um programa ou um “cliente” do IRC, capaz de lhe indicar a vasta gama de redes ofertada. Hoje existem centenas de redes IRC

mundo afora, algumas alinhadas com as ideias de várias organizações como o WikiLeaks. A EFnet, uma das mais antigas, é amada por hackers veteranos como Sabu. Assim que a rede se estabelecia, era possível contar com dezenas e até centenas de salas de bate-papo para visitar, conhecidas como “canais”. Alguns canais tinham uma pessoa; outros, milhares. A maioria tinha entre cinco e vinte e cinco pessoas. Você simplesmente entrava e logo começava a travar contato com os outros.

Quando alguém como Jake começava a utilizá-lo, o IRC parecia mais do que apenas uma sala de bate-papo casual. O IRC era direcionado a pessoas de pensamento tecnológico, graças a sua longa lista de comandos especiais que permitia navegar pelos canais e inclusive manipular a rede. Por exemplo, o comando /whois mostrava em quais canais outra pessoa estava e um endereço IP. O começo de um bate-papo privado era mais ou menos assim: “/msg topiary E aí, como vai?”. Dependendo de qual programa você usava, cada canal apresentava uma lista ao lado mostrando os participantes da sala, classificados por aqueles com status de “operador” e com o poder de expulsar quem estivesse falando EM MAIÚSCULAS ou importunando os demais. O linguajar do IRC era repleto de abreviações como rofl (*rolling on the floor laughing*, rolando no chão de tanto rir), lol (*laugh out loud*, cair na gargalhada) e ttyl (*talk to you later*, falo contigo mais tarde). A exemplo do 4chan, o IRC gradativamente desenvolveu cultura e linguagem próprias.

Era só entrar numa rede e você já podia criar um novo canal IRC.

Bastava digitar /join #channelname, e o canal aparecia. Se Jake quisesse organizar um novo ataque como a Operação Basement Dad, ele criava uma sala – por exemplo, #opbasementdad – e convidava pessoas escolhidas a dedo para entrar. Assim, qualquer sujeito interessado contribuía com ideias e ajudava a planejar o ataque ou o ardil.

Tão logo os planejadores tinham definido o que fazer, eles voltavam ao 4chan. Dessa vez, porém, usavam o *b* como ferramenta de recrutamento, criando um novo tópico e enviando spam com a seguinte mensagem: “TODO MUNDO VEM PARA CÁ”. Também colavam um link junto à mensagem que conduzia

outros usuários do *b* para seu novo canal IRC.

Logo havia dezenas e mesmo centenas de pessoas entrando na sala de bate-papo e escutando as instruções ou fornecendo ideias. O Anonymous tinha emergido pela primeira vez em painéis de imagem como o 4chan, mas evoluía por meio das redes do Internet Relay Chat. Tornava-se mais organizado. Embora as pessoas pudessem utilizar apelidos no IRC, a maioria mantinha o anonimato incentivado pelos painéis de imagem.

Personalidades individuais emergiam, mas as pessoas ainda não tinham identidades do mundo real.

As redes de IRC ajudavam o Anonymous a se transformar de uma massa volátil e imprevisível de usuários de painéis de imagem em grupos bem-organizados e, às vezes, ameaçadores. Se o ataque atraía interesse suficiente ou era anunciado com eficácia, mais pessoas participavam dele. O

patamar subiu quando hackers começaram a aderir. Quanto mais gente se unia a um canal de IRC, maior a probabilidade de que entre eles existissem indivíduos com talentos técnicos especialmente fortes: programadores e hackers capazes de violar uma rede ou escrever um script para ajudar a automatizar um ataque. Um desses hackers foi Kayla.

CAPÍTULO 4

Kayla e a ascensão do Anonymous Enquanto Topiary divertia os *b*tards no 4chan, a entidade internética conhecida como Kayla aprendia sozinha a abrir buracos no ciberespaço. Sua jornada ao mundo do Anonymous, conforme ela conta, havia iniciado com o isolamento e a descoberta de hackers na internet; depois, encontrou o seu lugar na ascensão do hacktivismo. Mas muita gente descobriu uma coisa sobre Kayla: ela mentia.

Não o fazia com má intenção. Kayla mentia em parte para se proteger, em parte para se manter amigável. Ser lacônico nas informações como o hacker conhecido como Tflow podia soar antipático até mesmo quando as pessoas sabiam que essa era a etiqueta do Anonymous. Em vez de se recusar a responder a uma pergunta pessoal ou evitar entabular bate-papos, Kayla fornecia livremente dados pessoais

sobre a vida dela e a de amigos on-line, relatos enfadonhos de como machucou o dedão na porta descendo a escada para pegar comida ou de um passeio à praia com os amigos da vida real. Ela compartilhava detalhes excepcionalmente cretinos sobre sua infância e seus pais e sobre outras hackeagens que promovera no passado. Não importa o quanto daquilo era mentira – pouco, nada ou tudo.

O fato é que a pessoa por trás de Kayla parecia ter uma profunda necessidade de contar histórias para provar o seu valor aos outros.

Após o ataque de fevereiro de 2011 contra a HBGary Federal, por exemplo, Kayla corroborou a história contada por Sabu, de que uma garota de dezesseis anos de idade tinha hackeado o site de Greg Hoglund, o rootkit.com.

– Após resetar a conta de Greg, eu a utilizei para fazer engenharia social com Jussi e obter acesso ao rootkit.com – afirmou Kayla numa entrevista de março de 2011. – Foi a cereja no topo do bolo.

Na realidade, tinha sido Sabu o hacker que fizera engenharia social com o administrador e hackeado o site.

Solicitada a esmiuçar a história poucos meses depois, Kayla mudou sua versão:

– Na real, o jeito que tudo aconteceu... Sabu fez a bola rolar com a engenharia social, depois finalizei apagando o diretório do servidor do rootkit.com.

Kayla não precisava mentir sobre suas façanhas. A maioria de seus conhecidos reconhecia o talento dela como hacker. Mas ela também não queria corromper a mentira de Sabu e dificultar as coisas para o amigo.

Assim era Kayla – mentia para evitar incômodos às pessoas.

Kayla contava que tinha dezesseis anos e que desde os onze era filha de pais separados. Conforme ela mesma relatava, o pai era mais estável que a mãe e, por isso, ela ficara sob sua custódia. Os dois se mudaram para uma cidadezinha remota, onde havia poucos garotos da idade dela nas redondezas. Com poucas opções de lazer, começou a bater papo com as antigas amizades no MSN Messenger, fazendo logon com o nome verdadeiro (que segundo ela também era “Kayla”) e outras credenciais. O

seu pai, dizia, trabalhava em casa como engenheiro de software.

Espalhados pela casa havia montes de livros sobre programação de computadores, Linux Kernel, Intel e formação de redes. Começou a ler os livros do pai e a fazer perguntas sobre suas atividades. Empolgado com o entusiasmo da filha, ele se sentava com ela defronte ao computador e mostrava como encontrar bugs em código fonte C, como explorá-los e, por fim, como superá-los. Logo ela mergulhava em linguagens de script como Perl, Python e PHP, aprendendo a atacar bases de dados na web utilizando injeção de SQL. Embora em geral fosse algo inofensivo, ao completar catorze anos, Kayla contou que escrevia scripts capazes de automatizar ataques cibernéticos.

Depois explicou como o hábito deixou de ser inofensivo: – Comecei a procurar fóruns sobre o que o pessoal chama de hackeagem. Tentei participar de alguns deles e a recepção foi igual: "Vá embora, garotinha, isso não é coisa para você". Tudo bem que eu tinha apenas catorze anos, mas ficava emputecida!

Lançando mão de certas habilidades aprendidas com o pai e em pesquisas on-line, ela relatou que hackeou um site de fórum e apagou a maior parte de seu conteúdo utilizando injeção de SQL. Os frequentadores nunca tinham visto ataque parecido.

Kayla relembrou que um dos hackers comentou: – Uau, você tem apenas catorze anos e é capaz de fazer isso?

Ele a convidou para entrar nos canais de bate-papo mais exclusivos na EFnet, uma das redes mais antigas de Internet Relay Chat. O usuário do fórum vislumbrou potencial em Kayla, deu dicas a ela e a incentivou a ler mais livros sobre programação, para que pudesse aprender ainda mais.

– Ficou meio esquisito, porque comecei a conhecer algumas pessoas suspeitas – afirmou Kayla, referindo-se a amizades puramente on-line. – Um cara bem mais velho que eu, tipo bem mais velho mesmo, sentia uma bizarra atração por mim. Será que uma garota hacker é o sonho de todo hacker? Quem sabe? Só que ele tinha 27 e eu apenas 14! Bizarro! Tenho nojo de quem acha que só gente velha é esperta. Só porque sou jovem, o que eu digo não conta?

Embora Kayla insistisse que a vida on-line era complicada por ela ser do sexo feminino, o contrário era a verdade mais provável. A pessoa real por trás do nickname certamente obtinha mais atenção e mais oportunidades para hackear os outros sendo uma moça simpática e misteriosa. O sexo feminino era uma

presença rara em painéis de imagem e fóruns de hackeagem. Daí o slogan on-line: “Não existem garotas na internet”. Por isso, fingir ser uma garota tornou-se uma tática popular para trolls da internet já há muitos anos. Isso não quer dizer que as mulheres genuínas tinham mais poder. Se revelassem seu sexo num painel de imagem como o *b*, muitas vezes deparavam com comentários misóginos como:

– Tetas ou GTFO.

Ou seja, “Mostre os seios ou dê o fora daqui”. Muitas garotas em painéis de imagem apaziguavam esses pedidos concordando em se tornar “camwhores”, tirando a roupa ou executando atos sexuais diante da webcam ligada, para ganharem atenção e serem aceitas. A alternativa se constituía em simplesmente esconder o sexo e ser homem on-line. Com tanto ego e tanta reputação em jogo, identificar o gênero de alguém num painel como *b* era quase impossível, mas fazia sentido desconfiar de quem logo afirmava ser uma jovem mulher. Por isso, o item 29 das Regras da internet reza que na internet “todas as garotas são homens e todos os pirralhos são agentes do FBI infiltrados”. Kayla provavelmente não era agente do FBI, mas com certeza alguém com uma história bem elaborada, que talvez indicasse quem ela era na vida real.

Kayla afirmava que, entrando na adolescência, outras crianças da idade dela se encontravam nas esquinas da cidade, enquanto ela ficava em casa decorando códigos operacionais do Windows, examinando códigos de fonte e aceitando convite para entrar em canais de IRC privados, onde podia aprender mais com outros hackers. Ela gostava de utilizar sua habilidade para pregar peças nos outros. Um trote comum era “desovar” ou publicar as bases de dados do MySQL de alguém, em essência, um mapa para outros hackers tentarem roubar os e-mails e documentos dessa pessoa. O objetivo final era penetrar as contas de alguém, devassá-las e depois revelar on-line os dados pessoais da vítima.

Trollagem e vigilantismo na internet já estavam em voga há algum tempo, mas se tornavam cada vez mais populares em 2008, e não é mera coincidência que por volta dessa mesma época ferramentas como Virtual Private Networks (VPN) e Tor também se popularizavam. A maioria das pessoas que utiliza VPN faz isso para criar uma conexão segura em seus lares ou empresas e impedir que pessoas aleatórias as espionem por meio do Wi-Fi ou da internet pública. Mas essas tecnologias também permitem que hackers e usuários habituais do 4chan, como William, escondam seus endereços IP – o número exclusivo, tipicamente longo

com vários decimais, atribuído a todos os computadores conectados à internet. Parte desse endereço pode corresponder à rede da qual o aparelho faz parte, e o restante, ao indivíduo. Se você conseguisse descobrir o endereço IP

verdadeiro de alguém, em geral também conseguiria o nome real da pessoa e seu endereço na vida real. Mas se ela estivesse utilizando uma VPN, então as pessoas (como a polícia ou hackers rivais) tentando "penetrar seus documentos" encontrariam o endereço IP errado, geralmente apontando para outro computador de outro país.

Trollar era como pregar peças, mas em última análise significa causar algum tipo de perturbação emocional a alguém, em geral por meio de constrangimento ou medo. Para certas pessoas que não conseguiam aceitação no mundo real, trollar era um caminho fácil para conquistar poder e se destacar na multidão. Após exibir suas habilidades no fórum de hackers que ela invadiu, Kayla começou a fazer trollagem com as pessoas só para se divertir. Obcecada em autoafirmação, ela se ressentia com a mínima insinuação de dúvida sobre seus talentos. Direcionava suas agressões a outros hackers, furfags (pessoas com tendência à prática de atos sexuais com animais) e pedófilos on-line. Cada vez que ela e outros hackers descobriam dados pessoais das vítimas, tentavam assustá-las com a posse das informações e depois as postavam on-line ou ameaçavam enviá-las à polícia. Por volta de 2008, alguém convidou Kayla para entrar no Partyvan, crescente rede de salas de bate-papo criada com o objetivo de unir outras redes de IRC conectadas a painéis de imagem como o 4chan. A ideia era aprimorar a colaboração em ataques e criar um ambiente para o fenômeno on-line que as pessoas cada vez mais chamavam de Anonymous.

***

Ataques como o perpetrado contra o Habbo Hotel significavam um passo além de trollagem, pois envolviam múltiplas pessoas trabalhando juntas para fazer traquinagens. Por fim, foi por conta dos ataques que o Anonymous apareceu, como entidade, pela primeira vez nas manchetes da grande mídia – talvez não surpreendentemente numa afiliada da Fox TV

News em Los Angeles. A reportagem, que foi ao ar em julho de 2007, recebeu o tradicional tratamento sensacionalista: efeitos sonoros sibilantes e luzes brancas piscando.

– Eles se chamam Anonymous e são hackers vitaminados – anunciou a âncora sem fazer pausa – que tratam a web como se ela fosse um videogame da vida real.

A câmera cortava para silhuetas de mãos digitando num teclado.

– Destrua. Morra. Ataque – outra voz desencarnada entoava. – Ameaças da gangue de hackers cibernéticos que se autodenomina Anonymous.

A reportagem apresentava uma entrevista com um usuário do MySpace chamado "David", que testemunhou: perseguidores do Anonymous tinham quebrado sete de suas senhas.

– Eles publicaram fotos de sexo gay no perfil do rapaz – observou o narrador. – Foi abandonado pela namorada... Eles atacam pessoas inocentes como se fossem uma máquina de ódio da internet.

As palavras "máquina de ódio da internet" aumentaram na tela enquanto o narrador acrescentava que o Anonymous ameaçara matar pessoas e explodir ginásios esportivos, trotes que na verdade tinham sido aplicados por visitantes do *b*.

– Acho que são terroristas domésticos – dizia uma mulher cuja silhueta aparecia contra o fundo claro, antes de a imagem cortar para um furgão amarelo explodindo. – O nome deles vem de seu site secreto – continuava o repórter, enquanto uma música cataclísmica tocava ao fundo. – Exigem que todas as pessoas postando no site permaneçam anônimas.

– Eles gostam disso – falou, com a voz profunda e distorcida, um homem do qual se via apenas a silhueta.

A Fox o descreveu como um ex-hacker que havia rompido com o Anonymous.

– Eles obtêm o que chamam de "lulz".

– "Lulz" – explicou o repórter enquanto a palavra surgia em fonte imensa na tela e trompetes soavam ao fundo – é uma corruptela de "LOL", que significa "*laugh out loud*"... Seus trotes são geralmente antissemitas ou racistas.

A reportagem dava o tom de como a mídia continuaria a dramatizar as façanhas

de adolescentes enfarados e travessos, uma nebulosa multidão composta em sua maioria por moços capazes de espontaneamente se unir contra um alvo. Se havia uma "máquina de ódio", como descreveu a Fox, suas engrenagens eram as redes de IRC e os painéis de imagem. E se, por um lado, estivessem longe de ser organizados como insinuou a Fox (e reportagens futuras), por outro os Anons se alegravam em se moldar a esse retrato.

Não havia um líder isolado acionando as alavancas, mas poucas mentes organizacionais que, às vezes, se associavam para começar a planejar um ataque. Era isso que aconteceria a seguir no Anonymous, numa escala bem maior. O 4chan tinha gerado muitos ataques a pequenos sites da web e indivíduos. Logo a multidão escolheria um alvo tão controverso que seus ataques receberiam bastante apoio popular e exigiriam um impressionante ato de planejamento. No ano seguinte, 2008, um dos ataques do *b* se transformou numa completa insurgência contra a Igreja da Cientologia.

CAPÍTULO 5

Projeto Chanology

Antes que Topiary, Sabu e Kayla se encontrassem, atacassem a HBGary e ficassem determinados a perpetrar uma série de novos ataques em nome do LulzSec, o Anonymous precisava crescer e se tornar algo maior do que apenas um aglomerado de jovens em painéis de imagem ou indivíduos como Topiary fazendo trotes telefônicos. Noutras palavras, mais do que apenas perturbação pública. Isso mudou devido ao ator Tom Cruise e a um vídeo que a Igreja da Cientologia não queria que ninguém visse.

Envolvido com a Cientologia desde 1990, Cruise rapidamente se tornou seu mais famoso defensor. Em 2004, ele participou de uma entrevista com documentaristas da igreja, a qual seria incluída num vídeo mostrado exclusivamente aos membros. O vídeo tinha acabamento todo publicitário: a imagem do planeta Terra no espaço, lampejos de luz e o som de lâminas cortantes enquanto o símbolo da Cientologia se aproximava da tela. Súbito, uma guitarra elétrica começava a tocar urgentemente o tema de *Missão: Impossível*, e Cruise aparecia, trajando blusa preta de gola alta, com o semblante sério, dizendo: – Acho que é um privilégio ser chamado de cientologista.

Enquanto o tema de *Missão: Impossível* continuava a tocar ao fundo, o vídeo mostrava trechos do estranho monólogo de Cruise, que se tornava cada vez mais incoerente: – Agora é a hora, certo? – prosseguia Cruise. – As pessoas estão prestando atenção em você, então é melhor você ter conhecimento. É

melhor você ter conhecimento. E se não tiver? – sorria ele. – Sabe de uma coisa? Vá e aprenda! Mas não finja que sabe ou coisa parecida. Saiba que estamos aqui para ajudar.

No início de outra parte, Cruise, de olhos fechados e sorrindo, subitamente gargalhava.

– E eles falaram, bem, daí você conheceu uma SP? [Acrônimo da Cientologia para Pessoa Supressiva.] Ha ha ha ha! E olhei para eles. Ha, ha!

Sabe, e que coisa linda, pois talvez um dia as coisas vão ser assim. Uau.

Embora trechos da fala de Cruise fizessem sentido, a maior parte não fazia. A

igreja não estava exatamente interessada em que o vídeo vazasse.

Em 2007, um membro anônimo dela decidiu tornar o vídeo público, enviando-o em DVD para Patty Pieniadz, pessoa que fazia campanha contra a Cientologia.

Ex-cientologista do alto escalão, Pieniadz guardou o vídeo por quase um ano, esperando a ocasião certa de revelá-lo. Ao ficar sabendo que uma nova biografia de Cruise seria lançada em 15 de janeiro de 2008, ela decidiu que o momento chegara. Ofereceu o vídeo com exclusividade à rede de televisão NBC, mas, para a surpresa dela, o negócio gorou no último minuto por conta de preocupações relativas a direitos autorais. Com apenas poucos dias para a data fixada, Pieniadz só tinha outra opção: a internet. Ela não fazia nem ideia de como carregar o vídeo na web, por isso enviou o DVD a várias outras pessoas na esperança de que por fim o material acabasse publicado no YouTube. Uma dessas pessoas foi Mark Ebner, jornalista investigativo com base em Los Angeles. Às duas horas da madrugada pelo horário da costa oeste em 15 de janeiro, Ebner enviou uma mensagem a Nick Denton, fundador do site de notícias Gawker, perguntando se o Gawker não queria hospedar o que mais tarde seria chamado de “o vídeo maluco de Tom Cruise”. De acordo com Ebner, Denton ficou “tonto” de empolgação.

Praticamente ao mesmo tempo, outras cópias do vídeo estavam sendo carregadas no YouTube e prontamente retiradas por aparente violação de direitos autorais. A Igreja da Cientologia era conhecida por processos litigiosos, e é provável que a empresa parental do YouTube, o Google, que no ano anterior havia sido processado pela Viacom por violação de direitos autorais envolvendo uma indenização de um bilhão de dólares, não quisesse se arriscar.

Isso não amedrontou o Gawker. No dia quinze, o fundador e editor Denton publicou o vídeo num post intitulado: “O vídeo de Cruise doutrinando que a Cientologia tentou suprimir”. No artigo que acompanhava o vídeo, ele escreveu: – O Gawker agora está divulgando uma cópia do vídeo; ele merece cobertura da imprensa e não vamos tirá-lo do ar.

O vídeo viralizou quase instantaneamente. Até hoje, o post do blog de Denton já recebeu mais de 3,2 milhões de visualizações, enquanto uma cópia do vídeo que acabou sendo publicada no YouTube recebeu mais de 7,5 milhões.

Mas as coisas ficariam ainda mais constrangedoras para a Igreja da Cientologia,

graças ao 4chan e ao *b*.

Mais tarde naquele dia, às 19h37 no horário da costa leste, uma usuária do *b* que lera a história do Gawker e que, reza a lenda, era mesmo mulher começou um tópico de discussão no painel. O título era apenas: “Ataque à Cientologia?”. Cada post original no *b* devia incluir uma imagem, e ela havia escolhido o logotipo dourado e branco da igreja. Repleto de lugares-comuns, o texto acompanhante incitava os usuários habituais do *b* a se mobilizarem: *Acho que é hora de o b fazer algo importante. As pessoas têm de entender que ninguém mexe com o b.* .

Estou falando em “hackear” ou “derrubar” o site oficial da Cientologia.

É hora de utilizar nossos recursos para fazer algo em que acreditamos.

É hora de fazer algo importante de novo, b.

Conversem uns com os outros, encontrem um melhor lugar para planejar o ataque e então executem o que pode e deve ser feito.

Chegou a hora, b.

De imediato, a reação dos colegas postadores do *b* foi ambígua.

– Sim, boa sorte ao meter os pés pelas mãos – falou um dos primeiros a responder.

– Um painel de imagens aleatórias não pode se voltar contra uma pseudorreligião apoiada por gente rica e um exército de advogados – comentou outro. – Até mesmo se cada pessoa que ao menos UMA VEZ

navegou no *b* participasse dessa invasão em massa, ainda assim não daria em nada. Além do mais... eles teriam quinhentos advogados prontos para processar nosso rabo antes de conseguirmos pronunciar a palavra “litígio”.

– 4chan contra cientologia = FRACASSO M-M-MONSTRUOSO.

– Que tal pegarmos o mormonismo depois? E em seguida o cristianismo? – indagou sarcasticamente outro postador Anonymous. – E

depois, se a gente tiver mesmo coragem, o islamismo?

Poucos usuários do *b* que tinham experiência na Cientologia também defenderam o grupo religioso: – A Cientologia não é fundamentalmente equivocada ou perniciosa enquanto sistema de crença – sentenciou um.

A discussão prosseguiu, mas logo os comentários originais e céticos foram dominados por outros de gente que apoiava a OP. Era como se, quanto mais o *b* pensasse em atacar a Cientologia de modo maciço, mais seus usuários apreciassem a ideia.

– Você não entende, não é mesmo? – comentou um usuário. – Somos o anti-herói; a gente faz o bem e fode com qualquer pessoa, boa ou ruim, que atravessar nosso caminho.

– Este é o primeiro passo rumo a algo maior, a algo épico – concordou outro.

– Podemos fazer isso – concluiu outro. – Somos o Anon; somos os super-heróis da internet.

De repente, a opinião do tópico precipitou-se rumo ao apoio completo ao ataque. O ceticismo e as objeções iniciais de que o *b* "não é seu exército pessoal" foram esquecidos pela agora entusiasmada multidão: – Temos a força de milhares; eles não podem processar todo mundo!

– Chegou a hora de pararmos de falar abobrinha e fazer algo que valha a pena, mesmo se for apenas incomodar um bando de artistas picaretas.

– Este dia vai entrar para a história das gerações futuras de *b*tards como o dia em que ferramos com esses loucos varridos adeptos da Cientologia.

– Vamos em frente, *b*.

– Tenho três computadores. Como posso ajudar? – indagou um.

– Caraca, alguém vai escrever alguma explicação aos newfags sobre como fazer um ataque com DDoS? E daí a gente pode ativar essa merda.

Antes de o Anonymous emergir, os ataques com DDoS tinham se restringido principalmente a criminosos cibernéticos atacando sites ou empresas financeiras

a partir dos quais seria possível extorquir dinheiro.

Mas, por volta de 2008, já se tornava uma das formas mais populares dos ataques do Anonymous. Dois anos antes, por meio de DDoS, os usuários do *b* tinham atacado o site de Hal Turner, apresentador de rádio do movimento nacionalista branco, derrubando-o temporariamente. Mais tarde ele tentou processar o 4chan, outro painel de imagens chamado 7chan e o eBaum's World, exigindo milhares de dólares em custos de banda larga, sem sucesso.

Você podia participar de um ataque de DDoS simplesmente baixando grátis uma das doze ou mais ferramentas de software disponíveis no painel *rs* do 4chan. Quando gente suficiente fazia isso e inundava o alvo com tráfego de lixo eletrônico, o efeito era igual ao de quinze gordos tentando passar numa porta giratória ao mesmo tempo, de acordo com uma analogia do autor Graham Cluley, especialista em segurança. Nada se movia. O

resultado: visitantes legítimos obtinham uma página de erro quando visitavam o site, ou o navegador apenas continuava a carregar. O período fora do ar sempre era temporário – semelhante ao que acontece quando um varejista on-line faz uma liquidação com 75% de desconto e não consegue administrar a inundação de visitantes. Talvez isso pareça trivial, pois todo mundo que surfa na web já deparou com problemas de conexão e páginas de erro. Mas ficar fora do ar durante horas ou dias tem um custo alto para as empresas, com grandes perdas de renda ou aumento em custos de banda larga. Participar de um ataque de DDoS também é ilegal, pois viola a Lei contra a Fraude e o Abuso do Uso de Computadores dos EUA, e também a Lei de Polícia e Justiça de 2006 no Reino Unido; nos dois países, os infratores podem ser condenados a até dez anos de detenção.

Isso, é claro, raramente impedia o *b*, e fazia os ataques se parecerem mais com um jogo de aposta alta. Com a Cientologia, os participantes concordaram que valia a pena atrair os newfags a bordo para criar um exército e disseminar o assunto por outros painéis de imagem da internet, também conhecidos como "chans". Esses painéis incluíam o 7chan, popular painel de imagem para ex-usuários do *b*; o GUROchan, painel de imagem cujos posts consistiam principalmente em sanguinolência; e o Renchan, site atualmente defunto cujo conteúdo beirava a pedofilia. O 4chan precisava reunir no mínimo mil pessoas, frisou naquele dia um usuário do *b* no ainda emergente tópico sobre a Cientologia. Mas ele sabia: provavelmente encontrariam pelo menos cinco mil

interessados em abraçar a causa.

***

Sem demora, o grupo foi direto ao ponto. Um *b*tard sugeriu a “Fase um”: fazer trotes na hotline da Dianetics e rickrolleá-los, ou perguntar ao call center “por que existe um vulcão na capa de Dianetics... em geral, isso os inferniza”.

Outro *b*tard instruiu a todos que desferissem ataques de DDoS contra uma lista de sites sobre Cientologia. Você podia fazer isso simplesmente visitando o Gigaloader.com e inserindo uma relação de URLs que direcionavam a oito imagens do Scientology.org. O site Gigaloader (hoje defunto) foi originalmente idealizado para testar servidores, mas já a partir de 2007 as pessoas se deram conta de que podiam explorá-lo para ataques ao estilo DDoS. Era possível inserir vários endereços de imagens de um site, e o Gigaloader recarregava constantemente as imagens em seu navegador – isso sobrecarregava o servidor de imagens e consumia a banda larga do site, efeito multiplicado pelo número de participantes.

A melhor parte era que o *b* podia incluir uma mensagem no tráfego sendo enviado. Em um incidente separado, um webmaster cujo site estava sendo atacado pelo Gigaloader em 2007 disse que o tráfego recebido pelo site tinha a seguinte aparência: **75.185.163.131 - - [27/Sep/2007:05:10:16 -0400] “GET *styles*xanime/top.jpg?**

23461411908647656_ANON_NAO_PERDOA

HTTP/1.1”

200

95852

“http://www.gigaloader.com/

user-message/ANON_NAO_PERDOA”“Mozilla/5.0

(Windows;

U;

Windows

NT

5.1;

en-US;

rv:1.8.1.7) Gecko/20070914

Firefox/2.0.0.7”

No caso do Scientology.org, o 4chan estava enviando a mensagem “DDOS PELO EBAUMSWORLD” aos servidores da igreja, parte de uma piada recorrente para jogar a culpa das traquinagens do 4chan ao site rival e um pouco mais domesticado. Assim que os participantes do tópico começaram a atacar o Scientology.org com o Gigaloader, outro postador descreveu a “Fase 2”: o *b* criaria um site shell e carregaria nele um vídeo que repetidamente piscava “fatos sobre Cientologia e o seu funcionamento interno”. Em seguida, os usuários do *b* sugeririam links ao Digg (site de compartilhamento de conteúdo) e carregariam o vídeo no YouTube e no YouPorn. A Fase 3 seria quando empresas de comunicação como a Fox e a CNN deparassem com o vídeo, e um endereço de e-mail no site shell recebesse uma ordem para cessar a atividade sob pena de ação judicial pelos advogados da Cientologia, a qual incluiria os nomes, números de telefone, endereços comerciais e números de fax dos advogados. Então o *b* devia assediar os advogados, fazer trotes telefônicos, enviar via fax imagens horripilantes do site Goatse, ameaçando “reclamar para o chefe dele ou dela que ele/a é uma puta/um estuprador ou seja lá o que for”.

Enquanto o tópico sobre Cientologia aumentava, surgiam comentários filosóficos. Esse ataque envolvia autopreservação, salientou um usuário. O

b estava morrendo. O painel se tornara elitista, alijando participantes que aparentavam ser muito nerds e discutindo assuntos cada vez mais domesticados.

– Os gaiafags, furfags, todos os fags que vocês expulsam; precisamos arrebanhar milhares de pessoas e então atacar – disseram eles. – O

programa de três fases que anon postou aí em cima é infalível, desde que trabalhemos juntos.

Usuários de longa data que haviam se desencantado com o site sabiam que ele tinha o potencial de ser mais do que apenas um painel de imagem e fazer jus à imortal expressão da Fox11: “máquina de ódio da internet”.

– Antigamente éramos algo poderoso – outro usuário antigo comentou tristonho. Agora o *b* estava cheio de “newfags” que “só reclamavam”

quando um novo ataque era proposto. – Tempos atrás, o pessoal não perdia oportunidade para causar lulz maciça, atazanar as pessoas e, quem sabe, fazer algum bem ao mundo. Descobri um exército que não pertencia a uma pessoa, mas a todos.

Agora um Anon tinha postado a Fase 4, que era penetrar na rede de computadores da Cientologia.

– Este é o clímax de tudo – defendeu o sujeito. – Quem completar essa fase, seja lá quem for, será um deus aos olhos do Anonymous.

Alguém teria de entrar realmente numa igreja da Cientologia, preferivelmente um pequeno templo numa cidadezinha remota. Deveria levar um pen-drive com um programa keylogger, software capaz de registrar todo o material digitado num computador.

– É preciso dar um jeito de se esgueirar atrás do balcão – explicaram eles. – Enquanto o pessoal da igreja estiver ocupado, mova-se sorrateiramente em direção ao gabinete do computador embaixo do balcão, carregue o keylogger e espere. Saia e volte dali um ou dois dias.

Cerca de uma hora e dez minutos depois daquele primeiro post de convocação às armas, alguém notou que já estava funcionando o ataque de DDoS espontâneo desejado por eles. O Gigaloader.com estava funcionando.

– O site da Cientologia está lento para caramba – comentaram.

Demorava dois minutos para baixar uma página que antes era instantânea.

– VAMOS LÁ PESSOAL – gritou um Anon. – CONTINUEM O ATAQUE

PELO GIGALOADER!

Tão frenética estava a atmosfera que apenas quatro posts entre centenas mencionaram utilizar uma VPN ou outras ferramentas de anonimato, para que os participantes pudessem ocultar seus endereços IP.

Às 21h30, o ataque se transformara na modalidade “todo mundo vem para cá”. Alguém havia postado uma rede de IRC e um canal para o pessoal entrar e discutir com mais detalhes o que aconteceria em seguida. O canal chamava-se #raids, e, por fim, o postador original que criara o tópico criou um novo canal de IRC chamado #xenu. No sistema de crenças da Cientologia, Xenu era o ditador da Confederação Galáctica responsável por trazer os humanos ao planeta Terra, há cerca de 75 milhões de anos, para depois colocá-los ao redor de vários vulcões e matá-los com bombas de hidrogênio.

A essa altura, centenas de pessoas se acumulavam no #xenu e depois no #target, onde planejadores autonomeados podiam determinar alvos com um título específico na parte superior. Todo mundo conversava ao mesmo tempo no canal #xenu sobre qual a próxima ação a tomar.

– EI, *B* – escreveu alguém às 21h45 no 4chan. O Anon alegava ter encontrado “um monte de” vulnerabilidades no XSS, ou cross-site scripting, da Scientology.org, a segunda técnica de hackeagem mais comum depois da injeção de SQL. – VOU TENTAR EXPLORAR ISSO.

O endereço do canal de IRC continuava a sofrer spam. Havia uma sensação de que o tópico estava chegando ao fim, por isso algumas pessoas postaram uma guinada essencial das discussões no IRC: lembrem-se da data de 20 de janeiro.

– A coisa vai feder.

O tópico inteiro tinha atraído 514 posts em cerca de três horas. O moral estava alto. O antepenúltimo postador estimou que os debates contaram com cerca de duzentos participantes. A essa altura, os centros de Cientologia mundo afora já estavam recebendo uma amostra dos trotes tocando a música de Rick Astley, mensagens de papel preto que secariam seus cartuchos de impressora, entregas de pizza não encomendadas e táxis inesperados. O principal site da igreja agora carregava lentamente.

No dia seguinte, 16 de janeiro, alguém com o apelido Weatherman começou uma página na Encyclopedia Dramatica, a miscelânea on-line cujo slogan era “Confiamos em lulz”. Essa página incluía uma declaração de guerra contra a

Cientologia. Em seguida, às 17h47 no horário da costa leste, a postadora original que primeiro havia sugerido um ataque coordenado parabenizou as tropas estimuladas no *b* e as incitou a ações mais drásticas.

– Em 15/1/08 a guerra começava. O site da Cientologia já está sob um pesado bombardeio – comunicou a OP. – Essa é apenas a ponta do iceberg, o primeiro ataque de muitos que vão se seguir. Mas, sem o suporte dos chans, a Cientologia irá repelir esse ataque. 4chan, responda ao chamado!...

Precisamos destruir esse mal e substituí-lo por algo maior: a Chanology!

A palavra que mesclava "chan" com "Scientology" marcava um evento que uniria os diferentes painéis de imagem, transformando suas batalhas individuais contra pedófilos, usuários do MySpace e outras em uma batalha maior, contra uma organização maior. Talvez a Cientologia pareça uma escolha estranha como alvo – até então, a maioria dos visitantes dos chans provavelmente sabia apenas que se tratava de uma excêntrica religião com algumas celebridades entre seus seguidores. Súbito, tornou-se o maior alvo já atacado pelo Anonymous (estima-se que em 2008 existiam cerca de 25

mil cientologistas nos EUA), com o que parecia ser uma enorme onda de interesse. Ninguém, nem mesmo a postadora original, tinha ideia do rumo disso tudo, se seria um incidente isolado ou uma evolução em termos de anarquia criativa na internet.

Mas por que a Cientologia? Inicialmente, o depoimento bizarro de uma celebridade e o incomum sistema de crenças da Cientologia atraíram as pessoas que navegavam pelos painéis de imagem e no eBaum's World em busca de coisas estranhas, novas e excitantes. Além disso, as tentativas da Cientologia de suprimir o vídeo de Cruise serviram de convite a um ataque ao estilo vigilante para desfazer o mal causado. Outro fator era a quase neurótica postura defensiva da Cientologia. Nessa ocasião, a igreja era bem conhecida por ter utilizado táticas de intimidação contra os críticos, tanto na vida real quanto na web, o que a tornava uma perfeita "isca de troll"

para o deleite do 4chan e dos cada vez mais organizados Anons do Partyvan. As prévias rusgas da Cientologia com detratores on-line já eram tão bem conhecidas que o canadense *Globe and Mail* denominou suas tentativas de remover o vídeo de Cruise do YouTube "Cientologia *versus* Internet, parte XVII". A igreja

travava uma guerra contra os detratores on-line há quinze anos, desde os velhos tempos de grupos informativos da Usenet, como o alt.religion.scientology, em 1994, quando ex-membros enfureceram a igreja com o vazamento de documentos secretos.

Outro motivo, que costumava se aplicar às coisas aparentemente aleatórias feitas pelo Anonymous: mostrar que eram capazes. A tecnologia evoluía a ponto de qualquer pessoa com conexão de internet conseguir acessar, sem ônus, ferramentas na web como o Gigaloader e ajudar a tirar um site do ar. O vídeo de Tom Cruise e o postador original no *b* tinham entrado no momento certo. À medida que o ataque evoluía, também evoluía a oportunidade de participar. O "fogo cerrado" contra a Cientologia não amainou; se uma pessoa parasse de usar o Gigaloader, duas ou três começavam a se envolver.

Isso marcou o começo de um novo capítulo do Anonymous. A OP tinha continuado em seu segundo post: – Se conseguirmos destruir a Cientologia, poderemos destruir qualquer coisa que desejarmos!

Ela lembrou ao 4chan que seus usuários tinham de "fazer a coisa certa"

por ser o maior dos chans, mantendo a força humana de que a "legião"

precisava. O novo tópico se tornou tão popular quanto o do dia anterior, obtendo 587 respostas, inclusive as repetidas instruções para utilizar o Gigaloader e comentários como "ESTOU NESSA".

Em breve, os Anons estavam realizando ataques de DDoS a outros sites afiliados

à

Cientologia:

rtc.org,

img2.scientology.org e

volunteerministers.org. Em decorrência disso, o Scientology.org saiu do ar por vinte e quatro horas, até a igreja transferir seus servidores para uma empresa externa chamada 800hosting. Havia cerca de dez ferramentas de software distintas à escolha dos Anons para ajudar a minar os sites da Cientologia, mas a

mais popular era o Gigaloader.

A essa altura, tanta gente fervilhava no canal #xenu que se tornava impossível organizar tudo. Foi quando, no segundo dia, praticamente do nada, um Anon do sexo masculino, que também era administrador da Encyclopedia Dramatica, berrou, em maiúsculas: – GALERA VOCÊS PRECISAM CONVERSAR COM A IMPRENSA.

ELABORAR UM COMUNICADO DE IMPRENSA. ESSE NEGÓCIO É

IMPORTANTE.

Até então, ninguém havia organizado um grupo de pessoas para lidar com a publicidade, e dificilmente alguém no canal queria se candidatar.

Mas alguns se dispuseram. Com poucos cliques, uma pessoa criou um canal chamado #press, anunciou no #xenu que estava lá, e cinco pessoas se uniram. No topo do canal, estabeleceram um tópico: “É aqui onde vamos falar com a imprensa”.

Uma das pessoas que entrou no canal #press foi um homem de óculos com o rosto redondo, sentado lá em seu quarto em Boston. O quarto também servia de escritório para seu trabalho freelance em software. Nos próximos meses, Gregg Housh se tornaria fundamental para ajudar a organizar os Anons, embora, como outros no Anonymous, ele acabasse por ficar em segundo plano à medida que uma nova geração de figuras de proa, como Sabu e Topiary, emergiu mais tarde. Com raízes em Dallas, Texas, Housh adorava dar uma de troll e organizar trotes e era um visitante habitual na rede de IRC Partyvan. Tinha uma personalidade agregadora e comunicativa que desmentia qualquer aparência externa de um gênio da computação. Antes dos vinte anos, ele já havia sido preso por coordenar o compartilhamento ilegal de arquivos, e sua pena foi reduzida porque ele foi prestativo e concordou em cooperar com o FBI, de acordo com os documentos do tribunal, e o juiz levou em conta sua infância difícil. O pai de Housh havia abandonado a família quando o filho tinha apenas quatro anos, e a mãe de Housh trabalhava como faxineira, mas também cuidava de uma filha adulta com paralisia cerebral. Após um tempo fora da cadeia, Housh se esforçava para evitar confusão, já que ele também tinha uma filha pequena. Mas não pôde evitar a curiosidade pelo que estava acontecendo com a Cientologia. Precipitou-se rumo ao #press e, junto com outros participantes da sala de bate-

papo, redigiu um comunicado de imprensa chamado “O grupo Anonymous da internet declara guerra contra a Cientologia”, listando a fonte bem-humorada como “ChanEnterprises”.

Publicaram o comunicado.

Quando os participantes do canal #press leram o comunicado de imprensa, consideraram o efeito tão dramático e nefasto que decidiram que algo parecido deveria ser narrado também em vídeo. Um membro do grupo, cujo nickname era VSR, criou uma conta no YouTube chamada Church0fScientology, e o grupo passou as horas seguintes descobrindo imagens e música de domínio público, e, em seguida, redigindo um roteiro de vídeo que pudesse ser narrado por uma voz robotizada. A tecnologia de conversão de texto em fala era tão precária que eles precisaram voltar e reescrever a maioria das palavras com erros ortográficos – destroyed virou “deestroid”, por exemplo – para que o áudio soasse natural. O roteiro final terminou parecendo nonsense, mas o som era o de prosa normal.

Quando enfim fizeram a montagem, uma voz robótica ao estilo da voz de Stephen Hawking falava, enquanto a tela mostrava imagens de nuvens carregadas:

– Oi, líderes da Cientologia, somos Anonymous.

Atingia novos picos de hipérbole, prometendo “sistematicamente desmantelar a Igreja da Cientologia em sua forma atual... Para o bem de seus seguidores, pelo bem da humanidade – e pela diversão – vamos expulsá-los da internet”. Housh e o grupo de representantes publicitários não estavam levando nada disso a sério. Mas, enquanto davam os retoques finais no vídeo e brincavam sobre como essa “guerra” seria um dos mais engraçados eventos de trolling de todos os tempos, durando no máximo alguns dias, um doutorando francês que pertencia ao grupo fez uma declaração séria: – Pessoal, o que estamos fazendo hoje vai mudar o mundo – afirmou ele.

Os outros no grupo pararam por um instante e depois caíram na risada, Housh relembrou mais tarde.

– Gtfo – escreveu um. – Deixa de baboseira.

Mas o francês foi implacável: dezenas de milhares de pessoas assistiriam ao vídeo que eles estavam produzindo. Esse era o começo de algo substancial, “e a

gente nem sabe ainda o que é".

Housh e os demais deram de ombros e prosseguiram, de acordo com Housh. Chamaram o vídeo de *Mensagem à Cientologia*, publicaram-no em 21 de janeiro e postaram links em todos os chans e no Digg. Após varar a noite trabalhando no vídeo, a maioria deles foi dormir.

Na manhã seguinte, a namorada de Housh na época o acordou aos cutucões.

– Você tem que voltar ao seu computador – disse ela. – A coisa está arrebentando a boca do balão.

Housh caiu da cama, tateou desajeitado para localizar os óculos e fitou a tela. A rede de IRC Partyvan estava saindo do ar enquanto milhares de novos participantes tentavam aderir ao #xenu.

– A gente conseguiu fazer um ataque de DDos contra nós mesmos – mais tarde ele relembrou numa entrevista.

O vídeo tinha sido selecionado pelo Gawker e por outro site tecnológico chamado The Register, e milhares de pessoas haviam assistido a ele. Mais tarde naquele dia, cerca de 10 mil pessoas estavam tentando acessar o #xenu e os hosts da rede de IRC do Partyvan expeliu todos da rede. Housh e os demais tentaram manobrar para que todos se transferissem a outra rede de IRC, que imediatamente saiu do ar. Felizmente, os administradores do Partyvan voltaram, dizendo que haviam acrescentado mais cinco servidores para que a horda pudesse retornar. Agora, a maior parte da comunicação do Anonymous acontecia nos servidores de IRC do Partyvan.

Foi um turbilhão para Housh e os outros. Ao acordar e perceber que milhares de pessoas queriam participar desse trote, eles subitamente se deram conta de que as pessoas estavam prestando atenção, e que não podiam se dar ao luxo de fazer alguma besteira.

Ao longo das próximas quarenta e oito horas, o #press obteve novas adesões de pessoas que gostavam de estabelecer objetivos. Percebendo que a sala de bate-papo começava a se transformar num centro organizacional, o grupo, cujos componentes só recentemente tinham travado contato entre si, mudou o nome do canal para #marblecake. Ao escolher um nome aleatório, a sala tinha mais probabilidade de se manter privada, permitindo que eles evitassem a distração de

visitantes e se concentrassem na tarefa de organização. Nos primeiros dois dias definiram o que fazer na sequência e discutiram sobre como as massas deviam proceder.

– Não tínhamos nem ideia do que estávamos fazendo – relembra Housh.

Eles deveriam continuar a realizar ataques com DDoS contra a Cientologia? Pregar outro tipo de peças neles? Decidiram que o primeiro objetivo seria impedir o colapso do #xenu. Solicitaram aos operadores de IRC que limitassem o canal a uma centena de pessoas, de modo que qualquer excedente fosse automaticamente desligado. Depois instruíram as pessoas a que aderissem a canais sediados na cidade mais próxima à residência delas, tais como #London, #LA, #Paris ou #NY. Ao longo das seis horas seguintes, a legião se autossegregou.

Os primeiros ataques de DDoS contra a Cientologia tinham sido executados utilizando ferramentas simples da web, como o Gigaloader e o Jmeter. Em poucos dias, porém, essas ferramentas foram substituídas por aquelas que se tornariam as duas mais populares armas do arsenal do Anonymous: botnets e o Canhão de Íons de Órbita Baixa (*Low-Orbit Ion Cannon*, LOIC).

Embora o uso de botnets pelo Anonymous se disseminasse apenas anos depois, sem sombra de dúvida essa era a mais poderosa das duas armas.

Botnets são grandes redes de computadores “zumbis” que podem ser controladas por uma única pessoa digitando comandos de um canal de IRC

privado ou via rede peer-to-peer. Corre o boato de que os botnets foram utilizados somente uma ou duas vezes durante os primeiros ataques da Anonymous contra a Cientologia, embora poucos detalhes sejam conhecidos. Em geral, botnets são compostos por redes de dez mil até cem mil computadores mundo afora. Os maiores botnets, aqueles que têm o poder de desativar os servidores de pequenos governos, têm mais de um milhão de computadores. Os computadores pertencem a pessoas comuns como você e eu, sem consciência do que está acontecendo – muitas vezes a gente se vincula a um botnet ao baixar casualmente um software infectado ou visitando um site comprometido. A contaminação talvez ocorra quando alguém nos envia um por e-mail spam com um link prometendo impressões de fotos grátis ou um prêmio em dinheiro, ou quando clicamos num vídeo interessante que serve de disfarce para um código

pernicioso.

Nada parece estar errado após o download desse software. Ele se instala por conta própria de modo rápido e silencioso e, na maior parte do tempo, permanece dormente. Quando o controlador do botnet emite comandos para uma rede de “bots”, um sinal é enviado ao computador infectado, e o programinha baixado se ativa ao fundo, sem o dono se dar conta. (Quem sabe o seu computador esteja participando de um ataque de DDoS neste exato instante.) A rede de milhares de computadores age em uníssono, como se fosse um só computador. Em geral, botnets utilizam seus bots para enviar spam, descobrir vulnerabilidades de segurança em outros site ou desferir um ataque de DDoS contra um site corporativo enquanto o controlador pede resgate para sustar o ataque. Na cultura hacker subterrânea, botnets maiores se traduzem em maior crédito no mercado para os controladores, também chamados de botmasters.

Não está claro quantos computadores no mundo foram assimilados em botnets, mas o número chega ao menos a dezenas de milhões, com o maior número de computadores botinfestados nos Estados Unidos e na China. Em 2009, a Fundação Shadowserver relatou que havia 35 mil botnets identificados no mundo, mais que o dobro registrado em 2007. Em março de 2010, a polícia espanhola prendeu os três homens responsáveis pelo botnet chamado Mariposa. Descoberto em 2008 por hackers de chapéu branco (especialistas em segurança cibernética) e agentes executores da lei, o monstruoso botnet era composto por até 12 milhões de computadores zumbis e havia sido utilizado para efetuar ataques de DDoS, enviar e-mails de spam e roubar dados pessoais. Os líderes ganhavam dinheiro extra alugando a rede.

Alugar um botnet era bem menos arriscado que fazer um por conta própria e, com o conjunto certo de habilidades e contatos, era surpreendentemente fácil de encontrá-los. Um estudo feito em 2010 pela VeriSign, empresa de infraestrutura na web, mostrou que o valor médio para alugar um botnet no mercado subterrâneo era de US$ 67 por vinte e quatro horas e apenas US$ 9 por hora. Alugar um botnet capaz de desativar os servidores de um pequeno governo custava por volta de US$ 200 por hora. Nos ataques da Chanology, em 2008, e na Operação Vingança em 2010-2011, o Anonymous utilizou tanto botnets alugados quanto criados por conta própria, e fontes afirmam que também existiam botnets de diversos tamanhos. Mas os superbotnets, controlados por um punhado de pessoas, eram os mais potencialmente danosos.

A segunda arma no arsenal do Anonymous era o Canhão de Íons de Órbita Baixa, cujo acrônimo se pronuncia “lo-ick”. Em termos de poder, era irrisório em comparação a um botnet – como a diferença entre um míssil de longo alcance e uma pistola –, mas o software era grátis e fácil de acessar por qualquer usuário de computador. Desde o início do Chanology em diante, o LOIC começou a substituir o Gigaloader em popularidade. As origens do programa de software são um tanto obscuras, mas considera-se que tenha sido projetado por um programador com o nickname Praetox, com o objetivo legítimo de carregar servidores de teste na web. Em 2008, aos dezoito anos, morador de Oslo, Noruega, ele gostava de programação e “de correr na floresta”, de acordo com seu site.

Praetox fazia todo tipo de coisa em seu computador, inclusive trapaças para o RPG on-line Tibia e um programa que tornava transparentes as janelas da área de trabalho de um computador. Também era conhecedor da cultura chan e utilizava a imagem de desenho animado com um cartaz onde se lia “Piscina fechada” em sua conta do YouTube. O próprio nome LOIC se origina de uma arma da série de videogame Command & Conquer e, entre todas as suas criações, se destacaria como o legado de Praetox.

Ao que parece, Praetox criou originalmente o LOIC como um projeto de código aberto, ou seja, qualquer pessoa poderia aprimorá-lo. Por fim, um programador com o nickname de NewEraCracker fez melhorias que permitiam ao LOIC enviar solicitações inúteis, ou “pacotes”, a um servidor, tornando-o o que ele é hoje em dia. Pacotes de dados são parte de tudo que alguém faz na internet. Visitar uma página da web envolve uma série de pacotes, como também enviar um e-mail, com um pacote típico contendo de 1000 a 1500 bytes. Pacotes podem ser comparados aos envelopes endereçados utilizados no serviço postal. “Interceptação de pacotes”

significa desvendar o conteúdo de um correio espiando-se o interior do envelope. Os dados no interior de um arquivo podem ser criptografados, mas o próprio pacote sempre identificava o remetente e o destinatário.

De certa forma, um ataque de DDoS (negação de serviço distribuída) era como sobrecarregar alguém com milhares de mensagens de lixo eletrônico que a vítima não tinha alternativa senão abrir. Uma defesa era “filtrar os pacotes”, algo como pedir a um porteiro para não aceitar correio de certo remetente. Mas proteção contra DDoS exigia investimentos, e era difícil filtrar os pacotes de lixo

eletrônico do LOIC, oriundos de tantos usuários diferentes. Em última análise, se pessoas suficientes utilizassem o programa e "alvejassem" o mesmo site ao mesmo tempo, elas o sobrecarregavam com tráfego de lixo eletrônico capaz de derrubá-lo. O

efeito era parecido com o de um botnet, só que, em vez de ter computadores infectados, as pessoas participavam voluntariamente da rede. Uma diferença fundamental centreva-se na eficácia. O efeito do LOIC

era bem mais imprevisível em comparação aos botnets tradicionais, pois entravam em cena elementos como popularidade e erro humano. Seriam necessárias 4 mil pessoas para derrubar o site de uma grande empresa, como seriam necessárias 4 mil pessoas manejando pistolas para destruir um pequeno edifício. Seriam necessárias apenas poucas centenas de pessoas para tirar do ar um diminuto site feito em casa, pertencente a um indivíduo. A vantagem residia no fato de que baixar o LOIC era grátis e fácil – você podia baixá-lo de um site torrent ou do painel *rs* do 4chan.

***

Uma das centenas de pessoas que baixaram o LOIC e participaram de alguns dos pioneiros ataques de improviso à Cientologia foi um aluno da Iowa State University, Brian Mettenbrink. Aos dezoito anos, com cabeleira e barbicha castanhas, Mettenbrink, diante do computador de mesa no quarto do dormitório, navegava em seu site predileto, o 7chan, quando vislumbrou pela primeira vez posts sobre um ataque contra a Cientologia, em janeiro de 2008. Ele não se importava com a Cientologia, mas se interessava em explorar o mundo da segurança na Tecnologia da Informação (TI), e raciocinou que participar de um ataque desses era uma boa maneira de aprender sobre o outro lado da moeda. Além disso, com tantas outras pessoas contribuindo com o ataque, ele não seria capturado.

Mettenbrink, visitante habitual do 4chan desde os quinze anos, entrou no painel *rs* do site e baixou o LOIC. Poucos segundos depois o download estava concluído e incluía um arquivo "leia-me" para explicar como utilizá-

lo. O programa dava a impressão de conectar usuários a um exército de combatentes rebeldes. Quando Mettenbrink abriu pela primeira vez o LOIC, a janela principal que apareceu tinha um design ao estilo de *Guerra nas estrelas*:

caixas de texto em verde-claro e verde-escuro e uma maquete modificada por Photoshop do canhão de íons antiorbital utilizado em *Guerra nas estrelas: a guerra dos clones*, disparando um espesso raio laser esverdeado na direção de um planeta.

Havia opções para “Escolha um alvo”, por meio da inserção de um URL, e um botão dizendo “Bloquear”. Tão logo você tivesse um alvo bloqueado, uma grande caixa no meio mostrava o endereço de IP do servidor do alvo, enquanto o programa se preparava para um ataque. Em seguida surgia outro botão com o rótulo “TÔ CARREGANO MEU LEIZER”, seguido de opções para configurar o ataque. Durante os primeiros ataques de DDoS

contra a Cientologia, o LOIC sempre estava no “modo manual”, ou seja, os usuários decidiam onde e quando disparar e qual tipo de pacote de lixo eletrônico enviar.

Assim que um ataque estivesse em andamento, uma barra de status no rodapé mostrava a situação do programa: Ocioso, Conectando, Solicitando, Baixando ou Falha. Com status “Solicitando”, um número começava a aumentar rapidamente. Tão logo congelasse, isso significava que o LOIC

tinha travado ou o alvo tinha sido derrubado. Você podia conferir visitando o site alvo – se recebesse uma mensagem de erro “Tempo limite da rede”, isso queria dizer missão cumprida.

Mettenbrink não sentiu empolgação ou emoção ao disparar pela primeira vez o LOIC contra o Scientology.org, principalmente porque o programa congelou tão logo foi iniciado. Ele conferiu as configurações e, quando o programa voltou a funcionar, minimizou a janela e recomeçou a navegar ociosamente no 7chan. Ao contrário de Gregg Housh, Mettenbrink foi um participante casual do Chanology. Não se interessava em participar de um canal de IRC como o #xenu nem em descobrir o que os Anonymous fariam a seguir. Em vez disso, ele manteve o LOIC rodando por vários dias e noites a fio em segundo plano no seu computador, por fim se esquecendo completamente de que o programa estava funcionando. Só o desativou ao notar que começava a afetar a velocidade de sua conexão com a internet – cerca de três dias depois de iniciá-lo.

– Não sou responsável pelo modo com que você utiliza esta ferramenta – escrevera NewEraCracker, o programador do LOIC, como aviso de isenção de

responsabilidade a quem baixasse sua versão aprimorada na web. – Você não pode me culpar se for flagrado atacando servidores cujo dono não seja você.

As pessoas que utilizavam o LOIC não poderiam rodá-lo por meio da popular rede de anonimato Tor, já que isso perturbaria a própria rede. O

resultado era um festival de apoiadores desinformados como Mettenbrink rodando o LOIC diretamente de seus computadores e deixando expostos seus endereços IP. Com frequência, eles não percebiam que era ilegal utilizar o LOIC desse modo.

Como se isso não bastasse, mais Anons se comunicavam em redes de IRC, ou seja, eles tinham nicknames e reputações a zelar. Agora não havia apenas a atração de participar de uma gangue – havia um senso de obrigação para retornar e contribuir com ataques futuros. Alguns participantes de um canal de IRC do Projeto Chanology sabiam, por exemplo, que retornar ao canal de IRC no dia seguinte também significava reencontrar-se com um novo e estável círculo de amigos on-line, que talvez os desprezassem caso eles não aparecessem. Não era como no *b*, onde você podia desaparecer subitamente e ninguém percebia.

O Projeto Chanology se transformava numa nova comunidade de centenas de pessoas, a ponto de a comunicação do grupo gradativamente começar a se fracionar entre painéis de imagem e redes de IRC. Os painéis de imagem como o 4chan já utilizavam o LOIC há uns dois anos; os *b*tards eternamente declaravam guerra contra outros sites que, defendiam eles, roubavam o crédito de seus memes e seu conteúdo, como o eBaum’s World ou o site de blogs Tumblr. Porém, agora mais Anons começavam a utilizar redes de IRC para coordenar e seguir instruções em ataques de DDoS. A partir de janeiro de 2008, os organizadores também haviam iniciado a publicação de anúncios e guias sobre o projeto Chanology na rede Partyvan, de modo que o repentino exército de milhares de “newfags” do mundo pudesse participar desses novos protestos on-line, aprendendo sobre LOIC e canais de IRC sem precisar perguntar.

Os ataques de DDoS contra a Cientologia atingiram o ápice em 19 de janeiro, quando o site principal da igreja foi atingido por 488 ataques de computadores distintos. Vários órgãos da mídia, como o Fox e o Sky News, relataram que perturbações on-line estavam sendo causadas por uma “pequena gangue de super-hackers”. Esse era um ponto de vista redondamente enganado. Pouquíssimos apoiadores do Anonymous são hackers talentosos. O maior

número é composto de simples e jovens usuários da internet que sentiam a vontade de fazer algo além de matar tempo no 4chan e no 7chan.

Quando alguém postou um anúncio no Partyvan de que haveria um terceiro e maior ataque de DDoS em 24 de janeiro, supostamente cerca de quinhentas pessoas participaram. Mas a essa altura a Cientologia já havia contratado a Prolexic Technologies, empresa especializada em proteção contra DDoS sediada em Hollywood, na Flórida, para ajudar a proteger seus servidores. Logo o efeito dos ataques realizados com LOIC cessou, e os sites da Cientologia funcionavam normalmente.

A Cientologia então contra-atacou por meio da mídia, contando à *Newsweek* no começo de fevereiro que o Anonymous era "um grupo de terroristas cibernéticos [...] perpetrando crimes de ódio religioso contra as igrejas da Cientologia". As palavras contundentes não auxiliaram a causa da Cientologia, levando em conta uma famosa expressão da internet: "Não alimente o troll". Com a postura defensiva, a Cientologia inadvertidamente acabou provocando mais Anons a participarem dos ataques. E como entrar no Anonymous era tão fácil – bastava entrar num canal de IRC, ou no *b*, e participar da conversa –, centenas de novas pessoas começaram a aderir.

Então o Anonymous encontrou uma nova maneira de provocar agitação. De volta ao #marblecake, Housh percebera o silêncio de um membro da equipe nos últimos quatro dias. Ele havia solicitado ao membro que calculasse quantas cidades e países estavam sendo representados na rede de bate-papo. Ao voltar, a sentinela avançada relatou que havia entre 140 e 145 canais diferentes no Chanology e participantes de 42 países no total.

– O que fazemos com toda essa gente? – perguntou um componente da equipe.

Eles começaram a vasculhar a internet para ver o que os adversários da Cientologia tinham feito no passado e toparam com um vídeo de um expoente da causa anticientológica, Tory "Magoo" Christmam, que dançava e gritava diante de um centro de Cientologia.

– Isto é hilário – comentou um membro da equipe. – A gente devia fazer a internet sair da toca.

– Temos de colocá-los nas ruas – diagnosticou o membro francês que cursava o doutorado.

Housh não concordou e discutiu com o francês durante três horas. Por fim, Housh deu o braço a torcer, decidindo que uma confrontação entre os Anons e o público no mundo real poderia ser bastante divertida.

– Pensávamos honestamente que a coisa mais engraçada que podíamos fazer contra a Cientologia era protestar diante de seus templos – afirmou Housh mais tarde.

O grupo começou a trabalhar no próximo vídeo, sua "convocação às armas", e em seguida em um código de conduta após um ativista do Greenpeace dizer no IRC que eles precisavam se assegurar de que os manifestantes não jogassem coisas nos prédios nem esmurrassem policiais.

Housh assumiu um papel organizacional cada vez maior, delegando responsabilidades e mantendo o foco da discussão quando a conversa dispersava em piadas sobre bombardeios ou jogos Xbox.

Em 26 de janeiro, alguém que se chamava "Anon Ymous" enviou um email para o endereço de "dicas" do Gawker, sobre um protesto vindouro defronte à Igreja da Cientologia no Harlem.

– Utilize uma máscara de sua escolha – dizia o comunicado. – Traga aparelho de som portátil. Vamos rickrolleá-los até eles se renderem. Vamos fazer notícia LOL.

Também havia um slogan embaixo, que aparecia no YouTube, blogs e posts de fóruns: Somos Anonymous Somos Legião

Não perdoamos Não esquecemos Esperem por nós.

Essa hoje famosa assinatura, reminiscente dos Borg, os vilões de *Jornada nas estrelas*, vinha das 47 Regras da internet. Após as regras 1 e 2, que pregavam nunca falar sobre *b*, vinham: Regra 3. Somos Anonymous.

Regra 4. Anonymous é legião.

Regra 5. Anonymous nunca perdoa.

Alguns defendem que a legião na regra 4 vem da passagem bíblica de Marcos 5:9, na qual Jesus se aproxima de uma pessoa possuída por demônios.

“E Ele [Jesus] indagou ao homem: – Qual é teu nome?

E o homem respondeu: – Meu nome é Legião: pois somos muitos.”

O vídeo *Mensagem à Cientologia* publicado no YouTube dizia: – Se quiser outro nome para seu adversário, então nos chame de Legião, pois somos muitos.

Ao longo dos meses seguintes, mais pessoas do 4chan, 711chan e de redes de IRC participavam de protestos no mundo real. Em 2 de fevereiro de 2008, cerca de 150 pessoas se uniram pela primeira vez fora de um centro da Igreja da Cientologia em Orlando, na Flórida. Uma semana depois, o jornal *Tampa Bay Tribune* relatou que 7 mil pessoas tinham protestado contra centros da igreja em 73 cidades mundo afora. Com frequência os manifestantes eram adolescentes e jovens adultos, que ficavam agrupados em pé ou sentados em cadeiras de praia, segurando cartazes com memes da internet e gritando palavras de ordem aos transeuntes. Alguns participantes consideravam as manifestações divertidas, um sofisticado trote da própria internet contra uma organização estabelecida. Muitos outros levavam os protestos a sério e seguravam cartazes com os dizeres “A $ientologia mata”. Uma conta associada ao Anonymous publicava no YouTube um noticiário frequente chamado AnonyNews. O apresentador relatava os protestos da vida real mundo afora. Vestia terno escuro e gravata vermelha, cabelo penteado para trás e a risonha máscara branca usada pelo protagonista V no distópico filme *V de vingança*, que rapidamente se tornava um símbolo do Anonymous. Isso se devia a uma cena emblemática do filme, que mostrava milhares de pessoas usando a máscara do V em solidariedade ao protagonista, vagamente inspirado no revolucionário britânico Guy Fawkes.

Essa máscara do V aparecia em todos os protestos do Anonymous, escondendo os rostos dos manifestantes de modo que, pelo menos de certa forma, continuassem anônimos no mundo real. Ao longo do tempo, a máscara passaria a representar os 50% de componentes do Anonymous que levavam a sério a ideia de revolução e protestos. Gente como William, que considerava que o Anonymous devia se destinar a brincadeiras e trotes, abominava a máscara. (Por volta de 2001, a Time Warner lucrava com a venda de mais de 1 milhão de máscaras V, enquanto outras máscaras associadas com seus filmes vendiam a metade desse número.) Quando os transeuntes se aproximavam dos manifestantes para perguntar quem tinha organizado os protestos, os ataques de DDoS, os trotes e os ataques cibernéticos, ninguém sabia dar uma resposta oficial. A maioria dos voluntários habituais não percebia os grupinhos de

autonomeados organizadores que mexiam os pauzinhos nos bastidores.

Mas os protestos presenciais funcionavam e, quando eles começaram a se espalhar, Housh recordou a sentinela avançada que havia computado todos os diferentes países e canais citadinos e, supondo que ele gostava de trabalho pesado, pediu-lhe que entrasse nos canais de todas as principais cidades e procurasse a pessoa que aparentemente dava ordens e assumia a responsabilidade geral.

– Procure-a em Paris, Londres, Nova York – disse Housh.

O batedor passou os próximos três dias visitando uma gama de salas de bate-papo e identificando as mentes organizacionais, alguém que parecesse especialmente dedicado à causa. Em seguida estabelecia uma conversa particular com cada um deles, perguntando se tinham assistido ao primeiro vídeo *Mensagem à Cientologia* e acrescentando: – Um dos sujeitos que fez o vídeo quer falar com você.

Intrigados e provavelmente um tanto ansiosos, eles seriam então direcionados ao #marblecake e recomendados a não contar a ninguém sobre o canal. Housh lhes explicava: – Não estamos tentando controlar todo mundo, mas sim trazer listas com sugestões e torcer para que as pessoas concordem.

Ao longo dos dois meses seguintes, o #marblecake se expandiu para cerca de 25 membros talentosos, inclusive designers da web capazes de montar um site num dia e pessoas com tarimba organizacional que sabiam ligar para a polícia e obter permissões para realizar protestos.

Lá pelo fim de março, algumas pessoas também já tinham configurado novos sites para o projeto Chanology, inclusive fóruns de discussão. Esses locais serviam como ponto de encontro da comunidade do Chanology, e dois sites populares se destacaram: Enturbulation.org e WhyWeProtest.net.

Já não se discutia mais o Chanology no 4chan – o projeto se mudara definitivamente para esses sites e canais de IRC. Nos próximos meses, o Anonymous continuou a promover protestos geralmente pequenos e presenciais mundo afora, enquanto Housh ajudava a realizar encontros frequentes a cada três dias no #marblecake para discutir estratégias de ataque contra a Cientologia.

Os encontros duravam em média de três a seis horas, relembra Housh.

Ele postava uma pauta de assuntos, escutava os relatórios do que as pessoas tinham feito e distribuía missões, desde criar um site até bolar um folheto para anunciar o próximo ataque ou escolher a música de fundo para o próximo vídeo do YouTube. O grupo tentava planejar os eventos do Anonymous para o mês seguinte. Antes disso, ninguém na prática havia programado ataques ou trotes do Anonymous com antecedência.

Segue um exemplo da "pauta" do canal #marblecake com base no registro do bate-papo em 6 de junho, sexta-feira: **03[19:44] *Pauta é "comunicados de imprensa, vídeos, ideias, colaboração, basicamente coisas que precisamos fazer. || Encontro nas noites de sexta-feira às 21h horário da costa leste || /msg srsbsns para cosnews.net writefagaccounts ||**

vocês devem pensar em coisas que vocês odeiam no estado atual do chanology e querem modificar".

03[19:44] *Enviado por gregg em Sex Jun 06 19:27:08

– Comecei a gerenciar com pulso de ferro – conta ele. – Raros [encontros] eram perdidos.

Se alguém não conseguisse comparecer a um encontro, podia ler um doc no Google para se atualizar.

***

Por volta de junho, as motivações se arrefeciam e as pessoas no #marblecake sentiam saudade de quando o Chanology havia sido lançado em janeiro.

– Eu adorava os velhos tempos – disse um usuário chamado 007, numa reunião de junho. – Ninguém sabia o que ia acontecer IRL [*in real life*]. Todo mundo participou de corpo e alma. Eu queria que a gente conseguisse a mesma participação de antes.

A partir de junho de 2008, o Projeto Chanology começou a padecer de rivalidades internas entre os organizadores, e o número de manifestantes em protestos presenciais, ocorridos mensalmente nas grandes cidades, minguava. Housh considera que o ainda incipiente movimento recebeu um golpe duro naquele verão, quando uma dupla de Anons, com os apelidos de King Nerd e Megaphonebitch, expuseram o #marblecake e as pessoas que dele participavam,

rotulando-as de “leaderfags” e incitando a maioria das pessoas que começou o centro organizacional a abandoná-lo. Nos meses seguintes, o Chanology não teria um fim oficial; em vez disso, de modo informal, foi aos poucos se extinguindo. Muitos Anons estavam simplesmente entediados com o Projeto Chanology, sob qualquer ponto de vista, a mais longa e importante série de ataques que o Anonymous já havia perpetrado contra um alvo isolado desde a sua criação.

O Federal Bureau of Investigaton, nesse meio-tempo, apenas começava a entrar em cena. Também por volta de junho, o FBI (ou “feds”, como os Anons os chamavam) conseguira rastrear e deter duas entre as centenas de pessoas que participaram dos ataques de DDoS contra a Cientologia. Eles seriam os azarados bodes expiatórios e representariam as primeiras de muitas outras detenções ao longo dos anos seguintes. Os Anons sempre tinham pensado, até então, estar imunes à prisão ou bem escondidos das autoridades. Um dos primeiros a descobrir a dura verdade foi Brian Metterbrink, o enfarado universitário que em janeiro de 2008 havia deixado o LOIC rodando em segundo plano em seu computador por um tempo um pouco excessivo.

– Brian.

– Sim.

Brian Mettenbrink dormia no sofá do porão quando escutou a voz de seu companheiro de residência chamando-lhe. Manhã gelada de meados de julho de 2008, seis meses após ele ter baixado o LOIC e participado do primeiríssimo ataque do Anonymous contra a Cientologia. Ele mal se recordava daquele fim de semana enfurnado a maior parte do tempo no dormitório. Desde então, havia abandonado as aulas de engenharia aeroespacial na Iowa State, mudando-se com alguns camaradas para uma casa maior, verde-ervilha, em Omaha, Nebraska, e começado a procurar um emprego que o ajudasse a pagar o aluguel.

– Tem uns senhores aí que querem falar com você.

Sentou-se empertigado. Com olhar sonolento, Mettenbrink subiu tateante a escadaria e foi até a porta, trajando a mesma roupa com a qual dormira – camiseta lisa e bermuda. Dois homens vestindo ternos esperavam no degrau da porta. Sacaram distintivos e se identificaram como agentes do FBI. Perguntaram a Mettenbrink se ele tinha tempo para uma “conversa amigável”. Mettenbrink

respondeu que sim e convidou-os para entrar. Ele ainda não fazia ideia de que isso tinha a ver com os ataques de DDoS.

Os agentes passaram pelo pórtico arqueado da casa de Mettenbrink, os sapatos estalando contra as lajotas do piso enquanto adentravam na sala de jantar e sentavam-se junto a uma mesa de madeira. Mettenbrink ajustou no nariz os óculos de aros redondos. Nesse ponto, ele ainda estava mais alheio aos fatos do que nervoso. Os agentes começaram a fazer perguntas sobre os ataques de janeiro e sobre o próprio Anonymous.

– O que o Anonymous pensa sobre a Cientologia? – indagou um deles. – Qual a postura do grupo?

– Sei que o Anonymous não gosta da Cientologia – disse Mettenbrink, contando a rajada de posts animados sobre o ataque contra a Cientologia no 4chan e no 7chan. – Eles falavam que tínhamos de atacar os sites da igreja.

Mettenbrink estivera lendo sobre a Cientologia após os ataques e acrescentou que as crenças da religião eram “estranhas” e que cobravam centenas de dólares das pessoas interessadas em aderir.

– Envolveu-se nos ataques de DDoS? – indagou um dos homens.

Mettenbrink se remexeu na cadeira.

– Eu me envolvi um pouco – reconheceu.

O computador que ele havia utilizado para rodar o LOIC agora estava instalado no porão.

– E... gostou de participar dos ataques?

– Sim – falou Mettenbrink, recordando o quanto ele achava sem graça a universidade. – Foi divertido. Uma coisa nova e interessante para fazer.

– Sabia que seus atos eram uma violação criminal? – perguntou um dos agentes.

– Claro – respondeu Mettenbrink. – Só não imaginava que ia abria a porta e topar de cara com o FBI.

Fitou os dois homens. Mettenbrink sempre soube que o uso do LOIC era ilegal, mas não imaginava a gravidade da violação. Acreditava que o crime era tão sério quanto passar o sinal vermelho, com punição semelhante a uma multa por excesso de velocidade no valor de cem dólares. Mais tarde ele se arrependeria de ter sido tão franco com os agentes.

Os dois homens então revelaram que uma investigação do FBI demonstrara que um endereço IP utilizado nos ataques remetia ao computador de Mettenbrink.

– Entende isso? – indagaram.

– Sim – disse ele.

– Conhece alguém do grupo na vida real? – interpelou um dos agentes.

– Não – respondeu Mettenbrink.

A “conversa amigável” durou cerca de uma hora, fornecendo ao FBI e, mais tarde, aos advogados da acusação, representantes da Igreja da Cientologia, provas para utilizar contra o desafortunado Mettenbrink. Mais tarde, o FBI entraria em contato com a antiga universidade que o rapaz cursava para acessar seus registros na internet. Mettenbrink não teve notícias do FBI durante meses, e um ano se passou até que ele realmente percebesse, em uma conversa com seu advogado, a gravidade do crime.

– Tem ideia do dano financeiro que a Igreja da Cientologia alega que você causou? – perguntou o advogado durante uma das reuniões com Mettenbrink.

O rapaz parou um tempo para pensar.

– Nem sonhava que tinha havido dano financeiro – comentou.

Tudo que ele havia feito era ajudar a enviar um monte de lixo eletrônico a um site e deixá-lo lento por alguns dias.

– Cem mil dólares – informou o advogado. Mettenbrink ficou atônito.

Ele havia atacado o Scientology.org por um capricho, sua arma foi um programa frágil e disponível gratuitamente que ele havia rodado em segundo plano por três dias enquanto navegava num painel de imagem.

Como poderia ter custado a alguém cem mil dólares?

Por fim, a Cientologia baixou sua estimativa de danos para 20 mil dólares. Mettenbrink teria de pagar tim-tim por tim-tim, mas pelo menos não era cem mil. Os advogados da acusação, representantes da Igreja da Cientologia em Los Angeles, também solicitaram um ano de cadeia, acrescentando que uma sentença probatória, ou que evitasse o cumprimento da pena na prisão, "poderia encorajar outros a utilizar a internet para participar de crimes de ódio".

Conforme o memorando de sua sentença, Mettenbrink recebera "todas as vantagens na vida", com raízes numa família unida e "solidária" no Nebraska e com pais que o ajudaram a financiar seus estudos universitários. Ele também foi acusado de ter "habilidades especiais" com computadores e hardwares. No tribunal, um advogado da Cientologia utilizou palavras como *nazistas* e *terrorismo* ao descrever o Anonymous.

Em 25 de janeiro de 2010, quase dois anos depois do dia em que baixou a ferramenta do LOIC, num tribunal federal, Mettenbrink foi considerado culpado por acessar um computador protegido, tendo concordado em cumprir um ano de cadeia. Ele seria apenas a segunda pessoa a ser responsabilizada criminalmente por um ataque DDoS do Anonymous. Em novembro de 2009, Dmitriy Guzner, de dezenove anos, morador de Verona, Nova Jersey, tinha sido condenado a um ano de prisão numa penitenciária federal.

Nesse meio-tempo, os especialistas em segurança de TI coçavam a cabeça para entender essa nova raça de hacktivistas que parecia ter saído do nada. A Prolexic, empresa de segurança que obtivera certa experiência ao proteger a Cientologia dos ataques de DDoS, tinha algum conselho para futuros alvos do Anonymous: – Não cutuque a onça com vara curta – recomendou a empresa, acrescentando que, tão logo um ataque de DDoS terminasse, era melhor não tocar mais no assunto. – Não emita avisos nem ameaças aos agressores via mídia; isso só vai manter o assunto em pauta, acirrar os ânimos e aumentar muito a possibilidade de novos ataques. A maioria das pessoas que faz ataques de DDoS quer publicidade, então não lhes entregue isso de bandeja.

A Cientologia, é claro, fizera exatamente isso.

O que pouca gente se dera conta é que, embora Anonymous tivesse reagido às provocações da Cientologia, seus participantes também se dividiram em duas

facções. As pessoas já tinham percebido isso nas manifestações, com as diferenças entre os cartazes rabiscados com gracejos e aqueles com críticas rigorosas contra a Cientologia. Essa era a evolução de uma divisão fundamental entre os que acreditavam nas raízes do Anonymous de diversão e lulz e a nova direção ativista pela qual o grupo enveredava. Nos anos seguintes, essa separação nas motivações tornaria mais difícil definir o que o Anonymous tentava ser. Isso inclusive criaria um abismo entre Topiary e Sabu. E, à medida que o Chanology começou a definhar, entraria em cena um dos maiores adversários futuros de Sabu.

CAPÍTULO 6

Guerra civil

Embora a maioria dos participantes do Anonymous consistisse em jovens solteiros do sexo masculino, as mulheres também participavam, algumas delas casadas e com filhos. Quando a notícia sobre o Chanology chegou à Califórnia, Jennifer Emick, uma mulher casada, mãe de quatro filhos, decidiu investigar o assunto. Aos 36 anos, com cabelo preto e bijuteria celta, Emick ficou intrigada com as informações fragmentadas que ouvia sobre o Chanology. Quando ela era mais jovem, um membro da família se envolvera com a Cientologia e tivera uma experiência aterradora, convencendo Emick de que a igreja era maligna. Ela acabou se tornando escritora especializada em novos movimentos religiosos e em simbolismo religioso. Na época em que o Projeto Chanology surgiu, Emick redigia esporádicos artigos sobre religião e temas esotéricos para o About.com, site informativo afiliado ao *New York Times*.

Munida de um caderno, ela compareceu a um dos primeiros protestos do Anonymous diante de um centro da Cientologia em São Francisco, em 10

de fevereiro de 2008, para escrever uma reportagem. Havia entre duzentos e trezentos manifestantes no evento, inclusive ex-celebridades cientologistas e o filho do fundador L. Ron Hubbard. No mesmo dia, cerca de oitocentos sectários do Anonymous compareceram a protestos defronte aos centros da Cientologia na Austrália, e mais em Londres, Paris, Berlim, Nova York, Los Angeles, Chicago, Toronto e Dublin. Cerca de 7 a 8 mil pessoas participaram, em 93 cidades ao redor do mundo, conforme relatos dos noticiários locais. Mas Emick viu além da postura brincalhona dos manifestantes. Ficou fascinada pelo fato de essas novas manifestações parecerem tão decisivas. Emick resolveu voltar a outro protesto no mês seguinte, agora como participante.

Ela gostava do bom comportamento dos manifestantes em relação à força policial. Eles também ficaram igualmente impressionados com a personalidade enérgica de Emick e sua habilidade em lançar argumentos sólidos aos representantes da igreja. Eles a nomearam uma colaboradora especialista em Cientologia. Emick explicou que as táticas de intimidação da igreja eram perfeitamente normais. Os representantes da Cientologia tinham seguido os manifestantes até suas casas, acusando-os de “perpetrar crimes de ódio religioso”. No evento de Los Angeles, em março, um homem considerado por alguns manifestantes como defensor da Cientologia brandiu uma arma contra a

multidão. Um manifestante começou a segui-lo com um letreiro em que se lia: “Este homem tem uma arma”. Emick observou que, quanto mais a Cientologia reagia, mais entusiasmados ficavam os manifestantes. A irascível defensividade da organização a transformou na perfeita isca de troll.

À medida que mais partidários do Anonymous publicavam pesquisas sobre a Cientologia on-line, eles descobriam novos motivos para manter a luta.

– As pessoas pensavam: “Minha nossa, eles não são apenas loucos de pedra; eles machucaram outras pessoas” – recordou Emick alguns anos mais tarde.

Quando um pesquisador deparou com uma suposta lista de desertores da Cientologia assassinados, a postura em relação à igreja tornou-se consideravelmente mais sombria. A Cientologia deixara de ser um joguete doido e se transformara numa organização perversa, e os manifestantes sentiam que merecia ser punida e exposta. Emick abraçou a causa. Isso agora era ativismo puro.

Claro, nem todos gostavam do rumo que a coisa tomava. O ativismo não era o objetivo do Anonymous, alguns defendiam, e traía as origens do grupo de diversão e lulz. Muitos dos *b*tards originais que haviam incitado um ataque contra a Cientologia agora criticavam a continuidade da campanha por ter sido sequestrada por “moralfags”.

Um desses críticos era Wesley Bailey. Alto, magricela, com corte militar, Bailey, aos 27 anos, atuava como administrador de rede do exército, com sede numa base militar na empoeirada cidade de Killeen, no Texas. Em meados de 2008, ele era casado e tinha um casal de filhos pequenos.

Familiarmente, vivia de modo anticonvencional: Bailey e a mulher praticavam swing, e ele adorava passar horas surfando na web e batendo papo on-line. Quando topou a primeira vez com o 4chan, ficou confuso pelo anonimato compulsório e perturbado pela intensa criatividade e pelas imagens chocantes. Demorou meses para se acostumar com as expressões e o pornô esquisito, mas lentamente foi fisgado. Deu-se conta de que esse era um local incomparável onde as pessoas podiam dizer o que lhes desse na telha, não importa o quão sombrio ou inadequado. Também gostava de justiça vigilante, observando alguém postar no *b* a foto de um notório pedófilo e incitando um monte de gente a descobrir seu nome e endereço.

Ele começou a ver o termo “Anonymous” usado para definir uma entidade e compreendeu seu poder. Ao deparar com uma série de posts no 4chan sobre o Projeto Chanology, inclusive extensos artigos sobre a Cientologia produzidos por outros sites, como o Enturbulation.com, percebeu que esse era um novo nível de trote coletivo e atormentação on-line.

A exemplo de Emick, Bailey foi conferir um dos protestos simultâneos mundiais em 10 de fevereiro, em Houston, no Texas. A exemplo de Emick, ele também ficou fascinado com os manifestantes, mas não devido ao bom comportamento ou à colaboração. Atacar os cientologistas era divertido.

Ele viu uma mulher desenhar símbolos ocultos na calçada diante do centro de Cientologia, depois aspergir talco ao redor dos símbolos e acrescentar velas pretas bruxuleantes. A ideia era assustar os cientologistas, profundamente apreensivos com a magia negra e o ocultismo. Uniu-se a outros Anons para oferecer bolo aos cientologistas caso eles viessem participar do protesto. Isso era uma referência ao meme “delicious cake”.

Também reproduziram uma versão em áudio do OT3, conjunto de documentos confidenciais que os cientologistas acreditam levá-los a um estado espiritual chamado de Espírito Operativo. Os adeptos não devem escutá-los nem lê-los até estar preparados. Bailey achou aquilo hilário.

– Mas daí – lembrou-se ele poucos anos mais tarde –, eles pararam de sair para interagir.

No final de 2008, a Cientologia interrompeu as respostas, e as manifestações e os ciberataques cessaram completamente. Bailey e Emick ficaram no meio do turbilhão de brigas internas que se seguiu.

Aconteceram tremendos arranca-rabos entre os operadores de rede de IRC e os administradores do Partyvan, entre as pessoas que comandavam os fóruns do Anonymous e entre os organizadores dos protestos. Havia discórdia entre os anticientologistas originais que atuavam bem antes de surgir o dilúvio do Anonymous. Emick lembrou-se de um bate-boca entre duas organizadoras, uma acusando a outra de sair com o marido dela, e então “colocando na geladeira” amizades mútuas para criar uma ruptura. A guerra de palavras alcançou altos níveis de machismo – afinal de contas, essa era a internet.

Emick recorda-se de alguém ter falado: – Você não tem nem ideia de com quem

está se metendo. Só espere para ver o que vem por aí.

***

Se 2008 marcou a eclosão do Anonymous no mundo real com manifestações bem organizadas, 2009 representou o desenrolar de um caótico drama eletrônico. A maior disputa era sobre o objetivo do Anonymous. Ativismo? Ou lulz? E seria travada por moralfags como Emick e trolls como Bailey?

No final de 2008, pouco antes de ser destacado pelo exército a uma missão de um ano na Coreia do Sul, Bailey havia criado o site ScientologyExposed.com. Os protestos minguavam, mas os Anons continuavam a se comunicar on-line, embora mais caoticamente. A ideia de Bailey era criar uma alternativa ao site de Gregg Housh, o mais popular Enturbulation.com (que se transformou no site de aparência sofisticada WhyWeProtest.net). A essa altura, Housh, após ter o nome exposto, já dera muitas entrevistas a jornais e repórteres de televisão sobre o Anonymous e o Enturbulation era cria dele. Contou aos jornalistas que de maneira alguma ele era um "porta-voz" do Anonymous, já que ninguém podia falar em nome do grupo, mas apenas um observador. Nessa ocasião, ele já havia sido levado aos tribunais. A Igreja da Cientologia tinha processado Housh por invasão, assédio criminal, perturbação de uma assembleia de culto e perturbação da paz. Quando os protestos estavam em seu auge, um porta-voz da Cientologia contou à CNN que a igreja era alvo de "seis ameaças de morte, bombardeios e atos de violência" e vandalismo pelo Anonymous.

Housh não se enquadrava realmente no estereótipo de um ativista, mas Bailey não gostava dele nem de seu site.

Bailey acreditava que as pessoas que giravam em torno do Enturbulation eram muito sinceras, muito "moralfaggy" para ser eficazes. O

site de Housh tinha se tornado o ponto de encontro *de facto* e precisava existir uma alternativa. Bailey projetou seu site para encorajar pegadinhas e trollagem em vez de ativismo pacífico contra a igreja. O site continha fóruns ocultos, uma seção de "coisas divertidas" como senhas de roteadores WiFi utilizadas por organizações da Cientologia e dicas para pegadinhas. Uma era enviar uma carta de aparência oficial de aviso para cada um dos líderes do alto escalão da Cientologia para aterrorizá-los.

Bailey dedicou-se a manter o site mesmo durante sua missão na Coreia do Sul,

trabalhando nele por quatro a seis horas no período noturno e aos fins de semana. Era um cronograma puxado. Trabalhava no site até a uma ou duas da madrugada, acordava às cinco da manhã para fazer uma hora de corrida e exercícios físicos treinando com outros soldados antes do amanhecer. Bailey odiava correr e sofria de canelite, mas esperava ansioso o cair da noite para voltar ao seu laptop no dormitório. Abraçara de corpo e alma o objetivo de destruir a Cientologia e fez novas amizades nesse caminho. Uma delas foi Jennifer Emick.

O primeiro contato entre Bailey e Emick aconteceu num fórum on-line.

Bailey apreciava a petulância de Emick e a convidou para ser administradora em seu site. Ao longo do tempo, porém, ele percebeu que os dois tinham visões diametralmente opostas sobre o Anonymous. Emick não compreendia o lado mais sombrio da cultura chan e parecia pensar que o foco do Anonymous devia ser protestos pacíficos. Os dois argumentativos indivíduos começaram a protagonizar calorosas brigas públicas. A gota d'água foi o dia em que a dupla brigava no fórum anônimo do site, e Emick súbito disparou: – Sei que é você, Raziel.

Ao revelar o nickname habitual on-line de Bailey, Raziel, Emick havia traído um costume fundamental em fóruns como este: o de que esconder sua identidade on-line, ou nickname, poderia ser tão relevante quanto esconder sua identidade no mundo real. Enfurecido, Bailey removeu o acesso administrativo de Emick e os dois pararam de conversar.

Avaliando hoje o que aconteceu naquela época, Bailey disse que Emick havia percebido que o Anonymous não era um grupo de protesto pacífico, mas "cheio de hackers e pessoas na web que fazem coisas perversas para se divertir. Isso a desnorteou". E acrescentou: "Ela investiu muito orgulho pessoal nisso".

Anos mais tarde, Emick também encontrou dificuldades para explicar por que se afastou do Anonymous.

– O próprio grupo estava perdendo o foco... não quero entrar em detalhes – disse ela. – Em 2008 e 2009, havia uma filosofia no grupo. A gente não confrontava a comunidade, não xingava a polícia, dávamos um bom exemplo. Ao lutarmos contra um culto maligno, não podíamos ser malignos. Daí de repente alguém disse: "Bem, e por que não?".

Emick parecia se divertir com o drama e a fofoca, mas odiava as ameaças e os danos na vida real. Que fim levara a filosofia bem comportada dos primeiros protestos? O Anonymous se tornava cada vez mais vingativo, não apenas contra a Cientologia, mas contra outros Anons que discordavam de seus métodos. Essa torpeza não era novidade nenhuma para gente como Bailey, que encontrara o Anonymous por meio da terra de ninguém do 4chan, mas para Emick significava uma esmagadora traição.

– Tentamos avisá-la de que o Anonymous não é bonitinho nem amiguinho – disse Bailey. – Tentamos avisá-la de que eles não são boa gente. Estão fazendo malvadezas porque é engraçado.

Por fim, a própria Emick tornou-se um alvo. Quanto mais ela tentava explicar aos Anons que eles estavam sendo valentões irresponsáveis, mais eles a insultavam e a ameaçavam como represália. Descobriram seu nome e endereço verdadeiros e postaram essas informações on-line, junto com os dados do marido dela. Gente de várias facções do Anonymous começou a perseguir a enteada de Emick. Foi aventada a possibilidade de *SWATar* a casa dela – ligar ao FBI para enviar uma equipe da SWAT, pegadinha surpreendentemente fácil de executar. Logo Emick se mudou com a família para Michigan e começou a entrar na internet a partir de um servidor proxy para ofuscar seu verdadeiro endereço IP. Embora estivesse rompendo com o grupo, Emick voltaria mais de um ano depois, após aprimorar suas habilidades de engenharia social e "doxeagem", ajudando a praticamente despedaçar o Anonymous.

***

Nesse meio-tempo, o militar Bailey havia se encantado com uma facção do Anonymous à qual todos queriam se unir, mas poucos conseguiam entender: os hackers. Observara que um pequeno contingente de hackers peritos participara do Projeto Chanology logo no começo, mas depois se afastara. Enquanto o Anonymous decaía numa caótica guerra civil entre moralfags e trolls, Bailey partiu para descobrir os hackers. Queria ser capaz de fazer o que eles faziam: rastrear um inimigo, roubar o botnet de alguém ou hackear seus servidores. Ele não se perdoava por ainda não ter essas capacidades. Primeiro, porém, teria de fazer uma drástica mudança em sua vida pessoal, após deixar o exército em 2009.

Desde a infância, Bailey cultivara sentimentos arraigados e secretos de que no

fundo era mulher. Mesmo quando ele e sua esposa mantiveram um relacionamento aberto e começaram a trocar de parceiros, ele reprimira esses sentimentos íntimos. Logo após deixar o exército, porém, Bailey fez amizade on-line com uma linda e confiante mulher transexual e sentiu uma atração instantânea. Ele começou a acreditar que talvez fosse possível ter aquela aparência e sentir-se como ela. Em 26 de maio de 2009, comprou on-line um estojo de terapia de substituição hormonal e começou a se autoadministrar secretamente. Empolgado, decidiu ver como se sentia antes de informar a família sobre sua decisão. Os comprimidos acabaram funcionando com mais rapidez do que ele havia esperado; um mês depois ele havia desenvolvido pequenos seios.

Convidou a mãe e o irmão para visitá-lo, e, sentado na sala de estar com a mulher e os filhos, na época com três e dois anos, fez rodeios durante uma hora até enfim entrar no assunto e contar o motivo pelo qual estavam ali.

Ele queria realizar uma mudança de sexo e se tornar mulher. Todos ficaram emudecidos. Por fim, um deles indagou se Bailey tinha certeza de que era isso que desejava. Ele informou sem delongas que já havia começado a tomar suplementos de estrogênio. Ele sabia que os familiares tentariam dissuadi-lo, por isso resolveu mostrar firmeza.

Bailey lhes deu duas alternativas: aceitar que ele estava se tornando uma mulher ou saírem de sua vida. Não muito tempo após a reunião, ele e a esposa encaminharam o divórcio, concordando em compartilhar a custódia dos dois filhos. A mãe e o irmão aceitaram a situação. Bailey passou a se chamar Laurelai, o nome que a mãe ia lhe dar caso ele tivesse nascido menina.

Laurelai deparou com uma montanha educacional diante de si.

Aprender a ser do sexo feminino foi como enfrentar a puberdade novamente: Difícil, mas ela sentia que estava se tornando a pessoa que desejava. Logo o cabelo curto de soldado cresceu e ela andava pela casa de regata cor-de-rosa. Pela manhã, sentava-se defronte ao computador e tomava comprimidos hormonais regados a Coca-Cola. À medida que deixava para trás a antiga sexualidade, também quis modificar sua personalidade on-line, de simples administrador de site para hacker de qualidade. Começou a explorar as artes sombrias da web ao mesmo tempo em que mantinha seu site, o Scientology Exposed. O ano de 2009 se aproximava do final, e como o site era cada vez menos frequentado, Laurelai se deu conta de que o objetivo de “destruir a

Cientologia” talvez fosse grandioso demais.

Um dia, alguém começou a atacar o site dela. Laurelai conferiu os arquivos de registros e percebeu que ele estava sendo inundado com tanto tráfego de lixo eletrônico que chegou a sair do ar – um clássico ataque de DDoS. Saltou para outra rede de IRC e, enquanto discutia o problema com alguns moderadores do site, uma pessoa recém-chegada na sala de bate-papo assumiu a responsabilidade. Os moderadores suspeitavam tratar-se apenas de um troll, mas, quando Laurelai trocou mensagens particulares, a pessoa explicou que alguém estava usando um botnet para atingir o site.

Para a surpresa de Laurelai, o estranho a convidou a entrar no canal de comando do botnet e falar com o responsável pelos danos. Ela concordou e entrou em um novo canal de outra rede de IRC. Lá, no controle do botnet que derrubara o site de Laurelai, estava Kayla, de quem Laurelai jamais ouvira falar.

– Quem diabos é você? – disparou Kayla.

Um pouco surpresa, Laurelai explicou que era a proprietária do site ScientologyExposed, justamente o que Kayla estava atacando. Kayla demonstrou surpresa. Explicou que seu alvo não era o ScientologyExposed, mas o Enturbulation.org. Laurelai sabia que esse era o site de Gregg Housh.

Graças a algumas complicações técnicas decorrentes de uma ocasião anterior quando os dois tinham trabalhado juntos, ela e Housh compartilhavam o mesmo servidor. Ao atacar o Enturbulation, Kayla provocou efeitos colaterais no site de Laurelai. Então ela explicou que seu site servia de alternativa ao de Housh, concentrando-se mais em trollagem.

O humor de Kayla subitamente aliviou.

– Ai, me desculpe – disse ela. – Por que você usa o mesmo servidor desses moralfags, afinal?

Laurelai percebeu que Kayla odiava moralfags; por esse motivo primordial, ela estava atacando o Enturbulation. Kayla explicou que não tinha gostado do modo como os organizadores do Chanology haviam cessado a hackeagem de chapéu preto. Ela acreditava que atacar a Scientology de maneira rigorosa e rápida era mais eficaz do que por meio de um protesto demorado. Laurelai sentiu uma instantânea conjunção mental e ficou especialmente intrigada quando Kayla

mencionou a expressão hackers de chapéu preto. Adversários dos hackers de chapéu branco, os hackers chapéus pretos eram pessoas que utilizavam suas habilidades de programação para invadir redes de computadores por motivos próprios, às vezes mal-intencionados. As duas conversaram durante quase uma hora, quando Kayla disse que cessaria o ataque por algumas horas para que Laurelai transferisse o site a outro servidor diferente. Então Kayla retomaria seu ataque de DDoS.

Mais tarde, Laurelai indagou a alguns hackers de chapéu preto que conhecera recentemente se eles já haviam ouvido falar no nome Kayla.

Ficou sabendo que a nova conhecida tinha a reputação de alguém que era melhor não irritar.

– Muita gente tinha medo dela – Laurelai recordou tempos depois.

Algumas pessoas ficaram surpresas pelo fato de Kayla ter simplesmente conversado com Laurelai – que na época era apenas dona de um site.

Apesar disso, as duas mantiveram contato. Poucos dias depois, Kayla encontrou Laurelai em uma rede de IRC e a convidou para participar da rede de bate-papo pública que costumava frequentar. As duas começaram a se conhecer um pouco melhor. A certa altura, Laurelai perguntou a idade de Kayla. A resposta: catorze. Quando ela perguntou o sexo da outra na vida real, Kayla afirmou que era feminino, devolvendo as perguntas. Ao saber que Laurelai era transgênero, Kayla entrou em assuntos como suplementos hormonais. Para a surpresa de Laurelai, a garota parecia saber, melhor do que ela, os detalhes sobre doses de hormônio e seus efeitos colaterais.

Kayla inclusive utilizava como nickname as pequenas pílulas azuis vendidas como Estrofem: titty skittles.

Laurelai ficou se perguntando se não estava falando com um hacker transgênero.

Não existiam muitas pesquisas sobre hacker trans, mas havia bastante evidência casual sugerindo que o número de pessoas transgênero visitando o 4chan com certa frequência ou participando de comunidades hacker era desproporcionalmente elevado. Talvez existisse um motivo para isso: à medida que as pessoas passavam mais tempo nessas comunidades e experimentavam a “troca de gênero” on-line, elas conseguiam com mais facilidade pensar em trocar

de gênero no mundo real. As linhas divisórias entre suas personalidades off-line e on-line se tornavam turvas, e alguns participantes dessas comunidades eram conhecidos por falar sobre gênero como se fosse apenas outra coisa a ser "hackeada", de acordo com Christina Dunbar-Hester, professora da Rutgers University, especialista em diferenças de gênero no meio da hackeagem de hardware e software. Se as pessoas já personalizavam máquinas ou códigos, elas podiam enxergar os próprios corpos como o próximo e cativante desafio, em especial se já se sentiam desconfortáveis com o gênero com o qual tinham nascido. Mesmo assim, conforme Dunbar-Hester, muita gente imergia em outro gênero on-line, mas não replicava a atitude na vida real. Em outras palavras, Kayla podia ser apenas um homem que gostava de ser mulher on-line, nada além disso.

– Você é trans? – arriscou-se Laurelai.

– Não – disse Kayla. – Só conheço alguém que é trans. :) – respondeu sem pestanejar, aumentando as suspeitas de Laurelai.

– Bem, não importa se você é trans ou não é – respondeu Laurelai, acrescentando que, se Kayla quisesse ser chamada de "ela" on-line, então Laurelai a chamaria de "ela" em consideração ao desejo da amiga. As duas conversaram mais sobre hackeagem, trollagem e engenharia social, Laurelai como aluna e Kayla como professora. Nos anos seguintes, Kayla introduziria Laurelai em seu mundo secreto, enquanto o Anonymous seria relegado às sombras. Ela precisava mais que tudo do surgimento de uma nova causa, e no final de 2010 enfim isso aconteceu, colocando o Anonymous sob os holofotes internacionais.

CAPÍTULO 7

FOGO FOGO FOGO

Setembro de 2010. Por dois anos o fenômeno do Anonymous havia sumido das manchetes. Ataques se restringiam a ações pequenas e isoladas contra outros sites, a maioria executada por canais ou pelo próprio *b*. Pouquíssima coisa acontecia em redes de IRC, também. Os milhares de usuários que se encontravam no #xenu tinham se dispersado, espantados pela discórdia interna e interessados em novidades.

Em 8 de setembro, um artigo sobre uma empresa de software da Índia, chamada Aiplex, começou a ser repassado on-line. Girish Kumar, o diretor executivo da Aiplex, tinha se vangloriado para a imprensa que a empresa dele atuava como "matador de aluguel" para Bollywood, a florescente indústria cinematográfica da Índia. A Aiplex não apenas vendia software.

Trabalhava em nome dos estúdios de cinema para atacar sites que permitiam às pessoas baixarem cópias piratas de seus filmes.

Por exemplo, recentemente a Aiplex tinha lançado ataques de DDoS

contra diversos sites torrent, inclusive o mais famoso deles, The Pirate Bay.

Fundado em 2003, The Pirate Bay era o mais popular e procurado site BitTorrent da web, um baú de tesouros a partir do qual qualquer pessoa podia baixar ilegalmente filmes, canções, pornografia e programas de computador. A Aiplex tinha utilizado um botnet para inundar The Pirate Bay com tráfego, sobrecarregar seus servidores e temporariamente derrubá-lo. Kumar explicara que, quando os sites torrent não respondiam a um comunicado da Aiplex, a medida seguinte era "inundar o site com solicitações, o que resultava em erro na base de dados, causando negação de serviço".

Bloggers e jornalistas da área técnica já suspeitavam de que grupos antipirataria desferiam ataques de DDoS contra sites torrent como The Pirate Bay, mas a declaração de Kumar reconhecendo o fato era a primeira prova disso. E também um reconhecimento espantoso: ataques de DDoS

eram ilegais nos EUA e tinham resultado em um ano de cadeia para Brian Mettenbrink. Agora a empresa indiana se vangloriava abertamente de utilizar o

mesmo método.

Logo os usuários do *b* começaram a debater a notícia. Eis que muita gente desejava contra-atacar a Aiplex. Alguns começaram a colar um link “todo mundo vem para cá” que conduzia a um canal de IRC para um planejamento adequado. Dessa vez, não apareceram milhares de interessados, como havia acontecido com o #xenu. A luta por direitos autorais não era tão sexy quanto atacar um nebuloso grupo religioso que havia suprimido um vídeo de Tom Cruise. Mas a pirataria era tão popular entre os usuários do *b* que, sem demora, umas 150 pessoas tinham entrado no novo canal de IRC, criado pelo Anonymous para fazer a Aiplex provar um pouco de seu próprio veneno.

Coordenar um ataque não seria fácil. Nessa época, os anfitriões de redes de IRC já estavam mais conscientes sobre o Anonymous e logo fechavam uma sala de bate-papo se consideravam que ela estava sendo usada para combinar um ataque de DDoS. Para lidar com isso, os Anons iam pulando de uma rede de IRC para outra, colando links para as novas salas de bate-papo no 4chan e no Twitter a cada transferência, de modo que os demais pudessem segui-los. Ninguém era responsável por encontrar novos locais; sempre que o grupo precisava se mudar, alguém encontrava uma rede nova e criava um canal. Os canais sempre recebiam nomes inócuos para não atrair a atenção, mas o nome habitual do canal sobre os ataques contra a Aiplex era #savethepb, abreviando Pirate Bay.

Após algum planejamento, o grupo fez o primeiro ataque de DDoS

contra a Aiplex no dia 17 de setembro, às 21h, horário da costa leste.

Exatamente como desejado, o site da empresa saiu do ar – e permaneceu fora do ar por vinte e quatro horas. Sentindo-se confiantes, os Anons rapidamente ampliaram o ataque, postando folhetos digitais no *b* para que outras pessoas pudessem utilizar o LOIC contra outra organização que tentava combater a pirataria: a Associação da Indústria de Gravação dos EUA (*Recording Industry Association of America*, ou RIAA). O blog tecnológico TorrentFreak.com postou uma notícia intitulada “A próxima vítima do 4chan será a RIAA. Esse ataque de DDoS será o protesto do futuro?”. Em seguida, o grupo dirigiu seu fogo contra outra organização a favor dos direitos autorais, a Associação de Cinema dos EUA (*Motion Picture Association of America*, MPAA).

Dois dias depois, os Anons começaram a circular um comunicado à mídia

dizendo que o Anonymous estava se vingando do ataque contra The Pirate Bay, contra-atacando as associações de direitos autorais e o "matador de aluguel" contratado por elas, a Aiplex. Chamaram os ataques de "Operação: Vingança é um prato que se come frio", e alegavam ter derrubado o site da Aiplex graças a um "ÚNICO ANON" com um botnet.

"O Anonymous está cansado de interesses corporativos controlando a internet e calando os direitos das pessoas de divulgar informações", dizia a carta. E acrescentava: "Regozijem-se, irmãos do *b*".

Ao romantizar de modo despudorado a pirataria de filmes e músicas, os Anons também classificavam os ataques da Aiplex contra The Pirate Bay como "censura", aumentando o apelo do contra-ataque. Pela primeira vez em dois anos, parecia que o Anonymous poderia estar embarcando em outro importante projeto após o Chanology, e a centelha tinha sido aquela relevante provocação na cultura hacker: quem fere com DDoS, com DDoS

será ferido.

Por volta dessa época, Tflow, o discreto hacker que mais tarde reuniria Sabu, Topiary e Kayla, leu o artigo do TorrentFreak e embarcou em sua primeira operação no Anonymous. Mais tarde viria à tona que a pessoa por trás de Tflow morava em Londres e tinha apenas dezesseis anos de idade.

On-line, ele nunca comentava sua idade nem origens.

– Achei que era uma boa causa – lembrou-se mais tarde. – Claro, ataques de DDoS se tornaram chatos depois disso.

O que Tflow quis dizer era que ele estava mais interessado em descobrir modos para os Anons perturbar organizações antipirataria do que em derrubar os sites dessas organizações. Ele entrou no #savethepb para observar o que os outros sectários diziam e ficou agradavelmente surpreso. Algumas pessoas pareciam ter tanto conhecimento técnico quanto ele. Após Tflow abordar alguns em particular e se encontrar com eles num canal de IRC separado, a reduzida equipe começou a procurar vulnerabilidades nos grupos antipirataria e encontrou uma no site CopyrightAlliance.org.

Cerca de uma semana após o ataque de DDoS contra a Aiplex, os hackers do grupo de Tflow executaram o primeiro ataque com injeção de SQL de sua

campanha, talvez o primeiro realizado sob a bandeira do Anonymous. Eles hackearam o servidor da web do CopyrightAlliance.org e substituíram o site com a mesma mensagem utilizada em 19 de setembro, “Vingança é um prato que se come frio”. Fazer o deface de um site era mais difícil do que executar um ataque de DDoS – necessitava--se obter acesso ao diretório raiz de um servidor –, mas tinha um impacto maior. Eles transformaram o CopyrightAlliance.org em um repositório de filmes, jogos e canções pirateadas, inclusive, naturalmente, “Never Gonna Give You Up”, de Rick Astley, e o jogo Classic Sudoku. Também furtaram 500 megabytes de e-mails da ACS:Law, empresa jurídica londrina especializada em direitos autorais, e os publicaram no mesmo site desfigurado.

Tflow e os outros estavam todo o tempo recrutando defensores por onde passavam. Entre setembro e novembro de 2010, ele ajudou a convocar aproximadamente trezentos participantes de bate-papo habituais entre dez diferentes redes de IRC, para que se tornassem colaboradores contínuos.

– Na verdade, escolhíamos qualquer IRC ao qual tivéssemos acesso – contou mais tarde. – Não existiam muitas opções. Poucas redes de IRC

permitiam ataques de DDoS.

O grupo de organizadores então criou o que se tornaria um importantíssimo canal privado, o #command. Como o #marblecake, era um local para fazer planos sem desviar o foco. Eles começaram a elaborar folhetos digitais e a convidar novas pessoas para participar dessa nova e mais ampla batalha contra os direitos autorais, promovendo ataques de DDoS contra empresas jurídicas, organizações comerciais e até mesmo o site de Gene Simmons, o baixista do Kiss. Logo parecia que o Anonymous atacava alvos benignos – por exemplo, o escritório da U.S. Copyright –, e o apoio público obtido em blogs se extinguia. Em meados de novembro de 2010, os próprios Anons perdiam o interesse no assunto e só poucas dezenas continuavam a conversar na sala de bate-papo da Operação Vingança. A campanha tinha entrado num hiato.

Com mais tempo para se concentrar, alguns dos organizadores da Operação Vingança começaram a trabalhar numa até então inédita infraestrutura de comunicações para o Anonymous. Espalhadas pela Inglaterra, pela Europa continental e pelos Estados Unidos, essas pessoas, em sua maioria jovens do sexo masculino, repartiram o acesso a dez servidores mundo afora. Alguns tinham alugado os servidores, outros eram seus proprietários, mas, com esses

servidores à disposição, tornou--se possível estabelecer uma rede de bate-papos que o Anonymous, enfim, podia chamar de lar. Agora não seria mais necessário arrebanhar centenas de pessoas em diferentes locais antes de realizar os ataques. Naquele mês, foi criada a chamada AnonOps, uma nova rede de IRC, com dezenas de salas de bate-papo exclusivas para Anons, algumas públicas, outras privadas. Um dos primeiros a se registrar foi Topiary.

***

Nessa ocasião, Topiary tinha quase dezoito anos e, no mundo off-line, na pele de Jake, havia se mudado da casa materna, na pequenina ilha de Yell. Morava numa pequena residência financiada pelo governo em Lerwick, a capital de Shetland, e completava quatro anos longe das salas de aula. Lerwick era mais moderna que Yell – mas não muito. Também não contava com redes de fast-food nem grandes lojas de departamentos. Local gélido e fustigado pelo vento, com campos verdejantes, penhascos marrons escarpados e ruínas de pedra acinzentadas salpicando as intermináveis colinas. Jake praticamente não conhecia ninguém ali, mas, seja como for, preferia andar sozinho.

Sua casa fazia parte de um conjunto de casinhas de madeira ao estilo chalé, na encosta de uma colina, cerca de vinte minutos a pé do centro de Lerwick, numa área conhecida como Hoofields. Batidas policiais para apreender drogas eram comuns na rua dele, e alguns de seus vizinhos se tornaram ávidos consumidores de heroína. A casa de Jake era pequena, amarela e tinha apenas um piso, com uma ampla sala de estar conjugada com a cozinha de um lado e o quarto do outro. No pátio frontal às vezes floresciam margaridas primaveris, e nos fundos havia um galpão onde ele mantinha um velho refrigerador – ainda impregnado com o cheiro da ocasião em que ele acidentalmente o deixou cheio de salmão cru, sem energia elétrica, por três semanas. Ele comprara toda a mobília de pessoas locais, muitas vezes aproveitando bons negócios disponíveis na unida comunidade da ilha. Por exemplo, o valor original do fogão dele beirava as quinhentas libras (uns oitocentos dólares), mas ele o havia comprado de uma família amiga por vinte e cinco libras (aproximadamente quarenta dólares).

Jake arranjara um emprego em meio-turno numa loja de autopeças e estava se adaptando. Ainda ansiava ficar on-line, onde a maioria de seus amigos estava, e ainda se divertia fazendo trotes telefônicos.

Uma noite, ao visitar a mãe, Jake recebeu uma ligação de um homem que

alegava ser amigo de seu pai. Isso foi um choque. Jake não falava com o pai há muito tempo. Recebera telefonemas eventuais em seu aniversário, mas mesmo esses contatos haviam minguado após ele completar treze anos. Foi estranho ouvir falar do pai assim de supetão. O homem perguntou se podia anotar o número do celular de Jake e do irmão, acrescentando que o pai queria contatá-los. Ao que parece, ele se sentia culpado por alguma coisa. O irmão não quis conversa, mas Jake forneceu ao homem seu próprio número para ver o que ia acontecer.

Durante várias semanas, o rapaz manteve o celular sempre com carga e perto da cama quando dormia, mas o telefone não tocou. Súbito, em meados de outubro, uma semana após completar dezoito anos, Jake recebeu nova ligação do amigo do pai, mas com o peso de más notícias na voz. O homem se desculpou pelo que estava prestes a informar e explicou: o pai de Jake havia falecido. Contou que nas semanas anteriores ele passara horas tomando coragem para pegar o telefone.

– Mas ele não tinha coragem – disse o homem, acrescentando que, “em vez disso”, tinha se suicidado.

Jake não sabia ao certo o que pensar. Primeiro ficou entorpecido. O pai não tinha sido membro da família, por isso, de certa forma, Jake não precisava se importar nem se aborrecer. Ao perguntar o que havia acontecido, o amigo explicou que ele tinha se asfixiado com gás, invadindo com o carro a garagem de uma igreja na madrugada, fechando a porta de duas folhas e deixando o motor ligado.

Imagem surreal. Nos primeiros dois dias após a ligação, Jake ficou zangado. Parecia quase egoísta o fato de seu pai ter pedido o número dele e insinuado que ligaria, quase como se quisesse que Jake prestasse atenção no que realmente estava prestes a acontecer. Com mais análise, porém, deu-se conta de que provavelmente estava enganado, e que o pai talvez não quisesse magoá-lo.

Jake continuou a praticar games on-line e a visitar o 4chan, e um mês depois descobriu a nova rede de bate-papos que havia sido estabelecida pelo Anonymous: o IRC AnonOps. Intrigado, inscreveu-se, escolhendo o nome Topiary, e tentou obter uma melhor compreensão de como poderia participar. Não se enxergava como um ativista, mas a Operação Vingança parecia bem-organizada e potencialmente influente. Não tinha ideia de que, embora a batalha antidireitos autorais estivesse morrendo, a Operação Vingança estava prestes a

explodir com o apoio de uma pequena organização chamada WikiLeaks.

***

Jake, agora como Topiary, explorava as salas de bate-papo da rede AnonOps, enquanto Julian Assange, ex-hacker australiano amplamente reverenciado pela comunidade hacker, se preparava para soltar uma bomba no governo dos EUA. No começo de 2010, um soldado do exército estadunidense chamado Bradley Manning tinha supostamente repassado a Assange e entregue a seu site delator, o WikiLeaks, 250 mil mensagens internas via cabo, também conhecidas como cabogramas, enviadas entre embaixadas dos EUA. Esses cabogramas diplomáticos revelavam manobras políticas dos EUA e relatórios diplomáticos confidenciais. Ao expor esses documentos, Assange causaria um imenso constrangimento aos formuladores de políticas externas do governo dos EUA.

O fundador do WikiLeaks fechara negócio com cinco importantes jornais, inclusive o *The New York Times* e o britânico *The Guardian*, e, em 28

de novembro de 2010, eles começaram a publicar as mensagens. Quase de imediato, Assange tornou--se simultaneamente um pária e um herói de âmbito mundial. Até então, o WikiLeaks era moderadamente conhecido por coletar dados vazados que indicavam coisas como corrupção governamental no Quênia ou as mortes inoportunas de jornalistas iraquianos. Mas expor dados privados do governo dos EUA acendeu um nível de controvérsia completamente novo. Os analistas do noticiário norte-americano começaram a apregoar que Assange fosse extraditado, condenado por traição e até mesmo assassinado. Sarah Palin, a ex-governadora do Alaska, afirmou que os Estados Unidos deviam perseguir Assange com a mesma urgência que perseguiram o Talibã, enquanto o analista Bob Beckel, da Fox News, ao vivo em rede nacional, sugeriu que alguém, “de modo clandestino, desse um tiro no filho da puta”. A ministra das Relações Exteriores Hillary Clinton afirmou que os vazamentos “ameaçavam a segurança nacional”, e a equipe do Ministério das Relações Exteriores foi impedida de visitar o site do WikiLeaks.

Rapidamente o WikiLeaks passou a ser atacado. Um hacker ex-militar apelidado de The Jester realizou um ataque de DDoS contra o site, derrubando-o por mais de vinte e quatro horas. Jester fazia o tipo de hacker patriótico conhecido por atacar sites islâmicos jihadistas; mais tarde se tornaria um inimigo declarado do Anonymous. Agora defendia no Twitter que estava atacando o WikiLeaks “por

tentar colocar em risco as vidas de nossas tropas".

Para tentar permanecer na web, o WikiLeaks mudou seu site para servidores da Amazon. Novamente foi derrubado, com a Amazon alegando violação de seus termos de serviço sobre direitos autorais. As recusas continuaram a surgir: uma empresa de hospedagem chamada EveryDNS

negou a prestação de serviços para o WikiLeaks. Em 3 de dezembro, a gigantesca empresa de pagamentos on-line PayPal anunciou o corte de doações para o site, afirmando no blog oficial que havia "restringido permanentemente a conta utilizada pelo WikiLeaks em decorrência de uma violação da Político de Uso Aceitável do PayPal". Logo a Mastercard e a Visa cortaram os serviços de financiamento.

É duvidoso que qualquer pessoa dessas empresas cogitasse que uma facção de usuários da internet – conhecida por aplicar trotes em gerentes de restaurantes, assediar pedófilos e protestar contra a Igreja da Cientologia – subitamente se uniria para atacar seus servidores.

As pessoas que criaram o AnonOps trocavam ideias sobre a controvérsia do WikiLeaks em seu canal privado #command. Estavam indignadas com o PayPal, mas, mais do que isso, vislumbraram uma oportunidade. Com Anons já desinteressados em direitos autorais, essa podia ser a causa para fazê-los retornar em peso. As empresas de direitos autorais tinham agido mal, mas a humilhação submetida ao WikiLeaks pelo PayPal era pior ainda. Isso se tornara uma violação profana da livre informação num mundo em que, de acordo com o slogan dos ativistas da tecnologia, "as informações querem ser livres" (mesmo se *fossem* mensagens diplomáticas secretas via cabo). A vitimização do WikiLeaks, concluíram eles, despertaria a simpatia dos Anonymous e atrairia hordas de usuários à sua nova rede. Uma excelente publicidade.

Quem era esse pessoal no #command? Conhecidos como "operadores"

da nova rede de bate-papo, não eram hackers *per se*, mas indivíduos entendidos em computação que mantinham a rede e exerceriam um papel crucial na organização de grupos eventuais de pessoas, grandes e pequenos, ao longo das semanas seguintes. Muitos sentiam imenso prazer em hospedar centenas de pessoas em seus servidores. Em geral se comentava que esses operadores, que tinham nomes como Nerdo, Owen, Token, Fennic, evilworks e Jeroenz0r, eram

os verdadeiros e secretos líderes do Anonymous, devido ao poder que detinham sobre a comunicação. Eles evitavam a culpabilidade pelos atos do Anonymous, da mesma forma que Christopher “moot” Poole evitava o litígio alegando não ser responsável pelo que acontecia no 4chan.

Agora, porém, os operadores faziam bem mais do que apenas manter a rede de bate-papo. Estavam organizando um ataque contra o blog do PayPal, onde a empresa fizera seu comunicado sobre o WikiLeaks. Na manhã de sábado, 4 de dezembro, um dia depois de o PayPal anunciar o corte de transferências, os organizadores do AnonOps derrubaram o thepaypalblog.com por meio de um ataque de DDoS. O blog saiu do ar às oito da manhã, horário da costa leste.

Pouco depois, a conta do Twitter @AnonyWatcher postou: “Alvo derrubado – the paypalblog.com”. E acrescentou: “Fechem suas contas no #PayPal à luz do descarado abuso de poder para parcialmente incapacitar o financiamento do #WikiLeaks. Participem do #DDoS se quiserem”.

O blog do PayPal permaneceu off-line pelas próximas oito horas.

Qualquer visitante enxergava uma tela branca e a mensagem “error403, Acesso proibido!” em letras grandes.

No dia seguinte, domingo, alguém postou um anúncio no Anonops.net, o site oficial do IRC AnonOps, informando que o Anonymous planejava atacar “vários alvos patrocinadores da censura”, e que a Operação Vingança tinha “agido em apoio ao WikiLeaks”.

Por volta da mesma hora, um folheto digital circulava nos painéis de imagem e redes de IRC, com o título Operação Vingue Assange e uma extensa nota que declarava: “O PayPal é o inimigo. Ataques de DDoS serão planejados”. Assinado: “Somos Anonymous, Não perdoamos, Não esquecemos, Esperem por nós”.

Esses folhetos vinham de novos canais no AnonOps chamados #opdesign e #philosoraptors, que mais tarde se combinaram para fazer o #propaganda. Ali, quem desejasse colaborar com publicidade escrevia comunicados de imprensa e projetava folhetos digitais para anunciar ataques futuros. Outros então postavam os folhetos em todo o 4chan e no Twitter. Outro canal, o #reporter, era onde os Anons se dispunham a responder às perguntas de quaisquer jornalistas confusos que tinham descoberto como acessar o IRC. Topiary pulava de um canal de

publicidade para outro, mais interessado em espalhar a notícia do que em disparar armas.

Por volta das 17h, horário da costa leste, na segunda-feira, 6 de dezembro, os organizadores do AnonOps começaram um ataque de DDoS

contra o PostFinance.ch, site suíço de pagamentos eletrônicos que também tinha bloqueado transferências financeiras ao WikiLeaks. O site permaneceu fora do ar por mais de um dia.

O ataque teve o efeito de “prejudicar os clientes que faziam negócios com a empresa”, frisou Sean-Paul Correll, pesquisador da Panda Security, num post de blog naquele dia. Correll, que estava na costa oeste dos Estados Unidos, ficou acordado na madrugada para monitorar os ataques, que pareciam intermináveis.

Naquele dia, novecentas pessoas subitamente entraram no #operationpayback, a principal sala de bate-papo pública no IRC AnonOps, que estivera sem movimento durante meses. Umas quinhentas delas ofereceram seus computadores para se conectarem à “colmeia” LOIC. A essa altura, o LOIC tinha função automática; você só precisava selecionar o modo colmeia e alguém no #command estabelecia o alvo e o horário. Eles apenas digitavam instruções simples em seu canal IRC configurado – “lazor começa” e “lazor termina”. Usuários normais não tinham de saber quem era o alvo ou quando você supostamente devia disparar. Era só deixar o programa rodar em segundo plano.

Na terça-feira, às 14h, horário da costa leste, o AnonOps começou a atacar o site dos advogados suecos que processavam Assange, o qual agora procurava extraditá-lo para a Suécia, onde ele enfrentava uma investigação envolvendo má conduta sexual contra duas mulheres no país escandinavo.

Muitos no Anonymous consideraram o caso uma represália. Novamente, cerca de quinhentas pessoas estavam utilizando o LOIC, e agora mais de mil estavam no principal canal de bate-papo. Às 18h52, o AnonOps anunciou um novo alvo: EveryDNS.com, o provedor de servidor que tinha puxado o tapete da WikiLeaks.org. Um minuto depois, o site havia sido derrubado. Às 20h, o alvo se transferiu para o site principal do senador Joseph Lieberman, o diretor do Comitê de Assuntos Governamentais e Segurança Doméstica do Senado dos EUA, órgão que pressionou a Amazon a interromper a hospedagem ao WikiLeaks. Um por um, como num efeito dominó, todos esses sites saíram do ar

durante minutos, às vezes durante horas.

Ainda na manhã de 8 de dezembro na costa oeste, Correll havia registrado noventa e quatro horas de tempo fora do ar, na soma combinada desses sites, desde 4 de dezembro. Os problemas mais graves aconteceram no site do PostFinance e no blog do PayPal. Mas isso era apenas o começo.

Corria a notícia de que, se você quisesse ajudar o WikiLeaks, toda a ação acontecia no IRC AnonOps. Recém-chegados obtinham uma rápida atualização do que estava acontecendo ao visitar diferentes canais de bate-papo: no #target o assunto eram ataques futuros ou atuais e o #lounge funcionava só para jogar conversa fora. No #setup, novos recrutas achavam um link para baixar o LOIC e obtinham ajuda de usuários experientes.

A sala continha um link para um folheto digital com instruções passo a passo intituladas “COMO SE UNIR À MALDITA COLMEIA – FAÇA ATAQUES

DE DDoS COMO PROFISSIONAL”.

1. Baixe o mais recente LOIC a partir de github.com/NewEraCracker 2. MELHORE SUA MALDITA CONEXÃO. ISSO É MUITO, MUITO

IMPORTANTE

(Se sua banda larga sempre fica caindo, o LOIC não vai funcionar de modo adequado.)

As coisas andavam rapidamente. Topiary agora obtivera um status de “operador” mais elevado nos canais de publicidade, e, com isso, aumentara sua capacidade de atiçar os participantes e de se fazer ouvir com mais poder na sala. Seu entusiasmo, suas ideias e suas observações argutas chamaram a atenção de um dos operadores do AnonOps no #command, e eles enviaram a Topiary uma mensagem privada convidando-o para aderir a um canal de comando secreto, do qual ele nunca tinha ouvido falar.

Intrigado, ele entrou.

Ali, os operadores conversavam empolgadamente sobre todos os novos voluntários e a atenção da mídia que repentinamente estavam granjeando.

Decidiram escolher um alvo maior: o site principal do PayPal. Rapidamente escolheram datas e horários e colaram as coordenadas no alto dos principais canais de IRC, e depois as tweetaram. Topiary e os outros no #command esperavam que a convocação às armas obtivesse um feedback mais forte do que o costume, mas nada os preparou para o que estava prestes a acontecer.

Em 8 de dezembro, apenas quatro dias após o AnonOps ter lançado o primeiro ataque contra o blog do PayPal, o número de visitantes do IRC

AnonOps tinha subido de trezentos para sete mil e oitocentos. Era tanta gente aderindo simultaneamente que o cliente IRC de Topiary congelava a toda hora e tinha de ser reiniciado. As linhas de diálogo entre as pessoas no canal principal, ainda chamado #operation payback, avançavam na tela com tanta rapidez que era quase impossível estabelecer uma conversa.

– Foi enlouquecedor – mais tarde recordou Topiary. – Insano.

– Acha que este é começo de algo grande? – alguém chamado MookyMoo indagou em meio à agitação no canal principal.

– Sim – respondeu um operador chamado shitstorm.

Circulavam piadas sobre como a grande imprensa tinha começado a relatar o ataque.

– Estão nos chamando de hackers – disse alguém chamado AmeMira.

– Enquanto a gente na verdade não hackeia nada – respondeu outro chamado Lenin.

A própria rede de IRC estava travando devido à inundação de usuários.

– Estamos sendo atacados ou apenas tem muita gente neste servidor? – indagou um participante.

Tão logo a rede de LOIC começou a cair, instruíram os recém-chegados a configurarem seus “canhões” para o modo manual, digitando diretamente o endereço alvo e clicando “TÔ CARREGANO MEU LEIZER”.

Por volta da mesma hora, Topiary observou a entrada de duas pessoas muito

importantes na sala privada do #command. Dois botmasters. Cada qual controlava seu próprio botnet, Civil com 50 mil bots infectados e Switch com mais ou menos 75 mil. Anons que tinham botnets poderiam esperar um tratamento com reverência incomum no Anonymous – com apenas alguns cliques, eles tinham o poder de derrubar um site, uma rede de IRC, seja lá o que desejassem. Switch possuía o ego maior e, às vezes, tornava-se intragável para conversar.

– Tenho os bots, por isso dou as cartas – costumava dizer ele.

Tudo era controlado a partir do IRC. Civil e Switch inclusive controlavam seus botnets a partir de salas de bate-papo privadas, com nomes como #headquarters e #thedock. Esse último era bem adequado, já que chamavam os bots muitas vezes de “boats”, como na frase “Quantos barcos vamos lançar ao mar?” – e “dock” em inglês significa estaleiro. No canal público, os milhares de novos visitantes só precisavam digitar “!botnum” e apertar enter para ver quantas pessoas estavam utilizando o LOIC. No dia anterior, 7 de dezembro, o número de pessoas que optou pelo LOIC colmeia tinha sido de quatrocentos e vinte. Para o ataque contra o PayPal em 8 de dezembro, chegava a quatro mil e quinhentos.

Topiary percebeu que Civil e Switch tinham seus botnets preparados para ajudar o ataque, mas esperavam as hordas dispararem primeiro com o LOIC. O horário de lançamento seria às 14h GMT, quando a maioria das pessoas na Europa estava em suas mesas e na América o pessoal acabava de chegar ao escritório. Com poucos minutos para o horário marcado, os participantes e operadores do IRC postaram uma série de tweets, links a pôsteres digitais e posts no 4chan lembrando todo mundo: “FOGO ÀS 14H

GMT”. Quando enfim chegou o horário combinado, os canais de IRC, o Twitter e o 4chan explodiram com *FOGO FOGO FOGO FOGO* e FOOOOGO!!

Junto com todo o tráfego de lixo eletrônico, a colmeia LOIC configurou uma mensagem

aos

servidores

do

PayPal:

“Boa_noite_PayPal_Bons_sonhos_do_AnonOps”.

Houve uma onda de empolgação à medida que milhares de cópias do LOIC em todo o mundo começaram a disparar dezenas de toneladas de pacotes de lixo eletrônico contra o PayPal.com, colocando os servidores da empresa sob repentina pressão que parecia vir do nada.

– Se você estiver disparando manualmente, continue disparando em “api.paypal.com:443” – continuava avisando repetidamente um usuário chamado Pedophelia no canal principal. – Não troque de alvo; todos juntos somos fortes!

Um operador de IRC chamado BillOReilly, em uma sala de bate-papo chamada #loic, conseguia direcionar a colmeia de usuários do LOIC do mundo inteiro para atacar seja qual fosse o próximo site da lista de alvos.

Todo mundo que desse uma olhada no canal deparava com uma comprida lista de cada pessoa que utilizava o LOIC no ataque. Cada participante era identificado por seis letras aleatórias e o país de origem de seu computador (embora muitos tivessem mascarado essa informação com servidores proxy, em essência um computador intermediário, para evitar a detecção de origem). Os países com maior número de computadores participantes eram a Alemanha, os Estados Unidos e a Grã-Bretanha.

Poucos minutos após o início do ataque, os operadores de IRC

conferiram o PayPal.com e descobriram que o site funcionava devagar – mas tecnicamente ainda funcionava. Isso provocou certa confusão na horda. Havia algo errado com o LOIC ou com o AnonOps, ou o PayPal tinha uma forte proteção contra DDoS?

– O ataque NÃO está funcionando – alguém chamado ASPj escreveu para Kayla (nome que Topiary ainda não reconhecia) na sala do canal principal. – Repito, o PAYPAL NÃO ESTÁ FORA DO AR.

Ninguém fora do #command sabia disso, mas eles precisavam de Civil e Switch.

– Vamos acrescentar alguns milhares de bots – sugeriu alguém no #command. Civil sabia o que ele tinha de fazer. Digitou comandos para todos seus bots se

unirem ao botnet dele. O operador evilworks enviou uma mensagem a Topiary.

– Confira esses bots – solicitou ele, convidando-o a entrar na sala de controle do botnet de Civil, ansioso para se exibir.

Na sala de controle do botnet, parecida com qualquer outro canal de bate-papo, Topiary deparou com uma lista dos bots de Civil subitamente descendo a tela em ordem alfabética, à medida que começaram a se interligar mundo afora. Havia poucas centenas nos EUA, algumas outras centenas na Alemanha; todos estavam invisivelmente conectados a esse canal de IRC. Cada bot tinha nicknames como:
[USA|XP] 2025

[ITA|WN7] 1438

Muito semelhante à lista que BillOReilly via na sala, à exceção de que esses computadores eram infectados com um vírus que os havia conectado ao botnet de Civil. Não eram participantes voluntários. Nenhum dos computadores nesta sala pertencia às pessoas que desejavam fazer parte do ataque. Conforme a expressão corrente, chamavam-se computadores zumbis.

Se um deles de repente sumisse da lista, provavelmente isso significava que uma pessoa aleatória no Nebraska ou em Berlim tinha desligado o seu computador naquele dia, deixando o botnet com um computador a menos.

Por isso, Civil não gostava de utilizar todos os 50 mil bots de uma vez só; em vez disso, ele ia trocando poucos milhares a cada quinze minutos para deixar os outros “descansarem”. Tão logo o botnet disparasse, as pessoas por trás de cada computador infectado notariam que sua conexão com a internet se tornava vagarosa. Pensando que era um problema de roteador, em geral começavam a mexer na conexão ou simplesmente desligavam o computador. Reinicializar com frequência os bots garantia que seus proprietários não os desligassem ou, pior ainda, chamassem o pessoal da TI. (A propósito: alguns acreditavam que os melhores usuários a serem infectados com vírus para possíveis participações em botnets eram os frequentadores do *b* – eles deixavam os computadores ligados noite e dia.)

Civil deu a ordem para disparar. A ordem tinha mais ou menos esta aparência:

!fire 30000 SYN 50 296.2.2.8

Um SYN era um tipo de pacote, e isso significava inundar o PayPal.com.

com trinta mil bots cada um com cinquenta pacotes por trinta segundos. O

tipo de pacote era importante, pois simplesmente inundar um servidor com tráfego nem sempre bastava para derrubá-lo. Por exemplo, no caso de um servidor de um call center operado por centenas de pessoas, enviar pacotes "ping" era como ligar todas elas e simplesmente dizer "Alô" antes de desligar. Mas enviar pacotes "SYN" era como ligar aos operadores e ficar na linha sem falar nada, deixando a pessoa na outra extremidade repetindo "Alô?". O processo enviava milhares de pedidos, que o servidor não podia ignorar, então os deixava em espera.

Poucos segundos depois, o site do PayPal tinha saído completamente do ar. Ficaria inativo durante uma hora inteira. Os milhares de Anons na #OpPayBack comemoraram por ter derrubado o maior site de pagamentos eletrônicos do mundo. Importantes sites de notícias, desde a BBC até o *The New York Times* e o *The Guardian*, informaram que o "grupo de hackeagem global" Anonymous tinha derrubado o site do PayPal.

Correll, da Panda Security, entrou no IRC usando o nickname muihtil (lithium escrito de trás para frente) e enviou uma mensagem para o próprio Switch, perguntando qual o tamanho de seu botnet e explicando que era um pesquisador sobre segurança. Positivamente surpreso, Switch respondeu que o amigo dele (presumivelmente Civil) tinha ajudado no ataque oferecendo trinta mil bots, enquanto havia quinhentos na colmeia LOIC, e que o próprio Switch tinha atacado com mil e trezentos bots.

Isso confirmava que cerca de 90% de toda a potência de fogo no ataque contra o PayPal.com viera não de voluntários do Anonymous, mas de computadores zumbis.

Topiary silenciosamente começou a pensar sobre o real poder da colmeia. Quando entrara no canal #command, dois dias antes, ele pensava que os ataques de DDoS do Anonymous eram desferidos principalmente pelos milhares de pessoas com LOIC, com apoio de retaguarda de misteriosos botnets. Agora tinha se dado conta que acontecia o contrário.

Quando o assunto era atacar sites maiores como o do PayPal.com, o dano real provinha de um ou dois grandes botnets. Milhares de usuários de LOIC

podiam ter derrubado um site menor como o Scientology.org, mas não o maior fornecedor de pagamentos on-line do planeta. Na prática, encontrar alguém disposto a compartilhar seu botnet se revelava mais útil do que conseguir milhares de pessoas para disparar o LOIC ao mesmo tempo.

As observações de Correll foram relatadas pelo Computerworld.com, mas vastamente ignoradas pela grande mídia. Alguém apelidado de skiz colou um link com a reportagem na principal sala de bate-papo do AnonOps, comentando ceticamente: – Eles afirmam que o Anonymous utilizou um botnet de 30 mil pessoas.

:D.

A maioria desses ávidos voluntários não queria acreditar que os botnets tinham maior potência de fogo que todos os esforços coletivos.

Os operadores no #command também não gostavam de dar publicidade ao fato. Essa informação poderia não só desmotivar a participação de outros, mas atrair atenção indesejada ao canal, tanto de hackers quanto da polícia. Mas Civil e Switch continuaram a se vangloriar do quão grandes e potentes eram seus botnets. Instigados por reportagens da mídia e por seu público no #command, estavam ansiosos para se exibir novamente. Os operadores concordaram: já que tinham o poder de lançar novo ataque, deveriam fazê-lo. Planejaram um segundo ataque contra o PayPal para 9 de dezembro. Novamente escolheram o período da manhã – horário da costa leste – para atrair a atenção dos usuários de internet e da mídia dos EUA.

Dessa vez, porém, houve menos entusiasmo e coordenação. Só um dia se passara desde que 7800 pessoas tinham se registrado na principal sala de bate-papo do AnonOps, mas o número de participantes utilizando o LOIC começava a minguar. Então, quando chegou a hora de disparar contra o PayPal pela segunda vez, os voluntários na sala de bate-papo #operationpayback foram solicitados a aguardar. Ninguém explicou por quê. Topiary também estava no #command esperando a hora do ataque para que ele pudesse redigir o primeiro comunicado de imprensa. O

problema é que, em alguma parte desconhecida do mundo, Civil ainda dormia.

– Temos algum tópico sobre o qual escrever? – quis saber Topiary. – Porque não aconteceu nada.

– É. Temos de esperar que o Civil entre on-line – foi a resposta.

Uma hora depois, Civil enfim fez logon no #command e acrescentou uns resmungos. Enquanto os operadores mandaram a colmeia disparar seus (altamente ineficazes) canhões, Civil ligou seu botnet e derrubou o PayPal.com. Então desconectou e foi tomar o café da manhã.

Topiary assistiu a tudo isso e confirmou o poder secreto dos botnets.

Eles tinham amplificado o primeiro ataque contra o PayPal, já que a colmeia era tão grande, mas na segunda vez um botnet sozinho fizera todo o trabalho. O segundo ataque não teria acontecido se Civil não fosse tão exibido. No entanto, os operadores ainda queriam que o Anonymous e a mídia pensassem que milhares de pessoas

tinham

sido

responsáveis.

Ignorando

essas

verdades

desconfortáveis, Topiary escreveu um comunicado de imprensa sobre o novo ataque da “colmeia”.

Após o segundo ataque contra o PayPal, houve mais fanfarronice por parte de Civil e Switch, e os operadores do AnonOps lhes disseram que eles podiam atacar o MasterCard.com em 12 de dezembro. Eles anunciaram a data e o horário do ataque pela internet, sabendo que, com os botnets fazendo a maior parte do trabalho, seria engraçado, mas não crucial, obter outra horda de pessoas disparando. Dessa vez, apenas cerca de novecentas pessoas tinham conectado seus LOIC à rede de bate-papo do AnonOps e disparado contra o MasterCard.com. Não importava. Graças a Civil e a Switch, o site de uma das maiores empresas financeiras do mundo saiu do ar por doze horas, cumprindo à risca o cronograma.

***

Ao longo do tempo, um punhado de outras pessoas com botnets ajudaria o AnonOps. Um deles era um jovem hacker chamado Ryan. Aos dezenove anos e morando com os pais em Essex, Inglaterra, seu nome completo era Ryan Cleary. No mundo off-line, Ryan, que mais tarde seria diagnosticado como portador da síndrome de Asperger, raramente saía do quarto, nem para jantar: a mãe deixava um prato de comida na frente da porta. Mas sua dedicação para se tornar poderoso on-line tinha surtido efeito; ao longo dos anos, ele acumulara servidores e formara um monstruoso botnet com 1,3 milhão de computadores, conforme sua própria estimativa. Outras fontes on-line calculavam um número menor, mas ainda gigantesco: 100 mil computadores. Embora ele alugasse o botnet, também o sublocava para fazer dinheiro extra.

Como Civil e Switch, Ryan gostava de se vangloriar de seu botnet para operadores e hackers, e fazia segredo de seu verdadeiro poder para os novos voluntários. Por exemplo, mais tarde, em fevereiro, quando cerca de cinquenta pessoas no AnonOps anunciaram ataques contra pequenos sites do governo italiano, Ryan silenciosamente disponibilizou seu botnet para os ataques. Durante eles, sempre que alguém digitava "!botnum" para descobrir quantos estavam usando o LOIC, aparecia o número 550.

– Você simplesmente acrescentou quinhentos computadores a seu botnet? – indagava Topiary a Ryan em uma mensagem privada.

– Não – respondia Ryan. – Só mudei os comandos do LOIC para dar a impressão de que 512 pessoas o estavam utilizando.

Em outras palavras: Ryan não só fornecia a potência de fogo real, como também manipulava deliberadamente outros Anons para pensarem que eles causavam o dano. Não era difícil fazer isso. Se você estivesse controlando a rede de usuários do LOIC, podia fraudar o número de pessoas que usava a ferramenta digitando +500 ou até mesmo +1000 no canal de IRC correspondente. Essa capacidade de falsificar os números era um segredo de polichinelo no #command, mas as pessoas desdenhavam o tópico sempre que ele vinha à tona. Afinal de contas, Anonymous era "Legião".

– Não tinha nada de incompleto – afirmou uma fonte que conhecia o uso de botnets em apoio ao AnonOps em dezembro de 2010 e janeiro de 2011.

– Mais trapaça divertida, acho eu.

O alto escalão de operadores e botnet masters também não se enxergavam como manipuladores. Em parte, isso ocorria porque eles não faziam diferença entre a colmeia das pessoas reais utilizando o LOIC e a colmeia dos computadores infectados de um botnet. No fim das contas, tudo não passava de números para eles, acrescentou a fonte. Se não conseguissem

computadores

suficientes

no

cômputo

geral,

os

organizadores apenas acrescentavam mais, e não importava se fossem computadores zumbis ou voluntários verdadeiros.

Botnets, não voluntários em massa, foram os reais motivos que permitiram ao Anonymous derrubar com sucesso, em duas oportunidades, o site do PayPal, e depois o MasterCard.com durante doze horas em 8 de dezembro, e o Visa.com por mais de doze horas no mesmo dia. De acordo com uma fonte, no máximo dois botnets apoiavam os AnonOps antes de 30

de novembro, alcançando um pico de aproximadamente cinco botnets até fevereiro, antes de o número baixar de novo para um ou dois. Só um punhado de pessoas podia acionar os disparos com bots. Na maior parte do tempo, a potência de fogo era entregue sem interesse financeiro.

– As pessoas ofereciam as coisas porque acreditavam na mesma ideia – alegou a fonte.

Mais do que isso, eles gostavam de se pavonear do quanto eram poderosos.

Naturalmente, com o ego sendo um grande motivador dos ataques do começo de

dezembro, os debates no #command logo se arruinaram. Após Civil, Switch e as novecentas pessoas infrutiferamente utilizando LOIC

atacarem o MasterCard.com, o pequeno grupo no #command decidiu, num capricho orgulhoso, atacar o Amazon.com no dia seguinte, 9 de dezembro, às 10h da manhã, horário da costa leste. Foi quando os operadores se deram conta de que Civil e Switch tinham sumido.

Eles, então, transferiram o ataque para 9 de dezembro às 14h, desejando que os botmasters voltassem. Às 13h30, toda a rede de IRC

AnonOps parou de funcionar. Civil e Switch, após entrarem em atrito com alguns dos operadores no #command, agora utilizavam seus botnets para atacar o AnonOps e tirar a desforra. Quando a rede de IRC voltou a ficar on-line, cerca de uma hora depois, com uma centena de participantes, ninguém mais queria atacar a Amazon. Não havia bots suficientes e o objetivo parecia ter se dissipado.

Topiary estimou que os usuários de LOIC representavam em média de 5

a 10% dos danos feitos contra sites como o PayPal, MasterCard e Visa no começo de dezembro de 2010, e nos meses seguintes menos de 1%, à medida que diminuía o número de pessoas envolvidas. Outra fonte com acesso aos operadores na época estimou de modo mais complacente que a ferramenta LOIC contribuía com em torno de 20% da potência do DDoS

durante os ataques do AnonOps em dezembro e janeiro. A verdade tornou-se especialmente difícil de aceitar quando, sete meses mais tarde, o FBI prendeu catorze pessoas que tinham participado dos ataques contra o PayPal baixando e utilizando o LOIC. Entre esses usuários, estavam universitários e uma mulher de meia-idade.

– As pessoas que lutavam por seus ideais não deviam saber que faziam aquilo em vão – acrescentou a fonte próxima aos operadores.

De certo modo, o LOIC ajudava realmente. Fazia as pessoas sentirem que estavam contribuindo com algo, o que incentivava outras mais a participar. Além disso, Civil, Switch e outros botmasters talvez não tivessem ajudado se não tivessem visto a onda de apoio.

Independentemente disso, Topiary decidiu manter a versão oficial em 10 de dezembro, ao ser contatado por um repórter da Russia Today, rede de televisão com financiamento estatal, e convidado a dar sua primeira entrevista na tevê, um debate em áudio pelo Skype. Embora não escondesse o nervosismo nos instantes que antecederam a entrevista, durante a transmissão ele afirmou com convicção que a colmeia tinha derrubado o PayPal e os demais alvos.

– Mentimos um pouco para a imprensa – contou ele meses depois – para passar aquela sensação de abundância.

A imprensa gostava de dar informações sobre esse novo e poderoso fenômeno de uma colmeia que ninguém parecia capaz de quantificar.

– Eles gostavam da ideia e intensificaram a atenção.

“Mentir para a imprensa” era prática comum no Anonymous, por motivos compreensíveis. Afinal, a rede de pessoas surgira de uma cultura de pregar peça nos outros, um mundo paranoico cujos habitantes nunca faziam perguntas pessoais uns aos outros e mentiam de modo habitual sobre suas vidas reais como forma de autoproteção. Também pertencia à cultura do Anonymous fazer declarações aleatórias e ultrajantes. Por exemplo, alguém prestes a sair da frente do computador por alguns minutos para tomar café podia dizer: – Já volto; FBI na porta.

O Anonymous não só cultivava uma aura de objetivos nobres a partir da qual se tornava aceitável inflar personagens e mentir para a mídia; os Anons também faziam parte de uma instituição secreta sobre a qual ninguém do mundo real entendia.

Em especial, os Anons desdenhavam jornalistas que entravam no canal #reporter e indagavam: – E aí, quem será a próxima vítima?

Ou pressionavam para conseguir alguma frase de efeito para citar.

Alguns primeiro exageravam, dizendo que havia dezenas de milhares de pessoas atacando um site. Em uma ocasião, um Anon contou a um repórter de uma revista que o Anonymous tinha “colônias” mundo afora, um quartel-general concreto, e que o nome do grupo se baseava num homem verdadeiro chamado Anonymous.

– Então quem é o Anonymous? – indagou um repórter sobre o suposto homem.

– Ele é esse cara. Mora em nosso quartel-general, no oeste da Filadélfia.

Na verdade, isso não passava de um meme da internet: contar uma história elaborada, depois fazer uma pegadinha citando o rap introdutório do sitcom *The Fresh Prince of Bel Air.*

Mais tarde, em fevereiro de 2011, Topiary criaria um canal de IRC

chamado #over9000 – em referência a outro famoso meme, que envolvia poucos Anons do núcleo de comando discutindo uma falsa operação de hackeagem para confundir uma jornalista do *The Guardian.* A repórter tinha solicitado acesso aos canais internos “secretos”.

– Temos que brincar com ela para valer – Topiary tinha contado aos outros.

O grupo começou a enviar spam na sala com mensagens crípticas como: – Charlie está com c85 de excesso; façam o rootlog de cadeia em cascata e detonem com o modo aurora.

Mentir era tão comum no Anonymous que as pessoas raramente ficavam surpresas ao ouvir versões diferentes dos fatos, ou ao descobrirem que o nickname com quem conversavam estava sendo sequestrado por outra pessoa. Havia um constante clima de desconfiança e ceticismo sobre quase tudo. Até mesmo quando alguém declarava admiração genuína por alguém ou pelas operações efetuadas contra o PayPal e a MasterCard, suas opiniões podiam mudar poucos dias depois. Não quer dizer que as pessoas no Anonymous eram frívolas ou que havia pouco valor em suas experiências – apenas os eventos e relacionamentos na internet se moviam com rapidez e dramaticidade bem maiores do que na vida real. A inserção de dados pelos Anons podia ser esmagadora e, muitas vezes, o resultado era o desapego – de emoções, de princípios morais e da consciência sobre o que realmente acontecia. Mas uma verdade em especial pelo menos uma dúzia de Anons mais tarde se arrependeria de ter ignorado. Em relação ao LOIC. A sua arma tão importante não só era inútil contra alvos grandes como o PayPal, como também poderia atrair a polícia direto para as portas do grupo.

CAPÍTULO 8

Tiros que saíram pela culatra Quando por volta de 8 mil pessoas rapidamente se aglomeraram no principal canal do IRC AnonOps em 8 de dezembro, ansiosas por vingar o WikiLeaks, os cerca de doze operadores no #command ficaram atônitos e depois sobrecarregados. Centenas de pessoas imploravam instruções, e a óbvia era baixar e usar o LOIC. Os operadores se certificaram de que no alto dos principais canais de bate-papo houvesse um link para baixar o programa, junto com um documento explicando como usá-lo.

Mas ninguém sabia ao certo se o LOIC era seguro. Corria o boato de que o LOIC estava rastreando seus usuários, de que os agentes do FBI o monitoravam, ou de que ele transmitia um vírus. De modo mais desnorteante, o LOIC que grande número de Anons baixou durante a Operação Chanology, três anos antes, era muito diferente do baixado agora na Operação Vingança. No mundo altamente dinâmico do software de código aberto, os desenvolvedores adaptavam coisas o tempo todo, e ninguém se preocupava se isso estava ajudando ou estorvando o Anonymous. Uma pessoa que resolveu analisar o LOIC com mais cuidado chegou à conclusão de que a ferramenta estava atrapalhando.

Por volta da mesma época em que os ataques contra o PayPal estavam sendo efetuados, um habilidoso desenvolvedor de software entrou no IRC

AnonOps pela primeira vez. O programador, que não queria revelar seu nickname nem seu nome verdadeiro, havia trabalhado no WikiLeaks no passado e estava disposto a atacar os detratores da organização. Ao baixar o LOIC do link no alto dos principais canais de bate-papo, teve a ideia de conferir o código fonte do programa.

– Eu o decupei – contou ele –, e parecia muito frágil.

O maior problema era que o aplicativo enviava tráfego de lixo eletrônico diretamente dos endereços IP dos usuários. Não fazia nada para esconder o computador do usuário na rede. Ou seja, as pessoas que utilizavam o LOIC faziam isso com seus endereços IP expostos, como quem pede para ser preso.

O programador logo enviou mensagens privadas a alguns dos operadores e lhes contou suas preocupações, pedindo que o link do LOIC

fosse removido dos canais. Cerca de metade deles concordou – mas a outra metade se recusou. De acordo com o programador, os operadores que se recusaram não entendiam a tecnologia por trás do LOIC. Complicava ainda mais a situação a gama de operadores, todos oferecendo interpretações diferentes sobre o LOIC na rede de bate-papo. O AnonOps tinha níveis diferentes de operadores – operadores de rede no topo e operadores de canal abaixo deles. Os últimos atuavam como gerentes intermediários, com a capacidade de expulsar pessoas dos canais com alguns comandos simples.

Uma jovem estudante, que atendia pelo nickname de “No”, galgou posições até obter o cargo de operadora de canal na época dos ataques contra o PayPal, e ficou conhecida por banir pessoas do canal principal #operationpayback se elas tentavam convencer outros usuários a não usar o LOIC. (Ironicamente, meses mais tarde, a polícia acabou rastreando No e prendendo-a porque ela havia utilizado o LOIC.) Novos voluntários e operadores partiam do pressuposto de que havia segurança nos números. O Anonymous, como dizia o ditado, era todo mundo e ninguém.

– Posso ser preso por fazer isso? – uma pessoa chamada funoob indagou no canal #setup em 8 de dezembro.

– Não, eles não vão prendê-lo – respondeu alguém chamado Arayerv. – É muita gente. Você pode alegar que tem spyware. Eles não podem acusá-

lo.

Outro chamado whocares entrou na conversa: – Se você for preso, é só dizer que não sabe de nada, que provavelmente seja um vírus.

– De certa forma, eu torço para ser preso – brincou alguém com o nickname isuse. – O julgamento seria hilário. (Aqueles que mais tarde realmente foram julgados pelo uso do LOIC provavelmente não concordam com isso.)

– Eles acreditavam sinceramente que, devido à quantidade de gente, seria impossível processar um indivíduo isolado – recordou mais tarde o programador. – Ninguém falava sobre processos criminais. Eles não queriam ouvir falar sobre seu IP estar exposto ou coisa desse tipo.

E a esmagadora sensação de camaradagem e realização dominava os argumentos racionais. A mídia global prestava atenção ao Anonymous e à sua extraordinária

mente colmeia; a última coisa de que o grupo precisava era começar a remexer na tecnologia na qual confiavam e diminuir o ritmo.

Mesmo quando a polícia holandesa agilmente prendeu Jeroenz0r, 16, operadora de IRC do AnonOps, e Martijn “Awinee” Gonlag, 19, em 8 e 11 de dezembro de 2010, a reação inicial das pessoas do AnonOps foi de ceticismo.

– Besteira, ninguém está sendo preso – falou um usuário chamado Blue quando links com os relatos das prisões começaram a circular. Então, logo que mais artigos sobre as prisões apareceram on-line, uma inundação de defensores holandeses surgiu no AnonOps. Era tanta gente que um novo canal foi iniciado para hospedá-los, chamado #dutch.

Por volta de 13 de dezembro, um raro folheto digital foi publicado avisando a todos usuários recentes do LOIC que eles corriam “elevado risco” de serem presos e precisavam apagar todos os registros de bate-papos. O organizador shitstorm comentou: – Ridículo. Essa é uma manobra óbvia para tentar assustar e espantar as pessoas.

– É um troll – contou outro organizador a Correll, da Panda Security.

Os operadores, inclusive um que atendia pelo nome de Wolfy, continuaram a incentivar as pessoas a utilizarem o LOIC, até mesmo quando Correll relatou no blog da Panda Security, por volta de 9 de dezembro, que o LOIC não mascarava o endereço IP dos usuários.

– As pessoas estavam tão empolgadas – relembrou o programador. – Estavam contaminadas pelo espírito natalino e ensandecidas.

O programador não jogou a toalha. Decidiu ajudar a construir uma nova ferramenta para substituir o LOIC. Começou a requisitar entre os AnonOps voluntários interessados

que

conseguissem

provar

que

eram

desenvolvedores. Após reunir uma equipe de oito pessoas de todo o mundo, passaram a se encontrar num servidor de IRC separado e, nas três semanas seguintes, se concentraram na missão de reescrever o LOIC a partir do zero. Foi a mais rápida produção de programa da qual ele participou, impulsionada por um senso de justiça contra as corporações e os governos e a ideia de contribuir com a coletividade. O programador ficava em seu computador o dia inteiro, inclusive durante o trabalho em seu emprego diário, deixando de fazer refeições e tomando bebida alcoólica simultaneamente com os novos colegas em outras partes do mundo.

A equipe acrescentou novos recursos ao programa, que se parecia com o LOIC, mas permitia aos usuários disparar pacotes de lixo eletrônico a um alvo por meio da Tor, a popular rede de anonimato. A ferramenta era não só mais segura que o LOIC, como também mais poderosa e de maior alcance. O programador alega ter obtido 200 mil downloads no IRC

AnonOps quando finalmente compretaram o software em 23 de dezembro.

Logo que foi postado num blog popular administrado por um operador do IRC AnonOps chamado Joepie91, foi baixado mais 150 mil vezes. Ainda assim, muitos Anons novatos continuavam a baixar o LOIC, porque era muito conhecido. O link para baixá-lo continuava em todos os lugares no IRC AnonOps. E a nova ferramenta do programador era bem mais complicada para configurar. O LOIC talvez tenha alcançado um verniz de legitimidade a partir de menções frequentes na grande imprensa – desde o *The New York Times* até a BBC News.

Mais tarde, em março de 2011, o programador e sua equipe novamente decuparam o LOIC e descobriram que realmente tinha sido infectado com um programa pernicioso, o Trojan.

– Um código gravava o que você tinha enviado e quando tinha enviado e, em seguida, repassava a informação a um servidor – disse ele, acrescentando que era possível que os endereços IP dos usuários estivessem sendo enviados ao FBI.

Na realidade, o FBI já investigava o Anonymous desde os ataques contra empresas de direitos autorais em outubro e novembro de 2011, e também estivera trabalhando intimamente com o PayPal desde o começo de dezembro.

Dois dias após o ataque de DDoS de 4 de dezembro contra o blog do PayPal, os agentes do FBI conversaram por telefone com Dave Weisman, gerente de segurança cibernética do PayPal. À medida que os ataques se intensificaram, as duas partes mantiveram contato, enquanto um engenheiro de segurança da empresa mãe do PayPal, o eBay, decupou o LOIC e analisou seu código fonte.

Em 15 de dezembro, um membro da equipe de segurança cibernética do PayPal deu um pequeno pen-drive ao FBI. Era a mina de ouro. Havia nele mil endereços IP de pessoas que tinham utilizado o LOIC para atacar o PayPal, justamente aqueles que enviaram o maior número de pacotes de lixo eletrônico. Assim que os feriados natalinos acabaram, o FBI começaria a emitir intimações a provedores de banda larga, como a AT&T Internet Services, para desmascarar os assinantes por trás daqueles endereços IP.

Em seguida, o FBI iniciaria as detenções.

***

– Switch está praticamente em uma lista de pessoas vigiadas que, se aparecerem, devem levar chumbo – contou o operador Owen a outros operadores em 20 de dezembro.

O botmaster que ajudara a perpetrar os ataques contra o PayPal acontecidos no começo de dezembro encontrava-se “ausente sem licença”

após criar problemas na rede e ser banido de alguns dos principais canais de bate-papo, inclusive do #command. Ele se ressentira do fato de sua contribuição aos ataques não resultar em ganho de poder.

Comentava-se à boca pequena que Civil também demonstrava amargura parecida. Depois dos ataques contra a Visa e a MasterCard, ele contou aos operadores do AnonOps como Owen que estava sendo usado e que fingiam gostar dele por causa de seus bots. Embora esse não fosse o caso para todos os botnet masters que apoiavam o AnonOps, Civil e Switch não ligavam nem um pouco para o ativismo que o Anonymous liderava publicamente, de acordo com Topiary, e estavam mais interessados em alardear seu poder aos operadores do Anon e causar impressão com sua habilidade de derrubar um site importante num estalar de dedos.

Nesse meio-tempo, enquanto seus ex-aliados começavam a atacar a rede do

AnonOps a partir de 13 de dezembro, os operadores da rede ficaram sobrecarregados com trabalho extra de manutenção. Com gente como Civil, Switch, The Jester e sabe--se lá quem mais atacando a rede, não havia tempo para definir um estratégia central a partir do #command.

Como resultado, a massa de participantes originais começou a se dividir e a iniciar operações próprias. Em geral dentro da lei e coerentes. Um ex-operador chamado SnowyCloud deu início à Operação Leakspin, trabalho investigativo que incitava as pessoas a lerem os cabogramas publicados pelo WikiLeaks e depois postarem resumos em vídeos do YouTube que podiam ser pesquisados com tags enganosas como Tea Party e Bieber.

Também havia a Operação Leakflood, em que os Anons postaram um folheto digital com os números de fax das sedes de empresas como Amazon, MasterCard, PayPal e outras, com instruções para enviar via fax “cabogramas aleatórios do WikiLeaks, cartas do Anonymous...”. As pessoas criavam os folhetos no #propaganda, onde Topiary continuava a passar a maior parte de seu tempo. A partir do #propaganda, alguns lançaram a Operação Paperstorm, convocando os Anons a dominarem as ruas da “vida real” – não para protestar como antes, mas para colar logotipos impressos do Anonymous nas ruas, no sábado, 18 de dezembro. Outro canal chamado #BlackFax listava os números dos fax de vários quartéis-generais corporativos e incentivava os Anons a remeter fotos pretas via fax a esses estabelecimentos para drenar a tinta de suas impressoras.

Logo, o AnonOps se dividia em toda sorte de operações colaterais, muitas vezes envolvendo causas completamente diferentes do WikiLeaks, mas sempre como “Anonymous”. Em meados de dezembro, alguns Anons desferiram um ataque de DDoS contra o site oficial de Sarah Palin e o Conservatives4Palin, e um grupo de 25 atacou um site do governo venezuelano para protestar contra a censura na internet. Outro projeto chamado Operação OverLoad reuniu hackers irlandeses a fim de mapear a rede inteira do governo num esforço para desfigurar todo e qualquer site .gov e .edu que eles pudessem.

Cada vez que alguém apresentava um comunicado de imprensa anunciando um ataque do Anonymous, a mídia insinuava que vinha do mesmo “grupo de hackers” que atacara o PayPal e a MasterCard. Além de não pertencerem ao mesmo grupo, essas pessoas muitas vezes nem eram hackers, e não sabiam uma vírgula sobre injeção de SQL. Estavam munidas apenas com a habilidade de

coordenar outras pessoas e tinham acesso a ferramentas de software grátis, disponíveis no painel *rs* do 4chan.

Topiary andava envolvido com algumas das operações distintas que decolaram logo após os ataques contra o PayPal e a MasterCard. No final de dezembro, enquanto espreitava o canal #operationpayback, ele observou algumas pessoas conversando com um participante chamado ‘k.

– Então você é *a* Kayla? – indagou alguém.

Eles perguntaram sobre um incidente no 4chan – alguém tinha tomado o controle completo do painel *b* e enviado spam com ciclos repetidos de “Kayla <3” em 2008. ‘k disse sim e acrescentou um rosto sorridente. Outro nome, Sabu, espreitava entre os participantes, sem falar nada, só escutando.

Logo Sabu e Kayla se mudaram para outro canal secreto que lentamente substituía o #command como centro tático do Anonymous: o #InternetFeds. Esse canal era tão confidencial que nem pertencia à rede AnonOps, mas supostamente ao servidor de um hacktivista radical do Anonymous. Cerca de trinta pessoas conseguiram entrar nele, principalmente por meio de convites, incluindo Sabu, Kayla e Tflow, alguns dos operadores originais do AnonOps, e um ou dois botmasters. Em sua maioria, hackers de extrema perícia.

Ali eles podiam compartilhar vulnerabilidades encontradas em servidores que hospedavam uma série de instituições, desde o Partido Verde oficial dos EUA e a Universidade de Harvard até o laboratório da CERN (Organização Europeia para a Pesquisa Nuclear), na Suíça. Sabu inclusive colou uma lista de exploits – uma série de comandos que se aproveitava de uma brecha de segurança – em vários iPhones que qualquer pessoa podia espiar. Eles lançavam ideias sobre alvos futuros: Adrian Lamo, o hacker que dedurou Bradley Manning, o informante militar do WikiLeaks, ou Switch, o botmaster desertor.

– Se alguém tiver os dox dele – disse Kayla –, eu descubro seu número de segurança social e podemos infernizá-lo.

Para quem não a conhecia, Kayla dava a impressão de alguém especialmente interessada em justiça vigilante.

À medida que os participantes do InternetFeds começaram a se conhecer melhor, eles também observaram que Sabu era a pessoa com mais voz, as opiniões mais

consistentes e a maior vontade de coordenar os outros para agir. Sabu também mantinha boas ligações com o cenário hacker underground e desejava reviver os dias do assim chamado movimento Antissegurança. Por fim, deu-se conta de que poderia fazer isso com um grupo de elite de Anons como Kayla, Topiary e Tflow. O mais extraordinário é que, enquanto seus atos foram traindo a retórica, Sabu gradativamente se posicionou como o mais espetacular herói revolucionário do Anonymous.

CAPÍTULO 9

O revolucionário O dramático envolvimento de Sabu com o Anonymous talvez nunca tivesse acontecido não fosse um importante encontro: em meados de dezembro de 2011, Tflow convidou Sabu, na vida real um nova-iorquino de 28 anos de idade com longa ficha corrida de contravenções, para entrar na sala de bate-papo #InternetFeds. Nela, Sabu travou contato pela primeira vez com Kayla e outros hackers que o ajudariam a atacar uma miríade de outros alvos tendo em mente uma missão revolucionária. Até aquele momento, os ataques do Anonymous haviam reagido às circunstâncias: Chanology devido a Tom Cruise; Operação Vingança devido ao desprezo de algumas empresas em relação ao WikiLeaks. Mas Sabu almejava que o Anonymous fosse mais do que apenas pirralhos brincando de hackers.

Desejava que ele mudasse o mundo.

Sabu era um antigo ciberpunk. Não utilizava palavras como *moralfag* ou *lulz* e não entrava no 4chan. Conquistava redes e depois se deleitava com suas realizações. Interessava-se mais pelo selo de prestígio resultante de dominar redes inteiras de provedores de serviço da internet (ISP) do que por azucrinar cientologistas. Enquanto os trolls do 4chan como William procuravam diversão aleatória, Sabu queria ser um herói baixando a crista de gente em postos de autoridade. Não se constrangia ao citar alvos importantes nem ao manter conversas filosóficas. Em sua década no subterrâneo, ele alegou conseguir controlar sistemas de nomes de domínio dos governos de países como Arábia Saudita, Porto Rico, Bahamas e Indonésia.

Sabu era conhecido por exagerar, e outros hackers que lidavam com ele escutavam suas conquistas com certo ceticismo. Embora fosse um hacker de extrema perícia, Sabu muitas vezes mentia sobre sua vida, contando às pessoas

coisas que talvez desejasse que fossem verdadeiras – que ele vinha de Porto Rico; que sua mãe verdadeira era uma destacada líder na comunidade política local; que, na vida real, ele era casado e “altamente bem--sucedido em seu ramo”. Na verdade, ele era desempregado, inseguro e lutava para sustentar a família.

O nome verdadeiro de Sabu é Hector Xavier Monsegur. Morava num condomínio de baixa renda em Lower East Side, Nova York, e, com a ajuda da assistência social do governo, sustentava cinco irmãos, uma irmã, duas primas, de sete e doze anos, a quem ele costumava chamar de filhas e das quais ele tinha a guarda legal e um pitbull branco chamado China. Seus antepassados eram de Porto Rico e Monsegur tinha uma queda por ativismo de esquerda. Quando criança, os mais velhos lhe contavam histórias sobre a revolta de El Grito de Lares. Sabu contava à família que, um dia, ele conflagraria sua própria revolução.

Nascido na cidade de Nova York em 1983, Monsegur cresceu em relativa pobreza. O pai, também chamado Hector, e a tia Iris vendiam heroína nas ruas. Quando Monsegur completou catorze anos, os dois foram presos por tráfico de drogas e condenados a sete anos de cadeia. Monsegur foi morar com a vó Irma num apartamento no sexto andar do conjunto habitacional Jacob Riis, em Lower East Side.

Enquanto se adaptava à nova casa, ele descobriu *The Anarchist Cookbook (Livro de receitas do anarquista),* o famoso livro publicado originalmente em 1971, que lhe deu acesso a dicas para hackear linhas telefônicas a fim de fazer telefonemas de graça e também a instruções sobre como construir bombas napalm a partir de sabão. A avó não conseguia bancar uma conexão de internet rápida, por isso o jovem Monsegur seguiu as instruções para conectar o computador da família ao serviço de internet EarthLink gratuitamente. Enquanto explorava a web, ele também enveredou na EFnet, popular rede de bate-papo interativo frequentada por hackers (anos mais tarde, Kayla também participaria). Por fim, Monsegur acabou deparando com um ensaio on-line redigido por um afamado hacker da década de 1980, apelidado de Mentor. Intitulado *The Hacker’s Manifesto*, o texto provocou no garoto mais efeito do que qualquer outro material lido on-line. Mentor, cujo nome verdadeiro era Lloyd Blankenship, escrevera o curto ensaio por um capricho em 8 de janeiro de 1986, duas horas antes de a polícia prendê-lo por hackeagem de computadores.

“Você, com sua psicologia de três peças e seu cérebro de tecnologia dos anos 1950, já se deu ao trabalho de fitar os olhos de um hacker? Sou um hacker, entre em meu mundo...”

– Puxa vida – falou Monsegur, relembrando o fato numa entrevista, anos mais tarde. – Foi aquela leitura que me tornou o que sou hoje.

A última linha do manifesto teve especial ressonância para ele: “Meu crime é ser mais esperto do que você, e você nunca vai me perdoar por isso”.

A ideia de que pessoas detentoras de autoridade, desde professores até a mídia, não compreendiam os verdadeiros talentos dos hackers era algo que Monsegur entendia muito bem. Na condição de jovem latino morando no conjunto habitacional onde sua própria família negociava drogas, ele não se enquadrava na descrição de um nerd e hacker de computador.

Assim, tornou-se muito comum ser confrontado por pessoas que duvidavam de sua capacidade. Mas ele tinha muita vontade de aprender.

Após conectar com sucesso sua família à internet grátis, Monsegur queria descobrir o próximo desafio a conquistar.

Ele lia mais on-line, experimentava e pegava algumas dicas com pessoas das redes de IRC como a EFnet. Ainda com apenas catorze anos, Monsegur aprendeu sozinho a fazer programas de software em Linux, Unix e redes de código aberto.

Fora da escola, Monsegur mostrava seus talentos: entrou num projeto local para treinamento de jovens programadores talentosos, chamado NPowerNY Technology Service Corps, e logo conseguiu experiência de trabalho pesquisando segurança de rede no Welfare Law Center. Aos dezoito anos, participava do programa de aconselhamento iMentor, como estagiário de tecnologia.

Nessa ocasião, ele se tornara um jovem alto de ombros largos, que relutava em aceitar a autoridade. Segundo o ensaio escrito pelo adolescente Monsegur, em agosto de 2001, a origem de tudo havia sido um incidente ocorrido em seu colégio, Washington Irving High School, em Manhattan.

Hector trabalhava no colégio durante o horário das aulas, instalando Windows

nos computadores por ele rotulados de “obsoletos”, quando um dia, ao passar pelo detector de metais, o chefe da segurança o mandou parar e o questionou sobre a chave de fenda que portava.

Ele relembra ter declarado: – Sou o especialista em computadores que conserta seu sistema quando vocês se esquecem de que não devem rodar programas com vírus.

– Ei, olha como fala comigo, garoto – respondeu o chefe da segurança, encarando-o.

Monsegur explicou de novo. Ele era um aluno que trabalhava nos “computadores não funcionais durante meu horário escolar”. O chefe da segurança apreendeu a chave de fenda.

– Obrigado – disse ele. – Vou ficar com isto.

Constrangido e indignado, Monsegur escreveu uma reclamação e entregou-a às autoridades do colégio, acusando o chefe da segurança de “punição corporal” e “desrespeito”. Ao perceber que o protesto fora ignorado, distribuiu um “artigo controverso” a seus professores. Durante a aula, o diretor do colégio foi chamá-lo, pedindo-lhe se podia vir até a porta para que conversassem. Explicou que ele e outros funcionários do colégio consideraram que o texto de Monsegur continha ameaças.

“O sujeito me olhou da cabeça aos pés”, escreveu Monsegur em seu ensaio. “Desrespeitou-me fisicamente diante de dezenas de alunos. O que aconteceu com minha reclamação? Onde está a justiça que procuro?”

Monsegur sentiu-se abandonado. Semanas mais tarde, recebeu uma ligação de seu professor. Nas palavras de Sabu, foi então informado de que ele estava “temporariamente expulso da escola”.

Monsegur respondeu: – Muito bem, então. Mas é uma vergonha que eu seja privado de minha educação por causa de um texto que escrevi.

Quando o professor estava prestes a rebater, Monsegur desligou. A Administração de Serviços para a Criança do governo municipal de Nova York solicitou, então, que ele consultasse um psicólogo para realizar uma avaliação mental. Monsegur afirma ter sido aprovado na avaliação. Mas abandonou o

ensino médio sem terminar o primeiro ano.

On-line, ele satisfazia suas ambições e evitava o “desrespeito” que sentia pelos detentores de autoridade. A essa altura, ele já aprendera a invadir os servidores de grandes organizações, desde universidades japonesas até governos terceiro-mundistas. Monsegur gostava da empolgação de subjugar um sistema de computador, e logo dava uma guinada de protegê-los em seus estágios para invadi-los em seu tempo livre.

Nesse meio-tempo, ele tomara contato com o hacktivismo. Aos dezesseis anos, um belo dia, defronte à tevê, Monsegur assistiu a uma reportagem sobre protestos em Vieques, ilha ao largo da costa de Porto Rico. A Marinha dos EUA estivera utilizando as águas circundantes para testar bombas e, um ano antes, em 1999, uma bomba perdida tinha matado um guarda civil local. O funeral do guarda recebeu atenção da imprensa mundial e provocou uma onda de protestos contra os bombardeios. Nas transmissões da tevê, soldados arremetiam contra os manifestantes, inclusive o reverendo Al Sharpton, líder comunitário em Nova York sobre o qual Monsegur tinha ouvido falar, por conta de seu crescente interesse em ativismo de esquerda. Algo estalou dentro dele.

O rapaz foi até seu computador, desenhou um mapa de rede de todo o espaço de IP em Porto Rico e descobriu que uma empresa chamada EduPro administrava os sites do governo. Hackeou os servidores da empresa, descobriu a senha raiz e obteve acesso administrativo. No calor do momento, também digitou uma indignada missiva no Microsoft Word, ignorando os próprios erros ortográficos: “Deem a nós o Respeito que merecemos”, escreveu ele. “Ou devemos conquistá-lo à força? Cabron”.

Ele derrubou os sites do governo porto-riquenho e os desfigurou com sua mensagem, que ficou no ar durante vários dias. Satisfeito com o trabalho, Monsegur analisou que esse havia sido seu primeiro ato de hacktivismo. Quando, duas semanas depois, os militares dos EUA concederam o controle da base de Vieques ao governo local, ele sentiu que isso se devia parcialmente a seus atos.

Monsegur queria continuar a hackeagem. Passou a se dedicar plenamente a ela, participando dos primeiros movimentos de uma guerra cibernética entre hackers dos EUA e da China, que em sua maioria envolveu rapazes de cada país trocando farpas e desfigurando sites do país do outro lado do mundo. A

Operação China aconteceu em 2001, mesmo ano em que Monsegur parece ter abandonado o ensino médio. Pequim naquela época tinha se recusado a dar ao presidente Clinton acesso a um avião espião dos EUA que colidira com um caça da Aeronáutica chinesa e fizera um pouso de emergência na ilha de Hainan. A tripulação sobrevivente dos EUA permaneceu detida por onze dias, e durante esse período alguns hackers dos EUA sequiosos por violência, como Monsegur, invadiram centenas de sites chineses e os picharam com mensagens como "Odiaremos a China para sempre". Os hackers chineses contra-atacaram com frase do tipo "Abaixo o imperialismo dos Estados Unidos". A essa altura, Monsegur já utilizava habitualmente o nickname Sabu, emprestado de um lutador de luta livre popular nos anos 1990 por seu estilo extremo, e que se vangloriava de pertencer a uma minoria, alegando ser da Arábia Saudita, quando na verdade era natural de Detroit, de uma família de origem libanesa. Sabu, de modo semelhante, alegava on-line ter nascido e crescido em Porto Rico.

O grupo de Monsegur, chamado Hackweiser, foi fundado em 1999 por um talentoso hacker canadense apelidado de P4ntera. Contava com de dez a quinze hackers quando Monsegur entrou. Seu papel no grupo permaneceria igual uma década depois: ele invadia, ou hackeava, o máximo de servidores que conseguia. Mais tarde, em 2001, após Sabu ter passado vários meses aprendendo o caminho das pedras com o Hackweiser, P4ntera de repente saiu de cena. Monsegur se deu conta: se o carismático líder do grupo podia ser preso, o mesmo poderia acontecer com ele. Lutou contra seu ego. Amava ver "Sabu" ganhar notoriedade pelas audaciosas invasões que perpetrava, mas não queria ir para a cadeia.

– Nós, humanos, temos um ego frágil – lembrou-se mais tarde Sabu. – Assim, é necessário que nosso trabalho seja reconhecido.

Mas Monsegur decidiu atuar de modo seguro e interrompeu todo e qualquer uso público do nome Sabu, agindo nos porões pelos próximos nove anos. Quando "Sabu" por acaso reaparecia on-line, era apenas em salas de bate-papo privadas. Também tentou utilizar suas habilidades como programador para fins legítimos. Em 2002, fundou um grupo para programadores locais em Python, popular linguagem de programação.

Apresentando-se como Xavier Monsegur, ele convidava os outros a "integrar seus conhecimentos em uma grande massa de informações assustadoras", e afirmava que o site feito por ele estava "quase em seu layout final... Será sobre todos nós, nosso conhecimento, nossas ideias, só a 'gente' se divertindo e

apreciando o que temos e podemos fazer”.

O sociável programador começou a realizar trabalhos como freelancer para a Tiger Team, empresa sueca do ramo de segurança em TI, e depois conseguiu emprego na LimeWire, empresa de compartilhamento de arquivos peer-to-peer. Continuava morando com a avó e usando seus talentos de hacker para ajudar os vizinhos do prédio a aumentar de modo fraudulento suas classificações de crédito. Assim, Monsegur recebia esporadicamente dinheiro de fontes tanto legais quanto ilegais: às vezes por trabalho legítimo; outras vezes por vender maconha nas ruas ou por hackear uma rede de computadores para vender números de cartão de crédito.

Mas um tsunami de problemas surgiu em 2010, quando ele tinha 26

anos. O pai e a tia tinham sido soltos da cadeia, mas a tia havia voltado a vender heroína e naquele ano foi presa novamente. Ela deixou as duas filhas sob os cuidados de Monsegur, e ele obteve a custódia legal das garotas. Por volta da mesma época, perdeu o emprego na LimeWire, após o grupo RIAA da indústria de gravação abrir um processo de 105 milhões de dólares contra a empresa, que foi obrigada a dispensar os funcionários.

Pior: a avó de Monsegur, com quem ele havia morado desde os catorze anos, veio a falecer.

– Isso o deixou alterado – mais tarde um membro da família contou ao *The New York Times*, referindo-se à morte da avó.

Monsegur tornou-se antissocial, hackeando fabricantes de veículos para encomendar motores de carros e perturbando a vizinhança tocando música em alto volume, muitas vezes até as quatro da madrugada, na casa em que sua avó não mais residia.

Desempregado e à deriva, no começo de dezembro Monsegur deparou com uma causa apaixonante: o Anonymous entrava em cena no caso do WikiLeaks. Ele assistiu ao primeiro ataque contra o PayPal se desenrolar e viu nessa ação ecos de seu trabalho com o Hackweiser e seu ataque de protesto a favor da ilha de Vieques, mas numa escala bem mais grandiosa.

Mais tarde, diria que o Anonymous era o movimento que ele estivera esperando todos esses anos no “subterrâneo”.

Em 8 de dezembro, quando o AnonOps teve seu pico de visitantes para o grande ataque inicial contra o PayPal, Monsegur registrou-se na sala de bate-papo pública, utilizando o nome Sabu pela primeira vez em quase uma década. No IRC AnonOps reinava o caos, com centenas de trolls e script kiddies (aspirantes a hackers) falando ao mesmo tempo.

– a gente precisa do nome do funcionário da wired que acabou de falar na cnn – falou, referindo-se ao chefe do escritório da revista *Wired* da cidade de Nova York, John Abell. – john swell? john awell? me digam o nome, por favor!!

Usando o codinome Sabu, ele repetiu o pedido três vezes. Por fim topou com Tflow, que conversava sobre termos avançados de programação. Após conversarem via mensagens privadas, nenhum deles revelando sua localização verdadeira ou qualquer outra informação identificadora, Tflow mostrou a Sabu o acesso ao canal secreto dos hackers: #InternetFeds.

Seguro e pacato, o #InternetFeds era bem diferente das salas de bate-papo abertas do AnonOps, em que centenas clamavam por alvos grandes e impossíveis como Microsoft e Facebook. Fazia pouco sentido tentar explicar à horda os motivos por que esses alvos não funcionariam, que primeiro se tornava necessário encontrar uma vulnerabilidade em um servidor. Era como tentar explicar a história do futebol a um ruidoso estádio lotado de gente louca para vibrar com um gol. Tinha acontecido o mesmo no Chanology, quando o canal #xenu recebeu o apoio do planejamento tranquilo do #marblecake. A discórdia se acirrou no #operationpayback sobre quem deveria sentir o ódio do Anonymous em seguida; a controvérsia envolvendo o WikiLeaks sumia das manchetes, e os hackers estavam entediados de tentar atacar os críticos de Assange. Sabu, Kayla e os demais no #InternetFeds conversavam cada vez mais em concentrar seus esforços em outra crescente notícia: a revolução no Oriente Médio.

Sabu já tinha interesse na região, tendo participado, quando mais jovem, de uma ou duas marchas pró-Palestina. Agora, ele e os outros liam artigos sobre manifestações na Tunísia, cuja centelha fora a publicação dos documentos pelo WikiLeaks. O governo da Tunísia censurava rigorosamente o uso da internet pelos cidadãos. Os sites que criticavam o governo eram hackeados, seus conteúdos apagados e seus servidores cortados. Habitantes que visitavam sites e blogs pró-democracia muitas vezes deparavam com mensagens de erro.

No começo de janeiro de 2011, a censura do governo tornou-se ainda pior. A Al Jazeera relatou que o governo da Tunísia começou a sequestrar os registros e a senhas de seus cidadãos no Facebook, no processo conhecido como phishing. Normalmente essa tática era de criminosos cibernéticos; nesse caso, um governo a utilizava para espiar o que os cidadãos comentavam nas redes sociais e nos serviços de correio eletrônico como Gmail e Yahoo. Se os fiscais farejavam dissidentes, às vezes essas pessoas eram presas. Os nativos precisavam mudar constantemente suas senhas no Facebook para tentar escapar do controle do governo. Em um período em que o país de mais de 10 milhões de habitantes estava à beira da revolução política, os manifestantes e os cidadãos comuns lutavam para evitar os espiões do governo.

Os hackers no #InternetFeds tiveram um ideia, em parte graças a Tflow.

O jovem programador escreveu um script da web que os tunisianos podiam instalar em seus navegadores e que lhes permitiria evitar os olhos abelhudos do governo. O script tinha a extensão de duas páginas, e Tflow o testou com outro Anon da Tunísia, que usava o nickname Yaz, e depois o colou num site chamado userscripts.org. Ele e mais alguns então fizeram propaganda do link na sala de bate-papo #OpTunisia no AnonOps, no Twitter e por meio de folhetos digitais. O assunto foi veiculado em alguns noticiários. O hacktivista Q, um dos membros do #InternetFeds e também um dos doze operadores do canal #OpTunisia, começou a falar com os tunisianos no AnonOps – aqueles que tinham conhecimento cibernético suficiente para acessá-lo via servidores proxy – e os incentivou a espalhar a notícia sobre o script pelas redes sociais.

– A OpTunisia me fascinava – mais tarde Q afirmaria numa entrevista. – Realmente provocamos um impacto ao atrair a atenção da mídia ocidental para as coisas que estavam acontecendo lá.

Em poucos dias, chegaram notícias de que o script tinha sido publicado no site de notícias tecnológicas ArsTechnica e havia sido baixado mais de 3

mil vezes por usuários da web tunisianos.

Sabu ficou impressionado, mas ele queria causar uma espécie de impacto diferente – um mais barulhento. Relembrando o tempo em que fizera o deface dos sites do governo porto-riquenho, decidiu que apoiaria a revolução tunisiana constrangendo o governo local. Facilitava a missão o fato de os sites de governos

daquela região serem relativamente fáceis de hackear e desfigurar.

Sabu e mais alguns do #InternetFeds descobriram que apenas dois servidores de nome hospedavam o site do governo da Tunísia. Isso era incomum – a maioria dos governos e grandes empresas com presenças na web rodavam em vários servidores de nome, de modo que, se um hacker invadisse alguns, em geral isso não causava danos substanciais. No caso da Tunísia, porém, um ataque eficaz contra apenas dois servidores de nome derrubaria completamente os sites do governo.

– Era uma configuração bastante vulnerável – relembrou um hacker que participava do #InternetFeds. – Foi moleza tirá-los do ar.

Para colocar os servidores tunisianos off-line, Sabu não utilizou um botnet. Em vez disso, mais tarde ele explicaria, sequestrou servidores de uma empresa londrina de hospedagem de sites, o que lhe permitiu arremessar 10 gigabytes de dados por segundo aos servidores tunisianos.

Esses servidores eram de transmissão, o que amplificava muitas vezes a quantidade de dados de spam de um servidor básico; funcionava como usar uma lente de aumento para intensificar os raios do sol e destruir um grupo de formigas. Agindo sozinho, Sabu deixou os servidores tunisianos inativos por cinco horas. Logo, porém, as autoridades do outro lado começaram a filtrar os pacotes falsificados, como o dono de uma mansão que manda o mordomo não trazer correspondência de determinada pessoa. O tráfego enviado por Sabu perdia a eficácia. Inabalável, ele pediu a ajuda de um velho amigo, alguém que conhecia da época em que dava seus primeiros passos no crime cibernético. Enquanto Sabu atacava o primeiro servidor de nome, o amigo derrubava o segundo.

O ataque aos sites da Tunísia foi o primeiro envolvimento real de Sabu no Anonymous. Ele não só eliminou a presença do governo on-line; ele e um punhado de outros também acessaram dezenas de e-mails de funcionários do governo.

Mas o governo contra-atacou novamente. Bloqueou todas as solicitações de internet com origem externa, blindando suas operações contra Sabu e outros usuários estrangeiros da web. Sabu queria fazer o deface do site do primeiro-ministro tunisiano Mohamed Ghannouchi, mas teria de fazê-lo em terras

tunisianas – e não estava de voo marcado. Por isso, em 2 de janeiro, registrou-se no canal de bate-papo #OpTunisia com seus doze operadores de canal e várias centenas de outros Anons mundo afora, inclusive da Tunísia. O papo mencionava o uso de proxies e potenciais ataques de DDoS; o pessoal queria saber o que estava rolando.

Então Sabu apertou a tecla que fixa as maiúsculas e fez sua entrada triunfal: – QUEM ESTIVER NA TUNÍSIA E QUISER SER MEU REPRESENTANTE

NA INTERNET TUNISIANA FAVOR ENVIAR MSG PARA MIM.

Silêncio na sala. Poucos minutos depois, Sabu recebeu uma resposta privada de alguém com nome de usuário automatizado como Anon8935 – se você não escolhia um nickname exclusivo no AnonOps, a rede lhe fornecia um semelhante a esse –, sujeito que alegava estar na Tunísia. Sabu não sabia o nome verdadeiro do homem, e nem perguntou. Nem sequer sabia se Anon8935 digitava no sufocante calor urbano ou no isolado e pacato subúrbio. O homem disse apenas que havia participado dos protestos nas ruas e agora queria tentar algo diferente, algo com a internet.

Só havia um problema: ele não sabia nada sobre hackeagem. Sabu lhe deu diretrizes básicas e disse: – Meu irmão. Está pronto?

– Sim – respondeu o outro.

– Percebe que vou utilizar o seu computador para hackear o site pm.gov.tn?

– Ok – respondeu o homem. – Diga-me o que fazer.

Sabu enviou algumas instruções breves para baixar e instalar um programa que permitiria a Sabu assumir o controle do computador do homem. Logo ele operava uma versão antiquada do Windows e uma conexão de internet dolorosamente lenta.

– Está me enxergando? – indagou Sabu, movendo o cursor do mouse.

– Ok! – exclamou o homem.

Sabu arregaçou as mangas e pôs mãos à obra, enquanto o tunisiano recostou-se e só ficou assistindo. Sabu abriu a solicitação de comando e começou a digitar

códigos de programação que seu novo amigo nunca tinha visto antes: uma espessa coluna de texto branco contra um fundo preto representando as estradas vicinais da web. Cerca de quarenta minutos depois, Sabu entrou no site oficial do presidente da Tunísia, imaginando os olhos arregalados do tunisiano. Minutos depois, o site oficial do presidente tinha sido derrubado, substituído por uma simples página branca com letras pretas. No alto, em fonte Times New Roman de bom tamanho, lia-se "A vingança é um prato que se come frio, não é mesmo?". Embaixo dessa frase, via-se a gigantesca silhueta negra de um navio pirata e o nome Operação Vingança. A palavra *operação* reforçava a ideia de que não era um mero protesto ou anarquia; era uma missão.

Nesse ínterim, Tflow dissera a Topiary que uma hackeagem na Tunísia estava em andamento, solicitando-lhe se podia criar uma declaração oficial para o deface. Topiary redigiu e repassou a declaração a Tflow, que a enviou para Sabu, que, por sua vez, a utilizou para substituir o site oficial do primeiro--ministro tunisiano Ghannouchi.

"Saudações do Anonymous", lia-se na página inicial do pm.gov.tn.

"Estivemos acompanhando o modo como o governo da Tunísia trata os cidadãos tunisianos, e estamos ao mesmo tempo profundamente entristecidos e enraivecidos com o comportamento do governo."

Continuava em tom dramático até arrematar com o slogan: "Somos Anonymous, Somos Legião... Esperem por nós".

Sabu fitou a nova página, recostou-se na cadeira e abriu um sorriso.

– Você nem imagina a sensação de ter usado a internet desse cara para hackear o site presidencial – recordou ele mais tarde. – Foi incrível.

O governo da Tunísia tinha criado um firewall para impedir que hackers estrangeiros atacassem seus servidores; jamais contava que alguém dentro de suas fronteiras perpetraria um ataque.

– Obrigado, irmão – disse Sabu. – Certifique-se de apagar tudo que você baixou e resetar sua conexão.

Após alguns minutos, o homem se desconectou e, poucos dias depois, Sabu pendurou uma bandeira tunisiana em sua casa. Então ficou sabendo que o

homem fora preso. Ao mesmo tempo em que teve pena de seu voluntário, Sabu não se sentiu culpado. Uma causa mais nobre havia sido priorizada. Mais tarde, recordou: – A Operação Tunísia marcou o começo de um relevante avanço técnico do Anonymous.

Em 14 de janeiro, o presidente tunisiano Ben Ali renunciou. Foi um momento histórico, após um mês de milhares de tunisianos se manifestarem contra o desemprego e o poder abrangente de Ali, culminando em uma nova forma de protesto on-line, uma aliança com pessoas do outro lado do mundo cooperando com cidadãos locais.

Ali fugiu da Tunísia e pegou um avião para a Arábia Saudita, e Sabu, depois de semanas a fio, encerrou seu ataque contra os sites do governo tunisiano. Em fevereiro, Ghannouchi também renunciou, e, ao longo dos meses seguintes, a censura da internet no país diminuiria de modo significativo. Nesse meio-tempo, Sabu, os hackers do #InternetFeds e os Anons do AnonOps voltaram suas atenções a outros países do Oriente Médio. Sabu trabalhou com outros hackers para derrubar sites governamentais da Argélia, e depois acessar e-mails do governo do Zimbábue em busca de provas de corrupção. Sabu e Kayla continuavam a fazer a hackeagem; Tflow, a coordenação; e Topiary redigia as mensagens de deface. A nova campanha do Anonymous no Oriente Médio movia-se na velocidade da luz, com equipes de voluntários atacando um site árabe diferente quase todos os dias. Sentiam-se estimulados pelas vulnerabilidades que descobriam, pelos novos sentimentos de camaradagem – e pela resultante atenção da mídia.

Kayla, em especial, estava nas nuvens, não só porque apreciava apoiar a revolução. A hacker tinha feito um acordo secreto com alguém que alegava pertencer ao WikiLeaks.

CAPÍTULO 10

Conhecendo a ninja

À medida que o Anonymous dedicava suas atenções ao Oriente Médio no início de janeiro de 2011, Topiary continuava a organizar e a redigir mensagens de deface no #propaganda e a conversar com os jornalistas no #reporter. O #command não era mais o canal – muitos operadores e muito lero-lero. Havia cerca de vinte Anons em cada canal de publicidade, a maioria deles redatores de mão-cheia que já tinham escrito comunicados de imprensa para o Anonymous no passado. Lá, de vez em quando, Topiary conversava com Tflow, que aparecia no #propaganda para solicitar uma mensagem de deface; logo Topiary veria seu texto publicado no site do governo oficial do Zimbábue. Com a ajuda de um Anon francês, uma versão em francês também foi postada.

Topiary gostava de explicar o Anonymous a repórteres e de escrever mensagens de deface que chocavam os visitantes e os proprietários de um site. Também gostava de aprender a como lidar com a imprensa, como deixá-la interessada numa história pela oferta de informações exclusivas.

Ficava se perguntando se os redatores e porta-vozes como ele estavam entre os membros mais influentes do Anonymous no mundo fora do grupo.

Logo as pessoas começaram a convidá-lo a frequentar mais canais sobre os quais ninguém conversava publicamente. Em 2 de janeiro, ele recebeu um importante tapinha no ombro, dessa vez de Tflow.

Sabu, por intermédio de um voluntário local, estivera se preparando para assumir o controle do site do primeiro-ministro e precisava de uma boa mensagem de deface, e rápido.

– Os principais sites do governo da Tunísia vão ser hackeados – contou Tflow a Topiary. – Pode bolar a mensagem de deface?

Topiary sentiu uma animação instantânea. Essa era a primeira vez que alguém lhe havia confiado a informação de que uma invasão estava prestes a acontecer. Ansioso por ajudar, ele e Tflow comentaram sobre o horário da operação de deface. Depois Topiary escreveu sua costumeira mensagem nefasta para o repressivo governo tunisiano.

Quando a invasão acontecia e a mensagem de deface estava sendo carregada, Topiary e Tflow entraram nas principais salas de bate-papo do AnonOps e fizeram um rápido comentário sobre o ataque, para inspirar um pouco as tropas.

Assim que a missão acabou, Tflow surpreendeu Topiary novamente ao convidá-lo a entrar no #InternetFeds. Definitivamente ele demonstrava confiança em Topiary para colaborar e trocar ideias com alguns dos mais habilidosos hackers que trabalhavam com o Anonymous. Topiary tinha sido um forasteiro aos olhos dessas pessoas, mas aos poucos foi ganhando sua atenção.

Ao longo do mês seguinte, grande parte da hackeagem de Sabu e dos textos de Topiary estaria na vanguarda dos ataques cibernéticos do Anonymous contra os governos de países como Líbia, Egito, Zimbábue, Jordânia e Bahrein. O Anonymous não só desfigurava sites, mas também publicava endereços de e-mail e senhas do governo. Os ataques também continuavam em outras partes do mundo em nome do Anonymous; dois hackers irlandeses fizeram o deface do site do principal partido de oposição da Irlanda, o Fine Gael. Em meio à onda de atividade revolucionária, o Anonymous passou a ser encarado menos como um bando de pirralhos enfarados e mais como verdadeiros ativistas.

Então, em 5 de fevereiro, Tflow enviou a Topiary outra mensagem privada pelo IRC AnonOps, convidando-o a um canal IRC ainda mais secreto, que incluía apenas um punhado de gente importante do #InternetFeds. Quando Topiary entrou na exclusiva sala de bate-papo, esqueceu que tinha (de brincadeira) configurado um script de programação para rodar no seu software de IRC que expulsava qualquer pessoa da sala que não utilizasse pelo menos 80% de letras maiúsculas. Sua primeira interação com Sabu envolveu expulsá-lo da sala de bate-papo.

Constrangido, Topiary se desculpou e rapidamente desativou o script. Sabu relevou, e o quinteto – Topiary, Sabu, Kayla, Tflow e Q – rapidamente começou a trocar ideias. O tópico: HBGary e o artigo de Aaron Barr no *Financial Times*.

Topiary não conseguia captar quem ou o que Kayla era. Vagamente recordava ter visto o nome em sua velha lista de bate-papo do MSN, em uma inundação do 4chan em 2008 e em artigos sobre ela na Encyclopedia Dramatica. Em meio a vários rostos sorridentes e lols, ela conversava sobre hackeagem como se fosse um vício. Não conseguia entrar num site sem conferir se existiam furos no código fonte que ela pudesse explorar, talvez lhe permitindo furtar uma ou duas

bases de dados. Ela revelava-se uma charada: parecia ser a pessoa mais falante e afável do grupo, mas também era paranoica e aparentemente perigosa. Desenvolvera uma proteção blindada sobre sua identidade verdadeira, e o ousado reconhecimento de que tinha dezesseis anos, junto com a esmagadora quantidade de emoticons e corações (<3), sugeria que se esforçava muito para soar feminina.

Topiary sabia que era uma raridade encontrar hackers do sexo feminino; um hacker que se declarava mulher provavelmente não o era na vida real, embora talvez fosse transgênero, gay ou pelo menos algo nessa linha. Um amigo on-line de Topiary, com o nickname de Johnny Anonymous, conduziu sua própria e específica pesquisa no final de 2010.

Fez uma série de perguntas a cento e cinquenta usuários do começo da rede AnonOps. Cerca de sessenta, ou um terço, se identificaram com LGBT

(gays, lésbicas, bissexuais, transexuais e transgêneros), enquanto os demais se declararam héteros.

– A gente brinca com os travestis porque existem muitos deles entre nós – contou Johnny Anonymous numa entrevista.

De tão obcecada por ocultar sua identidade, Kayla recebeu de Topiary a alcunha de “a ninja”. Ela modificava suas senhas quase diariamente.

Alegava manter todos os seus dados num minúsculo cartão microSD e mantinha seu sistema operacional num único pen-drive, que ela utilizava para inicializar seu netbook. Como a maioria dos hackers, ela utilizava uma VM (máquina virtual) para fazer toda a sua bruxaria cibernética; funcionava como efeito tampão entre seu computador e a vida on-line.

Assim, se alguém um dia a hackeasse, teria acesso apenas à máquina virtual. Ao contrário de Topiary e muitos outros Anons, ela evitava o uso de redes privadas virtuais (VPN). Não confiava nelas, já que um provedor de VPN sempre poderia entregar dados de Kayla à polícia. Mantinha um celular de baixo custo com cartão SIM não registrado, o aparelho mais seguro usado por ela, no qual anotava todas as suas senhas. Subdividiu um pequeno drive chamado sys no celular para armazenar códigos maliciosos.

Parecia paranoia, mas Kayla disse mais tarde numa entrevista que havia

aprendido uma terrível lição sobre a necessidade de esconder sua identidade na web logo após começar a atacar fóruns de hackers. Reza a lenda que, quando Kayla era mais jovem (segundo ela, aos catorze anos), ao tentar doxear outros hackers por pura diversão, em uma oportunidade acabou escolhendo o alvo errado. Tratava-se de um hacker do sexo masculino que retaliou fazendo sua própria hackeagem, encontrando um dos velhos endereços de e-mail da garota em outro fórum. Obteve seu nome, data de nascimento, a cidade onde morava e certas informações sobre sua família. Ligou para sua casa e ela atendeu. Enfurecido, ele ameaçou chamar a polícia. Ao revisitar a história, Kayla contou que o homem se recusava a acreditar em como ela era jovem, o que a levou às lágrimas. Quando, por fim, ele se acalmou, os dois combinaram de se encontrar numa cidade próxima. Escolheram um shopping movimentado onde se encontraram e sentaram para conversar. O homem mostrou interesse na vida de Kayla e nos motivos pelos quais ela hackeava. Revelou ter encontrado seus dados a partir de antigos perfis no MSN e em fóruns de hackers. Para Kayla, essa informação foi uma bofetada na cara: suas informações estavam lá, só esperando para serem descobertas.

Assim que Kayla chegou em casa, apagou todo o conteúdo de suas contas, excluindo todos os e-mails, e leu mais sobre como se tornar completamente invisível na internet. Um ano depois, havia estabelecido seu regime quase militar e se tornara confiante o suficiente para hackear nomes maiores. Não conseguia se livrar da atração pela hackeagem – havia algo mágico em ter acesso a informações que outros não tinham. Seu nome on-line, afinal de contas, significa “a responsável pelas chaves” em inglês arcaico. E o ataque que selaria o seu lugar na sala de bate-papo #InternetFeds e nas mentes de outros hackers foi a invasão do site de notícias Gawker.

O Gawker outrora estivera em alta entre os Anons. Tinha sido o primeiro site de notícias a publicar audaciosamente o vídeo maluco de Tom Cruise, a centelha do Chanology. Depois, porém, a tão famosa e irritável voz do site se voltou contra o Anonymous, descrevendo importantes ataques do 4chan como exemplos de bullying em massa. Quando Adrian Chen, repórter da internet, publicou no Gawker várias histórias que ridicularizavam o Anonymous, caçoando de sua falta de perícia em hackeagem e as brigas infantis do 4chan com o Tumblr, os usuários do *b* tentaram arremeter um ataque de DDoS contra o próprio Gawker, mas fracassaram. Em resposta, Ryan Tate, redator do Gawker, publicou um artigo em 19 de julho de 2010 sobre o ataque fracassado, frisando que o Gawker se recusava a ser intimidado. Se os “infelizes usuários do 4chan tiverem um

problema com isso, sabem onde me encontrar", acrescentou ele. Kayla, na época, se magoara com o comentário e sentira o habitual impulso de punir todos que a subestimassem ou subestimassem o Anonymous.

– A gente não deu bola até eles começarem a se exibir, tipo "lol vocês não conseguem nos hackear, ninguém consegue nos hackear" – comentou mais tarde numa entrevista. Embora o Gawker não tivesse dito isso literalmente, foi a mensagem que Kayla recebeu.

Ela decidiu perseguir o site. Encontrou-se com um grupo que mais tarde ela alegou ser composto por cinco outros hackers em um canal de bate-papo chamado #gnosis, numa rede de IRC que ela mesma havia criado chamada tr0ll. Um número de três a nove pessoas sempre estava na rede a qualquer hora. Kayla na verdade tinha várias redes de IRC, embora, em vez de hospedá-las por conta própria, fizesse outros hackers hospedá--las em servidores legítimos de países que não dariam a mínima para uma ordem de um tribunal dos EUA. Kayla não gostava de ver seu nome ou seu pseudônimo usado por muito tempo.

Pessoas próximas a Kayla contaram que ela criara o tr0ll e o preenchera com hackers habilidosos escolhidos ou treinados por ela. Kayla aprendia rápido e gostava de ensinar dicas e truques a outros hackers. Paciente, mas exigente: um aluno lembra que ela ensinava como fazer injeções de SQL

primeiro explicando a teoria e em seguida instruindo os hackers a repetir e repetir usando diferentes abordagens por dois dias a fio.

– Era um inferno mental, mas funcionava – contou o aluno.

Kayla compreendia profundamente as inúmeras e complexas camadas de métodos como a injeção de SQL, o que lhe permitia explorar vulnerabilidades que outros hackers não conseguiam.

No tr0ll, Kayla e os amigos debatiam as complexidades dos servidores do Gawker, tentando vislumbrar um modo de roubar algum código fonte do site. Em agosto, poucas semanas após a publicação da reportagem sobre os "infelizes usuários do 4chan", eles toparam com uma vulnerabilidade nos servidores que hospedavam o Gawker.com. A brecha lhes conduziu a uma base de dados repleta com nomes, endereços de e-mail e senhas criptografadas de 1,3 milhão de pessoas que haviam se registrado no site do Gawker para que pudessem deixar comentários sobre os artigos. Kayla nem acreditou em sua sorte. Seu grupo fez

logon na conta privada de Nick Denton no Campfire, ferramenta de comunicação para os jornalistas e administradores do Gawker, e espionou tudo que a equipe do site andava comentando. Em certo ponto, notaram os editores do Gawker brincando e sugerindo manchetes uns aos outros como “Nick Denton [fundador do Gawker] afirma: Pode vir, 4chan, espero em minha casa”, e outra manchete com um endereço residencial.

Espreitaram durante dois meses, decifrando as senhas criptografadas e vendo onde mais elas tinham sido utilizadas, antes de um membro do grupo enfim hackear a conta do Twitter do blog tecnológico Gizmodo, pertencente à Gawker Media, e Kayla decidir publicar os dados das contas privadas de 1,3 milhão de usuários do Gawker numa página da web simples. Um membro da equipe sugeriu vender a base de dados, mas Kayla quis torná-la pública. Isso não tinha a ver com lucro, mas com vingança.

Em 12 de dezembro, por volta das onze horas da manhã na costa leste dos EUA, Kayla entrou no #InternetFeds para comunicar aos outros sobre sua operação colateral contra o Gawker, que estava prestes a se tornar pública. A essa altura, os ataques contra o PayPal e a MasterCard tinham chegado ao ápice, e Kayla pouco se envolvera neles. Era assim que ela costumava agir – escolhendo alvos por conta própria e, com a ajuda de poucos amigos hackers, vingando-se de alguém que lhe provocara sentimentos de afronta pessoal.

– Galera, se vocês estiverem on-line amanhã, eu e meus amigos vamos liberar tudo que temos no *b* do 4chan – avisou.

No dia seguinte, ela e os outros agraciaram os “infelizes usuários do 4chan” com milhões de contas de usuários do Gawker, de modo que gente como William pudesse se divertir à custa dos proprietários das contas.

O Gawker postou um anúncio de violação de segurança, dizendo: “Estamos profundamente constrangidos com essa falha. Não devíamos ter confiado na boa vontade dos hackers que identificaram as fraquezas de nossos sistemas”.

A declaração repercutiu no #InternetFeds.

– KKKKKKKK – disse um hacker irlandês chamado Pwnsauce. – Estrupado [*sic*] demais?

E tinha sido *uma* hacker, no “singular”, acrescentou ele.

– Nossa própria Kayla.

Kayla rapidamente acrescentou que o serviço fora feito com a ajuda de mais quatro amigos, e, quando outro hacker do #InternetFeds se ofereceu para redigir um comunicado sobre a queda do Gawker a fim de que fosse publicado no *b*, ela agradeceu e pediu: – Não mencione meu nome.

O Gnosis, em vez do Anonymous, recebeu o crédito pelo ataque. Kayla afirmou que participava do Anonymous desde 2008 e até aquele ponto raramente fizera hackeagens por outro motivo além de "rancor ou diversão", com o Gawker sendo seu maior escalpo. Mas, após entrar no #InternetFeds, ela começou a hackear alvos mais sérios, como servidores de governos estrangeiros.

Kayla não tinha participado dos ataques de DDoS do AnonOps contra o PayPal e a MasterCard porque não se importava muito com ataques de DDoS. Em sua opinião, eles eram perda de tempo. Mas mesmo assim ela ainda queria ajudar o WikiLeaks, e considerava que hackear era um meio mais efetivo de fazer isso. Não muito tempo após anunciar o ataque contra o Gawker, Kayla passou a espreitar a principal rede de IRC associada ao WikiLeaks. Por várias semanas, utilizou um nickname anônimo aleatório para ver o que as pessoas diziam nos canais principais. Observou um operador que parecia estar no comando daquele canal. Essa pessoa atendia pelo nickname q (aqui apresentado com letra minúscula, para não ser confundido com o hacktivista Q no #InternetFeds). Sectários e administradores do WikiLeaks muitas vezes utilizavam nicknames de uma letra só, tais como Q e P, porque era impossível fazer uma busca com letras avulsas no Google. Se alguém no canal tivesse uma pergunta sobre o WikiLeaks enquanto organização, ele ou ela com frequência se reportava ao geralmente calado q. Por isso, Kayla lhe enviou uma mensagem privada.

De acordo com uma fonte que acompanhou de perto a situação, na mensagem Kayla contava que era hacker e deu algumas dicas do que se imaginava fazendo em prol do WikiLeaks: hackear sites governamentais e descobrir dados que o WikiLeaks então pudesse divulgar. Não tinha certeza do que esperar, e principalmente só queria ajudar. Sem demora, q a recrutou, junto com mais alguns hackers que Kayla não conhecia na época.

Para todos eles, o WikiLeaks aparentava ser não só uma organização que "colocava a boca no trombone", mas que também solicitava a ação de hackers para obter informações roubadas.

O administrador q desejava que Kayla esquadrinhasse a internet para descobrir vulnerabilidades de sites governamentais e militares, conhecidos como .govs e .mils. Em geral, a maioria dos hackers não se envolvia com esses alvos, porque fazê-lo poderia resultar em severas sentenças de prisão, mas Kayla não se incomodava em perguntar aos amigos hackers se eles sabiam de alguma vulnerabilidade em sites .mil.

A própria Kayla passou a se dedicar de corpo e alma à missão encomendada por q, contou uma fonte, tentando identificar vulnerabilidades.

– Ela sempre foi espalhafatosa, descarada, do tipo “vou hackear e não dou a mínima” – explicou a fonte.

Mas Kayla nem sempre entregava tudo para q. Aproximadamente na mesma época em que começou a hackear para q, ela conseguiu acesso ao diretório raiz de uma importante empresa de hospedagem de sites – de todos os seus VPS (servidores virtuais privados) e de todos os servidores normais – e começou a entregar as informações garimpadas como se fossem “doce” aos amigos, inclusive a pessoas na rede de bate-papo do AnonOps.

– Ela simplesmente hackeava merda e depois jogava no ventilador – contou a fonte, explicando que Kayla largava um cache com números de cartões de crédito ou logins de raiz e depois sumia por um dia. – Ela era uma espécie de Papai Noel dos hackers.

– Para ser honesta, eu fico hackeando só por hackear – Kayla contou mais tarde em uma entrevista. – Se alguém está se queixando de algum site, eu apenas dou uma olhadela, e, se encontro um bug, conto a todos no canal.

Não tenho a ver com o que acontece daí em diante. :P

Kayla contou que ela não gostava de ser a pessoa que desfigurava um site, e preferia permanecer silenciosamente em segundo plano, “como uma ninja”.

– A chave é ser capaz de ir e vir sem deixar rastros – frisou.

Quanto mais tempo ela permanecia numa rede como a do Gawker, mais conseguia penetrar e obter, por exemplo, senhas administrativas e executivas. Gostava do Anonymous e das pessoas do grupo, mas em última análise se enxergava como um espírito livre, que não se importava em se alinhar com

qualquer grupo específico. Até mesmo quando trabalhava com o AnonOps ou com as pessoas no #InternetFeds, Kayla não considerava ter um papel ou uma área de especialização.

– Eu saio por aí e hackeio, volto com o acesso e deixo que os outros enlouqueçam – contou ela.

Seja como for, na maior parte do tempo Kayla não conseguia se conter.

Se estivesse lendo algo on-line, ela costumava começar a brincar com seus parâmetros e scripts de login. Quase sempre encontrava algo errado com eles.

Mesmo assim, trabalhar para q deu a ela uma grande desculpa para ir atrás dos alvos .gov e .mil, e os sites equivalentes dos países do terceiro mundo na África e na América do Sul, os quais eram mais vulneráveis do que os de países mais desenvolvidos. Cada dia representava uma busca por novos alvos e uma nova hackeagem. Kayla nunca encontrou algo tão importante quanto, digamos, o tesouro de e-mails da HBGary para q, mas conseguiu, por exemplo, detectar vulnerabilidades no principal site das Nações Unidas. Em abril de 2011, ela começou a compilar uma lista de "vulnes" das Nações Unidas. Por exemplo, **http://www.un.org.al/subindex.php?faqe=details&id=57**

era um servidor das Nações Unidas vulnerável à injeção de SQL. E na época esta página:

http://www.un.org.al/subindex.php?faqe=details&id=57%27

provocava um erro de SQL, ou seja, Kayla ou qualquer outra pessoa poderia inserir declarações da SQL e usurpar a base de dados. O URL original não tinha %27 no final, mas o simples ato de Kayla acrescentá-lo após testar os parâmetros de scripts php/asp a ajudou a encontrar as mensagens de erro.

Por fim, Kayla obteve acesso a centenas de senhas de empreiteiras governamentais e muitos endereços de e-mail militares. Os últimos foram inúteis, já que as Forças Armadas utilizam um sistema de token para e-mail embutido num chip de computador em um cartão de identidade individual, e é necessário um PIN (número de identificação pessoal) e um certificado no cartão antes de alguém ser capaz de acessar algo.

O trabalho de vasculhar listas de endereços de e-mail e caçar no lixo de outros

hackers quaisquer coisas relacionadas aos governos e aos militares era enfadonho e repetitivo. Mas Kayla atuava com alegria, segundo se comenta. Uma vez por semana, mais ou menos, ela se encontrava no IRC

com q e repassava as informações coletadas via e-mail criptografado, para em seguida aguardar novas instruções. Quando perguntava o que Julian Assange achava do que ela estava fazendo, q informava: ele estava satisfeito com a atuação da garota.

Mas q era um mentiroso de marca maior.

Quase um ano após Kayla começar a agir como voluntária para ajudar o WikiLeaks, outros hackers que já tinham trabalhado com q descobriram que ele era um operador trapaceiro que os havia recrutado sem o conhecimento de Assange. No final de 2011, Assange pediu a q que deixasse a organização. Kayla não foi a única voluntária a procurar informações em prol do que ela imaginava ser o WikiLeaks. O operador trapaceiro também tinha feito outros hackers trabalhar para ele sob falsos pretextos. E além disso, afirma uma fonte, q roubou US$ 60 mil da loja de camisetas do WikiLeaks e transferiu o dinheiro para sua conta pessoal. O

WikiLeaks nunca descobriu o que, afinal, q estava fazendo com as vulnerabilidades encontradas por Kayla e pelos outros hackers, embora fosse possível que as vendesse para outros no submundo do crime. De qualquer modo, parecia que ele não se importava nem um pouco em revelar a corrupção dos governos, e Kayla, mestre em ocultar sua verdadeira identidade até mesmo dos amigos on-line mais íntimos, tinha sido ludibriada.

Nada disso importava mais em fevereiro de 2011, quando Kayla começou a falar com Tflow, Topiary e Sabu na exclusiva sala de bate-papo que os uniria para a histórica investida do domingo do Super Bowl: o ataque contra a HBGary Federal. O maior segredo, desconhecido por Kayla na época, era que Sabu não só a faria mergulhar mais fundo em um mundo de hackeagem estampado na primeira página dos jornais, mas também ficaria assistindo enquanto os dados dela eram passados diretamente ao FBI.

CAPÍTULO 11

O rescaldo

Em 8 de fevereiro de 2011, na terça-feira após o domingo do Super Bowl, Aaron Barr pegava camisas do armário, rapidamente as dobrava e as acondicionava na mala de tamanho médio sobre a cama diante dele. Não era uma sangria desatada, mas Barr tinha de se mudar. Após trabalhar quinze anos no meio militar, ele e sua família já tinham prática nisso.

Fizeram os preparativos com agilidade e silenciosa eficácia. A mulher arrumava uma sacola separada, o silêncio interrompido apenas por uma ocasional pergunta sobre os detalhes da viagem. Somente duas horas antes, Barr tinha subido ao gabinete para se atualizar sobre a inundação de notícias acerca do ataque contra a HBGary e o novo e desastroso ponto de vista pelo qual a mídia interpretava as propostas de Barr para a Hunton & Williams contra o WikiLeaks e Gleen Greenwald.

Saber sobre a hackeagem do Anonymous fora estressante para ele. Mas o banquete da mídia sobre seus e-mails controversos estava tendo um efeito definitivo em sua pressão sanguínea. Barr ansiava por corrigir cada reportagem, mas os advogados o aconselharam a se calar por enquanto.

Tudo que podia fazer era ler e rilhar os dentes. De vez em quando, a curiosidade suplantava a razão, e ele mergulhava nas salas de bate-papo do IRC AnonOps sob pseudônimo para ver o que os Anons comentavam. Ele ainda era motivo de chacota para os centenas de participantes sedentos para ver Barr humilhado de novas maneiras. Houve convocações para que todos os moradores de Washington, D.C., passassem pela casa de Barr para fotografar ou enviassem coisas para ele via correio – ele recebeu uma bengala para deficientes visuais e um caminhão inteiro de caixas vazias.

Também recebeu uma pizza. Duas pessoas tinham batido aleatoriamente em sua porta da frente, e uma havia tentado tirar fotos do interior da casa.

Barr se sentira perturbado, mas simplesmente os mandara embora, calculando que isso não desencadearia grandes consequências. Além do mais, duas horas antes, ele visitara o Reddit, ácido fórum que se tornava cada vez mais popular entre as pessoas que gostavam do 4chan, mas desejavam discussões mais inteligentes. Um usuário postara a entrevista de Barr à *Forbes* da segunda-feira

anterior e, em meio à análise e ao machismo dos 228 comentários resultantes, havia algumas sugestões asquerosas sobre os filhos de Barr. Não passava de mera conversa fiada, mas ele preferiu não arriscar. Afinal de contas, só bastava um lunático para apertar o gatilho. Minutos mais tarde, ele trocou ideias com a esposa e os dois começaram a fazer as malas.

Naquela tarde, a família carregou tudo no carro, os gêmeos pensando que embarcariam numa empolgante viagem rodoviária. A esposa e as crianças dirigiram-se ao sul para ficar na casa de amigos por duas semanas, enquanto Barr saltou a bordo de um avião com destino a Sacramento. Lá, onde ficava a sede da HBGary Inc., ele se dedicaria ao “trabalho de limpeza”

e começaria a ajudar as investigações da polícia.

Nesse meio-tempo, Greg Hoglund, da HBGary Inc., trabalhava no controle dos danos. Entrou em contato com Mark Zwillinger, da empresa jurídica especializada em internet Zwillinger & Genetski. Mais tarde, Mark receberia a colaboração de Jennifer Granick, renomada advogada especializada em internet que já defendera hackers como Kevin Poulsen e trabalhara para a Electronic Freedom Foundation, instituição defensora da liberdade de informação. Depois de conversar com Zwillinger, Hoglund redigiu uma carta aberta aos clientes da HBGary. Ao concluí-la, publicou-a no agora restaurado site da HBGary, referindo-se especificamente à HBGary Inc. e não à empresa irmã administrada por Barr.

“No fim de semana do domingo do Super Bowl, a HBGary Inc. foi alvo de um ataque cibernético. Hackers ilegalmente acessaram as contas de e-mail de dois funcionários da HBGary Inc., mantidas por nosso provedor de serviços em nuvem, utilizando uma senha roubada, e divulgaram os e-mails roubados na internet.”

A carta de Hoglund não esclarecia para quem apontava o dedo – embora isso fosse mudar com o tempo. Parecia sugerir que os invasores da HBGary tinham feito um esforço tremendo para acessar os e-mails da empresa, quando na verdade o processo não fora nem um pouco difícil. Foi uma injeção de SQL, o mais simplório dos ataques. A senha de Ted Vera, satcom31, tinha sido fácil de quebrar. Só Hoglund utilizava uma série aleatória de números e letras não relacionada com nenhuma de suas outras contas na web. O ataque também poderia ter sido pior. Os hackers haviam obtido todos os tipos de dados pessoais

sobre os funcionários da HBGary, desde números de segurança social até endereços residenciais, e fotos dos filhos de Vera após acessarem sua conta no Flickr.

– Foi quando meu modo moralfag se ativou – lembrou-se mais tarde Topiary. Os outros concordaram que nenhuma criança devia ser envolvida e, numa decisão conjunta, não revelaram os números de segurança social. – Ainda bem que não fizemos isso.

Ainda assim, a combinação de mídias sociais, blogs e um dia inteiro de notícias na web e na tevê fez com que os nomes de Aaron Barr e da HBGary se espalhassem por toda a internet no dia seguinte ao domingo do Super Bowl. Os tweets falsos de Topiary na conta de Aaron Barr tinham sido retweetados no IRC Anonymous, conta com dezenas de milhares de seguidores, e agora havia milhares de notícias sobre Barr.

Ele logo descobriu que o ataque tinha sido conduzido principalmente por cinco pessoas.

– Estou surpreso por ser um número tão pequeno – comentou ele em uma entrevista por telefone no começo da manhã de segunda-feira, em Washington, D.C. – Existe um núcleo de pessoas que controla a direção da organização. E essas pessoas são, a meu ver, muito boas. – Com a voz cansada, ele prosseguiu: – Neste exato momento só estou me sentindo meio esgotado por tudo o que aconteceu. Surpresa, raiva, frustração, arrependimento, todos esses tipos de sensações. Sabe, se eu... Talvez eu devesse ter imaginado que esse pessoal ia fazer represálias assim.

Na época ninguém sabia que o conteúdo dos e-mails de Barr suscitaria tanta controvérsia e lhe valeria tanta atenção midiática quanto o próprio ataque, mas Barr já estava preocupado.

– A coisa que mais me preocupa é que eu preferiria que meus e-mails não estivessem expostos, mas não posso impedir isso agora – comentou, acrescentando que entraria em contato com todas as pessoas com quem trocara e-mails para explicar o que estava acontecendo. – No longo prazo, não vai causar qualquer dano significativo à nossa empresa. Isso não me preocupa.

Quanto a isso, Barr estava enganado.

***

Enquanto a invasão ao site da HBGary Federal acontecia, Kayla tinha enviado uma mensagem a Laurelai, a mulher transgênero que dois anos antes fora um soldado chamado Wesley Bailey e agora se tornava um rosto familiar no mundo dos hackers. Kayla disse a Laurelai que estava "dominando" uma empreiteira federal chamada HBGary e indagou se ela queria entrar no AnonOps e dar uma olhada.

Laurelai logo deu um pulinho na rede AnonOps e deparou com centenas de pessoas conversando sobre o que havia acontecido, enquanto a esposa de Greg Hoglund, Penny Leavy, fazia um apelo para os invasores no canal #reporter do AnonOps.

– Caos completo – recordou Laurelai, naquele momento voluntária de um site e blog chamado Crowdleaks, versão evoluída da Operação Leakspin.

Esse era o projeto resultante da Operação Vingança que motivara os Anons a peneirar os cabogramas revelados pelo WikiLeaks. Laurelai não havia apreciado a Operação Vingança, pois, como Kayla, ela acreditava que ataques de DDoS não tinham sentido. Gostava de peneirar dados e se considerava uma corretora de informações. Embarcou no Crowdleaks quando um amigo mútuo sugeriu ao gerente do site, que usava o nickname Lexi e era simpatizante do Anonymous, que Laurelai seria uma excelente administradora de servidor.

– Tem uma grande história fervilhando sobre essa invasão da HBGary – contou Laurelai a Lexi, que respondeu sugerindo que ela própria fizesse a cobertura para o blog. Ela baixou os e-mails de Barr e de Greg e começou a procurar termos como FBI, CIA, NSA e, por fim, WikiLeaks. Uma lista com os e-mails de Barr para a Hunton & Williams apareceu em sua tela.

Enquanto os escrutinava, ela deparou com a apresentação em PowerPoint que Barr havia preparado para a empresa jurídica, na qual sugeria modos de sabotar a credibilidade do WikiLeaks. Laurelai investigou um pouco mais sobre a Hunton & Williams e se deu conta de que a empresa representava o Bank of America. A essa altura, corria solto o boato de que o WikiLeaks tinha, pronto para ser publicado, um verdadeiro tesouro de dados confidenciais vazados do Bank of America. Foi quando caiu a ficha.

– Caramba – Laurelai conta que pensou na época. – O Bank of America está

tentando aniquilar o WikiLeaks.

Sua próxima conclusão foi ainda mais assustadora: Barr nem sequer havia tentado criptografar os e-mails sobre a proposta, nem parecera fazer tanto segredo sobre o assunto. Isso indicava que esse tipo de proposta, embora antiético, não se afastava muito das práticas padrão da indústria. A HBGary Federal não era uma operadora trapaceira; tinha parceiros de peso na indústria, como Palantir e Berico Technologies. Laurelai redigiu um post para o blog do Crowdleaks e colaborou com um jornalista do Tech Herald para relatar que a HBGary estivera trabalhando, junto com uma conceituada empresa jurídica e indiretamente o Bank of America, para prejudicar a imagem do WikiLeaks.

Dois dias após o ataque contra a HBGary, Sabu, Topiary e Kayla ainda não sabiam sobre as estranhas propostas de Barr acerca do WikiLeaks.

Topiary continuava a vasculhar os e-mails à cata de informações interessantes, e a equipe planejava publicá-las num site fácil de navegar que eles queriam chamar de AnonLeaks. Se esse tipo de coisa surtisse efeito, calculavam, o AnonLeaks poderia se tornar um correspondente mais agressivo e proativo do WikiLeaks. Lexi ofereceu o espaço de servidor utilizado pelo Crowdleaks, que utilizava a mesma empresa de hospedagem do WikiLeaks.

Tão logo um Anon chamado Joepie91 acabou de programar o visualizador de e-mails, o grupo começou a ver relatos da imprensa sobre o real conteúdo dos e-mails da HBGary, compilados por jornalistas que já tinham baixado o pacote inteiro via sites torrent.

O grupo decidiu que a mina de e-mails da HBGary seria a primeira publicação do novo site, AnonLeaks.ru. Mas eles não tinham planos para os rumos desse novo site e não sabiam como, ou mesmo se, ele seria organizado.

– Acho que a mídia vai se confundir e pensar que o AnonLeaks é separado do AnonOps e da Operação Vingança – disse Kayla. – Sei lá. Parece que a mídia SEMPRE entende errado quando o assunto é o Anon.

Ainda assim, a equipe passou alguns dias no começo de fevereiro esperando que dezenas de milhares de e-mails da HBGary fossem compilados, e Topiary sugeriu pinçar alguns trechos para publicar como “teasers” no novo site AnonLeaks. Assim, o site em branco não daria a impressão de que a equipe queria ganhar tempo. Clássica estratégia de relações públicas – primeiro espalhar

a notícia para depois desenvolver a história com remessas de informações exclusivas. Entre os teasers estava um vergonhoso e-mail de Barr aos funcionários da empresa no qual ele acabou entregando sua senha, “kibafo33”, de modo que eles pudessem participar de uma teleconferência.

Por fim, na segunda-feira, 14 de fevereiro, após alguns sites de notícias veicularem que um site ao estilo do WikiLeaks chamado AnonLeaks estava surgindo, a equipe lançou o novo visualizador da web com todos os 71.800

e-mails da HBGary. Incluíam 16.906 e-mails de Aaron Barr, mais de 25 mil e-mails dos 2 outros executivos da HBGary, e 27.606 e-mails de Greg Hoglund, diretor executivo da HBGary Inc., incluindo um apaixonado e-mail da mulher dele, Penny, que dizia: – Eu amo você de pijama e meias felpudas.

Agora mais jornalistas começaram a cobrir a história, o que se estendeu por mais de um mês. O ataque tinha sido inescrupuloso, mas os fins eram expor a espionagem, a desinformação e os ataques cibernéticos de um pesquisador de segurança. Dificilmente alguém salientou que as pessoas ligadas ao Anonymous estavam utilizando exatamente as mesmas táticas.

No final de fevereiro de 2011, Barr renunciou ao cargo de diretor executivo da HBGary Federal. Uma semana depois, Hank Johnson, o deputado federal do Partido Democrata, solicitou uma investigação nos contratos envolvendo o governo, as forças armadas e a Agência de Segurança Nacional (NSA) com a HBGary Federal e suas parceiras Palantir e Berico Technologies. Johnson havia lido reportagens sobre o escândalo e mandou seus assessores investigarem.

– Sinto-me na obrigação de encaminhar investigações mais aprofundadas – declarou numa entrevista na época.

Ele não gostava da ideia de que empreiteiros do governo, como a HBGary Federal, adaptassem ferramentas de software originalmente feitas para serem aplicadas no antiterrorismo “à vigilância doméstica e ao marketing de organizações empresariais”. “Espionar nossos próprios cidadãos”, acrescentou ele, “era uma prática deplorável”.

***

– Se algo semelhante a isso aparecer – pediu Laurelai a Kayla após dar uma espiada no caos criado pelo ataque à HBGary –, pode me informar para que eu

possa escrever sobre o assunto?

– Sem dúvida – respondeu Kayla.

Ela manteve a palavra. Dois dias mais tarde, perguntou a Laurelai se ela queria ver onde acontecia uma ação em tempo real, e então a convidou para um novo canal exclusivo de IRC, outra vez no AnonOps, chamado #HQ.

A essa altura, o #InternetFeds tinha sido fechado depois do boato de que um dos trinta e tantos participantes estava vazando os registros dos bate-papos. A nova sala, #HQ, era menor e tinha cerca de seis pessoas, no máximo, em qualquer tempo. Incluía todos os que haviam auxiliado no ataque contra a HBGary Federal.

– Fique por aqui e você vai ver quando alguma coisa estiver prestes a estourar – aconselhou Kayla.

Laurelai empolgou-se por estar no #HQ e imaginou se seria capaz de ajudar a expor outras empresas de segurança de chapéu branco operando conforme suas próprias leis e saindo incólume de atos semelhantes aos que resultavam em prisão para os Anons. Ainda em janeiro, o FBI havia executado quarenta mandados de busca e apreensão nas residências de pessoas suspeitas de participarem dos ataques de DDoS contra o PayPal, partindo de uma lista de mil endereços IP que a empresa havia detectado.

Embora ninguém mais soubesse, Laurelai secretamente registrava tudo que era dito na sala do #HQ, até mesmo quando ela não estava presente.

Tendo passado os últimos dois anos aprendendo a como hackear e fazer engenharia social, ela considerava importante documentar o que as pessoas ao seu redor diziam – futuramente, se necessário, os registros poderiam ser utilizados para corroborar os fatos ou refutá-los. Guardar cópia dos bate-papos era apenas o procedimento padrão de Laurelai. Nesse meio-tempo, ela gradativamente foi se decepcionando com o teor das discussões na sala.

– Eles agiam como um bando de pirralhos endiabrados – lembrou-se mais tarde.

***

– QUE TIMAÇO AQUI – comentou o hacker conhecido como Marduk (também

Q) em 8 de fevereiro, o mesmo dia em que Aaron Barr e sua família fugiram de casa.

– Uma festa Skype do Anon devia ser marcada – disse Topiary.

(Acabou acontecendo, mas apenas com as pessoas do AnonOps que desejavam revelar suas vozes.) Trocaram ideias ocasionais em relação a projetos breves. Marduk, incisivo em seus pontos de vista políticos e aparentemente mais velho do que a maioria, a certa altura solicitou que Kayla escrutinasse as vulnerabilidades nos sites de provedores argelinos de celulares. Ele procurava bases de dados de dezenas de milhares de números de celulares de cidadãos argelinos que pudessem então ser entregues ao partido de oposição daquele país, permitindo a remessa de uma mensagem de texto em massa em 12 de fevereiro. Seria outra tentativa de apoiar o levante democrático no Oriente Médio após os bem-sucedidos ataques na Tunísia e no Egito em janeiro.

Kayla parecia mais empolgada com a publicação dos e-mails de Greg Hoglund.

– Os e-mails de Greg estão prontos. Analisados e tudo mais – disse ela. – Chegou a hora de ferrar com Greg. :3

Esse era um objetivo com o qual todos eles concordavam.

– Quem está lidando com a mídia? – quis saber Kayla.

– Housh e Barrett – respondeu Topiary, referindo-se a Gregg Housh do Chanology, que agora falava com a mídia na condição de especialista sobre o Anonymous, e outro sujeito, chamado Barrett Brown, com quem Topiary faria contato mais próximo nas semanas seguintes.

Por fim, Laurelai se apresentou: – Oi – disse Laurelai ao entrar pela primeira vez na sala naquela manhã.

– E aí – saudou Marduk. – Bem-vinda ao local onde a tempestade de merda começou. – E logo tocou no assunto: – Laurelai, não podemos conectar [a HBGary Federal] com o WikiLeaks pra valer? – indagou ele.

– Eu já conectei – respondeu ela. – Temos material suficiente para tirar o couro deles.

Essa confirmação agradou a Marduk.

– Que empresa estranha – comentou ele. – Na verdade, tenho certeza que é um disfarce do governo.

– O governo utiliza essas empresas para fazer seu trabalho sujo – explicou Laurelai.

O vínculo com o WikiLeaks encontrado por Laurelai convenientemente fazia uma suave transição com o *modus operandi* da Operação Vingança, dando quase a impressão de que o Anonymous havia planejado tudo.

– *Kayla afaga Laurelai :3 Muuito <3 – digitou Kayla com sua alegria de sempre.

– Haha – riu-se Topiary. – Mulheres na web.

– Você ouviu falar que a HBGary foi contratada pelo Bank of America para atacar o WikiLeaks? – informou Kayla a um raro novato na sala de bate-papo do #HQ, orgulhosa por dar a notícia.

– Sério? – indagou o recém-chegado. – Puxa, esta merda é profunda.

– Caiu direto da prancha e afundou – disse Topiary. – E vamos ver a fundura que alcança.

Por fim, o grupo começou a conversar sobre o que iam fazer na sequência. Após sumir por uma semana, Sabu voltou a aparecer on-line, alegando estar com laptop novo e ansioso para debater os próximos ataques.

– Então vamos nos concentrar no AnonLeaks, ou devo começar a procurar alvos? – indagou ele ao grupo.

Embora estivesse exausto – ele havia ficado desperto nos dois últimos dias –, queria fazer progressos e atacar mais empresas de segurança digital.

– A HBGary foi só a ponta do iceberg.

Ofuscando tudo havia uma crescente sensação de desconforto em relação às autoridades e, pior, à ação de espiões e delatores realizada por hackers

antiAnonymous, como The Jester e sua equipe. Os Anons desconfiavam de que Greg Hoglund, da HBGary Inc., tinha entrado no AnonOps com um codinome diferente, tentando rastrear Topiary e Marduk.

Mas um dos críticos mais incisivos do Anonymous naquela ocasião atuava no Twitter sob o nome de usuário @FakeGreggHoush. Ninguém no #HQ sabia a identidade verdadeira por trás dessa conta, criada em 16 de fevereiro, um dia depois que o visualizador dos e-mails da HBGary foi publicado on-line. Essa pessoa tecia constantes observações ácidas e até mesmo ameaçava expor os nomes verdadeiros dos responsáveis pelos ataques contra a HBGary numa data específica: 19 de março. Na verdade, @FakeGreggHoush era Jennifer Emick, a ex-Anon do Chanology que odiava o Gregg Housh verdadeiro. Após romper com o Anonymous, ela havia começado sua própria campanha contra o grupo, com a ajuda de alguns amigos da web.

Outras cinco contas do Twitter logo surgiram, todas igualmente malévolas e todas afirmando publicamente que sabiam a identidade verdadeira de Topiary. As declarações não eram direcionadas apenas a Topiary, mas a toda a comunidade do Anonymous e a todos os seus seguidores. Alguns enviaram tweets a repórteres afirmando que ele liderava o Anonymous.

– É só assediar o Anonymous com a tenacidade suficiente que eles entregam o nome de seus próprios membros – proclamava uma das mensagens. – Quem será o primeiro?

Outra dizia:

– Topiary, estamos aqui fora de seu apartamento, tirando fotos. Vamos lhe enviar algumas, só para você saber com quem está lidando.

Topiary respondeu pedindo impressão de alta qualidade. Ler os tweets era como ser cutucado por um lápis sem ponta. Não machucava, mas cada vez mais perturbava a atenção. O fato era que ninguém que desejasse doxear os hackers da HBGary podia ser mais perigoso que o FBI, especialmente se motivado por uma vendetta pessoal.

– Quantas informações estão disponíveis na web sobre você, Marduk? – quis saber Topiary. – Eu me refiro a coisas antigas, como pequenos dados pessoais inseridos há uma década, digamos.

– Tudo, mas não como Marduk – explicou ele. – E ninguém, absolutamente ninguém no AnonOps sabe quem eu sou.

– Apenas tenha cuidado – aconselhou Sabu. – Não posso me dar ao luxo de perder nenhum de vocês.

Sabu também se preocupava com a própria segurança. Enquanto Topiary poderia dormir sossegado que seu nome real, Jake Davis, não estava em nenhum lugar da web conectado com ele, Sabu sabia que "Hector Monsegur" se pontilhava web afora. Também, a julgar pelas poucas informações que os membros da equipe compartilhavam entre si, Sabu acreditava (corretamente) que ele era o único hacker da HBGary que morava nos Estados Unidos. Isso significava que o FBI quase certamente já estava em seu encalço. Forneceu a Topiary um número no Google Voice e pediu que ele ligasse todos os dias, sem falta. Na primeira vez que Topiary ligou,

notou

um

forte

sotaque

nova-iorquino e

uma

voz

surpreendentemente jovem: – Ei – Sabu respondeu.

– Oi – disse Topiary.

Era a primeira vez que os dois se falavam com voz, e, embora no começo tenha sido estranho, logo estabeleceram uma conversa normal.

Depois, Sabu sempre responderia com uma saudação codificada que homenageava um meme da internet: – Aqui é David Davidson.

Às vezes ele atendia ao telefone enquanto estava ao volante de seu carro; outras vezes em casa, com o som ambiente da tevê e das duas filhas brincando no fundo. Sabu se assegurou que seu número no Google Voice fosse ricocheteado por vários servidores mundo afora antes de enfim chegar ao seu telefone. Mas sua voz sempre soava clara.

Se, por um lado, a dimensão do ataque do Anonymous tornava Sabu paranoico, por outro ele também ficava cada vez mais desconfiado de Laurelai, a mais recente participante do #HQ. Sua irritação aumentou quando descobriu que escrevera um manual para visitantes do AnonOps sobre trabalhar em equipe para executar ataques semelhantes ao realizado contra a HBGary.

– Apague esta porcaria para sempre – disse ele.

Não havia hierarquia, liderança nem cargos definidos no Anonymous e, por isso, necessidade alguma de um manual de operações.

– Com porcarias como esta é que os caras do FBI vão enquadrar os Anons dos Estados Unidos por transgredir a Lei de Combate a Organizações Corruptas e Influenciadas pelo Crime Organizado, ou outras leis contra o crime organizado.

Laurelai começou a argumentar com Sabu sobre como o caso da HBGary havia sido executado, defendendo que os hackers deviam ter destinado tempo para explorar mais informações internas da empresa. Mas Sabu não engolia nenhuma dessas sugestões. Com aguda consciência sobre a reputação e a imagem de seu grupo e sempre temeroso de ser capturado, ele salientou que um documento operacional com diretrizes para atacar outros sites não era diferente das propostas que Aaron Barr havia criado sobre atacar o WikiLeaks e a Câmara do Comércio.

– Vai nos fazer parecer hipócritas – frisou ele. – Quem diabos é Laurelai e por que esse/a homem/mulher/coisa está questionando nosso ataque à HBGary?... Quem a convidou, afinal?

Sabu afirmou que tinha a sensação de que o canal havia sido comprometido e o abandonou.

Ao longo dos dias seguintes, o grupo de ainda cerca de meia dúzia de pessoas tornou-se cada vez mais distraído por teorias sobre seus inimigos, uma facção de pessoas de outra rede de IRC que eles acreditavam estar tramando doxeá-los e

expô-los. Quem era esse tal de @FakeGreggHoush no Twitter? Topiary descobriu o verdadeiro Gregg Housh no IRC e perguntou se ele sabia. Housh sugeriu que era uma mulher da época do Projeto Chanology (três anos antes – quase uma vida em termos de internet) chamada Jennifer Emick.

Topiary nunca tinha ouvido falar nesse nome, mas compôs um documento mencionando Jennifer Emick e alguns supostos colaboradores e mostrou aos outros no #HQ. Quando Laurelai deu uma olhada no documento, repentinamente se mostrou nervosa. Todas as pessoas da lista a tinham apoiado no site Scientology Exposed. E, embora ela e Emick tivessem brigado e se separado, elas ainda conversavam de vez em quando.

Laurelai acreditava que Emick estava sendo instruída por alguém, provavelmente Housh. Recentemente, Emick havia contado em particular a Laurelai que Housh estava tentando mexer os pauzinhos junto ao AnonOps, com o objetivo de criar um caos na rede. Na pior das hipóteses, havia o dedo de Housh nisso, tentando incitar o AnonOps a agir como seu exército pessoal contra Emick e gerenciar as coisas como ele fizera no #marblecake, concluiu Laurelai. Ela não tinha nem ideia que os planos verdadeiros de Emick envolviam rastrear as pessoas por trás do Anonymous e desmascará-las publicamente.

– Topiary, eles não estão por trás disso – ponderou ela. – Algo bem mais sinistro está acontecendo. – Ela invocou lembranças do Chanology e disparou uma pergunta incômoda. – Alguém sabe o que “marblecake”

significa?

Silêncio na sala. Ninguém sabia. Uma pessoa tinha vagamente escutado o nome e o associado com brigas mesquinhas em fóruns, algo relacionado com uma geração prévia do Anonymous. Laurelai continuou: – Jen é um pouco estranha, mas é inofensiva.

Enquanto os demais silenciosamente reviravam os olhos, Laurelai começou a formular uma teoria na qual, com o tempo, começou a acreditar plenamente: Gregg tentava atingí-la novamente por vingança em relação ao Chanology, e fazia isso envolvendo Jennifer Emick. Ou seja, Emick corria risco iminente de ser atacada pelo Anon. Laurelai passou a acreditar nessa teoria até o tutano dos ossos. Ela acabara de expor a conspiração de Barr contra o WikiLeaks, não é mesmo? Mas também passava doze horas por dia on-line enquanto a mãe

cuidava de seus dois filhos. A internet estava se tornando sua vida, e era difícil abrir mão disso.

Laurelai entrou em contato com Emick e contou tudo sobre as acusações e sobre o que Housh andava tramando, e disse que ela estava num canal privado chamado #HQ com os hackers da HBGary. Emick, demonstrando surpresa, negou qualquer espécie de trama.

– Não me importo com o que está acontecendo no AnonOps – falou Emick a Laurelai pelo telefone. – Não tenho ideia do que está acontecendo.

Laurelai levou essas informações aos demais no #HQ como prova de que Emick não era sabotadora e de que todos os boatos criados por Housh tinham o objetivo de “me atingir”. Marduk e Topiary deram ouvidos, mas estavam precavidos quanto às teorias de conspiração. Elas eram ruidosas.

– Na verdade essa merda não afeta nada – concluiu Topiary.

Mas não havia acabado. De volta ao Twitter, a conta @FakeGreggHoush começou a alfinetar Laurelai, acusando-a de fazer parte de um grupo de pessoas que havia trabalhado com Housh na antiga sala de bate-papo marblecake (afirmação inverídica). Foi a gota d’água. Laurelai respondeu pelo Twitter que dispunha de registros provando que ela não conversava com Gregg Housh e que ela podia fornecê-los, em particular, em troca de novas informações sobre Housh que a ajudassem a montar o quebra-cabeça da conspiração e livrar a barra de Emick.

– A única coisa que me importa é proteger Jen e os amigos dela – disse Laurelai. A conta do Twitter @FakeGreggHoush concordou.

Laurelai analisou, nos registros de bate-papo que ela diligentemente guardava, tudo que havia sido dito no #HQ nos últimos doze dias (de 8 a 19

de fevereiro). Ingenuamente, ela acreditava que se mostrasse isso a seja lá quem fosse @FakeGreggHoush, limparia a barra de Emick e ninguém precisaria ficar sabendo que ela havia vazado o conteúdo das conversas.

Laurelai copiou o registro inteiro das conversas, em torno de 245 páginas, e postou no aplicativo da web Pastebin. Então enviou uma mensagem direta pelo Twitter a @FakeGreggHoush, dizendo para a pessoa dar uma olhada nos

conteúdos. Poucos minutos depois, Emick tinha copiado as conversas, e Laurelai, ainda de boa-fé, havia apagado o arquivo Pastebin.

– Caramba – pensou Emick enquanto fitava a tela.

Rapidamente começou a vasculhar o enorme registro das conversas, um prêmio que lhe fora entregue de bandeja. Bizarramente, não havia nada que realmente envolvesse Gregg Housh, mas muita coisa que envolvia Sabu, Kayla e Topiary no ataque contra a HBGary Federal. Ela começou a ler o imenso material com mais atenção.

Os embustes de Emick diante de Laurelai, assim como seu *alter ego* personificado em @FakeGreggHoush, consistiam em táticas com o objetivo de desvendar as pessoas reais por trás do Anonymous. Após o ataque contra a HBGary, Emick havia percebido que a melhor maneira de derrotar o Anonymous seria simplesmente mostrar que as pessoas no grupo não tinham nada de anônimas. Para isso, precisava descobrir seus nomes verdadeiros. E, graças à Laurelai, ela estava prestes a descobrir o nome real de Sabu.

PARTE 2

Fama

CAPÍTULO 12

Encontrando uma voz

Em meados de fevereiro de 2011, enquanto Jennifer Emick vasculhava os registros do #HQ entregues por Laurelai, Topiary desfrutava uma inédita popularidade na rede de bate-papo AnonOps. Agora as pessoas ali sabiam que ele estivera envolvido no ataque contra a HBGary e que havia sequestrado a conta do Twitter de Aaron Barr. Para os Anons, esse tinha sido um ataque épico, e Topiary era o Anon que sabia tornar a coisa divertida, ou "cheia de lulz". Agora, sempre que Jake entrava no AnonOps como Topiary, recebia meia dúzia de mensagens privadas convidando-o para participar de uma operação, oferecendo-lhe o registro das atividades do computador do diretor executivo de uma empresa de segurança francesa, solicitando que ele interviesse numa disputa pessoal ou pedindo-lhe conselhos sobre publicidade.

A mesma coisa parecia acontecer com o próprio Anonymous. Ao longo de fevereiro, os canais públicos do AnonOps foram inundados com solicitações de usuários de fora da rede, sugerindo certos alvos a quem eles consideravam se tratar de um grupo organizado de hackers. Os sites sugeridos incluíam outras empresas de segurança digital, indivíduos, sites governamentais da Líbia, Bahrein e Irã, e, naturalmente, o Facebook.

Nenhuma das sugestões foi aceita.

A maioria dos ataques vinha de discussões ocorridas diretamente no IRC AnonOps, em especial entre operadores como Owen e Ryan. Não havia cronograma, nenhuma etapa sendo seguida. Em geral, as pessoas começavam a planejar uma operação, topavam com um obstáculo e a engavetavam. Tudo parecia se sobrepor. O próprio Topiary raramente terminava um projeto antes de iniciar outro – num minuto escrevia mensagens de deface, no outro voltava a ler os e-mails de Aaron Barr.

Após o recente convite para entrar no #InternetFeds, Topiary passou a receber dos operadores um status extraordinariamente elevado nos canais de bate-papo. Às vezes, ele passava um dia inteiro borboleteando entre as salas, fazendo piadas, depois acrescentando um conselho sério sobre uma operação colateral antes de ir para a cama, sentindo-se realizado. Era melhor do que a emoção de fazer trotes telefônicos na época do 4chan, e diferente de tudo que já havia experimentado no mundo real, sem falar da escola. Os operadores e outros

hackers confirmavam que ele tinha fama de “charmoso” e “engraçado”. Ser um escritor talentoso era útil num mundo em que as pessoas se comunicavam pelo texto, e o estilo de Topiary tinha nuances de impassível maturidade que fazia a cabeça dos Anons.

Topiary raramente interagia com gente do mundo real. Havia a ocasional visita à família, uma ida ao mercado ou, de vez em quando, um encontro com velhos amigos de jogos on-line, ali mesmo na cidade onde morava. Agora, talvez 90% de toda a sua interação social aconteciam on-line. E isso encaixava como uma luva em sua personalidade. Gostava de entreter as pessoas, e estava prestes a pregar a maior peça de sua vida.

***

A partir do começo de janeiro, muitos sectários do Anonymous tinham sugerido ataques à Igreja Batista Westboro, controverso grupo religioso sediado no Kansas, conhecido por fazer piquetes nos funerais de soldados com gigantescos cartazes alardeando DEUS ODEIA BICHAS. A Westboro defendia que Deus estava punindo os EUA porque o país “permitia” a homossexualidade. A igreja parecia um alvo óbvio ao Anonymous, mesmo se estivesse praticando seu direito de se expressar de modo livre e, supostamente, a liberdade de expressão fosse uma das bandeiras do Anonymous.

Mas logo alguém chamou os demais à luta. Em 18 de fevereiro, sem aviso prévio, uma carta pública foi postada no AnonNews.org (qualquer um podia postar no site) lançando uma ameaça com o floreio de uma linguagem desnecessariamente formal.

– Sempre consideramos vocês e sua laia uma reunião de sociopatas desagradáveis e chauvinistas maníacos – dizia a mensagem endereçada à Igreja Westboro. – O Anonymous não pode mais tolerar esse comportamento.

Se a mensagem fosse ignorada, a Westboro iria “conhecer o braço cruel e vingativo do Anonymous”. A carta terminava com o slogan “Somos Anonymous, Somos Legião”. No primeiro dia, ninguém notou a carta. No dia seguinte, porém, um membro do #Philosoraptors indagou se alguém sabia sua origem. Ninguém sabia. Uma ameaça vazia que, se não fosse cumprida, comprometeria a imagem do Anonymous diante da mídia, fazendo o grupo soar fraco se ela noticiasse o caso. Um dos operadores realizou uma busca em todos

os canais de bate--papo da rede e descobriu uma sala secreta, que exigia convites para entrar, chamada #OpWestboro. Parecia que uma dupla de trolls entediados tentava atrair a atenção da imprensa.

Para a decepção de todos, os trolls conseguiram. O ataque contra a HBGary tinha empolgado tanto os repórteres de vários meios de comunicação que qualquer insinuação de ameaça do Anonymous subitamente recebia uma aura de credibilidade. Vários órgãos de comunicação, inclusive o site tecnológico Mashable, noticiaram a mais recente "ameaça" do Anonymous, atualizando seus artigos no mesmo dia com uma alegre resposta pública da Westboro. Megan Phelps-Roper, a neta de cabelos encaracolados do fundador da igreja, Fred Phelps, rapidamente enviou um tweet: – Obrigada, Anonymous! Seus esforços para calar a palavra de Deus apenas servem para divulgá-la ainda mais... Venham, seus covardes.

A igreja também postou um folheto oficial em seu site numa fonte gritante em negrito com a manchete: "Venham!" e chamando o Anonymous de "hackers covardes chorões", "uma poça de nerds sardentos", acrescentando que "nada vai calar estas palavras – nunca". Claramente festejavam a perspectiva de uma luta acirrada.

Cerca de cinco redatores do #Philosoraptors se uniram às pressas para escrever um novo comunicado de imprensa, com ares de oficial, para apagar o incêndio.

– Estão falando muito numa tal carta que supostamente lhes enviamos esta manhã – dizia o comunicado. – O problema é que estamos meio grogues e não nos lembramos de ter enviado carta alguma.

Vários noticiários rapidamente o publicaram.

– É um embuste – anunciou o PCWorld.com. – O Anonymous não ameaçou a Igreja Batista Westboro.

Agora as pessoas começavam a ficar confusas. O Anonymous ia ou não atacar a Igreja Batista Westboro? Isso perturbou Topiary. Não lhe agradava essa confusão pública sobre o que o Anonymous planejava fazer. Ele já tinha visto situação parecida em dezembro de 2010, quando o Anonymous declarou que ia derrubar o Amazon.com e não o fez devido ao arranca-rabo com os botmasters Civil e Switch. Ele não queria que a organização desse a impressão de novo fracasso.

Topiary entrou no #InternetFeds e observou que um dos participantes trazia uma notícia interessante. A primeira e falsa ameaça contra a Westboro tinha atiçado a sua curiosidade de bisbilhotar a rede de computadores da igreja, e ele descobrira uma vulnerabilidade. Dois outros hackers haviam descoberto um modo de explorar a brecha de segurança. Se quisessem, eles poderiam derrubar vários sites importantes da Westboro, inclusive o principal, GodHatesFags.com, e também desfigurá-los.

– Podemos fazer isso agora sem problemas – contaram eles.

As pessoas que estavam no #InternetFeds (em torno de doze), inclusive Tflow e Evilworks, operador do AnonOps, começaram a conversar sobre um ataque à Westboro, uma animando a outra com a perspectiva de mais um ataque espetacular. Liberdade de expressão à parte, o ataque ao menos acabaria com a confusão.

– E aí, o que a gente faz agora? – indagou alguém.

O pessoal do #InternetFeds era craque em hackeagem, mas péssimo em publicidade. Foi quando Topiary deu sua opinião: – A gente deve tornar isso um acontecimento, não apenas uma desfiguração de página corriqueira – disse ele. E teve uma ideia. – Vou conferir uma coisa. Já volto.

Topiary queria confirmar algo antes de dar esperanças ao grupo, mas, durante todo o papo sobre a Westboro, lembrou-se de comentários sobre um vídeo no YouTube de um recente programa em que a porta-voz da Westboro, Shirley Phelps, comentava a suposta ameaça do Anonymous.

Que tal se ele mesmo participasse do programa e confrontasse Shirley?

***

The David Pakman Show era um programa de atualidades gravado na faculdade comunitária Greenfield, em Massachusetts, simultaneamente para rádio e tevê. Bem iluminado, o estúdio contava com múltiplas câmeras. Aos 27 anos de idade, Pakman era um dos mais jovens anfitriões de programa de rádio dos EUA; ele havia entrado no negócio ao começar seu próprio programa de entrevistas na faculdade. Ao longo dos seis anos seguintes, Pakman convidara pessoas da Igreja Batista Westboro para participar do programa umas seis vezes. Sabia que temas controversos atraíam ouvintes, seja um pastor que desejava queimar o

Alcorão em 11 de Setembro, seja um ativista antigays, ex-capelão da Marinha, que alegava ter feito um exorcismo lésbico. Pakman justificava o tempo concedido a essas pessoas porque considerava certo expor o que eles pregavam.

A Igreja Batista Westboro, fundada por Fred Phelps, ex--advogado especializado em direito civil, contava com cerca de 85 membros. Durante anos, Phelps liderou a família com mão de ferro. O único filho que se afastou, Nate, declarou que o pregador abusava de seus filhos, embora em sua maioria eles tivessem permanecido pupilos do pai. Shirley Phelps (filha de Fred) tornou-se uma espécie de convidada frequente no programa de Pakman, sempre que a Westboro fazia manifestações no funeral de um soldado ou outra atividade igualmente desagradável. Dizia que ele ia acabar no inferno por ser judeu e o povo judeu ter matado Jesus. O

apresentador se divertia com isso.

– Esses medrosos de meia pataca vão ver o que é bom para tosse – disse Shirley no mais recente programa sobre a "ameaça" do Anonymous contra a Westboro; ela sorria com o rosto sem maquiagem. – E vão retinir os tímpanos de quem escuta. Eles cometeram um erro terrível.

Depois do programa, quando Pakman recebeu uma mensagem de Topiary pelo Twitter declarando que ele pertencia ao Anonymous e desejava se manifestar, Pakman mostrou-se cético. Então outra ideia lhe veio: "Essa pode ser uma entrevista muito interessante".

Trazer dois grupos controversos ao mesmo programa parecia uma oportunidade muito boa para ser desperdiçada.

Topiary enviou um e-mail a Pakman contando que o Anonymous tinha acesso aos sites da Westboro e insinuando que a hackeagem podia acontecer durante o programa. De acordo com Topiary, Pakman respondeu de modo cifrado: – Se algo desse tipo acontecer, será obrigação minha imediatamente chamar atenção para o caso.

Topiary concluiu que Pakman se interessara bastante, já que ele mais tarde voltou ao assunto, perguntando se o "evento" estava confirmado.

Pakman, que mais tarde negou que tivesse alguma noção prévia de que o Anonymous iria hackear os sites da Westboro durante a transmissão do

programa, tomou providências para que Topiary viesse ao programa no dia seguinte. Ele se asseguraria, acrescentou, de que o programa tivesse maciça atenção on-line, postando links em fóruns populares como Reddit e Digg.

– Bom trabalho – alguém no #InternetFeds parabenizou quando Topiary voltou à sala de bate-papo e informou que o grupo em breve marcaria presença no programa de Pakman, tendo a oportunidade de fazer uma hackeagem em tempo real e desfigurar os sites da Westboro.

Perguntou a todos se alguém mais queria fazer a ligação telefônica ao vivo, pois ele já tinha emprestado sua voz na rede de tevê Russia Today. Mas as pessoas queriam ouvir Topiary *versus* Shirley. Muitos no AnonOps o consideravam talentoso para falar em público, embora seu discurso pudesse se deteriorar em frases tartamudeadas com o que ele imaginava ser um pateta sotaque britânico.

Conformado com seu papel no desafio verbal, Topiary começou a escrever uma mensagem de deface para o site da Westboro. Súbito percebeu algo bizarro: a maioria dos principais sites da Westboro já estava fora do ar. Não desfigurada – apenas off-line. Parecia que alguém havia percebido a agitação ao redor da falsa ameaça do Anonymous e derrubado os sites por conta própria. Topiary se deu conta de que era The Jester.

Então, foi até a sala de bate-papo de Jester, abordou o hacktivista e indagou se ele podia deixar os sites voltarem pelo menos durante umas duas horas.

Ele não forneceu nenhum horário a Jester nem comentou que era para um programa de rádio, para evitar que alguém da sua equipe tentasse sabotar a operação. Não entrou em detalhes.

Jester confirmou seu envolvimento, mas recusou atender ao pedido, acrescentando misteriosamente estar “sob pressão extrema para mantê-los fora do ar”. Um pouco desconcertado e irritado, Topiary desistiu e voltou ao #InternetFeds. Eles teriam de se contentar com um ataque contra uma página da web menos importante.

Arregaçou as mangas e começou a redigir uma mensagem de deface no programa simples Notepad++, da mesma forma que fizera todas as dez mensagens de deface para o Anonymous nos últimos trinta e poucos dias.

Após escrever a declaração, colou-a numa caixa de texto no Pastehtml e

escreveu o código HTML. Todas as páginas de desfiguração consistiam em textos simples sobre fundo branco. Topiary havia tentado leiautes mais complicados, mas eles nunca obtinham o mesmo impacto do simples preto e branco, um contraste completo em relação aos sites de projeto incrementado que supostamente deviam estar ali. Em geral, ele explorava as diferentes salas de bate-papo do IRC AnonOps e tomava nota de quaisquer comentários filosóficos que as pessoas faziam sobre o Anonymous e o mundo em geral; depois, tentava incorporá-los em suas mensagens. Os Anons já começavam a se dar conta de que as opiniões deles tinham importância, à medida que jornalistas citavam comentários aleatórios feitos nas salas de bate-papo do AnonOps.

Em parte, Topiary fazia isso para seu próprio bem. Durante o caso Westboro e especialmente após o programa de Pakman, seu apelido se tornara mais conhecido.

– Eu não queria toda essa atenção – declarou ele mais tarde.

No fundo, ele não queria que sua "voz" em texto e áudio se tornasse familiar ao público e às autoridades. Quando escrevia um comunicado de imprensa, dava-se ao trabalho de postar no Pirate Pad e implorava que outros sectários e Philosoraptors o editassem.

– Eu deixava lá por dez minutos e ninguém mexia – contou ele. – As pessoas só diziam: está ótimo. Eu não sabia se eles estavam nervosos ou se não queriam dizer que no texto havia alguns erros.

No dia seguinte, pouco antes do programa, Topiary perguntou a um amigo do AnonOps como ele devia tratar a porta-voz da Batista Westboro.

– Deixa que ela coloque os pés pelas mãos – respondeu o amigo. – Você não precisa se esforçar para ela parecer má. Ela mesma vai se encarregar disso.

Topiary então passou alguns minutos ouvindo música para tentar acalmar os nervos, uma canção do suave artista techno World's End Girlfriend, o que sempre o deixava mais relaxado. Trinta segundos antes de o programa começar, Pakman ligou para Topiary, que escutou Shirley Phelps-Roper ao fundo, resmungando num arrastado sotaque sulista sobre o posicionamento das câmeras.

Pakman imediatamente reconheceu a voz de Topiary das entrevistas que ele

concedera ao Russia Today e do programa Tom Hartman. Em cima da hora, soltou um suspiro de alívio por estar falando com um autêntico porta-voz do Anonymous.

Sem demora, Phelps-Roper também entrou na linha, e o vídeo mostrou três imagens: Pakman num blazer preto com seu microfone; Shirley com impressora e estante de livros ao fundo, o cabelo preso num rabo de cavalo e o olhar incandescente; e a imagem de um tubarão gigantesco sendo atacado por Batman brandindo um sabre de luz – esse era Topiary. Sempre que Topiary falava, sua imagem brilhava em azul.

– Bem, hoje temos todo mundo aqui – começou Pakman, apresentando Topiary como uma "fonte interna do Anonymous" e depois se referindo a ele apenas como "Anonymous".

– O Anonymous emitiu uma ameaça à Igreja Batista Westboro? – quis saber ele.

– Não, ninguém falou isso, ahn...

A voz grave de barítono de Topiary quase rosnou nas ondas do rádio.

Ele tinha um sotaque incomum – uma alegre cadência escocesa mesclada a uma metálica pitada nórdica. Repousou o laptop na mesa e desviou o olhar da tela. Todos os trotes telefônicos tinham sido assim – ele concentrava o olhar em simples pontos focais, como o teto ou a lombada de um livro, ou janela afora.

– Shirley, você acredita que o Anonymous não pode prejudicar os sites da Westboro de algum modo? – indagou Pakman.

– Ninguém pode calar essas palavras que estão sendo... ESBRAVEJADAS

do Monte Zion! – bradou ela. – Quer dizer, estou falando com um carinha que é judeu.

David relanceou o olhar a seu produtor e abriu um sorriso.

– Ok – de repente Pakman ficou sério. – Então, Anonymous, pode explicar isso? Quer dizer, os sites de Shirley não estão todos fora do ar neste exato instante?

Shirley não conteve uma risada de surpresa. Topiary respondeu: – Sim, neste

exato instante. Hum... GodHatesFags.com está fora do ar, YourPastorIsAWhore.com está fora do ar.

Listou vários outros sites de nomes contundentes e explicou, desanimado, que o crédito devia ser dado a The Jester, e não tecnicamente ao Anonymous.

– Dá na mesma! – gritou Phelps-Roper, interrompendo Topiary por um instante. – Todos vocês são um bando de criminosos e brutamontes... E

TODOS vocês vão enfrentar uma destruição iminente.

– Anonymous – arriscou-se David –, isso está o irritando a ponto de realmente tomar alguma medida?

– Por favor, tome – brincou Phelps-Roper, com tom sério na voz.

– Bem... – disse Topiary.

– Espere um pouco, Shirley – falou Pakman.

– Nossa resposta à carta dos “hackers chorões” foi madura – disse Topiary. – Nossa resposta foi que não queremos entrar em guerra contra vocês.

Os olhos de Phelps-Roper se arregalaram.

– Você acabou de chamar criminosos e brutamontes de... MADUROS?

Topiary empacou e decidiu mudar de abordagem.

– Você afirma que a internet foi inventada apenas para que a Igreja Batista Westboro divulgasse sua mensagem, certo? – indagou ele.

– Exatamente – respondeu ela.

– Bem, então como é que Deus permitiu sites de namoro gay?

– Tsc, tsc. Bobagem – riu-se Phelps. – Isso se chama seu terreno de provas.

– Vou para o inferno?

Súbito, Phelps-Roper soou preocupada.

– Bem, querido, só sei o que estou escutando porque você é – ela ergueu as sobrancelhas – Anonymous, e vou lhe dizer que você me parece um cara destinado a ir para o inferno.

– Bem, em minha vida já cometi 9 mil pecados – falou Topiary. – Então...

– AH! E você anota! Tem uma planilha?

– Sim, mais de 9 mil pecados. Eu anoto.

Pakman sorria. Topiary mirou de relance para o seu laptop e nos próximos trinta segundos observou uma janela no IRC AnonOps, onde um punhado de gente assistia a uma transmissão ao vivo do programa no site de Pakman. Eles riam. Pakman parecia estar esperando que Phelps-Roper se irritasse e dissesse que ninguém poderia hackear o site da Westboro, antes de retomar o tópico da hackeagem com Topiary.

Phelps-Roper explicava por que ter orgulho de pecar não “se enquadrava como arrependimento... É claro que você vai para o inferno”.

– Humm... – suspirou Topiary. – A internet é assunto sério.

– Deixe-me retomar o tópico central – atalhou Pakman. – Existe um próximo passo? O Anonymous pretende provar que pode realmente manipular a rede de sites da Igreja Batista Westboro? O que podemos esperar na sequência, Anonymous?

Se algo ia acontecer, deveria ser agora. Phelps-Roper tentou se interpor de novo, mas Topiary foi em frente: – Na verdade – disse ele estalando os lábios –, estou trabalhando nisso neste exato instante.

Topiary fixou o olhar na tela de seu laptop, clicou numa aba de suas janelas de IRC, entrou na sala particular #over9000 e rapidamente digitou *gogogo*, o sinal combinado. Tflow estava pronto e à espera com o arquivo HTML de Topiary.

O sarcasmo de Phelps-Roper se intensificou.

– Ele está trabalhando nisso NESTE EXATO INSTANTE! Oh yay! – gritou ela. Súbito, fechou a cara. – Ei, olha só, mocinhas...

– Espere um pouco; vamos ver o que o Anonymous tem a dizer, Shirley – pediu Pakman.

– Não, não – disse Shirley.

– Tenho algo interessante, uma surpresa para você, Shirley – anunciou Topiary.

– Espere um pouco – pediu ela. – Espere só um minuto! – As outras vozes se calaram. – Foi isso que você conseguiu. Atraiu os olhares do mundo todo. Tudo que estamos fazendo é publicar uma mensagem... Uma ENORME explosão global da palavra de Deus.

Os outros permaneceram em silêncio.

Sem hackeagem ao vivo, o segmento se aproximava do final, e Pakman precisava redirecionar a palavra a Topiary.

– Anonymous, vá em frente.

– Eu só ia dizer na hora em que Shirley começou a tagarelar sua pregação religiosa que na verdade acabei de fazer um serviço, e acho que, se você conferir a página de downloads ponto com da Igreja Batista Westboro, vai encontrar uma bonita mensagem do Anonymous.

Phelps-Roper permaneceu fleumática.

– Legal – disse ela, revirando os olhos.

– Ponto com, não é? – indagou Pakman.

A equipe de Pakman já sabia o exato URL do site que seria hackeado, pois Topiary tinha enviado um e-mail de antemão.

– Por isso a produção dele achou tão rápido – contou mais tarde Topiary.

– Sim, a gente publicou uma bonita mensagem enquanto Shirley dava seu sermão. Exatamente enquanto fazíamos esta entrevista.

Pakman deu uma risadinha de aparente espanto. Olhou ao produtor e apontou algo fora da tela.

– Sim, aguentamos ao máximo! Respondemos com maturidade, dizendo que não queríamos confrontos. Então Shirley veio à rádio e começou, bem...

pensa que vou para o inferno, por isso lhe fornecemos algo para que dê uma olhada.

– Não desligue – pediu Pakman, fazendo novo aceno para alguma coisa fora da tela. – Minha produção confirma que uma mensagem foi postada e aparenta ser do Anonymous.

Súbito, uma captura de tela com a mensagem previamente escrita por Topiary apareceu na tevê: um simples fundo branco com o logotipo do Anonymous (homem sem cabeça trajando um terno) na parte superior substituía o que supostamente seria a principal página da Igreja Batista Westboro para downloads.

– Anonymous, você se responsabiliza por isto? – indagou Pakman novamente.

– Sim – disse Topiary. – Acabamos de fazer neste exato momento.

– Isso é tão especial – atalhou subitamente Phelps-Roper. – Tão especial.

Topiary tentou explicar: – Você falou que a gente não podia afetar seus sites e acabamos de fazê-

lo – disse ele. – Quer dizer...

– Eu disse – retorquiu Phelps – que você não pode nos calar. Obrigada.

Esse foi o fim do segmento.

Não foi a derrocada da Westboro que Topiary tinha almejado, mas estava aliviado, pois evitou um fiasco. Com certeza Phelps-Roper tinha ficado surpresa pela desfiguração do site ao vivo, mas anos refutando os argumentos mais sensatos lhe deram uma habilidade para urdir comentários ácidos embebidos de sarcasmo. Era um alvo difícil de trollar.

– Já topei com alguns trolls e antitrolls asquerosos na minha época, mas Shirley parecia ter as qualidades de uma supertroll new-wave. Isso me pegou de surpresa – avaliou Topiary.

Até mesmo os comentários mais fracos de Shirley tinham um fundo de verdade. No fim das contas, a principal arma do Anonymous não era assim tão destrutiva. Eles estavam desfigurando uma página pouco conhecida da rede da igreja – "tão especial" –, com o anticlímax ainda mais enfraquecido pela confusa campanha colateral do The Jester.

Nada disso teve importância nos primeiros dias após o que veio ser chamado a hackeagem ao vivo da Westboro, pois o enfrentamento entre Topiary e Shirley Phelps-Roper rapidamente se tornou um dos vídeos mais populares do YouTube daquela semana. Topiary acompanhou os números subirem todos os dias, inicialmente com fascinação empolgada, depois com certo pavor. Primeiro alcançou a marca dos 10 mil, depois 200 mil, e, após cinco dias, mais de 1 milhão de pessoas havia assistido ao vídeo.

A essa altura, Topiary já tinha aprendido que existia uma tênue linha entre o sucesso e o fracasso quando o assunto era o lado público do Anonymous.

– Precisava ter humor, um ou dois memes, mas definitivamente não muitos – lembrou-se ele mais tarde. – Precisava ter algo inexplicável, uma espécie de que-diabos-estou-vendo.jpg, por isso o Batman atacando um tubarão com um sabre de luz.

Por fim, precisava ter algo descaradamente óbvio para pegar no pé: Shirley.

– Ela é mandona como a senhora dos gatos dos Simpsons, com a diferença de que fala sobre o Monte Zion e soldados mortos. – Era difícil para Topiary não parecer o mocinho ao falar com ela. – Fiquei tão, tão feliz por não ter visto aquele olhar insano – acrescentou ele. – A primeira vez que vi o rosto dela foi ao clicar no vídeo do YouTube. Que coisa.

No entanto, um pensamento mais sério passara por sua cabeça na época: "Mais de 1 milhão de pessoas escutaram minha voz". Junto com o orgulho veio uma terrível inquietude – se uma só pessoa que assistisse ao vídeo o conhecesse pessoalmente, sua identidade seria revelada. Não tinha utilizado alteração de voz nem mudara o sotaque, porque queria soar verdadeiro. Não conseguia decidir se falar no programa fora um equívoco tolo ou seu ato mais audaz em todos os tempos.

Ninguém do Anonymous entrou em contato com Pakman após o programa, mas houve uma inundação de feedback de ouvintes, com os pontos de vista divididos

entre o quão maravilhoso tinha sido ver a Igreja Batista Westboro ser derrubada e outros frisando que, seja qual fosse o alvo, o Anonymous havia apenas cometido um crime. Pakman não levou o assunto a sério.

– Considerei a coisa toda uma espécie de paródia em alto nível – recordou ele.

– Relembrando tudo que aconteceu no Anonymous e no LulzSec, tem muita coisa de que me arrependo em ter me envolvido – disse mais tarde Topiary. – Mas o ataque contra a Igreja Batista Westboro, bem... será *orgulhoso* a palavra certa? Honrado. Sentime honrado por ter participado.

Parecia que a Westboro e o Anonymous tinham certas semelhanças.

Uma chave para a insondável capacidade da Westboro de sobreviver e se manter era seu isolamento. Os membros conheciam seu grupo exclusivo como "nós contra o mundo". Suas manifestações em funerais não tinham o real objetivo de salvar almas ou divulgar a palavra de Deus, mas de provocar a raiva e o ódio nos outros – exercício de autosserviço para abastecer seu próprio senso de retidão. Essa cultura do ódio era tamanha que só seus participantes de longa data conseguiam realmente entender.

Aceitação profunda mesclada com dessensibilização quanto à sua própria e cruel trollagem. Quando o assunto era motivação, o Anonymous muitas vezes agia igual.

O Projeto Chanology e a Operação Vingança tinham mostrado que o Anonymous, como grupo, podia assumir características repulsivas, mas a hackeagem ao vivo da Westboro com Topiary indicou o caminho a seguir: menor e mais extremo.

Kayla havia desferido seu ataque vingativo contra o Gawker; Sabu havia provocado uma reviravolta revolucionária na Tunísia; Topiary tinha experimentado a emoção de uma apresentação ao vivo. O Anonymous talvez fosse um movimento capaz de mudar o mundo, mas também existia para o bel-prazer de seus membros. Dava-lhes algo a fazer, e assim se sentiam úteis, e mais, embora ninguém fosse admitir, possibilitava-lhes executar anseios que pareciam justificados e necessários. O Gawker e a HBGary tinham mostrado que o Anonymous podia revelar sua face mais destrutiva quando se vingava e quando um grupo pequeno, mas focado, comandava as operações. Mas, apenas quando um coringa e comunicador público como Topiary foi acrescentado à mistura, o

grupo alcançou as qualidades de um time cada vez mais poderoso: Sabu com sua paixão, Kayla com sua perícia e Topiary com sua língua ferina.

CAPÍTULO 13

Conspiração (que nos une) Poucos dias após a hackeagem ao vivo da Westboro, Topiary não conseguia deixar de se preocupar com o mais de um milhão de pessoas que agora tinham escutado sua voz real. Um modo de se distrair dessas preocupações era escrutinar mais e-mails de Aaron Barr. Com o olhar fixo no material que aparecia na tela de seu laptop Dell, quanto mais tempo dedicava à missão, mais encontrava indícios de uma conspiração suja e sombria. No final de fevereiro, enquanto Jennifer Emick criava suas próprias teorias sobre quem era o Anonymous, Topiary mergulhava em teorias que extrapolavam o mundo da organização e envolviam os militares dos EUA. Sabu e Kayla não se interessavam tanto assim pelo assunto nem pelos e-mails, mas uma sensação de possibilidade manteve Topiary fisgado, e muito disso se deveu a Barrett Brown, escritor freelancer texano; loiro, aos 29 anos, sua paixão era expor a corrupção do governo.

Topiary ouvira falar de Brown pela primeira vez no dia anterior ao ataque contra a HBGary. Ele publicara uma paródia em nome do Anonymous no blog esquerdista The Daily Kos, no sábado, 5 de fevereiro. O

título: “Anonymous aceita a derrota”. Incoerente e cômico, o texto alegava que Barr havia descoberto que os verdadeiros líderes do Anonymous eram “Q e Justin Bieber”.

E acrescentava: “O Sr. Barr conseguiu penetrar com sucesso em nosso campo de 9 mil servidores proxy e em nosso covil secreto e insurgente, nosso IRC completamente privado, onde então aniquilou com vigor nosso labirinto de fogo, arrecadou todos os anéis de ouro do caminho, abriu um baú com cinquenta chaves de prata para descobrir a senha dos lendários hackers vitaminados do Anon”. Era uma transcrição literal de Topiary no IRC, e ele ficou lisonjeado por ser citado.

Após o ataque, Brown publicou um “comunicado de imprensa” mais formal no Daily Kos, intitulado “Anon domina a HBGary Federal”. A maioria dos comunicados de imprensa do Anon era postada no AnonNews.net, mas, de

verdade, quem controlava isso? O que incomodava muitos Anons era que Brown tinha publicado o comunicado de imprensa com seu nome real, e depois o batizado com um namefag. Ainda assim, Topiary não deu bola; na verdade, desde o começo simpatizara com ele. Após o ataque, Topiary elogiou Brown pelo post paródia. Brown ficou ansioso por ver os e-mails da HBGary, que na época ainda estavam sendo publicados em sites torrent, pouco a pouco.

– Preciso de mais desses e-mails para conseguir conectar os fatos – Brown contou a ele.

Brown acabou se revelando um grande pesquisador. Ele havia baixado a primeira batelada dos 23 mil e-mails de Barr, procurando pistas que pudessem escancarar um caso mais amplo de corrupção que começasse com a campanha de desinformação da HBGary contra o WikiLeaks e terminasse com as forças armadas dos EUA. Após umas poucas semanas de escrutínio, ele pegou o telefone e ligou para William Wansley, um dos vice-presidentes de uma empreiteira militar chamada Booz Allen Hamilton, um nome que aparecia nos e-mails de Barr.

– Alô, é o Sr. Wansley?

– Sim – respondeu uma voz fraca.

– Oi, Wansley, aqui é, hã, Barrett Brown, eu sou um, hã, tipo de porta-voz do Anonymous – falou Brown, disfarçando o nervosismo. – Estou ligando porque estávamos lendo alguns e-mails e casualmente deparamos com uma correspondência entre o senhor e Aaron Barr, da HBGary. Fiquei curioso por saber qual é exatamente o projeto em que vocês estão trabalhando, no que se refere ao Anonymous.

Seguiu-se um demorado silêncio.

– Ah – disse Wansley. – Se quiser ligar para nosso escritório de assuntos públicos, eles podem ajudá-lo...

– Bem, eu acho que o senhor pode me ajudar mais do que eles – vociferou Brown, a autoconfiança crescendo –, porque estava de fato mais envolvido nessas discussões. Na minha experiência, não creio que o setor de assuntos públicos seja tão bom em, sabe, fornecer informações verdadeiras.

Seguiu-se novo e demorado silêncio, enquanto Wansley absorvia o que tinha ouvido em meio a um estrondo em Houston – um avião sobrevoava a casa de Brown.

– Basicamente, por exemplo, estou lendo um e-mail agora mesmo – continuou Brown, gritando para ser ouvido por causa do ruído do avião. – Diz que você tinha uma reunião no escritório da empresa Booz Allen, às dez e meia, deixe-me ver, perto do fim de janeiro, com Aaron Barr. Claro, como o senhor sabe, Barr andava pesquisando o Anonymous para tentar descobrir os nomes de nossos líderes. Ele ia vender uma lista com o meu nome para o FBI, com os nomes de muitos que na verdade *não pertencem* ao Anonymous. A metodologia dele era meio errante, por assim dizer...

Hum, e calculo que a esta altura o senhor provavelmente não esteja trabalhando...

– Eu... eu conheço a organização – cortou Wansley, mostrando cansaço.

– Em primeiro lugar, não comentamos o trabalho de nossa clientela, para proteger a confidencialidade de todos os nossos clientes.

– Certo.

– Posso lhe afirmar que não temos mais quaisquer transações comerciais com a HBGary.

Brown fez uma pausa e indagou: – Então o senhor não ia fazer negócio com eles; só estava discutindo o assunto?

– Não posso comentar sobre o que outra pessoa me pediu para fazer, mas não tínhamos nenhuma transação comercial com a HBGary.

– Mas, antes disso, vocês fizeram outras transações comerciais com eles, não é mesmo? – tentou Brown novamente.

– Nunca.

– Mas o senhor se encontrou com ele não por assuntos sociais, e sim para discutir sobre o Anonymous.

– Não tenho qualquer relacionamento e não posso fazer nenhum comentário.

– Não tem relacionamento com Aaron Barr?

Brown sabia que a conversa chegava ao fim, e começou a se atrapalhar.

– Por gentileza, ligue para meu gabinete de assuntos públicos e eles terão prazer em falar com você.

– Obrigado – disse Brown.

– Obrigado. Até logo.

Click.

Brown desligou, depois caiu na risada sem sorrir.

– Hehehe!

Rapidamente redigiu um post intitulado “VP da Booz Allen Hamilton entra em contradição”, no qual explicava: “Ele declarou não ter relacionamento com a HBGary, fato estranho levando em conta o conteúdo deste e-mail”. Brown acrescentou um link para um dos e-mails de Barr que mencionava: “Tive uma reunião com Bill Wansley na Booz ontem”.

Ao longo dos dias seguintes, Brown continuou a enviar mensagens a Topiary sobre a HBGary. Topiary logo percebeu que Brown falava sério e o convidou para participar de um grupo privado de Skype, com Gregg Housh e mais algumas pessoas, para se concentrar no aprofundamento da pesquisa dos e-mails. Topiary manteve o grupo aberto em tempo integral e descobriu nas duas semanas seguintes que cada vez mais se sentia atraído pelas conversas, gastando pelo menos sete horas por dia na investigação sobre o real trabalho de Barr. Brown batizou a operação de Metal Gear, em referência a um velho jogo da Nintendo, e o objetivo, em suma, era descobrir como a comunidade da inteligência estava se infiltrando na internet e nos sites das mídias sociais como o Facebook e o Twitter para espionar os cidadãos dos EUA. Jargões da segurança cibernética, por exemplo *sockpuppets*, software de gestão de experiência de usuário, monitoramento de dados e infiltração cognitiva, muitas vezes surgiam, cada pista se ramificando a partir do trabalho e da pesquisa da HBGary e Barr. Sempre que Topiary deparava com um e-mail de Barr que pudesse conduzir a novas

informações sobre esses assuntos, encaminhava o link a Brown e o deixava ciente.

O projeto era intenso, principalmente devido ao próprio Brown, que parecia não dormir nunca. Topiary acordava de manhã em sua parte do mundo e descobria que o texano tinha varado a madrugada lendo o tesouro de e-mails da HBGary. Brown então passava mais duas horas explicando o que havia descoberto durante a noite, em geral falando a mil quilômetros por hora. Uma conversa particularmente demorada via Skype com ele durou treze horas, e outra seis horas, com Brown muitas vezes lançando mão de expressões formais como “no que tange à nossa investigação”.

Primeiro, Topiary achava isso irritante, mas depois teve de reconhecer e admirar a ética de trabalho de Brown e sua paixão pelo ativismo. Parecia um nível acima até mesmo dos moralfags mais radicais do Anonymous.

Filho de um rico investidor imobiliário, Brown tinha uma queda por camisas risca de giz e botas de caubói, além de um talento para atiçar o interesse de Topiary.

– Estamos prestes a desvendar algo importante – dizia ele.

– Eu sentia pena dele – lembrou-se mais tarde Topiary. – Ele trabalhava arduamente, mas não entendia o espírito do Anon. – Também não ajudava o fato de o apelido dele no IRC ser Barrett-Brown. – Todo mundo odiava ele. Acontecia toda sorte de debates antiBarrett nos canais privados, em geral tirando sarro de seus métodos e de seu vício em drogas.

Na comunidade Anon, Brown era amplamente conhecido por consumir drogas pesadas. Um jornalista que o entrevistou durante o almoço mencionou que ele começou fumando maconha, bebendo álcool e evitando a comida ao longo da refeição, culminando com uma dose de heroína em forma sintética – em todo o tempo falando com lucidez notável. Sempre que podia, Topiary fazia comentários de que Brown não era assim tão mau se fossem relevadas algumas coisas, mas as confusões de Brown (vídeos no YouTube, conspirações) “só pioravam as coisas”.

O Projeto Chanology e a Operação Vingança tinham mostrado que, se fossem manipulados de modo correto, os Anons, em número de centenas, súbito queriam colaborar em um ataque ou projeto. Mas o essencial nisso era tornar um

ataque engraçado e empolgante. Topiary, que estava se tornando o contato de Brown com o AnonOps, observou que, embora a campanha de Brown para revelar a corrupção tivesse certo apelo ao Anons no começo, o fato de que ele precisava se esforçar para manter o interesse deles mostrava o quão difícil era provocar o espontâneo e imprevisível poder do Anonymous. Brown queria que o Anonymous o ajudasse a executar uma pesquisa de longo prazo, mas era complicado convencer uma comunidade enraizada em lulz a se envolver num projeto por semanas a fio, ou até meses. Tornou-se ainda mais difícil quando Brown tentou colocar o Anonymous no noticiário noturno.

Entre janeiro e março de 2011, o nome de Brown circulou entre os jornalistas que faziam a cobertura do Anonymous, já que ele era um dos raros membros da comunidade que aceitavam atender a uma ligação telefônica e não apenas ficar numa confusa rede de IRC. Vários órgãos de comunicação, como a *Newsweek*, a *Rolling Stone* e a CNN, queriam falar com ele. Então, em 8 de março, a NBC Nightly News transmitiu uma matéria "exclusiva" do repórter Michael Isikoff, que descrevia Brown como um "comandante subterrâneo de um novo tipo de guerra". A entrevista aconteceu no apartamento de Brown e o mostrava digitando em seu netbook Sony branco sobre a mesa repleta de maços de cigarro espalhados e outras parafernálias. Perto do fim da reportagem, Brown aparecia recostado em sua cadeira verde de plástico, falando enfaticamente com um quase pasmado Isikoff, enquanto balançava um cigarro entre os dedos.

– É guerra cibernética – falou ele com voz de barítono sulista, parecendo à vontade. – Pura e simples.

Brown na verdade não se aguentava de dor ao longo da entrevista, tendo interrompido o consumo de Suboxone quatro dias antes. Seus ossos doíam de um modo que a maioria das pessoas jamais experimentará. (Ele teria uma recaída em abril, durante uma viagem a Nova York na qual consumiria heroína, e depois voltaria ao Suboxone quando retornasse para o Texas.)

Durante a entrevista, a câmera brevemente abriu uma panorâmica sobre a tela do laptop de Brown para revelar o recorte de um bate-papo dele com Topiary, Q e vários outros, enquanto Isikoff permanecia sentado ali perto e mirava de relance a equipe da tevê. Os nicknames eram visíveis.

– A-ham – digitou Barrett. – A NBC está aqui.

– Superlegal – disse alguém chamado &efg. – Bem-vindo à internet.

– Querem fazer umas perguntas – falou Brown no próximo segmento. – Ele diz que se sente honrado. Então, qual o próximo passo do Anonymous?

Parecia que a pergunta tinha sido ditada por Isikoff.

Depois a reportagem mostrava Isikoff e Brown passeando lado a lado numa rua movimentada e conversando, Brown gesticulando, as calças cáqui de Isikoff esvoaçando ao vento enquanto ele escutava com atenção.

Em seguida, voltava a mostrar o apartamento, com Brown novamente esparramado na cadeira.

– Tipo, a gente pegou o Stuxnet nessa brincadeira – comentou ele com um floreio de mão, referindo-se a um arquivo anexo entre os e-mails de Barr, que na verdade era uma versão enfraquecida do infame vírus de computador mais conhecido por atacar a infraestrutura nuclear iraniana no começo da década de 2000.

– Não devia ter sido disponibilizado por esse empreiteiro federal para ser arrebatado por uma garota de dezesseis anos e os amigos dela.

– E não devia estar nas mãos do Anonymous! – exclamou Isikoff.

– Mas está – respondeu Brown, abanando a mão de novo e meneando a cabeça sombriamente. – *C’est la vie*.

Brown não ficou contente com a entrevista quando ela foi ao ar. Queria que a matéria aprofundasse as informações reveladas pela hackeagem da HBGary – os contratos militares sobre software de gestão de experiência de usuário –, mas, em vez disso, tinha se focado mais nele e feito o Anonymous se parecer com uma organização séria, o que piorou ainda mais a reputação de Brown junto ao grupo. Isso exemplifica o quão difícil era forçar um assunto na pauta do Anonymous – você tinha de convencer não só os Anons da importância do assunto, mas também a mídia. Mais gente o criticava no AnonOps e no Twitter como um namefag, moralfag e leaderfag. Outros Anons postaram o endereço, número de telefone e outras informações pessoais de Brown no Pastebin.org. Eles odiavam o fato de ele se referir ao Anonymous como uma força do bem, um combatente da corrupção e dos regimes perversos.

Brown ignorava a todos.

– Se eu não respeito nem as leis dos EUA, imagine como eu me sinto em relação às antirregras do Anonymous – explicou ele mais tarde.

Afinal de contas, a origem do Anonymous remontava a uma piada com fundo de verdade. Mas tanto Topiary quanto Brown concordavam que a reputação do último dificultava o recrutamento de sectários para a Operação Metal Gear, e eles precisavam de outra abordagem. Brown decidiu anunciar o projeto nas rádios. Nos meses recentes, alguém do IRC

AnonOps tinha criado uma estação de rádio digital chamada Rádio Payback, consistindo principalmente em música techno tocada vinte e quatro horas por dia, sete dias por semana, entremeada com bate-papos ocasionais de DJs anônimos. Brown abordou um dos DJs no canal de IRC #RadioPayback para indagar se ele podia ir ao ar e anunciar as recentes descobertas da Operação Metal Gear, mas sem sucesso. Em seguida Topiary tentou.

– Barrett não é de todo mau – Topiary contou ao DJ. – A gente devia dar uma chance a ele. No final pode valer a pena.

Por fim, o anfitrião deu o braço a torcer, e Brown, Topiary e outro membro da equipe, com o nickname de WhiteKidney, ganharam as ondas de rádio digital na noite de 16 de março e passaram uma hora inteira contando sobre sua pesquisa a todo e qualquer Anon que estivesse na escuta. Topiary havia solicitado a Brown que falasse devagar, repetindo a palavra “devagar”.

– Vozes não são trens-balas – tentou explicar. – Acho que não funcionou – recordou mais tarde.

No ar, a voz de Brown parecia alta, como se ele estivesse muito perto do microfone.

– A Booz Allen se encontrou com Aaron Barr – denunciou com certa distorção na voz. – A especialidade dele era esse software que utilizava mídia social.

Topiary explicou o software controverso, os soldados que controlavam dezenas de perfis falsos nas mídias sociais, o modo pelo qual podia subverter a democracia e deformar a opinião on-line.

– Temos informantes – acrescentou Topiary, referindo-se às pessoas que ofereceram informações sobre a Booz Allen.

– A gente não conversa sobre informantes – emendou Brown sem demora. Aparentemente havia dois informantes. Um tinha entrado em contato com Brown, e o outro era alguém que ele havia encontrado no meio dos e-mails de Barr. – Foi para isso que treinamos durante cinco anos – acrescentou perto do final da transmissão, antes de a discussão baixar o nível e envolver piadas sobre o pênis de Brown.

Mesmo assim, a apresentação funcionou. Em dois dias, a equipe da Metal Gear tinha inflado para vinte pesquisadores fixos. Durante a transmissão na rádio, centenas de pessoas haviam baixado um link para acessar a pesquisa atual da equipe, indicando que o número de ouvintes deve ter passado dos milhares. Um operador de IRC que anteriormente tinha caçoado de Brown e descartado a Metal Gear como pura trollagem agora falava no IRC sobre o sucesso da operação. A equipe de investigação se isolou em seu grupo privado de Skype e passou muitas horas mais vasculhando os e-mails, fazendo ligações telefônicas e escutando Brown. Às vezes, ele delegava missões, no entanto era mais frequente as pessoas se voluntariarem.

– Só foi a gente explicar sobre *sockpuppets* (falsas identidades) e robôs que todo mundo se empolgou – lembrou-se mais tarde Topiary.

Nessa ocasião, nnão existiam provas – apenas especulações. Por exemplo, o governo do Azerbaijão havia recentemente detido dissidentes políticos on-line, e Topiary e Brown declararam na Rádio Payback que o software de espionagem da Booz Allen devia ter sido utilizado. O raciocínio deles: a Booz Allen tinha um escritório no Azerbaijão.

Era uma pista plausível, mas, como sempre, o grupo precisaria se esforçar para encontrar tempo e concentração para segui-la. Outros Anons descobririam pistas ainda mais promissoras do tesouro de e-mails de Barr.

De vez em quando, alguém aparecia com uma pista completamente nova.

Então aconteceu uma distração maior, mostrando o quão facilmente uma pessoa podia deixar a grande mídia agitada com uma suposta operação do Anonymous. Um rapaz de apelido OpLeakS abordou Brown na rede de bate-papo, alegando que havia obtido um tesouro de e-mails e precisava de conselhos. O vazamento,

afirmou ele, envolvia o Bank of America.

Intrigado, Brown o convidou para entrar no grupo secreto de Skype e fazer uma conferência com Topiary e WhiteKidney. OpLeakS tinha um forte e monótono sotaque de Nova Jersey. Primeiro Brown e Topiary ficaram empolgados com o que ouviam. OpLeakS, convicto sectário do Anonymous, afirmou que tinha sido procurado por um ex-funcionário do Bank of America, alguém que havia trabalhado lá por sete anos, a partir da aquisição da Balboa Insurance pelo banco. Ele e o ex-funcionário trocaram e-mails durante vários dias. Sempre que OpLeakS fazia uma pergunta sobre o Bank of America, obtinha respostas cada vez mais condenatórias sobre como o banco estivera ocultando empréstimos fraudulentos ou como os gerentes praticavam favoritismo. Tudo indicava práticas desonestas de hipotecagem, contou ele a Brown e aos outros no Skype, coisas capazes de derrubar o Bank of America.

– Por que você não envia o material para a gente dar uma olhada? – sugeriu Brown, já meio cético em relação àquela história toda. No assunto em foco, OpLeakS parecia estar tateando no escuro.

– Talvez eu possa ajudá-lo a botar a boca no trombone – ofereceu-se Topiary, pensando que qualquer vazamento envolvendo o Bank of America criaria interesse após o caso do WikiLeaks. Acrescentou que eles podiam hospedar a correspondência de OpLeakS por e-mail no novo site AnonLeaks.

OpLeakS não se interessou por nenhuma das propostas, mas encaminhou um punhado de e-mails na esperança de alguma validação.

Agora Brown ficou definitivamente impressionado – as alegações do ex-funcionário soavam embaraçosas para o Bank of America, mas OpLeakS

não dispunha de nada capaz de derrubar um banco multinacional inteiro.

Devido aos recentes boatos de que o WikiLeaks tinha um lote de dados explosivos sobre o Bank of America, era fácil se confundir com a alegação de OpLeakS e pensar que as denúncias mantinham alguma relação entre si.

A essa altura, o Anonymous e o WikiLeaks estavam intimamente associados um com o outro, por meio dos ataques de DDoS da Operação Vingança e depois pelo anúncio do nome AnonLeaks. Mas, é claro, os dados de OpLeakS não tinham nada a ver com o WikiLeaks, e também não ofereciam e poder de dano.

– Parecia que ele não tinha o que pensava ter – recordou--se mais tarde Brown numa entrevista. Topiary lembrou que o homem prometeu mais informações, mas não as entregou. – Ele não abriu o jogo – acrescentou Brown.

Apesar das frágeis evidências e da limitada compreensão sobre finanças, OpLeakS postou vários tweets durante o fim de semana de 12 e 13

de março, insinuando que o "Anonymous" tinha e-mails que expunham "corrupção e fraude" no Bank of America.

De modo espantoso, os tweets receberam a atenção da mídia e foram levados a sério.

"O Anonymous, um grupo de hackers simpatizante do WikiLeaks, planeja liberar e-mails obtidos do Bank of America", anunciou sem fôlego a Reuters no domingo, 13 de março. Sites de blogs como o Gawker e o Huffington Post ecoaram as notícias. OpLeakS tinha, por um acidente fortuito, esbarrado na história que todo mundo esperava. Em dezembro de 2010, a revista *Forbes* publicara uma reportagem de capa em que Julian Assange prometia vazar um importante lote de informações secretas do Bank of America que seria altamente prejudicial à reputação do banco.

Aaron Barr aproveitara essa mesmíssima ameaça ao sondar a Hunton & Williams, empresa consultora jurídica do banco, com propostas para fazer uma campanha de descrédito contra o WikiLeaks. O problema era que ninguém sabia a data do grande vazamento, por isso, quando pareceu que o Anonymous, os algozes da HBGary, do PayPal, da Visa e da MasterCard estavam prestes a atacar o Bank of America por conta própria, as expectativas ficaram altas. Altas demais.

Na manhã de segunda-feira, como prometido, OpLeakS postou sua correspondência por e-mail com o ex-funcionário do Bank of America no site hospedado por seu próprio blog Wordpress, o bankofamericasuck.com, sob o título "Segunda-feira negra: ex-funcionário do Bank of America pode provar fraude em hipotecas – parte 1" (nunca houve parte 2).

– Sou OperationLeakS – começava o post. – Leia todas as linhas e capturas de tela.

E seguiam-se capturas de tela com os e-mails entre OperationLeakS e o ex-

funcionário do banco. Entre as perguntas, estavam: – Você tem provas de que trabalhou no Bank of America?

– É uma espécie de culto?

– Então por que você quer a cabeça do BoA com tanta gana?

– Quando foi despedido você levou suas coisas, como fotos?

Acompanhava essa última pergunta uma foto, fornecida pelo ex-funcionário, de uma planta mutilada, um pouco de terra e uma pequena bandeira nacional enfiada numa caixa de papelão.

O tráfego no www.bankofamericasuck.com se intensificou tanto naquela manhã que muitas pessoas que o tentaram acessar recebiam a mensagem de erro ou tinham dificuldades para carregar a página. Halah Touryalai, redatora da *Forbes* sobre assuntos de Wall Street, foi uma das primeiras pessoas a conferir os e-mails, e no comecinho da manhã de segunda-feira preparou um post chamado "Vazamentos de e-mails do Bank of America estão aqui. Que estrago eles vão fazer?". Em poucas horas 30 mil pessoas tinham lido o artigo. Até hoje ele recebeu mais de 40 mil visualizações.

– É difícil afirmar se há algo realmente incriminador nesses e-mails – arriscou-se Touryalai no artigo. Ela frisou que, enquanto Julian Assange dissera à *Forbes* em dezembro que tinha uma riqueza de dados que poderia "derrubar um banco", em fevereiro a Reuters relatara que Assange não tinha mais certeza se suas mercadorias teriam um impacto realmente negativo. O departamento de publicidade do banco já estava rotulando as afirmativas de OperationLeakS de "extravagantes". O mercado bateria o martelo.

Touryalai e outros repórteres da área de finanças controlaram o preço das ações do Bank of America naquela manhã. Quando soou o sino na abertura da Bolsa de Valores de Nova York, os traders nova-iorquinos depararam com os e-mails – e não fizeram nada. O valor da ação do banco caiu apenas 15 centavos ao final do pregão de segunda, indicando que os investidores não tinham se importado.

A grande mídia, desde a CNN até a BBC, passando pelo *USA Today*, tinha relatado empolgadamente sobre os e-mails, mas no fim da semana todos concordavam que a "derrubada" fora um fiasco.

– Desculpem-me se eu disfarçar um bocejo – comentou Annie Lowrey na revista *Slate*.

Os comentários feitos pelo ex-funcionário para o OpLeakS eram café pequeno e por demais mirabolantes para ter algum significado.

Esse talvez tenha sido o momento em que a mídia aprendeu uma lição decepcionante sobre o Anonymous. O grupo causara danos, com certeza, mas era tão bom em criar agitação sobre verdadeiros segredos quanto sobre descobertas que de secretas não tinham nada. Pior ainda: a agitação não viera de um grupo de hackers, mas de um homem de voz monótona com limitada compreensão sobre finanças, a qual fora amplificada globalmente por invocar o nome "Anonymous" na hora certa e com o assunto certo. Se o Anonymous desejava atenção confiável, precisava existir alguma semelhança com uma organização central, como aconteceu na Operação Vingança e no Projeto Chanology, mesmo se eles odiassem a ideia de leaderfags.

***

Após cerca de duas semanas de trabalho com a Operação Metal Gear, Topiary sentiu-se dividido entre dois grupos distintos: os hackers que tinham atacado a HBGary e os agora dez ou doze investigadores que apoiavam Brown (número que definhava aos poucos desde o programa na Rádio Payback). Ele descobriu que não conseguia explicar a uma das facções o que a outra fazia. O grupo informacional de Brown era complexo demais; o de Sabu e Kayla, secreto demais.

As ideias de Brown também começaram a soar estranhas, especialmente depois que ele começou a sugerir que alguém das forças armadas poderia assassiná-lo. Primeiro Topiary achou que ele estava brincando, mas Brown falava sério.

– Estou no centro do mundo das informações e temo pela minha segurança – confessou-lhe Brown a certa altura. – Sei muita coisa sobre os governos do Oriente Médio que trabalham com os Estados Unidos.

Meses depois, Brown confirmou isso numa entrevista: – Outra pessoa que entabula um diálogo semiconstante com pessoas do Ministério das Relações Exteriores e tem uma boa conexão com esses assuntos estava levantando essa possibilidade. Não levei tão a sério assim – acrescentou rapidamente.

Na época, Topiary não duvidou da sensação de iminente perigo preconizada por Brown – ele também sentia que estava envolvido demais.

– Foi intenso – concordou Brown. – Informantes nos contavam coisas bem mais insanas. Boa parte de nossa equipe ficou com a impressão de que tudo que a gente investigava e acidentalmente ficava sabendo era parte de algo muito maior. E, devido à investigação, estávamos entrando numa enrascada.

Os tópicos escavados por eles prenunciavam perigo porque encapsulavam a única coisa que os Anons tinham a temer: tecnologia melhor que a deles, capaz de identificá-los. Então, no final de março, o Congresso começou uma pequena investigação sobre os contratos da HBGary.

– A merda está se tornando realidade – observou Topiary.

– Imagine perder nosso anonimato – Topiary tinha falado durante o programa da Rádio Payback para explicar de que se tratava o software de gestão de experiência do usuário. – Imagine criar uma conta on-line com um apelido e, meses depois, criar outra... Imagine um software que consiga correlacionar cada horário de logon dessas duas contas, cada detalhe de gramática que você utiliza, cada apelido... automaticamente descobrindo quem você é on-line.

Topiary sabia que as pessoas podiam descobrir a identidade verdadeira de um Anon simplesmente seguindo um rastro no Google que começasse com o nome de seu filme predileto. Odiava a ideia de um software contratado pelo governo fazendo isso com eficácia cem vezes maior.

Mas o estresse, os debates em fluxo de consciência no Skype, as conspirações sobre os militares estavam prestes a extrapolar os limites. Ele começou a pensar no outro grupo – Sabu, Kayla e os demais no #HQ. As hackeagens contra a Igreja Batista Westboro, o governo tunisiano, os sites do governo egípcio, a aliança de direitos autorais, o script antiespionagem tunisiano, a HBGary – tudo havia acontecido pela ação das pessoas dessa reduzida equipe. Topiary pensou que, se esse grupo se retirasse, o Anonymous, como o mundo externo o conhecia, morreria. Mais importante que a pesquisa de Brown era manter unido esse grupo.

– Barrett – disse ele enfim em meados de março. – Preciso saltar fora disso. Está ficando muito esquisito e conspiratório.

– Ok – respondeu Brown. – Não podia contar que você fosse continuar tão envolvido como já se envolveu.

Brown parecia silenciosamente aborrecido, mas Topiary teve a sensação de que ele compreendera. Fechou seus documentos da Operação Metal Gear e os organizou numa pasta, guardando por volta de 150

megabytes de dados – arquivos de texto e arquivos de áudio das conferências telefônicas de Brown – que ele provavelmente jamais voltaria a olhar.

Enquanto arrumava tudo, Topiary foi indagado numa entrevista se achava que essa “equipe reduzida” poderia um dia se desmembrar do Anonymous e tomar suas próprias iniciativas.

– Não realmente – respondeu ele. – Posso imaginar isso agora. A gente provavelmente causaria rebuliço na web, criaria um grupo de hackers de nome nerd que não sairia das manchetes. Vazamentos, desfigurações, destruição. Com o tempo, ficaria cansativo. Sob a bandeira do Anonymous temos uma causa, e um significado, deixando o ego de lado.

Poucas semanas depois, ele mudaria de ideia completamente.

CAPÍTULO 14

Backtrace ataca

Fazia um frio de rachar em Michigan no fim de fevereiro. Após uns dias de falsa primavera, uma nevasca cobrira o gramado frontal de Jennifer Emick com mais de um metro de neve. Esquilos escarafunchavam a caixa de correio e roubavam pacotes na esperança de que contivessem biscoitos, mas Emick nem cogitou a hipótese de sair para conferir. Além do frio enregelante lá fora, agora ela estava profundamente imersa na investigação que iniciara sobre o Anonymous. Alcançara um novo nível após Laurelai ter repassado os registros com o conteúdo dos bate-papos do canal HQ. Emick almejava mostrar ao mundo a verdadeira face do Anonymous – vingativa, corrupta e nem um pouco anônima.

Em dezembro de 2010, quando a Operação Vingança havia realmente decolado com seus ataques contra o PayPal e a MasterCard, Emick já tinha se afastado completamente do Anonymous. Não que ela não gostasse dos alvos – o problema era a crueldade com a qual, cada vez mais, ela deparava na rede, desde o Projeto Chanology. Emick mantivera amizade com alguns Anons, hospedava alguns sectários na casa dela e participava de um grupo no Skype, às vezes chamado de Treehouse. Ela os descrevia como “apenas uns amigos que se reuniam para conversar”. O Chanology havia gerado novas células no Anonymous, ou, às vezes, apenas grupos de amizades.

Alguns deles definharam, e muitos participantes do Chanology foram para a faculdade ou interromperam definitivamente a participação no Anonymous. Poucos membros dedicados, como Laurelai e Emick, tinham retornado para a próxima onda em 2010. Só que Emick se tornara parte de uma minoria que desejava brecar o Anonymous.

Como Barrett Brown, Emick tendia a ver o mundo filtrado por teorias, e a mais grandiosa era a de que o Anonymous se tornara exatamente como a Cientologia: vingativo, reacionário e fraudulento. Quando ela presenciou a criação da rede de IRC AnonOps, acreditou que os operadores tentavam reviver “esse velho espírito de ser intimidante”. Emick enxergava jovens que queriam ser parte de um grupo de valentões sem nome, pois sofriam bullying na escola. De repente, eles podiam fazer parte de um grupo que inspirava medo nas pessoas, conforme explicou.

Aos poucos, Emick criava uma cruzada embasada parte em princípios, parte em motivos pessoais. Com quatro filhos, três deles adolescentes, magoava-lhe a ideia de que pudessem se atrair por “alguma história idiota”

on-line que desse uma aura romântica às táticas de bullying.

– A garotada é trouxa – explicou ela. Não dão bola para legalidades. – Só dizem: “Ok, joia”.

Ela estava certa quanto à falta de consciência jurídica. Quando milhares de pessoas se inscreveram nas salas de bate-papo da rede AnonOps, ansiosas para ajudar a derrubar o PayPal, a maioria não se deu conta de que utilizar o LOIC tinha potencial de levá-las à cadeia. Na época, Emick ficava indignada ao entrar nas salas de bate-papo e ver os operadores do IRC dizendo aos novos Anons que não precisavam temer ao participarem de um ataque digital. Quando, utilizando um pseudônimo, Emick confrontou os operadores Wolfy e Owen e os acusou de tentar formar um exército pessoal, eles a baniram da rede.

No fim de fevereiro, as autoridades na Holanda e na Grã-Bretanha tinham detido cinco pessoas envolvidas na Operação Vingança; nos EUA, o FBI continuava a executar os quarenta mandados de busca e apreensão.

Mais tarde, em julho, as autoridades prenderiam dezesseis suspeitos. A lista com mil endereços IP que o PayPal havia fornecido ao FBI dava resultado.

Os operadores tinham se enganado, ou possivelmente mentido, e o que deixava Emick mais chateada era que eles sabiam como evitar a cadeia melhor que os novos voluntários.

Logo após saber do ataque contra a HBGary, Emick começara a passar horas diante do computador, alimentando suspeitas de que as pessoas que controlavam o Anonymous eram criminosas. Criou um interesse especial pelo nickname Kayla, e, quando começou a procurar em fóruns, o nome apareceu num site popular de aspirantes a hacker, o DigitalGangster.com.

Fundado por Bryce Case, 29 anos, conhecido na internet como YTCracker (pronunciado “whitey cracker”), o DigitalGangster foi criado como um fórum de hackers de chapéu preto, e um dos usuários se chamava Kayla, jovem de 23 anos de Seattle. Emick continuou a investigar. O próprio YTCracker era hacker; programava computadores desde os quatro anos de idade, ganhando notoriedade

após hackear os sites do governo dos EUA e da NASA e desfigurá-los. Ele passou a apreciar hip-hop, inaugurou uma gravadora independente e promoveu shows na convenção de hackers DEF

Con. Originalmente, o DigitalGangster servia de produção para suas raves e clubes noturnos, mas ele o transformou num fórum para seus amigos hackers que migravam das salas de bate-papo do AOL para redes de IRC.

Era um núcleo de hackers descolados e um terreno de provas para os novos. Em 2005, um de seus usuários, com dezesseis anos de idade, sediado em Massachusetts, hackeou a conta de Paris Hilton no T-Mobile e obteve acesso a fotos dela nua. Quatro anos depois, um hacker de dezoito anos conseguiu as credenciais de senha para a conta oficial do presidente Obama no Twitter. Outro hacker conseguiu fotos de Hannah Montana. O

fórum era um local onde crackers podiam negociar direitos de vanglória cada vez mais ambiciosos; um local onde uma pessoa podia entrar em contato com spammers (também conhecidos como marqueteiros da internet) e vender uma ou duas bases de dados.

YTCracker não gostava do Anonymous porque não gostava do modo como pessoas inocentes eram pegas no fogo cruzado. Acontecera com ele.

Em março de 2011, poucos hackers de seu fórum, inclusive um chamado Xyrix, atacaram seu site sem motivo algum, exceto por ser frequentado por alguns dos inimigos deles. Para obter o acesso administrativo, eles ligaram para a AT&T, informaram que o telefone de YTCracker tinha sido roubado, conseguiram novos número e cartão SIM e também sua senha no Gmail. A partir daí, foram capazes de hackear o fórum do Digital Gangster, depois pichá-lo com uma mensagem que afirmava que ele tinha sido “hackeado por Kayla, moça de dezesseis anos”.

Foi então que Emick ficou confusa. Neste site, Kayla era descrita como jovem de 23, mas ela havia lido um artigo na Encyclopedia Dramatica dizendo que em 2008 “Xyrix fingia ser mulher utilizando o nome ‘Kayla’ na rede Partyvan”. Todo mundo sabia que Xyrix era um corpulento homem de 24 anos de Nova Jersey chamado Corey Barnhill. Emick pensou, incorretamente, que isso significava que Kayla era Barnhill.

Kayla tinha uma explicação sobre por que todo mundo pensava que ela era

Xyrix: nos idos de 2008, ela havia hackeado a principal conta da web dele e fingira ser ele para obter informações de um administrador da Partyvan; o administrador então erroneamente concluíra que Xyrix e Kayla eram a mesma pessoa, e a acrescentara na página de Xyrix na Encyclopedia Dramatica. A mensagem de deface “hackeado por Kayla, moça de dezesseis anos” no site de YTCracker pode muito bem ter sido obra de Xyrix, aproveitando-se desse mal-entendido para tentar humilhar YTCracker.

Emick seguia o caminho errado em relação à Kayla, mas sentia que descobria algo valioso. Começou a passar mais tempo nesses fóruns, montando o quebra-cabeça de apelidos, identidades falsas e informações falsas, sendo conduzida a novos rastros. Enquanto muitos hackers variavam seus nicknames, a cobiça pela credibilidade compelia outros tantos a permanecer com um só nome. Em muitos casos, tudo que Emick precisava fazer era inserir um nickname no Google, pesquisá-lo em fóruns como DG e Reddit, e depois conversar com amigos daquela pessoa em redes de IRC. Ela utilizava um software de tomar notas para cruzar todas as referências.

– É preciso ser obcecada com os detalhes – explicou ela mais tarde.

Logo havia reunido gigabytes de dados em seu computador, e tinha material suficiente para descobrir os verdadeiros nomes, e até mesmo os endereços, de alguns Anons.

***

Emick sentiu urgência em transformar sua pesquisa em algo que aprimorasse a abordagem fracassada de Barr. Derrotá-lo em seu próprio jogo tornou-se um desafio pessoal. Percebendo que precisaria de ajuda, ela começou a conversar com um amigo virtual dos velhos tempos do Chanology sobre formar uma equipe antiAnonymous.

Aos 26 anos de idade, Jin Soo Byun atuava no ramo da segurança cibernética, no monitoramento de penetrações. Ex-decodificador da força aérea, ele se aposentara ao ser atingido pelo bombardeio de um dispositivo explosivo improvisado, no Iraque. O acidente o deixara com graves sequelas cerebrais e perda de memória, mas ele se lançou nos protestos do Chanology em 2008 e construiu uma reputação na engenharia social, sob os nicknames Mudsplatter e Hubris. Ele e Emick trabalharam como administradores no site de Laurelai, e a

dupla cultivou uma amizade via Skype, bate-papos de mensagens instantâneas e ligações telefônicas. Com frequência eles apenas fofocavam sobre o cenário de hackeagens, desfrutando o gostinho de detratar seus inimigos.

Emick contou seu plano a Byun. O Anonymous havia se tornado um grupo quase impossível de ser barrado.

– Alguém precisa pará-los antes que algo ruim aconteça – contou ao amigo.

Ele entrou no jogo. Durante alguns anos, Emick e Byun haviam conversado sobre começar uma empresa de segurança digital que utilizasse a perícia tecnológica de Byun e as habilidades investigativas de Emick. Agora tinham algo para trabalhar juntos; algo que Emick chamava de “operação psicológica”.

Byun entrou em contato com amigos da indústria de segurança cibernética, reunindo por volta de meia dúzia de voluntários para auxiliar em sua pesquisa. Entre eles estava Aaron Barr.

– De imediato, após auxiliar na investigação [do FBI], eu quis entender o grupo ainda mais – explicou ele mais tarde. – Em especial aqueles que nos atacaram.

Eles precisavam agir com rapidez. O Anonymous se preparava para atacar a Sony e, para piorar as coisas, o caso HBGary deixara o grupo com a sensação de ser invencível.

Emick e companhia decidiram chamar a recém-criada agremiação de Backtrace Security, nome surgido diretamente da fábrica de memes que é o 4chan. Referia-se ao incidente com Jessi Slaughter, quando os usuários do *b* tinham trollado cruelmente uma moça que havia postado vídeos de si mesma no YouTube, levando o bigodudo pai dela a dar uma bronca nos trolls pela webcam – e depois ela fez o upload. Citações pinçadas como “Eu sei de quem está partindo isso! Porque eu fiz um backtrace!”, junto com “Vocês foram desmascarados!” e a menção à “polícia cibernética”, todas viraram

memes.

O

uso

sarcástico

da

palavra

backtrace

(retrorrastreamento) tinha o objetivo de enfurecer o Anonymous, porque reciclava uma de suas piadas internas.

Emick fez todos se conectarem a uma planilha que podiam editar. Uma barra de bate-papo corria paralelamente para a discussão do trabalho em tempo real. Ela forneceu uma lista extensa de nicknames do IRC AnonOps que eles iriam tentar doxear. Todos escolhiam nicknames ao acaso e depois escarafunchavam a web em busca das identidades verdadeiras. Às vezes, alguém no grupo obtinha uma pista que o levava a adicionar um novo nome à lista. Barr também começou a participar dos debates on-line, compartilhando informações gerais sobre o Anonymous que compilara durante sua pesquisa. A tarefa mais demorada era a de peneirar os dados coletados. Emick e os demais baixavam grandes volumes de informações, mas verificá-las levava dias a fio.

Tão logo os filhos saíam de casa e entravam no ônibus escolar, Emick sentava à mesa, às vezes nas próximas dezoito horas ou até sua concentração vacilar. Deixava de almoçar e, muitas vezes, mandava os filhos prepararem a janta. A família encomendava muita pizza. Emick disse que os filhos a apoiavam, embora na maior parte do tempo não os informasse do que fazia. Ela os criou para serem autoconfiantes. O pai e a madrasta de Emick tinham sido alcoólatras que deixavam por conta dela, a mais velha dos cinco filhos, tarefas como cozinhar, lavar roupa e controlar as contas da casa. Às vezes, o pai cozinhava, mas a madrasta raramente saía do sofá.

Emick trabalhava em uma mesa construída sob encomenda, com 2,10 m de largura, disposta num canto de sua sala de dois ambientes. Sobre o tampo, o telefone, cadernos, arquivos, luminárias portáteis, uma caixa de cartões natalinos do ano anterior e dois computadores. Um deles era um laptop com Linux, o sistema operacional de código aberto que ela utilizava para bater papo em redes de IRC. Ela precisava de dois PCs para quando fingia ser duas pessoas ao mesmo tempo nos canais de bate-papo ou enviava tweets a mais de uma conta de Twitter. Sua conta principal era @FakeGreggHoush. Quando Emick espionou o

AnonOps e tentou extrair informações, operadores com olhos de águia notaram o nickname dela e tentaram identificar seu endereço IP. Cada computador trabalhava a partir de um servidor proxy que a colocava em dois fusos horários distintos, para impedir que alguém conseguisse localizá-la.

Muitos nomes na lista de Emick foram rastreados em apenas dez ou vinte minutos. Alguns Anons reaproveitavam seus nicknames em sites como Facebook, Reddit, YouTube e Yelp, onde discutiam abertamente seus locais de origem ou falavam em um IRC público sem ocultar os endereços IP por trás de uma VPN. Em vez disso, os endereços IP dessas pessoas estavam "nus" e se vinculavam a seus endereços residenciais. Em certos casos, Emick e sua equipe usavam nomes distintos, alegavam pertencer ao Anonymous e falavam com os Anons no IRC, às vezes até os convencendo a participar de bate-papos com vídeo.

A investigação decolou de verdade quando a velha amiga Laurelai foi envolvida pela tática de intimidação que Emick utilizava por intermédio da conta @FakeGreggHoush. Quando Laurelai entregou o registro com 245

páginas de extensão dos bate-papos dos hackers da HBGary no canal #HQ, Emick não pôde acreditar em sua sorte. Além de incriminar os nicknames de Sabu, Kayla, Tflow e Topiary no ataque da HBGary, o registro lhe forneceu algo ainda mais revelador.

Um diminuto fragmento do registro mostrava Sabu dizendo aos outros hackers que eles ainda podiam fazer logon numa conta backdoor que ele havia criado no servidor da HBGary Federal – algo que lhes permitia espionar os e-mails da empresa novamente, caso desejassem. Mas, quando ele digitou o endereço da web, acidentalmente entregou o nome de seu servidor privado: www.google.com.*a*prvt.org.

– Epa – dissera ele. – Domínio errado. – Em seguida digitou www.google.com*a*hbgary.com. – Agora sim.

Mas o endereço do servidor de Sabu tinha permanecido no log de Laurelai. Emick rapidamente realçou a informação e, sabendo que deparava com algo importante, colou-a no Google. Sem demora, ela topou com um subdomínio chamado ae86.prvt.org. O nome ae86 era relevante. O

subdomínio conectava-se ao cardomain.com, site para entusiastas de

automóveis, onde Emick descobriu fotos e o vídeo de um Toyota AE86

envenenado. Com esse número de modelo, só podia ser o carro de Sabu.

Cruzando as referências do site automobilístico com o vídeo do YouTube do AE86, ela por fim descobriu uma página do Facebook com o URL, facebook.com/lesmujahideen, e o nome Hector Xavier Montsegur. Ela havia soletrado um pouco erroneamente o último sobrenome, mas isso era o mais próximo que alguém havia chegado de doxear Sabu. Emick não conseguiu seu endereço no complexo habitacional Jacob Riis, mas realmente concluiu que ele morava no Lower East Side, em Nova York.

Ela aprofundou a pesquisa sobre as façanhas de Sabu on-line, Descobriu que, anos antes, ele havia hackeado um obscuro site pornô chamado ChickenChoker.com e, bizarramente, o pichara com uma mensagem em que revelava a origem porto-riquenha: – Olá, sou “Sabu”, ninguém especial por enquanto... ultimamente tenho visto UM MONTE de pichadores brasileiros e asiáticos dando o ar de sua graça, mas não vi nenhum hacker de Porto Rico, ou melhor, “pichador”, aparecer, por isso acho que agora vou ser o pichador porto-riquenho deste site, que tal? elite...”

– Tinha um cunho político, mas de uma política sem sentido – afirmou mais tarde Emick.

Sabu subiu ao topo de sua lista de procurados. Ele era “megalomaníaco”

e “não muito inteligente”, acrescentou ela.

Por fim, Emick e sua equipe compilaram uma pesquisa sobre setenta identidades e começaram a insinuar pelo Twitter e junto à mídia que um grande grupo de Anons logo seria exposto. Enfim ela publicou seu nocivo perfil sobre Sabu no site da Backtrace Security, concluindo que ele era de etnia porto-riquenha, beirava os trinta anos e nascera em Lower East Side, Nova York. Tivera uma experiência “problemática” no ensino médio, era relativamente inteligente, mas se ressentia com a autoridade e o “sucesso de gente que na percepção dele valia menos que ele próprio. Depois de sofrer humilhações, uma década atrás, após postar manifestos confusos e incoerentes em sites desfigurados, ele caiu na obscuridade até se associar publicamente com o grupo de protestos Anonymous”. Ela se preparou para anunciar ao mundo o nome verdadeiro de Sabu.

Sabu, o famoso e bem relacionado hacker que penetrara domínios nacionais, havia acabado de ser descoberto por uma mulher de meia-idade de Michigan.

***

Em meados de março, Emick compilara setenta nomes num arquivo em PDF de quatro páginas, que ela batizou de Namshub. O arquivo listava Kayla como Corey “Xyrix” e Sabu como Hector Xavier Montsegur, morador do Lower East Side, Nova York. Ela e Byun entraram em contato com alguns jornalistas e se ofereceram para remeter a lista. Naturalmente, disponibilizaram o registro do conteúdo dos bate-papos do #HQ a Adrian Chen, o repórter do Gawker renomado por escrever com ceticismo sobre o Anonymous. Já que seria difícil corroborar a lista de nomes, e Chen não queria acusar pessoas inocentes, ele se concentrou no conteúdo dos bate-papos do #HQ. O material trazia suculentos petiscos sobre o funcionamento interno do grupo de hackers Anonymous. Em 18 de março, ele publicou um artigo intitulado “No interior da secreta sala de guerra do Anonymous”, apresentando citações pinçadas a dedo do canal #HQ. Mostrava Sabu espinafrando Laurelai, o grupo presunçosamente se parabenizando após a renúncia do presidente egípcio e a insinuação de que pertenciam a uma cúpula do Anonymous, sendo Sabu o chefão.

Sabu, nesse meio-tempo, destilava fel. Avisou aos outros: – Vou pegar meu carro, ir até a casa dele e perturbá-lo.

Topiary e Kayla tentaram acalmá-lo. Sabu se referia a Laurelai, observando com raiva que ele sempre suspeitara que aquele “homem/mulher/coisa” um dia trairia a confiança do grupo. Pior ainda para Sabu – fato que ele não contou a ninguém – era que a Backtrace tinha percebido seu comentário de “epa, domínio errado” que conduzia a “Hector Montsegur”. Com a exposição pública de uma íntima aproximação de seu nome real e de seu endereço de servidor, Sabu tinha um problema potencialmente grande. Se a polícia seguisse as descobertas da Backtrace, bateria à sua porta a qualquer hora.

Mas havia o lado positivo. Ninguém ouvira falar na Backtrace até agora, e era possível que ninguém levasse a sério os doxeadores por trás do site.

Além disso, Sabu raciocinou, seu sobrenome fora soletrado erroneamente, seu endereço verdadeiro não tinha sido encontrado, e provavelmente houvesse várias pessoas com o nome Hector Monsegur em Lower East Side, Nova York. (Isso

era verdade.) Sabu avaliou se poderia achar graça disso como todo mundo e continuar a hackear com essa nova equipe de pessoas que parecia se entender tão bem. Apesar de todos os perigos, ele estava tentado a continuar sua trajetória de hacker.

***

– Tudo errado – disse Topiary num canal de IRC com os outros após ter lido as quatro páginas de nomes do documento da Backtrace. Emick identificara Topiary como Daniel Ackerman Sandberg, da Suécia. – Nunca fui à Suécia e não faço ideia de quem é Daniel Sandberg – alegou.

Ele, Kayla, Tflow e AVunit tinham se reunido novamente numa nova sala de IRC para discutir a "exposição" e obter algum alívio cômico.

– Todos eles pensam que sou Xyrix! – exclamou Kayla.

– Até parece que o Aaron Barr está trabalhando com eles ;) – gracejou Tflow.

O grupo há tempos desconfiava (com razão) de que Barr colaborava secretamente com a Backtrace para tentar atingir as pessoas que haviam atacado a HBGary.

– Não conseguiram literalmente nada sobre mim – comentou AVunit, que havia sido descrito no documento de Emick como um "codificador"

chamado Christopher Ellison, de Ipswich, Grã-Bretanha. – Bem, imagino que "codificador" esteja certo.

– Também sou um fraudador do paypal – brincou Tflow; ele não recebeu um nome no documento. – A única parte que acertaram sobre mim foi "Tflow" e "codificador php". Mas, sabe, eu me sinto lisonjeado. Meu nome está em vermelho.

– Será uma nova tendência :D ver quem consegue fazer o pior arquivo de doxeagem do mundo? – indagou Kayla.

O grupo sentia-se confiante. A pesquisa de Aaron Barr estava errada; a da Backtrace parecia estar errada. As pessoas tentavam, mas ninguém conseguia pegá-los.

Eles não sabiam que, embora a Backtrace tivesse se enganado em muitos nomes, uns poucos, inclusive o de Sabu, tinham sido identificados corretamente. Um hacker que viu seu nome verdadeiro na planilha logo interrompeu todas as suas atividades com o Anonymous e nos meses seguintes viveu apavorado, com medo de que o FBI viesse prendê-lo.

– Ainda tenho palpitações cardíacas – contou ele numa entrevista presencial há cerca de meio ano. – O que mata é a incerteza; o tempo todo na dúvida se a gente vai escapar ou pegar vinte e cinco anos de cadeia.

Casualmente, Emick não teve pena de sua informante, Laurelai, que aparecia em sua lista com o antigo nome do mundo real, Wesley Bailey, descrito como "transgênero" e "ex-soldado de Duncan, Idaho". Laurelai ainda não acreditava (ou ao menos não queria acreditar) que Emick era a força motriz por trás da Backtrace, ou que ela a havia traído. Ninguém ainda tinha provas de quem estava por trás desse grupo antiAnonymous.

Emick apreciava essa situação. Tão logo a planilha dos nomes e os registros do HQ foram vazados, ela continuou a oferecer um ouvido solidário a Laurelai, enquanto o "ex-soldado" se queixava sobre toda a experiência e sobre o quão amargamente se arrependia de ter passado os registros do bate-papo à pessoa no Twitter chamada @FakeGreggHoush.

Só meses depois, na conferência anual de hackers DEF Con em Las Vegas, Emick fez um discurso e se revelou como cofundadora da Backtrace.

– Fiquei tão fula de raiva [com Emick] – disse Laurelai após assistir ao vídeo do discurso de Emick no YouTube. – Acredite em mim; penso nisso todos os dias.

Em outubro daquele ano, François Paget, analista da McAfee, gigante digital em TI, faria um estudo sobre o Anonymous e a eficácia de tentativas investigativas por gente como os membros da Backtrace, Aaron Barr e The Jester, que saiu da toca no fim de dezembro para desmascarar pessoas da Operação Vingança. Sua conclusão foi que essas tentativas eram amplamente malsucedidas, até mesmo um estorvo para a polícia. Na época de seu estudo, grupos antiAnonymous como o Backtrace tinham publicado cerca de 230 nomes de pseudônimos, enquanto a polícia mundo afora (com exceção da Turquia) fizera 130 prisões. Nessas prisões, a polícia chegou a mais trinta nomes, e dificilmente havia alguma sobreposição entre os nomes liberados pelos doxeadores vigilantes e aqueles

descobertos pelas autoridades. Paget escreveu: – Imagino que eles mais confundiam do que ajudavam.

Às vezes, porém, era preciso apenas um nome certo. Poucas semanas depois de a Backtrace publicar a lista, o FBI entrou em contato com Emick e pediu seu auxílio na investigação. Estavam interessados no nome que ela havia descoberto para Sabu, mas precisavam corroborar suas provas com as dela, para ver se este Hector Monsegur era definitivamente o sujeito certo. O que Emick tinha descoberto até então não bastaria para resultar numa prisão, e o FBI queria se assegurar de que o verdadeiro Sabu não fosse afugentado. Ele poderia mostrar-se útil.

Nesse meio-tempo, os hackers do ataque contra a HBGary tinham algumas decisões difíceis a tomar sobre como lidar com o caso Backtrace.

Previram (corretamente) que mais tarde apareceriam novos grupos tentando superar o trabalho de Emick, da mesma forma como ela tentara superar o de Barr. Se eles realmente quisessem evitar as algemas, Topiary e os demais precisavam planejar seus próximos passos com muito cuidado.

CAPÍTULO 15

Dando um tempo

No Anonymous havia três modos de responder a uma doxeagem: (1) Negar peremptoriamente. Tática comum, mas que nem sempre funcionava. Mesmo se as informações fossem verdadeiras, a maioria das pessoas negava. Também era perigoso. O pior a fazer era declarar honestamente o que havia de certo e de errado nas informações, já que isso colocaria um investigador no caminho certo.

(2) Retornar aos doxeadores e bombardeá-los com um fluxo de informações falsas e teorias da conspiração, fazendo-os pensar que você passou para o lado deles e ao mesmo tempo confundindo a pesquisa que faziam. Foi nessa linha que Sabu agiu. Não muito tempo depois da revelação da Backtrace, Sabu entrou na rede de discussão frequentada ocasionalmente por Emick e os colegas e fingiu oferecer a ela uma conversa particular com a equipe que hackeara a HBGary. Sabu colou todo o conteúdo de suas próprias conversas com Emick ao grupo, mostrando que eles tinham ficado amigos. A equipe caiu na gargalhada.

(3) Não falar nada e sair de cena.

Topiary decidiu que a exposição da Backtrace tinha fornecido a desculpa perfeita para um afastamento do Anonymous. Outra vez, ele sentia o impulso de aprender e experimentar coisas novas. Nos três meses que participara do Anonymous, de dezembro a fevereiro, havia conhecido cada recanto do grupo: desde escrever mensagens de deface, folhetos eletrônicos e comunicados de imprensa até assistir a um botnet derrubar o PayPal.com; desde humilhar um empreiteiro de segurança federal e assistir ao fato se transformar num escândalo internacional envolvendo um importante banco e o WikiLeaks até capitanear uma hackeagem em tempo real da Igreja Batista Westboro.

Embora Topiary tivesse aprendido e experimentado tantas coisas, ele andava inquieto. O Anonymous começava a se tornar entediante. O que começara como uma operação relevante tinha se pulverizado em muitas operações colaterais. O assunto parecia esgotado. Ele não sabia afirmar se estava amadurecendo ou se entediando por ter destruído tanta coisa num período tão curto. E estava cansado pelo fato de as pessoas esperarem que Topiary, Sabu ou Kayla estivessem na vanguarda de tudo.

Topiary tinha abandonado seu emprego de meio período numa loja de bicicletas

e automóveis após se cansar de seu chefe, e inscrevera-se no seguro-desemprego, do qual ele dependia completamente agora. Estava interessado em sair mais de casa e voltar aos estudos. Pensava em se matricular num curso na faculdade local em Lerwick o qual o conduzisse a uma graduação plena em Psicologia. Nesse meio-tempo, as autoridades habitacionais do governo se dispuseram a lhe oferecer um novo lugar para morar na Inglaterra. Em poucos meses, ele planejava se mudar das remotas ilhas Shetland, encontrar um novo emprego e talvez cursar uma faculdade.

Ele não era o único que desejava dar um tempo. Sabu tinha conversado com Topiary sobre o desejo de desaparecer do mapa após o caso Backtrace e deixar a poeira baixar. Até mesmo Tflow recentemente saíra da rede AnonOps. O pequeno grupo formado por eles era a única coisa que Topiary queria levar consigo. Ele não só apreciava sua companhia, mas aprendia com eles. Kayla lhe ensinou como se manter oculto on-line, e Sabu lhe ensinou sobre o que havia de errado no mundo – desde boatos no Anonymous de que o Facebook espionava para a CIA até as práticas corruptas de executivos de segurança cibernética de chapéu branco como Barr. A pressão da Backtrace e de outros inimigos os aproximara e os tornara cada vez mais isolados do restante do Anonymous.

O grupo agora consistia em Topiary, Sabu, Kayla, Tflow, AVunit e, de vez em quando, o hacktivista chamado Q – um supergrupo de elite de Anons. O

AnonOps tinha sido uma reunião da elite no Anonymous; o #InternetFeds, um grupo de elite ainda mais apurado; e o #HQ era o suprassumo disso tudo. A nata da nata, Topiary pensava. Certa vez, Sabu utilizara a expressão *Anons externos* para descrever os sectários do Anonymous nos principais canais de IRC, e agora essas palavras não saíam da cabeça de Topiary.

O grupinho agora se encontrava numa pequena rede de IRC no servidor próprio de Sabu. Raramente entravam no IRC AnonOps, rede que nessa época fervilhava com operadores rabugentos e supostos agentes do FBI disfarçados. Além disso, sua equipe era firmemente unida. Os relacionamentos entre os Anons podiam ser mais importantes que as circunstâncias que os aproximaram quando se tratava de decidir o quão bem-sucedido seria perseguir alvos significativos. Não importava a popularidade de um alvo ou mesmo a facilidade com que ele podia ser atacado. Se um grupo trabalhasse bem junto, tinha maior probabilidade de sucesso em ataques contra alvos externos. Em vez disso, se os membros entrassem em atrito, podiam afoitamente atacar-se entre si, às vezes por meio de uma guerra de

palavras, de doxeagem ou talvez até mesmo tentando desferir ataques de DDoS contra as redes de IRC uns dos outros.

Muito do drama entre as pessoas do Anonymous provinha de disputas por status nas salas de bate-papo interativo. Organizar as coisas na rede era meio como organizar uma empresa em sua sede. Algumas salas, como a da diretoria, eram locais bem conhecidos e designados para a reunião de executivos e o debate de assuntos importantes. Mas com a mesma probabilidade negócios importantes podiam ser entabulados e fechados no banheiro ou no bar local. No IRC isso também acontecia, à exceção de que ali o prédio inteiro permanecia em fluxo constante, com salas criadas do nada e destruídas num piscar de olhos, nas quais você podia decidir quem entrava, quantas pessoas podiam entrar e o tipo de status de conversação que cada participante teria. Nunca existia um canal onde se discutiam todas as coisas importantes e, se tivesse existido, não duraria muito tempo. Os Anons sempre pulavam de uma rede para outra, a fim de impedir vazamentos como os de Laurelai, e os hackers em especial raramente frequentavam os mesmos servidores, canais ou redes por muito tempo, com medo de serem delatados por alguém.

– Às vezes, eu amaldiçoo a quantidade de canais – disse AVunit, membro da equipe de hackers do #HQ.

Em geral, os hackers precisavam manter suas salas secretas por motivos de segurança, e, às vezes, existiam centenas delas flutuando no AnonOps. Claro, isso fazia outros Anons sentirem que havia uma hierarquia e que as operações estavam sendo comandadas por trás de portas fechadas.

(Premissa não completamente equivocada.) Adicionar um modo +i ou apenas para convidados num canal como o #InternetFeds era como balançar uma bandeira vermelha diante de um touro.

– Faz as pessoas pensarem as coisas mais bizarras – comentou AVunit, referindo-se à curiosidade sobre o que realmente acontecia.

E, apesar do nome #HQ, o canal não funcionava como quartel-general (*headquarter*) para todo o Anonymous. Era apenas um nome que alguém escolhera por simples capricho. Criar um canal era como fazer um café para todos no grupo. As pessoas se revezavam.

Havia modos diferentes de entrar nos canais secretos. Uma ideia de Aaron Barr

tinha sido infectar o programa LOIC e, a partir daí, com um novo nickname, utilizar a infecção para se inserir em canais de código privado. E você podia participar de canais múltiplos ao mesmo tempo. Em meados de março, o próprio Topiary frequentava 23 diferentes canais do AnonOps, inclusive Command, OpMetalGear, OpNewBlood (para treinar novos Anons) e StarFleetHQ, o canal que sediava um imenso botnet pertencente ao operador Ryan do AnonOps. Tflow participava de mais de cinquenta. As pessoas fingiam ser outro alguém, mas muitas vezes isso não funcionava, pois os nicknames eram registrados com senha.

Uma série de símbolos (~, &, @, % e +), cada um deles correspondendo a um dos cinco níveis de status, mostrava o status e o poder de cada pessoa em cada canal. Esses níveis de status eram conhecidos como proprietário do canal, superoperador, operador administrativo, semioperador e voz. A visão desses ícones aparentemente inócuos podia significar tudo para quem costumava frequentar o IRC, pois indicava o que era permitido fazer.

Se você fosse um operador (% ou acima), poderia calar a maioria dos usuários sem símbolo teclando +m. Alguém com % podia expulsar qualquer pessoa abaixo de seu status. Com @ você podia editar um tópico de canal e banir pessoas, enquanto & podia banir um usuário ao bel-prazer.

A ideia por trás disso tudo era garantir que os canais de IRC não se transformassem num festival de spam. Infelizmente, o poder muitas vezes subia à cabeça das pessoas, e os operadores brigavam com participantes de quem não gostavam e os expulsavam. A capacidade de ameaçar com banimentos permanentes lhes dava poder para eliminar operações inteiras caso desejassem.

No, o nome da operadora do sexo feminino que havia dito aos novos Anons que o uso do LOIC era legal e tranquilo, tornou-se conhecida por habitualmente expulsar usuários do canal informal #lounge se eles estivessem fazendo muito spam. Não ficava claro se ela fazia isso só para se divertir ou porque genuinamente tentava manter a paz. Não era necessário ter servidores próprios ou habilidades técnicas para virar um operador de IRC no Anonymous. Corria o boato de que No obtivera seu status flertando com outros operadores do sexo masculino.

Muitos Anons odiavam ou temiam os operadores de IRC – eles eram como chefes que não mereciam o cargo de chefia. E os operadores podiam se safar

dizendo à polícia que não faziam parte do Anonymous. A polícia visitou a casa de No em Las Vegas às seis da manhã em fevereiro. Mercedes Renee Haefer, na época com dezenove anos, abriu a porta vestindo pijama e deparou com policiais de colete e armados. Fizeram uma busca em sua residência, apreenderam dois computadores (um deles um Mac), um iPhone e um roteador, tudo parte de uma varredura do FBI para encontrar pessoas envolvidas na Operação Vingança e no ataque contra o PayPal.

Quando descobriram um folheto eletrônico feito por gozação, que mesclava a foto de sua irmãzinha com imagens revolucionárias, parte de uma piada familiar, eles perguntaram seriíssimos se era uma futura operação do Anonymous. Ela riu e quase disse que sim.

Outros Anons também tinham sido presos, em sua maioria homens na faixa dos vinte e poucos anos. Em 27 de janeiro, cerca de uma semana após o ataque contra a HBGary, a polícia britânica prendeu cinco homens envolvidos nos ataques da Operação Vingança contra MasterCard, Visa e PayPal. Dois deles supostamente eram operadores do AnonOps: Christopher “Nerdo” Weatherhead, um rechonchudo estudante de vinte anos de idade da cidade de Northampton, na Inglaterra, e “Fennic”, um magricela cabeludo de dezessete anos da zona sul de Londres cujo suposto nome verdadeiro não podia ser publicado por motivos jurídicos. Por volta de junho de 2011, pelo menos setenta e nove pessoas em oito países seriam detidas em conexão com as atividades do Anonymous.

Com as notícias sobre essas recentes prisões em janeiro, somadas à persistente doxeagem por pessoas como Emick, a principal preocupação de Topiary deixou de ser o que ia acontecer com o Anonymous se o grupinho dele silenciasse. Outros encontrariam um modo de levar o movimento adiante. Se a rede de IRC entrasse em colapso, eles retornariam aos painéis de imagem. Se alguém fosse preso, outros entrariam. Quase nada havia acontecido com o Anonymous por dois anos até que #savethepiratebay repentinamente se tornou uma bola de neve que levou ao WikiLeaks, e milhares de recém-chegados começaram a vislumbrar uma sólida infraestrutura no Anonymous. Em seguida, a agitação no IRC AnonOps quase arrefecera até que, num passe de mágica, surgiu o ataque contra a HBGary. Muitas vezes era apenas uma questão de circunstâncias – importantes fatos dos noticiários como o WikiLeaks ou um solitário toque de clarim no *b* para combater a Cientologia.

Topiary marcou sua retirada do Anonymous com um plano bem bolado.

Digitou um registro de IRC com um bate-papo falso entre dois amigos comentando como Topiary havia sido preso e depois se assegurou de que o trecho fosse passado adiante até várias pessoas caírem na história.

<contact> tenho de falar com... alguém... você é o Q?

<marduk> lol. depende. e você quem é?

<contact> me disseram para entrar no anonops e falar com Q ou Tflow. alguém que você conhece me deu um contato de emergência. você deve conhecer esse cara, o topiary <marduk> top? faz um tempinho que ele não dá as caras <contact> eu o conheço na vida real. moro perto dele. houve uma confusão nas imediações da casa dele. uma aglomeração de pessoas e veículos. depois não vi mais ele <marduk> não foi a polícia, foi?

<contact> não sei, mas acho que não.

O registro completamente falso era longo e cheio de erros de digitação, perguntas ineptas do "contact" sobre o AnonOps para dar a impressão de que ele não conhecia a rede, junto com um saudável ceticismo da parte de Marduk. O propósito era fazer o "amigo" soar assustado, mas nunca forçar a ideia de que Topiary tinha realmente sido preso. Se ele deixasse lacunas suficientes, outras pessoas tratariam de espalhar o boato.

Topiary vazou o registro para cinco indivíduos confiáveis, assegurando-se de que cada versão fosse um pouco diferente – um sinal de pontuação extra ou uma pequenina diferença na ortografia. Se o registro um dia vazasse para uma associação como a Backtrace, ele seria capaz de identificar quem havia sido o responsável. Topiary mudou seu nickname para Slevin e, com o coração meio dividido, reduziu seus contatos no Skype para três pessoas não identificadas.

***

Em meio ao tilintar da louça, Jake colocou os pratos na pia, inclusive uma travessa coberta de farelos de uma torta de peixe recém-consumida por ele. Ainda frequentador assíduo do painel "gastronômico" do 4chan, ele apreciava cozinhar as próprias refeições, em especial tortas de peixe ou de carne. Abrindo a torneira, ele relanceou o olhar janela da cozinha afora e avistou um furgão da polícia estacionado na rua, algumas casas adiante. Seu coração disparou. Rapidamente voltou a seu laptop e contou ao seu grupinho o que estava rolando.

– Volto em 15 – explicou para AVunit com seu novo nickname, Slevin.

Não conseguiria manter o nome por muito tempo; simplesmente não era conhecido por ele.

– Boa sorte e fique seguro, Top.

Quando Jake desconectou dos canais de IRC e vestiu o casaco, o camburão tinha desaparecido. Dia ensolarado, gélido e revigorante, com a brisa costumeira carregando os aromáticos meios-tons do mar salgado.

Jake colocou seus fones de ouvido e fez uma caminhada de vinte minutos pela cidade, cabisbaixo como sempre, ombros levemente caídos. Correu o olhar em volta tentando vislumbrar a viatura de polícia. Nem sinal.

Rumou a um bar e restaurante perto de uma colina. Resplandecente com cadeiras de couro, mesas de madeira e iluminação indireta, provavelmente era o mais moderno ponto gastronômico da cidade.

Encomendou um latte para viagem e subiu ao topo da colina a fim de sentar-se em seu habitual local de meditação na relva bem cortada, onde podia beber e admirar a paisagem. Perto dele havia um punhado de canhões de ferro pretos, utilizados gerações atrás para abrir rombos no casco dos navios dos saqueadores que tentavam invadir Shetland. Agora não passavam de relíquias silenciosas, os cascos envernizados com tinta protetora. Ele poderia ter sentado num deles, mas de certo modo isso lhe pareceu desrespeitoso.

Caminhou de volta para casa. Nem sinal do veículo da polícia.

Provavelmente tinham ido lá conferir os drogados locais. Jake morava num bairro pobre, e os vários usuários de heroína das redondezas em geral tocavam música em volume alto. Um habitante do sexo masculino certa vez de tão alucinado pendurara um pesado tapete no varal, embora estivesse chovendo. Na manhã seguinte, com esforço ele o tirou e o balançou ao redor na tentativa de secá-lo, embora o tapete estivesse definitiva e irremediavelmente encharcado. Quando os drogados se tornavam violentos ou incômodos, Topiary redirecionava a conexão wireless deles, de modo que cada clique remetesse ao site de surpresas Goatse, e depois renomeava a conexão Wi-Fi para heroína-escondida-no-porão. No ano passado, o máximo que tinham feito era jogar uma lata de cerveja no gramado frontal de sua casa.

Jake voltou para casa e ligou o laptop. Entrou on-line e deparou com uma manchete sobre o Anonymous. Parecia que o grupo acabava de declarar guerra contra a Sony, um alvo colossal. Dessa vez, ele não tinha nem ideia de quem comandava o ataque, e se sentiu confortável com essa situação, até mesmo mais feliz por já ter se afastado de tudo.

***

Era 1º de abril, e alguns Anons tinham publicado um novo folheto digital, onde se lia: “Parabéns, Sony. Agora você recebeu a atenção completa do Anonymous”.

Nessa ocasião, enquanto Topiary se encontrava “ausente sem licença”, o vigilante do 4chan William tinha embarcado no ataque com ímpeto; seu principal papel foi ajudar a doxear os executivos da Sony e suas famílias, como parte de uma operação colateral chamada SonyRecon. Tudo isso acontecia porque, no começo daquela estação, a Sony havia processado um hacker chamado George “Geohotz” Hotz, após ele ter descoberto como desbloquear o até então impenetrável console do PlayStation 2 e depois anunciar em seu blog como as pessoas podiam baixar, gratuitamente, jogos em seus próprios sistemas. Com 21 anos na época, Geohotz já era bem conhecido por desbloquear o iPhone e o iPad da Apple. Agora a Sony o acusava de violar a Lei contra a Fraude e o Abuso do Uso de Computadores, por ter hackeado o console do PlayStation.

Ao longo dos dias seguintes, os Anons que tinham baixado o LOIC

lançaram um ataque de DDoS contra vários sites da Sony e sua rede para gamers PlayStation Network (PSN). A PlayStation Network então saiu do ar, irritando milhões de gamers mundo afora.

William, que em geral encarava com ceticismo os ataques de maior amplitude do Anonymous, sentiu-se inspirado por esse ataque específico e pela operação colateral na qual participava. A equipe dele já havia arrancado informações sobre vários executivos da Sony e suas famílias, inclusive o diretor executivo da Sony, Howard Stringer, e seus filhos adultos.

– Este é o ataque mais focado até hoje – entusiasmou-se em uma entrevista na época. – Os engenheiros sociais sabem sua função e os hackers também. Esta é uma das poucas vezes que vou fazer parte da equipe, sabendo EXATAMENTE qual o meu papel nela.

Ele concluiu dizendo que a Sony havia tratado Geohotz (“um dos nossos”) de um modo que era contra a liberdade, contra a expressão, contra o individualismo e, portanto, “contra o Anonymous”.

William não se importava com a existência de óbvias camadas no Anonymous, com hackers e redatores no topo e engenheiros sociais e usuários de LOIC perto da base. Cada categoria se aproveitava da reputação da outra – William assustava seus alvos alegando ser um hacker, e os hackers podiam se aproveitar da infâmia do Anonymous devido ao fato de pessoas menos capacitadas mencionarem o nome por aí.

Os ataques de DDoS contra a Sony continuaram por diversos dias e se tornaram tão malquistos que, pouco antes de 7 de abril, o Anonymous anunciou o fim deles.

“O Anonymous não está atacando a PSN desta vez”, afirmava um comunicado de imprensa. “Percebemos que atacar a rede do PlayStation não é uma boa ideia. Por isso, temporariamente suspendemos nossas ações, até encontrarmos um método que não cause impactos tão graves aos clientes da Sony.”

Estranhamente, porém, a PlayStation Network permaneceu fora do ar, e os gamers ficaram ensandecidos. Em 22 de abril, o Anonymous postou um novo comunicado de imprensa no AnonNews.org, intitulado: “Desta vez, não fomos nós”. A rede já estava fora do ar há quase três semanas agora, e claramente isso não acontecia devido a um ataque de DDoS em andamento.

Não menos estranho, a própria Sony não se manifestou durante várias semanas. Enfim, em 2 de maio, a empresa fez um comunicado espantoso.

Teria acontecido uma “invasão” em sua rede em algum momento entre 17 e 19 de abril. Os hackers haviam comprometido dados pessoais e financeiros de mais de 75 milhões de contas da PlayStation Network, hackeagem que afetava dezenas de milhões de pessoas. Ninguém no Anonymous assumia a responsabilidade, e ninguém no AnonOps parecia saber quem tinha roubado todos esses dados de usuários. No entanto, por volta do fim do mês, a Sony havia gastado 171 milhões de dólares tentando consertar a falha de segurança e, poucos meses depois, os órgãos de comunicação noticiavam que os custos afins arcados pela Sony em decorrência da falha superavam 1 bilhão de dólares.

Em seguida, a Sony escreveu uma carta explicativa ao Congresso Nacional dos

EUA. Os criminosos cibernéticos, dizia a empresa, tinham deixado um arquivo com a marca “Anonymous” e “Somos legião” no sistema. Podia ser um cartão de visitas ou uma tentativa dos hackers criminosos para lançar a polícia numa pista errada, mas, seja como for, a notícia rapidamente removeu qualquer legitimidade pública que o Anonymous granjeara com os protestos a favor do WikiLeaks e dos países do Oriente Médio, bem como com as informações reveladas durante os ataques contra a HBGary.

Num primeiro momento, muitos Anons apreciaram a ideia de que hackers tinham causado danos tão drásticos à Sony – mas o gosto era agridoce. Ninguém sabia quem tinha levado a cabo o ataque, e não houve declaração oficial do Anonymous – apenas um estranho arquivo deixado em segredo. O caso inteiro transmitia uma sensação de desonra.

Para piorar a situação, o AnonOps logo teve problemas internos para resolver, à medida que começou a correr o boato sobre um importante vazamento na rede. Um operador trapaceiro publicara uma lista de 653

nicknames e seus endereços IP, a série de números que, se revelada, podia levar a polícia, os trolls da internet e qualquer um que soubesse como usar o Google direto à porta desses indivíduos. Novamente os neófitos, não os hackers verdadeiros, corriam o risco maior.

Quase de imediato, o IRC AnonOps tornou-se uma cidade fantasma. As centenas de participantes habituais que frequentavam a lista ficaram muito assustadas para reaparecer. Alguns bateram em retirada para outras redes de IRC, como a EFnet e a Freenode, enquanto outros continuaram a conversar em blogs e fóruns. O Anonymous subitamente viveu uma diáspora e ficou sem ponto de encontro.

Ex-administradores do AnonOps, incluindo Owen, Shitstorm, Blergh e Nerdo, publicaram um comunicado oficial dizendo que estavam “profundamente entristecidos com esse drama”, e instavam os visitantes a ficarem afastados dos servidores do IRC AnonOps.

Dois dias depois, o nome do culpado enfim emergiu. Ryan tinha sido um operador de IRC que utilizava seus servidores para hospedar dois sites populares para sectários do Anonymous. Ele era conhecido como um temperamental administrador de web que se divertia hospedando milhares de pessoas em seus servidores. Também ganhou fama como o sujeito que contara a Topiary sobre

falsificar o número da colmeia LOIC, em janeiro.

Sem falar que era uma das raras pessoas que controlava um grande botnet.

Consideravam Ryan uma espécie de canhão independente, e, à medida que os conflitos com os operadores da rede se acirraram, ele passou a se comportar de modo antissocial.

Ryan devia ter esperado repercussões, e elas vieram quando alguém trouxe à luz seus dados da vida real. Ryan tinha supostamente implorado a Sabu que impedisse a publicação de seus dados. Quando viu que isso não resultaria em nada, utilizou seu botnet para lançar um ataque de DDoS

contra a rede do AnonOps e vários outros sites relacionados ao Anonymous. Mesmo assim, em 11 de maio, o nome completo de Ryan foi publicado on-line, junto com seu endereço residencial em Essex, Grã-

Bretanha, idade, número do telefone celular, nome no Skype e o e-mail associado com sua conta no PayPal – todos apresentados numa simples página da web com fundo preto. O doxeador tinha listado seu nome completo corretamente: Ryan Cleary. No alto do documento, lia-se: “Doxeado por Evo”, acrescentando: “Viva Kayla, Sabu, Owen, #krack, #tr0ll e todos os AnonOps”. Evo frequentava a rede de IRC de Kayla, #tr0ll. Como alguns órgãos de comunicação relataram uma “guerra civil” no Anonymous, Ryan negou a veracidade dos dados, alegando num bate--papo da rede se tratar de dados falsos publicados por ele três anos antes.

O Anonymous começava a parecer uma piada. A Operação Sony tinha sido cancelada e em seguida aparentemente sequestrada por hackers que tentaram usar o movimento para acobertar seus atos. E agora um ex-operador do AnonOps havia se voltado contra a rede também. Ninguém mais se interessava em ataques e operações, apenas em fofoca, política e defesa da razão de existência do Anonymous.

– A Sony e Ryan podem ter significado o fim de um alucinante passeio de montanha-russa – observou Topiary na época.

Mas, embora ele estivesse feliz por dar um tempo e afastar--se do drama em andamento, ele também tinha voltado a conversar com Sabu.

Não conseguiu evitar o impulso de reviver o turbilhão de experiências do começo do ano. Se reunissem os hackers da operação HBGary novamente, eles podiam mostrar ao Anonymous algo novo, que não apenas inspirasse as pessoas, mas as deixasse boquiabertas.

CAPÍTULO 16

Falando sobre uma revolução Distanciar-se do Anonymous, para Jake, significava realizar coisas na vida real. A casa nunca estivera tão limpa. No lado esquerdo de sua escrivaninha, havia um amplo mural com tarefas a fazer e um calendário.

Um monitor de 38 polegadas suplementava seu laptop. O sofá na sala estava limpo e, perto dele, cabos bem organizados passavam sob a mesa.

Em cima dela, uma pilha de livros sobre psicologia, junto com um romance de James Patterson sobre feitiçaria chamado *The Gift* (no Brasil, *O Dom*). Ele tinha tempo para passar as roupas adequadamente, e acabar com as pregas que lhe davam a sensação de vestir papel amarrotado. Penduradas num varal portátil, algumas de suas roupas secavam com o calor de uma estufa a um palmo de distância. Apesar da primavera, fazia um frio intenso lá fora.

A faculdade local tinha gostado de sua solicitação para fazer um curso preliminar de Psicologia e o aceitara imediatamente. Fora do sistema educacional há quatro anos, Jake esperava ansioso pela caminhada puxada de vinte e cinco minutos até a universidade, e afastava as preocupações de que alguém na sala de aula pudesse reconhecer sua voz a partir do vídeo da Igreja Westboro. Sempre soubera que o Anonymous era instável, e não queria ofuscar sua primeira participação real na faculdade. Com economias que alcançavam cerca de setecentas libras na conta bancária que raramente tocava, ele inclusive havia começado a se permitir um jantar todas as terças-feiras no Gurkha, que considerava o melhor restaurante indiano da ilha. O caril de Madras com frango, completo com batatas fritas, pão nan de alho e cerveja Gurkha, custava 13,75 libras (21,8 dólares), mas ele sempre pagava com uma cédula de 20 libras e não pedia troco. Gostava dos garçons e do modo como eles conversavam cordialmente sobre suas vidas e o escaldante sol indiano, enquanto o gélido vento de Shetland soprava lá fora. O interior do restaurante lhe servia de refúgio, ornamentado com decoração asiática e com uma relaxante cítara tocando no

ambiente. Jake em geral se sentava sozinho e ficava ali matutando. Ao longo dos meses seguintes, à medida que ele voltava a ficar ocupado, visitaria o Ghurka mais de vinte vezes como forma de terapia, uma oportunidade para descansar a cabeça antes de subir a colina até sua porta e abri-la para deparar com linhas de texto freneticamente se movendo tela acima em seu laptop aberto.

Kayla, Tflow, AVunit e Q também tinham dado um tempo e se afastado do Anonymous, deixando apenas Jake (com o codinome de Topiary) e Sabu na sala de bate-papo privada do grupo. Tempos depois, Sabu explicaria que os outros haviam saído porque tinham “se assustado”, e ele e Topiary permaneceram juntos em sua “própria ilhota”.

Às vezes, os dois conversavam horas a fio diariamente, entre seus afazeres cotidianos. Passaram a se conhecer melhor. Topiary nunca ousava perguntar a Sabu o que ele fizera no passado, mas o hacker mais velho contava assim mesmo. Ele contou histórias sobre hackear o governo de Porto Rico, sobre a guerra cibernética com hackers chineses, sobre sua farra de deface, sobre se esconder nos subterrâneos e sobre por que ele resolveu apoiar o Anonymous no dezembro prévio. Topiary se maravilhou com o ímpeto implacável de Sabu para se tornar um hacktivista após incríveis onze anos e com seus extensos monólogos sobre a recusa em aceitar uma sociedade autoritária. Até mesmo quando Sabu estava cansado após um longo dia de trabalho e tarefas familiares, ele se empolgava toda vez que o assunto recaía em política e sociedade.

Embora Sabu amasse tecnologia e hackeagem, parecia que seu coração pulsava por mudanças sociopolíticas. No mundo real, Hector Monsegur provinha da cidade de Nova York, estivera envolvido em lutas corporais com outros homens e até mesmo cumprira um tempo na cadeia. Tinha profundo ressentimento de pessoas que abusavam de posições de autoridade, mostrando um desdém especial por empresas de seguranças de TI de chapéu branco e policiais corruptos. Desde a adolescência e quando jovem adulto, ele habitualmente era parado e revistado pela polícia, sensação não muito diferente daquela vez em que o chefe de segurança da escola de ensino médio apreendera sua chave de fenda.

Monsegur alegou numa entrevista que, no começo de 2011, dois policiais, um afro-americano e outro com raízes na República Dominicana, tinham parado seu carro enquanto ele dirigia numa parte rica da cidade.

Um dos guardas chegou perto de seu vidro lateral e o acusou de passar o sinal vermelho. Monsegur suspeitou que fosse mais provável ter sido abordado por não se adequar ao ambiente local. O guarda solicitou sua carteira de motorista e os documentos do veículo, depois o interpelou sobre o que ele fazia ali. Monsegur mostrou os documentos. Em seguida, foi orientado a sair do veículo.

– O que houve? – indagou.

– Só vá até a parte traseira do carro – pediu o policial.

Monsegur obedeceu e, ao chegar perto do porta-malas, o segundo policial o algemou.

– O que está acontecendo? – gritou Monsegur enquanto era colocado na viatura policial. – Tenho família. Por que estão me algemando?

– Você se encaixa na descrição de alguém que estamos procurando – contou enfim um dos policiais.

– Ok. Está certo – falou Monsegur, tentando se acalmar. – Me passem a descrição.

Os policiais hesitaram a princípio, mas enfim descreveram um homem que, embora um tanto parecido com Monsegur, apresentava diferenças em características como altura, data de nascimento, cor de cabelo e tom de pele. Por fim os policiais mostraram a ele uma foto do suspeito.

– Ei, olha só – falou após examinar a foto. – Me observem. Somos diferentes em tudo. Ele tem tatuagens no pescoço. Eu uso cabelo curto.

Súbito se voltou para o guarda dominicano e perguntou em espanhol por que estava sendo preso.

– Vocês são um pouco parecidos – respondeu o guarda em inglês.

– Mas... cadê as tatuagens? – indagou Monsegur fitando o guarda.

– Você pode ter mandado removê-las.

Monsegur revirou os olhos e se deixou recostar no banco, com a cabeça quente.

Ele tinha tatuagens mesmo, mas nada no pescoço. Enquanto o levavam embora, escutou um dos policiais falando pelo rádio com a delegacia: estavam levando um “garoto” que combinava com a descrição do suspeito. Uma voz desincorporada e crepitante, lá da base, solicitou detalhes para saber se as características realmente combinavam. Assim que um dos guardas mencionou a altura e a idade de Monsegur, a voz indagou por que eles o estavam trazendo. Os guardas se entreolharam.

– Soltem-no imediatamente – continuou a voz.

Os dois deram de ombros e fizeram o carro dar meia-volta.

Monsegur soltou um suspiro de alívio. Enquanto estacionavam perto do carro dele, percebeu que seus faróis e o rádio tinham ficado acesos. A bateria estava morta, e ele encalhado às dez horas da noite.

Foi uma experiência especialmente enlouquecedora, mas longe de ser a única. Monsegur afirma que estava acostumado a caminhar na rua e ser parado, revistado, com a frase “Você combina com a descrição” ecoando em seus ouvidos. Crescendo no Lower East Side nos anos 1990, ele presenciara os efeitos da ordem do prefeito Giuliani ao Departamento de Polícia de Nova York para concentrar suas ações em bairros com alto índice de consumo de drogas. Com o recente aumento de impostos usado para contratar cerca de 3 mil novos policiais a fim de patrulhar as ruas, o efetivo policial do NYPD alcançou 40 mil guardas. Monsegur os encarava como a principal gangue da cidade, patifes autoritários que faziam os cidadãos como ele se sentirem semelhantes a animais. Ele queria mudar isso. Além de sua ânsia por reconhecimento e respeito como hacker habilidoso, ele queria que as pessoas tais quais ele, criadas em conjuntos habitacionais, soubessem seus direitos.

Monsegur não vinha de uma família de ativistas políticos, mas a hackeagem lhe fornecera uma voz. Passou a ser observado. Invadir bancos de dados e interromper servidores era um modo de subverter os poderes corruptos do mundo moderno. À medida que foi ficando mais velho, ele se tornou mais desencantado com o mundo a seu redor e mais temperamental quando ele próprio se tornava alvo de críticas. Talvez de modo significativo, não havia nada que ele odiasse mais do que ser chamado de delator.

Mas o desencanto foi esquecido por um tempo, quando a Operação Vingança

surgiu no final de 2010. Ficou tão empolgado com o potencial da operação que não teve como deixar de inflar a importância do Anonymous e, depois, sua própria relevância no grupo.

– Concedemos aos policiais dos EUA o poder de atirar em nós e se safar com isso. Agora o Anonymous pode se rebelar contra essa ameaça – falou ele numa entrevista em abril de 2011. – O mundo permitiu que ditaduras e tiranos permanecessem incontestados. Agora, organizações como o Anonymous podem fazer essas contestações.

Sabu acreditava que o maior poder do Anonymous era sua falta de hierarquia. Ele indicava um programa de contrainteligência do governo dos EUA nas décadas de 1960 e 1970 chamado Cointelpro, que viu o FBI silenciosamente subverter organizações ativistas e políticas. Eles tinham utilizado táticas similares às da HBGary, de subterfúgio e desinformação, para erodir o poder das organizações desde os Panteras Negras até a porto-riquenha FLN, desde a KKK até gangues mexicanas, muitas vezes com agentes infiltrados. O motivo pelo qual essas organizações minguaram, acreditava Sabu, justificava-se pelo fato de terem uma hierarquia estruturada.

O Anonymous era diferente. Se alguém prendesse Monsegur, haveria outros dez como ele para preencher seu lugar. Ao vazar e-mails ou ajudar usuários da internet do mundo todo a ultrapassar os filtros do governo, o Anonymous podia ajudar pessoas como Julian Assange e seu suposto informante Bradley Manning quando elas fossem presas. Tão logo ficou sabendo sobre a prisão de Assange, Monsegur entrou on-line como Sabu e buscou vulnerabilidades nas redes de organizações relacionadas com o caso de Assange, desde o tribunal que permitiu o mandado contra o rapaz até as pessoas que o acabaram levando para a cadeia. Sabu alegou que sua pesquisa resultou numa riqueza de informações para operações futuras, embora nunca as tenha tornado públicas.

– [É para] uso futuro – contou ele numa entrevista. – Estou certo de que mais cedo ou mais tarde verão meus resultados. Aguardem.

Uma provocação verbal dessas sobre descobrir desonestidades dos promotores que acusavam Assange era típica da persona de Sabu. Insinuar a perspectiva de uma grande operação ou vazamento tornara-se essencial no modo como ele mais tarde atrairia a atenção de outros Anons, como Topiary, e até mesmo de jornais importantes, todos a partir do conforto de seu computador. Na pele de Sabu, ele

muitas vezes fazia afirmações do tipo: – Vem algo grande por aí. Descobri algo. Vocês vão querer ver.

Depois não entrava em detalhes e se calava por várias semanas, e, às vezes, nunca mais retomava o assunto.

Sabu sabia que muitos encaravam o Anonymous como um grupo de trolls canalhas.

– E eu tenho certeza de que certas pessoas querem que a coisa permaneça assim – disse ele.

Até mesmo quando o AnonOps tinha se tornado um caos, Sabu acreditava que os Anons poderiam se reorganizar e mudar o mundo.

– Vive, pensa e respira – disse ele.

Enquanto ele e Topiary refletiam sobre o Anonymous ao longo do mês de abril, os dois se deram conta: o desejo de se afastar era igual ao desejo de permanecer. Para Sabu, tratava-se de ativismo e reconhecimento; para Topiary, de diversão, aprendizado, capacidade de causar agitação. Se Topiary na vida real era socialmente desajeitado, on-line ele se tornara um herói sarcástico. A dupla se perguntava como poderia continuar essas experiências agora que o Anonymous havia se calado.

Numa noite de meados de abril, Sabu falou com Topiary novamente sobre o quanto ele ainda acreditava no Anonymous, mas, ao mesmo tempo, pensava em se ocultar de modo mais permanente. Súbito, sirenes de alarme dispararam na cabeça de Topiary. Algo em relação a isso não soava bem, como se estivessem prestes a deixar escapar algo realmente notável. Ele começou a tentar demover Sabu de se afastar.

– Agora você já está exposto – falou a Sabu.

A equipe deles tinha criado uma tempestade na mídia; em outras palavras, havia atenção e embalo suficientes para trabalhar rumo a esses objetivos, para continuar o movimento hacktivista.

– Se não acontecer agora, não vai acontecer nunca mais – acrescentou.

As palavras calaram fundo em Sabu.

– O momento atual é uma boa oportunidade para agirmos – salientou Topiary. – Temos a atenção, os contatos, temos os servidores do AnonOps funcionando e tudo transcorrendo com tranquilidade. Essa pode ser nossa última chance de fazer a diferença.

Na verdade, Topiary não estava tão interessado em hacktivismo quanto Sabu. Ele apenas apreciava conversar com sua equipe e queria se divertir. O

grupo de elite deles tinha se separado, com Kayla, Tflow e AVunit ainda em suas respectivas folgas de hackeagem. Mas os dois com frequência sentiam falta da antiga harmonia do grupo, e agora Topiary acalentava a ideia de reunir todos novamente. Ele dera um argumento convincente, e Sabu começou a concordar que, embora o seu nome verdadeiro já tivesse sido exposto na web, ele e os outros poderiam fazer algo significativo juntos.

Sabu mais tarde conversou sobre atingir um ponto de não retorno, e pode muito bem ter sido durante essas discussões com Topiary que ele decidiu atravessar a linha e não voltar atrás.

Mais tarde, ele relembrou que a coisa “deu liga” com Topiary quando a conversa recaiu em inspirações e aspirações. Não era que eles subitamente quisessem hackear o planeta.

– Era mais o fato de nós dois acreditarmos no Anonymous. Vamos trabalhar juntos e prosseguir a partir daí. E, é claro, ele [Topiary] gostava da atenção da mídia... Acho que surgiu uma conexão óbvia: eu faço a hackeagem e você lida com a imprensa.

Sabu tinha certa cautela sobre o quão público Topiary podia ser, mas admirava os talentos de oratória e a articulação do companheiro. Isso explica a natureza rara de sua colaboração mútua; embora fossem quase polos opostos em termos de personalidade, de certa forma os dois se complementavam. Sabu parecia apreciar o estilo “tábula rasa” da visão de mundo de Topiary, que resultava numa boa caixa de ressonância para suas críticas contra o sistema. Topiary não tinha uma rusga pessoal contra as empresas de segurança de chapéu branco, mas, após conversas suficientes com Sabu sobre o tópico, ele logo as odiava também.

Sabu também se sentia atraído pela celebridade de Topiary no mundo do IRC

AnonOps. O nickname dele causava auê – se aparecia numa sala de bate-papo, as conversas cessavam e as pessoas o incitavam a falar. Foi esse ponto que mais tarde faria Topiary refletir ao recordar o motivo pelo qual acabou colaborando com Sabu. Não era que Sabu necessariamente o estivesse usando: – Mas com certeza havia um motivo para ele me querer por perto.

Sabu não escondia o jogo sobre isso: – Quando você está numa sala de bate-papo, a galera fica empolgada – falou a Topiary, que não teve outra reação além de sentir-se lisonjeado. E

Sabu também contaria a Topiary que ele era seu "cérebro de raciocínio". A tautologia se referia ao modo como Topiary ajudava Sabu a se acalmar quando ele ficava muito empolgado ou aborrecido com um assunto.

– Eu explicava as coisas – recordou-se Topiary mais tarde. – Eu o orientava sobre qual a maneira de abordar uma operação, em vez de se atirar com o pé no fundo do acelerador. Não libere tudo de uma tacada só.

Libere a conta-gotas.

A HBGary era um exemplo relevante: os e-mails de teaser, as mensagens no Twitter para atrair a atenção da mídia. Haveria muitas ações semelhantes nos meses seguintes.

No período de duas semanas, cada um tinha de algum modo convencido o outro a permanecer na ativa e recrutar o velho time da HBGary novamente. Com seu pequeno grupo, talvez eles pudessem motivar as massas outra vez. Eles poderiam apoiar o Anonymous 100%, mas não precisavam se chamar Anonymous.

– Isso significa que, se a gente quisesse atacar alguma empresa de chapéu branco, a gente não ia estragar a imagem do Anon – declarou Topiary numa entrevista em abril de 2011, enquanto ele e Sabu ainda discutiam a ideia. – Achamos que seria um exagero nos rotularmos de um time de hackers com bandeira cafona, por isso não decidimos muita coisa.

Kayla andava surfando on-line, por isso eles criaram um canal de IRC

chamado #Kayla_se_você_estiver_aqui_entre_neste_canal. Tão logo Kayla voltou, ela mostrou interesse, e os três começaram a fervilhar de ideias.

Uma era estabelecer uma nova rede de IRC para o Anonymous, já que o vazamento de Ryan em abril tinha afugentado centenas de usuários dos canais antigos. Detratores haviam bombardeado a rede com ataques de DDoS e, embora o número de visitantes habituais tivesse minguado, o número de pessoas que se declaravam operadores inchara para quarenta.

Com o AnonOps agora com mais caciques do que índios, reinava o caos em nove diferentes canais de “comando”, canais de cúpula e canais secretos para conversar sobre outros operadores. A rede estava prestes a entrar em colapso devido ao próprio peso, e o Anonymous precisava de um lugar seguro e organizado para se encontrar. Mas, no começo de maio, os operadores do AnonOps concentraram suas forças. Eles reduziram seus servidores de oito para dois, e o número de operadores de quarenta para oito. Uma rede de IRC agora parecia menos necessária.

– Talvez eu tivesse desistido se não tivéssemos conversado tanto e acabado trazendo Kayla de volta – afirmaria Topiary muitos meses depois.

– De certa forma, eu gostaria que Sabu não confiasse tanto em mim.

Em poucos dias, AVunit voltou de sua folga e também se reintegrou ao grupo. Agora havia quatro componentes da antiga equipe interessados em fazer algo grandioso – eles não tinham bem certeza do quê – para voltar a inspirar o Anonymous. Agora era impossível voltar atrás.

***

Certo fim de manhã, durante um período em que os membros da equipe ainda cogitavam o que podiam fazer juntos, Topiary se levantou, pegou seu laptop e viu Sabu on-line, junto com Kayla. Devia ser umas cinco da madrugada em Nova York.

– Pessoal, varei a noite procurando sites alvos – disse Sabu. – E

encontrei este grande site do FBI. – A respiração de Topiary se acelerou instantaneamente. – Obtive acesso a ele – acrescentou.

Sabu então colou uma extensa lista de cerca de noventa nomes de usuário (número que representava metade da base de usuários do site) e hashes criptografados (que correspondiam às senhas de cada um) de um site chamado

Infragard. Topiary e Kayla imediatamente começaram a tentar decodificá-los, empolgados com a perspectiva de “hackear o FBI”.

Poucos minutos depois, Topiary digitou Infragard no Google e deu-se conta de que estavam lidando com uma afiliada sem fins lucrativos do FBI, não com a própria organização. Por um átimo pensou em indagar a Sabu como ele havia descoberto a brecha de segurança ou em salientar que não se tratava exatamente de um “grande site do FBI”. Mas ele não queria jogar um balde de água fria na empolgação da equipe.

Todos os usuários tinham sido verificados pelo FBI para obter acesso e todos trabalhavam no ramo de segurança; alguns inclusive como agentes do FBI. No entanto, suas escolhas de senhas eram, na melhor das hipóteses, questionáveis. Um dos usuários tinha utilizado “shithead” como senha para todas as contas on-line; outro escolhera “security1”. Só 25% deles usavam senhas que eles não conseguiram decodificar. Representa uma regra geral em TI que é fraca toda e qualquer senha que não for uma combinação de letras, números

e

símbolos.

Não

é

tão

difícil

memorizar

“###Crack55##@@” ou “esta é uma senha 666”, mas essas duas seriam extremamente difíceis de decodificar. (As senhas mais difíceis de decifrar são frases, também mais fáceis de serem memorizadas pelos titulares.) Após alguém ter baixado a base de dados inteira de usuários e depois convertê-la num arquivo de texto simples, Sabu carregou os 25% de hashes das senhas que a equipe não havia conseguido decodificar no serviço de quebra de senha “não pergunte, não diga” utilizado por ele no ataque à HBGary Federal, o HashKiller.com. Às vezes os pirralhos utilizavam o site para enviar mensagens criptografadas uns aos

outros, com o desafio de decodificá-las. Quando hackers nefandos invadiam a base de usuários de um site, em geral carregavam todos os assim chamados hashes MD5 numa base de dados e começavam a quebrar os mais fáceis primeiro, depois deixavam que os usuários do HashKiller terminassem o serviço.

Um hash MD5 era um idioma críptico que correspondia a palavras ou arquivos, com a seguinte aparência típica:

11dac30c3ead3482f98ccf70675810c7

Essa série específica de letras e números é traduzida como “parmy”, então o resultado no site seria: **11dac30c3ead3482f98ccf70675810c7:parmy** Em seguida essa informação seria armazenada na base de dados do HashKiller, de modo que, se alguém tentasse quebrar a senha “parmy” e tivesse o hash MD5, conseguiria fazê-lo de modo instantâneo. O resultado do HashKiller.com teria a seguinte aparência: **Quebrando hash: 11dac30c3ead3482f98ccf70675810c7**

Buscando hash...

Texto decodificado de 11dac30c3ead3482f98ccf70675810c7 é parmy Simples assim. Por esse motivo, é uma péssima ideia utilizar senhas de palavras únicas, como “parmy” ou – pior ainda, porque é de uso comum – “shithead”. Cada senha sempre tem o mesmo hash MD5. E tão logo esse hash estivesse no HashKiller.com, todo mundo o conheceria. Uma falta de contexto mantinha as coisas relativamente secretas: todos podiam ver os hashes e as senhas decodificadas em texto sem formatação, mas nada além.

A utilização do site era gratuita, e Sabu só precisava se recostar na cadeira e esperar que as senhas fossem quebradas por voluntários.

Tão logo alguém quebrou a senha do administrador, a surpreendentemente fácil “st33r!NG”, Sabu criou uma página da web que ele secretamente anexou ao site da Infragard Atlanta, conhecida como site shell. Era o mesmo tipo de página que os administradores do site utilizavam para controlar seu conteúdo, permitindo-lhes acrescentar novas páginas ou excluir outras. A diferença era que os administradores não sabiam absolutamente nada sobre a página de Sabu. Já que a página do painel de controle original era xootsmaster, Sabu batizou sua página shell de /xOOPS.php. Ele poderia simplesmente entrar no painel de controle principal, pois tinha a senha certa, mas isso significaria clicar em uma série de opções e uma extensa lista de diretórios. A página shell tinha um projeto mais simples que tornava mais ágil e mais fácil causar bagunça.

A equipe espreitou o site por mais algumas semanas, encontrando na completa base de nomes de usuário e senhas: 25 mil e-mails de contas pessoas dos usuários do site, mescla de consultores de segurança e agentes do FBI. Topiary e seus amigos tinham todas as senhas, nomes completos e e-mails. Se Topiary tivesse sido mal-intencionado, ele poderia ter feito logon nas contas do PayPal de um dos usuários de alto escalão e começado a espalhar dinheiro por todos os lugares.

– Isso seria ruim – falou ele na época.

Eles tinham acesso que poderia levá-los a desfigurar o site em segundos, mas resolveram aguardar. A equipe ainda sentia a pressão da HBGary, dos vazamentos do conteúdo do #HQ e da Backtrace, e ainda não tinha bem certeza

em que estava se transformando. Assim, eles combinaram de espiar as contas dos usuários no Gmail, apenas observando o desenrolar das mensagens. Nada especialmente significativo estava sendo discutido, mas o grupo decidiu que, se um deles fosse preso, eles publicariam tudo.

– As hackeagens mais profissionais e de alto nível nunca são detectadas – disse meses mais tarde um hacker do Anonymous que passou a auxiliar a equipe de Sabu e Topiary.

Não muito tempo após a invasão da Infragard, outro grupo de hackers invadiu a rede de computadores do parlamento japonês, roubando informações de logon e e-mails. Só três meses depois alguém percebeu o que acontecera. A hackeagem envolvera a infecção de computadores com um vírus, mais provavelmente pela remessa aos funcionários de e-mails infectados com Trojans. Esse era o modo de atuação de script kiddies, desdenhou o hacker do Anonymous. Método barulhento, batido e que não exigia muita perícia.

Bisbilhotar passivamente sem ninguém saber sempre fazia sentido. Era possível furtar uma base de dados, enviá-la a spammers e fazer outras práticas para levantar dinheiro. Com o Anonymous, também existia aquela obrigação de causar furor. Mas isso dependia de quem você tinha hackeado.

Esse hacker do Anon alegou que, ao invadir uma rede, na maior parte do tempo agia “passivamente”. Certa vez, por exemplo, ele e outra equipe encontraram uma brecha num grande servidor de um governo estrangeiro a qual conduzia a dados de diversos hospitais. A equipe não os publicou; em vez disso, notificou a administração sobre o problema. Até mesmo apagaram sua própria cópia dos dados, já que a liberação das informações seria “contraproducente”. Mas naquela mesma invasão também encontraram um servidor administrativo do mesmo governo estrangeiro, com todas as categorias IP de seus serviços on-line.

– Com certeza publicamos isso – contou ele.

O paradoxo para os hackers que se tornaram parte do Anonymous era que subitamente havia um motivo para trazer à tona seus vazamentos, com o objetivo de provar uma teoria. Com a Infragard, Sabu, Kayla e Topiary adotavam a rota de bisbilhotar passivamente. O que o grupo fez com essas informações os diferenciaria de outros hackers que agiam por dinheiro, curiosidade ou uma sensação de conquista pessoal. Eles só precisavam do momento exato.

CAPÍTULO 17

Lulz Security

Logo ficou claro para Sabu, Topiary e Kayla o que eles realmente estavam discutindo: a criação de uma nova equipe de hackers. Seria, de certa forma, como o WikiLeaks. Publicaria informações sigilosas que não tinham sido vazadas, mas roubadas. A ideia não soava tão nerd quanto Topiary tinha pensado meses atrás.

Eles decidiram com unanimidade que não queriam ser limitados pelos amplos princípios subjacentes ao Anonymous, que eram: 1. escolher alvos porque eles eram opressores da liberdade de expressão;

2. não atacar a mídia.

A ideia era fazer o que fosse necessário para inspirar o Anonymous com novo lulz e, talvez, atrair os holofotes novamente. Na cabeça de Topiary, isso levaria a algo bem mais grandioso do que qualquer trote que ele já havia aplicado. A ideia toda de lulz não agradava muito a Sabu, mais interessado em hackear como forma de protesto. Mas ele percebeu que o Anonymous precisava de alguma inspiração e imaginou que podia direcionar Topiary e os demais rumo a propósitos mais sérios. Kayla apenas estava contente pela oportunidade de bulir na internet outra vez, e, já que eles precisavam de mais alvos além do site da Infragard, ela começou a procurar furos de segurança ocultos da web, da mesma forma como secretamente fizera para o q do WikiLeaks.

Kayla tinha um poderoso script da web que lhe permitia esquadrinhar sites da internet em busca de vulnerabilidades. Esse processo automático de busca por furos de segurança em muitos sites diferentes ao mesmo tempo chama-se varredura ou rastejo. Quando estava pronta para usá-lo, Kayla conectou o bot ao servidor de bate-papo de Sabu e em seguida o lançou como uma tarrafa. Precisava apenas digitar comandos na caixa de bate-papo, como *encontrar SQLI*, para direcioná-lo. O bot constantemente produzia grandes quantidades de novos endereços de páginas da web que apresentavam vulnerabilidades, então as filtrava novamente. Ela havia passado horas configurando o script, de modo que certos tipos de URL

apareciam em cores diferentes. Havia centenas cada dia, e cerca de 20%

conduziam a brechas de segurança, enquanto aproximadamente 5%

conduziam a bases de dados de 10 mil usuários ou mais. Ao longo de dois dias, Kayla esquadrinhou os sites de hotéis, aeroportos e clubes de golfe, até mesmo do Serviço de Saúde Nacional da Grã-Bretanha, conduzindo a equipe a centenas de milhares de dados de usuários. Eles começaram a furtar (ou descartar) as informações e terminaram com oito bases de dados com pouco mais de 5 mil nomes de usuários e senhas e 2 grandes, de 500

mil e 50 mil.

Nessa ocasião, Tflow, AVunit e o hacker irlandês do #InternetFeds chamado Pwnsauce tinham se unido ao grupo, totalizando um sexteto. Esse número e essa composição permaneceriam fixos até o fim. Habilidoso e simpático, Pwnsauce se envolveu com o Anonymous a partir de outubro de 2010, quando ajudara nos ataques contra os grupos antipirataria. Agora estava feliz por ajudar a vasculhar a internet em busca de brechas de segurança. Tão logo encontrou algo, avisou: – Sabu, talvez eu tenha uma pista.

Ao ser indagado por que trabalhava com a equipe, ele afirmou que, embora concordasse com os objetivos do Anonymous, “estou aqui principalmente pelas pessoas”.

– Em minha vida, nunca encontrei gente mais respeitável e trabalhadora do que as pessoas desse grupo – acrescentou Topiary, que participara da conversa. – E agradável.

O Anonymous atraía hackers com consciência, Pwnsauce explicou.

Numa vida passada ele tinha se envolvido com uma “terrível mistura” de hackers que “não sabia o que estava fazendo ou apenas queria perpetrar roubos”. O tipo de pessoa que roubava dados de cartões de crédito de pequenas redes e cadeias de varejo. Com frequência, as microempresas familiares e os postos de gasolina eram os estabelecimentos mais fáceis de hackear, pois armazenavam informações de cartões de crédito no fim do dia, dados que muitas vezes incluíam os códigos de segurança que constam no verso dos cartões das pessoas – embora essa prática fosse ilegal. Eles consideravam esses alvos presa fácil, mas Pwnsauce havia encontrado um pessoal mais interessante e variado no AnonOps, e, como eles tinham um leque mais amplo de habilidades, ele alegou ter aprendido três vezes mais sobre programação e a própria internet com o

Anonymous do que em círculos de hackeagem mais obscuros.

Pwnsauce estudava biologia, mas ansiava sair da Irlanda. Quando não estava estudando ou tratando de assuntos que descrevia apenas como “questões de família”, ele, como Kayla, sentava-se diante de seu computador, bisbilhotando os becos de sites naquela que parecia ser a exploração de uma vida inteira sobre as vulnerabilidades ocultas da web.

– Ele é a mescla perfeita de habilidade técnica e imaginação – mencionou mais tarde Topiary referindo-se a Pwnsauce.

Certa vez, os dois discutiram horas a fio sobre a melhor maneira de romper o sistema de segurança de um aeroporto, o que lhes permitiu penetrar à distância na tela do menu de um McDonald’s e importar texto de hacker verde para confundir os atendentes.

– Estávamos numa histeria – recorda Topiary. – Eu queria mesmo tomar um pint com esse encantador cavalheiro irlandês.

Um dos amigos de Pwnsauce nesse cenário era um hacker irlandês chamado Palladium; os dois tinham hackeado o partido de oposição irlandês Fine Gael e alegado responsabilidade do Anonymous, isso em fevereiro. Palladium havia entrado quando a equipe descobrira uma vulnerabilidade, mas precisava de meticulosa ajuda e explorações secretas para obter informações internas.

Em meados de abril, Tflow descobriu uma vulnerabilidade nos servidores da gigante midiática Fox, mas não tomou qualquer iniciativa a respeito. Ele a mostrou a Palladium, que conseguiu aplicar um shell e penetrar. Os dois decidiram hackear a Fox em colaboração mútua. Um deles por fim descobriu um banco de dados de vendas, com informações pessoais de funcionários da Fox e jornalistas, totalizando 73 mil endereços de e-mail e senhas de pessoas que desejavam receber atualizações sobre as gravações do próximo *X Factor*, show de talentos da rede de tevê dos EUA.

Esse foi um modelo para futuras operações do grupo – manter as decisões estratégicas no sexteto principal, mas trabalhar com um segundo escalão de colaboradores confiáveis para ajudá-los na execução dos ataques.

Após penetrar nos servidores da Fox em 19 de abril, os membros da equipe permaneceram ali durante vários dias sugando todos os tipos de dados, desde

logons de usuários até as senhas dos patrocinadores da estação de rádio. A equipe não tinha decidido atacar a Fox, mas sua vulnerabilidade se destacava entre todas as outras, porque era uma força midiática com viés direitista, que a maioria das pessoas da comunidade do Anonymous detestava. Eles torciam para encontrar algo divertido no tesouro de informações pessoais.

Demorou uma semana para os administradores de TI da Fox detectarem a invasão, mas a essa altura a equipe dispunha de toneladas de dados para peneirar; o material tinha sido entregue por Tflow, que o recebera de Palladium. Topiary contou a ambos que investigaria uma lista de cerca de 350 funcionários da Fox e testaria seus nomes e suas senhas em sites de redes sociais, com o Twitter e LinkedIn. Seria um processo lento e metódico, mas com sorte ele encontraria os poucos desafortunados que tinham reutilizado as mesmas senhas (como Aaron Barr fizera), de modo a conseguir hackear as contas deles e criar outro pandemônio.

O script de varredura de Kayla tinha produzido uma fértil lista de vulnerabilidades, e Topiary, com apenas um conhecimento básico de hackeagem obtido cinco meses antes, também encontrou os registros das transações de 3100 caixas eletrônicos no Reino Unido. Com grupos de hacker normais, nenhuma dessas informações viria à tona. Teriam sido armazenadas nas coleções pessoais deles próprios ou vendidas a spammers. Mas Topiary, Sabu e Kayla vinham do mundo do Anonymous, em que você não hackeava apenas para obter dados, mas para algum tipo de objetivo social ou político. Ao menos por enquanto, a abordagem deles seria de que não havia significado algum para a publicação. Eles o fariam apenas pela diversão, por lulz. Era uma insígnia do Anonymous e também dessa pequena – e cada vez mais unida – gangue, e isso significava uma gama mais vasta de alvos potenciais para hackear e vazar os dados. Antes de qualquer coisa: a equipe precisava de um nome.

Essa tarefa recaiu sobre Topiary e Tflow, e a dupla concordou: era fundamental que o nome incluísse a palavra *lulz*. Eles brincaram com a combinação de vários nomes até chegarem a Lulz Leaks. Parecia se encaixar com seu *modus operandi*, de modo que Topiary criou uma conta de Twitter com esse nome em 3 de maio e postou um único tweet: – Há muita coisa a fazer... Preparem-se.

Pouco tempo depois, ele precisou fazer um segundo tweet, mas não conseguiu entrar na conta – tinha se esquecido da senha.

Os dois voltaram à planilha de desenho. Lulz4ULeaks e Lulz Cannon eram nomes trava-língua, e Lulz Boat, que eles apreciavam, já tinha sido criado no Twitter. Então pensaram num nome que faria um trocadilho com Backtrace Security: Lulz Security. Topiary conferiu e ainda não existia a conta @LulzSec no Twitter. Ele criou uma conta nova, assegurando-se de anotar a senha. Em seguida, redigiu uma biografia que resumia apenas: “Lulz Security®, líderes mundiais em entretenimento de alta qualidade às suas custas”.

Precisavam de uma imagem, por isso Topiary vasculhou uma pasta de 2

mil imagens chamada Reaction Faces, mantida por qualquer usuário do 4chan para ilustrar respostas num tópico. Ele escolheu o desenho de um bigodudo de monóculo e cartola segurando uma taça de vinho tinto.

Topiary não tinha ideia da origem, jamais considerando que, devido ao problema visual que o atingia, o homem com uma única lente poderia ser uma referência a si mesmo.

Estava na hora de deixar o Anonymous dar uma espiada no que eles andavam fazendo. Quando os nomes Topiary, Kayla e Sabu de repente apareceram numa importante sala de bate-papo do AnonOps pela primeira vez em mais de dois meses, houve um frisson quase instantâneo.

– A gente sabe que vem merda no ventilador quando os hackers da HBGary estão aqui – comentou alguém.

– Vocês são OS Sabu/Topiary/Kayla? – indagou outro.

Ao descobrirem que os sectários do Anonymous na época planejavam atacar a Câmara de Comércio dos EUA, Topiary e Kayla logo começaram a procurar vulnerabilidades no site, competindo para ver quem descobria mais. Topiary foi rapidamente derrotado. Os dois então começaram a colar, na sala de bate-papo, os endereços de página de cada brecha de segurança no site da Câmara de Comércio. Os participantes do bate-papo comemoraram e agradeceram. Logo correu o boato de que o trio central da HBGary tramava algo grande.

***

O LulzSec, como hackers, desbravava novos territórios. Roubar dados era uma coisa, mas anunciar o fato no Twitter para que a imprensa pudesse relatar ficava

esquisito. Topiary se candidatou para escrever uma breve declaração para acompanhar os vazamentos de dados da Fox e do *X Factor*, os quais, caso contrário, seriam apenas extensas listas de dados. Todos concordaram. Ficou claro que o papel de Topiary sempre seria o de porta-voz do grupo. Na realidade ninguém pensou em quem deveria abastecer as mensagens na conta do LulzSec no Twitter – simplesmente era óbvio que Topiary se encarregaria disso. Ele publicou a declaração via aplicativo Pastebin.

– Olá, bom dia, como vão vocês? – começava. – Beleza! Somos o LulzSec, pequena equipe de indivíduos fissurados em lulz. Acreditamos que o enfado da comunidade cibernética só atrapalha o que realmente interessa: diversão.

Isso era muito diferente dos avisos sérios que ele redigira para os comunicados de imprensa do Anonymous, os textos que tinham repreendido o PayPal por "censurar o WikiLeaks" ou avisado em tom beligerante à HBGary que "ninguém mexe com o Anonymous". Se o Anonymous era o noticiário das seis, o LulzSec era *The Daily Show*, publicando conteúdo semelhante por um processo semelhante, mas dedicado principalmente a entreter, não a informar ou a motivar. Eram agentes livres.

Em 7 de maio, ele postou o primeiro tweet do LulzSec anunciando que o site Fox.com tinha sido hackeado.

– Esta noite vamos publicar a base de dados dos competidores do X-Factor – falou ele. E acrescentou: – Fiquem ligados. Piscadela, dupla piscadela!

Poucos minutos depois, ele mandou ver.

– E aí vai, meus adoráveis amigos da internet, a base de dados dos competidores do X-Factor 2011.

Topiary acrescentou um link com o arquivo torrent que Tflow havia empacotado e instalado no site The Pirate Bay, como fizera meses antes com os e-mails da HBGary. Topiary não esperava uma resposta imediata dos usuários do Twitter nem dos blogs, mas o silêncio dos próximos segundos, depois minutos, então horas, foi ensurdecedor. Três dias depois, Topiary publicou mais quatro páginas de Pastebin com os dados do Fox.com, com outra apresentação espirituosa e mais tweets. A essa altura, mas só por pouco tempo, pouca gente dava bola.

CAPÍTULO 18

A ressurreição de

Topiary e Tupac

Topiary continuou a conferir no Google News quaisquer menções sobre o Lulz Security ou o vazamento dos nomes de usuários da Fox e do *X*

Factor. Observou que praticamente não havia menção alguma, além de poucos posts de blogs de sites de notícias tecnológicas. Ninguém parecia se importar com o assunto.

Se um indivíduo ou grupo tinha milhares de seguidores no Twitter, aumentava a probabilidade de gerar sensação entre blogueiros e jornalistas e, por fim, criar manchetes. O estilo imaginativo de redação de Topiary, lapidado por tantas horas escrevendo no satírico site Encyclopedia Dramatica, entrou em ação aqui. Num piscar de olhos, ele era capaz de redigir uma série de comentários ácidos embebidos no jargão da subcultura internética. Vinha naturalmente.

Ao cabo do primeiro dia de utilização da conta do LulzSec no Twitter (7

de maio), Topiary tinha arrebanhado cinquenta seguidores com onze tweets. Com estilo irônico, alegre e irreverente, citava letras da pegajosa canção “Friday”, de Rebecca Black, e provocava o Twitter oficial do *X*

Factor: “Roubamos a porcaria de vocês e agora vamos publicá-la!

Pensamentos?”.

O Twitter, apesar de seu limite de 140 caracteres e de seu status de engenhoca das elites das mídias sociais e entendidos em tecnologia, podia se revelar uma poderosa ferramenta de comunicação. Se fosse utilizado com argúcia e prolificidade, milhares de pessoas talvez começassem a prestar atenção ao LulzSec. Ao utilizar o símbolo da @, ou apenas ao mencionar um nome, ele podia conversar com qualquer pessoa que tivesse conta no Twitter.

Na manhã seguinte, ele empregou a tática de Sabu, ou seja, acenar com a perspectiva de mais vazamentos tentadores: – Galera, estamos preparando mais diversão! Aqui vai um segredinho dominical: ainda não terminamos com a Fox.

No domingo, dia 9, o número de seguidores tinha subido para 75, mas Topiary

manteve o entusiasmo ao estilo de showman, como se fosse um diretor de circo alardeando cada tweet no megafone: – Estraga-surpresa da segunda-feira: o vazamento de hoje será bem menor em quantidade, mas bem maior em qualidade – transmitiu. – Ei, pessoal, vocês gostam de senhas? Nós também!

Ele acreditava na importância de manter o fluxo de teasers, por isso tweetou:

– O show começa em poucas horas, galera! Vai ser superinterativo, com um final que vocês vão apreciar. Estamos tão, tão, tão empolgados! :3

Se dependesse de Sabu, ele teria revelado todos os dados da Fox assim que estivessem aptos, independentemente se fosse na sexta-feira ou ao longo do fim de semana. Mas Topiary calculou que seria mais provável atrair a atenção dos principais órgãos de comunicação em uma segunda-feira do que numa sexta, quando muita gente já diminuía o ritmo de trabalho semanal, o que parecia mesmo fazer sentido.

Os teasers continuaram na manhã de segunda: – O LulzSec informa o hashtag do dia: #FuckFox. Ainda vamos esperar mais uma ou duas horas; avise seus amigos. ^____^

E na sequência: – Daqui a trinta minutos... #FuckFox.

Vinte e oito minutos depois: – Estão prontos?! #FuckFox.

Quando chegou o momento, Topiary não postou um extenso documento de informações, mas tweetou uma série de endereços de URL das contas que os funcionários de uma afiliada da Fox TV em San Diego, Califórnia, tinham na rede social profissional LinkedIn.

O primeiro dizia: “Conheça Karen Poulsen, consultora de marketing na Fox 5 KSWB”.

Quem clicava no link descobria que a foto do perfil de Poulsen no LinkedIn agora era o logotipo do LulzSec (homem de monóculo). Topiary fez o mesmo com Jim Hill, executivo do setor de vendas, e com seis outros membros da administração da empresa midiática.

Outros sete gestores tiveram suas contas no LinkedIn hackeadas e tweetadas, inclusive Marian Lai, vice-presidente da Fox Broadcasting.

Nesse meio-tempo, Topiary deu um toque para seus antigos admiradores do AnonOps:

– Ei, AnonOps, ouvi falar que o clima por aqui anda pesado. Vamos animá-los um pouquinho. O Anonymous não quer participar? Vocês vão poder muito breve!

Seguiram-se mais tweets sobre um segundo comunicado de imprensa, todos envolvidos em humor extravagante, utilizando o instrumento de hash tags no fim de cada mensagem como espécie de bordão. Definitivamente esse não era um grupo hacker comum. Três dias depois, Topiary postara 35

tweets e continuava esbanjando confiança.

Logo ele havia tweetado uma segunda e mais danosa fase do vazamento da Fox: uma planilha com mais de oitocentos usuários do Fox.com e dados sobre o funcionamento interno dos servidores da empresa.

Agindo com rapidez, postou um link paródia aos “Arquivos secretos de IRC do LulzSec”, referência ao vazamento do #HQ e à ansiedade nos círculos hacker de espiar a conversa dos outros. O post não continha registro algum, apenas as imagens, em preto e branco, de navios piratas feitos com asteriscos, junto com diálogos parodiados entre os nicknames como Bottle of Rum (“garrafa de rum”, apelido de Tflow), Kraken (Kayla), Seabed (“leito do mar”, Sabu) e Whirlpool (“redemoinho”, Topiary).

Topiary decidira com os outros que piratas e barcos seriam o tema do LulzSec.

– Olha só, pessoal, parece que aquele barco pertence à minha banheira – comenta Whirlpool.

Em seguida, Kraken utiliza doze linhas de registro de bate-papo para criar um navio de batalha maior, seguido por uma nuvem em forma de cogumelo. Daí Whirlpool alega estar “derrotado”, “vencido” e “sozinho para sempre”. O texto de Topiary deixava claro que o LulzSec não levava nada, nem a si mesmo, a sério. Como subtítulo da página, lia-se: – Não contem ao FBI sobre isso, p0r fav0r. Estaremos encrencados e poderemos ir em cana.

Ele publicou outro documento com informações sobre caixas eletrônicos britânicos, nenhuma delas especialmente danosa, mas uma demonstração de que

eles podiam acessar material mais sigiloso. Vinculou o lançamento a um vídeo do YouTube da canção tema “Love Boat” e colou sua própria letra, que arrematava: – Sim, LULZ! Bem-vindo a bordo: é LULZ!

Após alguns dias, a maioria dos 250 seguidores do LulzSec no Twitter pertencia à comunidade do Anonymous. Corria o boato de que algo estava rolando e o pessoal queria conferir. Raras pessoas, à exceção de poucos usuários habituais dos canais de IRC do Anonymous, imaginavam que esses eram os mesmos hackers que tinham atacado a HBGary; os mesmos que tinham sofrido com o imprudente vazamento feito por Laurelai do conteúdo dos bate-papos do #HQ.

Súbito, Topiary percebeu que a conta do LulzSec no Twitter tinha um novo seguidor: Aaron Barr. Ele não escondeu a emoção ao ver isso, e de imediato começou a pegar no pé dele via Twitter.

– Temos o lendário Aaron Barr como seguidor... Ouvimos falar que ele se divertiu pra caramba com o #Anonymous, tanto que acabou largando o emprego. #ai. É melhor tomarmos cuidado agora – acrescentou ele. – Aaron Barr vai comparar o horário de nossos tweets com toda e qualquer logon em contas do Facebook.

E depois:

– Estamos seguindo 0 pessoas. Se seguirmos uma pessoa, isso significa que os e-detetives vão cair em cima dela? Será que devemos seguir Aaron Barr?... Ok, agora estamos seguindo Aaron Barr: ele é nosso líder. Ele roubou aquelas bases de dados da Fox, ele comprometeu mais de 3 mil caixas eletrônicos. Esperem... merda.

Topiary pensou por um instante em qual seria a impressão que toda essa atenção a Barr ia sugerir: qualquer um que soubesse do ataque contra a HBGary teria certeza de que os mesmos hackers agora faziam parte do LulzSec. Deixou a cautela de lado e se adiantou: – Ei, e-detetives: temos um grande interesse pelo Sr. Barr, portanto, devemos ser os hackers da HBGary. Certo? É claro.

***

A equipe passou as semanas seguintes escrutinando dados de que já dispunha para planejar o próximo ataque. Topiary, Sabu e Kayla agora tinham um pequeno conjunto de pistas potenciais a serem trabalhadas. Em segundo plano permanecia

sempre a Infragard, sobre a qual eles podiam vazar os dados de cerca de trezentos nomes de usuários e desfigurar a página inicial.

Nesse ínterim, o relacionamento de Topiary com Kayla se alterava; ele deixava de ser apenas amigo para se tornar pupilo. Sabendo que ia se envolver em atividades sérias com o LulzSec, ele lhe indagou qual sua estratégia para permanecer tão incógnita. Kayla ensinou a Topiary como manejar uma máquina virtual e depois sugeriu que ele rodasse o Linux como sistema operacional virtual e um programa de bate-papo chamado X-chat por intermédio da máquina virtual. Ele seguiu os conselhos.

Ele também começou a armazenar seus sistemas operacionais num cartão microSD no interior de seu MP3 player criptografado: um microSD

SanDisk de 32 GB dentro de um MP3 SanDisk de 8 GB com volume criptografado. Agora, para abri--lo, eram necessários uma senha e vários arquivos chave: cinco canções do MP3, no meio dos milhares de canções do menu. Ele aprendera toda essa configuração com Kayla.

Apesar de muitas horas de conversação, Topiay continuava intrigado com Kayla. Ela desconectava entre quatro e cinco horas da madrugada, no horário do Reino Unido, na maioria das noites, sugerindo que estava indo dormir. Contou a Topiary que não morava nos EUA nem no Reino Unido.

Mas, durante as conversas, ela muitas vezes se referia a coisas como Lemsip, antigripal encontrado nas farmácias britânicas, e feijão na torrada, tradicional prato britânico preferido por alunos endividados.

Noutra ocasião, quando Kayla havia combinado um encontro on-line para uma entrevista no horário britânico, ela havia esquecido, e depois se desculpado por ter “confundido o fuso horário”. Em maio, Kayla também criou uma conta no Twitter, com o nome @lolspoon, que funcionava como recurso adicional para confundir as pessoas sobre sua verdadeira localização. Às 14h, horário britânico, ela tweetava, talvez de modo irônico: – Recém acordei, manhã cedinho XD.

Topiary tinha visto capturas de tela do computador de mesa de Kayla, que mostravam um relógio marcando 08:41, GMT -8 horas. Ela havia alegado tratar-se de uma instalação virtual; em outras palavras, o relógio não tinha sido configurado corretamente. O Sistema Operacional (OS) virtual de Topiary também estava definido como GMT -8 horas. O

computador de mesa de Kayla aparentava ser muito feminino. Estrelas coloridas ilustravam o fundo de seu sistema operacional principal; um arco-íris, o sistema operacional virtual; e uma moça de anime, outra janela de terminal. Talvez fosse feminino demais para ser feminino – mas o desktop de Topiary também parecia masculino demais: mostrava uma colagem de histórias em quadrinhos sobre tubarões e outra de um imenso Slenderman – criatura mítica criada poucos anos antes num painel de imagens – de terno preto e gravata vermelha.

No mundo on-line, mentirosos consumados não faltavam. Topiary lembrava-se de uma moça de uma antiga rede de IRC que enganosamente levara todo mundo on-line a crer que ela era magrinha, fornecendo fotos falsas e agindo defensivamente ao falar sobre distúrbios de alimentação.

Certa vez, ela contou a um grupo de um canal de IRC que ia fazer uma tatuagem. Três horas depois, voltou a conectar e carregou uma foto de um esbelto dorso humano coberto com asas tatuadas.

– Ficou assim – disse ela.

Topiary na mesma hora desconfiou. Carregou a foto num site chamado tineye.com e fez uma busca para ver onde mais a imagem aparecia na web.

A tatuagem já estava em toda a web, por isso não era real. Por fim, descobriu um site de vídeo e uma conta que incluía outro avatar de imagem (uma pintura) que a moça tinha utilizado em sua conta de Skype. Um dos vídeos mostrava uma moça obesa tocando ukulelê. A voz e os dados batiam.

Topiary riu um pouco, mas não revelou os dados. Não queria aniquilar a vida on-line da moça.

***

Embora soubesse que isso tornaria sua prisão mais provável, Topiary começou a pensar em voltar a trazer seu nickname na web pública, utilizando-o no Twitter e no IRC AnonOps. Mas precisava de algo convincente, da mesma forma que Sabu precisara ser convencido a reunir a equipe novamente.

– Por que você manteve “Kayla” após tanto tempo? – indagou Topiary.

– Nunca ninguém me doxeou – respondeu ela. – Simplesmente faz sentido

mantê-lo.

E ela explicou: o pessoal sempre tenta doxear o nickname Topiary.

– Mas se os seus dox não são conhecidos, você deve simplesmente ser Topiary e dizer “Vão se foder” a todos que te odeiam.

O mantra de Kayla era agir sempre com total segurança, e depois sair por aí e desconsiderar todo mundo que duvidasse dela.

– As palavras de Kayla realmente calaram fundo naquele dia – contou mais tarde Topiary. – Adorei seu argumento simplista, mas persuasivo: ninguém sabia quem ela era, então por que devia se sentir pressionada a mudar de nome? Era um chute atrevido no traseiro dos doxeadores. Uma espécie de “Sim, continuo aqui, desgraçados, e daí?”. Isso me deixou inspirado.

Durante os últimos dois meses, Topiary estivera mudando constantemente de nicknames, oscilando entre coisas como Slevin e Mainframe, tentando não mencionar nada que levasse as pessoas a desconfiar de que ele era o Topiary original. Estava cansado do estresse; talvez fosse legal seu nome on-line receber algum crédito pelo que estava prestes a acontecer, e ele não gostava da ideia de as pessoas pensarem que Topiary tinha sido preso e se transformado em delator.

Por isso, reabriu a velha conta pessoal no Twitter, chamada @atopiary, e postou um tweet apenas. O pessoal na sala de bate-papo #anonleaks do IRC AnonOps surtou. Alguns insinuaram que a pessoa por trás da conta era um espião. Coisa típica do Anonymous. Topiary sabia que os boatos logo morreriam. Sempre morriam.

***

Em meados de maio, a série de documentários da rede PBS, *Frontline*, mostrou um episódio sobre o WikiLeaks do qual Sabu não gostou nem um pouco: pintava Julian Assange com tintas não lisonjeiras. Quando ele conversou sobre isso com o grupo, todo mundo concordou. Casualmente, Kayla encontrara uma vulnerabilidade em um dos sites da PBS, poucas semanas antes, com seu bot de autovarredura. Agora Sabu indagou se o grupo concordava em eleger a PBS como o próximo grande alvo. Tratava-se do serviço público de radiodifusão dos EUA, lar do seriado Vila Sésamo.

Mas isso não importava – ninguém levantou objeções.

Como sempre, Sabu entrou na rede PBS pela brecha de segurança encontrada por Kayla e logo começou a coletar dados de usuários – uma base de dados de 38 funcionários aqui, centenas de usuários da sala de imprensa ali. Às vezes, era difícil saber o que estava sendo coletado. Não importava. Seja como for, eles publicariam. A equipe utilizou uma ferramenta chamada Havij para baixar mais rapidamente as bases de dados para fácil visualização. Enquanto Sabu e Kayla faziam o trabalho operário de hackeagem, Topiary e AVunit lidavam com certos cartões de visita dramáticos, algo que provocaria risos no Anonymous. O grupo trabalhou noite adentro, acrescentando várias novas páginas ao site da PBS, começando com www.pbs.org/lulz/, que conduzia a uma gigantesca imagem do Nyan Cat. Essa imagem consistia no cartum de um gato voando no espaço sideral, deixando um rastro nas cores do arco-íris, um dos memes mais famosos de todos os tempos na web.

Construíram outra página, www.pbs.org/ShadowDXS/, apresentando a foto de um gorducho comendo um enorme hambúrguer de 30 cm de altura, com a legenda: "LOL HI I EAT CHILDRENS". Isso era uma alusão a outro Anon apelidado de ShadowDXS, sujeito de proporções avantajadas que se parecia com o Hugo da série de tevê *Lost*. (Topiary inclusive tweetou algo sobre Hugo do *Lost*, mas depois excluiu, considerando muito bobo. The Jester passou a acreditar que isso significava um disfarce, que Sabu era na verdade alguém chamado Hugo.) Antes da hackeagem da PBS, Topiary, Shadow, Pwnsauce e cerca de quinze Anons que eles conheciam do AnonOps tinham entrado no TinyChat no sábado à noite e se embriagado enquanto trocavam mensagens de texto, com um número pequeno de participantes falando com voz e um número menor ainda com a webcam ligada. Topiary acabou postando uma série de tweets ébrios a vários milhares de seguidores em sua conta pessoal, como: "dudd, you have no idea how uch hotgowg repeat the same proces as the nigger behing barry shadow exx rainbows ubunche fa...". As pessoas continuavam a lhe enviar números de telefone, torcendo por um bom show, e Topiary continuou a ligar para esses números e a passar trotes.

Na manhã seguinte, Barrett Brown acordou e viu que havia várias mensagens de voz no celular. Era Topiary avisando que "concordava em estar de acordo". E também mensagens de alguns travestis obscenos que tinham recebido o número de Brown e prometido fazer uma "ligação para combinar sexo casual". Topiary dormiu a maior parte do domingo, e então, só por curiosidade, escolheu um dos

diversos números aleatórios dos EUA obtidos durante os trotes da noite anterior. Um homem zangado com sotaque sulista atendeu: – Se você me ligar de novo, seu indiano estúpido, vou arrancar sua maldita cabeça fora.

Topiary não conseguia se lembrar do homem, mas imaginou que tinha se divertido à custa dele. A diversão daquela noite parecia superar o próprio Lulzsec. A bebida havia inebriado Topiary enquanto ele fazia trotes telefônicos. A pequena audiência do LulzSec e as capacidades da equipe fizeram a mesma coisa quando eles atacavam a PBS.

Para irritação posterior de Sabu, a página do Nyan Cat de Topiary parecia mencionar que essa hackeagem não tinha a ver com Assange, mas com lulz. Para deixar isso bem claro, nas primeiras horas de segunda-feira, horário britânico, Topiary entrou no sistema de gestão do *NewsHour*, em essência o sistema que a PBS utilizava para publicar artigos em seu site, e se deu conta de que podia publicar um artigo jornalístico de aparência legítima diretamente no site do *NewsHour* da PBS.

Primeiro ele quis fazer um texto sobre Obama se engasgando com um marshmallow. Mas, ao sugerir isso aos demais, o grupo decidiu que seria melhor bolar uma história sobre Tupac Shakur, o rapper dos EUA que fora fatalmente baleado em Las Vegas em 1996, mas que depois de morto desfrutara boatos à Elvis de que ainda estaria vivo. Em cerca de quinze minutos, Topiary havia elaborado um artigo, parágrafo após parágrafo, no IRC, intitulado "Tupac encontrado vivo na Nova Zelândia": *O eminente rapper Tupac foi encontrado vivo e bem de saúde em um pequeno resort da Nova Zelândia, conforme relatos locais. A cidadezinha – não identificada por motivos de segurança – supostamente hospedou Tupac e Biggie Smalls (outro rapper) por vários anos. Um habitante, David File, faleceu recentemente, deixando evidências e relatos da visita de Tupac num diário, que, solicitou, devia ser enviado à família dele nos EUA.*

– Ficamos maravilhados ao ver o que David nos deixou – declarou uma de suas irmãs, Jasmine, 31. –Achamos que era melhor contar ao mundo, pois sentimos que isso merecia ser revelado.

David, 28, foi recentemente vítima de um atentado motorizado perpetrado por gângsteres locais. Depois de levar vários tiros a caminho do trabalho, ele foi declarado morto no local. A polícia encontrou o diário na gaveta da mesinha de

cabeceira.

– Naturalmente, não lemos o diário – afirmou um policial. – Apenas observamos o pedido para remetê-lo a um endereço nos EUA, e fizemos isso em respeito ao desejo de David.

A polícia fechou as estradas que levam à cidade e nega especulações sobre se Tupac e Biggie foram transportados a outra região ou país.

Os moradores se recusam a comentar exatamente quanto tempo ou por que motivo os rappers estavam sendo abrigados; um nativo disse apenas "aqui ninguém comenta sobre isso".

Depois disso, a família de David File solicitou ações adicionais para prenderem os responsáveis pelo crime.

– David era um rapaz amável e inocente – garante sua mãe. – Quando ele se mudou para a Nova Zelândia, ficou mais feliz do que nunca.

O irmão dele, Jason, solicitou que parte do diário de David se tornasse pública, numa tentativa de decifrá-lo.

– Perto do final – conta Jason – tem uma linha que menciona "yank up as a vital obituary", coisa que até agora não conseguimos entender.

A namorada de David, Penny, preferiu não se manifestar.

A linha final do artigo elaborado fazia uma referência a Penny Leavy, da HBGary, enquanto a frase *yank up as a vital obituary* não passava de outro cartão de visita: um anagrama com as letras de *Sabu, Kayla, Topiary* e *AVunit*.

Os administradores de TI da PBS se esforçavam em vão para reacessar seu sistema; Sabu e Kayla desferiam um ataque de negação de serviço, por isso eles estavam paralisados. Topiary acrescentou uma foto de Tupac Shakur ao artigo e clicou publicar. Em seguida, tweetou links para um post Pastebin com senhas de quase todos os jornalistas que trabalhavam com a PBS, depois para um post com todas as senhas de logon das estações afiliadas da PBS, depois para um post com as senhas raízes MySQL do PBS.org (a senha raiz para o banco de dados), de modo que as pessoas pudessem hackear o site sempre que quisessem, ou pelo

menos até que alguém remendasse a brecha de segurança. E tinha mais: dados de logon de todos que trabalhavam na série *Frontline* da PBS, e um mapa da rede de servidores da PBS. Na maior parte do processo, ele não queria dar a impressão de que a hackeagem tinha sido motivada pelo WikiSecrets ou que a diversão deles tinha fundo político. Mas pelo menos em uma ocasião ele frisou isso no Twitter: – A propósito – postou Topiary. – O WikiSecrets foi uma droga.

Quase imediatamente, leitores começaram a compartilhar o artigo sobre Tupac com os amigos, postando-o no Facebook e no Twitter, e interessando-se vividamente pelo boato de que Tupac estaria vivo. O

sistema de gestão de conteúdo da PBS podia ser lamentavelmente desprotegido, mas continuava a ter excelente reputação como fonte de notícias. Teresa Gorman, do setor de mídia social e atividade on-line da *NewsHour* da PBS, apressou-se para responder a uma dúzia de leitores que a indagaram publicamente no Twitter sobre a veracidade do artigo: – É inverídico. Pura hackeagem.

– Não, obrigada. É hackeagem.

– É hackeagem.

Então a quatro pessoas de uma vez só: – É uma hackeagem, não um artigo da PBS: nossas desculpas.

Na mesma hora, o @LulzSec tinha recebido 150 tweets e retweets.

– Galera. Claro que Tupac está vivo – tweetou a conta do LulzSec. – Não leram o artigo oficial no @PBS? Por que iam mentir para mais de 750 mil seguidores? Tá louca, Frontline? – acrescentou ele.

Em três horas, 4 mil pessoas tinham apertado o botão Curtir do Facebook ao lado do artigo falso de Topiary. O sistema de publicação da PB

estava tão ultrapassado que os hackers podiam fazer atualizações ao conteúdo armazenado em trinta servidores diferentes por meio de interface com apenas um servidor. O resultado: quando os administradores de TI excluíram a história sobre Tupac, o LulzSec deletou todas as postagens do blog no site da *NewsHour* da PBS. Felizmente para a PBS, os administradores tinham gravado o conteúdo do blog em outra pasta e puderam republicar os posts excluídos em poucas

horas. Até então, qualquer um que tentasse clicar em outra história obtinha um erro 403 – mas o artigo sobre Tupac aparecia na página inicial da PBS. Os hackers tinham apagado todos os dados de logon de usuários e administradores do site e se autodeclarado administradores, o que tornou impossível para os verdadeiros admins recuperarem o controle imediato. Quando os admins fizeram mudanças, os hackers estavam sempre ali para transformá-las novamente conforme seus interesses. E quando a série *Frontline* da PBS

postou uma declaração oficial sobre a hackeagem em seu site, o LulzSec a substituiu por uma página em branco com os dizeres: “FRONTLINE CHUPA CARALHOS LOL”.

Era o Memorial Day (feriado celebrado na última segunda--feira de maio nos EUA, em homenagem aos militares mortos), dia com poucas notícias, e importantes órgãos midiáticos, como o *The New York Times* e o *Wall Street Journal*, veicularam notas sobre o artigo inverídico, destacando o grupo hacker Lulz Security pela primeira vez. Às 10h30 de segunda-feira em Londres, o Google News mostrava um total de 53 artigos sobre a hackeagem. O nome do grupo ainda era obscuro a essa altura – alguns repórteres se referiam a ele como LulzBoat, e mais tarde, na tevê, numa leitura errada do teleponto no Sky News de Rupert Murdoch, Louise Boat.

Quando um órgão de comunicação relatou que o grupo hacker era o Anonymous, Topiary postou um tweet dizendo: “Não somos Anonymous, seu pum líquido bovino mal resolvido”.

Cerca de uma hora depois, esse tweet virou notícia, com o respeitado noticiário tecnológico Venture Beat postando um artigo com a manchete: “Hackeagem da PBS não é obra do Anonymous”. Para a surpresa de Sabu, os membros da imprensa não se interessavam muito pelos dados de usuários vazados nem pelo fato de que a hackeagem tinha sido motivada em retaliação ao documentário sobre Assange. Estavam principalmente fascinados pela falsa história sobre Tupac Shakur.

O LulzSec deu uma única entrevista após o ataque, à revista *Forbes*, alegando que haviam atacado a PBS por dois motivos: – Lulz e justiça. Embora nossa meta principal seja difundir o entretenimento, também desejamos do fundo do coração que Bradley Manning ouça falar sobre isso e pelo menos abra um sorriso.

– Certas pessoas diriam que vocês foram longe demais ao atacar uma empresa midiática... Sem mencionar o fato de ser um serviço público de radiofusão – ponderou o repórter da *Forbes* na entrevista com Topiary, que respondia às perguntas com o nickname Whirlpool. – O que você tem a dizer em relação a isso?

– Cê tá doido, mermão.

Depois disso, num instante de honestidade, Topiary falou que o LulzSec não buscava fama, e sim fazer as pessoas rirem.

Ele começou a aceitar pedidos no Twitter de páginas para adicionar ao site da PBS, da mesma forma como pegara números aleatórios de telefone das pessoas durante sua ébria noite no TinyChat. Um usuário do Twitter solicitou uma página da web mostrando unicórnios, dragões e gostosas com espadas. Tudo isso se tornou possível porque a equipe ainda tinha acesso administrativo ao site.

– Pode apostar – respondeu o feed do LulzSec. – Peraí um segundo.

Topiary e Tflow se apressaram para montar uma imagem e cerca de uma hora depois postaram o link à nova e espalhafatosa página: pbs.org/unicorns-dragons-and-chix-with-swords.

Topiary queria responder a certos detratores que acusavam o grupo de utilizar simples técnicas de injeção de SQL para penetrar na PBS. Então, redigiu uma nota explicando como a hackeagem tinha sido feita e a publicou no Pastebin com um tweet dizendo: “Caros trolls, o site PBS.org foi dominado via um ponto fraco dia zero que descobrimos no mt4, ou Moveable Type 4”.

E continuava descrevendo em detalhes como a hackeagem fora executada com um shell site e como os hackers obtiveram o controle raiz dos servidores da PBS. Eles tinham sido capazes de dominar a rede porque vários funcionários da PBS com acesso a suas partes mais seguras haviam reutilizado suas senhas mais de uma vez. Ele então colara uma lista desses 56 funcionários. Poderiam ter destruído definitivamente o conteúdo integral do site e desfigurado sua página inicial, mas não o fizeram.

A empolgação tomou conta de Topiary. Não sentia fome, sono nem nada além do interesse pela bolha agora habitada por ele com Sabu, Kayla, Tflow, AVunit e Pwnsauce, o grupo mais seleto do qual já participara. Com a ajuda dos

prodigiosos comunicados de Topiary ao mundo exterior, o LulzSec começava a parecer menos uma equipe de hackers e mais uma banda de rock. Topiary iniciou o monitoramento dos seguidores do LulzSec no Twitter e das menções ao grupo na imprensa num site chamado IceRocket, e viu que tudo subitamente tinha disparado após a PBS. No dia seguinte, o LulzSec apareceu na maioria dos jornais impressos pela primeira vez. Um grupo de hackers havia dominado "o site do sistema de radiofusão pública dos EUA e postado um artigo alegando que o falecido rapper Tupac Shakur fora encontrado com vida na Nova Zelândia", noticiou o *Wall Street Journal*.

"O grupo postou uma série de mensagens no Twitter responsabilizando-se pela hackeagem."

Topiary começou a solicitar doações para o LulzSec e utilizou o Twitter e o Pastebin para fornecer um número de 31 dígitos que funcionava como o novo endereço Bitcoin do grupo. Qualquer pessoa podia fazer doações anônimas à conta anônima do grupo; bastava converter dinheiro em moeda Bitcoin e fazer a transferência. O Bitcoin era uma moeda digital que utilizava redes peer-to-peer com o objetivo de realizar pagamentos anônimos. Tornava-se cada vez mais aproximadamente na mesma época em que o LulzSec começou a hackear. Por volta de maio, o valor da moeda tinha aumentado um dólar em relação ao começo do ano, alcançando US$

8,70. Poucos dias após solicitar doações, Topiary agradeceu de brincadeira a um "misterioso benfeitor que nos enviou 0,02 Bitcoins. Sua bondade será utilizada para financiar terror da mais alta qualidade".

Ele utilizou o Twitter para dar dicas sobre quem o LulzSec atacaria em seguida.

– Pobre Sony – falou de modo inócuo em 17 de maio. – A coisa não anda bem para eles ultimamente: Os jornais se apressaram a veicular a mensagem, mencionando que a Sony parecia ser o próximo alvo do grupo.

Pelo Twitter, a fundadora da Backtrace Security, Jennifer Emick, criticou publicamente o LulzSec pela sua conta @FakeGreggHoush, recebendo o crescente apoio de outros colegas on-line que não gostavam do Anonymous nem desse aparente grupo dissidente. Um dia depois da hackeagem da PBS, um desses detratores tweetou a frase *yank up as vital obituary* no falso artigo sobre Tupac. Seria um anagrama para "Topiary, Kayla, Sabu e AVunit", acrescentava a

mensagem. “O que [Topiary] quis dizer com isso? Quer levar o crédito? Elefante na sala?”Pouca gente fora da equipe do LulzSec e raros de seus mais íntimos amigos virtuais sabiam que o LulzSec era composto pelos antigos hackers da HBGary, e o caso do anagrama foi rapidamente esquecido. Centenas de pessoas no Twitter conversavam animadamente sobre esse novo grupo de hackers e a audaciosa investida contra a PBS. Muitas mais começaram a seguir a conta @LulzSec no Twitter para receber comunicados diretos de Topiary. Num piscar de olhos, a conta recebeu dezenas de milhares de seguidores.

CAPÍTULO 19

Guerra hacker

A vitória do ataque contra a PBS deixara Topiary aturdido num misto de fama e presunção recém-descobertas. Ele sabia que não liderava os hackers, nem sequer contribuía com a mecânica dos ataques, mas atuar como porta-voz do LulzSec certamente fez parecer a Topiary, e às vezes aos outros do grupo, que era ele quem estava no timão do barco. Isso significava falar em nome do LulzSec e participar, via Twitter, de bate-bocas com alguns inimigos às vezes fervorosos.

A hackeagem da PBS havia atraído uma explosão de atenção da mídia e granjeado ao grupo uma súbita onda de admiradores, que incluía até mesmo os administradores do Pastebin, o aplicativo de texto grátis usado pelo LulzSec para publicar o fruto de suas pilhagens, aparentemente felizes com o tráfego extra na web obtido com cada publicação. Mas, num mundo já mergulhado em trollagem, drama e guerra civil, detratores ávidos não faltavam. Jennifer Emick lançou alguns desaforos inflamados contra a conta do LulzSec no Twitter, como também o fez o adolescente holandês Martijn "Awinee" Gonlag, que havia sido preso em dezembro de 2010 ao utilizar o LOIC contra o governo holandês sem esconder seu endereço IP.

Awinee e muitos outros "trolls de Twitter" pareceram se alinhar com The Jester, o ex-militar hacker que desferira um ataque de DDoS contra o WikiLeaks em dezembro de 2010, e depois derrubara os sites da Igreja Batista Westboro em fevereiro. Ele nunca era tão perigoso quanto a polícia de verdade, mas certamente representava uma fonte de drama e desvio de atenção. The Jester frequentava um canal de IRC chamado #Jester, numa rede alinhada com a revista *2600: The Hacker Quarterly.*

O nome 2600 originava-se da descoberta, nos anos 1960, de que um apito de brinquedo, feito de plástico, encontrado no interior de certas caixas do cereal Cap'n Crunch, nos EUA, produzia o exato tom de 2600

hertz que levava uma central telefônica a considerar que uma ligação tinha se encerrado. Foi assim que os primeiros hackers dos anos 1980, conhecidos como *phone phreaks,* subverteram os sistemas telefônicos conforme seu bel-prazer. Diferentemente do IRC AnonOps, na rede de IRC

2600, qualquer conversa sobre atividades ilegais era geralmente vista com maus

olhos. Se as pessoas falavam em desferir um ataque de DDoS, a discussão abordava as dificuldades tecnológicas desse tipo de ataque. Se o 2600 era uma loja de armas onde entusiastas discutiam gatilhos de ação dupla ou simples, o AnonOps era o bar num beco escuro onde os bandidos resolviam qual o próximo alvo a ser atacado.

Após a investida contra a PBS, os fundadores do LulzSec decidiram que, à medida que o grupo despertasse mais atenção, eles iam acabar precisando de sua própria rede de IRC, exatamente como o AnonOps e o 2600. Sabu também queria criar um segundo escalão de partidários, uma rede intimamente interligada além dos seis membros principais, que os ajudassem nas hackeagens. Desde o começo, a equipe decidira que o sexteto nuclear jamais seria desmanchado ou ampliado, e, ao ouvir os planos de Sabu, Topiary mostrou ceticismo: “Olha só o que aconteceu no #HQ quando Kayla convidou Laurelai”. Mas Sabu argumentou que eles precisavam de um segundo escalão de colaboradores, mesmo que este tivesse fluidez. Sabu já conhecia essas pessoas dos porões da internet e depositava 100% de confiança nelas. Sabu começara a falar com alguns de seus antigos colaboradores e os convidara a uma sala de bate-papo criada para esses novos seguidores, chamada #pure-elite, homenagem a um site criado por seus amigos hackers em 1999. Entre os convidados, havia gênios da programação, gente com botnets poderosos e hackers veteranos dos anos 1990, que já tinham invadido as redes da Microsoft, da Nasa e do FBI.

Os talentos combinados do grupo eram quase assustadores. Topiary lembrou a Sabu que não se sentia à vontade com todo esse pessoal novo – parecia arriscado. Sabe-se lá; um deles poderia vazar o conteúdo dos chats, como Laurelai fizera de modo tão devastador no #HQ. Também suscitava a questão de por que motivo Sabu continuava a precisar dele.

Ao mesmo tempo, ele mal podia acreditar que participava de um grupo como aquele. Concentrou-se em pegar dicas dos outros. Se utilizassem terminologia hacker que ele não compreendia, ele consultava o Google: jargões como máquinas virtuais, métodos de hackeagem como injeção de SQL, vários tipos de vetores de ataque e terminologia de programação. Se não entendia, eles lhe faziam um breve resumo.

Logo havia onze sectários no #pure-elite com quem aprender, mais os seis originais. Sabu continuava a pessoa principal a ser consultada sobre como encontrar vulnerabilidades; Kayla, sobre como manter a identidade secreta;

AVunit e Tflow, experts na infraestrutura. Para Sabu, os sectários extras não estavam ali para lhe ensinar nada – acreditava que ele e o LulzSec os estavam treinando. Sabu tendia a pensar em todos no subgrupo como pupilos, e contou a Topiary em conversa particular seu desejo de que isso pudesse conduzir a outro movimento antissegurança, ou Antisec. A última vez que o Antisec ganhara as manchetes tinha sido no começo dos anos 2000, quando os perturbadores da web eram poucas centenas de hackers habilidosos, em comparação aos milhares de pessoas com conhecimento técnico que atualmente participavam do Anonymous.

A essa altura, Kayla e os outros que estiveram escrutinando vulnerabilidades em sites importantes tinham conseguido centenas de opções para trabalhar. Mas cada uma precisava ser conferida, primeiro para ver se podia ser explorada de forma a alguém conseguir penetrar na rede, e segundo para verificar se havia algo interessante a ser vazado. Tudo isso demandava tempo, e era muitas vezes realizado de modo esporádico, sem atribuição de cargos. As pessoas se voluntariavam para conferir uma vulnerabilidade. O LulzSec agora tinha um leque de alvos potencialmente maiores que a PBS e a Fox para atacar, alguns inclusive com endereços de web .mil ou .gov. Nenhum desses correspondia a algum tema ou princípio em especial; se os hackers encontrassem uma organização famosa que parecesse interessante, eles a atacariam e depois explicariam seu raciocínio. Sabendo que Sabu tinha a tendência de inflar sua retórica sobre os alvos, Topiary ainda não compreendia a real dimensão do que significava atacar alguns desses sites.

Os colaboradores incluíam hackers como Neuron, um bonachão entusiasta em descobrir brechas de segurança; o misterioso, mas altamente capacitado Storm; Joepie91, o bem conhecido e extremamente loquaz Anon que gerenciava o site AnonNews.net; M_nerva, jovem hacker meio arredio, mas diligente; e Trollpoll, dedicado ativista antichapéu branco. Nos períodos mais movimentados do LulzSec, tanto o escalão principal quanto o secundário passavam a maior parte do dia, às vezes varando a madrugada, no #pure-elite ou on-line. Alguns eram talentosos codificadores que criavam novos scripts para a equipe e também para seus próprios projetos paralelos: Pwnsauce, por exemplo, estivera trabalhando num projeto para criar um novo tipo de criptografia.

No fim das contas, Topiary nunca convidava alguém que ele conhecia para entrar no #pure-elite, e, embora Kayla tivesse recomendado alguns amigos, Sabu também não se sentia confortável em aceitá-los. De acordo com Topiary, 90% dos hackers que entravam no #pure-elite eram amigos e conhecidos subterrâneos

de Sabu. A sala de discussão #pure-elite se tornara um centro de comando oculto apenas para convidados, mas os fundadores originais às vezes se refugiavam num canal ainda mais secreto para conversar sobre os novos recrutas, os inimigos e, em raras ocasiões, estratégia. Em geral, a atmosfera no #pure-elite era barulhenta, enquanto a equipe comemorava o ataque mais recente e a resultante atenção da mídia.

Quando M_nerva entrou na sala, ele pareceu notar isso pela primeira vez.

– Muita cobertura da imprensa – falou ele na noite de 31 de maio.

Topiary lhe mostrou uma foto da primeira página da seção Economia do *Wall Street Journal*. O artigo principal trazia a manchete “Hackers ampliam ataques”, e o subtítulo “Quase todos são alvos”. Embaixo, a grande imagem do Nyan Cat carregada por eles no site da PBS, e o homem de monóculo do LulzSec. Acima do arco-íris que emanava do traseiro do Nyan Cat em seu rastro no espaço sideral, o meme da internet: “Todos seus dados agora pertencem ao LulzSec”. Combinação quase surreal de mídia antiga e subcultura internética.

– O maldito Wall Street Journal imprimiu um maldito nome de Twitter e um gato no espaço – comentou Topiary, incrédulo.

Na maior parte do tempo, o grupo jogava conversa fora, papeando sobre as complexidades técnicas dos navegadores de internet, enquanto Topiary fornecia atualizações ao grupo sobre as doações no Bitcoin. Os participantes informavam acerca de possíveis vazamentos oferecidos por outros hackers fora do grupo e, cada vez mais, acerca do que os inimigos do LulzSec andavam tramando. Esses antagonistas se compunham de colegas virtuais da Backtrace e hackers como The Jester; ambas as facções conversavam na rede IRC 2600. Não havia necessidade de ser convidado para entrar na sala #pure-elite e nenhuma regra , além da óbvia de manter em segredo tudo que era dito ali. O tópico do canal, definido por Sabu, sempre dizia: “NADA DE VAZAMENTOS – RESPEITEM UNS AOS OUTROS – PESQUISEM E EXPLOREM!” A única política do #pure-elite era a de que ninguém deveria armazenar o conteúdo das conversas no canal.

Em geral, o segundo escalão conhecia seu lugar, ciente de que as instruções vinham de Sabu, Topiary e Kayla, e deviam ser seguidas. Acima de tudo, sentiam-se felizes por estar a bordo, embora alguns estivessem chocados com a

reação negativa obtida pelo LulzSec.

– A propósito – comentou Storm numa noite. – FailSec? Que merda é essa?

Ele se referia a outra conta de Twitter com uma centena de seguidores que tinha sido criada para provocar publicamente o LulzSec com mensagens do tipo "Carregar os canhões falhados!" e insinuações nefastas de que a equipe logo seria presa.

– Storm, tivemos perseguidores assim durante meses – disse Topiary. – Eles nos seguem aonde quer que a gente vá. Monitoram tudo que fazemos.

E criam contas imitações das nossas. – Pensou um instante e acrescentou: – Somos uma espécie de banda de rock.

Com o estrelato vinha a infâmia. Alguns dos detratores do grupo eram tão obcecados em importunar o LulzSec que, quando Topiary bloqueava um no Twitter, o detrator criava duas ou três outras contas para continuar a se manifestar.

Kayla realçou que Adrian Lamo, o hacker que alegava ter revelado a identidade do suposto informante do WikiLeaks, o soldado Bradley Manning, inclusive tinha registrado o endereço cibernético LulzSec.com para impedir que o grupo criasse um site com esse nome. Lamo, trinta anos, portador da síndrome de Asperger, tinha sido eleito o "hacker mais odiado do mundo" por passar informações sobre Manning à inteligência militar.

Storm ofereceu-se para encontrar um URL diferente, mas Topiary desistiu. Nas horas vagas, ele e Tflow já estavam projetando o site oficial do LulzSec. Com aparência simples e, naturalmente, com o Nyan Cat voando ao fundo, o site teria um modelo de template inspirado no da HBGary.com.

– Noite, galera – saudou subitamente M_nerva.

– Noite – responderam outros três.

M_nerva desconectou-se. Nos EUA era noite, mas o LulzSec e seus sectários estavam entediados e procurando coisas para fazer. Topiary indagou aos demais: – Querem encontrar um alvo para atacarmos?

– Claro – respondeu Storm.

– Tem um site bem interessante, o FBI.gov – brincou Topiary.

Seguiu-se uma pausa.

– Está mesmo a fim de dar sopa e ir para a cadeia? – indagou Storm.

– Talvez a gente possa interferir num IRC, só por lulz – comentou Topiary, indicando um alvo menos arriscado.

– Claro – disse Storm.

Topiary e Kayla decidiram que, no auge da vitória contra a PBS, era hora de buscar a desforra de seu principal detrator, The Jester. Não apenas enviariam spam ao canal dele, #Jester, e expulsariam seus Jesterfags, mas entupiriam toda a rede de bate-papo 2600 com tráfego de lixo eletrônico e a deixariam off-line. Podia abrigar centenas de participantes, mas continuava sendo o esconderijo de The Jester, e Topiary esperava que o resultado seria a irritação dos administradores do 2600 não com o LulzSec, mas sim com The Jester por ter provocado o grupo. Topiary tinha certeza de que os partidários de The Jester incluíam gente como Emick e Byun, da Backtrace, e estudava enviar espiões ao canal dele para verificar o que eles andavam tramando e talvez traçar o perfil de alguns de seus membros. Se o pessoal de Jester estivesse tentando provocá-los, estava funcionando. Nos últimos dias, Topiary e os outros andavam cada vez mais irritados com The Jester e determinados a atacar sua equipe, por diversão e vingança.

– Melhor coisa a fazer quando se está entediado – disse Kayla no #pure-elite. – Entrar no IRC 2600 e apenas causar drama :D.

– Que tal a gente só entrar no 2600, incendiá-los e depois empacotá-los?

– sugeriu Topiary, já se preparando para a ação. Conectou-se à rede 2600

para acompanhá-la em primeira mão saindo do ar.

O papel de Storm era desferir um ataque de negação de serviço (DoS) contra a rede da revista *2600*. Espécie de DDoS, mas sem o *D* para “distribuída”, já que Storm enviava pacotes de lixo eletrônico de um só computador ou servidor, não

de máquinas múltiplas. (Seja como for, esse é um termo vago – se o seu computador estiver rodando uma máquina virtual, ou VM, e você desferir um ataque DoS, isso pode ser considerado mais de um computador, caracterizando, assim, um ataque de DDoS.) Como um só computador lança um ataque de DoS contra uma rede de IRC? Seria necessário um ou dois servidores para ajudar a amplificar a transferência de dados. Sabu utilizara um método semelhante para seu ataque contra o governo tunisiano, embora em escala bem maior, com a ajuda de servidores de transmissão que ele alegara ter sequestrado secretamente de uma empresa londrina de hospedagem de sites. Storm alugou um servidor básico; por isso, embora seu ataque não fosse assim tão poderoso, facilmente poderia derrubar uma pequena rede de IRC. Muita gente no Anonymous e nos círculos hacker, especialmente quem atuava como operador no IRC AnonOps, era locatária ou dona de servidores. Controlar um servidor era mais comum do que controlar um botnet; era como ser o dono de um carro bonito. Você pagava um bom dinheiro por ele, mas ficava contente ao dar carona aos amigos naquele misto de símbolo de status com ferramenta útil.

Storm podia utilizar seu servidor para enviar 100 megabytes de tráfego de lixo eletrônico por segundo a um alvo. O processo não diferia daquele de carregar uma imagem ou gravação no Facebook ou em um site de compartilhamento de arquivos. Nesse caso, você está carregando algo útil numa velocidade de talvez 4 megabytes por segundo. O servidor extra de Storm agia como um amplificador de guitarra elétrica, mas aumentava a velocidade dos dados, não o som.

Storm utilizaria seu servidor para disparar pacotes de lixo eletrônico contra certos setores da rede de bate-papo da revista *2600*, os nós do servidor da rede conhecidos como folhas. Se você enviasse pacotes de lixo eletrônico em vez de dados úteis, isso podia sobrecarregar o servidor e retirá-lo do ar. Uma rede de IRC funcionava como uma árvore, e a *2600*

tinha três dessas chamadas folhas. Em vez de atacar a rede inteira de uma vez só, Storm sobrecarregou cada folha individual. Usando esse plano, ele podia forçar as centenas de participantes a pularem de uma folha a outra, em vez de logo se desconectarem e esperar que a rede melhorasse. O

objetivo final era incomodá-los o máximo possível.

Pelo mapa de comando do IRC, o grupo LulzSec monitorava quantos usuários estavam em cada folha da rede inimiga. Antes do ataque de Storm, havia cerca

de seiscentas pessoas em todas as folhas, e logo o número começou a cair. Em apenas dez minutos, uma das folhas caiu.

– Anulada – disse Storm.

– Haha – riu Kayla.

Sete minutos depois, à medida que os usuários tentavam manter a conexão, Storm derrubou outra folha e a manteve fora do ar por uns quinze minutos. Ele a liberou novamente por vinte minutos, para os participantes pensarem que estava tudo bem, e depois a derrubou novamente.

– Nem consigo me conectar na 2600 – relatou Kayla. Storm caiu na risada.

– É tão divertido ferrar com esses caras – comentou Topiary.

– Esperem :D primeiro deixa a gente trollar esse pessoal pra valer :D – sugeriu Kayla. – daí a gente pode PUSH/SYN/ACK/UDP e tirá-los do ar KKKKKKKK.

Essa era uma referência aos diferentes tipos de pacotes de lixo eletrônico. Atacar uma rede inteira para se vingar de um grupinho incomodativo não lhes pareceu abuso de poder nem ato de bullying. Em vez disso, com Storm agora ganhando os holofotes, Kayla não pôde evitar a menção de seus próprios ataques bem-sucedidos da época do Chanology, e ela começou a relembrar como havia derrubado três sites da Cientologia com ataques de DDoS, por três semanas, em 2009 – o incidente em que ela havia topado com Laurelai.

– Eheh, foi você então? – indagou Topiary.

– Sim :D – afirmou Kayla.

– Gregg Housh reclamou disso.

– Muita gente reclamou disso.

– Enviando pacotes tamanho 40 – relatou Storm.

Outra folha do servidor foi anulada.

– Cara, eles vão ficar sem ter onde conversar.

Agora três servidores principais que hospedavam a rede de bate-papo 2600 estavam fora do ar. Ele e Topiary tentaram se conectar com a rede e não conseguiram.

– Lolz – comemorou Storm.

– A gente devia fazer isso todos os dias, até eles se recusarem a abrigar Jester – ponderou Topiary.

Ele salientou que o grupinho que se comunicava com Jester pelo Twitter, e com Awinee, da Holanda, mostrava-se especialmente vingativo.

– São os mesmos caras que perseguiram Sabu e nossa equipe, em fevereiro, depois do ataque contra a HBGary – acrescentou Topiary. – Um adorável bando de patifes.

Topiary enviou algumas mensagens pela conta do LulzSec: – O que há de errado com o irc.2600.net, vulgo esconderijo do Jester?

Oops, acho que acabamos de foder com a rede. Desculpe, Awinee e companhia. Divirtam-se explicando aos admins da 2600.net que acabamos de derrubar a rede inteira por causa da turminha do Jester. Uh-oh!

De volta ao #pure-elite, as armas ainda disparavam contra os servidores do 2600.

– Deixo a rede voltar? – indagou Storm a Topiary.

– Você que sabe.

Ao ver mais críticas do pessoal de Jester no Twitter, Storm mudou para um tipo diferente de pacote de lixo eletrônico. E, enquanto Awinee mantinha sua retórica, o LulzSec mantinha o ataque. O LulzSec agia como outros grupos de hackers, com seu comportamento olho por olho, dente por dente, à exceção de que hackers mais tradicionais não teriam se irritado com um grupinho de importunadores relativamente inábeis agindo via Twitter. Talvez fosse porque o LulzSec era tão aberto e público, mas os críticos que falavam mais alto pareciam deixar o grupo mais irritado.

Storm revelava-se um membro útil com sua perícia em ataques de DDoS. Diante dos demais, Topiary o chamou de “oficial da artilharia” do LulzSec, trabalhando

em conjunto com Kayla, a espiã e assassina do grupo.

– A gente atraca no porto. Ela mergulha e elimina.

– E também asso biscoitos – acrescentou ela.

Todo mundo dava risada. Estavam todos dispostos a mais ataques quando enfim Sabu entrou na sala. Já amanhecia nos EUA.

– Acordo e deparo com os pacotes de Storm e com a empolgação de Kayla – começou ele. – Meus neguinhos, o que vocês andaram fazendo sem mim?

Seguiu-se um silêncio. O tom dele parecia brincalhão, mas a equipe já conhecia seu temperamento explosivo mostrado no canal #HQ naquela ocasião com Laurelai, e sua tendência geral a soltar as patas em quem discordava dele. Só sua presença já provocava certa ansiedade em algumas pessoas. Se fosse na vida real, todo mundo estaria se entreolhando ou fitando o chão.

– Dominando a 2600.net – explicou Storm.

– Lol, eles vão acabar perdendo alguns servidores – comentou Sabu. – Eu quero dominar os próprios servidores do 2600.

– Isso seria fantástico – falou Topiary.

– Topiary, meu irmão, como vai? – perguntou Sabu.

– Venerável Sabu, o que manda?

– Nada, irmãozinho. Acabei de acordar, cansado pra caramba.

Sabu deu um tempo dos debates, e o pessoal voltou a planejar maneiras de atrapalhar o grupinho de Jester ou configurar ferramentas de software e scripts para hackeagens futuras.

Logo a equipe se dividia em um leque de canais para encontrar novas pistas de hackeagens ou desentocar espiões. Pular de canal em canal e rede em rede não era problema para esse pessoal, alguns acostumados a frequentar 25 redes de IRC ao mesmo tempo.

Quando o 2600 voltou on-line, Topiary, Joepie91 e os demais começaram a saltitar na rede para espionar seus participantes antes de voltar com relatos de novas fofocas. De modo bastante ousado, eles então criaram seu próprio canal #LulzSec dentro da rede 2600. Sem demora se juntaram dúzias e então mais de cem pessoas ali. Era impossível definir à primeira vista quem eram todos eles, mas um olhar cuidadoso mostrou que se tratava de uma mescla de Anons, script kiddies, fãs em geral que tinham ouvido falar do LulzSec na mídia e hackers de chapéu branco. Ao longo do tempo, a equipe do LulzSec passou a acreditar que cerca de metade dos frequentadores daquele canal, que qualquer pessoa podia acessar, consistia numa mistura de espiões de grupos inimigos, como o de Jester e os Feds.

Em sua nova e pública sala de bate-papo #LulzSec no IRC 2600, a equipe se disfarçava com seus nomes de cunho marítimo: Whirlpool para Topiary, Kraken para Kayla e Seabed para Sabu.

Enquanto observava o desenrolar dos acontecimentos, Sabu ficou preocupado que o grupo estivesse muito empolgado com a diversão na rede 2600 – local que tinham atacado, mas onde já tinham criado sua própria e pública sala de encontro. Era impossível distinguir os fãs verdadeiros dos espiões que desejavam manipular o grupo para obter informações e acesso. A certa altura, parecia que Kayla havia tido uma recaída de Papai Noel e oferecido alguns códigos voucher roubados da Amazon para alguém de fora da equipe. Quando Sabu descobriu essa conversa, Kayla explicou que apenas tinha fornecido alguns dos cupons para que eles fossem testados e depois vendidos no mercado negro. Sabu, já cauteloso devido à conexão de Kayla com Laurelai, ficou perturbado.

Subitamente falou: – Ok, gente. Espero não ter de repetir isso. Mas no 2600 não tem amiguinho. 95% estão ali para fazer engenharia social. Para analisar o que a gente fala, para fazer conexões. Não façam amizades com nenhum deles.

Ele não se importava com o fato de a reprimenda estragar a atmosfera alegre. Quatro outros membros do segundo escalão rapidamente insistiram que estavam sendo cautelosos para esconder suas identidades, conversando em inglês macarrônico para dar a impressão de serem estrangeiros. Mas Sabu acrescentou que, se alguém lhes fornecesse informações privadas, eles deveriam registrá-las e mostrá-las à equipe. Se recebessem um link, deveriam conferi-lo a partir de uma conexão segura.

– Fiquem espertos – concluiu ele. – Se alguém de vocês for dominado, eu vou LOL.

Então Kayla, como se quisesse mostrar aos demais que concordava com Sabu, atalhou: – Outra dica. Mesmo se você for dos EUA, não escreva “color”, mas “colour”, mais amplamente usado no mundo todo. Basta escrever “color”

que as pessoas o identificam como estadunidense.

Sabu parecia não escutar e deu nova ordem a Kayla. Queria que ela mudasse o tópico da sala de bate-papo pública #LulzSec, citando que qualquer pessoa com vulnerabilidades dia zero e vazamentos devia enviar uma mensagem ao novo pseudônimo dela no canal. E recomendou: – Precisamos tirar vantagem disso. Conferir o que os neguinhos estão conseguindo acessar.

Kayla desconectou. Sabu gostava dos gracejos que rolavam no #pure-elite em meio à conversa organizacional, mas ele constantemente lembrava o grupo de que permanecesse focado em encontrar novas falhas de segurança e se mantivesse o mais fechado possível. Criava uma atmosfera tensa, mas era necessário fazê-lo. A exposição da equipe aumentava mais rápido do que esperado. Em 1º de junho, googlar o nome LulzSec havia resultado em 25 mil menções na internet. Em menos de 24 horas, esse número tinha subido a 200 mil.

CAPÍTULO 20

Mais Sony, mais hackers Até o dia 1º de junho, a equipe do LulzSec e seus colaboradores tinham coletado uma extensa lista de vulnerabilidades descobertas por membros como Kayla, Pwnsauce e Sabu. Nenhuma era armazenada num documento oficial do grupo, o que seria arriscado demais – em vez disso, a pessoa que encontrava uma vulnerabilidade a guardava em seu próprio computador e a compartilhava com os demais quando necessário. Nesse sentido, o LulzSec se diferenciava do Anonymous, não apenas porque escolhia empresas da mídia como vítimas, mas também devido ao foco no roubo de dados. O ataque à HBGary mostrara que o roubo e o vazamento selecionado de dados podia ser bem mais danoso – e “causador de lulz” por toda a atenção que atraía – do que um ataque direto de DDoS.

Ao deparar com uma vulnerabilidade, a equipe tinha esperança de que isso tornasse possível a publicação de importantes dados secretos. Muitas vezes, seguir uma pista acontecia de modo espontâneo. Kayla encontrara a brecha de segurança da PBS no começo de maio, mas o grupo só a tinha seguido devido ao documentário WikiSecrets. Descobrir a brecha de segurança era uma coisa, mas explorá-la demandava mais trabalho, e eles precisavam de um bom motivo para transformar isso numa operação. Com uma vulnerabilidade recentemente descoberta, porém, a própria empresa alvo já era motivo suficiente.

O processo judicial da Sony contra George Hotz em abril, o consequente ataque de DDoS do Anonymous e o devastador furto de dados por um pequeno grupo de hackers de chapéu preto tinham se tornado uma bola de neve entre os hackers, que agora tentavam atingir a Sony de qualquer maneira possível. Isso significava que ela se tornara alvo de algo parecido a uma “malhação de Judas” para os hackers. Em parte, os chapéus pretos achavam engraçado continuar a atacar a empresa sem parar, e em parte acreditavam que a Sony merecia essa ação, por só relatar a violação de dados duas semanas após a descoberta do fato.

A investida contra a PBS estava terminada, e a rede 2600 continuava remoendo o ataque sofrido, mas Sabu e Topiary agora estavam atolados até os joelhos na organização de dados roubados dos servidores da Sony: centenas de milhares de usuários, administradores, comunicados internos sobre futuros lançamentos de álbuns da Sony, junto com 3,5 milhões de cupons musicais. Três semanas antes, o grupo estivera investigando vulnerabilidades nos sites da Sony, encontrando-as e publicando-as no site da Sony Japan, mas também procurando no site da Sony em Hong Kong e outros. Sempre que alguém descobria uma vulnerabilidade, colava o endereço da web em sua sala de bate-papo privada, e outra pessoa utilizava o código fonte para ver como a falha podia ser explorada. Não havia ordem; as pessoas apenas contribuíam quando estavam disponíveis.

Só por divertimento, Sabu conferiu SonyPictures.com, o principal site da franquia Sony de filmes e televisão, de 7,2 bilhões de dólares. Para seu espanto, um buraco escancarado na inócua página do Ghostbusters deixava a rede completamente exposta, novamente, a um simples ataque por injeção de SQL.

– Ei, pessoal, a gente precisa copiar tudo isso agora – falou ele empolgado. Então se apressou em mapear a área e reunir todo mundo de modo a começarem a se dividir entre seções diferentes. – Dominamos algo substancial aqui. A Sony vai se despedaçar e se incendiar.

Quando o grupo entrou na rede, encontrou uma imensa catacumba de informações. Levou um tempo para apreender o valor dos dados, mas logo identificaram uma base de dados com 200 mil usuários.

Mais chocante era que todos os dados, inclusive senhas, estavam armazenados em texto simples. As únicas senhas criptografadas eram as dos administradores dos servidores e, de qualquer modo, a equipe conseguiu decifrá-las.

Isso representava um grave indício de negligência da segurança da Sony, poucas semanas após o grande vazamento de dados da PlayStation Network. Pequenas escolas e instituições de caridade tinham melhor criptografia da base de dados do que a Sony. Na verdade, nesse período corria um boato de que a PlayStation Network tinha sido hackeada porque um ex-funcionário despedido da Sony fornecera uma vulnerabilidade aos hackers; o vazamento dos dados aconteceu duas semanas após a demissão de vários funcionários responsáveis pela segurança da rede. Também corria o boato de que esses hackers tinham vendido por 200 mil dólares a base de dados com mais de 100 milhões de usuários.

Kayla deparou com outra base de dados que aparentava ser vulnerável, mas nem se deu ao trabalho de abri-la. Como de hábito, ela colou a localização na sala de bate-papo para que outros investigassem. Quando Topiary enfim a abriu, ele encontrou filas e filas de nomes e números que pareciam intermináveis. Perscrutando a lista, enfim observou um contador na parte superior com o número 3,5 milhões. Pareciam cupons. A sensação foi a de ganhar um incrível presente de Natal.

– Sabu, este aqui é enorme – avisou Topiary.

Sabu foi dar uma olhada na nova e monumental base de dados antes de dividir as tarefas da equipe.

– Diga tchau para a Sony – observou um membro da equipe.

– Kayla, você pode ficar com os usuários? – indagou Sabu.

Sabu encarregou uma pessoa de verificar os códigos musicais, outra, os 3,5 milhões de cupons. Ele em pessoa ficou com as tabelas de administradores. Colaboravam na operação quatro membros principais e dois outros membros do segundo escalão.

Esse era o tipo do trabalho árduo que teria espantado um hacker agindo sozinho. Envolvia baixar um monte de dados, às vezes manualmente. Trabalho monótono que poderia levar dias. Mas, sendo um esforço conjunto, o processo inteiro subitamente se tornou mais rápido e mais envolvente, com os membros da equipe motivados pelo fato de que estavam prestes a constranger publicamente um alvo poderoso. As tarefas de compilar as bases de dados – uma de 75 mil, outra de 200 mil – exigiam para cada pessoa de um a vários dias de trabalho, dependendo do quão detalhadas eram as informações sendo manipuladas. Em seguida, cada membro configurou um computador para baixar cada base de dados. De tão grandes, os arquivos levaram três semanas para ser baixados, normalmente em segundo plano em relação ao que a pessoa fazia on-line.

A equipe enfim decidiu que não ficaria com nenhum dos cupons – dos quais tentaram se apoderar e conseguiram apenas 125 mil. Então se deram conta de que os downloads aconteciam na velocidade glacial de um cupom por segundo; no frigir dos ovos, a coisa toda demoraria semanas a fio. Eles não dispunham de tempo nem de recursos para lidar com um download tão colossal. Em vez disso, pegaram uma amostra daqui, outra amostra ali, para mostrar que haviam obtido acesso. Também publicariam a localização exata, no site da Sony Pictures, da vulnerabilidade do servidor que dera acesso aos dados (a página do Ghostbusters), para que qualquer pessoa pudesse se dedicar a pilhar o tesouro antes que os admins de TI da Sony corrigissem a falha de segurança.

Sabu reuniu todos os dados, e Topiary deu aos números e às senhas uma roupagem palatável para o público em geral.

– Temos muitos arquivos diferentes de vários sites da Sony – explicou ele. – Parte da imprensa (a parte menos inteligente) vai ficar confusa.

Precisamos fazer um documento que resuma tudo.

Ele publicaria diversos documentos revelando o roubo em uma pasta maior. Criou um arquivo chamado “Para jornalistas”, que explicava o achado do grupo, lançando mão de palavras que emplacariam manchetes, como “comprometidos” em vez de “roubados”.

Acordado desde as seis da manhã para acompanhar o fuso horário de Sabu, Topiary nem se sentia cansado. Pelo Twitter, ele fazia uma contagem regressiva para o horário oficial de publicação, criando expectativa entre os seguidores e a

mídia. Adrian Chen, do Gawker, agilmente postou um artigo com a manchete “Os hackers mais sedentos por publicidade do mundo anunciam iminente vazamento de dados da Sony”.

Topiary tinha escrutinado a base de dados da Sony Pictures em busca de um endereço de e-mail .gov ou .mil. Encontrou alguns e começou a postar seus nomes e senhas no Twitter. Então, às 17h do horário da costa leste, naquele mesmo dia em que a Sony finalmente restaurou sua PlayStation Network, Topiary publicou tudo.

– Saudações, pessoal. Somos o LulzSec, e bem-vindos a Sownage – anunciou na introdução. – Seguem várias coleções de dados roubados de redes e sites internos da Sony, todas acessadas com facilidade e sem a necessidade de apoio ou financiamento externo.

O LulzSec golpeava a Sony no exato instante em que a empresa tentava se levantar. Trinta e oito minutos depois da publicação, Aaron Barr tweetou que o LulzSec havia publicado dados roubados da Sony.

– A quantidade de dados de usuários parece significativa.

Em 45 minutos, 15 mil pessoas tinham lido a mensagem, uma taxa de 18 pessoas por segundo, e 2 mil tinham baixado o pacote de dados da Sony do MediaFire, site de compartilhamento de arquivos.

Topiary não teve tempo de se recostar e assistir aos efeitos colaterais adversos. Ele e Tflow montavam o novo site do LulzSec, completo, com design retrô do Nyan Cat e a voz suave do cantor de jazz estadunidense Jack Jones entoando, ao fundo, a música tema de The Love Boat. A página inicial mostrava os versos renovados de “Lulz Boat”, de autoria de Topiary, na forma de texto simples no meio. Um link no rodapé oferecia aos usuários a opção de deixar no mudo – quando clicado, o link dobrava o volume da música. Sabu inicialmente odiou o site e censurou Topiary e Tflow por criarem algo com o potencial de sofrer ataques de DDoS, o que passaria uma impressão de fraqueza do grupo. Por fim, Topiary o convenceu de que deviam mantê-lo.

Eles agiram com rapidez para lançar o site, depois trabalharam para garantir que não entrasse em colapso com o peso de milhares de visitantes e os inevitáveis ataques de DDoS de hackers inimigos. Também se asseguraram de que o arquivo torrent com os dados da Sony permanecesse ativo, de que não houvesse mais

doações ao LulzSec pelo Bitcoin (totalizavam US$ 4 até o momento) e de que tudo o mais estivesse conferido. A conta do LulzSec no Twitter contava agora com 23.657

seguidores, e a sala de bate-papo pública #LulzSec tinha um grande movimento. Topiary ia dormir e tinha dificuldade em cair no sono, sabendo que recebia novos tweets a cada dois minutos. Caótico, mas recompensador. A cada dia voltava ao Twitter com mais confiança, dispensando seus detratores com tiradas fulminantes e mantendo os seguidores incitados. Se o LulzSec anunciava uma nova operação, a novidade tinha lugar garantido nas manchetes.

Muitas vezes, eles nem precisavam entrar em detalhes sobre o que estavam prestes a fazer – a mídia e o público geralmente consideravam que o LulzSec causava mais danos do que na realidade. Mas, à medida que crescia a expectativa das pessoas, as apostas também aumentavam.

– Não queremos ser o grupo hacker que apenas vaza café pequeno toda semana – explicou Topiary na época. – Só vamos lidar com coisas importantes de agora em diante... A não ser que encontremos alguém de quem não gostamos.

Uma dessas “coisas importantes” era iminente. Chegava a hora de o LulzSec tirar o ás da manga e anunciar a hackeagem da Infragard.

– Bem-vindo à FuckFBIFriday, quando vamos nos sentar e rir à custa do FBI – anunciou Topiary no Twitter. – Nenhum horário decidido, mas vamos preparar algo legal para hoje à noite. <3.

***

Enquanto o grupo se apressava para preparar a queda da Infragard, alguns membros da equipe decidiam dedicar especial atenção a um usuário da base de dados obtida no site da afiliada do FBI: um empreendedor do ramo de segurança digital chamado Karim Hijazi. Aos 35 anos, Hijazi liderava uma empresa chamada Unveillance. Quando a equipe conferiu a senha de Hijazi na Infragard com o Gmail e descobriu que combinava, começaram a espionar sua conta de e-mail para ver se podiam expor alguma roupa suja, como tinham feito com Aaron Barr.

Sabu odiava empresas de segurança de chapéu branco. Até aí Topiary sabia. E agora, em conversas privadas, ele tocava no assunto mais do que nunca, em

especial sobre um renascimento do movimento antissegurança.

A rusga de Sabu com os chapéus brancos remontava a tempos antigos. A antissegurança começou em 1999, quando uma vulnerabilidade nos amplamente utilizados servidores Solaris, conhecida por apenas uns duzentos hackers no mundo, conduziu à hackeagem de uma vasta gama de empresas e organizações. Em seguida, esses hackers começaram a roubar e-mails de empresas de segurança de chapéu branco. O motivo: eles odiavam uma prática adotada na segurança cibernética chamada “divulgação integral”. A ideia era a de que se peritos em segurança cibernética (chapéus brancos) pública e rapidamente divulgassem as vulnerabilidades de um site, as quais seriam solucionadas com maior rapidez. Mas os chapéus pretos preferiam manter as falhas ocultas, de modo que elas pudessem permanecer em poder da comunidade underground e continuar a ser exploradas.

O Antisec tivera sua parcela de grupos hacktivistas como o LulzSec, e um dos primeiros foi o mal-afamado grupo chamado ~el8. Após escolher como alvo pesquisadores e empresas de segurança de chapéu branco, os nebulosos hackers roubavam senhas e e-mails e os publicavam num zine eletrônico periódico. Tratava-se de uma única página de fundo branco com *el8* soletrado estilisticamente em símbolos na parte superior, não muito diferente dos posts Pastebin do LulzSec, e recheados de novos scripts de web, falhas de segurança, e-mails roubados e comentários de escárnio. O

grupo chamava esse projeto de *mayhem* (caos), ou “pr0j3kt m4yh3m”. A expressão foi emprestada do filme *Clube da luta*, e seus zines eletrônicos continham inúmeras referências ao filme de David Fincher. Os boletins nunca revelavam as motivações do ~el8, mas o projeto mayhem parecia uma violenta encarnação do movimento Antisec. Muitos da indústria chapéu branco imaginavam que a motivação real do ~el8 era combater a divulgação integral, de modo que os chapéus pretos e os chapéus cinza fossem as únicas pessoas a conhecer as vulnerabilidades secretas da internet.

– Dia desses, esses pirralhos vão ter de pagar uma hipoteca e conseguir um emprego – alfinetou Eric Hines, executivo de uma das empresas chapéu branco atacadas, num artigo da *Wired*. – E não vão se tornar advogados ou médicos... Vão fazer aquilo no qual têm habilidade. E isso significa seguir uma carreira na indústria de segurança cibernética.

Sabu cultivava uma antipatia pelos chapéus brancos mesmo após o movimento Antisec de 1999 definhar. Emick acreditava que ele apenas sentia mágoa após ter sido preterido numa seleção de emprego no ramo de segurança de TI. Seja como for, Topiary passou a compartilhar esse sentimento à medida que os dois tinham mais conversas tête-à-tête. Sabu salientaria que os chapéus brancos cobravam US$ 20 mil por testes de penetração, coisa que o grupo do LulzSec podia fazer sem custos. Ele explicava que o próprio Topiary poderia fazer grátis o que a HBGary fazia cobrando US$ 10 mil. A mensagem era a de que os chapéus brancos agiam como inescrupulosos mecânicos de automóveis, enganando as pessoas e convencendo-as a pagar milhares quando o custo real era bem mais baixo.

Essa linha de raciocínio diferia substancialmente do argumento original do Antisec sobre a divulgação integral. Isso porque, uma década depois, a web estava tão cheia de sites, dados e vulnerabilidades que os chapéus brancos nem preconizavam mais a divulgação integral. O ponto de vista havia sofrido uma guinada, e a divulgação integral de falhas de servidor se transformava em ofensa criminal. O mal-afamado troll da internet Andrew “weev” Auernheimer, responsável pelo meme “Internet is serious business”, tinha aprendido isso na pele. Em 2010, ele e alguns amigos hackers do grupo de trollagem Goatse Security bisbilhotaram o site da empresa de telecomunicações AT&T e descobriram uma brecha de segurança que conduzia a dados internos de 114 mil usuários de iPad.

Weev “divulgou integralmente” a brecha, embora por meio da grande mídia e não de uma mala direta de segurança cibernética. Em janeiro do ano seguinte, seis meses após os jornalistas do Gawker revelarem publicamente a falha de segurança da AT&T para usuários de iPad, o Ministério da Justiça dos EUA anunciou que processava weev por fraude e conspiração em virtude de ter acessado um computador sem autorização.

Um renascimento bem-sucedido da Antisec podia manter as autoridades ocupadas com mais gente semelhante a weev. Sabu queria manter o foco nos chapéus brancos, como nos velhos tempos, por isso era crucial encontrar alguma irregularidade na Unveillance, a pequena empresa de Hijazi. A empresa cobrava para caçar botnets perniciosos, mas, escarafunchando os e-mails da empresa, Sabu e os demais pensaram descobrir provas de que ele trabalhava com outros para espionar os usuários da web da Líbia. Decidiram confrontá-lo no IRC sob diferentes codinomes, a fim de informá-lo de que tinham todos os e-mails dele e

que podiam fazer coisa pior. Em 26 de maio, enviaram-lhe um e-mail com sua senha. Na mensagem intitulada “Vamos conversar”, eles mencionavam que queriam ver sua pesquisa sobre botnets.

Hijazi imediatamente pegou o telefone e ligou para o FBI. Quando enfim conseguiu falar com alguém responsável e tentou explicar o que estava acontecendo, teve a impressão de que as pessoas do outro lado da linha demonstravam desinteresse, ou talvez não estivessem entendendo o que ele falava. Eles o encaminharam a um agente do escritório local. Quando Hijazi ligou para o número fornecido e contou a um funcionário local que hackers mal-intencionados tentavam acessar sua pesquisa sobre botnets, ficou surpreso com a indagação do indivíduo: – O que é um botnet?

No fim das contas, um agente aconselhou Hijazi a começar a registrar todas as suas conversas com o grupo e fingir colaborar, para ver se conseguia obter quaisquer informações sobre eles. Do outro lado da cerca, Sabu, Topiary e Tflow tentavam convencer Hijazi a assumir a posição de quem almejava contratar os hackers para atacar a concorrência. Cada lado mentia um ao outro para obter informações, resultando num encontro confuso, repleto de interpretações errôneas.

– O objetivo é uma palavra nua e crua: extorsão – Topiary disse a Hijazi sob o nome Ninetails, acrescentando que Hijazi pagaria pelo silêncio deles.

– Você tem muita grana; queremos mais grana.

A equipe continuou a se oferecer para ajudar Hijazi atacando seus concorrentes corporativos. Fingindo cooperar, ele por fim respondeu: – Não posso pedir que vocês peguem alguém e ainda assim continuem a ser uma empresa “legítima”. Certo?

Quando Topiary leu isso, acreditou que Hijazi caía na armadilha, provando tratar-se de apenas mais um chapéu branco corrupto, exatamente como previra Sabu.

– Posso dar um palpite sobre a sua identidade? – Karim indagara mais tarde.

– Karim, estamos esperando você fazer isso desde o primeiro dia – respondeu Topiary com um segundo nickname, Espeon. – Fique à vontade.

– 808chan.

Sabu caiu na gargalhada.

– Está falando sério, bro? – indagou ele, utilizando o nickname hamster_nipples.
– Como ousa nos chamar de um maldito canal?

– Então me digam – respondeu Karim, que calculava suas respostas com toda a cautela e ao mesmo tempo jogava para a torcida.

– Se dissermos quem somos, você vai se borrar todo e calar o bico – disse Sabu.
– Mas, sim, somos muito conhecidos.

O grupo continuou a provocar Hijazi, chamando-lhe de obtuso e o avisando sobre o que poderiam fazer com os e-mails dele. Mas Hijazi tinha de simular ignorância – sabia tão bem quanto Sabu e os demais que simular estupidez era um dos modos mais eficazes de ludibriar alguém por meio de engenharia social. Às vezes podia levar a revelar fatos sobre si mesmo.

– Por que a hostilidade? Só estou curioso – defendeu-se Hijazi.

– Não somos um canal – respondeu hamster_nipples, que aparentava ter um problema com status. – Não nos chame assim. Somos pesquisadores de segurança.

– Sem estresse – disse Hijazi. – Vocês não são um canal.

– A-ham – retrucou hamster_nipples. – Está testando a minha paciência.

Embora Sabu parecesse ameaçador nos registros de bate-papo resultantes (publicados tanto pelo LulzSec quanto pelo próprio Hijazi), o adido de imprensa de Hijazi disse mais tarde numa entrevista que o hacker mais agressivo do grupo tinha sido Ninetails, o codinome de Topiary.

– Ele é muito rude – avaliou Michael Sias – e enérgico quanto à extorsão.

Hijazi, acrescentou ele, tinha se esforçado para fazer a coisa certa.

– Foi difícil, não agradável – lembrou-se Hijazi poucas semanas depois.

– Não tenho certeza da motivação deles. Gostam de desaforar as pessoas, o que parece muito juvenil. Achava que no mínimo teria algum sistema de crença, e não parecia haver nada por trás. Era insignificante.

Claro que nada disso atingia Topiary e Sabu, que imaginavam gradativamente estar obtendo provas da perversidade dos chapéus brancos. E os chapéus pretos seriam seus vingadores.

– Tem um monte de empresas que cobram preços exorbitantes e abusam do fato de que as pessoas não sabem nada – contou empolgadamente Topiary numa entrevista após uma recente conversa com Sabu sobre o tópico do Antisec.

– O conhecimento sobre computadores não é nossa prerrogativa.

Compre um livro ou dois e aprenda você mesmo. É isso que eu acho.

A mensagem que Topiary recebia de Sabu era a mesma: a de que a indústria de segurança chapéu branca mantinha o público em geral na ignorância sobre como navegar na internet, minando-o e emasculando-o quando ele poderia facilmente aprender as coisas sozinho, exatamente como ele havia aprendido.

***

Com o LulzSec desvelando essas corrupções aparentemente novas e até então inconfessas, o Anonymous começava a parecer irrelevante. O LulzSec tinha rapidamente arrebanhado 50 mil seguidores no Twitter e se preparava para espalhar a mensagem Antisec. Reinava o caos no IRC

AnonOps; todo mundo parecia com os nervos à flor da pele. Não havia mais atmosfera de emoção, nem humor. Salas de bate-papo que antigamente contavam com oitocentos frequentadores, como a #OpLybia, agora recebiam cinquenta ou cem pessoas no máximo. Os operadores de pavio curto tinham voltado a brigar entre si e a expulsar participantes por mero capricho. Os feds se insinuavam por toda a rede. Não era cordial nem seguro. Topiary e Sabu imaginavam estar criando um mundo bem melhor no LulzSec e em sua rede de bate-papo pública.

Enquanto Sabu acalentava ambições de reviver uma cruzada contra os chapéus brancos, ele incentivava o grupo no #pure-elite a buscar pistas, a partir de hackers de chapéu preto na sala de bate-papo pública do LulzSec, agora hospedada numa nova rede de IRC chamada luzco.org. A equipe ainda se

preparava para o vazamento da Infragard, e, nesse meio-tempo, Topiary, Joepie e os demais perambulavam por seu canal para sondar os visitantes. Mais tarde naquele dia, um hacker chamado Fox entrou na sala e abordou Topiary. Parecia ter algumas pistas para futuras hackeagens.

– Tem Messenger? – indagou Fox. – Queria trocar informações sobre vulnerabilidades.

Topiary nunca tinha ouvido falar no sujeito, mas avaliou que podia resultar em algo.

– Tem gente nos oferecendo vulnerabilidades – anunciou Topiary à equipe quando voltou ao canal #pure-elite. – Ele é autêntico, mas não sei se podemos confiar nele.

Não havia nem chance de Fox ser convidado ao canal da elite, a menos que Sabu dissesse as palavras *100% confiável*. Em vez disso, a equipe convidou Fox a um canal novo e neutro, onde outros podiam inferir suas intenções. Era difícil não ser paranoico.

– Provavelmente é um espião – Topiary contou aos outros.

Sabu sugeriu que ele podia ser o Jester em pessoa.

– Se for ele, a gente pode desviá-lo do rumo. Se não for, vulnerabilidades grátis.

Muitas vezes, quando o grupo iniciava uma conversa com um novo contato, aproveitava a oportunidade para praticar sua bazófia e se divertir um pouco. Assim que Sabu entrou no bate-papo com Fox, fingiu ser um hacker brasileiro do LulzSec. Os membros da equipe ficavam pulando de canal em canal, desde papear no canal neutro até cair na risada no canal de elite, em especial por conta do show de Sabu em pele de brasileiro.

– Já conversaram com um hacker brasileiro da pesada? – indagou Sabu à equipe. O rapaz conhecia muitos hackers brasileiros, a ponto de imitar o jeito que eles falavam, num inglês muito básico mesclado com gíria hacker, e em mensagens de texto em vez de mensagens de voz.

– HUAHUAHUAHUAHUAHUA – digitou rapidamente Sabu, imitando uma típica risada brasileira on-line. – Fox, um cavalheiro nunca entrega – contou

Sabu ao novo hacker, ainda se fazendo passar por brasileiro.

– Ah, eu adoro essa resposta – respondera Fox.

A equipe do LulzSec parecia se desmanchar de tanto rir.

– Sabu, você é um deus – cumprimentou Neuron.

– Obrigado – respondeu Sabu. – Considerem-se sortudos porque ninguém consegue realmente me ver em ação. Ninguém é confiável fora de nossa equipe. Lembre-se disso, Neuron.

A equipe continuou pulando do canal público #LulzSec para o privado #pure-elite, onde relatavam com mais franqueza (embora nunca com total franqueza) o que estava acontecendo. Novos participantes podiam instantaneamente identificar com quem era importante conversar, pois toda a equipe do LulzSec tinha status de operadores, revezando-se no topo da extensa lista com símbolos especiais antes de seus nomes.

Em certo ponto, Joepie foi abordado em particular na fervilhante sala por alguém chamado Egeste, nome conhecido de todos que participavam do canal de IRC de Kayla, o #tr0ll.

– Pois é, pessoal, eu quero brincar com vocês, e este canal é engraçado pra caramba e cheio de newfags – falou Egeste. Agora o LulzSec tinha mais participantes do que toda a rede 2600. – Onde fica o verdadeiro lulzsec?

– Brincar em que sentido? – respondeu Joepie, sob o codinome YouAreAPirate.

– Sabe o que eu quero dizer. Sei que vocês não me conhecem, mas provavelmente conheçam conhecidos meus. Zero, venuism, e insidious, nigg *etc. etc.* – Depois, acrescentou: – Kayla.

Joepie relatou a mensagem palavra por palavra à equipe no #pure-elite.

Aqueles nicknames eram muito conhecidos, frisou um membro do segundo escalão chamado Trollpoll. Outra pessoa caiu na risada.

– Ele só está chutando nomes – avaliou Sabu.

Neuron, Anon cordial e analítico, sugeriu pedir a Egeste que fornecesse uma vulnerabilidade dia zero como prova de suas habilidades. Também conhecida como *0day*, a expressão se referia a uma vulnerabilidade de servidor ainda inédita, e descobrir uma dia zero representava motivo de enaltecimento para qualquer hacker, de chapéu branco ou preto.

Sabu indagou a Kayla se ela conhecia Egeste, e no fim ficou confirmado que o sujeito também participara do canal #Gnosis quando ela coordenou o ataque contra o site Gawker, mas “ele não sabe hackear merda nenhuma”, comentou Kayla. Mesmo com todos os nomes que tinha mencionado, Egeste não passava de mais um desvio de atenção. Logo o encontro se revelou apenas uma gota no oceano de dezenas de outros envolvendo sectários e trolls potenciais.

De vez em quando, a sala de bate-papo do LulzSec era brindada com a presença de um funcionário despedido ansioso para vazar alguns dados internos por meio de um novo grupo carismático. Não mais de um dia após o primeiro ataque do LulzSec contra a Sony ganhar as manchetes, um novo visitante da sala de bate-papo do LulzSec abordou um componente do segundo escalão, Neuron, oferecendo o que aparentava ser o código fonte para o site oficial dos desenvolvedores da Sony. Neuron levou a informação à base operacional.

– Dá só uma olhada no código fonte desse cara para o site “sonydev.net”

– comunicou ele. – Parece legítimo. php file *etc.* Ainda investigando.

– Neuron, essa fonte que você conseguiu – disse Sabu. – [Posta no]

pastee.org para que também possamos analisar.

Neuron enviou aos outros o link de um arquivo com 55 megabytes, junto com a senha de 33 dígitos para acessá-lo.

– Baixando – avisou Sabu. – De qual site é? Sonydev.net?

– A-ham – disse Neuron. – Tenho certeza de que vamos conseguir alguma brecha para invadir a Sony.

– Analisando códigos fonte “scedev” agora – avisou Sabu.

Neuron foi conferir dez minutos depois.

– Qual a avaliação sobre aquela fonte? – indagou ele.

Sabu pareceu aprová-la.

– Que tal se apenas vazarmos o código fonte? – perguntou a Topiary e Neuron.

– Eu não sugeriria isso ainda – respondeu Neuron. – Podemos aproveitar melhor suas coisas. Ele é um desenvolvedor da Sony.

– Tá falando sério? – perguntou Sabu.

– Se a gente ficar quieto, talvez consiga mais – ponderou Neuron, que defendia o ponto de vista de que era melhor espreitar do que descarregar tudo de uma sentada só, como um script kiddie.

– Então peça a ele que nos forneça acesso à rede da Sony.

– Vou tentar. O sujeito disse que era um ex-desenvolvedor da Sony, mas tem acesso.

– Extraia as informações dele via engenharia social – atalhou Storm, que acompanhava a conversa.

– Ok – falou Sabu. – Certo, bro. O que está fazendo aqui escutando a nossa conversa? Engenharia social no rabo dele. Haha.

Neuron saiu para tentar novo contato com a fonte, mas já era tarde demais.

– Ele desconectou – avisou Neuron.

– Gay – falou Sabu, um tanto decepcionado. – Quer dizer que ele enviou uma mensagem, passou a fonte e desconectou?

– Sim – disse Neuron. – Gosta da gente ou coisa parecida.

Em geral era assim que funcionava. A promessa de vazamentos e vulnerabilidades vinha de hackers de chapéu cinza e preto ou de qualquer pessoa que tivesse algo útil a oferecer. Muitas vezes, os dados não eram tão empolgantes como prometiam, mas, no final das contas, a equipe utilizou o código fonte que o ex-desenvolvedor da Sony lhes repassara. E ao longo do

tempo deixaram de se surpreender com o fato de que muita gente de fora queria lhes transmitir vulnerabilidades a serem exploradas – parecia que todo mundo no campo de segurança de TI, por si só uma mescla de chapéus brancos com passado sombrio, conversava com o LulzSec. Alguns desejavam secretamente participar da diversão.

Um hacker adotou um método especialmente bizarro de exigir aceitação. Uma tarde, a equipe do LulzSec começou a ser expulsa, membro por membro, da sala de bate-papo pública do LulzSec.

– Uau, bro – comentou Sabu subitamente no #pure-elite. – Tem gente querendo desmoralizar nossos ops.

Alguém enviava pacotes de lixo eletrônico e expulsava cada membro da equipe do LulzSec para fora do canal de IRC. Não afetava seus computadores, mas o ataque minava as máquinas virtuais ou redes virtuais privadas utilizadas para despistar suas localizações verdadeiras. Fazer um ataque de DDoS contra o IP de alguém podia levar o alvo a desaparecer da internet por um tempo, mas, se a pessoa continuasse o ataque, ele também seria expulso de seu serviço de hospedagem.

– Temos que desligar aquele servidor – sugeriu um membro do segundo escalão chamado Recursion.

– Estamos sendo atacados – bradou Neuron.

Seguiu-se um rebuliço no meio do segundo escalão, enquanto tentavam bolar uma resposta ao ataque.

Sabu quase revirou os olhos.

– Neuron, desconectou? Olhe, pessoal.

Ninguém prestava atenção.

– A sala inteira sofreu um ataque – exclamou Storm. – Ele está atacando pessoas de modo aleatório.

Parecia que um mercenário solitário que atendia pelo nome de Xxxx tentava perturbar as tentativas do LulzSec de se comunicar com seus fãs.

Súbito, Joepie recebeu uma mensagem privada: – Olá, Kayla ou Sabu ou Tflow.

A mensagem havia partido de Xxxx. Joepie rodou uma busca no IP do usuário e deu-se conta de que se tratava de Ryan, o operador temperamental que manejava um botnet no AnonOps.

Neuron recebeu a mesma mensagem privada, assim como outros no segundo escalão.

– Todo mundo cale a boca – disse Sabu. O pessoal conversava na maior agitação. – TODO MUNDO. CALE A BOCA. – Com isso conseguiu atrair a atenção deles. – Relaxem – continuou ele. – Quanto a Ryan, ignorem o cara.

Ele não sabe que somos nós. Puxa vida.

– Relaxe – disse Joepie, acrescentando um rosto sorridente.

– Ryan, hein? – falou Topiary.

– A situação está se tornando horrivelmente estressante – comentou Trollpoll.

– Sei disso, puxa vida – falou Sabu. – Olha só. De agora em diante, ninguém entra no 2600 a menos que esteja preparado para engenharia social.

Agora todo mundo prestava atenção.

– Se não souber como fazer engenharia social, não entre no 2600 – recomendou ele. – Se não tiver um IP protegido contra DDoS, não entre no 2600. É isso.

– Certo – disse Neuron.

– Isso mesmo – concordou Storm.

– Certo, certo, Storm – endossou Recursion. – Err... Sabu. Quis dizer, certo, certo, Sabu, não Storm.

– Ok – disse Sabu. – A Sony foi vazada. Temos projetos maiores.

Ele se referia ao trabalho de Neuron sobre o novo código fonte do desenvolvimento da Sony.

– Quem não estiver muito ocupado pode investigar esse código fonte.

Todos voltaram ao trabalho.

CAPÍTULO 21

Estresse e traição Enquanto os alvos do LulzSec aumentavam de importância, Kayla começou a se afastar um pouco das operações, mais interessada em se vingar de inimigos como The Jester e Backtrace Security. Ela sempre cultivara um espírito livre, leal aos amigos, mas nunca se alinhando com muita proximidade a uma causa específica por muito tempo. Às vezes, ela se entediava. Também não estava interessada em reviver o movimento Antisec, como Sabu ou Topiary. Em vez disso, começou a desenvolver um plano elaborado para se infiltrar como espiã na sala de bate-papo #Jester, instalar-se profundamente e depois infectar os computadores de seus participantes com programa keylogger (registro de pressionamento de teclas), de modo que ela pudesse monitorar as teclas mais usadas, aprender algumas senhas importantes e dominar a sala. Isso se chamava ataque em movimento, e, embora nesse caso se tratasse de uma operação planejada, em geral o ataque consistia apenas em incitar alguém a visitar um site e instalar malware no sistema do visitante. Em outras palavras, agora ela passava só umas duas horas por dia conversando com a equipe, e depois sumia por um ou mais dias.

Nesse meio-tempo, notícias surpreendentes vinham dos EUA. O

Pentágono tinha anunciado que ataques cibernéticos originados de outras nações poderiam constituir um ato de guerra, e que os EUA eram capazes de responder com força militar tradicional. Quase ao mesmo tempo, um informe preliminar da OTAN alegava que o Anonymous se tornava “cada vez mais sofisticado” e “tinha o potencial de hackear arquivos sigilosos do governo, das forças armadas e de empresas corporativas”. Mencionava também que a organização havia demonstrado sua capacidade de fazer exatamente isso ao hackear a HBGary Federal. Ironicamente, declarava que os hackers tinham atacado a empresa de Barr e sequestrado sua conta no Twitter “em represália” ao fato de o Bank of America contratar a empresa de segurança para atacar adversários como o WikiLeaks. Até mesmo a OTAN parecia estar inflando as capacidades do Anonymous, observando raciocínio e conexões onde só havia coincidências. Os hackers só ficaram sabendo dos planos de Barr com o WikiLeaks após tê-lo

atacado. Ainda assim, as notícias chamaram a atenção de todos.

– Vocês leram o documento da OTAN sobre o anonymous? – quis saber Trollpoll no centro #pure-elite. Trollpoll não aparentava ser dos EUA, embora fosse impossível garantir a origem de qualquer um dos frequentadores do canal. – Vão colocar tanques em nossas casas?

– O Obama vai falar algo como “Lol vocês acabaram de atacar meu servidor com DDoS? Ataque nuclear” – comentou Kayla.

Com a atenção do mundo agora se direcionando ao LulzSec e as palavras bélicas da administração dos EUA, a ocasião estava propícia para vazar os dados da afiliada do FBI, a Atlanta Infragard. Eles mantinham o controle do site há meses e agora consideravam ter material suficiente sobre o chapéu branco Hijazi para expô-lo ao mesmo tempo. Isso atrairia uma pressão sem igual ao LulzSec, mas o grupo estava na crista da onda e se sentia seguro.

Os membros fundadores do LulzSec executariam a derradeira investida contra a Infragard. Enquanto se preparavam para desfigurar o site, Sabu entrou no shell, a página administrativa que ele havia configurado, chamada xOOPSmaster, abriu seu programa terminal de modo que pudesse começar a brincar com o código fonte, e, em um aparente capricho, digitou rm -rf/*. Código breve e de aparência simples com reputação notória: qualquer pessoa que o digitasse na retaguarda (back-end) de seu computador poderia efetivamente apagar todo o conteúdo do sistema.

Nenhuma janela surgia para indagar: *Tem certeza?* Simplesmente acontecia. Trolls da internet faziam fama ao induzir suas vítimas a digitar o código ou apagar o crucial arquivo 32 do sistema do Windows.

– Oops – contou Sabu aos demais. – Acabo de apagar tudo. rm -rf/*.

Kayla reproduziu o gesto de abaixar a cabeça e tapar o rosto com a mão, e todo mundo continuou o que estava fazendo. Comparado com tudo que eles já tinham aprontado, apagar o conteúdo do site da Infragard não parecia lá grande coisa. Então utilizaram o shell /xOOPS.php para carregar uma gigantesca imagem e a transformarem na página inicial da Infragard – a pichação deles. Não se tratava de crítica séria ao FBI, mas de outro trote direcionado ao grupo de Jester. A equipe tinha substituído a página inicial da Atlanta Infragard com um vídeo do YouTube apresentando um repórter de tevê de um canal da Europa Oriental

entrevistando um homem impecavelmente bêbado numa boate. Alguém havia acrescentado legendas fazendo o sujeito se passar por um aspirante a hacker do 2600 que não entendia o que o LulzSec fazia. Acima do vídeo, o título: “DEIXA ROLAR, ESTÚPIDOS ENCOURAÇADOS DO FBI” numa janela com a legenda “OTAN – Origamis Tacanhos do Atlântico Norte LOL”.

O comunicado oficial de Topiary teve um tom um pouco mais sério – mas não muito. Quando todo mundo estava pronto, ele clicou em publicar.

“Chegou ao nosso conhecimento que a OTAN e o nosso bom amigo Barraco Osama-Lhama do 24th-century Obama recentemente aumentaram as expectativas no que tange à hackeagem. Agora a tratam como um ato de guerra. Por isso, acabamos de hackear um site afiliado do FBI (a Infragard, mais especificamente, o ramo de Atlanta) e vazar sua base de usuários. Também tomamos o controle completo do site e o desfiguramos.”

Claro, o LulzSec não tinha hackeado a Infragard nos últimos dois dias nem em resposta ao anúncio do Pentágono, mas os órgãos de comunicação relataram que o ataque era uma “represália”.

O conteúdo da Infragard na web tinha sido excluído; o site, desfigurado; e detalhes de 180 pessoas de sua base de usuários haviam sido publicados na web, junto com suas senhas em texto puro, seus nomes verdadeiros e seus endereços eletrônicos. Topiary arrematara a missiva declarando: “Agora somos todos filhos da puta”.

Já que na véspera Topiary anunciara ao mundo pelo Twitter uma iminente hackeagem do FBI, os principais órgãos de comunicação embarcaram na história, gerando uma nova onda de seguidores do grupo no Twitter. O site deles já somava mais de 1,5 milhão de visualizações.

Apesar do dano que o LulzSec causara à rede 2600, a própria revista *2600*

parecia impressionada, a julgar por sua conta oficial no Twitter: “Sites hackeados, infiltrações/escândalos corporativos, guerras entre IRCs, novos grupos de hackers nas manchetes globais. Os anos 1990 estão de volta!”

As estações de tevê se apressavam em encontrar especialistas em segurança capazes de explicar o que acontecia e oferecer opiniões lúcidas.

– Estamos enfrentando um crime muito inovador, e a resposta deve ser inovação – avaliou Gordon Snow, diretor-assistente da divisão cibernética do FBI numa entrevista no canal Bloomberg, logo após o ataque contra a Infragard. – Com dinheiro, tempo e recursos suficientes, um adversário será capaz de acessar qualquer sistema.

No entanto, a hackeagem do LulzSec na Infragard não custara tanto em termos de "dinheiro, tempo e recursos". No frigir dos ovos, a operação custou US$ 0, foi executada com o método relativamente simples de injeção de SQL e se tornou mais virulenta porque uma senha decodificada, "st33r!NG", foi reutilizada para obter acesso administrativo ao próprio site da Infragard. Quanto ao quesito tempo, a equipe levara trinta minutos para decodificar a senha do admin e vinte e cinco minutos para baixar a base de dados dos usuários. Em duas horas, a equipe do LulzSec obteve completo acesso administrativo a um site afiliado do FBI, e durante várias semanas ninguém do FBI sequer desconfiou.

Claro, junto com o vazamento dos dados da Infragard veio a condenação de Hijazi pelo LulzSec. A equipe mantivera o registro de algumas de suas conversas com o chapéu branco e as publicara on-line como prova de corrupção. E, embora os membros do grupo tivessem afirmado a Hijazi que não publicariam os e-mails dele, foi exatamente o que fizeram.

– Desmascaramos uma operação orquestrada pela Unveillance e outros para controlar e avaliar o ciberespaço líbio por meios perniciosos – anunciou Topiary. Com a palavra "avaliar", ele queria dizer que a Unveillance desejava espionar os usuários de internet da Líbia.

– Denunciamos Karim porque tínhamos provas suficientes de que ele estava disposto a ser contratado como matador de aluguel – acrescentou Topiary no Twitter. – Não é uma prática lá muito ética, não é, Sr. Chapéu Branco?

Hijazi também publicou uma declaração logo depois, explicando que ele "havia se recusado a pagar o LulzSec" e a lhes fornecer sua pesquisa sobre botnets. Topiary respondeu com um segundo comunicado oficial dizendo que nunca tencionaram levar a cabo a extorsão; apenas queriam pressionar Hijazi até o ponto em que ele se mostrasse disposto a pagar pelo silêncio dos hackers e depois expô-lo publicamente. Guerra de palavras erigida sobre as pegajosas fundações de mentiras e engenharia social.

Topiary ainda incitava os jornalistas e outros escritores a “vasculhar” os e-mails de Hijazi com cuidado, ambicionando o mesmo tipo de entusiasmo que envolveu o tesouro de e-mails de Aaron Barr. Mas não houve nenhum.

Para começo de conversa, Hijazi simplesmente não tinha suficiente roupa suja. Além do mais, a infâmia do LulzSec ofuscava quaisquer objetivos mais sóbrios e sociopolíticos que o grupo tentava vagamente atingir com cada ataque – que não gostava da Fox, que o programa WikiSecrets era uma “droga”, que a OTAN aumentava a importância dos hackers ou seja lá o que a Unveillance andava fazendo na Líbia. Sem dúvida, uma vasta gama de alvos. O LulzSec parecia atacar todo mundo que podia, justamente porque podia.

Alguns membros do segundo escalão percebiam isso. O hacker Recursion entrou no #pure-elite, no fim do dia 3 de junho, após assistir ao desenrolar dos fatos da Infragard. Ele não havia participado da hackeagem e mostrou-se chocado ao ler o noticiário.

– Holy shit – exclamou Recursion. – Que diabo aconteceu hoje?

– Muita coisa – disse Sabu, sorrindo. – Confira o Twitter.

– O LulzSec declarou guerra contra os EUA? – atalhou Joepie em tom sardônico.

– Peguei o espírito da coisa – respondeu Recursion, e depois pareceu se calar.

Não falou mais nada sobre o assunto, mas vinte minutos depois, após supostamente manter uma conversa privada com Sabu, ele saiu do canal de uma vez por todas.

Sabu se decepcionava com qualquer pessoa que o deixava na mão no meio de uma batalha. Mas se apressou a guiar as tropas remanescentes.

Voltou à sala e se dirigiu a um punhado de participantes: – Bem, pessoal. Aqueles de vocês que ainda estiverem conosco nessa parada fiquem alertas, e mantenham suas identidades ocultas por VPN a qualquer custo. Não tenham medo. Tá tranquilo.

– Sabu, perdemos alguém? – quis saber Neuron.

– Sim.

– Quem?

– Recursion e Devurandom desistiram respeitosamente – respondeu ele –, alegando que não suportam pressão. Vocês já se deram conta de que hoje golpeamos o FBI. Isso significa que todo mundo aqui deve permanecer extremamente seguro.

Esse foi um sério lembrete das acusações potenciais que o LulzSec podia sofrer caso os membros da equipe fossem capturados.

Alguns dos componentes começaram a descrever como procediam para fortalecer sua segurança. Storm agora adotou um novo netbook e apagou completamente seu computador antigo. Neuron fez o mesmo. Utilizava uma rede virtual privada chamada HideMyAss, empresa sediada no Reino Unido utilizada e recomendada por Topiary.

– Você apagou os registros [de bate-papo] da PBS? – indagou Storm, dirigindo-se a Sabu.

– Sim. Todos os registros da PBS estão limpos.

– Então conte comigo para novas missões – disse Storm.

Sabu digitou um rosto sorridente.

– Tá tranquilo – repetiu ele. – Temos uma boa equipe aqui.

No entanto, nem todos estavam tranquilos e nem todos os registros estavam limpos. O arredio membro do segundo escalão do LulzSec, conhecido como M_nerva, o mesmo que dera “boa noite” aos demais há poucos dias e depois não participara muito das conversas, acabara de gravar os registros equivalentes a seis dias de bate-papo no canal #pure-elite, repetindo o desvairado ato que Laurelai cometera em fevereiro.

Vazou os registros. Em 6 de junho, o site de segurança seclists.org publicou o conjunto completo dos registros de bate-papo do #pure-elite mantidos no servidor

de

IRC

privado

de

Sabu.

O

vazamento

revelava,

constrangedoramente, que ninguém no #pure-elite merecia “100% de confiança” e que, apesar de todas suas bravatas, o LulzSec tinha fragilidades. A equipe agiu rápido, sabendo que precisava enviar uma mensagem de que não aceitava delatores, mesmo se outro hacker, chamado Hann, supostamente tivesse persuadido M_nerva a vazar os registros. Eles sabiam que podiam descobrir a identidade verdadeira de M_nerva, pois, entre os outros chapéus pretos que apoiavam o LulzSec, alguém tinha acesso a praticamente todas as contas existentes no AOL Instant Messenger. Já que muita gente um dia havia configurado uma conta AIM, eles só precisavam rastrear o nickname e o IP para obter nome e endereço verdadeiros. Eis que M_nerva era um rapaz de dezoito anos de Hamilton, Ohio, chamado Marshall Webb. A equipe resolveu não revelar a informação por enquanto.

Após ter sua confiança traída, Sabu, o hacker mais experiente, agora se mostrava ainda mais paranoico que antes. Topiary sentiu-se vingado. Ele já sabia que um vazamento podia acontecer se Sabu continuasse a convidar pessoas ao #pure-elite, e não deu outra. Mas ele não queria prolongar o assunto. Quando tocou no assunto com Sabu, o hacker rapidamente mudou de tópico. Não tinha nenhum comentário a fazer. Em vez disso, Sabu trabalhava para aumentar a segurança do grupo mais amplo, separando-o em quatro salas de bate-papo distintas. Havia um canal nuclear, que agora contava com quinze participantes, e o #pure-elite, e depois salas de bate-papo chamadas upper_deck, para os sectários mais confiáveis, lower_deck, kitten_core e family. Os membros podiam galgar os patamares do sistema, dependendo da confiança que inspiravam. Neuron e

Storm, por exemplo, por fim receberam convites para o upper_deck, de modo que podiam ser avaliados para entrar no canal principal dos seis membros principais do LulzSec: Sabu, Topiary, Kayla, Tflow, AVunit e Pwnsauce.

A pressão não vinha apenas da atenção midiática; todos os dias, Topiary presenciava hackers com endereços IP militares tentando comprometer a rede de IRC e os usuários do LulzSec. Já corria o boato de que o LulzSec tinha sido fundado pela mesma equipe que atacara a HBGary. Hackers inimigos postavam documentos repletos de detalhes coletados on-line sobre cada membro, a maior parte equivocada, mas alguns quase acertando em cheio. Os membros do LulzSec precisaram desviar o foco de encontrar novos alvos para proteger a si próprios.

Kayla sugeriu uma campanha de desinformação em massa. A ideia dela era criar um documento Pastebin revelando que Adrian Lamo era dono do domínio LulzSec.com; acrescentar detalhes de outros Jesterfags e alegar que eles eram membros do LulzSec; depois enviar via spam o documento para todos os lugares. Clássica tática de engenharia social que às vezes funcionava.

– Mas dizendo mais ou menos que o LulzSec é da CIA – sugeriu Trollpoll.

Era ultrajante, mas certas pessoas achavam lógica a ideia de que a CIA utilizava hackers freelancer para atacar o Irã e a Líbia, e construíam suas próprias teorias de conspiração em torno do assunto.

Topiary e Kayla escreveram um documento intitulado “Criminosos do LulzSec”, sob o disfarce do engenheiro social fictício chamado de Jux, que alegava ter sido convidado ao canal privado do grupo, dizendo: – Acredito que eles estão sendo encorajados ou contratados pela CIA.

No documento, Jux alegava que Lamo era um importante membro do grupo, junto com um hacker paquistanês chamado Parr0t, um francês chamado Stephen e um hacker desconhecido da Holanda. O documento foi visualizado mais de 40 mil vezes, retweetado pelo afamado hacker Kevin Mitnick e mencionado em alguns blogs tecnológicos na categoria de boato.

Quando Adrian Chen, do site Gawker, começou a entrar em contato com o LulzSec via Twitter para tentar investigá-los, a equipe, ainda ressentida pela publicação do vazamento dos registros do #HQ, decidiu atingi-lo com uma campanha de desinformação separada, construída diretamente para ele.

Convidaram-no a um canal de IRC neutro, onde Sabu fingiu ser um ex-membro do segundo escalão do LulzSec que havia desertado e queria contar alguns segredos. A equipe construiu o embuste para Chen de modo especialmente detalhado, elaborando registros falsos, ataques na web falsos e arquivos de dados falsos como provas para o jornalista. Sabu então começou a abastecer Chen com uma história de que o LulzSec não passava de uma ferramenta do governo chinês numa guerra cibernética com os EUA, que Kayla trabalhava com Pequim e que Topiary injetava dinheiro do governo chinês para as atividades do grupo.

– Se ele publicar, aquele velho saco de besteira está completamente arruinado – observou Topiary.

Planejavam deixar a história circular durante cinco dias, depois negá-la no Twitter, postando um link com todos os registros de bate-papo com o jornalista. Mas Chen nunca publicou nada. Como Hijazi, ele fingiu acreditar na história do LulzSec na esperança de arrancar alguma verdade, coisa que ele percebeu não estar obtendo. A falta de uma reportagem decepcionou os membros do LulzSec, os quais, por sua vez, estavam conseguindo evitar a aproximação de pessoas externas; ao menos por enquanto.

***

No começo de junho, os membros do LulzSec trabalhavam a todo vapor em diversas campanhas de desinformação diferentes e na operação adicional, tentando não pensar no dano potencial causado por M_nerva.

Uma luz na escuridão era a arrecadação de quinhentos dólares em doações no Bitcoin. Topiary controlava a conta e repassava parte do dinheiro a Sabu a fim de comprar contas em redes privadas virtuais, como a HideMyAss, para melhor esconder os componentes do grupo e também para obter mais espaço de servidor. Transformar esse montante em dinheiro irrastreável implicava uma tarefa demorada, mas relativamente fácil. Os Bitcoins compravam cartões virtuais pré-pagos a partir da Visa, com a ajuda de nomes, endereços, dados pessoais falsos e cargos em empresas falsas, gerados em segundos no site fakenamegenerator.com. Desde que o endereço de contato combinasse com o de cobrança, nenhuma loja on-line questionaria sua autenticidade. A conta na Visa era utilizada para entrar no mundo virtual Second Life e comprar a moeda interna do jogo, os dólares Linden. Converta essa moeda em dólares dos EUA via um site de transferência cambial (recomendado por Kayla) chamado VirWoX

e, em seguida, deposite esses dólares numa conta Moneybookers. Por fim, transfira essa grana a uma conta bancária pessoal. Esse era um método.

Outra rota mais direta, utilizada com frequência por Topiary, consistia em apenas transferir dinheiro entre alguns endereços Bitcoin diferentes: Endereço Bitcoin 1 a Endereço Bitcoin 2 a Endereço Bitcoin 3 à conta no Liberty Reserve (processador de pagamentos da Costa Rica) a Endereço Bitcoin 4 a Endereço Bitcoin 5 à segunda conta no Liberty Reserve à conta no PayPal à conta bancária.

Se tivesse a mínima desconfiança de que o número de transferências era insuficiente, ele adicionava várias outras etapas.

Assim, na segunda-feira, 6 de junho, Topiary conferiu a conta do LulzSec no Bitcoin. Caramba, pensou. Deparou com uma única doação anônima de 400 Bitcoins, o equivalente a aproximadamente US$ 7800.

Soma igual àquela Topiary nunca tivera na vida. Entrou direto na sala de bate-papo segura da cúpula.

– CARACA galera?! – exclamou e logo colou os dados do Bitcoin.

– DE JEITO NENHUM – falou AVunit. – LOL. Deve ser engano.

– Necas – disse Topiary.

Colou os dados novamente.

De repente todos pararam o que estavam fazendo e conversaram sobre dividir o dinheiro: mil dólares para cada um e o resto para investir em novos servidores. Começaram enviando mensagens privadas a Topiary com seus endereços exclusivos no Bitcoin, para que ele pudesse enviar a parcela de cada um. Topiary não tencionava esconder o jogo quanto aos valores nem ficar com uma fatia maior para si. Todo mundo processava o dinheiro por várias contas para evitar qualquer rastreamento. Sabe-se lá se a doação não tinha sido feita por Feds ou chapéus brancos militares oportunistas?

– Pessoal, por favor, tomem precauções com os Bitcoins – frisou AVunit.

– Deixe-os fluir através de alguns portões... Utilizem uma parte para saldar as

dívidas e depois guardem o restante.

– Ok, começando as remessas – avisou Topiary. – Todos vocês agora estão mil dólares mais ricos.

– Com licença, vou acender um charuto para comemorar – disse Pwnsauce.

– Só vou ficar olhando a grana – comentou Kayla. – Deixá-la crescer enquanto o Bitcoin se valoriza.

Tão volátil e popular era o valor do câmbio da criptomoeda Bitcoin que, no dia seguinte, um Bitcoin tinha subido para US$ 26, aumentando o valor da grande doação para US$ 11 mil. Três meses antes um Bitcoin valia um dólar.

– Sinto muito mesmo por vocês não estarem aqui – disse AVunit –, porque vou abrir uma garrafa de uísque de primeira qualidade. Um Highland Scottish.

Topiary mal notou a referência ao local onde morava.

– Agora vamos todos transar – comentou Tflow.

O grupo exultava de alegria, esquecendo os inimigos e a pressão. Sabu aproveitou a ocasião para parabenizar os companheiros.

– Obrigado, equipe – disse ele. – Todos nós fizemos um excelente trabalho. Foi merecido.

Para Sabu, as comemorações não durariam muito. No dia seguinte, enfim o FBI bateu à porta de Hector “Sabu” Monsegur.

***

Tarde da noite de 7 de junho, terça-feira. Dois agentes do Federal Bureau of Investigation entraram no bloco de apartamentos Jacob Riis e rumaram ao sexto andar, onde Hector Monsegur morava e, muitas vezes, promovia festas com a família e amigos. O FBI tentava pôr as mãos em Sabu há meses, e, semanas antes, eles enfim conseguiram corroborar o pronunciamento da Backtrace: Sabu tinha, inadvertidamente, entrado num canal de IRC sem ocultar seu endereço IP. Um único deslize era tudo de que eles precisavam. Para garantir sua cooperação, os Feds necessitavam de provas de que Monsegur tinha violado a lei. Assim,

intimaram o Facebook a fornecer dados da conta do rapaz e descobriram números de cartões de crédito roubados que ele estivera vendendo a outros hackers. Só isso já garantia uma condenação de dois anos de cadeia. Sabendo que ele tinha duas filhas e uma família, agora o FBI possuía certo poder de barganha.

O FBI havia assistido a tudo e esperado o momento exato. Então, na terça-feira, os agentes receberam a ordem de agir. Em meio ao crescente número de grupinhos que, como a Backtrace, tentavam doxear o LulzSec, um havia publicado o nome Hector Monsegur, junto com seu endereço verdadeiro. Sabu negligentemente continuara a hackear até aquele instante, talvez raciocinando que já tinha ido longe demais e que a prisão era inevitável. Mas o FBI não queria correr riscos. Precisava dele.

Os agentes bateram à porta bordô de Monsegur, e ela se abriu para revelar um jovem latino, os ombros largos, trajando camiseta branca e jeans.

– Sou Hector – disse ele.

Os agentes, que vestiam coletes à prova de bala como medida padrão de segurança, se apresentaram. Monsegur, aparentemente, negou tudo. De acordo com um relato posterior da Fox News, que citou fontes que haviam testemunhado a interação, ele disse aos agentes que não era Sabu.

– Pegaram o cara errado – ele afirmou. – Nem tenho computador.

Perscrutando o apartamento, os agentes vislumbraram um cabo Ethernet e as luzes verdes e piscantes de um modem DSL.

Continuaram a interrogar Monsegur, estabelecendo a tradicional rotina policial bonzinho/policial carrasco. Contaram que desejavam que o rapaz trabalhasse com eles como testemunha cooperativa, para ajudá-los a corroborar as identidades de outros hackers do LulzSec. Num primeiro momento, Sabu se recusou. Ele não ia delatar sua própria equipe.

Em seguida lhe informaram sobre as provas obtidas no Facebook de que ele havia vendido cartões de crédito roubados e lhe avisaram que isso já bastava para condená-lo a dois anos de cadeia. O que aconteceria às filhas se ele fosse preso? O policial bonzinho disse a Monsegur que a pena seria menor se cooperasse; ele precisava pensar nas crianças. Monsegur ainda resistia. Foi

quando o policial carrasco entrou em ação.

– É isto, não tem negócio, acabou – atalhou o outro agente, saindo afoitamente do apartamento. – Vamos colocá-lo atrás das grades.

Sabu enfim cedeu.

– Foi por causa das crianças – mais tarde um dos agentes contou a Fox.

– Ele faria qualquer coisa pelas filhas. Não queria ser preso e deixá-las desamparadas. Foi assim que o pegamos.

Na manhã seguinte, às dez horas, Monsegur compareceu ao tribunal do distrito sul de Nova York com sua nova advogada, Peggy Cross-Goldenberg, e concordou diante do juiz em permitir que o FBI monitorasse todos os seus movimentos – tanto on-line quanto na vida real. Levaria mais alguns meses para que os promotores o acusassem formalmente por uma série de crimes relacionados à hackeagem, mas sua punição seria amenizada como parte do acordo. A partir de quarta-feira, 8 de junho, Sabu tornou-se um informante do FBI.

Monsegur, que havia escalado ao ápice da comunidade hacker internacional graças a sua perícia técnica, charme e paixão política, agora fornecia informações sobre seus amigos ao FBI.

***

Enquanto Hector Monsegur era detido em seu apartamento secreto em Nova York, milhares de pessoas comentavam sobre sua equipe de hackers audaciosos. Após a hackeagem da Infragard, a conta do LulzSec computava 25 mil novos fãs, totalizando 71 mil seguidores. O nome alcançava 1,2

milhão de ocorrências no Google. Topiary descobriu que passava alguns segundos pensando em algo bobo para tweetar, em seguida tweetava e imediatamente a declaração era citada nas manchetes dos noticiários.

Quando ele tweetou um link ao canal de IRC público do grupo, irc.lulzco.org, num domingo às seis da tarde, mais de 460 pessoas rapidamente se aglomeraram no local para conversas aleatórias e a oportunidade de dar tapinhas virtuais nos ombros dos mais famosos hackers do planeta.

– Entre na festa – anunciara ele. – Estamos desfrutando um domingo pacífico.

– LulzSec, vocês são demais! – elogiou um visitante.

– Preciso de alguém para derrubar o site idiota de minha escola, só por lulz – comentou outro.

– Ei, alguém pode hackear esse cretino para mim? – indagou um terceiro, postando um endereço IP.

Cada vez que outro grupo de vinte ou trinta pessoas entrava no bate-papo, alguém gritava: – Aí vem a inundação!

– Pessoal, vocês publicaram o e-mail de minha mãe – contou outro fã no Twitter. – Eu ri para valer.

Nesse meio-tempo, jornalistas se esforçavam para acompanhar as evoluções de ritmo alucinante. Logo depois de publicar os códigos de desenvolvimento da Sony, o LulzSec carregou a base de dados de usuários do site pornô Pron.com, destacando usuários que tinham endereços de email .gov e .mil com a observação: “Estão muito ocupados se masturbando para defender nosso país”. Um piloto dos EUA tinha usado a senha mywife01, enquanto o endereço de e-mail flag@whitehouse.gov utilizara karlmarx.

O australiano Patrick Gray, especialista em segurança de TI e blogueiro responsável pelo blog de segurança cibernética Risky.Biz, escreveu um post chamado “Por que amamos secretamente o LulzSec”. Foi retweetado centenas de vezes e dizia: “O LulzSec sai por aí dando bordoada em algumas das organizações mais poderosas do mundo e as jogando na lona...

por diversão! Por lulz! Para tirar sarro! Com certeza isso revela o que você precisa saber sobre segurança de computadores: ela não existe”. A frase de efeito no final verbalizava o que muita gente da indústria da segurança cibernética estava pensando: “Então por que motivo a gente gosta do LulzSec? ‘Eu te disse.’ Por esse motivo”.

O uso flagrante pelo LulzSec de métodos tipicamente simples de injeção de SQL tinha escancarado o quão vulneráveis eram os dados privados das pessoas, e o fizera de modo mais envolvente do que qualquer campanha de marketing de segurança em TI o faria. A Cisco inclusive tirou proveito, a certa altura

patrocinando tweets promocionais no topo de quaisquer resultados de busca sobre o grupo no Twitter.

Logo uma empresa de segurança de chapéu branco também quis se aproveitar da situação. Na manhã seguinte, Topiary acordou e deparou com novas reportagens sobre o suposto mais recente ataque do LulzSec, o deface da página inicial da empresa de segurança digital Black & Berg. Na página, havia um imenso título dizendo: “Cibersegurança para o século XXI, desafio de hackeagem: mude a foto da página inicial deste site e receba US$

10 mil e um emprego de assessor do consultor de cibersegurança sênior, Joe Black”. Logo após se lia: “FEITO, FOI FÁCIL. GUARDE A GRANA, FIZEMOS POR LULZ”. Sob o título aparecia a foto de um prédio federal dos EUA coberto pela imagem em preto e branco do sofisticado homem de monóculo do LulzSec. A revista on-line *International Business Times* rapidamente postou um artigo com a manchete: “LulzSec vence competição de hackeagem e rejeita prêmio de US$ 10 mil”. Depois citava o próprio Joe Black, comentando: “O que posso dizer? Somos bons; eles são melhores”.

Quando a *Times* indagou Black sobre como o LulzSec fizera, ele respondeu: “Acredito que foi reconhecimento, varredura, obtenção de acesso, manutenção de acesso e extinção dos rastros”.

Mas, quando Topiary perguntou à equipe sobre o ataque contra a Black & Berg, ninguém sabia de nada, e essa mensagem de deface não tinha nenhum traço da criatividade doida, marca registrada de seus outros ataques. Topiary ainda não sabia na época, mas Black muito provavelmente havia desfigurado o próprio site como manobra para atrair clientes muito necessários à empresa de chapéu branco. (Um ano depois, a empresa tinha fechado as portas e seu fundador se bandeara para o lado do Anonymous e do Antisec.) Em outra parte do mundo, a radical comunidade hacker brasileira formava sua própria versão do LulzSec, chamada LulzSec Brasil. Outro grupo hacker autointitulado LulzRaft teve breve ascensão. Outros hackers chapéus pretos enviaram mais pistas. A cada dia, os membros da equipe do LulzSec recebiam dúzias de links a páginas da web que podiam infectá-los com vírus, mas entre elas havia algumas autênticas vulnerabilidades de segurança e muitas descargas de dados a torto e a direito; mil nomes de usuários e senhas aqui, outros quinhentos mil ali. Muitas vezes dados de empresas de jogos eletrônicos, alvo paradoxalmente popular para hackers, já que muitos deles também eram gamers. Desejavam vazar pelo LulzSec porque

geralmente tinham medo de fazer eles próprios e não queriam que as vulnerabilidades e os dados descobertos fossem desperdiçados. A equipe tinha de ser meticulosa na escolha do que vazar – Topiary aprendera de sua época no AnonOps a não dizer sim a todas as solicitações.

Embora Topiary tivesse dificuldades para manter o controle de tantas coisas simultâneas, o LulzSec estava prestes a acelerar o ritmo de hackeagens anunciadas. A equipe sentava num monte de dados não utilizados, a maior parte fornecida por outros hackers, que precisava ser exposta. O Pentágono lhes dera motivo para enfim vazar a Infragard, mas logo eles deixaram de esperar o momento certo. Seria apenas uma queima de estoque, ataque após ataque.

Sentindo a tensão naquela noite de quarta-feira, 8 de junho, Topiary enviou uma mensagem a Sabu perguntando se ele estava por perto e queria conversar. Queria um simples bate-papo sobre segurança ou talvez acerca da vida em geral. Mas Sabu não respondeu. Poucas horas antes, Monsegur estivera no tribunal, diante do juiz, assinando documentos de acordo com o FBI. Com Sabu off-line há várias horas, Topiary combatia um estranho mau presságio.

– Estou ficando muito preocupado. Talvez algumas prisões realmente aconteçam – observou aquela noite, horário do Reino Unido, numa rara expressão de emoção.

Isso não se devia aos hackers inimigos, a Jester, nem mesmo à doação Bitcoin vinda do nada. A Backtrace tinha acabado de publicar o documento alegando doxear os membros da equipe do LulzSec, embora novamente ele tivesse certeza de que todos os nomes de seus colegas estavam errados.

– Só estou com uma estranha sensação de que algo ruim nos espera, não sei por quê.

Lembrou-se de como havia mencionado a Sabu preocupações semelhantes poucos dias antes, após o vazamento de M_nerva, e de como ele também subitamente se mostrara mais preocupado. (Isso foi antes da detenção.) Topiary sempre fora o calmo do grupo, o cérebro racional de Sabu. O fato de ele começar a ficar nervoso talvez sugerisse a Sabu que o grupo tinha ido longe demais. À medida que continuavam a falar, os dois decidiram que, apesar de toda a pressão que sofriam, agora não podiam parar. O embalo era muito forte; as expectativas, muito altas.

Perseverariam e apostariam em sua habilidade de se manter ocultos. No fundo, uma parte de cada um deles também havia aceitado que a detenção talvez acontecesse em algum momento.

Topiary continuava a acreditar plenamente em Sabu e em Kayla? Ao responder a essa pergunta na quarta-feira à noite, ele disse que confiava neles “mais do que em qualquer outro” do grupo, sobretudo em Sabu.

– Eu trato Sabu como a pessoa on-line mais importante do que quase todas para mim – afirmou. – Se eu for preso, não vou delatar ninguém.

Mas a inquietação decorria em parte por saber que Sabu há uma década fazia engenharia social com as pessoas, e pelo estranho fato de confiar tanto nele, apesar de conhecê-lo há apenas poucos meses. Por exemplo, Sabu contara a Topiary seu prenome, Hector, um mês antes, confiara a ele seu número do Google Voice, contara-lhe os nomes de alguns de seus amigos e até mesmo mencionara que morava na cidade de Nova York.

Quando, semanas antes, Topiary perguntara o que Sabu sabia dele, imaginando se ele tinha a mesma quantidade de informações, Sabu havia respondido:

– Um sujeito do Reino Unido que faz bons sotaques, o que me leva a crer que você não é mesmo do Reino Unido.

Topiary, que tinha um raro sotaque escocês-norueguês desenvolvido em games on-line com amigos escandinavos, nunca contara a Sabu seu prenome verdadeiro nem confirmara ser morador das ilhas Britânicas, tampouco identificara quaisquer de seus amigos. Era quase como se Sabu realmente não se importasse mais sobre ocultar sua própria e real identidade.

Nesse sentido, Topiary se considerava menos descuidado do que Sabu.

Além do mais, habitar uma parte remota do mundo lhe transmitia uma sensação de segurança. Duvidava de que a polícia se desse ao trabalho de viajar até as ilhas Shetland.

Ele foi dormir. Não conseguia conciliar o sono. Ficou se revirando na cama, até dormir e ter um bizarro pesadelo, acordando aos gritos às cinco da madrugada. Há anos não fazia isso. Ainda estava escuro lá fora, mas assim mesmo ele saiu da cama e foi para a sala. Sentou-se em sua cadeira especial para jogos

eletrônicos e entrou no #pure-elite. De repente, foi bombardeado com mensagens.

– Sabu se foi – avisou um dos membros da equipe.

A equipe do LulzSec enfim se deu conta de que ele estivera ausente por mais de vinte e quatro horas.

CAPÍTULO 22

O retorno de Ryan, o fim da razão Ansioso e confuso, Topiary tinha certeza de que alguém estava mentindo. Primeiro Kayla relatara boatos de uma rede de IRC pública de que Sabu recebera uma visita surpresa da polícia. Depois alguém disse que as duas filhas dele tinham adoecido e ido parar no hospital. Outra pessoa que, Topiary sabia, era amiga de Sabu na vida real também alegou que ele fora acossado pela polícia. Em seguida ouviu a história do hospital de outra fonte. Havia uma divisão de 50%-50% sobre o que havia acontecido.

Topiary queria acreditar na história do hospital. Em geral, nos círculos de hackers paranoicos ou no Anonymous, se alguém sumia de um IRC público por um tempo e sem motivo aparente, as pessoas consideravam o pior (uma visitinha do FBI). Mas, se Sabu tivesse repentinamente desejado voltar ao subterrâneo, ele teria contado a algumas pessoas de confiança para fornecerem versões diferentes.

Topiary começou a ligar no número de Sabu no Google Voice de hora em hora, mas ninguém atendia. Era incomum para ele ficar off-line por mais de doze horas. Topiary esperou e torceu para que Sabu não estivesse numa cela sendo interrogado ou, pior, delatando. No IRC, Sabu continuava logado. Assim que o nickname dele ficou ocioso por vinte e quatro horas, a equipe o excluiu, só para garantir, caso os Feds estivessem vigiando.

– Estou muito preocupado – contou Topiary naquela manhã.

Sabu lhe dera instruções na semana anterior para que, se ele algum dia fosse capturado, Topiary acessasse sua conta no Twitter e tweetasse normalmente, enquanto a equipe deveria continuar anunciando hackeagens. Se os Feds realmente tinham detido Sabu, isso poderia ser sua salvação para evitar algumas

acusações. Topiary sentiu-se profundamente desanimado ao conferir a conta do rapaz no Twitter e se lembrar do quanto o hacker o motivara. No breve perfil, lia-se: “A todos os Anons: vocês fazem parte de algo incrível e poderoso. Não sucumbam a táticas de medo tão óbvias e arcaicas. Permaneçam livres”. Sabu podia ter pavio curto, mas também sabia ser inspirador.

Kayla mostrava igual preocupação e garantiu a Topiary: – Vou virar a internet de pernas para o ar se eu descobrir que Sabu foi atacado.

Ainda assim, a equipe viu-se num ardil 22, situação paradoxal em que não se consegue escapar devido a regras contraditórias. Se Sabu tivesse sido capturado e forçado a revelar informações, então existia uma grande chance de que os Feds pudessem monitorar o que eles estavam fazendo. Se eles não fizessem nada ou fugissem, isso imediatamente incriminaria Sabu.

À medida que a noite caía, Topiary tentou ligar no número de Sabu outra vez. Súbito, alguém atendeu ao telefone. Nenhuma voz se ouviu.

– Alô, quem fala? – indagou Topiary.

– David Davidson.

Sabu. Topiary soltou um suspiro de alívio. Parecia que o companheiro estava resfriado ou havia chorado. Explicou que a avó havia morrido e que tivera de providenciar os trâmites fúnebres. Em seguida indagou se o resto da equipe estava por perto e se Topiary podia informá-los de que ele estava de volta. Topiary primeiro não se importou com a possibilidade de Sabu ter mentido – simplesmente estava contente por falar com ele outra vez. Não muito tempo depois, Sabu modificou sua explicação e contou que na verdade tinha sido o aniversário da morte de sua avó. Quando os dois se falaram na primeira vez, Sabu talvez tivesse mudado a voz deliberadamente para fazer sua história soar mais autêntica. A essa altura, o FBI já registrava tudo que Sabu falava on-line com os membros do LulzSec, assim como tudo que ele falava pelo telefone com Topiary.

Sabu acabaria ficando off-line mais tempo do que de costume pelos próximos dias, à medida que começou a colaborar com o FBI, até mesmo trabalhando diariamente na base dos agentes. Às vezes mantinha o grupo informado sobre outros acontecimentos, mas o ainda alheio Topiary assumia mais responsabilidade pela equipe.

Como medida de precaução, Topiary apagou mais arquivos, e em seguida mudou todas as suas senhas e criptografias para torná-las ultraprotegidas. Mantinha todas as senhas no arquivo de um cartão SD

criptografado, com um caractere trocado em cada senha. Só ele sabia quais caracteres estavam trocados. Ainda assim, não conseguia deixar de espiar constantemente pela janela e ficar sobressaltado sempre que um furgão passava. Pela primeira vez, começou seriamente a imaginar se uma dupla de policiais uniformizados ia derrubar sua porta ao amanhecer do dia seguinte.

Poucos dias antes, ao sair para comprar comida, um dos drogados locais havia abordado Topiary quando ele retornava para casa.

– Ei – dissera o sujeito, acenando enquanto Topiary tirava os fones de ouvido. – Esses dias, a polícia bateu na sua porta – avisou o homem com forte sotaque escocês. O coração de Topiary começou a bater forte.

– Verdade? O que eles fizeram?

– Chegaram com a viatura. Daí dois deles saíram e bateram na sua porta, mas ninguém atendeu – contou ele, encolhendo os ombros.

Topiary fingiu não dar bola. O drogado podia estar mentindo, mas a polícia talvez tivesse aparecido quando ele passeava em seu local de meditação, com vista para o mar. E havia igual probabilidade de eles estarem fazendo uma batida antidrogas na área. Mesmo assim, ele decidiu apagar todo rastro de Topiary e do Anonymous de seu laptop, criptografar tudo que manteve e enviar todo o material para si mesmo via Hushmail.

Por fim, apagaria todo o conteúdo de seu laptop.

Se a polícia batesse à sua porta, eles encontrariam uma casa limpa com um computador de mesa raramente utilizado e seu laptop Dell de aparência inócua, dois monitores auxiliares para assistir a filmes e uma linha telefônica atravessando a sala presa com grampos. Nenhuma das caixas de pizza vazias associadas com hackers vivendo em porões. Quaisquer documentos que a polícia pudesse encontrar sobre o Anonymous em quaisquer de seus computadores poderiam passar por uma pesquisa que Topiary fazia para um livro. Encontrariam alguma música pirateada e um punhado de bases de dados com algumas centenas de milhares de nomes e senhas que ele obtivera de conhecidos

ou a partir de sua própria varredura para o LulzSec. Topiary a chamava de sua coleção pessoal. Às vezes a utilizava para suas próprias tentativas de doxear pessoas, mas na maior parte do tempo era só para colecionar.

Ele tentava não pensar que seu provedor de rede virtual privada, o HideMyAss, fosse um dia lhe entregar às autoridades. A sua lógica era a de que, se os clientes do HideMyAss um dia descobrissem que a empresa havia delatado um de seus usuários, eles a abandonariam em massa, e o provedor teria de fechar as portas. Com certeza eles nunca o entregariam.

***

Enquanto Sabu permanecia off-line sob o pretexto de cuidar de assuntos familiares, um rosto conhecido voltou a comparecer no LulzSec: Ryan. À primeira vista, isso fazia pouco sentido, levando em conta o comportamento temperamental de Ryan no passado e seus ataques cibernéticos contra os canais de comunicação do LulzSec, mas essa era a vida de um hacker. Até mesmo a mais explosiva das brigas poderia ser remediada quando alguém precisava de algo. Nesse caso, Ryan precisava de alguns amigos, e o LulzSec podia lançar mão do botnet mamute de Ryan, que infectava computadores via um aplicativo trapaceiro do Facebook.

Ryan tinha boas conexões no cenário hacker underground e atuava como administrador do Pastebin, a ferramenta de aplicativo textual que o LulzSec utilizava para publicar todos os seus vazamentos, e da Encyclopedia Dramatica. Ryan era como o garoto na escola de quem os colegas não necessariamente gostavam, mas com o qual se sentiam compelidos a fazer amizade porque ele tinha um Hummer novinho em folha e casa com piscina. Na vida real, Ryan não era rico, mas on-

-line ele parecia abastado; passara anos construindo um conjunto impressionante de recursos, desde servidores até seu botnet. Seus servidores ajudavam a hospedar a Encyclopedia Dramatica, e, depois de reatar a conexão com um membro da equipe do LulzSec na semana anterior, eles também hospedavam a nova rede de IRC do grupo, a lulzco.org.

Após Topiary primeiro reatar com Ryan no IRC, ele quis ouvir como soava a voz do novo aliado para melhor sondá-lo; por isso, os dois se adicionaram no Skype. Quando a voz de Ryan soou, o sotaque britânico dele era tão forte que parecia

quase australiano. Ryan falava num ritmo alucinante, abertamente gabando-se de seu botnet, de sua hackeagem e de como ele ganhava dinheiro no underground; carregava sua prosa com imprecações, depois descrevia em detalhes um sanduíche de presunto com pão caseiro que a mãe certa vez tinha lhe preparado. Ryan parecia desengonçado e inseguro, mas a opinião de Topiary sobre ele amenizou quando o rapaz explicou o motivo pelo qual vazara centenas de nomes dos AnonOps meses antes. Os operadores da rede o importunavam, e então outra pessoa reuniu os dados e os repassou para ele vazá-los. Águas passadas. Ah, acrescentou, aqueles dox com seu nome completo, endereço e número de telefone que haviam sido postados on-line? Isso se baseava em informações falsas criadas por ele há quatro anos. Ryan garantiu a Topiary que ele fizera os documentos falsos e os espalhara por todos os lugares de modo que suas informações verdadeiras permanecessem ocultas.

Topiary avaliou que percebia quando alguém não falava a verdade, em especial ouvindo a voz. Ryan, acreditava ele, era genuíno. De fato, começou a sentir pena do sujeito. O pessoal do AnonOps tinha acusado Ryan de ser um cretino perpetuamente zangado que gravava registros e atacava a esmo. Mas na verdade ele não era zangado; apenas inflamado. Talvez desse a impressão de ser rude, mas trabalhava arduamente e se envolvia nas coisas, pensou Topiary. Com Sabu fora de combate, sentia falta de alguém apaixonado e meio biruta com quem conversar, para contrabalançar sua personalidade pacata.

Ryan prometeu não gravar nenhum bate-papo e afirmou que daria à equipe do LulzSec controle completo sobre sua habilidade de realizar logging. Também disse que o grupo podia utilizar seu botnet a hora que desejasse. No passado, ele o utilizara para realizar ataques de DDoS em sites da Força Aérea dos EUA e depois ligar para debochar deles. Também podia ganhar centenas de dólares num dia sublocando o botnet a outros que desejavam usá-lo para propósitos escusos, como extorsão e batalhas entre hackers. Mas o LulzSec podia usá-lo grátis. Era como dar carne fresca a um cão faminto: com o botnet de Ryan, o LulzSec derrubaria qualquer site que desejasse num piscar de olhos.

Durante uma de suas ocasionais visitas no IRC, Sabu mencionou a Topiary que não gostava da ideia de contar com o apoio de Ryan. O LulzSec fazia contatos demais, acrescentou ele. (Não está claro se esse era o caso, ou por que o fato podia ter lhe causado preocupação a ele, agora que havia começado a trabalhar como informante do FBI.) Topiary argumentou que o próprio Sabu estivera convidando seus colaboradores de confiança para entrar no #pure-elite, inclusive

o vazador de registros M_nerva. Topiary venceu a discussão, e Ryan permaneceu. Com Sabu quase sempre afastado, Topiary desfrutava o lado mais divertido do que o LulzSec podia fazer com sua crescente horda de seguidores no Twitter. Depois de publicar as senhas administrativas de 55 sites pornô e 26 mil senhas de usuários pornô, recebeu comentários no Twitter dizendo que tinham usado a descarga de dados para hackear e-mails de outras pessoas ou, em um caso, descobrir que um cara estava “traindo a namorada”.

Topiary se deu conta de que era capaz de tornar as coisas mais interativas. Podia enviar um vídeo do YouTube a 100 mil pessoas e conceder ao dono da conta um imenso aumento nas visualizações, ou podia direcionar a horda para derrubar um pequeno site ou rede de IRC. Os ataques do LulzSec se tornariam bem mais divertidos. Ele e Ryan começaram a trocar ideias e a fazer alguns trotes telefônicos via Skype com alguns dos amigos de Ryan como plateia. Em seguida, Ryan configurou uma conta conjunta Skype Unlimited, de modo que o grupo conseguisse ligar a qualquer pessoa no mundo, gastando oitenta dólares sem pestanejar.

Topiary teve uma ideia. Em vez de aplicar trotes telefônicos, que tal se convencesse os seguidores do LulzSec no Twitter a ligar para eles? Topiary sugeriu configurar um número no Google Voice de modo que qualquer pessoa no mundo pudesse ligar para o LulzSec (ou pelo menos para ele).

Desejava que o número estampasse o nome do grupo, como 1-800-LULZSEC, mas não conseguiu encontrar um código de área em que o número funcionasse. Ansioso para provar sua capacidade, Ryan passou horas vasculhando cada número possível nos EUA até descobrir que 614, o código de área de Columbus, Ohio, estava disponível com os dígitos correspondentes. Agora eles tinham uma hotline telefônica: 1-614-LULZSEC.

Era um número grátis do Google que direcionava as ligações ao seu novo número no Skype Unlimited-World-Extra, que, por sua vez, podia retransmitir a dois outros potenciais números registrados com endereços IP falsos. A dupla criou duas mensagens na caixa postal, utilizando alteração de voz e sotaque francês exacerbado para os nomes ficcionais Pierre Dubois e François Deluxe, dizendo que eles não podiam atender ao telefone porque “Estamos muito ocupados deflorando suas internets”.

Tão logo Topiary anunciou a hotline na sala de bate-papo pública do LulzSec,

receberam várias ligações por minuto; atenderam a algumas e brincaram com os interlocutores. Sem fornecer quaisquer pistas, Topiary estabeleceu um prêmio de mil dólares para quem ligasse e acertasse a palavra mágica – *lemonade* –, mas ninguém deu o palpite certo e cerca de quarenta pessoas acharam que era *please*. No fim do dia, eles contabilizaram um total de 450 ligações.

Entre uma ligação e outra, Topiary redigiu um anúncio sobre o mais recente vazamento do grupo: um diretório listando todo e qualquer arquivo do servidor da web do Senado dos EUA, que lhes chegara de outro chapéu preto. Esse ataque grave podia levar alguém a vinte anos de cadeia, mas Topiary sentia-se mais ansioso para voltar à sua hotline do LulzSec.

– Esta é uma publicação pequena, só por diversão, de alguns dados internos do Senate.gov – escrevera Topiary. – Esse é um ato de guerra, cavalheiros? Algum problema?

Junto com esse vazamento, houve a revelação do código fonte e senhas da base de dados da empresa de jogos eletrônicos Bethesda – tópico completamente sem relação com o Senado, apenas um dos vazamentos que eles tinham ao dispor. Também dominavam uma base de dados de 200 mil usuários armazenada nos servidores da empresa de jogos eletrônicos Brink, mas não a publicaram porque "Na verdade gostamos dessa empresa e queremos que eles acelerem a produção do Skyrim. Não há de quê!". Na parte superior de cada publicação, agora havia uma breve lista de dados para contato e doações para o LulzSec, inclusive a linha direta e a sala de bate-papo na rede interativa.

– Não está claro o motivo pelo qual o LulzSec decidiu tentar constranger outra empresa de videogame a não ser se exibir – comentou o jornalista Chester Wisniewski, da Naked Security. – É difícil explicar atos aleatórios de sabotagem e desfiguração, por isso não vou tentar penetrar na mente das pessoas por trás desses ataques.

No entanto, isso não era uma questão de motivação, mas de circunstância. Na época em que Kayla tinha utilizado seu botnet para escrutinar a web em busca de vulnerabilidades, conectando-o a um canal de IRC e lançando mão de comandos básicos de bate-papo para rodar o programa, ela havia deparado com uma vulnerabilidade na rede do Bethesda que dava acesso aos servidores da empresa. Já que a empresa era tão grande, a equipe preferiu não vasculhar bases de dados imediatamente, utilizando a banda larga da Bethesda a fim de ajudá-los a buscar

outros sites para hackear e utilizando-a como local seguro para esconder bots. A empresa de jogos não imaginava que efetivamente estava sendo usada para hackear outros sites. Quando os servidores deixaram de ser úteis, chegara a hora de revelar os dados armazenados neles.

Agora as hackeagens estavam prestes a se tornar ainda mais arbitrárias. Sabendo que o botnet de Ryan podia derrubar qualquer coisa, Topiary anunciou a hotline do LulzSec pelo Twitter e informou ao público: – Escolham um alvo e vamos liquidá-lo.

Súbito a linha direta foi inundada com ligações, e as três pessoas que inicialmente entraram solicitaram empresas de videogame: Eve, Minecraft e League of Legends.

Em poucos minutos, o botnet de Ryan tinha derrubado as três, assim como um site chamado FinFisher.com, "porque aparentemente vende software de monitoramento ao governo ou merda parecida". Não era novidade alguma desferir ataques de DDoS a sites como esse. Também não era novidade obter uma ou duas horas de desativação, mas era a primeira vez que alguém se vangloriava por isso a 150 mil seguidores do Twitter ou chamava esse festival de DDoS de "Terça da Tomada Titânica".

– Se estiver bravo sobre a Minecraft, vamos adorar rir da sua cara pelo telefone – anunciou Topiary. – Ligue 614-LULZSEC e aproveite a chance de falar com Pierre Dubois!

Quando Topiary começou a pensar na expressão do meme da internet "Como funcionam os ímãs?", popularizada pelo duo de hip-hop Insane Clown Posse, ele ligou ao escritório do Magnets.com. Pediu à mulher que respondesse àquela pergunta, obtendo uma resposta perplexa, desligou, depois redirecionou a hotline do LulzSec à central telefônica do Magnets.com.

– Todo mundo ligue 614-LULZSEC para uma surpresa divertida – tweetou ele.

Uns três minutos depois, ligou o número novamente e escutou dezenas de telefones desligando ao mesmo tempo com respostas de "Aqui é Magnets.com... Ãhn...". Pediu para falar com um gerente. Quando surgiu uma voz masculina, Topiary explicou o motivo para a inundação de chamadas estranhas. Mérito do gerente que levou na esportiva.

– Como conseguiu fazer isso? – quis saber ele.

– Estamos testando nosso novo Canhão Telefônico Lulz – explicou Topiary. – Como estão se sentindo?

– Estou meio sem fôlego.

O Magnets.com estava recebendo mais de duzentas chamadas por minuto em seu centro de suporte ao cliente.

– Ok, vou cessar o ataque – disse Topiary.

– Ótimo, porque acho que estou prestes a desmaiar.

Com breves cliques, ele cessou o redirecionamento da hotline e escutou todos os telefones ao fundo subitamente silenciarem. Foi uma espécie de ataque de DDoS via telefone. Fazia sentido reutilizar o método. Logo ele estava redirecionando a hotline do LulzSec para o jogo on-line World of Warcraft, depois à central telefônica do FBI Detroit, e depois, naturalmente, aos escritórios da HBGary Inc.

– Cuide da turba enquanto estivermos fora, AaronBarr – tweetou Topiary em referência ao antigo executivo da empresa. – Obrigado, parceiro. Tchau por enquanto.

Nas próximas vinte e quatro horas, entre uma conversa e outra com hackers do LulzSec e o manejo da conta do Twitter, a ocupada mesa telefônica de Topiary recebeu 3500 chamadas perdidas e 1500 recados de voz; no dia seguinte, 5 mil chamadas perdidas e 2500 recados de voz.

Em breve, porém, Ryan começou a ficar inquieto. Queria fazer mais do que apenas brincar com as pessoas que ligavam para a hotline; queria voltar a atacar sites, grandes sites. Agora ele tinha uma plateia enlevada e uma gangue de pessoas dispostas a perseguir nomes grandes sob essa bandeira do LulzSec, ou do Antisec, ou do Anonymous. Seja qual fosse. Por iniciativa própria, conectou seu botnet, depois convocou a maioria de seus bots e mirou o principal site da CIA nos EUA. Então disparou.

Em poucos minutos, o CIA.gov saiu do ar.

– CIA no forno – avisou Ryan no Skype antes de começar um monólogo sobre o

quanto desprezava os EUA. Abismado, Topiary visitou o site principal da CIA e viu que realmente estava fora do ar. Não pôde evitar certo constrangimento. Era uma ação colossal. Mas não podia deixar sem propaganda. Por meio do Twitter, comunicou, quase discretamente: – Alvo derrubado: “cia.gov”. Por lulz.

Órgãos da mídia televisiva e impressa, bem como sites de notícias, instantaneamente prestaram atenção ao fato e publicaram manchetes garrafais de que o LulzSec havia acabado de atacar a CIA. Poucos informaram, incorretamente, que a CIA tinha sido “hackeada”. Agora, o LulzSec claramente estava provocando as autoridades, quase as convidando para vir e prender o grupo.

Por volta da mesma hora, Aaron Barr entrou no Twitter para enviar uma nova e pública mensagem ao chefe da HBGary Inc., Greg Hoglund: – Bom ver você – disse Barr. – Vamos estourar uma pipoca. Sinto que vem show por aí. – Topiary viu o comentário, que parecia ter vindo do nada.

– Oi, Aaron – respondeu Hoglund no primeiro tweet de sua vida, também direcionado ao LulzSec. – Criei minha conta no Twitter porque desejo assistir de camarote àquilo que está prestes a acontecer.

O instinto de Topiary foi reagir com ceticismo em relação à ameaça velada – ele recebia ameaças semelhantes todos os dias agora –, e respondeu com sarcasmo.

– O que significa kibafo33? – indagou a Barr via Twitter. – É uma combinação turco-portuguesa de “que” e “bafo”? Você também é um maçom do 33º grau?

Além do mais, Topiary tinha outras e mais importantes distrações. A cerca de 480 quilômetros dali, em Londres, o fundador do WikiLeaks, Julian Assange, ouvira falar que o LulzSec tinha derrubado o site da CIA e se divertia com o fato.

***

Para Assange, um simples ataque de DDoS contra o CIA.gov servia de inadiável alívio cômico. Desde que o Anonymous havia acorrido em sua defesa em dezembro, ele havia passado os últimos meses combatendo a ameaça de extradição para os Estados Unidos e as acusações de traição relativas à publicação, pelo WikiLeaks, de cabogramas diplomáticos.

Autoridades suecas tinham dobrado seus problemas também tentando a extradição, para que fosse investigado sobre suposto envolvimento em ofensas sexuais. Nesse meio-tempo, ele estava hospedado na casa de campo de um jornalista inglês, usando uma tornozeleira eletrônica e tentando acompanhar os acontecimentos do mundo da segurança cibernética. Difícil o LulzSec passar despercebido. Por um lado, o grupo parecia de comediantes destemidos. Por outro, havia claramente hackers hábeis na equipe.

Impressionado e talvez incapaz de se conter, Assange abriu a conta principal do WikiLeaks no Twitter e postou a seu quase um milhão de seguidores:

– O grupo LulzSec, defensor do WikiLeaks, derrubou a CIA... que tem uma força-tarefa sobre o WikiLeaks. – E acrescentou: – Enfim a CIA aprende o real significado de PQP.

Logo após algumas agências e sites de notícias relatarem que o WikiLeaks apoiava o LulzSec, ele apagou o primeiro tweet. Não queria ser associado publicamente com hackers que claramente eram chapéus pretos.

Em vez disso, decidiu que havia chegado a hora de secretamente tentar entrar em contato com o audacioso novo grupo que estava sob os holofotes.

Em 16 de junho, um dia depois de Ryan disparar seu botnet contra o CIA.gov, um colaborador do WikiLeaks entrou em contato com Topiary: – Tenho um contato do WikiLeaks que deseja falar com você – avisou a pessoa, e o direcionou a um novo servidor de IRC que podia servir de campo neutro para uma discussão particular. A rede: irc.shakebaby.net; o canal: #wikilulz. Inicialmente cético, Topiary acreditou estar sendo trollado pelo contato. Quando enfim conversou com um membro da equipe do WikiLeaks conhecido como q, que estava no canal com o nickname Dancing_Balls, solicitou para alguém postar algo na conta do WikiLeaks no Twitter. Assange, que supostamente tinha acesso exclusivo, fez o solicitado, publicando uma mensagem sobre o eBay e depois apagando o post. Topiary fez o mesmo na conta do LulzSec no Twitter. Mas ele precisava de prova adicional, já que a conta do WikiLeaks podia ter sido hackeada. “Posso fazer isso”, respondeu q. Em cinco minutos, colou um link para o YouTube na rede de bate-papo e avisou a Topiary que desse uma rápida conferida.

Topiary entrou no link e assistiu a uma gravação da tela de um laptop mostrando

a mesma rede na qual batiam papo, com o texto se movendo em tempo real. A câmera então abria uma panorâmica e mostrava um grisalho Julian Assange, sentado, fitando um laptop branco e apoiando o queixo com a mão, com ar pensativo. Trajava uma camisa alva, e a luz do sol se insinuava através de uma janela com cortinas sofisticadas. Momentos depois, q apagou o vídeo de vinte e dois segundos. Também no canal de IRC

com Topiary e q, apareceu Sabu, agora provavelmente cercado de agentes do FBI muito interessados monitorando a conversa.

– Diga a Assange que eu mandei um “oi” – disse Sabu a q.

– Ele também diz “oi” – disse q.

No começo, Topiary mostrou nervosismo. Ali estava o próprio Julian Assange, o fundador do WikiLeaks, fazendo contato com a sua equipe. Não conseguia imaginar por que Assange queria falar com o LulzSec. Em seguida, prestou atenção no que q e Assange diziam. Elogiaram o trabalho do LulzSec, acrescentando que tinham se divertido com o ataque de DDoS

contra a CIA. Com toda a rasgação de seda, quase parecia que *eles* é que estavam nervosos. Por um átimo, o LulzSec aparentou ter muito mais importância do que Topiary jamais sonhara.

A essa altura, alguns outros do núcleo da equipe, sabendo do que acontecia, também tinham entrado na sala de bate-papo. Sabu lhes forneceu um rápido resumo dos fatos e depois afirmou que isso podia significar ataques a alvos maiores.

– Minha equipe parece disposta a dominar sites tradicionais do governo – explicou ele a Assange e q no bate-papo. – Mas, ao ver como aquele vídeo foi removido, alguns deles estão céticos.

– Sim, eu removi o vídeo, já que era só para você, mas posso gravar um novo se você quiser J – disse q.

– Se precisarmos de confiança extra (principalmente minha equipe), daí ok – falou Sabu. – Mas por enquanto tudo bem.

Então q continuou a explicar por que ele e Assange tinham entrado em contato

com o LulzSec: precisavam de ajuda para infiltrar vários sites corporativos e governamentais da Islândia. Havia vários motivos para querer desforra. Um jovem membro do WikiLeaks havia recentemente ido à Islândia e sido detido no país insular. O WikiLeaks também estivera concorrendo ao acesso a um centro de dados num bunker subterrâneo, mas perdera para outro concorrente após o governo negar o espaço a eles.

Outro jornalista que apoiava o WikiLeaks encontrava-se detido pelas autoridades. Assange e q pareciam querer que o LulzSec tentasse dominar o serviço de e-mail dos sites governamentais, depois procurasse provas de corrupção ou pelo menos de que o governo atacava o WikiLeaks injustamente. Assim, tentavam sugerir que o governo islandês queria suprimir a liberdade do WikiLeaks de divulgar informações. Se pudessem vazar essas provas, explicaram eles, o fato poderia ajudar a instigar um levante alternativo na Islândia e além dela.

No dia seguinte, q e Assange quiseram falar com o LulzSec outra vez.

Talvez percebendo que Topiary continuava cético, q insistiu em carregar outro vídeo. Novamente mostrou a tela do laptop de q e o bate-papo interativo sendo atualizado em tempo real, depois um close em Assange em pessoa, apoiando o queixo na mão novamente, mas desta vez piscando e mexendo o touchpad em seu laptop. Em seguida, o rapaz conversava com uma mulher perto dele. Antes de o vídeo terminar, a câmera mostrava o ambiente ao redor de Assange. O vídeo tinha sido filmado e carregado em menos de cinco minutos. Topiary, que tinha experiência com Photoshop e manipulação de imagens, calculou que adulterar o vídeo para mostrar o bate-papo interativo e Assange na mesma sequência em um tempo tão curto teria sido incrivelmente difícil. Passou a acreditar que era tudo real.

Mas q não pedia que o LulzSec fizesse o papel de “matador de aluguel”

apenas pela bondade de seus corações. Havia potencial para ganho mútuo.

q oferecia fornecer ao grupo uma planilha de dados confidenciais do governo, um arquivo chamado RSA 128, cuidadosamente criptografado, que precisava ser decodificado. q não o enviou, mas descreveu o conteúdo.

– É um material bem pesado para decodificar – Sabu contou a q. – Vocês tentaram a simples força bruta?

q explicou que computadores no MIT tentaram decifrar os arquivos durante duas semanas sem sucesso. Topiary quis perguntar se Assange iria dar à equipe outras coisas para vazar, mas decidiu se calar. Parte dele não queria saber a resposta a isso. Já começava a parecer que o LulzSec estava prestes a se tornar uma versão chapéu preto do WikiLeaks. Se este tinha a seu dispor uma grande quantidade de dados confidenciais simplesmente muito arriscada de vazar, então agora dispunha de um primo mais sombrio e mais radical para providenciar o vazamento.

Topiary decidiu mencionar que o LulzSec era composto pela mesma equipe do ataque contra a HBGary. Assange comentou que havia ficado impressionado com a investida contra a HBGary, mas acrescentou: – Poderiam ter feito melhor. Primeiro deveriam ter vasculhado todos os e-mails.

– Poderíamos – reconheceu Topiary –, mas não somos um grupo de vazamentos. Apenas queríamos publicar o mais rápido possível.

– Sim, mas podiam ter publicado de forma mais estruturada – insistiu Assange.

– Não queríamos escrutinar 75 mil e-mails procurando provas de corrupção – rebateu Topiary novamente.

Ele se lembrou de como havia vasculhado o conteúdo daqueles e-mails não em busca de escândalo, mas para localizar a carta de amor de Penny Leavy a Greg Hoglund e para descobrir o personagem de Barr no World of Warcraft.

A equipe decidiu convidar Assange e q para a rede de IRC no servidor de Sabu. Topiary criou um canal para todos eles conversarem e o batizou de #IceLulz. Segundo q, o WikiLeaks estava disposto a ajudar mais o grupo, com coisas como servidores ou até mesmo aconselhamento constante, mas não desejava conectar a organização com o LulzSec de modo óbvio demais.

De fato, quando Topiary disse a q que fosse em frente e enviasse o arquivo RSA 128 a qualquer hora, ele pareceu hesitar.

– Sim, quem sabe no futuro a gente vê como vai funcionar isso – falou q.

Ele nunca enviou o arquivo, pelo menos não a Topiary.

Ainda assim, como Topiary lembrou-se mais tarde, Sabu mostrava-se “mais

empolgado do que nunca", nas nuvens, por-que o WikiLeaks pedia a ajuda dele. Não está claro se Sabu realmente estava assombrado pela perspectiva de que agora também ajudava a implicar Assange. Seis meses antes, acreditara de modo tão apaixonado na causa do WikiLeaks que se arriscara a trazer seu nome de hacker a público pela primeira vez em nove anos. Outra possibilidade: o FBI incitava Sabu a manter o contato com Assange para ajudar a coletar provas contra um dos mais notórios infratores de dados confidenciais governamentais dos tempos recentes.

Parecia provável que, se Sabu tivesse ajudado, por exemplo, a extraditar Assange aos EUA, isso teria melhorado drasticamente seu acordo.

– É o nosso momento mais sublime – vibrou Sabu com a equipe.

Ele e q começaram a conversar com mais profundidade sobre vários sites, e então Sabu enviou links de dois sites do governo e uma empresa para o restante da equipe, encarregando-os de encontrar um jeito de penetrar em suas redes e abiscoitar e-mails. Ao longo dos dias seguintes, Topiary passou a missão de manter contato com o WikiLeaks a Sabu, e, ao longo das semanas seguintes, Assange visitou a rede de bate-papo do LulzSec em mais quatro ou cinco oportunidades.

Topiary deixou aberto o canal de IRC #IceLulz em seu laptop e o manteve assim. Logo, porém, o canal se tornou apenas mais um entre trinta outros canais exigindo sua atenção, outra página de texto vermelho piscante.

CAPÍTULO 23

Fim explosivo

O LulzSec agora estava tão importante que fazia o Anonymous e seu manancial 4chan parecerem brincalhões inofensivos. No 4chan, dificilmente alguém gostava de conversar sobre o grupo.

– Literalmente ninguém se importa o suficiente com o LulzSec a ponto de postar sobre eles – observou William na época. – Esses caras estão conquistando fama por coisas que antigamente nos traziam fama.

A certa altura, Topiary criou um tópico no *b* indagando o que os frequentadores pensavam sobre o LulzSec. Obteve uma resposta de meio a meio, e o tópico recebeu 350 comentários após poucos minutos antes de desaparecer. Quando ele confirmou a legitimidade do primeiro post como OP na conta do LulzSec no Twitter, isso causou alvoroço no painel *b*.

Mas os newfags, sujeitos sempre ávidos por participarem de um ataque organizado no 4chan, agora andavam irritados porque o LulzSec roubava o poder do site deles e desejavam atacar os novos campeões da perturbação na internet. Quando Topiary e Ryan viram um tópico no *b* tramando "caçar" os hackers do LulzSec, o painel, que odiava que forasteiros soubessem de sua existência, tornou-se a próxima tenra vítima.

– Todo mundo entra no *b* para postar material sobre o Boxxy, o LulzSec lhe enviando lá, e triforces – solicitou Topiary aos seguidores do LulzSec no Twitter, referindo-se à gíria que significa postar três triângulos equiláteros Unicode em tal configuração que um quarto triângulo igual caiba no meio deles.

Em troca, ele prometeu publicar uma compilação de vários milhares de endereços de e-mail e senhas, sem mencionar que sairia de sua própria coleção pessoal. Perseguir o 4chan não significava que o LulzSec atacava o Anonymous, como alguns blogs sugeriram.

– É como dizer que entramos em guerra com os Estados Unidos porque pisoteamos um x-burguer – comparou Topiary.

O painel de imagem logo foi dominado por fãs do LulzSec.

– Como sempre, o LulzSec fornece – tweetou a conta. – 62 mil emails/senhas só para vocês. Aproveitem.

Em dez minutos, o banco de dados de Topiary havia sido baixado 3200

vezes, e as pessoas começaram a utilizá-lo para hackear contas aleatórias, desde o Facebook até o World of Warcraft. Uma pessoa encontrou uma combinação de e-mail e senha que havia sido reutilizada numa conta de Xbox, PayPal, Facebook, Twitter, YouTube e "O lote inteiro!", exclamou ele no Twitter. "SORTE GRANDE."

– Vocês todos foram a inspiração de que eu precisava para detonar com o Facebook de meu companheiro de quarto – comemorou outro.

– É bom ver uma revigorante carnificina – disse Topiary à horda, agora chamada por ele de "lagartos lulz"; e as vítimas planejadas, de "peões".

– A publicação de 62 mil possíveis combinações de contas é um tesouro para mentes criativas pilharem. Pensem nisso como a escavação de um incomparável poço de mina.

Sem demora, mais de 40 mil pessoas tinham baixado a base de dados e a utilizavam para hackear toda sorte de contas de redes sociais.

Para Topiary, os 220 mil seguidores do LulzSec no Twitter tinham se tornado não só uma comunidade, mas uma plateia. Nos dias seguintes, ele brincava constantemente com eles via Twitter, remetendo mensagens ao FBIPressOffice, a conta da assessoria de imprensa do FBI no Twitter, dizendo que "urinamos em seu Cheerios", depois canalizando mais solicitações para atacar sites menores, enviando os seguidores do Twitter a um vídeo engraçado e assistindo à derrubada do site.

Qualquer um que tenha conhecido Topiary dificilmente perceberia semelhança entre sua persona na vida real e a voz arrogante que ele costumava usar como porta-voz do LulzSec. Era tudo encenação, e para ele não passava de uma interpretação de ator. Algumas vezes ele tentava soar como Sabu ou Kayla, de modo a parecer que mais de uma pessoa abastecia as mensagens do Twitter, mas na maior parte do tempo falava como se fosse o homem de monóculo e cartola. E um constante fluxo de gente indagava como podia participar.

– Agora temos toda essa atenção – Topiary comentou discretamente com a cúpula da equipe –, e as pessoas pedem para se unir a nós. Que tal se eu redigisse algo sobre o novo movimento Antisec, atacando governos e bancos? Alguém apoia isso?

Os outros na equipe, inclusive Sabu, disseram sim. Agora, com o apoio silencioso de um nome respeitado como o WikiLeaks, fazia sentido, de uma vez por todas, dar um caráter sério às atividades do LulzSec.

Imediatamente Topiary escreveu um novo comunicado oficial informando que o Antisec "começaria hoje", convocando mais pessoas a participarem da insurgência cibernética que o LulzSec revivia de modo espontâneo. Na noite de domingo, 19 de junho, ele publicou uma declaração convidando chapéus brancos, chapéus pretos e chapéus cinza, e praticamente qualquer outra pessoa, a participar da rebelião. Mais tarde, disse que redigir o texto havia sido, como sempre, como redigir um conto de ficção: "Saudações, Lagartos Lulz", começava o texto. "Como sabemos, o governo e os terroristas de segurança chapéus brancos mundo afora continuam a dominar e a controlar nosso oceano da internet... Agora estamos nos juntando ao Anonymous e a todos os encouraçados afiliados...

Endossamos completamente a exibição do nome "Antisec" em qualquer desfiguração de site governamental ou arte de grafite verdadeira... A prioridade é roubar e vazar quaisquer informações governamentais sigilosas, inclusive coleções de e-mails e documentações. Alvos prioritários são bancos e outros estabelecimentos de alto escalão."

Nem tão interessado assim em atacar bancos e governos e mais interessado em como as pessoas responderiam à convocação às armas, ele postou o comunicado oficial e foi dormir. A cabeça fervilhava por mais um dia caótico acompanhando a mídia, as senhas pessoais sempre mutantes, as operações de ritmo acelerado, os novos sectários, os tweets, as reações, o alvoroço, o caos de ver mais de mil posts de noticiários e blogs comentando um post Pastebin que ele digitara no Notepad. Jamais sonhara que tanta coisa aconteceria quando ele e Sabu primeiro discutiram a reativação da equipe. Não parecia que as coisas saíam do controle no olho do furacão, pelo menos ainda não. Quando muito, Topiary começava a sentir aquele antigo e familiar incômodo no fundo da mente. Uma sensação de que essa mais recente experiência em perturbar a internet por meio do LulzSec tinha se esgotado e se tornava tediosa. Um eco da inquietude que ele sentira com

o AnonOps há poucos meses apenas.

Nesse meio-tempo, Ryan tornara-se cada vez mais irritante para Topiary, com seus solitários e desesperados pedidos de atenção. Dois dias antes, após doze horas distante de seu computador porque havia adormecido, Topiary descobriu em seu laptop mais de doze mensagens de Ryan perguntando por que ele estava sendo ignorado.

Claro, não havia como Topiary parar. Ele era o principal porta-voz do LulzSec, um supremo motivador para a equipe e seus sectários. Abandonar o grupo exigiria um imenso esforço prático e emocional.

Com dificuldade para dormir, agora Topiary habitualmente relanceava o olhar pela janela sempre que escutava um carro passar. Confessou em conversas privadas que esperava uma batida policial a qualquer dia. A aceitação parecia a melhor maneira de lidar com essas coisas. Suas emoções oscilavam da exultação por um novo e extravagante vazamento até a nauseante paranoia de que estava prestes a ser doxeado ou, pior, detido pela polícia. Ryan pensava o mesmo e comentava que, noite após noite, ia dormir esperando ser detido no dia seguinte.

– Joguei a toalha; não me importo mais – disse Topiary. Imaginava como seria a cadeia? – Não gosto de pensar nisso – respondeu ele.

Também não conseguia esquecer as palavras rigorosas adicionadas por Greg Hoglund no segundo tweet há poucos dias, a mensagem que ele na ocasião desprezara despreocupadamente.

– Aaron – Hoglund dissera. – Quero estar aqui para ver os frutos de nosso trabalho ao longo dos últimos dois meses. LOL.

***

Ao acordar na segunda-feira, 20 de junho, Topiary teve uma surpresa. A resposta ao comunicado Antisec havia sido bem superior ao que ele esperava. Dezenas de milhares de pessoas o tinham lido (por fim, quase 250 mil pessoas acessaram a página), e a mídia ansiosamente relatava que o LulzSec havia “se juntado ao Anonymous” e declarado guerra contra praticamente todas as pessoas em posição de autoridade na esperança de expor corrupção. Parecia que os anarquistas cibernéticos de todos os lugares estavam enlouquecendo. Naquele dia, o noticiário televisivo local da CBS de San Diego relatou uma misteriosa

grafitagem escura surgida no calçadão de Mission Beach: o tosco desenho de um homem de cartola e bigode com as palavras “Antisec” num balão de diálogo.

– Fiquei abismado – lembrou-se Topiary mais tarde. – Minha declaração feita em Notepad sobre o Antisec provocou grande afluência de usuários aos servidores do AnonOps. Parecia a Operação Vingança vitaminada. Por um instante, eu me senti incrivelmente culpado por algum motivo. As palavras eram quase ficção para mim, apenas outro texto qualquer, mas atingiram tantas pessoas, que agora arriscavam seus pescoços pela causa.

Alguém inclusive tinha saído e pichado Antisec na mureta do calçadão de Miami Beach, ganhando as manchetes.

Ryan também estava eletrizado com o novo entusiasmo em massa pelo Antisec. Naturalmente, ele se tornou mais ansioso do que nunca para fazer bom uso de seu botnet. Mais tarde naquele dia começou a atacar outros alvos importantes: o Ministério da Fazenda britânico, depois a NSA, depois o FBI. Enfim, obteve sucesso e derrubou o site da Agência Britânica contra o Crime Organizado Grave (SOCA, do inglês *Serious Organized Crime Agency*). Qualquer coisa que terminasse em .mil ou .gov transformou-se em alvo. Topiary assistiu, arrebatado, e após um tempinho decidiu que seria bom que Ryan se acalmasse. Não queria que as coisas fugissem do controle.

Ainda assim, não pretendia desperdiçar o crédito do ataque do LulzSec contra a SOCA, por isso anunciou no Twitter, novamente sem o costumeiro estardalhaço: – Alvo derrubado: soca.gov.uk. Em nome do Antisec.

Comparado com a CIA, isso parecia um ataque de menor proporção, e nem sequer funcionara plenamente, já que o site da SOCA ficou inativo apenas para certos visitantes. Mas, logo depois, alguém da SOCA enviou uma mensagem à Polícia Metropolitana de Londres dizendo que o site havia sido derrubado. Ryan estivera lançando ataques de DDoS a partir de seu computador durante meses, mas agora, enfim, a polícia era incitada a agir.

Mais tarde naquela mesma segunda-feira, por volta das 22h30, enquanto Ryan prosseguia os ataques de DDoS contra o site da Agência Britânica contra o Crime Organizado Grave, dez viaturas policiais silenciosamente estacionaram diante de sua residência. O endereço que eles tinham recebido pertencia a Ryan Cleary, dezenove anos, nerd de informática, que morava com os pais numa

discreta casa geminada em Essex, Inglaterra. Eis que eram verdadeiros os dox que Ryan tinha alegado serem falsos. Durante o tempo todo, ele realmente morava naquele endereço e realmente estivera utilizando seu prenome verdadeiro. Ao entrar no quarto retangular do rapaz, a polícia deparou com cortinas cobertas de papel laminado para bloquear toda e qualquer luz solar, cama de solteiro, escrivaninha bagunçada coberta de salgadinhos de batata e supostamente cerca de £ 7000 (em torno de US$ 11.340, com base no câmbio daquele dia) em dinheiro na gaveta. Pálido, com buço de adolescente e levemente rechonchudo, Ryan saíra de casa a última vez no Natal – há seis meses.

A polícia o interrogou durante cinco horas, depois deu voz de prisão.

Por volta das duas da madrugada, ele se desconectou do MSN com a mensagem de despedida: “largando”. Não foi a piada interna “volto logo; FBI na porta”, mas também não era a mensagem de despedida normalmente utilizada por ele. A polícia o conduziu nas primeiras horas da manhã de terça-feira até a delegacia de Charing Cross, no centro de Londres, para interrogatórios adicionais. Naquele momento, agentes do FBI estavam a bordo de um avião rumo a Londres, e Topiary estava ferrado no sono em sua cama, completamente alheio ao que acontecia.

Naquela manhã, a Polícia Metropolitana de Londres anunciou que um jovem de dezoito anos tinha sido preso e acusado de lançar ataques de DDoS contra várias organizações. Em poucas horas, os tabloides ingleses veiculavam as notícias, seguidos por importantes órgãos de comunicação dos Estados Unidos. Embora a polícia não tivesse mencionado o LulzSec em seu comunicado, vários jornais registraram, estranhamente, que o “cabeça”

do LulzSec fora preso.

Quando Topiary entrou nas salas de bate-papo privadas do LulzSec na manhã seguinte, deparou com o mesmo tipo de conversa assustada que havia acompanhado o sumiço de Sabu. Topiary lentamente se deu conta do que acontecia. Mesmo assim, Tflow e Sabu disseram que estavam aliviados.

Os dois tinham acompanhado as notícias sobre a prisão e pensado que era Topiary.

– Agora o Ryan está definitivamente ferrado – disse Topiary.

Sentia-se entorpecido. Por fim, o nome de Ryan foi publicado, e um jornal fez uma reportagem com a família dele. Entrevistaram a mãe, que explicou como ela precisava deixar os pratos de comida diante da porta porque ele nunca saía do quarto, e como ele quase tinha se suicidado numa ocasião em que ela tentara afastá-lo do computador. O artigo trazia uma foto de Ryan, um colegial de olhos grandes e expressivos, junto com uma foto mostrando seu quarto. Na foto havia legendas apontando todos os itens, desde a cobertura da janela com papel laminado até o pôster pseudomotivacional na parede, com duas mulheres seminuas, e o título "Trabalho em equipe". Topiary reconheceu tudo de seus bate-papos com vídeo ligado. Os jornais não pareciam conhecer nem a metade das excentricidades de Ryan. Um ano antes, ele tinha cultivado maconha no canteiro do peitoril da janela. Sua escrivaninha agora estava sem entulhos e salgadinhos de batata, provavelmente organizada pela mãe dele. Uma semana antes, Ryan, de agulha hipodérmica em punho, começou a perfurar o dedão do pé diante da webcam. Acima de tudo, a ideia da prisão agora parecia bem mais perto de se tornar realidade.

Sabu e Topiary conversaram pelo telefone. Concordaram em mudar seus endereços de e-mail, seus nicknames públicos e tudo que Ryan sabia, porque ele iria delatar. Conversaram sobre encontrar novos servidores para hospedar suas redes de IRC e o site LulzSecurity. Diante do público, Topiary fingiu que nada havia acontecido: – Parece que o glorioso líder do LulzSec foi detido – comentou no Twitter. – Agora está tudo perdido... esperem... continuamos todos aqui!

Quem foi o pobre miserável que eles prenderam?

Havia outro probleminha a resolver: M_nerva. Durante o tempo inteiro, eles sabiam que o hacker responsável pelo vazamento dos registros de bate-papo do #pure-elite havia trabalhado com Ryan em certos negócios escusos. Com Ryan saindo de cena, não havia mais a necessidade de perdoar a M_nerva. Enfim, agora era seguro buscar desforra. Topiary publicou um comunicado oficial sobre Marshall "M_nerva" Webb, remetendo-o ao FBI como oferta útil de novas informações.

– Quem dedura leva sutura – escrevera ele, sem saber que o seu confidente mais íntimo, Sabu, tornara-se um delator bem mais perigoso.

O público estava curioso por saber quem era o delator, e a página obteve mais de

mil visualizações em vinte segundos. Levou algumas semanas para que o FBI seguisse as informações sobre M_nerva, mas no final de junho as autoridades federais fariam uma batida na residência de Webb, em Ohio.

Nesse meio-tempo, havia mais de 300 mil pessoas seguindo o LulzSec no Twitter, mais de 135 ávidos adeptos no LulzSec Brasil, grupos hackers na Espanha e no Irã desejando unir forças, ofertas constantes de vazamentos de bases de dados, controle de algumas dúzias de sites governamentais e mais de um gigabyte de dados a serem publicados. Isso incluía 12 mil senhas de um site da OTAN, centenas de documentos policiais internos aleatórios, documentos governamentais, um vídeo da polícia acidentalmente desovando um cadáver de um avião, fotos de carne humana espalhada na rua; "o painel *b* adoraria esse material", pensou Topiary. Tentava não pensar no fato de que ataques adicionais resultariam em um maior tempo de condenação. Convenceu-se de que o LulzSec se tornara uma espécie de WikiLeaks – apenas vazava informações repassadas por outrem.

Nesse meio-tempo, o FBI se apressava para acompanhar o novo informante, plugado nesse mundo dinâmico. À medida que os hackers ofereciam vulnerabilidades para Sabu em encontros secretos de IRC, ele as repassava a seus novos supervisores a fim de que essas brechas de segurança pudessem ser corrigidas. Sabu habilmente manipulava o LulzSec, fingindo atuar com genuína cumplicidade enquanto secretamente cooperava com as autoridades para impedir a execução de muitos daqueles ataques potenciais. Com as coisas se movendo tão rapidamente, Topiary, Kayla, Tflow e os demais não tinham tempo de rastrear quantas vulnerabilidades conduziam a becos sem saída, graças a Sabu. O grupo estava sempre à espreita do próximo grande ataque.

– Estamos nos desafiando a progredir a empreitadas maiores – explicou Topiary na época. – Alvos divertidos e maiores.

Agora era impossível voltar atrás.

***

Entre o conjunto de ofertas que Topiary e Sabu receberam para fazer ataques e obter dados, uma delas se destacou. Caía a noite nas ilhas Shetland quando um hacker que estivera falando com Sabu e que não havia conseguido o seu objetivo entrou em contato com Topiary para informar que obtivera acesso a centenas de

arquivos secretos e informações de usuários, após hackear a rede do departamento de polícia do Arizona.

Ativista apaixonado que combatia o perfilamento racial (uso de estereótipos para prever comportamento criminal) naquele estado, ele desejava publicar os dados como represália. Topiary reconheceu o nome, pois Sabu o havia mencionado antes. Após o hacker ter carregado os dados em um servidor secreto, Tflow, Pwnsauce e Topiary ficaram curiosos para ver seu conteúdo. Tratava-se de uma pasta contendo mais de setecentos documentos. Havia e-mails constrangedores reclamando sobre um policial assustado que tinha corrido e se escondido numa vala durante um recente tiroteio, dados inócuos sobre uma nova campanha de trânsito seguro e endereços e dados para contato de policiais do Arizona. Com pesquisa suficiente, o hacker almejava que esse conjunto de documentos pudesse revelar práticas corruptas no departamento. Ele expôs de modo convincente a existência de preconceito sistêmico na polícia da fronteira, e Topiary, empregando sua costumeira percepção despreocupada em relação às coisas, imaginou que o hacker deveria redigir seu próprio comunicado de imprensa – a primeira vez que alguém, à exceção de Topiary, escreveria uma mensagem dessas para o LulzSec. Tflow criou um arquivo torrent.

Não se dispunha de muito tempo para conferir o comunicado de imprensa e não houve cortes. Assim que tudo ficou pronto, Topiary o publicou. O comunicado de imprensa recebeu o título de “Chinga La Migra”, e o subtítulo “Abaixo os porcos”; ao lado disso havia a imagem de uma metralhadora AK-47 desenhada com símbolos de teclado. Topiary fez uma releitura. Quando releu o comunicado de imprensa, agora já público, não percebeu o usual tapa com luva de pelica em uma instituição ampla e sem rosto, mas uma polêmica agressiva contra policiais verdadeiros que revelava seus endereços residenciais. Ao googlar Chinga La Migra, descobriu que significava “Foda-se a polícia” em espanhol. Imediatamente se arrependeu de postar o comunicado do outro hacker. Era quase um estímulo às pessoas atacarem a polícia. Nesse meio-tempo, Tflow também tinha googlado Chinga La Migra e teve exatamente a mesma sensação.

Enviou uma mensagem a Topiary. Era demais. A declaração o fez sentir-se “radical”.

– Não queremos que os policiais sejam mortos – respondeu Topiary, concordando. – Não é meu estilo.

Também não era o de Tflow.

Topiary acabara de combinar uma entrevista por meio de mensagens de texto instantâneas com o *Newsnight*, noticiário televisivo da BBC, para aquela noite, 24 de junho. Foi uma de suas poucas entrevistas à mídia enquanto o LulzSec permanecia ativo. Adotando sua postura de ator, fez declarações pomposas sobre antissegurança e a corrupção que o seu grupo combatia.

– As pessoas temem os "figurões" – contou ele ao produtor da BBC, Adam Livingstone –, e estamos aqui para fazê-los cair alguns níveis.

Mas sentiu as palavras se engasgarem na garganta.

Quando realmente pensou no que o LulzSec havia se transformado, percebeu que já estava longe de ser um grupo que simultaneamente entretinha e consertava o mundo. Não fazia nenhuma dessas coisas. Era o caos. Agora, todos os dias a cúpula passava mais tempo lidando com assuntos internos, conspirando contra trolls como Jester e Backtrace, extirpando delatores ou preocupando-se com o que Ryan poderia contar à polícia. Há mais de uma semana a equipe não se reunia para valer e trabalhava em um vazamento original ou coisa parecida. Apenas horas antes da entrevista de Topiary com a televisão BBC, o jornal *The Guardian* teve acesso ao registro dos bate-papos do #pure-elite, vazado semanas antes por M_nerva, e publicou um artigo dizendo que o LulzSec era "um grupo desorganizado obcecado com cobertura midiática e desconfiado de outros hackers". A aura que circundava o LulzSec parecia se apagar.

– Isso está ficando irritante – exclamou Topiary numa entrevista. – Dois meses atrás, éramos uma equipe pequena trabalhando em operações sem transtornos externos. Agora é um entra e sai de gente, grupos "inimigos", imprensa fazendo declarações idiotas, gente tentando envolver política no meio, gente começando a dramatizar a toda hora. Meio que fora de controle.

Boatos corriam até mesmo na página do LulzSec no Wikipedia.

As distrações causadas por hackers inimigos, trolls, imprensa e mal-entendidos pela blogosfera tornaram-se esmagadoras. Recentemente, alguém copiara e colara o logotipo do LulzSec num post Pastebin, alegando (fazendo se passar pelo LulzSec) que eles tinham hackeado toda a base de dados do censo britânico – mais de 70 milhões de pessoas. A imprensa nacional, de modo esbaforido, pintou a informação como outra ameaça legítima do LulzSec. O LulzSec estava

se tornando parecido com o Anonymous: qualquer um podia alegar pertencer ao grupo e ser levado a sério.

– Em toda parte tem gente fingindo que é o LulzSec – comentou Topiary.

Ignorar os trolls não era suficiente, pois, quando Topiary fazia o logon nas salas de bate-papo privadas do LulzSec para falar com sua equipe, percebia que o pessoal ali tinha passado a hora anterior conversando sobre delatores e inimigos. Muitas vezes era impossível não dar atenção ao fato, e, quando Topiary silenciava nessas conversas, Sabu questionava por que ele não estava se manifestando, e a conversa ficava estranha.

Topiary enfim tomou uma decisão. Na noite de sexta-feira, 24 de junho, quatro dias após a prisão de Ryan, decidiu contar aos demais que ele queria sair. Seria difícil porque, na condição de porta-voz do LulzSec, a saída significava a provável dissolução da equipe. Enquanto entrava no canal de bate-papo privado do LulzSec, Tflow se antecipou a ele: – Pessoal. Topiary, AVunit, estão aí? – indagou Tflow.

– Sim – respondeu Topiary.

– Bem, eu quero abandonar o LulzSec *Anon etc.* por um tempo. E

pretendo repassar qualquer material relacionado ao site a vocês, inclusive domínios.

Topiary sentiu uma súbita onda de alívio. A própria ideia de abandonar o LulzSec parecia dissipar todas as outras distrações e ansiedades. Era possível dar um fim a isso. Ele quis que Tflow explanasse seus motivos para sair, de modo que o grupo pudesse debater o assunto. Talvez outros dissessem que também queriam sair.

– Alguma razão para sua saída? – indagou.

– Vou ser honesto – respondeu Tflow. – A observação “Abaixo os porcos” no último comunicado de imprensa, sobre a qual eu não sabia o significado antes, está me fazendo sentir radical e deprimido, por isso preciso de um tempo. Agora os agentes do FBI provavelmente não vão deixar pedra sobre pedra, por isso vou apagar meu disco rígido e reinicializar do nada.

Outro vislumbre de otimismo. Seria difícil abrir mão do nome e da ação, mas havia algo atrativo em recomeçar do zero. Concordou na hora.

– Ando pensando em algo parecido – disse Topiary. – Como você disse, a pressão é insana... Quer dizer, um amigo que não tem nada a ver conosco viu Ryan na primeira página do jornaleco local. Sei que não quero estar na primeira página do jornaleco local. E nem vocês. – E em seguida acrescentou: – Todos os nossos vazamentos vieram de outras pessoas.

– Então acha que todos nós devíamos apenas nos separar por um tempo ou o quê? – indagou Tflow.

– Acho que seria classudo velejar mar adentro e nunca ser capturado – cismou Topiary. – Em dez anos seremos o maior grupo de hackeagem do mundo inteiro. De todos os tempos.

Parecia piada, mas o pensamento de sair de cena em alto estilo, como uma banda famosa de rock que se desintegra no topo das paradas, subitamente fez parecer o término do LulzSec uma boa ideia. Óbvia, inclusive.

Topiary e Tflow começaram a discutir sua derradeira e explosiva publicação de algumas das pilhas de dados que estavam em seu poder há semanas. Um hacker estadunidense dera a Tflow uma provisão de documentos corporativos roubados dos servidores da AT&T. Havia dados de logon de uma livraria da OTAN, assim como outros logons .gov e .mil.

Tflow tinha pensado que os documentos da AT&T eram valiosos o suficiente para constituir uma publicação separada, mas o Chinga La Migra abrira os olhos do grupo para o quanto as coisas se tornaram realmente fúteis.

– Já não dou mais a mínima – disse ele. – Publique tudo.

Então Tflow conferiu o calendário e viu que tudo isso fazia mais sentido.

– Na segunda-feira completamos exatos cinquenta dias de existência – acrescentou ele.

Poderiam chamar a publicação final de Cinquenta Dias de Lulz. E talvez parecesse que ela havia sido planejada desde o começo.

Sabu apareceu on-line.

– E aí – disse ele.

Topiary teve um pressentimento, mas continuou a discutir aspectos práticos com Tflow, enquanto Sabu se inteirava da conversa.

– Uau – exclamou Sabu enfim. – Compreendo seus pontos de vista, mas não há como voltar atrás. Ultrapassamos o ponto do não retorno.

Topiary já estava ficando cansado do raciocínio de “ponto do não retorno” de Sabu e quis lembrá-lo de que ele e o LulzSec não eram tão poderosos quanto Sabu pensava.

– Sabu, quando foi a última vez que, como LulzSec, vazamos algo descoberto por nós? – indagou Topiary.

Listou os vazamentos da Fox, Sony, OTAN, Senate.gov – alvos de ataques cibernéticos entregues de bandeja por outros hackers. Só os vazamentos da Infragard e da PBS tinham sido realmente executados pelos hackers do LulzSec. No fim, o grupo tornara-se como o Anonymous, uma marca que outros punks cibernéticos podiam explorar para seus próprios desideratos, seja para se acharem mais importantes, seja para se acobertarem. Se, por um lado, isso lhes trouxera fama e respeito, por outro aumentava amplamente sua culpabilidade perante a polícia.

– Podem sair – Sabu disse enfim. – Estou fodido mais cedo ou mais tarde, por isso não tenho alternativa senão continuar.

Apesar da empolgação, Topiary e Tflow nunca se sentiram verdadeiramente presos na armadilha do LulzSec. Assim, quando Sabu mudou de discurso e começou a pedir a eles que ficassem, acrescentando que o estavam abandonando, subitamente aquilo parecia a tentativa de rastejar para fora de um barril giratório. Logo AVunit e Pwnsauce também entraram na sala de bate-papo e concordaram que era hora de dar um tempo. Até mesmo Kayla apareceu e frisou que, embora não se importasse – “Só deixo rolar” foram suas palavras –, ela entendia o raciocínio por trás do desejo de parar.

Topiary soltou um suspiro.

– Sabem que sou adepto dessa teoria niilista “temos de continuar” – frisou ele –, mas gosto de minha vida, brothers. Não quero ser preso.

Encorajado por Tflow, ele começou a falar sobre como, de qualquer modo, o movimento Antisec continuaria sem eles; o grupo havia velejado ao alto-mar, deixando um rastro de tumulto e o revival de um movimento contra os chapéus brancos, governos e corporações. Mas, por mais que tentasse, não conseguiu apaziguar Sabu, que, até onde o IRC permitia, parecia exagerar em fazê-los se sentirem culpados: – Está bem, podem ir embora. Vou ser o único faggot a sobrar.

Parecia que Sabu havia passado por diversos estágios de intenção com o LulzSec, inicialmente empolgado com a perspectiva de criar o grupo, depois ainda mais entusiasmado à medida que recebeu apoio de outros hackers mais antigos e do próprio Julian Assange. Topiary começou a pensar que Sabu estava quase agindo de modo suicida. Mais provavelmente: Hector Monsegur não tinha mais nada a perder, e o FBI precisava de mais provas contra os hackers do LulzSec.

– Sabu, estamos deixando para trás o rosto público do LulzSec com uma retirada em grande estilo – arriscou ele. – O movimento pelo qual você lutou vai continuar.

Foi inútil. Após alguns minutos, Sabu começou a conversar com cada um dos hackers individualmente. Ele não escondia a raiva.

Logo Topiary viu um texto piscante em sua tela indicando que Sabu desejava uma conversa particular. Com relutância abriu o texto, e o companheiro começou a desabafar. Topiary continuou afirmando que terminar com o LulzSec fora uma decisão da maioria, e não apenas dele – a equipe inteira queria dar um tempo. Mas Sabu via uma equipe que havia se voltado contra ele pela manipulação de Topiary. Quando os ânimos se exaltaram, Topiary disse a Sabu que se afastasse do computador e tomasse um copo d’água para se acalmar.

– Não fale comigo com esse maldito ar superior, como se fosse da elite – disparou Sabu em resposta. – Eu o trato com todo o respeito, mas destruo pirralhos como você num piscar de olhos. Não se esqueça d isso. Então me trate com respeito.

– Sabu, o que você está pensando? – indagou Topiary. – Você tem filhos e

precisa dar um fim a isso. Pelo menos mude o nickname.

– Seja como for, é tarde demais – disse Sabu, contendo a raiva.

– O que você quer dizer? Não pode dizer que é tarde demais. Não quer que suas filhas cresçam com o pai na cadeia. Mude o nickname, apague todo o seu conteúdo e reapareça com um nome diferente. Se eu tivesse filhos, não estaria fazendo isso.

Sabu respondeu novamente que era tarde demais. A equipe o abandonava.

– Não estamos abandonando você – retorquiu Topiary. – Só estamos interrompendo as atividades do LulzSec. Nossa amizade continua.

Em vez de apaziguar Sabu, isso o deixou mais furioso. Topiary desistiu de tentar convencê-lo. Era impossível explicar por que as coisas aconteciam no LulzSec ou no Anonymous, além do fato de que muitas ações foram feitas de veneta: a própria criação do grupo, a escolha dos alvos, o súbito revival do movimento Antisec. O LulzSec nunca planejara suas atividades com mais de doze horas de antecedência. A mídia e as autoridades davam muito crédito ao grupo e não o enxergavam como ele realmente era: uma equipe de pessoas com todos os talentos certos que havia se reunido na hora certa e depois perdera o controle sobre sua criação. Agora até mesmo Topiary começava a se entediar com tudo.

Sabu começou a insinuar que via menos capricho e mais conspiração.

Entabulou conversas particulares com AVunit e Tflow, que mais tarde repassaram a Topiary as informações. Sabu conversou com cada um sobre como Topiary o havia usado, e a Kayla também, para hackear sites como o da PBS. Argumentou que, quando sua avó tinha morrido e ele precisou se afastar um tempo, Topiary havia realmente tentado usurpar o controle do LulzSec de suas mãos e depois decolar com as doações Bitcoin. O braço direito e conselheiro de Sabu agora se tornava seu bode expiatório. Era quase como se ele estivesse tentando convencer os outros membros da equipe a incriminarem Topiary o máximo possível antes de se separarem para valer.

Quando Topiary ficou sabendo pelos outros das conversas privadas de Sabu, repentinamente deu conta de outro motivo pelo qual desejava sair: a sinistra capacidade de Sabu de penetrar no cérebro do amigo. Sabu podia ser um bom hacker, mas era um engenheiro social ainda melhor. Apesar de sua índole

violenta, ele conseguia inspirar amor, admiração e culpa em quase todo mundo. Muitas vezes isso se baseava em algo intangível – a promessa de hackeagens maiores no horizonte ou a devoção que os membros do LulzSec dedicavam um ao outro como equipe. A árdua realidade era que cada participante agora tinha de se defender por conta própria.

Topiary tentou ignorar os protestos de Sabu e começou a escrever seu último comunicado de imprensa, intitulado “50 Dias de Lulz”.

– Que não reste dúvida: amamos cada um de vocês de um modo inteiramente sexual – Topiary contou aos mais de 325 mil seguidores do LulzSec no Twitter –, inclusive os trolls.

Dez minutos depois, publicou o comunicado: “Nos últimos cinquenta dias perturbamos e expusemos corporações, governo, muitas vezes a própria população em geral, e muito possivelmente tudo no entremeio, apenas porque podíamos”, dizia o texto. “Tudo para egoisticamente entreter os outros”.

Essas eram as palavras de Topiary, não de Sabu. Não incorporavam o estimulante discurso que ele e Tflow haviam discutido, mas uma metáfora do que o LulzSec tinha sido ao longo do último mês: errante, arrogante e sempre em busca de um sentimento de séria convicção em relação a um assunto e, ao mesmo tempo, nunca parecendo realmente comprometido com ele. Convocava mais pessoas a seguirem a conta Anonymous IRC no Twitter. Controlada por vários hacktivistas radicais que não desejavam ser identificados, tinha mais de 125 mil seguidores e lentamente se tornava uma espécie de canal oficial de comunicação do Anonymous.

O vazamento final consistiu numa mixórdia que incluía um documento técnico para engenheiros AOL, documentos internos do AT&T e informações de usuários de fóruns de gamers e hackers. O comunicado revelava pela primeira vez que o LulzSec fora uma “equipe de seis pessoas”.

Topiary avisara em alto e bom tom: o grupo tinha acabado.

CAPÍTULO 24

O destino do Lulz

A importância do LulzSec não havia sido completamente inventada.

Para quem passava a maior parte do tempo no mundo do ar respirável, semáforos e pagamentos quinzenais, significava que as empresas que armazenavam seus dados pessoais em bases frágeis reavaliaram a segurança com que estavam protegidos. O LulzSec apontara uma relevante falácia mantida por empresas como a Sony – que os dados dos clientes estavam seguros porque seus próprios especialistas em TI não conseguiam hackeá-los. Agora qualquer empresa poderia repentinamente se tornar um alvo aleatório conforme o capricho de alguém; não era necessário um exército de hackers para roubar mais de um milhão de senhas, mas um alegre sexteto. O LulzSec fazia o que a divulgação integral fizera no final dos anos 1990: difundia amplamente as falhas de segurança das empresas e permitia que chapéus pretos as roubassem, caso não se dessem ao constrangedor trabalho de corrigi-las.

Para quem passava mais tempo olhando as telas, imerso no mundo de navegadores, IRC e novos scripts de web, o LulzSec reacendera o interesse em perturbar a web. Você não precisava esperar um ataque interessante ou divertido o suficiente para obter uma centena de sectários no *b*, nem limitações financeiras ao WikiLeaks para servir de centelha a uma insurgência cibernética com milhares de participantes. Bastava um punhado de pessoas talentosas e motivadas com boas conexões na comunidade de chapéu preto. O LulzSec tinha lembrado o Anonymous de que pequenos grupos podiam causar muito barulho. Nem sempre necessitavam de grandes recursos ou conexões com a imprensa. Topiary mantinha contato diário com jornalistas via Twitter, mas apenas concedera um punhado de entrevistas durante o LulzSec. Sem utilizar qualquer software especial, de apenas recorrer às ferramentas de web anônimas do Twitter e do Pastebin, ao Notepad para redigir todas as suas missivas e a um site simples, de design retrô, que utilizava um template emprestado da HBGary Federal.

O Anonymous, como conceito, existia há milhares de anos. A certa altura, alguns homens das cavernas devem com certeza ter espalhado sangue de bisão nas rochas de um rival na calada da noite e depois fugido dando risadinhas, pensou Topiary. Com o advento da internet e dos painéis de imagens anônimos, o processo passou a atingir não mais só um punhado de pessoas, mas dúzias e

depois centenas de pessoas reagindo, pensando e contribuindo com um processo de pensamento coletivo num curto período de tempo. O Anonymous tinha se tornado um estado psicológico conjunto, um santuário onde a mente de alguém podia se aliviar das responsabilidades oriundas da identidade ou de pesos como culpa e medo.

Originou, assim, uma nova onda de criatividade – memes e redação figurativa – sem as amarras das convenções sociais. Quando esse pensamento-colmeia se transformou em ações, criou energia, uma força em massa que não podia ser contida. Poucos conseguiam ocasionalmente direcioná-la, mas na maior parte do tempo essa força nebulosa, como Topiary a denominava, parecia ter vida própria.

Para quem desejava mais controle e mais glória, havia os grupos dissidentes. Um mês após a dissolução do LulzSec, vários novos grupos de hackers apareceram para lançar suas próprias operações, muitas vezes em nome do Antisec e do ativismo cibernético. Em julho, um grupo chamado de Script Kiddies hackeou a conta do Twitter da Fox News para informar que o presidente Barack Obama tinha sido assassinado, depois desfigurou a página da importante empresa farmacêutica Pfizer no Facebook e alegou ter roubado dados do Walmart. Grupos das Filipinas, da Colômbia, do Brasil e do Peru desferiram ataques em nome do Antisec, principalmente publicando dados de autoridades governamentais e policiais. Mais grupos seguiram esse caminho. Sem nenhum claro objetivo próprio, Topiary, Sabu e Kayla tinham inspirado uma onda de hacktivismo anárquico.

Muitas vezes, porém, todo esse processo não beneficiava os hackers.

Embora Sabu tivesse demonstrado decepção com o fim do LulzSec, a ressurgência do Antisec significava que os hackers e os script kiddies continuavam a abordá-lo com vulnerabilidades que ele podia repassar ao FBI. Rapidamente ele se revelava um informante valioso. Dias após a derradeira publicação do LulzSec, mais de seiscentas pessoas na sala de bate-papo Antisec do AnonOps debateram formas legais e ilegais de protestar contra diversos alvos. Agora elas procuravam a orientação de Sabu, prestando atenção em todas as suas palavras, tentando impressioná-

lo com ideias para hackeagens.

– Estou fazendo o mesmo trabalho, só que mais revolucionário – afirmou Sabu

numa entrevista em 1º de julho, poucos dias após a amarga discussão com os membros da equipe do LulzSec e, é claro, agora trabalhando secretamente para o FBI. – Chega do esquema “POR LULZ”

defendido por Topiary e Tflow. Estou fazendo trabalho real com motivações reais.

Com Topiary fora de cena, Sabu, o alter ego de Hector Monsegur, podia confortavelmente tomar as rédeas do que parecia ser um movimento global ressurgente. Mesmo com base em falsos pretextos, ele podia continuar a viver a vida de um revolucionário. Talvez em um ato de autojustificação por delatar seus velhos camaradas, ele professava nada além de desprezo por Topiary e Tflow.

– Eles me induziram a violar as leis e a me expor lá fora, e, quando a pressão aumentou, caíram fora – contou ele. – São malditas fraudes.

Sabu descartou a ideia de ter algum dia controlado Topiary com táticas de intimidação.

– Besteira – disse ele. – Jamais tratei mal alguém, nem uma vez sequer.

Eu... tenho a sensação de que, se eles forem presos mesmo, todos vão apontar o dedo para mim. Quando, na real, foram eles que organizaram essa confusão. Não dê bola para mim. Só estou irritado com isso. Eu me sinto usado.

Se Sabu sentia alguma culpa, não o demonstrava. Parecia que sua percepção do mundo era a de que sempre estavam contra ele. Em sua versão dos fatos, a ideia do LulzSec tinha começado com uma brincadeira cujo objetivo era reunir a velha turma. Em seguida, Topiary o motivara a se envolver, depois transformou o grupo numa organização, depois algo bem mais sério, com um site, servidores e comunicados de imprensa. E depois Topiary se transformou no líder do LulzSec e fechou as portas.

– Queriam que eu hackeasse para eles – contou Sabu. – Daí, quando eu fiz isso, eles ficaram muito assustados. Simples assim.

Ironicamente, ele alegou que o incidente que mais o magoara ocorreu quando ele ficou off-line por mais de um dia, e Topiary preocupou-se com a possibilidade de Sabu ter sido detido pela polícia. Em retrospectiva, parece que ele odiava a ideia de que seu colega, do outro lado do Atlântico, pudesse ter corretamente

suspeitado da verdade.

– A verdade é que dei um tempo por uns dias porque eu precisava e minha família tinha uns problemas – explicou ele, agora fornecendo uma versão diferente daquilo que realmente acontecera naquele dia. – E

[Topiary] inventou alguma história na cabeça dele de que eu tinha sido detido pela polícia ou algo ainda mais sinistro. Ele me magoou profundamente com aquela atitude. Eu adoraria falar com ele, principalmente para vê-lo se retratar.

Sabu alegava que havia se ressentido com o fato de limpar o rastro de confusão reputacional deixado por Topiary na comunidade hacker, respondendo a comentários de que os membros do LulzSec estavam "se borrando de medo de serem capturados pelas autoridades" e tinham "fugido da raia". Após duas semanas, Sabu enfim se acalmou, e, talvez infelizmente para Topiary, reconciliou-se com o adolescente das ilhas Shetland. Os dois começaram a conversar habitualmente no IRC. No começo pareceu bizarro, mas ambos aceitaram que tinham sofrido uma tremenda pressão e que o nível de tensão fora elevado.

Nesse meio-tempo, Topiary se afastara temporariamente do Anonymous e tentava passar menos tempo on-line. Vendia mais os utensílios da casa, coisas como o fogão, a geladeira com freezer e a cama; empacotava os livros, jogava seu Xbox. A mãe e o irmão tinham se mudado para um subúrbio na Inglaterra. Topiary planejava ir morar com eles, e, depois, encontrar um local para morar sozinho na região sudeste de Kent.

Ele havia comprado uma mochila com capacidade para 65 litros como preparativo para sua grande mudança, e o que não coubesse nela ajeitaria na sacola do laptop e na pequena mala. Trocava ideias frequentes com Kayla, com quem ainda mantinha uma boa amizade. Ela alegava estar de férias na Espanha com o pai e uma amiga, e no Twitter distribuía relatos extraordinariamente detalhados sobre escutar ruídos no quarto de hotel acima do dela e sobre mergulhar na piscina. Entre esses flagrantes, Kayla ensinava Topiary mais a se esconder on-line e a praticar da "trollagem reversa".

Ele

havia

configurado

um

endereço

de

e-mail,

topiaryhatemail@gmail.com, e o postado no perfil de sua conta no Twitter.

Se alguém enviasse um link virulento para a conta, ele e Kayla o pegavam e faziam engenharia reversa com ele, depois constrangendo seja lá quem estivesse tentando infectá-los. Um pouquinho de diversão leve.

Uma semana depois, ele voltou a entrar no IRC AnonOps e foi inundado por umas quinze mensagens privadas. As pessoas lhe faziam perguntas sobre o LulzSec, mostrava-lhe vulnerabilidades de sites, convidavam-no a canais secretos.

– Caraca, é O Topiary – alguém falou sem qualquer ponta de sarcasmo.

Desesperados por obter respostas aos seus comentários e perguntas, vários Anons o seguiam de canal em canal. Uma pessoa lhe enviou setecentos logins do FBI. Outra pediu conselhos sobre como destruir alguns advogados. Foi convidado a ajudar em cinco operações diferentes. Tudo parecia ter ficado um pouco mais bizarro desde que ele havia se afastado, até mesmo os operadores.

– Topiary, seu verme. Seu anarquista. Eu amo você, bro – disse EvilWorks, um operador do AnonOps. – Aposto que o governo está fazendo ataques de DDoS contra nós... Mas eu tenho novidades para você. O

AnonOps não vai sair do ar. NUNCA JAMAIS.

– Minhas janelas de mensagens privadas voavam – relembra Topiary. – As pessoas que eu conhecia do canal em janeiro me lembravam de quem elas eram, embora eu me lembrasse delas perfeitamente.

Um usuário anônimo até esmagou seu teclado de empolgação quando Topiary

começou a interagir com ele, dizendo que não esperava que “alguém como Topiary” respondesse.

– Isso me deixou pasmado, para dizer o mínimo.

Se ele criava um novo canal, por exemplo, algo como #BananaEchoFortress, em poucos minutos estava tomado por doze pessoas simplesmente porque muita gente fazia solicitações /whois com seu nome para localizar de que canais ele participava.

– Fiquei imaginando o que eu tinha feito para merecer tantos elogios – contou ele. – Estou longe de ser o mais habilidoso hacker, ou comediante, redator ou projetista.

Topiary chegou à conclusão de que, ao longo do primeiro semestre de 2011, ele apenas estivera nos lugares certos nas horas certas, apoiado pelas pessoas certas.

***

Por fim, Topiary se encontrou com um novo operador a quem foi impossível dizer não. Ele não queria se envolver muito, mas um hacker com vínculos com o LulzSec havia encontrado uma vulnerabilidade no site do *Sun*, tabloide que era o jornal mais popular do Reino Unido. Também era um dos trunfos da News International, a poderosa empresa midiática de Rupert Murdoch. Por volta desse período, o assunto da hackeagem dominava as manchetes – não hackeagem de computadores, mas de telefones. O governo britânico lançara recentemente uma investigação sobre relatos de que repórteres do jornal de Murdoch, *The News of the World*, tinham hackeado o telefone de uma colegial britânica assassinada e, em seguida, abafado o caso após apagar certas mensagens de voz da moça.

A hackeagem telefônica era um segredo de polichinelo na imprensa britânica, utilizado com mais frequência contra celebridades. De fato, o modo de escutar o correio de voz de outra pessoa era bem conhecido no 4chan e em outros painéis de imagem: você simplesmente esperava um tom de discagem, depois apertava a tecla # e digitava a senha comum “0000”. Mas a notícia de que os repórteres tinham hackeado o telefone de uma colegial assassinada deixou o público sedento por justiça. O iminente depoimento de Murdoch diante de uma comissão parlamentar parecia a ocasião ideal para colocá-lo em seu devido lugar.

Os hackers que haviam entrado em contato com Topiary no AnonOps queriam

que ele escrevesse uma notícia falsa reminiscente do seu artigo sobre Tupac na PBS. Tarefa simples, e Topiary concordou, pensando se tratar de uma boa ideia. Os hackers tinham conseguido assumir controle quase absoluto sobre theSun.co.uk e, em 18 de julho, invadiram a rede do tabloide e redirecionaram todos os links no site do *Sun* ao artigo de Topiary. Com a manchete “Descoberto cadáver de manda-chuva da mídia”, o texto detalhava como Murdoch fora descoberto morto em seu jardim.

Topiary não se conteve e deixou um cartão de visita para si e para um dos hackers, acrescentando que Murdoch tinha “ingerido uma grande quantidade de paládio antes de desabar em seu famoso jardim de Topiary”.

Quando a News International publicou um comunicado oficial sobre o ataque, os hackers reconfiguraram a página de modo a lincá-la à conta do LulzSec no Twitter.

Importantes órgãos de comunicação logo se interessaram pela história, enviando-a ao topo do Google News e informando que o LulzSec havia atacado outra vez. Topiary recebeu mensagens da BBC e de repórteres de redes de televisão dos EUA, do Canadá e da Austrália, solicitando entrevistas faladas, mas ele recusou todas as ofertas. Sabu capitalizou o interesse, divulgando pelo Twitter que já tinha em seu poder uma enorme coleção de e-mails do *Sun*, e então anunciou: – Estamos trabalhando com certos órgãos de comunicação aos quais concedemos acesso exclusivo a alguns dos e-mails do The News of the World que estão em nosso poder.

Nada disso era verdade, mas vários órgãos da grande imprensa ficaram se mordendo de inveja e divulgaram a afirmação.

O LulzSec havia, com sucesso, transformado o mais poderoso homem midiático do mundo em motivo de piada, provocando o riso em milhões de pessoas. No dia seguinte após a hackeagem do *Sun*, Murdoch depôs diante da comissão parlamentar, e um velhaco pândego pôs lenha na fogueira gritando “Seu bilionário safado!” e depois jogando uma torta de creme de barbear no rosto de Murdoch.

Rebekah Brooks, ex-editora do *Sun* e do *The News of the World*, também estava sendo investigada pelo seu conhecimento sobre a hackeagem telefônica. No meio da investigação, um policial descobriu que o marido dela havia tentado

discretamente descartar um saco de lixo preto nos fundos da casa. O conteúdo: o laptop da mulher. A polícia o recuperou.

Topiary leu o artigo e pensou que o casal deveria ter queimado o laptop.

Considerou ele devia fazer o mesmo, mas imaginou que podia empurrar com a barriga. Estava pronto para virar a página, arranjar um novo apartamento e até mesmo se encontrar com sua namorada on-line pela primeira vez. Ela planejava voar do Canadá em setembro. Mas ele não havia apagado seu laptop nem se despedido do Anonymous. Não por enquanto.

Assim, em 20 de julho, dois dias após a hackeagem do *Sun*, Topiary leu as notícias com o coração na boca. De acordo com um novo relato da Fox, a polícia britânica prendera um membro da cúpula do LulzSec em Londres, um homem que usava o nickname de Tflow. O comunicado oficial informava que o rapaz detido tinha dezesseis anos. Topiary releu a matéria.

Tflow, o gênio programador que escrevera o web script antibisbilhotagem tunisiano, configurara o site do LulzSec, compilara todos aqueles dados, tinha apenas dezesseis anos. Conferiu seu programa leitor de e-mails e viu que a última mensagem recebida de Tflow ocorrera quatro horas antes da sua prisão:

– Belo trabalho com o Sun. Vocês têm tudo de que precisam para uma publicação de e-mail adequada? Não quero deixá-los na mão.

E foi isso. Tflow fora o mais reservado membro do LulzSec. Misterioso, maduro e calado, considerado pela maioria da equipe como um sujeito na casa dos vinte anos. Programador calmo e sensato, ele evitava a maioria das perguntas sobre si mesmo e sua vida pessoal – comportamento diametralmente oposto ao de Kayla. No entanto, ali estava a declaração da Polícia Metropolitana num artigo intitulado “Jovem preso com base na Lei contra o Mau Uso de Computadores”, acrescentando que o equipamento de computação havia sido apreendido para análise.

– Se pegaram o cara certo, eu devo me preocupar agora – Topiary comentou na época. – Uso o mesmo provedor que ele e tudo o mais.

Topiary assinara um contrato de doze meses com seu provedor de internet, e não podia se dar ao luxo de romper a cláusula e pagar o ano inteiro.

Mas então ele percebeu um padrão nas detenções. Procurou Sabu e sugeriu que Ryan e Tflow talvez já estivessem no radar da polícia há meses, mas foram presos apenas após um grande ataque no Reino Unido: Ryan após o ataque contra o site da SOCA, Tflow após o *Sun* (embora ele nem tivesse participado do ataque). Já que vários membros do LulzSec eram radicados na Grã-Bretanha, Topiary concluiu: – Agora a gente deve parar de atacar alvos britânicos.

Sabu mostrou indiferença.

– Então para você está tranquilo se pararmos de atacar alvos britânicos porque vocês babacas estão no Reino Unido, mas não pararmos de atacar alvos dos EUA porque eu moro nos EUA? Obrigado.

Topiary rilhou os dentes. Sentia que tinha o direito de se preocupar, considerando que também morava no Reino Unido na época das detenções, mas Sabu sugeria que era egoísmo evitar alvos britânicos.

– Senti sua falta, brother – acrescentou Sabu, antes de indagar se Topiary podia lhe passar a senha da conta do LulzSec no Twitter. Topiary negou e saiu da sala de bate-papo.

***

Topiary odiava admitir, mas o lulz lentamente chegava ao fim. A música tinha parado; a luz já invadia o salão. Quando o LulzSec terminou oficialmente, no final de junho, a polícia, em oito países, inclusive Estados Unidos, Grã-Bretanha, Espanha e Turquia, havia detido 79 pessoas em conexão com as atividades executadas em nome do Anonymous e do LulzSec. A maioria dos presos era do sexo masculino, com média de idade em torno de 24 anos. Ser parte de uma grande multidão não havia ajudado.

Catorze pessoas, inclusive Mercedes “No” Haefer, de vinte anos, foram presas por participarem dos ataques de LOIC contra o PayPal e agora estavam sendo julgadas.

À medida que as pessoas cada vez mais viam o Anonymous e o Antisec como um movimento, mais as que estavam presas eram pintadas como mártires. O absurdo dos trotes evoluíra a uma importância exacerbada, até mesmo ilusões de grandeza, mas suas fundações frágeis eram reveladas quando pessoas como Ryan finalmente precisavam confrontar os rostos sombrios de um tribunal. Gente

como Topiary e até mesmo William tinha entrado no 4chan, Anonymous, Antisec ou LulzSec por lulz, mas permanecido ao parecer que faziam parte de algo ainda maior, impossível de ser transformado em palavras.

Em 27 de julho, sete dias após a prisão de Tflow, dois agentes da Polícia Metropolitana saíram de um jatinho particular de quatro lugares contratado por £ 8 mil e desceram cuidadosamente os degraus de aço até a pista de asfalto. O sol brilhava e soprava uma brisa amena. Foram recebidos pelos agentes locais da polícia escocesa, que raramente tinham algum crime para investigar, sendo, portanto, rara a oportunidade de se encontrar com seus colegas de Londres. Os dois agentes entraram num carro e foram conduzidos pelas estradas estreitas e sinuosas da ilha.

Em sua cadeira de videogames, com o laptop nos joelhos, Topiary pensava em outras coisas. Escutou um tênue ruído de carro aproximando-se de sua casa e o ranger dos freios quando o veículo parou. Logo o som de várias portas abrindo e fechando em sequência. Parou o que fazia, erguendo os dedos do teclado. Fitou a porta da frente, torcendo para que ninguém batesse. Sentiu o coração pulsando forte. Sorveu um demorado instante de silêncio, e a doce, misericordiosa possibilidade de que o carro viera atrás dos vizinhos. Súbito, uma batida à porta.

PARTE 3

Desmascarados

CAPÍTULO 25

O verdadeiro Topiary

Chame de pressentimento ou de bom senso, mas, tão logo escutou a batida, Jake sabia que era a polícia. Agarrou-se a uma só esperança: a de que não tivessem vindo para prendê-lo. A polícia fazia batidas na vizinhança a toda hora, graças aos drogados. Havia uma grande probabilidade de ser apenas mais uma operação de varredura.

Quando abriu a porta, deparou com seis pessoas em traje à paisana no degrau da entrada.

– Estamos com a Polícia Metropolitana – anunciou um deles. – Viemos fazer uma busca neste endereço.

Na esperança de que estivessem ali atrás de drogas, ele indagou: – Por que motivo?

– Equipamentos de informática.

Uma onda de desespero tomou conta de Jake. Se Aaron Barr um dia torcera para que um de seus adversários experimentasse o mesmo tipo de pavor que ele sentira um ano antes, Jake acabava de experimentá-lo.

– Você é Jake Davis? – indagou um deles após todos terem mostrado as insígnias e se identificado. Jake assentiu: – Sim. – Acrescentaram que também estavam ali para prendê-lo. – Por que motivo? – indagou Jake.

– Conspiração para realizar um ataque de DDoS contra a SOCA.

Jake esperou para ver se eles mencionariam outra coisa, mas não o fizeram. Quase parecia que o ataque de DDoS contra a SOCA, a Agência Britânica contra o Crime Organizado Grave, tinha sido a gota d’água que motivara as autoridades a fazer um voo especial até as ilhas Shetland.

Não houve algemas nem armas de fogo; não houve gritos; apenas conversas polidas que tornavam a interação completamente surreal. Uma policial da divisão de crimes cibernéticos da Polícia Metropolitana caminhou reto ao laptop Dell de Jake e começou a mexer no touchpad.

Antes de ele esboçar reação, ela ordenou que não tocasse no aparelho.

Apesar de tudo que havia acontecido, Jake ainda não tinha apagado seu laptop conforme planejara. Todo o material incriminador – documentos, observações e bases de dados – ainda estava ali, embora em um disco rígido criptografado. Mas isso não foi problema para a polícia, que teve apenas de pedir a senha a Jake; ele a forneceu. A mulher tentou verificar o que havia no disco rígido, mas não conseguiu. Fez um sinal para que Jake se aproximasse e lhe permitiu uma última interação com seu computador: um clique no mouse para revelar seu disco rígido oculto, a fim de que a policial pudesse dar uma olhada no conteúdo. Ele tinha quarenta programas rodando ao mesmo tempo.

Exatamente como Barr tinha se censurado por reutilizar a mesma senha, Jake silenciosamente se arrependeu por não ter apagado tudo como Kayla o havia incentivado, como ele mesmo dizia a si mesmo para fazer.

Os policiais prosseguiram com gélido pragmatismo. Avisaram a Jake que agora ele precisava acompanhar quatro deles, enquanto os outros dois permaneceriam em sua casa para encerrar o laptop e vasculhar o local atrás de outros itens que pudessem ser utilizados como prova. Não havia tempo de arrumar uma mochila, pegar um livro ou ligar para a sua mãe.

Recebeu a permissão de pegar duas mudas de roupa. Abriram a porta da frente e o conduziram degraus abaixo até o carro, sem cerimônias. Se os drogados locais estivessem assistindo, talvez pensassem que o vizinho jovem e hermético estava sendo levado à cidade para passar uns dias na casa de parentes, nunca imaginando que a detenção ocorrera pelo fato de ele ajudar a comandar uma das mais afamadas gangues cibernéticas do mundo.

Na mesma hora, a centenas de quilômetros ao sul, na cidade de Spalding, ao norte da Inglaterra, a mãe de Jake, Jennifer, conversava com uma vizinha do outro lado da rua. Um policial apareceu ali e pediu a Jennifer que fosse para casa. Confusa, ela obedeceu. Ao abrir a porta de sua casa, deparou com uma azáfama de inspetores de crimes cibernéticos em meio a outros policiais que investigavam as coisas da família e interrogavam seu outro filho, Josh, de dezessete anos. Eles apreenderam todo o equipamento de informática da família.

Lá em Shetland, enquanto o jatinho particular que havia transportado os inspetores ao norte agora acelerava na diminuta pista e decolava rumo a

Londres, Jake pensava nas manchetes inevitáveis. Até então, as ilhas Shetland tinham sido apenas uma tênue luz piscante no radar da consciência pública britânica. Uma terra longínqua de escoceses com sotaque forte e uma queda por criar ovelhas. O maior evento local até então havia acontecido naquela mesma semana, com a cidade sediando regatas do Tall Ships Races de 2011. Muitos dos 7 mil habitantes da ilha tinham acompanhado as competições, enquanto dúzias de grandes veleiros com jovens tripulações atracavam na baía de Lerwick. Jake se lembrou de como ele havia saído de sua vida reclusa por um tempo, passeando até o porto e assistindo, maravilhado, à agitação de milhares de pessoas em meio a barracas, alimentos e música ao vivo.

Foi trazido de volta à realidade com um solavanco quando o avião aterrissou. Embora em outra ocasião ele tivesse demorado dezoito horas de ônibus mais uma travessia de balsa para chegar às Shetland, o voo durara apenas quarenta e cinco minutos. Uma hora depois, Jake foi conduzido até a delegacia de Charing Cross, com suas alvas e límpidas paredes de estuque, no centro de Londres, e logo conduzido a uma minúscula cela de detenção. Havia uma cama com colchonete azul, ao estilo dos utilizados em academias de ginástica, cobertor fininho e vaso sanitário em um canto. O calor do dia de verão contrastava com o frio da cela. Os sons de outros companheiros de cadeia – cantando e batendo – ecoavam no corredor. Por fim, ele acabou tendo a oportunidade de falar com a mãe, já bastante preocupada. Disse que estava bem e perguntou se ela podia trazer algumas roupas, livros e frutas. A comida servida nas celas de custódia era principalmente ao estilo de refeições para viagem: frango empanado ou salsicha com fritas.

No dia seguinte, uma mulher com calça de veludo cotelê marrom e sandálias de couro galgou os alvos degraus da escadaria externa e entrou na delegacia de Charing Cross. A mãe de Jake, Jennifer Davis, o cabelo marrom-escuro pintado em tons sutis de ruivo, carregava uma sacola com flores bordadas e uma mochila azul cheia de roupas e frutas que ela trouxera de trem de sua casa em Spalding. Esperava reencontrar o filho dali a alguns meses, quando ele se transferisse à Inglaterra para morar junto com ela outra vez; não dessa forma. Foi solicitada a presenciar todos os interrogatórios, pois, devido à idade de Jake, um adulto precisava estar presente.

Os interrogatórios duravam horas a fio, e Jake ansiava por eles, que representavam uma oportunidade de sair da cela. Ficou chocado com o volume de pesquisa detalhada que a polícia havia realizado sobre o Anonymous e o

LulzSec. Eles tinham cronologias completas de ataques cibernéticos, com tempos exatos, e tabelas de suspeitos que remontavam a 2006, muitas vezes espalhadas em gigantescas folhas de papel. Graças ao recente financiamento extra do governo, agora havia uma equipe dedicada formada por cerca de doze inspetores trabalhando no rastreamento do Anonymous. Eles o haviam prendido em conexão ao ataque contra a SOCA e sob a suspeita de várias outras infrações. Por fim, a polícia falou que, com base nos interrogatórios e no material encontrado no laptop de Jake, planejava acusá-lo de cinco infrações específicas. A polícia usava elementos inócuos como provas: printscreens com sua janela de navegador sendo aberta em um serviço de e-mail temporário e descartável (conhecido como “e-mail de dez minutos”); outra janela mostrando o Nyan Cat. Jake cooperava quando podia, fornecendo à polícia as senhas para acessar a conta do LulzSec no Twitter e tudo que havia em seu laptop.

Rapidamente se espalhou a notícia de que a polícia prendera a pessoa que ela acreditava ser Topiary e o interrogava em Londres, instaurando o caos no mundo dos Anon. Nas salas de bate-papo do AnonOps, corriam boatos acalorados sobre o que havia acontecido.

Sem demora, Sabu postou “Descanse em paz, Topiary” em sua conta do Twitter, acompanhada por vários milhares de seguidores, comparando a prisão com uma morte no mundo da hackeagem.

– Estou bastante deprimido – disse ele numa entrevista naquele dia.

Mas logo isso se metamorfoseou em raiva contra o governo e, talvez, contra novos supervisores.

– O problema não está nos hackers, mas no pensamento de nossos governos. Eles precisam mostrar a seus cidadãos que o governo pode fazer retaliações contra a desobediência civil.

Ainda não está claro como a polícia conseguiu rastrear “Topiary” e chegar à casinha amarela de madeira de Jake Davis, nas remotas ilhas Shetland. Talvez Sabu tenha ajudado, já que ele fora preso um mês antes.

Mas existem outras possibilidades. Como Sabu, nem sempre Topiary tomava as precauções cabíveis. Por alguns breves segundos, o nome Jake viera à tona na rede de bate-papo AnonOps. Isso aconteceu pouco depois de 8 de dezembro de 2010, quando o Anonymous lançava seus ataques pró-WikiLeaks. Embora Jake

tivesse duas ou três camadas de VPN para ocultar seu endereço de computador, um erro de conexão temporário de sua banda larga, que coincidiu com uma falha de conexão com uma de suas VPN, o deixou temporariamente desmascarado. Ele nem tinha ideia de que isso havia acontecido.

Depois correram boatos de que um amigo de Jake do tempo que ele participava de fóruns de Xbox, reconhecendo sua voz no vídeo da Igreja Batista Westboro, havia começado a postar mensagens no Twitter dizendo que Topiary era “Jake de Shetland”.

Outro motivo mais provável tem a ver com a empresa de VPN à qual Jake pagava uma assinatura mensal para ocultar seu endereço IP. Tanto Topiary quanto Sabu tinham indicado o provedor de VPN HideMyAss à cúpula e ao segundo escalão do LulzSec, com Topiary investindo algumas centenas de dólares das doações do grupo em sete contas on-line. Quando alguém precisava de VPN extra, Topiary emprestava à pessoa um nome de login com senha e a riscava da lista. Algum tempo após o vazamento dos registros do #pure-elite, que mostrou ao mundo que o LulzSec usava o HideMyAss, a polícia britânica enviou uma intimação judicial à empresa britânica de VPN. Mais tarde, a HideMyAss admitiu ter sido obrigada a divulgar informações sobre uma conta do LulzSec, alegando que habitualmente registrava os endereços IP dos usuários e seus horários de login para ajudar a extirpar usuários abusivos. A clientela ficou em polvorosa, mas uma intimação judicial era uma intimação judicial, em detrimento das perspectivas comerciais.

Durante os interrogatórios, Jake notou que os inspetores pareciam ver o Anonymous como um grupo criminoso organizado, exatamente como previra Sabu ao censurar Laurelai por escrever um guia de usuário. Quando os inspetores questionaram Jake, eles pareciam querer respostas que se enquadrassem nesse ponto de vista. Jake tentou explicar que o Anonymous não era um grupo, não era organizado e não tinha uma estrutura. Consistia mais em uma cultura ou uma ideia do que em um grupo.

Mas, após a explicação, Jake percebeu que a polícia tinha certa razão.

Em menos de um ano, o Anonymous realmente havia se organizado melhor.

Em novembro e dezembro de 2010, durante a Operação Vingança, não existia uma rede estável de bate-papo, e sim mais de vinte operadores de IRC enleados

numa confusão burocrática. Em julho de 2011, havia uma enxuta e sólida rede de bate-papo com cerca de seis operadores bem mais sincronizados uns com os outros. A essa altura, as contas do Twitter @AnonymousIRC e @anonymouSabu acumulavam, juntas, mais de 100 mil seguidores de Twitter, números não tão altos quanto os do LulzSec, mas ainda suficientes para granjear atenção em massa. O Pastebin havia se popularizado como forma rápida e fácil de publicar dados roubados. Mais gente sabia quais hackers deviam ser procurados para realizar as tarefas.

Havia servidores mundo afora, e as doações Bitcoin continuavam a entrar.

Aos trancos e barrancos, um sistema estava sendo criado.

As autoridades estadunidenses trabalhavam em uníssono com a Polícia Metropolitana. No começo de agosto de 2011, o Ministério da Segurança Nacional dos EUA informou que esperava ataques mais significativos do Anonymous nos próximos anos e que havia a possibilidade de um "agente de nível superior fornecer ao LulzSec ou ao Anonymous capacidades mais avançadas".

Na linha de frente ou em atividades paralelas, Topiary, Sabu e Kayla, junto com William no 4chan, tinham assistido ao Anonymous surgir e se tornar uma entidade nebulosa e potencialmente perigosa, com bolsões de influência e poder significativos. Como um adolescente petulante, permanecia volátil e incompreendido. A partir do WikiLeaks em dezembro de 2010, passando pela Tunísia em janeiro de 2011 e culminando com Aaron Barr em fevereiro de 2011, as operações tinham surgido quase aleatoriamente. Nada de financiamento, nada de planejamento e nada de líderes. Ninguém sabia o nome de ninguém nem havia se encontrado pessoalmente. O Anonymous surgira do nada para se criar a miragem de uma organização criminal que a polícia apenas começava a entender.

Agora ao menos eles possuíam um rosto para mostrar ao mundo. A polícia manteve Jake preso pelo máximo de tempo possível – noventa e seis horas. Após esse período, chegou a hora de anunciar seu nome verdadeiro.

***

No domingo, 31 de julho, a Polícia Metropolitana de Londres anunciou em seu site que estava indiciando um adolescente de Shetland chamado Jake Davis com

cinco acusações relacionadas a hackeagens de computador, inclusive a violação da Lei contra o Mau Uso de Computadores e conspiração para atacar a Agência Britânica contra o Crime Organizado Grave. Agora, pela primeira vez, o nome Jake Davis era associado publicamente a Topiary. Mais tarde naquele dia, o jornal britânico *Daily Mail* publicou um artigo com a manchete: “Adolescente autista de Shetland comandou uma onda global de hackeagem na internet, planejada a partir de seu quarto”. Tratamento típico de tabloides britânicos, agora com a insinuação de que Jake Davis era o “cabeça” do LulzSec (em vez de Ryan Cleary) e com nenhuma explicação sobre como alguém sabia que Jake era autista. (Ele não era.) A mídia que Topiary atraíra com tanto sucesso antes, e a qual ele praticamente mantivera na palma da mão, voltava-se contra ele, alegremente invocando os clichês hackers de distúrbio mental e inaptidão social.

No dia seguinte, Jake foi levado ao tribunal de Westminster Magistrates para sua primeira audiência, ocorrida no mesmo ambiente intensamente iluminado em que Ryan Cleary estivera há um mês apenas. Fora do tribunal, fotógrafos com lentes teleobjetivas miravam as janelas de qualquer furgão policial que chegava e tiravam fotos através dos vidros fumês. Conferiam o resultado e tiravam novos instantâneos. Cerca de duas dúzias de jornalistas estavam ali para fazer a cobertura, inclusive editores do *The Guardian*, da BBC e do *Financial Times*. Eles se aglomeraram para trocar ideias sobre a “novela” que a história do LulzSec tinha se tornado.

– Imagino que ele seja pálido e amarfanhado, magrinho ou gorducho – disse o editor de tecnologia do *The Guardian*, que havia publicado os registros do #pure-elite. Esse editor, Charles Arthur, tinha sido alvo da trollagem de Topiary em uma ocasião, tendo seu número de celular tweetado e rapidamente recebendo duzentas mensagens de voz antes de lotar a caixa de mensagens e Jake apagar o tweet. – Se tivessem atacado apenas corporações teria sido “Ok, traga alguns sanduíches” – falou Arthur enquanto cismava sobre o LulzSec –, mas atacar a SOCA...

Ele se calou com um encolher de ombros do tipo “sei lá”.

No tribunal, as pessoas se ajeitavam nos assentos quando Jake entrou cabisbaixo e subiu ao octogonal banco dos réus, trajando camiseta jeans e carregando um livro na mão. Correu o olhar ao redor enquanto confirmava o nome e endereço ao juiz, depois se sentou e coçou a cabeça. Fitou os jornalistas, que se esforçavam para ver a capa do livro, depois baixou o olhar novamente. Na maior

parte do tempo, mostrou calma e autocontrole.

– Senhor, a imagem que surge não é a de um hacker habilidoso e persistente – afirmou o advogado de Jake, sujeito alto, de óculos, chamado Gideon Cammerman –, mas de alguém que se solidariza e divulga, atuando como depósito de informações hackeadas por outras pessoas.

A promotora do governo, mulher encorpada de terno escuro, discordou.

Referindo-se ao grupo de Jake como "luke sack", ela insistiu que ele permanecesse detido até nova ordem. Após ouvir o suficiente, o juiz distrital Howard Riddle, homem severo, de rosto vermelho com cabelo grisalho curto em formato capacete, mirou Jake por um instante e depois novamente a promotora. Esse era o mesmo juiz que no começo daquele ano dera a sentença que definiu a extradição de Julian Assange para a Suécia.

– Por gentileza, esclareça-me – disse ele, espiando por cima dos óculos – a natureza do mal que ele causou.

A mãe de Jake assistia da galeria pública.

– Senhor, ele expôs informações pessoais de centenas de milhares de membros do público – mencionou suavemente a promotora enquanto erguia o olhar para o juiz. – Pessoas que usaram o Serviço Nacional de Saúde, as contas bancárias e dados pessoais dos usuários dos sistemas da Sony Entertainment.

Ela citou o leitor de e-mails temporário encontrado no laptop de Jake e o fato de que o computador tinha um disco rígido de 100 GB criptografado com dezesseis "pequenos computadores" separados – suas máquinas virtuais – operando independentemente um do outro.

O juiz Riddle indagou ao advogado de Jake qual havia sido o "temperamento" do rapaz durante a detenção.

– De um cavalheirismo perfeito – respondeu Cammerman, aproveitando para salientar que a mãe e o irmão de Jake recentemente haviam se transferido para Spalding, Inglaterra, e ainda estavam sem banda larga. Nenhum acesso a internet. O advogado sugeriu que Jake fosse libertado sob fiança e enviado para ficar com a família sob a condição de usar uma tornozeleira eletrônica e de não acessar a internet. Para alguém como Jake, que estivera on-line quase todos os

dias desde os onze anos, essa seria a pior das abstinências. Mas melhor que uma cela.

Em poucos minutos, o juiz tomou sua decisão: – Está claro que existem fortes indícios de que você se envolveu com um grupo que cometeu violações muito graves – sentenciou ele enquanto Jake balançava a cabeça positivamente. – As objeções contra a fiança eu entendo. Mas penso o seguinte. – Encarou Jake mais fixamente. – Você tem apenas dezoito anos. Não teve problemas com a polícia antes.

Apesar de sua aparência rígida, o juiz concedeu a Jake o direito de fiança, com uma lista de condições que incluía um toque de recolher às 22h.

O guarda se aproximou de Jake com uma prancheta. O rapaz lhe ofereceu um discreto sorriso e assinou a folha.

– É um sujeito de sorte – murmurou o guarda enquanto conduzia Jake para fora. – Eu não achava que eles iam lhe dar fiança.

O guarda acompanhou Jake pelo corredor até uma salinha onde ele se encontrou novamente com a mãe e outro advogado que trabalhava com Cammerman. Sabendo que havia câmeras esperando lá fora, o pequeno grupo imaginou o melhor caminho para sair do tribunal. O advogado relatou que membros da mídia se aglomeravam na frente e nos fundos do prédio, à espera da saída de Jake. Se saíssem pela frente, onde havia a maioria das câmeras, pelo menos estariam numa via principal com um táxi preto londrino já os aguardando. Se saíssem pelos fundos, precisariam caminhar até encontrar um táxi, correndo o risco de encontrar mais repórteres. A mãe de Jake decidiu que seria melhor saírem pela frente, juntos, como uma família.

Com as mãos nos bolsos, o livro enfiado embaixo do braço, Jake desceu até a iluminada entrada do fórum de justiça e estacou diante da porta principal. Olhando pelas janelas, percebeu que o dia estava perfeito lá fora, nesgas de luz solar dançando nas calçadas e através da copa das gigantescas árvores caducifólias do outro lado da rua. Na base da escadaria externa, uma multidão de fotógrafos e cinegrafistas de tevê esperava num semicírculo, todos petrificados de expectativa. A mãe de Jake os fitou cautelosamente do interior do prédio. O rapaz colocou um par de óculos escuros, que a mãe trouxera, para ocultar sua ambliopia.

– Vamos? – indagou ela.

– Sim.

Soltou um suspiro quando as portas de vidro se abriram diante de si, e, em seguida, atravessou o portal. A massa escura de fotógrafos entrou em erupção. Luzes de flashes acompanhadas por um sinistro silêncio. Nenhum grito e quase nenhuma fala, apenas o som dos carros passando e o farfalhar do vento nos ramos das árvores. Quando todos chegaram ao nível da rua, Jake se retraiu ao ser engolfado pela turba. Começou lenta e penosamente a se arrastar até o táxi preto que o esperava no outro lado da rua. A poucos centímetros de seu rosto, as câmeras explodiam em flashes. Os fotógrafos logo começaram a gritar para chamar a atenção de Jake, sabendo que o táxi estava perto e o tempo era curto.

– Jake! Jake! – chamava Charles Arthur, do *The Guardian*, que abria caminho em meio aos fotógrafos para ser visto por Jake. – Qual é o livro?

Jake estacou para fitá-lo, em seguida ergueu o livro de capa mole para todos verem a obra que estivera lendo em sua cela. Frenéticos cliques e nova explosão de flashes. Intitulava-se *Free Radicals: The Secret Anarchy of Science*, e falava como os cientistas eram capazes de fazer qualquer coisa – mentir, roubar ou trapacear – em busca de novas descobertas. Pela primeira vez, enquanto Jake mirava através de seus óculos escuros uma das câmeras, ele esboçou um pequeno e quase imperceptível sorriso.

***

Após comparecer ao tribunal, Jake pegou um trem para o norte da Inglaterra, onde ia morar com o irmão caçula, a mãe e o companheiro da mãe. A polícia instalaria nele uma tornozeleira eletrônica para controlar o cumprimento do toque de recolher. Ele jamais o violaria, tornando-se tão paranoico quanto a infringir as normas da liberdade condicional que se recusou a escutar um vídeo do YouTube pelo telefone quando alguém ofereceu. Fotos do rosto de Jake após deixar o tribunal foram compartilhadas internet afora. E qual a relação dos Anons ao verem o verdadeiro Topiary pela primeira vez? Eles o apresentaram como mártir, sobrepondo seu rosto em pôsteres de filmes como *Matrix* para criar novas imagens de propaganda. Sabu, Kayla e muitos outros mudaram seus avatares no Twitter para “Free Topiary”. Outros hackers do Anonymous que continuavam à solta acompanharam a evolução do julgamento de Jake e se

perguntavam como ele ia se sair. Mas já que números de telefone eram raramente fornecidos no Anonymous, nenhuma das centenas de pessoas com quem Topiary havia conversado no AnonOps sabia como entrar em contato com ele após sua prisão. Em outras palavras, ao chegar a sua casa, Jake foi brindado com um completo silêncio.

Três meses após sua aparição no tribunal, algumas cartas tinham chegado à sua porta – a maioria de jornalistas e uma ou duas de fãs. Jake havia deixado de se comunicar com centenas de milhares de pessoas todos os dias on-line para abrir uma carta eventual, conversando principalmente com os familiares mais próximos, assistindo à tevê, jogando videogames e tentando utilizar uma máquina de escrever para expressar seus pensamentos.

Súbito surgiu a oportunidade de algo diferente. Após alguns meses de sua nova e isolada existência, Jake recebeu a exclusiva chance de falar com alguém do Anonymous cara a cara. Não alguém com quem ele havia colaborado, nem mesmo encontrado pessoalmente. Era William.

***

Como William, Jake Davis jamais teria alcançado a linha de frente do fenômeno Anonymous se não descobrisse primeiro o 4chan. Esse site aparentemente inócuo, ainda em grande parte desconhecido do mainstream, mas adorado por milhões de usuários habituais, estava no coração do que motivara o Anonymous a conquistar a atenção mundial.

Apesar das ações de hackers que atraíam as manchetes, as raízes e o ethos lulz do Anonymous continuavam firmes nos painéis de imagem.

A partir dos catorze anos, Jake começou a aprender como manipular as hordas no 4chan e entretê-los em outros sites. William era diferente. Dos catorze até os vinte e um anos, sua idade em 2012, William ainda raramente saía do mundo do *b*, o sempre popular fórum de tópicos aleatórios do 4chan. Havia muita gente como ele – oldfags que se consideravam os verdadeiros Anons. O site continuava a receber 22

milhões de visitantes individuais por mês, 65% deles do sexo masculino, com idade entre dezoito e trinta e cinco, moradores na América do Norte ou na Europa Ocidental. Como muitos outros fóruns da web, o 4chan era um local para debater uma riqueza de assuntos toscos e sofisticados, desde lentes de câmera no

painel sobre fotografia até autores vitorianos no painel *lit*. Mas milhares de visitantes a cada dia ainda se encaminhavam direto ao *b*, na esperança de descobrir um “tópico épico” que levasse o 4chan a deixar sua marca no mundo real, qualquer coisa desde arruinar a vida de alguém até atacar um site para encontrar uma garota sequestrada.

William ainda varava as madrugadas no 4chan, aterrorizando os inimigos de seu amado *b* e tentando aprimorar sua perícia hacker. As notícias sobre a prisão de Topiary tinham sido decepcionantes – ele gostara do sujeito naquele vídeo da Westboro –, mas também o deixaram mais determinado a se tornar hacker. Já que suas emoções eram tão extremas, William imaginava que de duas, uma: a prisão seria entediante a ponto de entorpecer a mente (tanto fazia, já estava deprimido em casa) ou “uma diversão”. Seja como for, não se importava com as consequências.

– Não vou ser capturado, tenho certeza – explicou ele.

As façanhas on-line de William tinham se tornado mais audazes, às vezes incluindo uma gangue de outros usuários do *b* para ajudá-lo a atormentar um grupo mais amplo de pessoas. Por exemplo, perto do Natal de 2011, William navegava pelo painel chamado carinhosamente por ele de “meu *b*” quando deparou com um tópico que começava: “Poste as informações de contato de quem você odeia”. Comum no *b*, esse tipo de tópico muitas vezes oferecia uma noite de diversão para William.

Entre as respostas, um usuário tinha postado o número do telefone e o endereço no Hotmail de uma garota de dezesseis anos do Texas chamada Selena, acrescentando: – Transforme a vida dessa garota num inferno. É uma vagabunda.

Quando William conferiu o perfil de Selena no Facebook, descobriu que ela contava com mais de 3 mil amigos. Resolveu tentar hackear a conta da menina.

Escreveu o endereço de e-mail de Selena numa folha de papel, foi até o Hotmail, clicou no link que dizia “Não consegue acessar sua conta?” e depois selecionou “Resetar conta”. Inseriu o endereço de e-mail de Selena, depois respondeu à pergunta de segurança: “Qual é a cidade natal do seu pai?”. Conforme o perfil de Selena no Facebook, ela morava em Joshua, Texas, que era a resposta certa.

Depois perguntava: – Qual é a profissão de seu avô?

William soltou um suspiro. Entrou em um de seus perfis falsos no Facebook, Chrissie Harman, e enviou uma mensagem direta para Selena.

– Um grupo de hackers está em seu encalço – ele lhe contou sem sequer se apresentar. Como prova, colou uma captura de tela do tópico do *b* com os dados de contato dela. William contou que fazia parte dessa fictícia gangue de hackers e que eles eram perigosos. Desejava ajudar, mas não sem pagamento.

– Como eu lhe pago? – indagou Selena, preocupada.

– Tire uma foto sua com sapato na cabeça e carimbo de tempo.

No passado ele teria desejado fotos de nudez, mas a essa altura William já tinha o suficiente desse material e nem se dava ao trabalho de pedir. Em poucos minutos, Selena tirou um autorretrato e o enviou. William sentiu uma pequena vitória.

– Ok. Agora vou lhe fazer umas perguntas para ajudar a garantir sua conta – continuou William.

Ele podia ter apenas pedido a ela que removesse as perguntas de segurança. Em vez disso, bombardeou-a com bobagens tecnicistas envolvendo “respostas randomizadas”, “servidores” e “inserção de uma sequência de caracteres da base de dados” – tática deliberada de engenharia social. Distraia alguém com suficiente desinformação, e essa pessoa esquece o que você realmente está tentando obter ou esconder.

– Escolha um número de 1 a 100 – pediu. – Qual é o nome do meio da sua mãe? O da minha é Deborah.

Após cada resposta, ele replicava: – Sim, isso vai funcionar direitinho.

Até que ele perguntou: – O que seu avô faz?

– Petróleo – disse Selena.

William abriu a outra janela e digitou rapidamente *petróleo* no Hotmail.

Nada. Tentou *operador de petróleo*, *técnico de petróleo* e *executivo de petróleo*. Também não funcionaram. Teria de tentar algo mais: – Ok. Minhas perguntas

agora vão ficar mais técnicas, mas não se preocupe – avisou William. – Isso vai realmente garantir a segurança.

Depois de tudo, você será eternamente in-hackeável.

Pediu quantas contas de e-mail Selena tinha e quantos caracteres havia em sua senha mais usada. Depois lhe pediu que ela digitasse sua senha do Hotmail de trás para frente.

– Aqui está a minha – ofereceu ele, colando uma bobagem.

Após hesitar, Selena digitou a senha. Minutos depois, William havia dominado a conta de e-mail da garota e ativado uma série de etapas que lhe permitiu resetar também a conta no Facebook, continuando a lhe fazer perguntas para que ela não desconfiasse.

Antes que Selena pudesse responder à última pergunta de William, ele entrou na configuração da conta dela e a desconectou. Definiu navegação segura para mascarar seu endereço IP e depois mudou a senha outra vez.

Voltou ao *b*.

– Estou na conta desta garota – disse ele, começando um novo tópico e colando um link ao perfil dela no Facebook. – Me deem ideias do que fazer.

Uma pessoa sugeriu falar com o namorado de Selena, um garoto local chamado James Martinez. William decidiu que a ideia era boa. Foi em frente e mudou o status de relacionamento de “relacionamento sério” para “solteira”, e depois enviou uma mensagem direta a James.

– OMG eu acidentalmente nos deixei solteiros! – exclamou ele, agora se fazendo passar por Selena. – Pode me dar sua senha para que eu entre no seu Facebook e aceite nosso status de relacionamento outra vez?

James concordou e enviou a senha *boobies1*, mas ela não funcionou.

Exasperado, William repassou o trabalho de sondar James a outro pândego do *b*. Esse era o benefício de ter o *b* por trás de você – se atolasse num problema, alguém poderia ajudá-lo a sair dele. Uma dupla de usuários do *b* a essa altura havia entrado em contato com William via seus próprios perfis falsos no

Facebook, e um deles, que utilizava o nome Ben Dover, ofereceu-se para conseguir a senha certa de James. Em breve, o rapaz percebeu que não estava conversando com sua namorada de dezesseis anos, Selena, mas sim com um hacker mal-intencionado. Com o Caps Lock acionado, ele ameaçou: – EU VOU CHUTAR SUA CABEÇA. – William caiu na risada.

– Foi talvez o momento mais engraçado da noite para mim – contou mais tarde William. – Eu gostava mesmo quando as pessoas se irritavam, sem se dar conta do quanto elas eram impotentes. É como se dirigir ao cara mais encorpado numa boate e falar: "Eu vou nocauteá-lo". Simplesmente não vai acontecer.

A bronca de James prosseguiu: – Eu vou te degolar, sua bichona – escreveu ele.

Em outra janela, Ben Dover relatava que faltava pouco para dominar a conta de James no Facebook.

– Vou fazer agora – avisou Ben finalmente.

– Ok, faça agora – disse William.

Seguiu-se o silêncio de James por uns dez minutos. Logo veio uma nova mensagem da conta dele na mesma janela de bate-papo: – Estou dentro.

Era Ben. William abriu um sorriso. Após conversar mais um tempo com Ben, William se deu conta de que ele era um *b*rother que entendia a arte da trollagem suave, uma forma mais sutil de aplicar trotes. Por exemplo, era engraçado hackear o perfil do Facebook de alguém e postar material pornográfico, porém mais engraçado ainda era fazer parecer que a própria pessoa havia acidentalmente carregado um link pornô.

William e Ben criaram um grupo de Facebook privado e colaram um link para ele no *b*. Após meia hora, cerca de cinquenta outros perfis falsos no Facebook, todos conectados a usuários do *b*, tinham entrado no grupo e trocavam ideias sobre o que fazer na sequência.

Por enquanto, William queria manter para si as credenciais de logon para o perfil de Selena no Facebook. A jovem, com sua rede de 3 mil amigos no Facebook, era a joia da coroa. Tão logo ele entrou na conta dela, dez abas de mensagens para bate--papo piscaram de rapazes querendo falar com Selena. Era um lembrete da força magnética que adolescentes do sexo feminino exerciam on-

line, e do quanto os homens se tornavam cegos quando pensavam estar falando com uma garota assim. Esse era o benefício que a pessoa por trás de Kayla encontrava em se assumir uma garota de dezesseis anos on-line. William escolheu um dos rapazes que tentava falar com Selena, Max Lopez, e enviou uma resposta.

– E aí, baby *J* – escreveu William, ainda como se fosse Selena. – O que tá pegando?

Max respondeu, e os dois entabularam um papo inócuo, Max alheio ao fato de que na verdade conversava com um rapaz de 21 anos do Reino Unido.

– Estou meio excitada :D – digitou William.

A conversa que se seguiu foi igual a centenas de outras que William já protagonizara. Semanas mais tarde, quando ele a descreveu num calmo restaurante, desviou o olhar, as mãos firmemente entrelaçadas. Ao vasculhar a memória, pareceu entrar em transe, subitamente recitando um diálogo estranhamente sedutor, como se fosse Selena outra vez: – Sinto muito – dissera a Max Lopez. – Não devia ter dito isso. É terrível.

– Tudo bem – respondera Max.

– Nos últimos dias, meu namorado nunca faz nada, e eu só quero vadiar um pouco.

– Não devia fazer isso se você tem namorado.

– Eu sei. É horrível... Às vezes eu acho um cara que topa.

– Ah. Já fez isso com outros caras antes?

– Sim.

– Bem, espero que encontre alguém.

– Eu esperava que fosse você. – Pausa. – Eu me sinto uma idiota.

– Não esquenta.

– Você costuma enviar fotos?

– Na verdade não.

– Bem, se não for muito estranho, talvez eu possa lhe enviar uma foto. E, se você não gostar, tudo bem.

William então vasculhou sua coleção de fotos pornô e encontrou uma que mostrava os seios de uma jovem que ele calculou seriam parecidos com os de Selena, com base no que ele podia ver na foto do perfil dela. Em seguida, enviou a foto.

A meta era induzir Max Lopez a responder com uma foto da própria genitália. Funcionou como feitiço. Pouco depois de William enviar a foto dos seios, Lopez prontamente enviou uma foto de seu próprio pênis.

– Todos ficam desesperados para receber elogios ao pênis – contou William. – Não sei por que os caras acham que as moças querem ver isso, mas funciona.

– Ai, meu Deus, que tesão – digitou William enquanto abria outra janela e postava a foto de Max no grupo privado de Facebook com seus *b*rothers.

– Todo mundo adiciona Max Lopes – solicitou ele.

Em breve, Max viu-se bombardeado por solicitações de amizades dos cinquenta outros perfis falsos no Facebook. Aparentemente sem desconfiar, Max aceitou a amizade de quinze deles. William e seus colegas do *b* entraram no perfil de Max e procuraram amigos do Facebook com o mesmo sobrenome, Lopez.

Quando o grupo pensou ter identificado uma conta do irmão de Max, William corroborou a informação diretamente com ele.

– Ah, eu acho que estudei com seu irmão no ensino médio – contou, ainda se fazendo passar por Selena. – Como é mesmo o nome dele?

Max respondeu que era Kevin. Agora William e os *b*rothers tinham mapeado os familiares mais próximos de Max. Chegara a hora de atacar.

– Não me bloqueie – pediu William subitamente.

Até mesmo no texto, o tom mudou quando sua farsa como Selena chegava ao fim.

– Tenho a foto de seu pênis e vou enviá-la para toda a sua família se você não me der sua senha no Facebook.

Primeiro Max Lopez ficou atônito. Logo depois, consternado. Aos dezessete anos, trabalhava na igreja local. Isso não ia pegar bem.

– Eu me senti mal, mas só dei risada – recorda William.

Desesperado, Max forneceu a senha, mas William não teve pudor em descumprir o combinado. Assim que entrou na conta do rapaz, ele pegou a foto do pênis e a postou no mural do Facebook da mãe de Max, com a mensagem: – Oi, mãe. Aqui está uma foto de meu pau. Diga-me o que você acha.

LOL.

Outros *b*rothers de William, membros do grupinho particular do Facebook, também tinham obtido acesso à conta de Max e agora postaram a foto para cerca de dez amigos e familiares. O benefício de postar de contas diferentes era que se tornava impossível para uma pessoa bloquear todas elas. Enquanto os outros do grupo do Facebook se encarregavam de espalhar na rede social de Max a foto com sua genitália, William escolheu outros garotos na lista de bate-papo de Selena e repetiu toda a operação.

Fazia meses que William não ria tanto quanto naquela noite. Foi “uma noite perfeita”, concluída por volta das nove horas da manhã seguinte. No final, sua equipe hackeou mais de dez contas do Facebook distintas, tudo graças ao acesso à conta de Selena.

– Rompemos vários namoros e horrorizamos várias mães – lembra-se William. – Esta é uma das partes de que eu mais gosto: enviar uma foto do pau de alguém para a sua respectiva mãe. A ideia de isso acontecer comigo é tão inimaginavelmente constrangedora que me faz rir.

O que ele amava fazer ainda mais, desde os quinze anos, tempo em que começou a praticar *pedo-baiting* (fingir ser um menor para servir de “isca”

a pedófilos), era deixar outro homem on-line altamente excitado e súbito jogar

um balde d’água fria com a ameaça de exposição à família e aos amigos ou à polícia. Enquanto sua vítima era emocionalmente arremessada de um extremo a outro, William lhe oferecia um vislumbre daquilo que ele sentia na época. Em suas palavras: “banho de alvejante, depressão reativa, um jorro quente e calafrio ao mesmo tempo”. Hackear as contas de outras pessoas no Facebook não era realmente uma experiência transcendental, mas ele sentia prazer em saber que, ao menos por um instante, as suas vítimas sentiam a vida desmoronando.

– Eu estaria mentindo se dissesse que havia algum motivo importante – explicou, recostando-se na cadeira e esticando os braços para revelar um enorme furo no suéter, perto da axila. – Não me sinto culpado, me faz rir e ajuda a desperdiçar uma noite. É tudo que eu quero do 4chan. Quero algo que não me deixe deprimido, algo para eu me concentrar. E é divertido fazer alguém se sentir tão péssimo dessa distância. Eu nunca faria isso cara a cara.

***

William passou as noites seguintes guardando as credenciais de Selena, encontrando-se com seu novo grupo do Facebook composto por pândegos do *b* e aterrorizando pessoas da rede social de Selena, inclusive postando comentários sobre as fotos de suas amigas mulheres e as chamando de gordas. A mãe de uma das amigas de Selena no Facebook, casualmente uma policial, por fim remeteu um mandado antiassédio ao endereço residencial da garota. William comentou que Selena foi “o presente contínuo”. A certa altura, postou uma atualização de status no perfil da garota, anunciando aos amigos dela que sua conta havia sido hackeada, mas tudo ia voltar ao normal – em seguida uma nova atualização de um suposto amigo, dizendo que Selena tinha sido atropelada por um motorista bêbado e morrido. Era esse o tipo de alvoroço que William gostava de causar. Não entretendo uma plateia de milhares no Twitter, como fazia Topiary, mas constrangendo outras pessoas para seu próprio entretenimento. Ainda assim, William e Topiary tinham coisas em comum, entre elas o relevante fato de que os dois haviam descoberto o Anonymous por meio do 4chan.

***

Dois meses depois de hackear a conta de Selena, William aceitou a oportunidade de conhecer Jake Davis, que agora estava livre sob fiança, em um almoço organizado para conversar sobre o Anonymous. Seria a primeira vez em que os dois se falariam, off-line ou on-line, e a primeira vez que ambos encontrariam

outro Anon cara a cara e conversariam sobre o impacto do Anonymous na vida deles.

William e Jake compraram passagens de trem para uma discreta cidade inglesa onde iriam se encontrar. Embora Jake viesse a saber o prenome verdadeiro de William e o conhecesse cara a cara, ele nunca solicitaria qualquer outra informação de identificação e nunca saberia seu nome completo. Na manhã do encontro, o trem de William serpenteou através da paisagem rural, deixando para trás os campos verdejantes e cor de palha, calmos rebanhos ovinos e rios castanhos que tremeluziam sob o rígido sol invernal. Ele não conseguia conter o nervosismo. Com igual sensação, Jake rumava ao sul em seu trem, a tornozeleira eletrônica confortavelmente lhe avisando que devia estar de volta às 22h. Quando o trem de Jake chegou à estação, ele apeou, caminhou até uma parede no saguão e esperou.

Quinze minutos depois, o trem de William freou num chiado na plataforma oposta. Desceu, caminhando com dificuldade em meio à grande multidão de passageiros, até avistar Jake parado junto a uma parede, numa pequena nesga de luz solar. Jaqueta preta, estatura baixa e barba por fazer.

Levantou o olhar e sorriu para um inexpressivo William. Os dois se cumprimentaram com um aperto de mãos antes de rapidamente desviar o olhar.

Os Anons quase nunca se encontravam pessoalmente, pois, naturalmente, isso eliminava o objetivo do anonimato. Portanto, o encontro de William e Jake foi esquisito no começo. O que tornava a situação mais difícil era o fato de que William atravessava uma fase especialmente sombria, e, nos últimos dias, estivera constantemente lutando contra ideias de suicídio. Jake, que desejava falar com gente fora do círculo próximo de familiares, em especial com alguém com quem tivesse algo em comum, estava ansioso para conversar.

Enquanto a dupla sentava numa pizzaria local para almoçar, Jake conversou amigavelmente sobre seu caso no tribunal e algumas notícias recentes sobre o Anonymous que ele tinha visto na televisão. William permanecia calado e emburrado. Quando Jake contou uma história engraçada de seus dias de LulzSec, na esperança de que isso pudesse provocar uma risada, William reagiu com um silêncio sepulcral. O encontro não ia bem.

Enfim, tão logo a conversa recaiu no 4chan, William se abriu um pouquinho.

Conversou sobre sua frustração com o site que ele visitava tanto e como ele havia se tornado uma comunidade repleta do “câncer newfag” – ansiosos e novos participantes que não entendiam a cultura nem sabiam como causar transtornos reais.

Jake, como William, não era um hacker habilidoso, mas entendia um pouco de linguagens de programação. Quando William mencionou que estava interessado em desenvolver essas habilidades, Jake pegou o netbook na mochila. O pequeno laptop estava sem o cartão wireless e sem Ethernet, por isso não havia maneira de se conectar à internet. Mas Jake ainda podia brincar com o script Zalgo, tipo de fonte programável que empacotava muitos bytes digitais em cada letra. Se você procurava diversão, podia usar esse recurso para enviar a alguém uma mensagem no Skype; talvez travasse o programa da pessoa.

Jake começou a digitar: – Se você colocar isso no Skype, reverterá seu texto – disse ele.

William observou visivelmente impressionado.

– Sua memória é incrível – ele retrucou, balançando a cabeça e se inclinando à frente no assento.

Jake prosseguiu: – É só carregar o mapa de letras no Windows, descarregá-lo em qualquer lugar e está feita a confusão – explicou ele, agora digitando freneticamente.

– Então posso fazer isso no Windows?

– Sim, é meio complexo.

– Quer dizer que 8 bytes equivalem a... 1 bit – disse William, hesitando.

– Oito bits equivalem a um byte. – William recebia uma breve aula sobre fundamentos de programação.

– Sim, sim – confirmou William, rindo um pouco, agora mais à vontade.

– Não entendo nada disso.

– Sou meio entusiasta do Unicode – explicou Jake, sacudindo os ombros.

Tão logo o netbook foi fechado e posto de lado, os dois começaram a conversar sobre o Anonymous e como o grupo os havia mudado.

– O grupo me tornou uma versão mais extrema de mim mesmo – avaliou William. – Eu costumava dormir mal. Agora praticamente não durmo. Eu costumava ser irônico; agora sei que sou um babaca. – Ele não apenas "gostava" de atormentar as pessoas; ele amava. Não apenas "gostava" de pornografia; ele consumia isso todos os dias. E acrescentou: – Nada disso me afeta. Não me importo com nada.

William dissera no passado que não tinha código moral; tudo era caso a caso, tomando decisões numa reação instintiva. Ernest Hemingway enunciara melhor: "Moral é o que o faz se sentir bem depois, e imoral é o que o faz se sentir mal depois".

Jake assentia.

– Tenho de concordar com tudo isso – comentou. – Fiquei dessensibilizado. A gente pode assistir à queda das Torres Gêmeas ouvindo música eletrônica japonesa. Pode parecer horrível, depois parece uma coisa natural que você presencia todos os dias.

Essa era a cultura que tanta gente fora do Anonymous não conseguia entender. A interação com milhares de pessoas na internet havia criado um afastamento da realidade e uma sensação de estar alheio a certas consequências. O Anonymous fazia coisas ruins, mas seus membros não eram pessoas ruins, *per se*.

Como se para ilustrar o raciocínio, uma mulher sentada ali perto subitamente se virou para Jake e William e indagou se eles sabiam como acessar o WiFi do restaurante num celular. Os dois se entreolharam, inexpressivos. Em seguida, rapidamente explicaram que nenhum tinha um celular que podia conectar-se à internet. Em genuíno tom de desculpas, ambos tentaram ajudar a mulher com algumas dicas: – Quem sabe você pergunta a algum funcionário lá embaixo? – sugeriu William. – Vai me desculpar.

A mulher sorriu e voltou a dedicar atenção ao seu sanduíche italiano.

Ela jamais suspeitaria de que essa dupla de jovens atenciosos era composta por membros famosos do Anonymous. Era comum uma concepção errada sobre a falta de moral no *b* e no Anonymous.

– Não significa que você faça coisas ruins – disse William. – Apenas significa que não existem regras. Não revertemos isso para nos tornar canalhas em todas as oportunidades.

– Também é legal apenas ser legal – emendou Jake.

Muitos dos usuários mais radicais do *b*, como William, não se importavam com empregos, família ou típicos eventos marcantes da vida.

Jake e William saboreavam a ideia de viver uma vida sem impactos sobre as pessoas verdadeiras. Se William conseguisse descolar uma grana suficiente blogando – usava um perspicaz script da web que lhe permitia explorar o Google Ads sem ter de escrever muita coisa –, no fim do mês ele voaria para a Europa Continental e se tornaria morador de rua em uma capital importante. Estava cansado de ser um fardo para o pai e o irmão; cansado de tocar guitarra e saber que eles podiam escutá-lo.

– Viver exercendo o mínimo impacto em tudo que for possível é uma ideia realmente sedutora, equivalente a nunca ter nascido – ponderou Jake.

Nenhuma residência legítima, nenhum nome em um pedaço de documento governamental, nenhuma impressão digital. Permanecer inominado, sem identidade, sem ser travado por sistema algum, mas, ao contrário, "viver despreocupadamente em todos os lugares" era algo pelo qual os dois ansiavam na vida real.

Será que esse anseio vinha daquilo que eles haviam experimentado com o Anonymous: vandalizar as coisas, muitas vezes com poucas consequências?

– É a cultura Anon, a cultura da internet – explicou Jake. – On-line a gente vê de tudo. Coisas sanguinolentas, nojentas, e se dá conta de que não se importa. Vamos parar de fazer estardalhaço por coisinhas. Tem sempre algo maior ou menor, pior ou melhor. A maior parte do que fazemos é o que as pessoas já fizeram.

Nada do que ocorria no *b* tinha intenção de ser levado a sério, emendou William. Apenas eram coisas que aconteciam.

– Nada importa.

– Exato – concordou Jake. – Essa é a principal coisa sobre a vida. O

pessoal acha que somos superiores aos animais. E fica procurando esse elo perdido, mas que tal se formos o elo entre os animais e os seres humanos verdadeiros que ainda nem evoluíram? É pretensão pensar que somos superiores no universo só porque conseguimos nos comunicar entre nós.

– É tão arrogante – comentou William.

– Abelhas descobriram que o planeta era redondo antes de nós – frisou Jake. – Então elas são mais inteligentes que nós.

– Elas não fazem escândalo para reclamar – acrescentou William.

As pessoas levavam o Anonymous muito a sério?

– O Anonymous leva o Anonymous muito a sério – disparou William rapidamente. – Quando comecei a me envolver mais, era 50% diversão e 50% passatempo e nada mais. Agora existem todas essas mensagens políticas, e eu não dou a mínima. Fico incomodado ao ver um grupinho de meninos ricos se queixando de serem oprimidos. Existem coisas muito piores no mundo do que a lei dos direitos autorais [uma das grandes causas citadas pelos recentes ataques do Anonymous]. Seja como for, eu não acho que a gente deva fazer um escândalo para reclamar.

– Preciso lutar contra isso – admitiu Jake. – Às vezes, eu me importo muito com alguma coisa, mas no minuto seguinte já não dou bola. Quando eu tento explicar como me sinto para as pessoas do mundo real, eles atribuem o fato à esquizofrenia.

– Às vezes, algo vai acontecer e daí de repente você se importa com o fato – disse William. – Aquilo importa por trinta segundos.

Embora isso soasse estranho à primeira vista, não era nem um pouco diferente do ciclo de notícias de vinte e quatro horas ou do exagero que cercava novas reportagens populares; elas sumiam com igual rapidez da memória de curto prazo do público.

– Era essa a sensação de escrever comunicados de imprensa para o LulzSec – mencionou Jake. – “Eu me importo, eu me importo, eu me importo.” Daí

provoca um rebuliço nas notícias e eu penso: “Deixa pra lá”.

Eu me sinto mal que as pessoas estejam sendo presas, fico inspirado e depois não me importo. Como com o movimento Antisec.

– Opiniões sobre esse tipo de coisa são tão fluidas – opinou William –, talvez porque somos jovens e impressionáveis. Talvez sejamos honestos apenas quando mudamos de opinião.

– A gente se importa subitamente com alguma coisa porque estamos mais enriquecidos pela sensação de vitória – disse Jake, referindo-se aos ataques em larga escala feita pelo Anonymous e às grandes investidas do LulzSec. – Depois passa, e a gente não se importa mais.

Algum dia um deles já se sentiu manipulado pelo Anonymous?

– Nem um pouco – afirmou William.

Jake baixou o olhar por um instante antes de responder: – Não manipulado, mas influenciado – analisou ele. – Quando você está numa mentalidade de máfia com muitas outras pessoas, você também tem uma versão “extrema máfia” de si mesmo, esse raciocínio único e unificado de que não se importa com nada que existe e quer arruinar algo.

Nesse instante, William fez que sim com a cabeça.

– Eu disse que não, mas esse lance da máfia faz sentido – disse ele.

A questão da saúde mental significava muito para William pessoalmente, mas às vezes deparava com um tópico no *b* em que o postador original havia dito: – Estou realmente deprimido e quero me matar.

Se os participantes do tópico se inclinavam na direção de incentivá-lo a cometer suicídio, William entrava no bate-papo e postava uma foto de uma lata de cianureto, lembrando ao OP que o fizesse de modo adequado.

– Que é algo em que eu nem sequer acredito. Não quero que as pessoas morram, mas – sacudiu os ombros – é algo para escrever e algo para fazer.

Claro, tanto William como Jake também praticaram sua boa parcela de

manipulação. William desprezava os usuários mais jovens do 4chan (goombies e newfags) que levavam a sério os símbolos revolucionários de *V de vingança*, e às vezes os irritava só para se divertir.

– Eles querem pensar que o mundo está contra eles para justificar sua angústia – definiu. Por isso, era sempre fácil convencer as pessoas a participar da revolução no Anonymous. – Basta inventar um história [sobre corrupção governamental ou corporativa] que elas acreditam.

Para escrever um post incitador no *b*, por exemplo, bastava redigi-lo de um modo que atraísse a multidão Anon, utilizando dispositivos linguísticos como aliterações, repetições, frases de efeito e palavras dramáticas como *injustiçados*, *oprimidos* e *espezinhados* para descrever a maneira como o povo se sente em relação a corporações e governos, e *justiça*, *liberdade* e *rebelião* ao se referir ao Anonymous.

– Você consegue inspirar alguém de quinze anos de idade, ou alguém com mentalidade de quinze anos, a odiar uma pessoa, seja quem for, de acordo com sua vontade – constatou William sem mostrar emoção.

Não tendo um objetivo claro, o Anonymous se parecia com qualquer outro movimento dos dias modernos que se fragmentara pela natureza de uma sociedade habilitada pela internet – natureza gerada pelos usuários com participação coletiva. Movimentos como o Tea Party e Ocuppy Wall Street tinham o mesmo problema: objetivos muitas vezes vagos, mas defendidos apaixonadamente pelos partidários contra ideologias rivais. O

Anonymous tornara-se um novo movimento, um novo processo, para combater opressores identificados. E podia ser manipulado.

– É fácil dar exemplos de situações em que somos oprimidos, e algum idiota, algum estudante trouxa que tem o despertar político aos catorze ou quinze anos e que se acha esperto vai acreditar! – William quase gritava agora. Parou num instante de reflexão, como se surpreso pela força de sua própria opinião, e deu uma risadinha. – Sou apenas cinco anos mais velho que esse pessoal, mas tenho a impressão de que sou o pai deles.

Mas Jake balançava a cabeça positivamente outra vez. Se você sabia como se comunicar com os Anons, às vezes conseguia direcioná-los.

– É muito fácil mesmo – concluiu.

***

Enquanto Jake e William retornavam a pé para a estação ferroviária, enfrentando o vento cortante, contaram histórias sobre trollagens sofisticadas, praticamente sem perceber o quanto suas tensões iniciais tinham se esvaído. Jake descreveu um de seus episódios prediletos, enquanto William prestava atenção: anos antes, ele e um amigo tinham convencido um inimigo on-line a executar um ato sexual diante de sua webcam no meio da noite. Eles haviam filmado a cena e em seguida disseram ao garoto que mostrariam o vídeo à polícia local e à escola dele se não acordasse a mãe para que pudessem mostrar a ela. Às quatro da madrugada, ele fez isso, e ficou chorando na maior parte do tempo em que sua mãe assistia à cena horrorizada. Jake e o amigo dele riram à beça.

– Decidimos deixar o cara se safar apenas mostrando o vídeo à mãe dele – contou ele, erguendo a voz para ser escutado em meio ao vento sibilante.

William pareceu chocado.

– É isso que você chama deixar alguém se safar? – indagou incrédulo.

– Sim – Jake sacudiu os ombros.

William assobiou, impressionado.

O trem de William parou. Hora de embarcar. Seguiu-se uma despedida sem cerimônias, a relevante discussão e o desnudar das almas rapidamente esquecido nos últimos e desajeitados apertos de mãos. Jake e William acenaram ligeiramente com a cabeça e depois desviaram o olhar na direção oposta. William subiu no trem sem olhar para trás. Jake voltou para esperar seu próprio trem.

Eles tinham encontrado o Anonymous no mesmo local e adotado perspectivas semelhantes sobre a vida, mas estavam em caminhos divergentes. Mesmo após conhecer Jake e ver as consequências de ser preso por hackeagem, William ainda queria aprender a fazer mais do que apenas convencer alguém a lhe fornecer a senha do Facebook. Queria aprender a invadir uma rede de computadores. Durante semanas a fio, continuou a baixar e-books grátis e ler seções sobre programação na Encyclopedia Dramatica. Gradativamente, começou a testar

técnicas e ferramentas populares de hackeagem, como o decodificador de senhas Cain and Abel, mapas de SQL, Googledorks e Backtrack5. Assim, em 10 de março de 2012, William atingiu um marco. Após cinco horas experimentando, quebrou a senha do WiFi de seu vizinho e começou a utilizá-la. Comentou esperançoso:

– Depois vou tentar roubar seu conteúdo, mas acho que está velho, por isso não estou ansioso por n00dz.

William não tinha planos de parar de perturbar a vida alheia, e, exatamente como acontecera com Jake, Sabu e Kayla, estava certo de que nunca seria descoberto.

Jake, em março de 2012, fora proibido de utilizar a internet por oito meses. Se o caso fosse a julgamento, os milhares de páginas de registros de bate-papo e complexas configurações de computador que serviram de provas significavam que o processo facilmente podia durar um ano. Era difícil para ele pensar no futuro e no que poderia fazer após sair da cadeia.

Ainda gostava da ideia de “viver despreocupadamente em todos os lugares”, viajando a locais em que ninguém soubesse quem ele era.

Desejava um dia conseguir um emprego em que pudesse trabalhar ao ar livre, talvez dirigindo. Tinha praticamente certeza de que não queria trabalhar com computadores. Estava cansado de todo o estresse causado por eles no passado. Até mesmo sem internet, era difícil se livrar dessas lembranças atormentadoras e paranoicas. Mas naquele mês elas voltariam à tona mais fortes do que nunca, quando ele descobriu o motivo pelo qual Sabu permanecera solto por tanto tempo.

CAPÍTULO 26

O verdadeiro Sabu

O que acabou acontecendo com Hector “Sabu” Monsegur? Depois das prisões de Topiary e Tflow, ele continuou a liderar o revivido movimento Antisec, tweetando na conta por ele rotulada como “The Real Sabu” para um crescente grupo de dezenas de milhares de seguidores. Às vezes, incitava revolução: – Adoro o cheiro de guerra cibernética pela manhã #fuckisrael.

Outras vezes, direcionava sectários ao canal de bate-papo do Antisec: – Em breve, a matriz de choque do irc.anonops.li!

Se as pessoas que o controlavam ordenassem que ele puxasse as rédeas, ele obedecia, alertando o Anonymous em 21 de setembro de 2011

de que as tentativas de desferir ataques de DDoS contra empresas financeiras de Wall Street tinham sido “um fracasso... Não devido à falta de efetivo pessoal, mas sim a erros de comando. Tentem hackeá-los e não desperdicem recursos com ataques de DDoS”.

Para alguém que havia sido tão enfático em seu ódio contra a polícia, não fora tão difícil assim convencer Sabu a colaborar com o FBI. Em 8 de junho de 2011, no dia seguinte após seu sumiço no LulzSec causar preocupação no grupo de amigos hackers, Sabu foi ao tribunal, onde um juiz decidiu soltá-lo sob fiança. A condição: deixar o FBI supervisionar todos os seus passos on-line e na vida real.

Nos dois meses seguintes, enquanto o LulzSec terminava sua farra de hackeagem e os membros fundadores do grupo, Topiary e Tflow, eram presos, Sabu continuou a trabalhar silenciosamente com o Federal Bureau of Investigation. De acordo com relatos posteriores, ele se revelou um informante dedicado. Continuava a varar acordado quase todas as madrugadas, conversando com outros hackers e descobrindo seus ataques iminentes. Quando corriam boatos de que o Anonymous ou o LulzSec estavam prestes a atacar um governo ou uma empresa, ele tentava conversar com os hackers envolvidos para corroborar se o ataque estava prestes a acontecer. Talvez pela primeira vez na vida, Monsegur tinha a sensação de receber o respeito que merecia – desta vez, da polícia.

Em 15 de agosto, ele compareceu diante do juiz numa segunda audiência secreta

no tribunal do distrito sul de Nova York e se declarou culpado de doze acusações, a maioria relacionada com hackeagens de computador. Sabu concordou em ajudar o FBI, e os promotores federais concordaram em não processá-lo por vários outros crimes que ele havia cometido fora do mundo da hackeagem. Esses crimes incluíam porte de arma, venda de meio quilo de maconha em 2010 e dois quilos em 2003, compra de joias e equipamentos eletrônicos roubados e desfalque no valor de US$ 15 mil no cartão de crédito de um ex-empregador. Sabu cometera muitas outras contravenções on-line: os inspetores descobriram que ele hackeara um cassino on-line e, em 2010, invadira o site de uma empresa de peças automotivas, remetendo a si mesmo quatro motores de veículos que valiam US$ 3450. Levando em conta o entusiasmo com que Sabu se gabava de sua década "nos subterrâneos", quando havia "dominado governos inteiros", possivelmente a polícia deixara escapar muita coisa. Mas os Feds estavam mais interessados na ajuda de Sabu em outros processos.

– Desde literalmente o dia em que foi preso, o réu tem cooperado proativamente com o governo – informou ao juiz o promotor público James Pastore, advogado da acusação, na audiência de agosto. – Às vezes, passa a noite acordado envolvido em conversas com coconspiradores. Essas conversas ajudam o governo a reunir provas contra eles.

Pastore leu as acusações em voz alta e afirmou que elas poderiam resultar numa sentença máxima de 122 anos e meio de cadeia. Se Monsegur continuasse seu "acordo de cooperação" com o governo federal, a sentença poderia ser mais curta.

O juiz então se virou para Monsegur e indagou se ele estava disposto a se declarar culpado.

– Sim – respondeu ele.

Com isso, Monsegur agora podia se esquivar de qualquer tipo de julgamento. Em seguida, leu em voz alta uma declaração na qual admitia ter praticado uma série de atos ilegais entre 2010 e 2011.

– Participei pessoalmente de um ataque de DDoS contra sistemas computacionais, PayPal, MasterCard e Visa – reconheceu. – Eu sabia que minha conduta era ilegal.

Voltou a admitir após listar cada item de seu indiciamento, desde acessar os

servidores da Fox até a PBS, passando pela Infragard Atlanta.

– Muito bem – asseverou o juiz. – O pedido está aceito.

O juiz concordou em postergar a publicação da sentença porque Monsegur poderia correr "grande perigo pessoal" se fosse identificado.

Entre os riscos aparentes especificados no tribunal: os hackers poderiam enviar centenas de pizzas ao apartamento de Monsegur ou induzir o comparecimento de uma equipe da SWAT à casa dele (tática bem conhecida de usuários do 4chan como William).

– Na verdade, há um verbo para isso: "swatar" – explicou o promotor público Pastore.

Após a audiência, Sabu continuou a colaborar com o FBI, às vezes trabalhando diariamente nos escritórios do governo. Os agentes federais substituíram seu laptop, tão antigo que várias teclas já não se distinguiam, entre elas as teclas de Shift, L e 7, por um novo laptop que continha software de keylogging monitorando tudo que ele digitava. Instalaram câmeras de vídeo na casa dele para monitorar seus movimentos físicos.

Permitiram-no continuar a farsa pública de ser o hacker mais procurado dos EUA, incentivando outros a participar do movimento Antisec, do qual se comportava como líder, até mesmo caçoando da polícia e de quem o criticava.

– Fontes internas da Interpol me contam (além de "Eles gostam de manteiga na torrada") que o próximo preso serei eu – anunciou ele no Twitter em agosto. – Está todo mundo empolgado com a notícia? – Mais tarde, acrescentou: – Mensagem para a Interpol: CHUPEM MEU PAU.

Mas muita gente no Anonymous suspeitava de Sabu. Por que todos os demais fundadores do LulzSec tinham sido capturados enquanto o falastrão líder da gangue, que todos sabiam morar em Nova York e ter ascendência porto-riquenha, continuava livre?

Entre os mais desconfiados encontrava-se Mike "Virus" Nieves, hacker que havia colaborado com Sabu durante o LulzSec. Em 16 de agosto, um dia após a segunda audiência de Sabu no tribunal, na qual ele havia concordado por escrito em trabalhar para o FBI, Virus acusou Sabu explicitamente de ser um delator. A

conversa começou quando Sabu primeiro abordou Virus e fez uma acusação velada de que um amigo dele seria um informante. De imediato Virus percebeu a jogada por trás dessa tática intencional. Típica estratégica entre informantes hackers: para confundir alguém que suspeita ser você um delator, você parte para acusação de que o delator é *ele*. O

longo bate-papo, que acabou se tornando hostil, ocorreu duas semanas após Jake Davis ter saído de sua primeira audiência no tribunal.

– Quanto a Topiary – Virus contou a Sabu –, você o dedurou. É tão óbvio, Sabu.

– Melhor dobrar sua maldita língua, porque eu não sou dedo-duro – respondeu Sabu. – E com certeza não dedurei um parceiro.

Virus não prestava atenção.

– Sei identificar um roedor a quilômetros de distância. – Aproveitou para acrescentar: – O "Antisec" foi uma piada completa.

– Para ser uma piada completa está provocando mais desordem do que há uma década – retorquiu Sabu.

– Você nem entende o espírito do Antisec – alfinetou Virus. – Você não está dominando chapéus brancos, só sites idiotas de governos estrangeiros.

– Na verdade, eu participei do movimento original – rebateu Sabu. – Grande diferença, cara. Não fico aqui sentado e rodo ferramentas automatizadas. Sou um experiente pesquisador de segurança atuando desde o final dos anos 1990.

– Você é um chapéu preto de baixo nível que foi dominado – disparou Virus. – Larguei mão de sua amizade. Você é muito suspeito e estou muito velho para essas criancices. Seu movimento Antisec esfarrapado ataca tudo que pode.

Na verdade, os seguidores do Antisec de Sabu muitas vezes eram impedidos ao tentar atacar "tudo que pudessem". O FBI se aproveitava do status de Sabu como líder cultuado para acompanhar cada hacker que apresentava uma vulnerabilidade para seu mentor, na esperança de receber um elogio. Às vezes Sabu recebia mais de doze vulnerabilidades por dia, e em todas as ocasiões ele alertava seus supervisores do FBI. Por volta de agosto de 2011, ele havia auxiliado o FBI a remendar 150

vulnerabilidades em redes de computadores alvejadas por outros hackers, ou pelo menos ajudado a mitigar os danos. Ao longo dos meses seguintes, ele comprovadamente ajudaria a alertar cerca de trezentas organizações governamentais e corporativas sobre potenciais ataques por hackers ligados ao Anonymous, permitindo-lhes reparar as falhas em suas redes.

Ao encerrar o impasse com Sabu, Virus se mostrou pragmático em relação ao que ele provavelmente fazia.

– Para ser franco, não me importo se você está trabalhando com os Feds para limpar a bagunça que fez e colocando seus "amigos" na cadeia – disse ele. – É a natureza humana.

– Meu neguinho – retrucou Sabu –, tem de parar de repetir isso. Sério.

– Caso contrário?

– Vamos nos encontrar em Manhattan e falarmos cara a cara.

– Conheço suas táticas, e você não vai ganhar acesso a nenhum dado meu – atalhou Virus.

– Bro, você me conhece menos do que os Feds – disse Sabu, momentaneamente insinuando seu relacionamento de trabalho com o FBI.

– Mas vamos falar sério.

A conversa recaiu sobre o quanto a palavra *delator* era ofensiva, até que Sabu observou: – Você está falando muita merda, como se tivesse um problema comigo.

Eu sempre te tratei com amor louco desde o primeiro dia que te conheci.

– Não dou a mínima para o seu amor – rebateu Virus convicto. – Não existe "amor" na internet.

Isso parecia mais verdadeiro do que todo o resto. Sabu podia ter sido um hábil hacker capaz de descobrir vulnerabilidades na rede e explorá-las, mas sua principal habilidade era hackear as mentes das pessoas. Mentia aos próprios membros da equipe formada e liderada por ele, durante todo o tempo auxiliando

a polícia a construir acusações contra os companheiros e corroborar suas identidades. O mais impressionante era que o carisma e as mentiras de Sabu soavam tão eficazes que os outros hackers continuavam a trabalhar com ele, até mesmo após a prisão de Topiary, Tflow e Kayla, e até mesmo à medida que outros hackers levantavam suspeitas sobre ele. Inclusive se considerava um segredo de polichinelo no meio hacker da cidade de Nova York que “Sabu” era Monsegur, e até corria o boato de que os hackers locais tinham pichado o prédio dele.

No mesmo dia do confronto de Sabu com Mike Virus, um grupo de autointitulados investigadores antiAnonymous publicou um post de blog alegando ter doxeado Sabu. Dessa vez, os documentos incluíam uma foto de um corpulento sujeito de aparência latina beirando os trinta anos, vestindo jaqueta de couro e chapéu. A foto era de Monsegur. Também trazia um relato detalhado de suas façanhas e seu endereço IP. Talvez fossem os dox mais abrangentes até aquela data. No dia seguinte, 17 de agosto, Sabu postou uma mensagem críptica no Twitter, invocando uma citação do filme *Os suspeitos*, sobre o mítico vilão, Keyser Söze: “A maior peça que o diabo já pregou foi convencer o mundo de que ele não existia. E, num piscar de olhos, ele sumiu”. Durante as semanas seguintes, ninguém ouviu um pio de Sabu no IRC público nem no Twitter. A maioria supôs que ele havia fugido ou sido capturado. Então, exatamente um mês depois, 17 de setembro, ele voltou a tweetar, começando assim: – Tentaram me delatar, me trollar, doxear todo mundo ao meu redor, me atrair com argumentos intermináveis. Mas tem uma coisa que eles não conseguem fazer: ME PARAR!

De imediato, Sabu mergulhou simultaneamente no mundo do Anonymous e do Antisec, entabulando conversas em canais públicos de IRC

e solicitando relatos de outros hackers Antisec. Na maior parte do tempo, ele não participava de quaisquer ataques. Outros hackers próximos a Sabu na época não se lembravam de ele ter hackeado alguma coisa durante meses após sua volta. Sabiam que ele se vangloriava publicamente no Twitter dos ataques que havia executado, mas imaginavam que isso fazia parte do seu papel como porta-voz do Anonymous e do Antisec. Sabu, em vez disso, incentivava os “mais jovens” no Anonymous, elogiando-os e oferecendo-se para facilitar os ataques, contou uma fonte.

A certa altura, por exemplo, ele se ofereceu para ajudar os hackers do

Anonymous no Brasil a obter acesso aos servidores do governo. (O

hacktivismo é extremamente popular no Brasil, em parte porque o país tem a taxa mais alta de uso do Twitter e também devido à controvérsia duradoura sobre a corrupção governamental.) Sabu atuou como mediador, conversando com os hacktivistas brasileiros e depois contando à sua equipe de hackers os sites escolhidos como alvos de deface pelos brasileiros. A equipe penetrou nos servidores brasileiros e depois enviou a Sabu as credenciais de logon para serem repassadas aos hackers brasileiros.

– Não conseguimos nos lembrar de uma [hackeagem] feita por ele, até mesmo antes de se envolver com a polícia – falou um hacker que trabalhava com Sabu desde o fim de 2011, pelo menos. – Ele gostava de falar que fez tudo. Não fez.

Não está claro até que ponto Sabu teve permissão de hackear impunemente durante o período em que auxiliou o FBI. Existem relatos distintos. Alguns defendem que, em seu papel de corroborar as alegações públicas do Anonymous de que uma empresa ou agência governamental havia sido hackeada, ele penetrava na rede alvejada e conferia a existência da vulnerabilidade. Outros afirmam que ele apenas conferia as alegações conversando com outros hackers em salas privadas de IRC. Provavelmente acontecia um pouco de cada. Na maior parte do tempo, ele fornecia conselhos, vociferava ordens e tentava manter-se no completo controle da situação. Por exemplo, em dezembro de 2011, solicitou a um hacker chamado Sup_g que havia roubado dados do nychiefs.org: – Qual é a novidade sobre a dominação do nychiefs? Encerrou o assunto ou tem coisa nova?

Naquele mês, Sabu ajudou o FBI a obter um vislumbre de um dos maiores ataques do Anonymous, jogando a isca para esse mesmo hacker. O

ataque foi contra a Stratfor, serviço de inteligência com sede em Austin, a qual lucrou vendendo um informativo a clientes que incluíam o Ministério da Segurança Nacional.

Em 6 de dezembro, Sup_g, empolgado, indagou a Sabu sobre a Stratfor num canal privado de IRC.

– E aí, está disponível? Trabalho nesse novo alvo – contou ele.

– Sim – disse Sabu. – Estou aqui.

Sup_g colou um link para o painel de administração do Stratfor.com, explicando sobre o potencial de obter dados de cartão de crédito. Tinha certeza de conseguir decodificá-los.

Sabu notificou os supervisores do FBI. Ao longo dos próximos dias, Sup_g e outros hackers batizaram a hackeagem da Stratfor de *lulz natalina*, consideraram-na um marco para o Anonymous e o Antisec. Uma semana depois, Sup_g passou umas oito horas invadindo a rede da empresa, e, no dia seguinte, 14 de dezembro, contou a outro hacker que agora estava nos e-mails da Stratfor: – Estamos no páreo, baby. Hora de se esbaldar com as bobinas [de email] deles... Acho que eles vão apenas desistir quando isso vier à tona.

Enquanto o FBI assistia, aparentemente impotente, aos hackers roubaram 60 mil números de cartões de crédito, junto com dados de 860

mil clientes da Stratfor, e-mails dos funcionários e dados financeiros, e incríveis 2,7 milhões de e-mails confidenciais. Sob a orientação do FBI, Sabu mandou a equipe armazenar tudo num servidor de Nova York.

Na noite da véspera de Natal, 24 de dezembro, os hackers fizeram o deface do site da Stratfor e publicaram os dados dos cartões de crédito de 30 mil clientes, alegando tê-los utilizado para doar US$ 1 milhão para instituições de caridade – inclusive publicando os recibos. Mais tarde, o FBI confirmou que os cartões de crédito tinham sido utilizados para gastos fraudulentos de ao menos US$ 700 mil. A Stratfor teve de interromper a cobrança da assinatura de seu relevante informativo, estimando que a falha de segurança resultara em danos materiais e lucros cessantes de US$ 2

milhões.

Sabu talvez não tenha impedido o ataque, mas realmente ajudou o FBI a identificar a pessoa por trás da investida contra a Stratfor, Sup_g. Fez isso corroborando que Sup_g também utilizava outro nickname, Anarchaos. Em 26 de dezembro, Sabu abordou Sup_g on-line, talvez exacerbando na encarnação do papel de hacker ainda fora da lei.

– E aí – saudou. – Ouvi falar que estamos nas manchetes dos jornais.

Ainda vou ser preso por culpa de vocês, seus desgraçados. HAHAHAHA.

– Cara, o negócio é grande – disse Sup_g.

– Se eu for preso, anarchaos, o seu trabalho é causar confusão em minha honra – pediu Sabu, sutilmente deixando escapar o outro nickname de Sup_g, anarchaos, e acrescentando inclusive um coração – <3.

– Assim será – respondeu Sup_g, sem ter a consciência de que já havia se incriminado.

Ao longo dos meses seguintes, enquanto os Feds escrutinavam os registros de bate-papo com Sup_g no computador de Sabu, eles juntaram informações pessoais suficientes para construir um quadro de quem o hacker realmente era. Chegaram a Jeremy Hammond, 27 anos, ativista político de Chicago, adepto de compridos dreadlocks e do freeganismo – os agentes federais relataram tê-lo flagrado procurando comida em contêineres de lixo após terem começado a vigiá-lo pessoalmente. Mais tarde, a mãe dele informou aos repórteres que Hammond tinha sido um gênio da computação que não conseguiu conter seu impulso de "torrar a paciência dos EUA".

Talvez o FBI tivesse um alvo maior em mente do que Hammond e seu penteado dreadlock: Julian Assange. Logo após os hackers terem vazado os e-mails da Stratfor e começado a vasculhá-los, observaram que muitos emails tratavam do WikiLeaks. Então eles decidiram que fazia sentido repassá-los à organização denunciadora e que o WikiLeaks, de qualquer modo, faria um melhor trabalho em disseminá-los.

É possível, porém não conclusivo, que, ao assistir àquilo que estava prestes a acontecer, o FBI torcesse para se aproveitar da hackeagem da Stratfor e obter mais provas contra Assange, de modo a conseguir finalmente extraditá-lo aos EUA. Mais tarde, o FBI negou ao *The New York Times* ter "deixado o ataque [à Stratfor] acontecer com o objetivo de coletar mais provas", afirmando que os hackers já estavam atolados até os joelhos nos arquivos confidenciais da Stratfor em 6 de dezembro. E acrescentou: a esta altura, já era "tarde demais" para impedir a execução do ataque.

Documentos do tribunal, porém, mostram que os hackers só acessaram os e-mails da Stratfor por volta de 14 de dezembro. Em 6 de dezembro, Sup_g não estava exatamente "atolado até os joelhos" nos arquivos: havia apenas descoberto dados de cartões de crédito criptografados, que ele se considerava

capaz de decodificar.

Também vale dizer que Sabu, o sujeito que entrou no Anonymous para ajudar Assange a se vingar, repentinamente parecia muito disposto a conversar com o fundador do WikiLeaks depois que os supervisores do FBI começaram a vigiá-lo. Segundo fontes hackers, além do contato inicial feito durante o LulzSec, Sabu mostrou-se especialmente interessado em falar com Assange repetidas vezes após a hackeagem da Stratfor, "assediando" o adjunto de Assange para conseguir contato.

– Sabu há um bom tempo tentava entrar em contato [com Assange] – informou um hacker.

Outros acrescentaram que, ao Sabu escutar pela primeira vez que o Anonymous planejava fornecer os e-mails da Stratfor ao WikiLeaks, ele "surtou": logo fez uma ligação telefônica ao WikiLeaks e exigiu falar pessoalmente com Assange. Não está claro se conseguiu falar com o próprio Assange ou com seu adjunto, mas, de acordo com várias fontes, Sabu então pediu dinheiro em troca dos e-mails da Stratfor. Ao que parece, Assange disse não.

Ao saber que Sabu pedira dinheiro pelos e-mails que eles haviam roubado, os hackers da Stratfor ficaram chocados e rapidamente transferiram os e-mails ao servidor do WikiLeaks, sem cobrar nada. O

WikiLeaks não negou, em público ou em particular, que Sabu pediu dinheiro da organização. Mas, se o WikiLeaks tivesse pagado pelas informações, as autoridades dos EUA poderiam ter construído um caso bem mais consistente contra Assange. Parece duvidoso que o FBI tivesse tempo ou inclinação para decidir, de cima para baixo, fazer jogo duplo a fim de tentar prender o WikiLeaks, mas talvez um agente em algum lugar tenha tido a ideia de incitar Sabu a pedir dinheiro de Assange e ver no que dava.

Tão logo o WikiLeaks pôs as mãos nos e-mails de Stratfor, formou parcerias com 25 organizações da mídia, inclusive a *Rolling Stone* e o *Russia Reporter*, e publicou uma sequência de informações confidenciais. O

WikiLeaks os chamou de Arquivos de Inteligência Global.

Analistas da imprensa observaram que isso marcou a primeira vez que as fontes do WikiLeaks consistiam em arquivos a partir de dados hackeados pelo

Anonymous. Até então, dificilmente alguém fora da comunidade de hackers do LulzSec, do WikiLeaks e do FBI soubera que Assange estivera negociando com Sabu e outros hackers do Anon desde junho de 2011. Tal situação, é óbvio, não significava que existia uma parceria sólida. Duas fontes distintas do meio hacker informaram que, por um longo tempo, Assange não confiou em Sabu. O motivo exato não está claro, mas Assange não seria o único a perceber que havia algo estranho.

– Uma coisa me surpreendeu mesmo após a volta dele – disse outro hacker, referindo-se a quando Sabu voltou ao LulzSec após sumir por vinte e quatro horas (ocasião em que sofreu a investida secreta do FBI em junho de 2011). – De repente começou a falar sobre a família. Mencionou num bate-papo privado comigo que tinha duas filhas.

Esse comportamento era profundamente inquietante. Apesar da regra velada no Anonymous de nunca falar sobre a vida pessoal, Sabu súbito dizia coisas como: – Minha família é a coisa mais importante.

Antes disso, nunca havia mencionado as duas filhas. Outra esquisitice: quando membros do Anonymous eram interrogados pela polícia e depois voltavam a ficar on-line, comentavam com outros hackers que estranhavam o fato de as autoridades nunca lhes fazer perguntas sobre Sabu.

Sabu mostrava-se inabalável ao negar aos hackers e nas entrevistas que ele era “Hector Monsegur”, utilizando a implausibilidade da situação a seu favor e tweetando em 26 de junho de 2011: – Quantos de vocês realmente embarcaram naquelas informações furadas sobre identidade? Haha. Pra começo de conversa, o nome “hector monsegur” é postado todos os dias, há seis meses.

Em particular, ele repetiu esse argumento a outros.

No entanto, de modo surpreendente, Sabu admitiu a seus mais íntimos amigos hackers que os diversos atos para doxeá--lo – e outras pessoas além de Emick vieram à tona com Hector Monsegur – estavam corretos. Isso, novamente, era bizarro, mas muitos supunham tratar-se do costumeiro niilismo de Sabu, o sujeito cujo ditado predileto era: “Já passei do ponto do não retorno.”

Sabu parecia degustar a confusão em que se metia e, a certa altura, o pessoal imaginava, ele acabaria atrás das grades.

No fim de novembro de 2011 e depois novamente em janeiro de 2012, um hacker confrontou Sabu quanto a não hackear quaisquer alvos por conta própria.

– Cara, suje as mãos pelo menos uma vez – falou o hacker em tom exasperado, acrescentando que ser esse o único modo de provar aos outros que ele não era um delator.

Sabu respondeu com histrionismo, alegando que já fizera muito pela causa, depois emendando que "gente que me odeia" queria caçá-lo a qualquer custo. Enquanto Sabu vociferava, o hacker digitou um emoticon para demonstrar tédio, -.-, e voltou ao trabalho.

Apesar de suas suspeitas, a maioria dos colaboradores de Sabu nunca realmente acreditou que esse veterano hacktivista revolucionário, tão apaixonado pela causa, pudesse realmente ter se transformado num delator.

– Ideia tão horrível. E a gente não sabia em quem confiar para tocar no assunto – contou o mesmo hacker.

Sabu tinha um domínio psicológico tão forte sobre sua equipe que os componentes na verdade temiam ficar perguntando por aí sobre as intenções verdadeiras do rapaz, com medo de que o vulto volátil subitamente caísse em cima deles.

Em sua atuação como informante, Sabu mentia não apenas aos hackers, mas também aos jornalistas. Junto com seus supervisores do FBI, ele mentia aos repórteres que desejavam uma entrevista on-line, os quais, às vezes acabavam falando com agentes federais, outras vezes com Sabu, mas acompanhado pelos agentes. No fim das contas, não passava de outra campanha de desinformação.

Ao longo de seu ano volátil com o Anonymous, Sabu tinha provado ser um mestre da mentira. Mas uma coisa ele parecia incapaz de inventar: seu nome. A certa altura em 2011, antes de ser preso pelo FBI, Hector Monsegur abandonou o nickname Sabu e tentou utilizar o novo nickname Kage ou Kaz em canais de IRC privados. O objetivo era virar a página, incinerar o velho nome Sabu e evitar ser preso e doxeado. Se ele tivesse mantido os novos nomes, talvez nunca fosse capturado pelo FBI e ainda hoje morasse com as duas filhas no apartamento de Lower East Side, assistindo a vídeos do YouTube e pagando as contas com números de cartão de crédito roubados. Mas Monsegur não conseguiu lidar com a nova identidade on-line. Após algumas semanas, retomou

o apelido Sabu.

Esse era o dilema dos hackers no Anonymous. Havia problemas de ordem prática quando alguém bem conectado nos porões hackers, como Sabu, adotava um nome novo. Ele perdia seus contatos e a confiança conquistada. Sabu trouxera dúzias de contatos úteis de sua época underground para trabalhar com o LulzSec, o Anonymous e o Antisec.

Hector Monsegur nunca seria capaz de orquestrar toda essa colaboração sem o nome Sabu. No fim, o ego e a ânsia por controle falaram mais alto.

No começo de 2012, os administradores do FBI começaram a discutir sobre a hora certa de revelar que Sabu atuava como informante. Até então, ele havia auxiliado a consertar várias vulnerabilidades em redes alvejadas e a identificar Jeremy Hammond, além de haver e ajudado a indiciar Donncha “Palladium” O’Cearrbhail, da Irlanda. No começo de janeiro de 2012, O’Cearrbhail (nome gaélico que se pronuncia “Carol”) tinha hackeado a conta Gmail de um membro da polícia nacional irlandesa, agente que rotineiramente enviava e-mails de sua conta oficial na polícia para sua conta Gmail. Um dos e-mails continha dados de uma chamada em conferência marcada para 17 de janeiro, entre agentes do FBI e a Polícia Metropolitana da Grã-Bretanha, para discutir a investigação do LulzSec e do Anonymous. Palladium rapidamente avisou Sabu de que ele ia escutar a conversa e gravá-la.

– Fico contente em vazar a ligação apenas para você – disse empolgado.

– Vai ser épico!

Após gravar a ligação de dezoito minutos, Palladium passou o arquivo de áudio para Sabu, que então o repassou ao FBI para corroborar a veracidade. Confirmou-se. Quando Sabu não publicou o arquivo on-line, alguém mais o colocou no YouTube, para o deleite da comunidade Anon e o constrangimento do FBI. Nos bastidores, o FBI atuava para identificar Palladium (graças a uma ordem de busca obtida numa conta do Facebook de um de seus amigos) e montava uma acusação significativa contra o hacker (graças aos registros de bate-papo com Sabu). Sabu havia auxiliado a reunir provas contra cinco pessoas: Topiary, Kayla, Tflow, Sup_g (Jeremy Hammond) e Palladium.

No começo de 2012, a polícia nos dois lados do Atlântico se preparava para apresentar acusações contra os cinco Anons. O momento de expor Sabu se

aproximava, mas escolher uma data não era fácil.

– Existiam problemas constantes de relacionamento entre as autoridades britânicas e o FBI – comentou uma pessoa envolvida na investigação do FBI sobre o LulzSec e o Anonymous.

Embora Sabu morasse em Nova York, pelo menos quatro hackers do LulzSec moravam nas ilhas Britânicas, ou seja, a Polícia Metropolitana britânica estava mais ansiosa que os colegas dos EUA para acionar o gatilho contra os hackers. Enquanto a polícia dos EUA contava com um informante de peso que podia ajudá-los a agarrar mais hackers à solta, os britânicos tinham quatro hackers na mira e estavam prontos para enviá-los aos tribunais.

O FBI queria capitalizar o máximo possível o seu delator de Lower East Side. Ele havia auxiliado a remendar aquelas falhas de segurança, e o anúncio de sua prisão e a revelação de sua duplicidade devastariam as ideias socialmente perturbadoras do Anonymous e do Antisec. Mas os Feds não podiam ter certeza do quanto Hector Monsegur continuaria a ser útil.

Embora fosse esperto e tivesse boas conexões, ele também era uma metralhadora giratória. Certa noite, no começo de fevereiro, um guarda do NYPD encontrou Hector em outro apartamento da vizinhança. Ele pediu sua identidade.

– Meu nome é Boo. O pessoal me chama de Boo – respondeu Hector. – Relaxe. Sou agente federal. Sou agente do governo federal.

Parecia que Hector havia começado a acreditar que tinha dupla personalidade: Sabu e um confiável agente do FBI. Naquela mesma noite, ele foi acusado de personificação criminosa.

Igualmente complicado: durante o monitoramento de Sabu, os Feds obtinham uma percepção do quão rápido as coisas se moviam nos mundos do Anonymous e do Antisec. Sabu via dezenas de ideias para ataques surgirem todos os dias, e enquanto algumas eram descartadas, outras eram seguidas com rapidez superior à que a burocracia do FBI podia acompanhar. Os hackers se vangloriando no Twitter, o drama da internet, lulz – tudo isso era território novo para o FBI.

Quando a Polícia Metropolitana de Londres contou ao FBI que tinha a data limite de 7 de março para prender e publicamente apresentar acusações contra a pessoa que alegava ser Kayla, data que não podia ser postergada, os Feds

também concordaram em expor Hector pouco antes desse dia. Tudo viria à tona ao mesmo tempo: as identidades não confirmadas de Kayla, Pwnsauce, Palladium e o hacker da Stratfor Sup_g, e a notícia de que Sabu estivera trabalhando com o FBI durante o extraordinário tempo de oito meses. Era uma bomba, e a polícia estava prestes a largá-la diretamente no Anonymous.

CAPÍTULO 27

A verdadeira Kayla,

os verdadeiros Anonymous

Sete meses antes, em 2 de setembro de 2011, a polícia britânica tinha estacionado diante de uma residência familiar no pacato subúrbio inglês de Mexborough, South Yorkshire. Na manhã fria e cinzenta, um dos policiais carregava um laptop aberto e controlava a conta @lolspoon no Twitter, esperando que a hacker conhecida como “Kayla” postasse um novo tweet.

Quando ela o fez, vários outros agentes se precipitaram casa adentro por uma entrada dos fundos, subiram as escadas até o quarto de Ryan Mark Ackroyd, entraram e o prenderam. Ackroyd, 25 anos, tinha servido no exército britânico durante quatro anos, parte desse tempo no Iraque.

Agora, desempregado, morava com os pais. Baixinho, olhos encovados, cabelo escuro com corte militar, ao abrir a boca, falou em voz grave de barítono e acentuado sotaque do norte da Inglaterra. A irmã mais nova de Ackroyd, pequenina e loira, chamava-se, talvez de modo revelador, Kayleigh.

Da mesma forma como a polícia havia interrogado simultaneamente o irmão de Jake Davis, os inspetores também sincronizaram a prisão de Ackroyd com a de seu irmão mais jovem, Kieron, que servia no exército em Warminster, Inglaterra. Após interrogar Kieron, a polícia o soltou sem indiciá-lo. Kieron e Kayleigh Ackroyd pareciam irmãos chegados, com Kayleigh habitualmente postando no mural do Facebook do irmão mais novo, incentivando-o em uma das mensagens a ir bem num iminente teste de direção.

– Você vai pegar o jeito – ela comentou em janeiro de 2011.

Mas o irmão mais velho dos dois, Ryan, nunca aparecia em suas conversas públicas.

– Ele é o arquetípico infante inglês – sentenciou uma pessoa que conhecia Ackroyd. – Fica em posição de sentido e, se o mandarem pular, pergunta qual a altura... Esse tipo de personalidade. De duas, uma: ou ele é esperto ao extremo para ter tramado isso ou genuinamente não se trata dele.

– Ela é um soldado no Reino Unido – Sabu informou em voz baixa durante uma entrevista telefônica em 5 de novembro, ao ser indagado sobre quem ele pensava

que Kayla era. – É um cara. – Em seguida, mostrava-se incerto, dizendo que tinha ouvido falar que era alguém que compartilhava a identidade “Kayla” com um grupo de hackers transgênero.

– Não sei que confusão é esta. São todos travestis estranhos e coisa parecida. É de foder o cérebro da gente.

Seja como for, naquela manhã gelada em setembro de 2011, a então prolífica conta de Kayla no Twitter, @lolspoon, emudeceu. (Ficou inativa desde então.) Em seguida, em março de 2012, enquanto o FBI se preparava para vir a público com a verdade sobre Sabu, as autoridades britânicas obtiveram o ok para indiciar Ryan Ackroyd com duas acusações de conspiração para hackear uma rede de computadores.

Em 6 de março de 2012, a Fox News, alvo de múltiplas provocações do Anonymous e do LulzSec e de pelo menos uma hackeagem em 2011, anunciou ao mundo que Sabu, o “hacker mais procurado do mundo”, era um informante do FBI. A manchete: “EXCLUSIVO: Infame grupo hacker internacional desmantelado pelo próprio líder”.

A Fox trabalhava na reportagem há meses e baseou a maior parte de suas informações em agentes do FBI e em hackers que conheciam Sabu. O

artigo revelava a identidade de Sabu como Hector Monsegur e relatava que a polícia ia prender e acusar cinco outros homens, principalmente com base nas provas fornecidas por Hector “Sabu” Monsegur.

– Isso é devastador para a organização – declarou um agente do FBI, de acordo com o artigo. – Estamos decapitando o LulzSec.

Todos os principais órgãos de comunicação veicularam a notícia, a maioria deles se baseando na reportagem da Fox. Jornalistas rumaram ao conjunto habitacional Jacob Riis, tirando fotografias da porta do apartamento de Sabu, batendo, mas sem ninguém atender. Outros ouviram a opinião dos vizinhos, que apresentaram diferentes relatos sobre Hector Monsegur. Calado, mas cordial, disseram eles. Sempre sorria quando cruzava com alguém no corredor. Uma vizinha de mais idade que morava embaixo confirmou que havia se queixado ao conselho comunitário de Manhattan sobre os ruídos de “crianças gritando, cães latindo, berros e pancadas” que vinham do apartamento dele, em geral durando até as quatro da madrugada.

As revelações sobre a delação deixaram atônitos milhares de pessoas que seguiam ou apoiavam o Anonymous. Algumas das contas mais populares da organização no Twitter simplesmente tweetaram a notícia, incapazes de fornecer qualquer comentário. Um tweet sugeriu que as prisões eram como cortar a cabeça de uma hidra: elas cresceriam novamente. O Anonymous, a comparação insinuava, daria a volta por cima.

Jennifer Emick teve um dia de glória, salientando pelo Twitter que o Anonymous agora estava definitivamente acabado.

Gabriella Coleman, titular da cátedra Wolfe na Faculdade Científica e Tecnológica da Universidade de McGill, em Montreal, foi uma das raras pessoas que conheceram Sabu pessoalmente enquanto o rapaz morava em Nova York. Ele não era tão diferente de sua persona on-line, recorda.

Embora tenha estudado o Anonymous durante anos, Coleman ficou chocada. Ela havia suspeitado de que Sabu tramava algo (por que outro motivo concordaria em encontrá-la?), mas no dia que a notícia estourou, ela alegou que "era bem diferente passar pela experiência e saber". Pouco antes de ser exposto, Sabu obtivera permissão para avisar familiares e amigos sobre o que estava prestes a acontecer. Coleman foi uma das pessoas a quem ele ligou. Ao recapitular aquela última conversa, Coleman a descreveu como "parte desculpas, parte 'não é bem o que parece'".

Quando pessoas importantes no Anonymous e no Antisec ficaram sabendo da notícia, demonstraram surpresa quanto à extensão da cooperação de Sabu. Mas também houve igual surpresa sobre tudo que o FBI estivera a par durante seus ataques contra a Stratfor, a chamada em conferência do FBI interceptada e outros ataques.

– Se eu fosse da Stratfor, estaria indignado com o FBI – comentou um hacker. – Basicamente sacrificaram a Stratfor para prender um sujeito [Jeremy Hammond]. Que droga, cara... Que tipo de investigação é essa?

Outros hackers que tinham colaborado com Sabu agora "surtavam", e muitos diziam que sairiam de cena por um tempo.

– Eu sabia que havia algo desonesto no ar – frisou Jake Davis pouco depois de ser informado sobre a grandeza da traição de Sabu contra as pessoas com quem ele tinha iniciado o LulzSec. Como de costume, Jake se mostrava frio diante das

notícias. Não parecia zangado com Sabu, talvez porque já cultivara uma mágoa em relação ao ex-amigo que o induzira a abraçar a causa Antisec. O que mais chocou Jake foi o quanto o FBI aparentemente desenvolvera sua investigação monitorando os ataques cibernéticos em tempo real.

– Não imaginava que o FBI fosse tão doido assim.

***

Agora ficou claro: Sabu, Topiary, Kayla, Tflow e Pwnsauce, cinco membros do sexteto nuclear do LulzSec (não se sabe o que aconteceu com AVunit), tinham sido presos. Parecia quase impossível tornar-se um herói no Anonymous e evitar as algemas. Mas isso significava o fim do Anonymous? O derradeiro tweet de Jake como Topiary fora: – Você não consegue prender uma ideia.

A frase soava verdadeira. No Anonymous, não existiam líderes, mas símbolos e pequenos grupos que ocasionalmente trabalhavam juntos.

Havia até culturas diferentes: a velha escola de hackers da EFnet, como Sabu, que abraçara a visão do Antisec; os usuários do 4chan como William, que adoravam o Anon porque os ajudavam a “desperdiçar uma noite”. E

havia aqueles que se situavam no meio-termo, como Topiary, Kayla e Tflow, enxergando o Anonymous como um meio amplo de encontrar plenitude, ter novas experiências e fazer diferença no mundo, tudo isso mesclado ao prazer que sentiam com computadores e internet. Era impossível atar o Anonymous num só aglomerado e destruí-lo.

Esse fenômeno surgiu do mundo nascente dos memes, da participação coletiva e das redes sociais, coisas com um potencial de viralizar impossível de ser previsto, controlado ou interrompido. Enquanto alguns membros eram presos, outros entravam. O FBI afirmou que estava “decapitando o LulzSec”, mas, em março de 2012, após o LulzSec ter se dispersado há mais de nove meses, outras células hackers assumiam a causa Antisec; só em fevereiro de 2012, sectários do Anonymous assumiram o crédito por atacar os sites da CIA, da Interpol, do Citigroup e de uma série de bancos no Brasil, entre outros alvos.

Em seguida, aconteceu o crescente movimento internacional chamado “Occupy”, que emergiu em setembro de 2011 e presenciou dezenas de milhares tomarem as ruas nas principais capitais para protestar contra a desigualdade

socioeconômica, muitas vezes utilizando o slogan “Somos os 99%”. Sectários do Anonymous com estilo ativista mostravam amplamente seu apoio ao Occupy, promovendo-o no Twitter ou em blogs e usando as máscaras de *V de vingança* nos protestos. A polícia prendera mais de 6800

pessoas relacionadas ao Occupy por volta de abril de 2012, ocasião em que o movimento entrou em hiato. Mas, enquanto observadores se maravilhavam com o quanto essa multidão global aparentemente sem líder conseguia se organizar de modo tão amplo on-line e em manifestações presenciais, eles precisariam apenas observar o Anonymous para notar que o mesmo já havia sido feito antes.

Para o FBI, contar com Sabu como informante representara uma boa cartada, mas perseguir o excesso cotidiano de bravatas, discussões secretas, conspirações e ameaças provavelmente logo deve ter se tornado um pesadelo burocrático. Embora tenham feito Sabu trabalhar para eles durante oito meses, não está clara a dimensão instrumental da atuação dele na identificação preliminar de qualquer um dos cinco hackers acusados em 6 de março – no máximo ele deve ter ajudado a corroborar as acusações.

Sabu foi exposto, mas o Anonymous parecia se recusar a ser destruído.

Mais tarde, naquela tarde de 6 de março, um grupo de hackers anunciou que o Anonymous havia hackeado e desfigurado o site da Panda Securities, a mesma empresa de TI que observara os ataques de DDoS do Anonymous contra o PayPal em dezembro de 2010. A mensagem dos hackers: não acabou.

Então, ao longo dos dias seguintes, os hackers que tinham trabalhado com Sabu fizeram um brainstorm sobre novas maneiras de cooperação mútua.

– Depois da merda que o Sabu fez, as coisas ficaram diferentes – salientou um deles. – Agora desconfiamos bem mais.

Em meados de março, os hackers discutiam outros métodos de conversar entre si além do IRC e como eles poderiam elevar o padrão para aceitar novos participantes das discussões privadas. Como movimento ativista, o Anonymous permaneceria público, mas as atividades de hackeagem se tornariam bem mais subterrâneas. A organização emergira das sombras, acrescentou o hacker, e voltaria à escuridão por um tempo.

– Mas não se preocupe. Existimos.

O Anonymous já promovera mudanças. Por exemplo, as ferramentas de software utilizadas por seus sectários tornavam--se cada vez mais fáceis de disseminar. Quando, em janeiro de 2012, membros do Anonymous desferiram ataques de DDoS contra diversas empresas em protesto pelo cancelamento do Megaupload, um site de videotransmissão, eles não utilizaram o programa de LOIC tradicional. Não havia necessidade de baixar nada. A essa altura, os sectários podiam disparar um LOIC

diretamente de um navegador de web. Isso significava que, ao postar um link pelo Twitter ou Facebook, os organizadores ludibriavam centenas, talvez milhares de surfadores da web a participarem, sem se dar conta, do ataque. O método de ataque, apelidado de LOIC móvel pela empresa de segurança digital Imperva, foi utilizado já a partir de agosto de 2011 no primeiro de vários ataques de DDoS contra o Vaticano e se tornou muito popular ao longo dos meses seguintes.

No começo de 2012, os ataques do Anonymous já não eram mais executados por milhares de voluntários, como nos ataques da Operação Vingança em solidariedade ao WikiLeaks. Exatamente como nos protestos do mundo real feitos no Projeto Chanology, eles eram utilizados uma só vez, como se o Anonymous estivesse aprendendo o que funcionava e o que não funcionava. A organização migrava de ajuntamentos em massa e ataques de DDoS para grupinhos roubando dados, como o LulzSec. Para isso, crescia o uso da ferramenta da web Havij. Após o LulzSec utilizá-la para colar dados durante a investida contra a PBS, um grupo dissidente chamado CabinCr3w lançou mão da Havij (ou coisa parecida) para expor dados pessoais de quinhentos policiais em Utah, enquanto outros Anons usaram a mesma ferramenta para tentar roubar dados do Vaticano em agosto de 2011. Os estudos da Imperva mostraram que, apenas um ano após a sua criação (segundo se acredita, por programadores iranianos), a Havij se tornara, no primeiro semestre de 2012, uma das ferramentas mais populares para ataques de injeção de SQL. O programa era tão simples que um executivo da Imperva ensinou em quinze minutos seu filho de onze anos a utilizá-la. A ferramenta com download grátis executava SQLi automaticamente, até mesmo filtrando dados em categorias úteis como “Senhas” e “Números de cartões de crédito”. Com os programas certos e gratuitos e uns poucos cliques, parecia que qualquer um podia se tornar hacker.

Claro, manter acesa a ideia do Anonymous seria complicado. A mídia, a polícia e até mesmo os próprios hackers tinham seus próprios conceitos do que

realmente era o Anonymous: uma ideia, um movimento, uma organização criminal e outras coisas mais. Por volta de março de 2012, o público e uma parcela da mídia ainda pareciam pensar que o Anonymous consistia em um grupo muito grande que fazia planos e os executava de modo organizado. Embora essa noção estivesse profundamente equivocada, era compreensível. Um fenômeno de última geração como o Anonymous, nascido da própria internet, inicialmente exigia esforço da sociedade para entendê-lo. Como se isso não bastasse, o mistério cercando o que realmente acontecia no interior da mente colmeia havia deixado o espaço exato para permitir que o público criasse suas próprias versões sobre a narrativa do Anonymous, exatamente como quando Topiary espalhara uma vaga história acerca de ter sido alvo de uma batida policial, na ocasião em que ele desejava sair do AnonOps. O Anonymous não consistia apenas em um grupo ou um processo; também consistia em uma história que as pessoas contavam a si mesmas sobre como a internet estava reagindo. Os Anons ganhavam manchetes simplesmente tweetando ameaças, motivo pelo qual o poder do Anonymous remete ao poder mítico.

O Anonymous representava outro exemplo de engenharia social, mas em grande escala. Não muito diferente da própria Kayla.

Ao longo dos últimos anos, a entidade on-line Kayla estivera contando a seus amigos histórias diferentes sobre quem ela era na vida real, incitando-os a tentar montar o quebra-cabeça de sua identidade verdadeira. Uma adolescente que odiava o pai; uma adolescente que o amava. No fim das contas, porém, seus colegas hackers pararam de se interessar pela verdade.

– Dissemos que preferíamos que ela nos mentisse – lembra--se um amigo de longa data. – Todos nós amávamos a história. Acho que não nos importávamos se era verdade ou não.

Como crianças querendo manter viva a mágica do Papai Noel um pouco mais de tempo após começar a duvidar de sua existência, para seus amigos hackers, o mito de Kayla havia se tornado mais importante do que a verdade em si.

Isso remetia à luta constante no seio do Anonymous: equilibrar o seu inerente etos de anonimato e mentiras com a necessidade de confiança e verdade. Os Anons comentam o quanto mentiras persistentes os alienam da realidade e “deformam” sua ética. Quando alguém mente a toda hora às outras pessoas, fica difícil se lembrar do que, em última análise, está tentando alcançar. Até mesmo

Sabu começou a acreditar nas próprias mentiras ao alegar abertamente para a polícia que ele era um agente federal.

Durante a Operação Vingança, milhares de novos voluntários tinham confiado nas afirmações dos operadores do AnonOps de que utilizar o LOIC

não levaria a prisões. Foi um ato de ingenuidade dos voluntários, mas também houve manipulação em ação, ou pelo menos uma grande divisão de motivos. Os operadores no #command tinham silenciosamente se interessado pela ideia de vingar o WikiLeaks, porque isso traria publicidade para sua nova rede de bate-papo. Ansiavam pela fama de receber milhares de pessoas visitando seus canais e seguindo suas ordens.

Então os botmasters atacaram o PayPal, a MasterCard e a Visa para mostrar seu poder. Os milhares de voluntários estavam alheios a isso, acreditando que faziam parte de uma pacífica manifestação digital, por uma causa com que eles se importavam. De modo semelhante, em 2008 Gregg Housh e sua equipe do #marblecake pensaram que estavam encabeçando o maior trote da história, mas o Chanology se transformou em ativismo sério. Em múltiplas maneiras, o Anonymous se revelava uma espécie de fraude – as pessoas se atraíam pela camaradagem, pelo aprendizado e pelas novas experiências, mas se afastavam desiludidas pela desorganização, pelos egos inflados e pela grave ameaça de ser preso. Mas o Anonymous também era algo mais: um portal ao ativismo político, um estranho, mas inebriante elixir contra a apatia da juventude na atual sociedade de tempo real.

O Anonymous teria de lidar com essas questões ao longo do tempo.

Nenhuma pessoa isoladamente tomaria uma decisão final sobre como esse processo evoluiria; seria um esforço coletivo. As pessoas dessa atual geração do Anonymous abandonariam o grupo, cansadas do drama de Sabu. Mas inúmeros novatos tomariam seus lugares e fariam mudanças. E

alguns poucos, inclusive hackers que participaram do #InternetFeds e até mesmo do Chanology, permaneceriam. Na verdade, alguns permanecem até hoje.

– Ainda não pegaram Kayla – falou Emick em 6 de março, o dia em que Sabu foi exposto. – É um garoto de dezoito anos na Califórnia.

Ela riu e depois voltou a ficar on-line. Emick ainda dava andamento a suas

investigações, tentando rastrear a identidade verdadeira de Kayla.

Não tinha dúvidas de que era um nome composto utilizado por mais de uma pessoa e de que, embora Ryan Ackroyd fosse indiciado por alguns dos seus crimes, outros continuavam à solta. Se o Anonymous podia compartilhar uma identidade coletiva, por que não Kayla?

Quanto a Jake, a proibição de utilizar a internet lhe deu uma oportunidade para refletir sobre a própria web, uma nova entidade que se tornou parte integral da vida de todo mundo. Em fevereiro de 2012, ele mandou um pen-drive pelo correio, e nele havia essa curta carta, apresentando sua percepção de como a internet nos enxerga: **Olá, amigo, e bem-vindo à internet, a luz guia e o laser letal de nosso mundo agitado e moderno. Já faz um tempinho que a horda da internet tem o observado de perto.**

Ao longo dos anos, ela presenciou você entrar no Facebook e no Twitter, ela o observou penetrar na casa dela e tentar ultrapassá-la com seus escândalos e fofocas do "mundo real". Saiba que o domínio do ciberespaço sempre pertencerá à mente colmeia. A internet não pertence a suas amadas autoridades, forças armadas ou pessoas donas de empresas multimilionárias. A internet pertence aos trolls e aos hackers, os entusiastas e extremistas; jamais deixará de ser assim.

Sabe, a internet há muito tempo perdeu seu lugar no tempo, e sua coletividade obscura continua a se esquivar do fato de que vive num ano específico como 2012, e precisa seguir os princípios morais de 2012 e a sociedade de 2012, com suas regras e punições. A internet dá risada de cenas de estupro em massa e carnificinas horripilantes com um toque de canibalismo, tudo ao som da envolvente batida de música japonesa. Simplesmente não dá a mínima para conseguir um "emprego", conseguir um carro, conseguir uma casa, criar uma família e ensiná-los a continuar o círculo enquanto a espécie humana organiza a própria morte. Caixões com placas personalizadas e planos de aposentadoria feitos de burocracia... a internet se pergunta: por quê?

Você não consegue fazer a internet se sentir mal, não consegue fazer a internet se arrepender nem sentir culpa ou compaixão; apenas consegue fazer a internet sentir a necessidade de obter mais lulz à sua custa. Lulz flui por tudo enquanto o exército sem rosto assiste à queda das torres gêmeas

com um Hitler dançando no canto esquerdo inferior da tela. Lulz ataca quando eles abrem um jornal e não se importam com nenhum dos supostos problemas mundiais. Caem na risada ao deparar com setas vermelhas que apontam a queda de bancos e empresas; caem na risada ao deparar com nossos gloriosos soberanos do governo tentando consertar uma situação injetando mais dinheiro na economia. Caem na risada quando você tenta fazê-los sentir a necessidade de "fazer algo da vida" e morrem de rir quando você os chama de trolls repugnantes e terroristas cibernéticos desalmados. Caem na risada porque você é incapaz de rir de si mesmo e de todas as inúteis quinquilharias que o cercam. Mas, acima de tudo, eles caem na risada porque podem fazê-lo.

Isso não quer dizer que a internet é sua inimiga. É sua principal aliada e sua amiga mais íntima; suas compras significam que você não precisa pôr o pé fora de casa, e seus cassinos lhe permitem perder o seu dinheiro a qualquer hora do dia. Suas muitas salas de bate-papo lhe garantem: não é mais necessária interação direta com nenhum outro membro de nossa espécie, e uma rede social detalhada mapeia cada um de seus passos e pensamentos. Seus relacionamentos íntimos e mais obscuros segredos pertencem à horda, e jamais serão esquecidos. Sua existência será eternamente codificada no infinito repertório de belas sequências de bytes, armazenadas de modo seguro na nuvem cibernética para todos observarem.

E como a internet mudou a vida de seus usuários mais viciados? Simplesmente não se importam o suficiente para lhe contar. Então bem-vindo ao baixo-ventre da sociedade, à anárquica nebulosa em fluxo de consciência que, cada vez mais, dia após dia, se insinua no mundo não alternativo – o seu mundo. Você não pode escapar dela e não pode antecipá-la. É o pesadelo no limiar de seus sonhos e o nefasto pensamento que crava as garras em sua vida on-line como ofuscante força virtual, desconsiderando suas filosofias e se esbaldando com suas emoções.

Prepare-se para entrar na mente colmeia, seu filho da mãe.

Desde 2008, o Anonymous destruíra servidores, roubara e-mails e derrubara sites do ar. Mas, no ato coletivo de engenharia social, sua maior façanha foi convencer as pessoas a acreditarem no poder de sua "mente colmeia". Foi isso que atraiu os sectários, que causou suas prisões e que serviu de inspiração para outros vingarem suas prisões. O Anonymous foi como uma nova geração de

indivíduos habilidosos em tecnologia conseguiu mostrar ao mundo que tinha uma voz e que podia fazer a diferença.

Como eles agirão na sequência ainda terá de ser escrito. Esses pequenos grupos de jovens do mundo todo, geralmente do sexo masculino, geralmente pobres e desempregados, que na maior parte do tempo apenas trocam ideias nas salas de bate--papo da internet, enfim conseguiram atrair a consciência pública. Eles ainda a mantêm e não pretendem largá-la.

EPÍLOGO

Um ano depois

Sentado de cócoras na relva verde da praça de Peterborough, cidade inglesa de porte médio, Jake Davis respira o ar quente do verão.

Embora seja o meio de uma semana de trabalho em agosto de 2012, dezenas de homens, mulheres e crianças caminham por ali carregando sacolas de compras e empurrando carrinhos de bebê, curtindo o sol que ficou ausente dos céus locais durante a maior parte do verão.

Já faz mais de um ano que policiais londrinos à paisana bateram à porta do chalé de madeira de Jake nas uivantes ilhas Shetland, conduziram-no a um avião e depois o trancafiaram numa cela. Desde então, quase todo o tempo ele utilizou uma tornozeleira eletrônica, confinando-o à casa de tijolo à vista onde ele hoje mora com a mãe e o irmão, das sete da manhã até as dez horas da noite, todos os dias.

Em abril de 2012, Jake praticamente limpou a conta no banco para, pela primeira vez na vida, comprar terno e gravata. Vestiu o traje em 11 de maio e respondeu às acusações criminais contra si. Três outros jovens ficaram em pé ao seu lado: Ryan Cleary, Ryan Ackroyd e um menor suspeito de ser Tflow. A cada qual foi imputado certo grau de culpabilidade no indiciamento formal com oito acusações. Cleary foi indiciado nas oito acusações; Acroyd, o menor de idade e Jake Davis, em quatro.

Ackroyd, com calça jeans e suéter bege que tapava as tatuagens escuras ao redor do braço, negou todas as acusações de crimes cibernéticos cometidos sob o apelido de Kayla.

– Inocente – alegou com forte sotaque anglo-nortista, cerrando o punho e a cada palavra soqueando o ar para baixo, como para fortalecer suas próprias convicções.

Jake se declarou culpado das duas acusações mais graves envolvendo conspiração para atacar as instituições da News International, HBGary Federal e o Departamento de Polícia do Arizona, mas alegou inocência da acusação da tentativa de obter vantagens financeiras por meios fraudulentos durante a sua participação no LulzSec. Cleary declarou-se culpado em seis das oito acusações,

e o menor de idade, inocente de todas as quatro acusações.

Cerca de trinta minutos depois, os quatro jovens silenciosamente saíram em fila indiana; três deles de volta para casa. Ryan Cleary foi conduzido de volta à cadeia, após ter descumprido suas condições de fiança no começo do ano. Os quatro estão com julgamento marcado para 8 de abril de 2013, e há a possibilidade de que Hector "Sabu" Monsegur voe ao Reino Unido para depor contra eles. O julgamento pode durar oito semanas.

Reconhecer a culpa eliminou um pouco do peso da cabeça de Jake. Ele podia conversar sobre o LulzSec com relativa de liberdade; podia ir atrás de oportunidades de emprego. Mas o maior contentamento veio de outra coisa: estar off-line.

– Progredi muito ao me afastar de toda aquela "máquina de ódio da internet". De toda aquela máquina de trollagem. Estou mais feliz e mais realizado – afirma, ainda sentado na relva, os tornozelos cruzados e os joelhos afastados. – Eu aprecio o ar livre. Não que eu pensasse que não ia gostar, mas não é tão ruim.

– É outro mundo agora, preenchido de silêncio. Minha cabeça está bem mais clara.

Antes ele transitava em meio a cinquenta canais de IRC, textos instantâneos, cliques constantes, zunidos cerebrais, sempre no limite.

Agora os pensamentos frenéticos e paranoicos se esvaíram. Ele admira ver o quanto tudo é devagar, como aquele pombo caminhando em sua frente.

Jake sentira a vida sendo sugada de si quando estava nas ilhas Shetland.

O problema não era o arquipélago em si. Era o isolamento e o enfado em que ele se viu preso, atiçando a displicência e o desrespeito pelas consequências do que praticava on-line. Ele fora feliz como Topiary.

– Mas isso não significa que eu era feliz na vida real. Eu estava inerte.

É estranho ouvir Jake mencionar tais palavras, já que seu cérebro fervilhara num turbilhão de atividade frenética na primeira metade de 2011. Em comparação, agora sua vida parecia amordaçada: nada de emails, nada de smartphones, nada de Twitter, nada de YouTube, nada de bate-papo on-line, nada de aprendizado

instantâneo. Esse último era um dos mais difíceis de tolerar.

No entanto, por “inerte” Jake se refere aos costumeiros altos e baixos da vida. Os fatos agora parecem mais potentes sem o mundo on-line onde se refugiar depois, fatos importantes como comparecer perante o tribunal, morar com a família outra vez e viver sob o fantasma de uma sentença de prisão.

Um tanto desconcertante é o fato de que Jake pode pegar anos de cadeia por coisas que ele falou em salas de bate-papo, atmosfera etérea e livre de fricção em que pensamentos se traduzem instantaneamente em textos.

Muito do que ele disse no Twitter e nos canais de IRC na pele de Topiary agora tinha sido impresso e se convertido em milhares de páginas que a polícia utilizava como provas.

A principal prova contra ele se relaciona a uma acusação de conspiração – a conspiração para atacar o site da Agência Britânica contra o Crime Organizado Grave, SOCA – e inclui o registro da conversa entre ele e Ryan Cleary, com Topiary dizendo que o outro pode ir em frente e desferir um ataque de DDoS contra o site. Ele digitara algo parecido com *Soca works. Do whatever.*

Agora ele comenta: – E aquela decisão tomada numa fração de segundo vale uma acusação criminal inteira. É por isso que estou feliz por ficar longe da internet.

Porque um pensamento e um pouquinho de ação podem deixá-lo em maus lençóis. Botnets são tão fáceis. Tudo é tão fácil.

Pode ser que daqui a uma década ou mais as leis criminais estabeleçam um tipo de julgamento mais circunspecto sobre o comportamento das pessoas on-line, talvez mais leniente com as “conspirações” urdidas em salas de bate-papo por jovens que só querem se divertir e causar confusão.

Neste exato momento, é muito cedo para isso. Os juízes não são jovens; o de Jake tem cabelos brancos e usa óculos.

– Eles nos encaram falando numa bizarra retórica on-line e pensam que somos racistas imaturos, quando na verdade ninguém é – explica Jake olhando o gramado. – O IRC é apenas o lixo mental de cada internauta transferido constantemente via teclado para uma sala cheia de gente.

Jake tem bons motivos para se arrepender de coisas que ele “digitou em fluxo de pensamento” nas salas de bate-papo, agora que a polícia as havia imprimido em documentos que serviam como provas. Lendo seus posts no Twitter, ele não vê sentido naquilo.

– Todo mundo está disparando contra o outro em 140 caracteres. Não é uma conversa real. São disparates – analisa ele. – No fim você acaba retirado da internet, sentado à mesa e obrigado a ler uma folha de papel e [avisado] “Eis um dia de seu uso na internet”. Não consegue se imaginar fazendo ou falando aquelas coisas.

Ele se retrai ao mencionar a raiz de suas ambições.

– Eu tentava vestir essa máscara, a máscara do “Topiary” para ser aceito na cultura em voga. Mas era idiota e [sobre] tentar impressionar os outros, sei lá, nem imagino quem realmente se importava com o que ia acontecer comigo. Risadas fáceis. Nem consigo me identificar com essa pessoa, sabe? Eu não repetiria esse tipo de coisa agora.

O escárnio de Jake em relação a sua vida passada pode ter ecos das palavras de um advogado, mas parece ser autêntico. Ele prossegue sua análise e admite: seria muito fácil voltar a executar conspirações elaboradas e se meter em encrenca outra vez na internet.

– Talvez daqui a um ano – explica sobre a possibilidade de uma volta completa on-line. – Se eu continuasse agora, haveria uma chance remota de ter vontade de conversar de novo com as pessoas.

Com as pessoas erradas, ele quer dizer. E prossegue: – Eu acabaria trollando alguém... Entrando numa comunidade, ascendendo ao topo daquela comunidade e depois organizando as coisas e dizendo coisas idiotas para tentar impressionar as pessoas... E, com minha lábia insidiosa, penetraria em grupos estranhos. Posso ver isso acontecer com muita facilidade.

Nesse ínterim, nos Estados Unidos, Hector “Sabu” Monsegur manteve-se distante dos olhos públicos e, até onde a maioria sabe, deixou de frequentar os canais de IRC do Anonymous. Mas parece que ele tem permissão para entrar on-line e está enviando e-mails. Seus advogados alegam que, devido à sua substancial cooperação com o FBI, ele está qualificado a receber uma sentença inferior a dois anos. Um advogado envolvido no caso sugeriu que ele até poderia

escapar “sem cumprir pena alguma”. Quando este texto foi escrito, ele receberia a sentença em fevereiro de 2013, mas os promotores podiam postergar essa data, adiando-a para depois do depoimento de Sabu contra os demais.

Entre eles, Jeremy Hammond, o suposto líder da hackeagem da Stratfor que liderou o roubo de milhares de e-mails corporativos.

Também há Raynaldo “Royal” Rivera, administrador de TI texano cuja história nos remete à facilidade de fazer coisas estúpidas, até ilegais, on-line. Royal, jovem tranquilo – inteligente o bastante para frequentar cursos de faculdade durante o ensino médio –, saiu de casa para cursar a Universidade de Tecnologia Avançada no Arizona, no segundo semestre de 2010. Na ocasião, concluía os estudos na mesma e conceituada universidade um jovem de 24 anos, Cody Kretsinger. Amigo on-line de Sabu desde os dias do Antisec original, em 2000, Cody ainda falava com Sabu pelo telefone de vez em quando. Por volta de maio de 2011, Sabu convidou Cody para entrar na sala de bate-papo exclusiva do LulzSec, “pure-elite”.

Cody se inscreveu usando o nickname Recursion. Sabu então o convidou a encontrar mais jovens recrutas habilidosos, pessoas 100% confiáveis.

– [Sabu] queria começar a criar um grupo de elite capaz de fazer qualquer coisa – lembrou-se mais tarde Royal.

Cody pensou em dois amigos que compartilhavam seus interesses na época da faculdade, um colega chamado Chase Shultz e o companheiro de quarto de Chase, Royal. Na época, Royal tinha dezoito anos, e Chase, vinte.

Os dois ambicionavam conseguir empregos na National Security Administration (NSA) após a formatura. E ambos tinham qualificações para isso. Apesar da idade e do status de calouro, Royal já trabalhava como administrador de TI na instituição técnica.

Ao convidar os dois jovens a se encontrar com ele, Cody sugeriu que o acompanhassem para fumar um cigarro no lado de fora de um dos prédios da faculdade.

– Quero conversar com vocês sobre um assunto – anunciou.

Entre uma tragada e outra, Cody lhes contou seu envolvimento no LulzSec, o

grupo hacker que já atraía muita atenção da imprensa e que incluía os mesmos caras responsáveis pela histórica hackeagem da HBGary.

Ele também lhes oferecia a oportunidade de conversar em particular com Sabu e de participar de tudo. Os dois mostraram interesse.

Mais tarde, Royal e Chase se conectaram na internet e entraram numa sala de bate-papo privada com Sabu em pessoa. O jovem lhes contou que sua equipe podia aproveitar a perícia deles e também mencionou os benefícios de trabalhar com o LulzSec: o tipo de conhecimento que nunca iam aprender numa faculdade. Ele chamou isso de “habilidade de nível superior”, de acordo com o advogado de Royal, Jay Leiderman.

– Foi isso que atraiu Royal – acrescentou Leiderman. – O conhecimento.

Claro, Royal ou Chase acabaram não obtendo qualquer conhecimento de “nível superior”, mas na ocasião os dois ficaram seduzidos o suficiente para embarcar na aventura. Durante uma semana e meia, por volta de 20

de maio de 2011, eles conversaram com os outros rock stars na sala de bate-papo #pure-elite, com Royal utilizando o nome Neuron, e Chase, Devrandom. Chase logo desistiu, mas Royal ajudou na hackeagem da Sony Pictures, após Sabu delegar a pessoas diferentes a extração de porções diferentes de dados – dados pessoais de usuários que tinham participado de competições no site da Sony – dos servidores da empresa. Foi um período empolgante para Royal e Chase.

Então Sabu começou a falar em atacar alvos governamentais e o sangue deles congelou. Hackear a Sony tinha parecido válido para punir uma grande e arrogante corporação que processara George Hotz. Mas era difícil entender a lógica em atacar o Senate.gov, coisa que lhes podia causar graves problemas.

Royal começou a falar com alguns dos outros que não se sentia à vontade. Quando por fim contou a Sabu que ia sair, o hacker veterano respondeu: – Não, você não vai.

Sabu lembrou a Royal que ele já tinha sujado as mãos, como os demais, auxiliando no ataque à Sony. Royal continuou mais um tempo, mas, quando Sabu repentinamente sumiu do IRC (por ter sido preso) durante mais de um dia, o jovem achou que enfim podia se afastar. Ele continuou nervoso e consciente de que Sabu conhecia Cody muito bem, e, provavelmente, sabia que todos

frequentavam a mesma faculdade.

Royal tinha razão em se preocupar. Em algum momento perto do fim de 2011, a polícia assediou Cody e o transformou num informante. Em seguida, em janeiro de 2012, Cody começou sem mais nem menos a conversar com Royal sobre o LulzSec, “fazendo perguntas muito estranhas”, de acordo com ele, que intuiu o que estava acontecendo.

Parte das provas contra Royal veio dos registros de bate--papo armazenados no computador de Ryan Cleary.

– O moço gravava tudo – contou Leiderman sobre Cleary.

Mas o depoimento oral foi um recurso ainda maior para os promotores.

Em 2 de abril de 2012, cerca de um mês antes de Sabu ser exposto como informante, o FBI fez uma visita a Royal, e o universitário acabou se entregando para interrogatórios adicionais. Os agentes o haviam rastreado por meio de uma combinação de declarações de Cody e uma intimação judicial ao serviço de VPN HideMyAss que revelara seu endereço IP.

Em outubro de 2012, Royal declarou-se culpado da conspiração para causar dano a um computador protegido, principalmente os servidores da Sony. A empresa solicitou uma indenização de US$ 605 mil de Royal, inclusive o custo de atualizar a rede. Caberia a ele convencer outros supostos companheiros de conspiração, inclusive Sabu, Chase e Cody, a ajudá-lo a pagar a fiança. O ex-aluno com mérito universitário foi suspenso da faculdade e impedido de concluir o curso, correndo o risco de pegar até cinco anos de cadeia. É improvável que ele algum dia consiga trabalhar em projetos de alto nível com empreiteiros de defesa, como ele almejava, e menos ainda que consiga um emprego na NSA.

Leiderman, seu advogado, se esforçou para diminuir a sentença de Royal, talvez um tipo de prisão domiciliar, de modo que ele pudesse continuar a trabalhar e estudar. Ficou frustrado com o sistema jurídico nessa questão.

– Estamos supercriminalizando travessuras infantis – avaliou. – Um pirralho de doze anos com conhecimento moderado de computadores poderia ter se registrado numa VPN e utilizado essa ferramenta de SQL, a Havij, e, com as instruções que meu cliente recebeu, feito esse ataque.

[Royal] sempre teve uma conduta exemplar e é isso que ele recebe. Não precisamos trancafiar pessoas assim.

Na época da redação deste texto, pouca gente havia sido enviada à prisão. Em janeiro de 2013, um juiz britânico condenou Christopher Weatherhead, 22 anos, o operador da rede AnonOps conhecido como “Nerdo”, a dezoito meses de cadeia. Também condenou a sete meses de prisão Ashley “NikonElite” Rhodes, 28 anos. Os dois foram acusados de desferir ataques de DDoS contra os sites Mastercard.com, Visa.com e PayPal.com em dezembro de 2010. Embora milhares de voluntários também tenham participado, Weatherhead e Rhodes estariam entre os poucos a serem presos, e seus casos ajudaram a criar jurisprudência para punir essas atividades.

Os advogados de defesa esperam mais precedentes jurídicos e estão especialmente interessados em ver o que vai acontecer com Hector “Sabu”

Monsegur. O velho amigo de Sabu, Cody Kretsinger, declarou-se culpado de causar dano a um computador protegido, bem como de conspiração, e pode pegar até quinze anos de prisão, com fiança de US$ 500 mil, além de sua parcela na indenização de US$ 605 mil devida à Sony. Mas tanto ele quanto Royal estão esperando para ver qual será a sentença de Sabu.

Alguns ainda estão com raiva pelo fato de o FBI parecer fazer de Sabu uma ferramenta de armadilha.

– Sabu disse para trazer mais gente. Daí eu trouxe Neuron – contou um dos ex-membros do sexteto principal do LulzSec, enquanto se sentava numa cafeteria na Europa em outubro de 2012. Ele quer permanecer no anonimato, por conta de sua delicada situação jurídica. – Isso foi quando ele recrutava em segredo. Mas, tão logo a coisa veio à tona, não se tratava mais do LulzSec, mas desse lance do Antisec. [Sabu] falava: “Se você conhece gente com habilidade, traga-os, porque precisamos substituir fulano e beltrano”. Em retrospectiva, ele precisava de mais gente para sujar as mãos.

A pergunta inevitável: se Sabu não tivesse se tornado um informante, será que o Antisec nunca teria sido revivido e se tornado um movimento cibernético popular e perturbador entre o fim de 2011 e o começo de 2012?

– Depois disso os Feds ficaram contentes, até certo ponto – acrescentou ele. – Não gostavam dos danos causados, mas pegavam mais gente. Muitas pessoas

praticamente caía numa armadilha, mas isso não se sustenta como defesa.

Hoje, essa é a principal preocupação de todos os réus. Já não importa se a ética de sua prisão pareça injusta: eles desejam a sentença mais amena possível. Em especial, os réus britânicos, inclusive Jake Davis e Ryan Ackroyd, pretendem evitar uma extradição aos EUA, onde provavelmente enfrentariam punições mais severas.

De modo estranho, parece restar pouco antagonismo em relação à polícia. Enquanto faziam parte do Anonymous e do LulzSec, vários réus viviam provocando os feds, tratando-os nas salas de bate-papo como seus piores inimigos. Claro, deparar cara a cara com esse inimigo em uma mesa lhes despertou a solene compreensão de que não passam de profissionais cumprindo suas missões, com os quais até se podia negociar. A insurgência cibernética – tão fácil de embarcar e tão drástica em seus dogmas – não era maniqueísta em se tratando de aliados e adversários. Antigos companheiros de armas podiam tornar-se delatores, e inspetores muitas vezes faziam seu dever de casa.

– Por mais doloroso que seja reconhecer, eles foram extremamente profissionais – afirmou Leiderman sobre os agentes do FBI que haviam trabalhado no caso de Royal. – Foram polidos. Na verdade, é possível até chamá-los de cavalheiros.

– Os caras da perícia técnica foram competentes – avalia o ex-hacker do LulzSec. – São bons.

Os inspetores da Polícia Metropolitana de Londres inclusive adotam uma postura descontraída sobre o caso que atraiu milhares de manchetes internacionais.

– É apenas um caso como qualquer outro – sacudindo os ombros um inspetor que compareceu a uma recente sessão no tribunal.

Mas ainda existem outros grupos para deixá-los ocupados, novas facções de hackers com nomes como PrivateX e Team Ghost Shell que surgiram na área de encontro do Anonymous e acenam com mais vazamentos. Em setembro de 2012, uma declaração do Pastebin aparentemente alinhada com o Antisec anunciou o vazamento de um milhão de números de ID de dispositivos da Apple, alegando que tinham sido obtidos do laptop hackeado de um agente do FBI. Mais tarde, um desenvolvedor de aplicativo de celular assumiu ser a fonte do material vazado. De modo lento, mas seguro, isso está minando a credibilidade das frequentemente dramáticas alegações do Anonymous.

Analistas continuam a encarar o Anonymous como um novo exemplo de juventude descontente, uma geração que utiliza a internet como válvula de escape para expressar sua angústia, da mesma forma que os punks faziam com a música nos anos 1980. O problema é que desta vez as autoridades não podem ignorar seu modo de expressão da mesma forma que ignoraram a música. A internet é uma ferramenta poderosa que hospeda infraestrutura importante – uma paisagem com poucos jardins murados, onde script kiddies com poucas ferramentas simples e instruções básicas podem perturbar as – às vezes mal protegidas – propriedades on-line de empresas e agências governamentais. Os formuladores de políticas se esforçam para vislumbrar como melhor proteger e regular a internet, sabendo que não podem lançar mão das mesmas normas estruturais do mundo off-line.

Chris Poole, que não passava de um adolescente quando começou o 4chan em seu quarto em Nova York há nove anos, acredita que restringir o uso da internet simplesmente não vai funcionar.

– As pessoas são cretinas – afirmou ele durante uma entrevista paralela em um simpósio em outubro de 2012, trajando como de costume moletom cinza e jeans skinny. – Acho que é mais representativo de um problema humano. A educação é obtida ao longo de uma vida inteira, e, como a história revela, existem pessoas bem-educadas e pessoas mal-educadas.

Mas ele admite: a internet torna um pouco mais fácil enveredar pelo caminho errado, porque a quantidade de investimento que demanda para se tornar um babaca é pequena.

– Nunca me meti numa briga na vida real. Exige muito esforço e incômodo. Na net você precisa de cinquenta e cinco segundos para causar confusão. É realmente muito simples.

Jake Davis entende isso com perfeição. Ele não pode se arriscar a falar com outros on-line para incentivá-los a parar e pensar no que estão fazendo. Mas, se pudesse voltar no tempo e falar consigo mesmo no ano passado, o que diria? Jake medita um pouco antes de responder.

– Eu não diria: “Pare”. Eu diria: “Não se sinta pressionado”.

Dizer “pare” não funciona para alguém que se sente tão envolvido com um grupo e tão desconectado do mundo real, que acredita piamente ser impossível a

polícia tocá-lo. Nem para alguém que está convencido de que sempre precisa estar no computador, porque, se o abandonar por algumas horas, algo mágico poderá acontecer em sua ausência. Nesse estado de espírito, a pior coisa que pode acontecer será on-line – ser doxeado ou ridicularizado, por exemplo –, eclipsando os mais graves riscos off-line de tempo desperdiçado, saúde precária ou cadeia.

O truque teria sido lembrar o Jake do passado sobre a pressão e questionar sua fonte.

– Se alguém o pressiona a estar ali, então não se sinta pressionado, pois eles não se importam com seus interesses – afirma ele com um quê de amargura. – Fodam-se.

Uma vez, alguém tentou convencê-lo a parar, mas não interrompeu seu mergulho mais fundo no que se tornava uma insurgência digital em massa.

Foi em 2010. Um amigo norueguês com quem ele havia jogado games on-line ficava na internet vinte e quatro horas por dia, sete dias por semana, utilizando a rede como depósito de lixo emocional. Em seguida, ele se mudou para uma casa sem internet e tudo mudou. Conseguiu emprego, namorada, e hoje tem um filho. O amigo voltou a se conectar on-line no começo de 2010 e alertou Jake sobre passar muito tempo na web: – Tenha cuidado – avisou o amigo. – Vai corroê-lo.

– Optei por não dar ouvidos – conta Jake, embora hoje ele dê o mesmo conselho a outros. – Quando a internet representa tudo para você, é difícil enxergar o que está acontecendo – acrescenta.

Agora Jake contempla seu futuro.

– Faltam oito ou nove meses para eu receber a minha sentença – explica. – Antes disso, espero conseguir um emprego em meio turno em algum lugar, talvez começar um curso.

Não será fácil. Existem poucas oportunidades na cidade onde ele mora, a vinte minutos ao norte via trem, e é difícil resistir ao desejo de fazer algo capaz de utilizar de modo tão dramático suas habilidades de comunicação da mesma forma que o Anonymous utilizava. Ele espera acabar ingressando em alguma espécie de curso superior, talvez enquanto estiver preso, e depois ver o rumo das coisas.

Seu amigo viciado na internet havia conseguido encontrar algo de que gostava – seu trabalho.

– Se ele conseguiu mudar assim, então deve funcionar – aposta Jake. – Deve haver algo útil nas palavras.

Com esse comentário, Jake se levanta e limpa a grama e a terra dos jeans. O sol ainda brilha, e ele planeja ficar na cidade por mais algumas horas. Seu rosto está descontraído. Os sorrisos breves agora surgem com mais naturalidade. Um ano atrás, em Shetland, Jake não se expressava com tanto autoconhecimento. Agora ele é outra pessoa, não mais aquele jovem quieto e desajeitado, e sim alguém de bem consigo mesmo, mais convicto do que quer ser e ainda mais convicto do que não quer ser. Precisou apenas de alguns meses sendo Topiary e tendo essa vida arrebatada para chegar lá.

O futuro ainda é duvidoso, e, nesse mundo off-line, Jake é apenas mais um anônimo transeunte. Mas isso parece lhe agradar por enquanto. Enfiando as mãos nos bolsos, Jake sai da praça gramada e se mistura à multidão.

Agradecimentos

Este livro jamais teria se concretizado não fossem as contribuições de vários indivíduos essenciais. Em primeiríssimo lugar está Jake Davis, que forneceu percepções ininterruptamente úteis e claras sobre o desconcertante mundo do Anonymous, do LulzSec e da cultura cibernética em geral. Existe muito mais conteúdo em Davis do que fui capaz de enquadrar neste livro, e defendo que ele deve, quando chegar a hora, escrever um livro da própria lavra. Eu não teria começado a conversar com Davis, nos idos de dezembro de 2010, não fosse uma crucial conexão estabelecida via e-mail por Gregg Housh, cujo próprio papel na história do Anonymous é detalhado no Capítulo 5. Naquela época, eu havia começado a fazer a cobertura do Anonymous para a *Forbes* em sua nova plataforma de blogs, mas, sediada em Londres, interessei-me por falar com um representante do Reino Unido. Perguntei a Gregg se ele podia recomendar alguém, e ele me deu um endereço de e-mail geral do AnonOps. Tive a sorte de uma das pessoas que administravam aquele endereço ser Jake “Topiary”

Davis. À medida que trocava e-mails com esse endereço, fui ficando cada vez mais intrigada. Esse representante falava com confiança em “nós” ao referir-se ao Anonymous; por outro lado, defendia que o sistema da organização era fluido, permitindo que as missões fossem executadas por “qualquer um e todo mundo”. Indaguei como ele havia descoberto o Anonymous, e ele me explicou sobre os painéis de imagem. Eu nunca tinha ouvido falar neles.

– Sei que parece meio idiota – acrescentou ele –, mas de fato é um mundo completamente diferente depois que você se aprimora nele. Você começa a ver a vida de um outro prisma.

Achei isso fascinante. Quando essa pessoa revelou que seu nickname era Topiary, coloquei a palavra no Google e descobri referências sobre jardinagem. Quem era esse pessoal?

Após fazer a cobertura do ataque contra a HBGary, esforcei-me para vislumbrar os rumos da história e liguei para Tom Post, o editor administrativo da *Forbes*, em busca de respostas. Depois de ouvir as minhas divagações sobre as vulnerabilidades das mídias sociais, ele me deu talvez o conselho mais valioso que recebi no ano inteiro: – Junte tudo sobre o Anonymous que ainda não foi publicado, e, a partir daí, vamos tentar encontrar um foco.

Ele me orientou a descobrir mais sobre as pessoas por trás do Anonymous, como Topiary. Segui seu conselho e fui atrás disso. A ideia de fazer um livro me veio após alguns incentivos de colegas da *Forbes* em fevereiro de 2011, inclusive do redator da *Forbes* em assuntos de segurança cibernética, Andy Greenberg. Mais tarde, Andy se tornaria um companheiro de armas à medida que nós dois pelejávamos com o processo de redigir um livro – ele escrevia uma obra sobre o WikiLeaks e hacktivismo, publicada em 2012. A partir daí, passei a receber conselhos e orientações inestimáveis de Eric Lupfer, da agência de talentos William Morris, a quem não tenho como agradecer o suficiente por ter me ajudado a formular e reformular uma proposta decente sobre o livro.

A essa altura, eu já tinha sido apresentada (via e-mail) ao extraordinário jovem mencionado neste livro como William. Nossa aproximação começou quando ele primeiro tentou me adicionar no Facebook e depois enviou uma mensagem críptica e direta: – Oi. O que você deseja saber? Se eu responder, em troca posso fazer algumas perguntas sobre você? Eu realmente gostaria de uma resposta, negativa ou não. Obrigado, Chelsea.

Sem saber quem ou o que era essa “Chelsea”, ignorei a mensagem. Uma semana depois, veio outra mensagem: – Por favor, não me ignore; é rude.

E mais:

– Será que é demais pedir para estabelecer um simples diálogo?

Hoje me congratulo por ter concordado, não só porque talvez, caso contrário, eu tivesse acabado como alvo e visse minha “vida arruinada”, como ele costumava fazer, mas também porque por fim descobri alguém bem mais articulado, útil e promissor do que a mensagem original de William sugeria. Embora ele passe a impressão a muitas pessoas de ser meio vingativo, William respondeu a quase todas as perguntas que fiz sobre o 4chan, o Anonymous, a vida dele e até mesmo os recantos sombrios de sua mente. Por isso, e por me ajudar a dar a este livro

uma importante perspectiva sobre a cultura do 4chan, ele merece um colossal agradecimento.

Entre as outras pessoas essenciais que merecem reconhecimento está o diretor de produtos da *Forbes*, Lewis D'Vorkin. Ele enfrentou certo ceticismo ao estabelecer pela primeira vez a plataforma de colaboradores da *Forbes* em meados de 2010, mudando completamente a maneira de os jornalistas da revista postarem histórias on-line. Mas este livro jamais teria se transformado em realidade se D'Vorkin não tomasse essa ousada e brilhante medida. Forneceu aos jornalistas mais liberdade para ir atrás das histórias que realmente nos intrigam e, depois, também teve a capacidade de medir o quanto nossos leitores estão intrigados por elas. Graçasa D'Vorkin ter repaginado completamente a arquitetura da *Forbes*, descobri a existência de um saudável apetite por relatos sobre o mundo do Anonymous, e agora tinha uma oportunidade sem precedentes de investigar essas histórias. O editor de tecnologia da *Forbes*, Eric Savitz, que também é o meu chefe, me deu amplo e útil apoio durante a confecção deste livro. Coates Bateman, o produtor executivo de desenvolvimento de produtos da *Forbes*, foi um colaborador inestimável dos editores desta obra, a Little, Brown, enquanto o consultor jurídico da *Forbes*, Kai Falkenberg, também me ofereceu conselhos sensatos sobre assuntos jurídicos.

Sou grata a todas as outras pessoas ligadas ao Anonymous com quem falei para construir este livro, inclusive os membros principais do LulzSec: Hector "Sabu" Monsegur, Kayla, Tflow, AVunit e Pwnsauce, junto com Barrett Brown, Laurelai Bailey, Jennifer Emick e vários outros que pediram para ficar, apropriadamente, anônimos. Algumas dessas pessoas, em especial hackers, não se mostraram completamente abertas ou honestas quando conversaram comigo; seja como for, tive a sorte, como jornalista, de pelo menos elas terem falado comigo. Muita gente me pergunta como fui capaz de me aproximar de pessoas que frequentavam locais tão recônditos da web, e a resposta é que recebi a imensa ajuda de fontes que fizeram apresentações e endossaram meu nome. Também acredito que as pessoas, seja lá o quão sociopatas, narcisistas ou falsas possam ser, têm uma necessidade autêntica de contar suas histórias e entalhar alguma espécie de legado. Por isso acredito que me ajudou o fato de eu ter mencionado, quando comecei a falar, em março de 2011, com os hackers que atacaram a HBGary e depois formaram o LulzSec, que os entrevistados colaborariam com um livro preparado por mim sobre o Anonymous.

Além disso, Gabriella Coleman, hoje titular da cátedra Wolfe na Faculdade

Científica e Tecnológica da Universidade de McGill, em Montreal, me forneceu uma constante e revigorante dose de clareza sobre quem era o Anonymous e como o grupo funcionava em termos de coletividade.

Coleman revelou uma dedicação extraordinária ao estudo do fenômeno do Anonymous. Ela passou mais tempo conversando com uma base mais ampla de habituais Anons nas redes de IRC do que eu provavelmente fiz para redigir esta obra e, com toda razão, é considerada a especialista sobre o Anonymous e sua evolução. Fique de olho no livro que ela está prestes a lançar sobre o grupo.

Sinceros agradecimentos vão para minhas ex-colegas da *Forbes*, Anita Raghavan, que me ofereceu alguns conselhos inteligentes sobre minha proposta de publicação, e Stephane Fitch, que também me apresentou a David Fugate, da Launch Books. David se revelou um agente brilhante e seu contínuo incentivo me ajudou a encontrar a melhor editora possível: a Little, Brown. Desde o começo de meu relacionamento com ela, eu fiquei impressionada com a forma genuína e sólida que a editora abraçou a ideia deste livro e com a edição clara e incisiva de John Parsley. Considerando os detalhes intricados e as complexidades do assunto, suas múltiplas identidades e às vezes narradores não confiáveis, imagino que *Somos Anonymous* teria sido um manuscrito problemático para alguns editores, mas John fez um trabalho de mestre em me manter focada. Ele me ajudou a contar a história da forma mais clara possível e me auxiliou apenas com a quantia exata de intervenções editoriais.

Muitos agradecimentos também a Chester Wisniewski e Graham Cluley, da Sophos, a Theodora Michaels e aos leitores que ajudaram com correções técnicas no manuscrito.

Por fim, é necessário agradecer a meu maravilhoso círculo de amizades e familiares, cujo constante apoio e incentivo me permitiram perseverar e enfrentar o processo, às vezes ulceroso, de pesquisar e redigir esta obra ao longo da maior parte de 2011 e do começo de 2012. Esses amigos incluem Miriam Zaccarelli, Natalie West, Luciana e Elgen Strait, Victor Zaccarelli, Nancy Jubb, Il-Sung Sato, Anthea Dixon, Leila Makki e o hacker ético Magnus Webster. Meu pai foi meu incentivador número um para escrever este livro, enquanto meu marido mostrou força e paciência inacreditáveis à medida que a coisa foi evoluindo desde a ideia, depois a proposta e enfim o manuscrito. Outro membro de minha família não sabia sobre o livro, mas, apesar disso, foi uma luz que me guiou: minha avó, que faleceu no dia que terminei de revisar o rascunho final do

manuscrito e a quem este livro é dedicado. Embora ela estivesse com 96 anos de idade e fosse natural de uma aldeia agrícola de uma remota ilha vulcânica do arquipélago dos Açores, acho que até mesmo ela teria descoberto algo familiar nas histórias por trás do Anonymous e seus seguidores. Ainda que o mundo em que vivem seja moderno, misterioso, carregado de jargões técnicos, acho que minha avó poderia ter visto, como eu vi, que o Anonymous escreveu uma história muito humana.

Linha do tempo

5 de novembro de 1994 – Em um dos primeiros atos conhecidos de hacktivismo e desobediência cibernética, um grupo chamado de Zippies desfere um ataque de DDoS contra os sites do governo britânico, derrubando-os por uma semana, começando no Dia de Guy Fawkes.

1999 – O movimento Anti-Security é criado: um post no site anti.security.is apregoa o fim da divulgação integral de conhecidas vulnerabilidades e falhas de segurança de sites da web.

29 de setembro de 2003 – Christopher "moot" Poole registra a 4chan.net. (Hoje é 4chan.org.) **15 de março de 2006 –** Jake Brahm, vinte anos, posta falsas ameaças no 4chan sobre detonar bombas em estádios da Liga Nacional de Futebol Americano; dois anos depois, ele é condenado a seis meses de prisão.

12 de julho de 2006 – Usuários do painel *b* do 4chan atacam o Habbo Hotel, um badalado site para adolescentes. Eles se conectam aos jogos on-line em massa e inundam o site com avatares de um negro com terno cinza e cabelo estilo afro, impedindo a entrada à piscina virtual e formando suásticas. Isso originou o meme "A piscina está fechada".

Janeiro de 2007 – O controverso radialista e blogueiro Hal Turner tenta, sem sucesso, processar o 4chan, após usuários do *b* lançarem um ataque de DDoS contra seu site.

7 de junho de 2007 – O site *i*nsurgency do Partyvan é fundado como centro de informação sobre ataques e, mais tarde, comunicações por meio do estabelecimento da rede de IRC

Partyvan.

Julho de 2007 – Uma afiliada da Fox News em Los Angeles descreve o Anonymous como “hackers vitaminados” e “máquina de ódio da internet”.

15 de janeiro de 2008 – O Gawker publica um vídeo de Tom Cruise que a Igreja da Cientologia tentava abafar. A Igreja emite uma reivindicação de violação de direitos autorais contra o YouTube. Em resposta, um postador original no *b* convoca o 4chan a “fazer algo importante” e derrubar o site oficial da Cientologia. Utilizando a ferramenta da web chamada Gigaloader, os usuários do *b* conseguem derrubar o Scientology.org, mantendo-o esporadicamente fora do ar até 25 de janeiro de 2008.

21 de janeiro de 2008 – Um punhado de participantes do Chanology publica um vídeo no YouTube com uma voz robótica declarando guerra contra a Cientologia. No dia seguinte, milhares de novos participantes entram no canal de IRC onde os ataques do Chanology estão sendo discutidos.

24 de janeiro de 2008 – O Anonymous lança um ataque maior contra o Scientology.org, tirando-o do ar.

10 de fevereiro de 2008 – Sectários do Anonymous usam máscaras do filme *V de vingança* e promovem manifestações diante de centros da Cientologia em cidades importantes mundo afora, como Nova York, Londres e Dallas, no Texas.

Final de 2008 – Protestos e ataques cibernéticos contra a Igreja da Cientologia arrefecem, à medida que os partidários do Anonymous perdem interesse pela causa.

25 de janeiro de 2010 – Brian Mettenbrink, sectário do Anonymous e aluno de engenharia, se declara culpado de baixar e utilizar a ferramenta da web LOIC para atacar a Cientologia, como parte do Projeto Chanology, e é condenado a um ano de prisão.

17 de setembro de 2010 – Sectários do Anonymous desferem um ataque de DDoS contra uma empresa de software indiana, a Aiplex, após ela admitir ter lançado ataques de DDoS contra o site BitTorrent do The Pirate Bay. O Anonymous realiza vários outros ataques contra empresas de direito autoral sob a bandeira Operação Vingança. Sectários colaboram numa série de redes de IRC.

Outubro de 2010 – O FBI começa a investigar os ataques do Anonymous contra empresas de direito autoral, a ponta do iceberg do que se tornaria uma

aprofundada investigação internacional.

3 de novembro de 2010 – Os sectários do Anonymous com recursos de servidor instalam o IRC AnonOps, rede de bate-papo mais estável para hospedar debates sobre a Operação Vingança e outras operações do Anonymous.

28 de novembro de 2010 – Cinco jornais começam a publicar os cabogramas diplomáticos dos EUA que lhes tinham sido repassados exclusivamente pela organização denunciadora WikiLeaks. Ao longo dos dias seguintes, um conhecido hacktivista chamado The Jester desfere um ataque DDoS contra o WikiLeaks.org, tirando-o do ar.

3 de dezembro de 2010 – A empresa líder em pagamentos on-line, PayPal, anuncia em seu blog que está cortando os serviços de financiamento ao WikiLeaks, instituição que depende de doações.

Pouco depois, alguns organizadores no canal #command do IRC

AnonOps coordenam um ataque de DDoS contra o blog do PayPal.

4 de dezembro de 2010 – Um anúncio postado no Anonops.net declara que o Anonymous planeja atacar "vários alvos relacionados à censura" e que a Operação Vingança "surgiu em apoio ao WikiLeaks".

6 de dezembro de 2010 – Gestores do AnonOps lançam um ataque de DDoS contra o postFinance.ch, empresa de pagamentos eletrônicos suíça que também bloqueou os serviços de financiamento ao WikiLeaks. Aproximadamente novecentas pessoas participam da sala de bate-papo #operationpayback no AnonOps e cerca de quinhentas participam do ataque utilizando LOIC.

8 de dezembro de 2010 – O AnonOps lança um ataque de DDoS

contra o PayPal.com, utilizando quatro mil e quinhentos voluntários com LOIC, mas só obtendo sucesso quando uma pessoa utilizando botnet tira o site completamente do ar. Por volta de sete mil e oitocentas pessoas agora participam da sala de bate-papo #operationpayback. Mais tarde, nesse mesmo dia, o Anonymous ataca o MasterCard.com e o Visa.com, que também vetaram serviços de financiamento ao WikiLeaks, colocando os dois sites off-line por cerca de doze horas.

9 de dezembro de 2010 – Controladores de botnet que antes tinham auxiliado a derrubar o PayPal.com, o MasterCard.com e o Visa.com voltam-se contra os operadores do AnonOps e começam a atacar a rede de IRC, estragando o ataque planejado contra a Amazon naquele dia.

11 de dezembro de 2010 – A polícia holandesa prende Martijn "Awinee" Gonlag, dezenove anos, por utilizar o LOIC e participar do ataque de DDoS do Anonymous, uma das primeiras das dezenas de prisões que aconteceriam na Europa e nos Estados Unidos ao longo do ano seguinte.

15 de dezembro de 2010 – Um membro da equipe de segurança cibernética do PayPal entrega ao FBI um pen-drive com os endereços IP de mil indivíduos que utilizaram o LOIC para atacar o PayPal.

Meados de dezembro de 2010 – Os administradores do AnonOps enfrentam dificuldades de manutenção enquanto sua rede é continuamente atacada, deixando-os incapazes de supervisionar a estratégia. Em decorrência disso, a Operação Vingança se divide em várias operações colaterais, tais como Operação Leakspin, Operação OverLoad e um ataque contra o site oficial de Sarah Palin.

Meados de dezembro de 2010 – Alguns sectários do AnonOps com perícia técnica criam um canal de IRC privado fora da rede, chamado #InternetFeds, onde cerca de trinta hackers de chapéu preto (como Sabu, Tflow e Kayla, junto com outros Anons interessados que foram convidados a participar do canal) podem debater as operações futuras.

Começo de janeiro de 2011 – Os hackers no #InternetFeds discutem ataques contra sites de regimes repressivos do Oriente Médio, como o da Tunísia, onde levantes democráticos populares estão acontecendo. O hacker Tflow escreve um script da web que permite aos tunisianos driblar a espionagem cibernética do governo, enquanto Sabu hackeia o site do primeiro-ministro tunisiano e faz um deface com uma mensagem do Anonymous.

Meados a fins de janeiro de 2011 – Membros do #InternetFeds continuam a colaborar na hackeagem e desfiguração de sites de outros governos do Oriente Médio, inclusive Argélia e Egito.

27 de janeiro de 2011 – A polícia britânica prende cinco homens envolvidos nos ataques da Operação Vingança contra o PayPal, a MasterCard e a Visa, inclusive

os operadores do AnonOps com os apelidos Nerdo e Fennic.

4 de fevereiro de 2011 – Um pequeno grupo de hackers do #InternetFeds se reúne em outro canal privado de IRC para debater um ataque contra a HBGaryFederal, empresa de segurança de TI, após o diretor-executivo dela ser citado no *Financial Times* daquele dia dizendo que, investigando o Anonymous, havia descoberto as identidades verdadeiras de seus principais líderes.

6 de fevereiro de 2011 – Os noticiários publicam que o Anonymous roubou dezenas de milhares de e-mails corporativos de Aaron Barr, bem como de dois executivos da empresa irmã HBGary Inc. A organização também hackeia a conta de Twitter de Barr e promove ataques de DDoS contra o site da empresa, desfigurando-o.

Começo a meados de fevereiro de 2011 – O mesmo grupo do #InternetFeds publica os e-mails particulares de Aaron Barr num visualizador de e-mails. Jornalistas e sectários descobrem que Barr estivera propondo controversos ataques cibernéticos contra o WikiLeaks e adversários da Câmara de Comércio dos EUA. Barr pede demissão.

24 de fevereiro de 2011 – O Anonymous realiza uma hackeagem em tempo real e desfigura um site pertencente à controversa Igreja Batista Westboro, enquanto Topiary, membro do Anonymous, confronta uma representante da Westboro num programa de rádio e tevê. O resultante vídeo no YouTube recebe mais de um milhão de visualizações.

Meados a fins de fevereiro de 2011 – Jennifer Emick, ex-colaboradora do Projeto Chanology, se transforma em detratora do Anonymous e decide investigar as verdadeiras identidades de importantes hackers e sectários da organização, revelando dados de Sabu, também conhecido como Hector Monsegur.

Meados de março de 2011 – Emick e um punhado de colegas publicam uma lista com setenta nomes, inclusive o de Monsegur, sob o disfarce de uma empresa de segurança cibernética chamada Backtrace. Logo depois, Emick recebe o contato do FBI.

1º de abril de 2011 – Sectários do Anonymous publicam um folheto digital declarando guerra contra a Sony, após a empresa processar um hacker chamado George “Geohotz” Hotz. Na sequência, o grupo desfere um ataque de DDoS

contra os sites da Sony e da PlayStation Network da Sony, deixando os gamers muito aborrecidos.

7 de abril de 2011 – Organizadores do Anonymous sustam os ataques de DDoS contra a Sony, alegando que não desejam perturbar a PlayStation Network, mas a rede permanece off-line pelo resto do mês.

Abril de 2011 – Topiary e Sabu discutem sobre dar um tempo do Anonymous, então decidem reunir a equipe de hackers por trás do ataque contra a HBGary para colaborarem em mais investidas. Os hackers Tflow e Kayla voltam a se unir com Topiary e Sabu, junto com outro sectário do Anonymous chamado AVunit e, mais tarde, o hacker irlandês chamado Pwnsauce. O sexteto forma um grupo dissidente e não limitado sequer pelos mais frouxos princípios do Anonymous – tais como não atacar empresas da mídia. Eles batizam o grupo de LulzSec. Começam a esquadrinhar sites importantes em busca de vulnerabilidades que "rooters" como Sabu e Kayla então podem explorar para roubar e publicar dados.

2 de maio de 2011 – A Sony anuncia uma invasão de sua rede ocorrida em meados de abril, a qual comprometeu os dados pessoais e financeiros de mais de 75 milhões de contas da PlayStation Network. Embora o Anonymous não tenha assumido a responsabilidade, mais tarde a Sony alegou que os hackers deixaram um arquivo marcado com as palavras "Anonymous" e "Somos Legião".

7 de maio de 2011 – O LulzSec anuncia no Twitter, pela nova conta @lulzsec, que hackeou o Fox.com e publicou uma base de dados confidencial de competidores potenciais do show de talentos *The X Factor*.

9 de maio de 2011 – Um ex-operador do AnonOps se rebela e publica uma lista de 653 nomes de usuário e endereços IP, os quais, caso não estivessem protegidos com VPN ou outros proxies, poderiam identificar as pessoas por trás deles.

30 de maio de 2011 – O LulzSec invade a rede de computadores da PBS, após alegadamente desaprovar o documentário sobre o WikiLeaks transmitido pelo programa *PBS NewsHour*. O LulzSec publica uma lista de endereços de e-mail e senhas dos funcionários da PBS, enquanto Topiary redige uma notícia falsa sobre o rapper assassinado Tupac Shakur ter sido encontrado com vida, publicando-a por intermédio do site da *PBS NewsHour*. Os fundadores do grupo

discutem a formação de uma rede de colaboradores de segundo escalão, muitos deles amigos hackers de Sabu.

2 de junho de 2011 – O LulzSec anuncia ter hackeado o SonyPictures.com e afirma que o grupo teve acesso às informações pessoais de mais de um milhão de usuários do site.

3 de junho de 2011 – O LulzSec desfigura o site da Atlanta Infragard, afiliada do FBI, e publica uma lista de e-mails e senhas de 180 usuários do site, alguns deles agentes do FBI.

6 de junho de 2011 – O LulzSec recebe uma doação de 400

Bitcoins, equivalente a US$ 7800 na época.

7 de junho de 2011 – Dois agentes do FBI visitam Hector “Sabu”

Monsegur em sua residência em Nova York e ameaçam prendê-lo por dois anos por roubar informações de cartões de crédito caso ele não queira cooperar. Monsegur concorda em se tornar informante e ao mesmo tempo continuar a liderar o LulzSec.

8 de junho de 2011 – Os hackers do LulzSec notam que Sabu ficou off-line por vinte e quatro horas e ficam preocupados, achando que ele recebeu uma “visitinha” do FBI. Mais tarde naquela noite, horário britânico, Topiary consegue contato com Sabu, o qual alega que sua avó morreu e que ele ficará uns dias inativo no LulzSec.

15 de junho de 2011 – O LulzSec assume a responsabilidade por desferir um ataque de DDoS contra o site oficial da CIA. O ataque foi executado pelo ex--operador do AnonOps Ryan, que tem um botnet e agora apoia o LulzSec.

16 de junho de 2011 – Um representante do WikiLeaks entra em contato com Topiary para dizer que organizadores da cúpula querem conversar com o LulzSec. Ele e Sabu por fim entabulam uma conversa via IRC com um representante do WikiLeaks e alguém que alegava ser Julian Assange. O representante “confirma” a presença de Assange carregando temporariamente um vídeo no YouTube que mostra seu bate-papo interativo acontecendo em tempo real numa tela de computador, depois abrindo a imagem para mostrar Assange com seu laptop. O grupo debate maneiras de mútua colaboração.

19 de junho de 2011 – O LulzSec publica um comunicado de imprensa incentivando o renascimento do movimento Anti-Security (ou Antisec) e defendendo ataques cibernéticos contra os sites de governos e suas agências.

20 de junho de 2011 – Empolgado pela significativa resposta ao anúncio do movimento Antisec, Ryan utiliza seu botnet para desferir ataques de DDoS contra vários sites importantes, inclusive a Agência Britânica contra o Crime Organizado Grave.

Mais tarde, às 22h30 naquela noite no Reino Unido, ele é preso em sua casa.

23 de junho de 2011 – O LulzSec publica documentos sigilosos roubados da polícia do Arizona, inclusive os nomes e os endereços de policiais. Com a sensação de terem ido longe demais, os membros do LulzSec, inclusive Topiary e Tflow, discutem o término do grupo.

24 de junho de 2011 – Topiary e Tflow contam a AVunit e Sabu que desejam terminar o LulzSec, causando um caloroso debate.

26 de junho de 2011 – O LulzSec anuncia sua dissolução após “50

dias de lulz”.

18 de julho de 2011 – O LulzSec retorna para mais uma hackeagem, carregando um artigo falso sobre a morte do dono da News International, Rupert Murdoch, na página inicial de seu tabloide britânico líder de vendas, *The Sun*.

19 de julho de 2011 – A polícia britânica anuncia a prisão de um garoto de dezesseis anos que ela afirma se tratar do hacker Tflow, componente do LulzSec.

27 de julho de 2011 – A polícia prende o habitante das ilhas Shetland, Jake Davis, suspeito de ser o Topiary do LulzSec.

2 de setembro de 2011 – A polícia prende Ryan Ackroyd, 24

anos, suspeito de ser Kayla.

24 de dezembro de 2011 – O Anonymous anuncia que roubou milhares de e-mails e dados confidenciais da Stratfor, empresa de inteligência de segurança dos EUA, sob o lema “Lulz Natalino”.

Sabu, que alega ainda estar solto enquanto outros membros do LulzSec foram presos, mantém registros sobre a operação a partir de canais de bate-papo privados e repassa ao FBI as informações sobre os organizadores do ataque.

6 de março de 2012 – Irrompe a notícia de que Hector Monsegur tem agido como informante do FBI nos últimos oito meses, ajudando o órgão a indiciar Jeremy Hammond, de Chicago, e cinco pessoas envolvidas com o LulzSec.

Notas e fontes

Parte 1

Capítulo 1: O ataque As páginas de abertura, inclusive as descrições sobre o início da carreira, a residência e a vida familiar de Aaron Barr, baseiam-se em entrevistas conduzidas com Barr, tanto pelo telefone quanto num encontro presencial em Londres. Dados adicionais sobre seu trabalho na HBGary Federal foram obtidos de um artigo investigativo publicado no blog ThreatLevel da revista *Wired*, que escrutinava seus e-mails publicados e dava um panorama sobre seus planos para a empresa, junto com as propostas que ele fazia para a Hunton & Williams. O artigo intitulava-se “Spy Games: Inside the Convoluted Plot to Bring Down WikiLeaks”, assinado pelo articulista Nate Anderson. O artigo do *Financial Times* em que Aaron Barr revelou sua pesquisa vindoura intitulava-se “Cyberactivists Warned of Arrest”, de autoria do repórter Joseph Menn, de São Francisco, e foi publicado pela primeira vez na sexta-feira, 4 de fevereiro de 2011, e depois atualizado no dia seguinte.

Mais detalhes sobre os e-mails entre Barr e Greg Hoglund da HBGary Inc. antes do ataque vieram do visualizador de e-mails da HBGary publicado pelos hackers em meados de fevereiro.

Os dados sobre Sabu hackeando computadores na adolescência baseiam-se em entrevistas com o hacker conduzidas via Internet Relay Chat em abril de 2011, dois meses antes de ele ser preso e se tornar informante do FBI. Dados adicionais sobre Sabu e o fato de ele ter nascido e crescido em Nova York provêm de documentos do tribunal após sua prisão mais tarde naquele ano.

Ao longo do livro, dados pessoais alegados por Kayla originam-se de entrevistas com a hacker conduzidas entre março e setembro de 2011 via e-mail e Internet Relay Chat. O boato sobre ela ter esfaqueado a webcam veio de uma entrevista on-line com Topiary.

Também ao longo do livro, dados sobre Topiary vieram de entrevistas on-line, por telefone e presenciais com ele (Jake Davis) entre dezembro de 2010 e o primeiro semestre de 2012. Dados sobre Tflow vêm de entrevistas com Topiary e com o próprio Tflow; a informação de que Tflow tinha convidado Sabu e Topiary para o canal secreto de IRC veio de Topiary, de outro hacker que expressou o desejo de permanecer anônimo e do próprio Sabu.

Dados sobre como os hackers planejaram o ataque contra a HBGary, inclusive como utilizaram o site HashKiller para decodificar as senhas da empresa, vieram de entrevistas com Topiary conduzidas via IRC e Skype (apenas voz).

Dados acerca da pesquisa de Barr sobre o Anonymous, inclusive as "observações apressadas como *Mmxanon – states. . ghetto*", têm como fonte anotações pessoais, postadas on-line pelos hackers.

O diálogo entre Barr e os hackers, inclusive com CommanderX, vem de registros de bate-papo que foram publicados on-line – em parte pela ferramenta da web Pastebin – e também no artigo da Ars Technica "(Virtually) Face to Face: How Aaron Barr Revealed Himself to Anonymous", de Nate Anderson. O diálogo entre Barr e Topiary, que termina com "Morra nas chamas. Você está acabado", vem de um fragmento do registro de bate-papo cortado e colado em uma conversa via Skype entre mim e Topiary, poucos dias após o ataque. Dados adicionais sobre o ataque provêm de entrevistas com Jake Davis, assim como de entrevistas on-line com Sabu, Kayla e outros hackers. Dados sobre o Super Bowl de fevereiro de 2011 foram obtidos com base em diversas notícias e no meu próprio testemunho da partida real enquanto seguia on-line o andamento do ataque contra a HBGary Federal. Embora eu já estivesse entrevistando Topiary com certa frequência, o ataque me levou a ser apresentada a outros do grupo – primeiro Kayla, depois Sabu, em seguida Tflow.

SQL se lê como uma série de fórmulas. Um exemplo é: "Selecione o cartão de crédito da pessoa cujo nome=SMITH". Se alguém fosse executar um ataque de injeção de SQL, eles podiam injetar o código dizendo: "Selecione a de b onde a=SMITH".

Como os hackers sabiam que Barr era CogAnon? Mais tarde, Topiary explicou que, quase imediatamente após ver o artigo do *Financial Times* e entrar na rede da HBGary Federal, um deles notara que seus cabeçalhos internos de e-mail listavam o endereço IP da VPN (rede virtual privada) dele. Barr tinha utilizado essa mesma conexão de VPN para se registrar numa rede de IRC

utilizada pelo Anonymous, conhecida como AnonOps. Os hackers só precisaram entregar o endereço IP a um dos operadores de rede de bate-papo, que executou uma busca rápida. Sem sombra de dúvida, apareceu o nome CogAnon.

Capítulo 2: William e as raízes do Anonymous Dados sobre como Christopher

Poole criou o 4chan vêm de uma entrevista que Poole deu ao blog Bits do *New York Times*. O artigo, intitulado "One on One: Christopher Poole, Founder of 4chan", foi publicado em 19 de março de 2010.

Eu baseei as informações sobre o 2chan do Japão no artigo do *New York Times*, publicado em 2004, "Japanese Find a Forum to Vent Most-Secret Feelings", e no artigo da *Wired*, publicado em maio de 2008, "Meet Hiroyuki Nishimura, the Bad Boy of the Japanese Internet".

Dados adicionais sobre o desenvolvimento do 4chan, como seu anúncio "DUAS VEZES O CHAN" no Something Awful, vêm de um artigo sobre a história do 4chan de autoria do desenvolvedor da web Jonathan Drain, em jonnydigital.com. O comentário de moot sobre o *b* ser um "recipiente para retardados" vem de um anúncio na página de "notícias" do 4chan, o 4chan.org/news?all, em 2 de outubro de 2003.

Embora a história da adoção do anonimato compulsório no 4chan pela influência de Shii seja relativamente bem conhecida entre os usuários do painel de imagem, os dados vêm de depoimentos fornecidos no site de Shii, shii.org.

Dados sobre a vida, os pontos de vista e as façanhas de um jovem chamado neste livro de William vêm de dezenas de e-mails e vários encontros presenciais, todos acontecidos entre fevereiro de 2011 e o primeiro semestre de 2012. Depois de me contar – em um encontro realizado em julho de 2011 – a história da hackeagem da conta de "Jen" (não é o nome real dela) no PhotoBucket, William me enviou fotos de Jen e "Joshua Dean Scott". Tenho as imagens guardadas. Por exemplo, a foto mostra Scott segurando um pedaço de papel em que se lê: "'Jen' é dona de meu rabo, 02/03/11". Com boné preto, piercing labial e tênis Converse preto em cima da cabeça, ele ainda esboça um sorriso.

Em várias ocasiões, William me mandou via e-mail capturas de imagem com as conversas que ele mantinha com as pessoas que trollava no Facebook, bem como com os tópicos de ataques dos quais ele às vezes participava no *b*, para corroborar seus relatos.

As brincadeiras e intimidações on-line dos indivíduos descritos neste livro são apenas uma pequena fração das muitas façanhas noturnas sobre as quais William me alertou.

Mais detalhes sobre o *b* e o 4chan têm como fontes os repositórios

de

memes

Encyclopedia

Dramatica

(agora

redirecionados a ohinternet.com) e KnowYourMeme.com, bem como entrevistas com Jake Davis.

Capítulo 3: Todo mundo vem para cá A grande maioria dos dados sobre a infância e a vida em Shetland de Topiary vem de entrevistas on-line e presenciais com Jake Davis, com mais detalhes e confirmações vindo de discussões com a mãe dele, Jennifer Davis, após a prisão de Jake. A partir de meados de abril, ele estava morando na casa dela sob fiança, aguardando a audiência de um recurso no tribunal da coroa inglesa em 11 de maio de 2012. Alguns dados importantes, como a morte de seu padrasto, Alexander "Allie" Spence, foram corroborados por reportagens de jornais. Descrições da paisagem e a falta de lojas modernas nas ilhas Shetland vêm de minha própria visita de um dia a Lerwick, onde conheci Davis no final de junho de 2011.

Dados sobre os frequentes trotes de Davis ao restaurante Applebee's em San Antonio, Texas, resultam de entrevistas com ele. Embora ele não tivesse como fornecer gravações das ligações feitas ao Aplebee, ele realmente forneceu arquivos de áudio de outros trotes semelhantes.

Uma característica comum dos ataques do *b* era uma "onda" de usuários contra um alvo on-line, com a ideia geral de sobrecarregá-lo. Entre os exemplos fornecidos, encontra-se a remessa via spam de fotos chocantes a um fórum; essa tática comum dos usuários do *b* foi recentemente perpetrada no site de piadas 9gag. O ataque no qual o *b* influenciou a votação para "Pessoa do ano" da revista *Time* aconteceu em 2009, quando os usuários do 4chan famosamente se uniram para programar um bot que trapacearia para colocar Christopher "moot" Poole no topo do ranking da *Time*. Além de lhe dar inexequíveis 16 milhões de votos, eles manipularam o sistema para que as primeiras letras dos próximos vinte nomes do ranking soletrassem as palavras "Marblecake also the game", suposta referência ao canal de IRC no qual a maior parte do Projeto Chanology foi

organizada em 2008

(consultar Capítulo 5). A revista *Time* forneceu detalhes da hackeagem num vídeo e citou moot, dizendo que não tinha ideia de quem estava por trás da manipulação de votos.

Os relatos sobre o ataque contra o Habbo Hotel e a Operação Basement Dad baseiam-se principalmente no testemunho de Davis, mas também são corroborados por reportagens on-line, como o artigo da ReadWriteWeb de 16 de abril de 2009, intitulado "Operation Basement Dad: How 4Chan Could Beat CNN & Ashton Kutcher", e, no caso do Habbo Hotel, o artigo da Fox de 8 de abril de 2009, com o título "4Chan: The Rude, Raunchy Underbelly of the Internet".

Dados sobre as origens do Internet Relay Chat vêm do artigo on-line "History of IRC", do consultor de informática e hacker Daniel Stenberg, postado em seu site, http://daniel.haxx.se/. Algumas descrições extras, como as dos números de canais de IRC e números de usuários nos canais, vêm de minha própria exploração do IRC. A fonte da expressão "Todo mundo vem para cá" é Jake "Topiary" Davis, e eu verifiquei o uso frequente da frase por meio de depósitos de conteúdo de painéis de imagem, como o chanarchive.org.

Capítulo 4: Kayla e a ascensão do Anonymous A principal fonte acerca da retrospectiva de Kayla sobre sua infância e pais consiste em entrevistas on-line com a própria Kayla (eu me refiro à sua entidade on-line como "ela").

A ideia de que Kayla mentiu quanto a ser uma garota de dezesseis anos de idade vem de minhas próprias observações e da discussão com outros hackers, com indícios adicionais provenientes da prisão de Ryan Ackroyd pela Polícia Metropolitana, em setembro de 2011. Até meados de abril de 2012, não posso confirmar que a pessoa que entrevistei via Internet Relay Chat entre março e setembro de 2011 era Ackroyd. Quanto aos boatos de que Kayla era "um hacker transgênero", Ackroyd não aparentava ser transgênero em sua primeira aparição diante do tribunal de Westminster Magistrates, na ocasião com 25 anos, em 16 de março de 2012.

A citação "Kayla parecia ter uma profunda necessidade de contar histórias para provar o seu valor aos outros" vem da leitura de comentários feitos por Kayla nos registros de bate-papo vazados dos canais #HQ e #pure-elite durante os dias

do LulzSec, inclusive aqueles nos quais ela se vangloriava de ter instigado ataques durante o Projeto Chanology. Tão enganosa Kayla tinha sido on-line que entrevistas telefônicas e presenciais conduzidas com Hector Monsegur, Jake Davis, Aaron Barr, Gregg Housh, Jennifer Emick, Laurelai Bailey e outras fontes anônimas produziram nada além de especulações sobre a sua identidade verdadeira.

Informações contextuais sobre a tendência de certos homens alegarem ser mulheres on-line vêm de conversas com hackers e do conhecimento geral com base no mundo dos memes e da cultura da internet. A expressão “There are no girls on the Internet” tem um verbete próprio em KnowYourMeme.com, a partir do qual parte desse contexto se baseia, enquanto o popular comentário no *b* “Tits or GTFO” vem da minha própria exploração do *b* e de discussões com William. A propósito, a lista das 47 Regras da internet foi amplamente publicada on-line.

Na minha explicação sobre endereços IP, estou me referindo nesse caso a endereços IPv4 (agora esgotados). Os mais recentes endereços IPv6 apresentam oito grupos de quatro dígitos hexadecimais segmentados por dois-pontos.

Dados sobre o Partyvan se baseiam em entrevistas com um organizador da época do Chanology que preferiu permanecer anônimo, em entrevistas com Kayla, e em conteúdo no site partyvan.info, também conhecido como *i*nsurgency W*i*ki.

Dados sobre o relato da televisão Fox de Los Angeles de julho de 2007 foram originados de um vídeo do YouTube com a reportagem.

Capítulo 5: Projeto Chanology Dados sobre a publicação do vídeo de Tom Cruise provêm de entrevistas com a militante antiCientologia Barbara Graham e de e-mails trocados com o jornalista Mark Ebner. Patty Pieniadz escreveu seu próprio relato detalhado, intitulado “The Story Behind the Tom Cruise Video Leak”, e o postou no fórum WhyWeProtest.net, sob a alcunha de “pooks”, em 4 de setembro de 2011; alguns itens da primeira parte deste capítulo também se baseiam nesse relato. Descrições do conteúdo baseiam-se em assistir ao próprio vídeo no YouTube. Segundo Ebner, o ex-cientologista e jornalista de tevê Mark Bunker havia originalmente carregado o vídeo em sua conta do YouTube e notificado vários de seus contatos com a mídia. Então, algumas horas depois, ele tirou o vídeo.

O dado sobre a ação judicial de direitos autorais no valor de 1

bilhão de dólares da Viacom contra a empresa mãe do YouTube, o Google, tem como fonte várias reportagens, incluindo o artigo do *The New York Times*, intitulado “Whose Tube? Viacom Sues YouTube Over Video Clips”, publicado em 14 de março de 2007.

O texto do tópico de discussão original no *b* sobre um ataque contra a Cientologia em 15 de janeiro vem do 4chanarchive.org. O

boato de que o postador original no *b* do primeiro tópico antiCientologia era uma mulher veio de uma entrevista com Gregg Housh.

Dados sobre ataques de DDoS vêm de numerosos artigos da web sobre como funcionam ataques cibernéticos, junto com discussões em segundo plano de profissionais de segurança de TI e hackers do Anonymous. A analogia de Graham Cluley sobre “15 homens gordos” vem originalmente de um artigo de 6 de agosto de 2009, assinado por Cluley, publicado no blog Naked Security da empresa de pesquisa Sophos. Contexto sobre o ataque do 4chan contra Hal Turner vem de vários posts do blog, bem como de tópicos do 4chan arquivados. O detalhe de que alguém poderia baixar “pelo menos uma dúzia de ferramentas de software grátis” do painel *rs* do 4chan para participar de algum tipo de ataque de DDoS

vem de uma entrevista com Housh. Dados sobre as fases 1, 2, 3 *etc.*

e sobre o *b* estar atacando o Scientology.org especificamente com o Gigaloader baseiam-se em um arquivo do tópico real. Dados sobre o Gigaloader vêm de comparar e corroborar vários fóruns de discussão na web sobre essa ferramenta da internet.

Outros dados ao longo do capítulo sobre as centenas de pessoas que se aglomeraram no canal de IRC #xenu e, em seguida, a migração para manifestações presenciais e o estabelecimento do centro organizacional #marblecake vêm de uma entrevista por telefone com Gregg Housh e de e-mails trocados com outro organizador do Chanology que deseja manter o anonimato. Existe também uma cronologia dos principais eventos do Chanology no site apropriadamente chamado chanologytimeline.com.

Housh confirmou em uma entrevista que havia sido preso por violações de direitos autorais. Detalhes adicionais se basearam em uma “moção por variação Booker” apresentada no tribunal distrital federal de New Hampshire em 23 de

novembro de 2005.

A moção mostrava que Housh tinha se declarado culpado de uma acusação de conspiração para violar leis de direitos autorais, relacionadas à criação de um programa de computador no verão de 2001 que procurava automaticamente novo software. Dados sobre antecedentes familiares de Housh têm como fonte a moção no tribunal e a seção “The History and Characteristics of the Defendant”. A moção também afirma que Housh foi abordado pelo FBI sobre o caso em 2001, e que ele procurou atenuar seus crimes, cooperando com o FBI “durante quatro anos”. Informações adicionais sobre a pena de Housh de três meses em penitenciária federal vêm da entrevista de Housh com o Huffington Post, no artigo “Anonymous and the War Over the Internet”, publicado em 30 de janeiro de 2012. O fato de Housh ter 35 anos também foi mencionado na entrevista.

O factoide sobre 25 mil cientologistas nos EUA em 2008 vem originalmente do *American Religion Identification Survey*, citado em um relatório pela Associated Press.

Informações sobre a postagem de documentos internos da Igreja pelo grupo de notícias alt.religion.scientology são originárias do artigo publicado em janeiro de 2008 no *Globe and Mail*, intitulado “Scientology vs. the Internet, part XVII”.

O dado de que o XSS é a segunda técnica mais comum de hackeagem depois da injeção de SQL baseia-se na Web Hacking Incident Database (WHID) de 2011, banco de dados on-line que rastreia incidentes de segurança relatados pela mídia e é liderado por Ryan Barnett, pesquisador sênior de segurança nos SpiderLabs da equipe de pesquisa da Trustwave.

Dados sobre o impacto técnico dos ataques de DDoS do Anonymous contra o site da Cientologia vêm da pesquisa da ArborNetworks, juntamente com os documentos judiciais relacionados com o caso de Brian Mettenbrink; esses documentos fornecem, entre outras coisas, a data em que a Cientologia contratou a Prolexic Technologies.

Dados sobre a ferramenta LOIC vêm de numerosos artigos on-line sobre o aplicativo da web, capturas de tela da interface, notícias do site de tecnologia Gizmodo e pesquisas da Imperva, empresa de segurança em TI. Dados sobre Praetox baseiam-se no próprio site do programador, http://ptech.50webs.com/, que parece ter sido criado em 2007, mas foi abandonado em 2009 ou 2010. O

surgimento de NewEraCracker como outro programador a desenvolver LOIC vem de informações obtidas no GitHub, serviço de hospedagem de projetos de software com base na web.

O comentário de que a Time Warner lucrava com a máscara de *V*

de vingança vem de um artigo de agosto de 2011 no blog Bits do *The New York Times*.

O exemplo de um tópico de canal no #marblecake veio de um *chatlog* fornecido pela Backtrace Security, de Jennifer Emick, por meio de registros obtidos de um vazamento entre os organizadores do Chanology.

A grande maioria dos dados sobre Brian Mettenbrink vem de uma entrevista por telefone realizada com ele em 16 de dezembro de 2011, bem como de documentos do tribunal e de uma transcrição do FBI, ambos publicados no site Partyvan. A fonte de alguns detalhes extras é um arquivo iniciado quando Mettenbrink escaneou e carregou uma página com sua carteira de motorista e foto, junto com o cartão de um dos agentes do FBI que o visitaram, no WhyWeProtest.net, bem como os comentários nesse tópico tecidos por Mettenbrink e outros. Mettenbrink foi proibido de usar a internet por um ano após cumprir sua sentença de prisão e, no momento da redação deste texto, ainda precisava receber e-mails por meio de um amigo.

Capítulo 6: Guerra civil A grande maioria dos dados sobre as experiências de Jennifer Emick é derivada de entrevistas por telefone com a própria Emick, bem como de algumas entrevistas conduzidas por mensagens de texto no Skype. Dados extras sobre os métodos de intimidação usados pelos representantes da Cientologia contra manifestantes anônimos vêm do testemunho de Emick, Laurelai Bailey, diversos relatórios da web e vídeos do YouTube.

Dados sobre a vida e as experiências de Laurelai Bailey (ex-Wesley Bailey) vêm de entrevistas por telefone com a própria Bailey, juntamente com várias discussões realizadas por Internet Relay Chat e bate-papo textual via Skype.

Os dados sobre “protestos simultâneos em todo o mundo em 10 de fevereiro” vêm dos próprios testemunhos de Bailey e Emick, assim como de vários posts de blogs que relataram os eventos mais tarde. Dados sobre reproduzir uma versão em áudio do OT3 nos protestos vêm do testemunho de Laurelai Bailey, bem como do artigo do *Der Spiegel*, “Tom Cruise and the Church of Scientology”,

publicado em 28 de junho de 2005.

O detalhe sobre uma suposta lista de “desertores da Cientologia assassinados” baseia-se originalmente em conversas com Jennifer Emick, que também me conduziram a discussões no painel de mensagens antiCientologia ocmb.xenu.net, também conhecido como Operação Clambake. Alguns militantes desse painel, por exemplo, acreditam que o antigo cientologista Ken Ogger, encontrado morto em sua piscina em 29 de maio de 2007, foi assassinado.

A descrição do Chanology como “ativismo puro” vem de entrevistas com vários participantes nas invasões e protestos, incluindo Emick, Laurelai Bailey e um organizador anônimo do Chanology, com pontos de vista distintos sobre se a guinada rumo ao ativismo era uma coisa boa ou não. A noção de que a Cientologia “parou de sair para interagir”, ou seja, parou de responder de modo defensivo às ações burlescas do Anonymous, baseia-se no depoimento de Bailey e Emick, bem como em vários fóruns on-line em que se discute o Chanology, como o WhyWeProtest.net.

Os arranca-rabos entre os operadores de redes de IRC, incluindo a frase “Você não tem nem ideia de com quem está se metendo”, baseiam-se no depoimento de Emick, e as rusgas também são narradas em detalhes no site principal do Partyvan. Dados sobre o litígio da Cientologia contra Gregg Housh são provenientes de várias notícias publicadas na mídia, inclusive um artigo de outubro de 2008 no *The Inquirer*, intitulado “Anti Scientology Activist Off the Hook. Sort of”. A perspectiva da Cientologia sobre receber “ameaças de morte” é originária de um vídeo da CNN de maio de 2008, no qual John Roberts, da rede de notícias, entrevistou um porta-voz da Cientologia que alegou que o Anonymous estava “aterrorizando a igreja”.

Dados sobre a forma como Emick “expôs” o nickname de Bailey on-line, Raziel, levando à desavença entre as duas, vêm de relatos de Emick e Bailey.

As informações sobre SWATar uma casa provêm do testemunho de Emick, bem como de entrevistas com William, que me direcionou a sites que mostravam os passos necessários para mandar a SWAT até a casa de alguém.

Dados sobre a primeira reunião on-line do Laurelai com Kayla provêm essencialmente das entrevistas com Bailey. O contexto extra sobre hackers transgênero vem de e-mails trocados com Christina Dunbar-Hester, Ph. D.,

professora adjunta em Estudos Femininos e de Gênero, em Rutgers, a Universidade Estadual de Nova Jersey.

Capítulo 7: FOGO FOGO FOGO FOGO

O parágrafo introdutório, que sugere que o Anonymous ficou quieto entre o Projeto Chanology em 2008 e o caso WikiLeaks no final de 2010, vem de entrevistas com vários protagonistas, incluindo Jake Davis, Jennifer Emick, Laurelai Bailey, e conversas com outros Anons, juntamente com a minha própria observação de uma queda na cobertura de notícias sobre o Anonymous entre essas datas.

A entrevista com Girish Kumar, da Aiplex, mencionada no início deste capítulo é originária do artigo publicado em 8 de setembro de 2010, "Film Industry Hires Cyber Hitmen to Take Down Internet Pirates", no *Sydney Morning Herald*. Declarações semelhantes de Kumar são citadas no artigo publicado no site TorrentFreak.com, intitulado "Anti-Piracy Outfit Threatens to DoS

Uncooperative Torrent Sites", em 5 de setembro de 2010. Não está claro se Kumar ou a Aiplex foram algum dia processados por desferir ataques de DDoS; não existe nenhum relato de imprensa desde que essa insinuação foi veiculada.

Dados sobre a discussão da Aiplex no *b* e, em seguida, sobre a criação de um canal de IRC para coordenar um ataque foram provenientes de uma entrevista on-line com o hacker Tflow em abril de 2011 e do artigo do TorrentFreak.com "4chan DDoS

Takes Down MPAA and Anti-Piracy Websites". Coligi parte do contexto sobre os ataques em uma cronologia dos acontecimentos postada no site Partyvan.info. A história de que sectários do Anonymous foram recrutados entre redes de IRC, juntamente com os nomes dos principais canais de IRC, também se originou da entrevista com Tflow. Dados extras sobre os ataques contra a Aiplex e contra a MPAA baseiam-se em outros artigos on-line, como o do TechCrunch, intitulado "RIAA Goes Offline, Joins MPAA as Latest Victim of Successful DDoS Attacks", de setembro de 2010, e um post de blog da empresa de segurança de TI, Panda Labs, "4chan Users Organize Surgical Strike Against MPAA", publicado em 17 de setembro de 2010.

Dados sobre a suposta idade e localização verdadeiras de Tflow têm como fonte o posterior anúncio (em julho de 2011) de sua prisão pela Polícia Metropolitana

do Reino Unido. A descrição de que ele era discreto e “nunca falava sobre sua idade ou história pessoal” vem de discussões com outros hackers, bem como das minhas próprias observações de Tflow em entrevistas, em salas de bate-papo com os outros, bem como em registros de bate-papo vazados. Dados sobre o modo pelo qual Tflow abordava as pessoas em canais de IRC com conhecimento mais técnico do que ele e a maneira como o grupo transformou a Copyright Alliance em um repositório de material pirateado vêm de uma entrevista com Tflow, e também de uma reportagem publicada em setembro de 2010 com o título “Wave of Website Attacks Continues – Copyright Alliance Targeted”, no site Skyck.com. Dados sobre os ataques a Gene Simmons e outros ataques de DDoS vêm de várias notícias on-line, enquanto a noção de que a campanha havia “entrado em hiato” vem do testemunho de Tflow e Topiary. Tflow alegou que o ataque de injeção de SQL contra o copyrightalliance.org foi o primeiro desse tipo sob a bandeira do Anonymous, embora seja possível que ataques semelhantes tenham sido realizados durante o Chanology.

Entre as observações técnicas que Tflow viu no canal #savethepb e o levaram a colaborar com indivíduos mais qualificados, textualmente: “O LOIC não sobrecarrega seus alvos com pacotes. É

uma questão de inundar a porta 80. A maioria dos servidores de web não consegue lidar com uma vasta quantidade de conexões abertas”.

O relato sobre a criação da rede de IRC AnonOps vem de entrevistas com Jake Davis, Tflow e outro importante organizador do AnonOps, bem como da página “History” no site do AnonOps: AnonOps.pro/network/history.html.

Lá,

os

organizadores descrevem o original “plano astuto” do final de 2010, acrescentando que eles haviam imaginado: “Que tal um navio para Anons, por Anons?”.

O testemunho de Topiary sobre primeiro “conferir” a Operação Vingança e então ficar sabendo sobre o suicídio de seu pai veio de entrevistas com ele mesmo.

Referências ao WikiLeaks e ao vazamento de 250 mil cabogramas diplomáticos baseiam-se numa grande diversidade de notícias de importantes órgãos de

comunicação publicadas em novembro e dezembro de 2010, como o artigo de 28 de novembro do *The Guardian*, intitulado “How 25,000 U.S. Embassy Cables Were Leaked”, além da reportagem da *New York Magazine*, “Bradley Manning’s Army of One”, publicada em 3 de julho de 2011. A afirmação de que a equipe do Ministério de Relações Exteriores foi impedida de visitar o site do WikiLeaks veio de minhas discussões com uma fonte anônima do referido ministério. A descrição do ataque de The Jester contra o WikiLeaks baseia-se em vários relatórios de notícias, como “The Jester Hits WikiLeaks Site with XerXeS DoS Attack”, da Infosec Island, publicado em 29 de novembro de 2010, bem como no testemunho de Topiary e em referências nos registros de bate-papos vazados. O relato sobre o posterior veto de serviços de financiamento por PayPal, MasterCard e Visa ao WikiLeaks vem de uma série de notícias dos principais órgãos de comunicação.

Dados ao longo deste capítulo sobre as discussões que aconteceram no canal #command do AnonOps – por exemplo, primeiro mirando o PayPal para angariar publicidade; nomes de operador como Nerdo, Owen e Token; ou a colaboração com os botmasters Civil e Switch – originalmente tiveram Topiary como fonte, que havia sido convidado para o canal e era amigo de vários operadores da IRC AnonOps. Boa parte dessas informações foi corroborada por relatos na mídia e por postagens de blog feitas pelo pesquisador Sean-Paul Correll, da Panda Securities, que rastreou minuciosamente os ataques contra o PayPal. Embora Correll estivesse em licença de saúde da Panda Securities durante a maior parte de 2011 e, portanto, não disponível para entrevistas, um de seus colegas me enviou dados adicionais, nunca antes publicados, sobre suas conversas via IRC com o botmaster Switch.

Os nomes de operador Peter, Nerdo, Token e Fennic foram associados com nomes e rostos verdadeiros quando os quatro jovens acusados de crimes cibernéticos sob esses nomes compareceram perante o tribunal de Westminster, em 7 de setembro de 2011: Peter David Gibson (acusado de crimes de computador sob a alcunha de Peter), Christopher Weatherhead (acusado de crimes sob o apelido Nerdo) e Ashley Rhodes (Nikon_elite). Por ser menor de idade, o verdadeiro nome do jovem de dezessete anos conhecido como Fennic não pode ser revelado por razões jurídicas. Mais dados, como o apelido de BillOReilly, vieram de capturas de tela da IRC AnonOps publicadas na Encyclopedia Dramatica.

Dados sobre o número de pessoas se aglomerando na IRC

AnonOps durante os ataques contra o PayPal e o MasterCard foram originados na pesquisa de Sean-Paul Correll, assim como no depoimento de Topiary um ou dois meses após os ataques.

Diálogos do canal público de IRC #OperationPayback, tais como “Acha que este é o começo de algo grande?”, têm como fonte uma base de dados on-line dos registros de bate-papos do AnonOps, de 8 de dezembro de 2010, que pode ser pesquisada aqui: http://blyon.com/Irc/.

Conteúdo do folheto digital com instruções para utilizar o LOIC foi obtido diretamente do folheto, ainda disponível on-line. A mensagem de LOIC para os servidores do PayPal foi citada no artigo da Ars Technica “FBI Raids Texas Colocation Facility in 4chanDDoS Probe”, publicado no final de 2010; a data exata não consta no artigo on-line, que menciona as entradas de registro numa solicitação de pesquisa pelo FBI.

A noção de que os operadores provavelmente não queriam a atenção pública voltada aos botnets porque isso poderia levar à pressão das autoridades vem de uma conversa com Gabriella Coleman, acadêmica especializada no Anonymous.

Dados sobre Ryan e o uso de seu botnet na OpItaly e sobre a manipulação de números provêm do depoimento de Topiary.

Informações sobre as catorze pessoas detidas por usar o LOIC

contra o PayPal vêm de notícias de amplo alcance, incluindo a reportagem do *Financial Times:* “FBI Arrests 14 Suspects in PayPal Attack”, publicada em 20 de julho de 2011. Os detalhes sobre a saúde mental de Ryan originam-se do testemunho de seu advogado, Ben Cooper, que afirmou numa audiência no tribunal, em 25 de junho de 2011, que seu cliente tinha sido diagnosticado com síndrome de Asperger, desde sua prisão.

Uma nota sobre mentir para a imprensa: os seguidores do Anonymous mentiram para mim em entrevistas? Às vezes, sim. Eu estava ciente de que isso estava acontecendo? Sim, embora eu admita que nem sempre desde o princípio. Ao longo do tempo, se eu não tinha certeza de um ponto importante, procurava corroborar com outras fontes. Um exemplo é o caso das declarações apresentadas como fato neste livro. Minha postura em relação aos Anons que estavam mentindo para mim era simplesmente dar corda para suas histórias, agindo como se estivesse impressionada com o que diziam, na esperança de

provocar mais informações que mais tarde eu pudesse confirmar.

Assinalei certas passagens neste livro com a palavra “alegou” – por exemplo, uma pessoa “alegou” que a história é verdadeira. Porém, nem todo mundo no Anonymous e no LulzSec mentia o tempo todo, e certas fontes fundamentais se revelaram mais confiáveis que outras. Minha tendência foi dar mais atenção a essas fontes mais confiáveis, principalmente Jake Davis.

Tflow criou o canal #reporter para AnonOps, de acordo com Topiary. Alguns diálogos que se referem ao canal #over9000 vêm dos registros vazados do canal #HQ.

Capítulo 8: Tiros que saíram pela culatra A maioria dos dados neste capítulo sobre os problemas com LOIC

vem de entrevistas on-line e presenciais com um programador e antigo sectário do Anonymous que prefere não ser identificado.

Descrições adicionais de IRC, tais como os tópicos na parte superior dos canais de bate-papo, vêm de minhas próprias observações ao visitar a rede de bate-papo e de boatos sobre “Feds” espreitarem a rede, que foram mencionados por Topiary e por outros Anons com quem ocasionalmente conversei, bem como de artigos on-line sobre o uso geral do IRC e do papel dos operadores, como “The IRC Operators Guide”, no site irchelp.org.

Alguns diálogos sobre a legalidade do uso do LOIC provêm do banco de dados on-line dos registros de bate-papo do AnonOps: http://blyon.com/Irc/. Estatísticas extras sobre o número de pessoas usando o LOIC e o IRC AnonOps podem ser encontradas no Pastebin (http://pastebin.com/qQgxtKaj) e na seção sobre a Operação Vingança, no site opensecuritylab.org. Detalhes adicionais baseiam-se no artigo “Behind the Scenes at Anonymous’

Operation Payback”, publicado no final de 2010 (o artigo não menciona a data exata da publicação).

Houve uma ampla gama de notícias sobre a detenção de Martijn “Awinee” Gonlag, incluindo “They’re Watching. And They Can Bring You Down”, publicada no *Financial Times* em 23 de setembro de 2010.

Com relação à frase sobre o uso de LOIC por trás de “software que permite o

anonimato”: usuários não podem disparar a ferramenta escondidos atrás de um proxy http, pois seus “pacotes” atingiriam o seu próprio proxy, deixando-os off-line; então era VPN ou nada.

Dados sobre as investigações do FBI na Operação Vingança se originaram em parte de um artigo no blog ThreatLevel, da *Wired*, intitulado “In ‘Anonymous’ Raids, Feds Work from List of Top 1,000 Protesters”, publicado em 26 de julho de 2011. Além disso, dados sobre o contato inicial entre o PayPal e os agentes do FBI, junto com a revelação de mil endereços IP em um pen-drive USB, são provenientes de um mandado de detenção do FBI apresentado em 15 de julho de 2011 e disponível on-line.

A citação de Owen “Switch está praticamente em uma lista de pessoas vigiadas que se aparecerem devem levar chumbo” vem de capturas de tela da sala de bate-papo #InternetFeds feitas pelo jornalista freelancer Matthew Keys, que me foram enviadas por email por Keys no início de 2011. Keys foi convidado a observar o desenrolar dos fatos no InternetFeds de dezembro de 2010 a janeiro de 2011. Ele usou o apelido AESCracked.

Dados sobre os ataques de DDoS no IRC AnonOps e dados sobre a Operação Leakspin e a Operação Leakflood vêm de testemunhos de sectários do Anonymous, inclusive Topiary, e de vários posts de blogs, notícias e reportagens. O relato sobre a pulverização de operações, tais como os ataques de DDoS contra o site de Sarah Palin e contra os sites do governo venezuelano, baseiam-se em diversas notícias em sites como o blog da Panda Security, ABCNews.go.com, e KnowYourMeme.com.

Dados sobre o canal #InternetFeds gradativamente usurpar do canal #command a função de núcleo organizacional popular entre os hackers do Anonymous vêm de Topiary, Kayla e dois outros hackers que estavam no canal. Descrições adicionais dos diálogos e do conteúdo das discussões no canal vêm de dezenas de capturas de tela fornecidas por Matthew Keys.

Capítulo 9: O revolucionário Pelo menos duas pessoas corroboraram que Tflow foi o primeiro a convidar Sabu ao canal #InternetFeds; Sabu também alegou isso.

Dados sobre os pontos de vista de Sabu provêm de dezenas de entrevistas on-line que realizei com ele tanto antes quanto depois de sua prisão pelo FBI, em 7

de junho de 2011. Minhas entrevistas por telefone com Monsegur forneceram perspectivas em relação ao seu sotaque, seu modo de falar, os sons de fundo que ouvi enquanto conversava com ele e a sua habilidade para mentir e manipular. Às vezes elas produziram pouco no que tange a perspectivas confiáveis, já que as entrevistas por telefone aconteceram depois de ele ter começado a colaborar com o FBI e ter sido encorajado a passar informações desencontradas a jornalistas. Dados adicionais sobre sua vida, educação e o endereço de Sabu provêm de uma série de documentos judiciais que foram publicados após o FBI revelar que ele estivera agindo como informante a partir de 7 de junho de 2011. Além disso, utilizei como fonte sobre alguns dados uma série de três reportagens da Fox News sobre Monsegur, publicada em março de 2012, uma das quais intitulada "Inside LulzSec, a Mastermind Turns on His Minions". Outra fonte útil para confirmar dados pessoais sobre Monsegur foi o artigo do *The New York Times*, intitulado "Hacker, Informant and Party Boy of the Projects", publicado em 8 de março de 2012, no qual os repórteres entrevistaram vizinhos do Monsegur para montar uma imagem do homem. Entrevistas com fontes próximas a Hector Monsegur e à investigação do FBI também contribuíram com as informações deste capítulo.

Dados sobre o incidente com o chefe da segurança na escola de ensino médio de Monsegur se basearam em um texto supostamente escrito por Sabu em 14 de agosto de 2001 contendo todas as suas habituais características estilísticas e verbais. Foi publicado via Pastebin em 7 de junho de 2011 (o dia de sua prisão) e também me enviado por e-mail por uma fonte. Texto completo aqui: http://pastebin.com/TVnGwSmG.

Os dados sobre os estágios de Monsegur quando adolescente foram originados de um arquivo de web do site iMentor de agosto de 2002, que listava Monsegur como membro da equipe e fornecia uma curta biografia que mencionava suas passagens no NPowerNY Technology Service Corp e no projeto Low-Income Networking and Communications (LINC), no Welfare Law Center.

O texto integral de The Hacker Manifesto escrito por Mentor pode ser encontrado

aqui:

http://www.mithral.com/~Beberg/manifesto.html. Troquei emails com Lloyd "o Mentor" Blankenship para confirmar detalhes sobre a redação desse texto em

1986.

Sabu/Monsegur forneceu-me links que ainda mostram a mensagem de deface que ele publicou nos sites do governo porto-riquenho. Dados adicionais sobre a guerra cibernética entre EUA e China, na qual Sabu se envolveu, foram corroborados por notícias como “It’s (Cyber) War: China vs. U.S.”, publicada na *Wired* em abril de 2001, e “China-U.S. Cyber War Escalates”, publicada pela CNN em 1º de maio de 2001. Dados adicionais sobre Monsegur e suas tentativas de iniciar um grupo para programadores locais em 2002 também vêm de um arquivo de “dox” postado por um pesquisador do ramo de segurança apelidado Le Researcher, que colou diversas capturas de tela de e-mails, mensagens de deface e posts de fóruns em http://ceaxx.wordpress.com/uncovered/. A mensagem de Sabu no AnonOps, na qual ele pergunta como encontrar John Abell, da *Wired*, veio do banco de dados on-line http://blyon.com/Irc/.

Dados sobre os protestos contra a corrupção na Tunísia foram amplamente divulgados no fim de dezembro de 2010 e início de janeiro de 2011, e dados sobre a campanha de phishing do governo, destinada a espionar os potenciais dissidentes, foram publicados pela Al Jazeera e Ars Technica. Sites censurados normalmente mostravam a mensagem “Error 404: page not found”. Um site oficialmente bloqueado mostrava a mensagem: “Error 403”, por isso o uso de 404 sugeria censura não oficial. Um jornalista e blogueiro, Sofiene Chourabi, alegadamente tinha sido impedido de acessar seu Facebook; seus 4.200 amigos também foram hackeados. Outros jornalistas alegaram que seus blogs tiveram os conteúdos integralmente excluídos, e suspeitavam de que a Agência de Internet da Tunísia estava por trás disso. Muitos tunisianos também alegaram serem incapazes de mudar suas senhas no Facebook. A operação de phishing era sofisticada, atingindo vários alvos de alto perfil em um único dia, e executada por um código de malware, de acordo com a Al Jazeera, que cita “fontes diversas”. Steve Ragan, do TechHerald, relatou ter visto exemplos do script incorporado e do novo código fonte injetado no Gmail, Yahoo e Facebook, confirmando com quatro diferentes especialistas que o código estava “desviando credenciais de login”

e que “plantio de código nesta escala só podia ter vindo de um ISP

(*Internet Service Provider*)”.

Dados sobre o script antiphishing desenvolvido por Tflow estão disponíveis

no

site

de

compartilhamento de

scripts

http://userscripts.org, sob o nome de usuário “internetfeds”. Sabu, Topiary e outro antigo componente do Anonymous contaram que Tflow escreveu originalmente o script. Tflow tinha escrito um conector ao navegador JavaScript que eficazmente desativava o código Java acrescentado pelo governo e afastava os usuários de internet da Tunísia para longe de seus servidores de phishing (em essência, sites falsos do Gmail, Yahoo e Facebook) e de volta aos hospedeiros originais e verdadeiros. Os internautas da Tunísia primeiro tinham de instalar o complemento Greasemonkey para o Firefox. Depois era só uma questão de abrir o Firefox, entrar em Ferramentas, depois em Greasemonkey e em New User Script, para colar o código. Tendo clicado em “OK”, os tunisianos poderiam em um minuto ou dois acessar Facebook, Twitter, Blogger, Gmail e Yahoo sem expor seus dados de login.

Eu baseei a história sobre Sabu ter controlado remotamente o computador de um tunisiano para desfigurar o do primeiro-ministro do país em entrevistas com o próprio Monsegur, realizadas em abril de 2011. Ainda não está claro exatamente como Sabu atacou o DNS tunisiano, mas um perito que o conhecia sugere que ele pode ter usado um ataque chamado smurf para derrubar os servidores de domínio do governo. Isso se refere a um tipo exclusivo de negação de serviço (DoS, sem o d de “distribuída”) que pode ser realizado a partir de um único computador. Em vez de usar um botnet, utiliza servidores com espaço e velocidade significativos para transferir os dados de lixo eletrônico. Um ataque smurf, especificamente, precisa de servidores de transmissão. Ele envia uma solicitação ping para um ou mais dos servidores, comunicando (falsamente) que o endereço IP do remetente é o alvo. No jargão dos hackers, eles estão enviando “pacotes falsos”. O servidor de transmissão, então, aciona toda a sua rede para responder à máquina alvo. Um computador por si só pode enviar talvez no máximo o equivalente a 500 megabytes de pacotes, mas o ataque smurf permitiu a Sabu amplificar ao equivalente de 40 gigabytes. Uma captura de tela da

mensagem de deface carregada no site do primeiro-ministro Ghannouchi está disponível on-line.

Capítulo 10: Conhecendo a ninja Os parágrafos introdutórios deste capítulo são provenientes de entrevistas on-line com Topiary. Sua mensagem de deface ao governo

da

Tunísia

é

ainda

visível

aqui:

http://pastehtml.com/view/1cw69sc.html. O assunto sobre ciberataques contra os governos de países como Líbia, Egito, Zimbábue, Jordânia e Bahrein veio do depoimento de Topiary e foi corroborado por várias notícias e reportagens on-line. Eu mesma vi o deface do site do Fine Gael e o confirmei por telefone com um porta-voz da imprensa do partido político irlandês.

A descrição do estilo de redação de Kayla, que inclui carinhas sorridentes e interjeições “lol”, baseia-se em minhas próprias observações, bem como nas observações de membros do Anonymous. Sua visão de a hackeagem ser um vício vem de uma entrevista posterior, on-line.

A votação on-line de Johnny Anonymous foi descrita para mim em uma entrevista por Skype com o próprio Johnny Anonymous, realizada em 7 de março de 2011.

Descrições das obsessivas tentativas de Kayla em manter sua identidade em segredo são provenientes de entrevistas com Kayla, conduzidas em grande parte por e-mail, em março de 2011. Fui apresentada a Kayla pela primeira vez (e a Sabu, Tflow e os outros que mais tarde comporiam o LulzSec) por Topiary. Dados sobre as experiências de vida de Kayla e sobre ser hackeada por um homem que “gritou” pelo telefone com ela vieram de entrevistas também

realizadas em março de 2011. O envolvimento de Kayla na hackeagem do Gawker, relatado pelo próprio Gawker, foi mencionado em uma entrevista via Internet Relay Chat com a hacker em 23 de maio de 2011, na qual descreveu em detalhes como ela e um grupo de amigos on-line no canal de IRC #gnosis executaram hackeagens ao longo de vários meses. Confirmação sobre a existência da rede de IRC “tr0ll” de Kayla vem de páginas da web arquivadas e posts no Pastebin que mencionam a rede, e também de uma fonte que prefere não ser identificada. Além de me contar sobre a “vulnerabilidade nos servidores que hospedam o Gawker.com”, Kayla explicou que ela e os outros hackers conseguiram obter acesso de raiz para os servidores quando depararam com o nome de usuário e senha de raiz do MySQL no código fonte de um dos scripts do site – então perceberam que o Gawker.com permitia conexões remotas do MySQL. Essas são as características essenciais que lhes deram acesso quase irrestrito ao banco de dados do site.

A vulnerabilidade que Kayla encontrou no site das Nações Unidas foi mostrada para mim em um bate-papo de IRC com Kayla no verão de 2011.

Diálogos do #InternetFeds vieram de capturas de tela do canal de IRC privado enviadas a mim por Matthew Keys.

Quanto à rede de IRC do WikiLeaks, onde Kayla se encontrou pela primeira vez com q, qualquer um pode acessá-la por meio de um navegador no chat.wikileaks.org. Várias fontes chegadas ao WikiLeaks confirmam que q (nome real conhecido, mas não divulgado aqui) habitualmente mentia para asseclas e que ele e Assange eram íntimos, um “enteado para Assange”, conforme uma fonte.

Capítulo 11: O rescaldo Os parágrafos de abertura deste capítulo são provenientes principalmente de entrevistas por telefone com Aaron Barr. Vi no Reddit o comentário sobre os filhos de Barr que levou ele e sua esposa a fugir temporariamente de sua casa.

Dados sobre a HBGary Inc. ter contratado o escritório de advocacia Zwillinger & Genetski são provenientes de entrevistas por telefone com os advogados Marc Zwillinger e Jennifer Granick. O detalhe referente a senhas de Ted Vera e de Greg Hoglund veio de entrevistas com Topiary.

As posteriores citações de Aaron Barr são provenientes de uma entrevista por

telefone com ele, que ocorreu mais cedo naquela manhã de segunda--feira, apenas horas depois do ataque dominical durante o Super Bowl. A carta aberta da HBGary é ainda visível aqui: http://www.hbgary.com/open-letter-from-hbgary.

Os hackers armazenaram os números de segurança social dos funcionários da HBGary e outros dados em um aplicativo de texto de web privado chamado Pirate Pad, que qualquer um do grupo poderia editar. Mais tarde, o documento on-line foi eliminado.

Dados roubados como esses acabam juntando poeira em algum lugar na nuvem, ou no computador de alguém – esquecido até que uma detenção o transforme em prova.

O relato de Kayla ter informado Laurelai Bailey sobre o ataque contra a HBGary e então a convidado ao #HQ (canal de IRC

privado frequentado pelo grupo que atacou a empresa) tem como fonte entrevistas com Bailey. Dessas entrevistas também surgiram dados sobre as controversas propostas de Barr para a Hunton & Williams. Antes de deparar com a importantíssima conexão de Barr com o WikiLeaks, Laurelai primeiro teve de exportar os emails publicados de Barr a um cliente de e-mail chamado Thunderbird e depois transferi-los ao Gmail. Isso a permitiu vasculhar os e-mails usando palavras-chave como “WikiLeaks”.

A noção de que Topiary, Sabu e Kayla não sabiam sobre as propostas antiWikiLeaks nos dias imediatamente após o ataque foram transmitidas a mim por Topiary, a quem eu entrevistava na época. Eu também estava seguindo os desdobramentos após o ataque e percebendo que o pequeno grupo dele executava uma varredura nos e-mails de Barr, procurando algo controverso, antes de Laurelai avistar o veio principal.

Diálogos do grupo na sala #HQ vêm de registros que acabaram vazados por Laurelai via Jennifer Emick (ver Capítulo 14). Dados sobre a publicação dos e-mails da HBGary e trechos de conteúdo foram originados do próprio visualizador da HBGary, em http://hbgary.anonleaks.ru (agora off-line).

Dados da investigação sobre a HBGary (parceiros e contratos militares) realizada pelo congressista americano Hank Johnson foram confirmados em uma entrevista por telefone com Johnson, em 23 de março de 2011. Ouvi pela

primeira vez sobre a investigação em 17 de março, quando, tarde naquela noite, Topiary leu em um artigo da *Wired* dizendo que o deputado Johnson começara a investigar contratos do exército americano com a HBGary Federal, a Palantir Technologies e a Berico Technologies. Logo depois, pelo menos dez democratas da Câmara dos Deputados tinham assinado uma petição para instaurar uma investigação sobre a Hunton & Williams e as três empresas de segurança.

A "crescente sensação de desconforto" entre os hackers vem de observações de suas conversas às vezes paranoicas no #HQ, bem como do testemunho de Topiary, que também foi a fonte da informação sobre as habituais ligações telefônicas com Sabu e a saudação codificada "Aqui é David Davidson". A desconfiança de Sabu em relação a Laurelai fica clara em seus comentários no #HQ, mas também foi corroborada pelo testemunho de Topiary.

Jennifer Emick confirmou que ela estava por trás da conta de Twitter @FakeGreggHoush; isso era um segredo de polichinelo no Anonymous desde que a Backtrace foi doxeada em julho de 2011.

Com base em entrevistas com Emick e Bailey, tentei montar o quebra-cabeça de como e por que Bailey acabou repassando a Emick os registros do canal #HQ.

Parte 2

Capítulo 12: Encontrando uma voz O parágrafo de abertura, descrevendo a popularidade de Topiary no AnonOps, incluindo detalhes como o número de mensagens privadas que ele costumava receber, tem como fonte entrevistas com Topiary, bem como observações de registros de bate-papo, conversas de IRC e estatísticas mostrando o número de vezes que as pessoas o buscavam pelo Twitter. O dado sobre solicitações para atacar vários alvos, como o Facebook, também vem dessas entrevistas. De acordo com Topiary, as pessoas às vezes mandavam e-mails diretos aos seguidores no AnonOps ou enviavam mensagens para certos blogs representativos. Era difícil rastrear o modo como o Anonymous escolhia seus alvos, já que isso muitas vezes era feito de modo caótico e espontâneo, nos bastidores. No entanto, raramente se aceitavam solicitações de alvos sugeridas por pessoas não pertencentes ao Anonymous.

Dados sobre a Igreja Batista Westboro são provenientes de várias notícias, bem como do fascinante documentário de Louis Theroux para a BBC, *The Most Hated Family in America*, que foi ao ar pela primeira vez em 2007. O detalhe de que Nate Phelps acusara de abuso o próprio pai, Fred, origina-se de vários relatos na imprensa, inclusive no site oficial de Nate Phelps, que em sua página de “Biografia” refere-se à “extremista versão de calvinismo” e aos “extremos abusos e punições físicas”

perpetrados pelo pai.

O comunicado de imprensa de 18 de fevereiro anunciando que o Anonymous ia atacar a Westboro – o primeiro anúncio desse tipo – apareceu no AnonNews.org. O dado sobre um operador de IRC

executando uma pesquisa nos canais de bate-papo da rede para encontrar os organizadores baseou-se em entrevistas com Topiary. Operadores de IRC, tanto no âmbito do AnonOps quanto em outras redes, executavam buscas constantes para se manter a par de quaisquer operações estranhas sobre as quais ninguém sabia, como conspirações para derrubar a rede ou discussões inapropriadas sobre pornografia infantil. Às vezes, os trolls criavam um canal pornô infantil para tentar fazer o AnonOps parecer ilegal. Esse era o único tópico de discussão proibido no IRC AnonOps; de resto era permitido tudo. Da mesma forma, falar de hackeagem foi proibido em outras redes, motivo pelo qual Tflow e os outros

adeptos da Operação Vingança migraram de redes como EFnet, Freenode e Quakenode no final de 2010 – esses operadores de IRC não gostavam de pressão.

O comunicado de imprensa sobre o ataque contra a Westboro, escrito por cinco redatores em #philosoraptors, originou-se quando uma pessoa começou a escrevê-lo em seu computador e depois o enviou ao Pirate Pad para que outros pudessem editá-lo.

Começava assim: “Caro Phred Phelps e phraternos amigos do WBC”. Esse comunicado de imprensa seguia mais a linha irreverente e pândega do Anonymous. Continuava dizendo: “Fiquem ligados, e vamos voltar para brincar outro dia. A gente promete”. E acrescentava um aviso em tom de censura: “Para a mídia: se algo é postado no AnonNews, isso não significa que cada Anon concorda”.

Dados sobre o David Pakman Show, o próprio Pakman e a hackeagem da Westboro ao vivo são provenientes de uma entrevista por telefone com Pakman realizada em 18 de novembro de 2011, bem como de entrevistas com Topiary. Comentários feitos por Shirley Phelps-Roper no show do Pakman são provenientes de vídeos do YouTube. Todos os diálogos do show concernentes à hackeagem ao vivo da Westboro baseiam-se no principal vídeo do YouTube com o programa. Os relatos de Pakman e de Topiary divergem sobre quanto Pakman sabia do que estava acontecendo com o site da Westboro durante o programa.

Pakman negou saber que Topiary ou qualquer outro do Anonymous ia atacar o site da Westboro no meio de seu programa.

“Não. Absolutamente não”, afirmou Pakman na entrevista por telefone, realizada cerca de oito meses após o evento.

“Basicamente disseram: ‘Vamos ao seu programa falar sobre isso’.

Foi muito vago. Eu disse: ‘Estou interessado. Você seria capaz de conversar com a Shirley?’, e eles toparam. Entrei em contato com a Westboro... Ambas as partes concordaram. O timing deu certo.”

Hoje, o número de acessos no vídeo da hackeagem ao vivo da Westboro aproximou-se da marca de 2 milhões e é o vídeo mais popular já postado pelo *The David Pakman Show*.

A respeito das mensagens de deface escritas por Topiary: ele as escreveu todas em um programa de edição de texto muito simples chamado Notepad + +. Cada PC tem o Notepad em sua pasta de acessórios, mas o Notepad + + é um programa gratuito melhor que o original no sentido de que permite aos usuários organizar seus documentos em abas, possibilitando-lhes ter vários arquivos abertos. Topiary só tinha de apertar a tecla de seta para a esquerda em seu laptop para obter formatos de texto diferentes, uma lista de links de sites vulneráveis ou outros comunicados de imprensa do Anonymous que ele ainda não tinha lido. Ele tornava todas as mensagens de deface compatíveis com a linguagem HTML

da web, convertendo-as em um site chamado Pastehtml.com. Se Topiary copiava e colava uma mensagem de duzentas palavras diretamente do Microsoft Word, seria provável aparecer no Pastehtml.com com um logotipo do Anonymous muito para a esquerda, ou com espaços estranhos dentro do texto, que ele então teria de mexer no chamado código fonte, os complicados comandos de programação por trás do texto. Escrevê-lo no Notepad + +, por outro lado, significava que o texto era automaticamente "limpo", de modo que, quando fosse convertido em um arquivo HTML, tivesse exatamente o mesmo aspecto on-line do que off-line em seu computador, sem necessidade de ajustes. No total, Topiary produziu aproximadamente dez mensagens de deface para o Anonymous utilizando esse método, e ajudou os outros a produzir mais dez. O uso de um programa simples e o conhecimento básico de Topiary sobre HTML são os motivos pelos quais todas as suas mensagens, que compõem a maioria das desfigurações relatadas pela mídia no primeiro semestre de 2011, aparecem como texto sem formatação sobre um fundo branco.

Capítulo 13: Conspiração (que nos une) Os parágrafos iniciais deste capítulo são provenientes de entrevistas na época (e depois nos meses seguintes em retrospectiva) com Topiary. Sabu e Kayla tinham deixado de lado o ataque à HBGary e não estavam envolvidos na leitura dos e-mails de Barr. Os dois também alegavam ter vidas ocupadas fora do Anonymous e da internet. Em minhas entrevistas por telefone com Sabu, por exemplo, ele era muitas vezes interrompido por pessoas em sua casa e por outras chamadas telefônicas.

Dados sobre a experiência do Barrett Brown escrutinando os emails da HBGary, formando uma equipe de pesquisadores, e sobre sua vida pessoal são derivados de minha entrevista por telefone com Brown, realizada em 24 de novembro de 2011. Dados adicionais sobre suas relações com Topiary e outros Anons vieram de entrevistas com Topiary. Também utilizei como fonte uma gravação de áudio

da entrevista por telefone de Brown com William Wansley, que ele carregou no site de compartilhamento MediaFire.com. Eu havia sido alertada com antecedência sobre a participação na Rádio Payback de Brown, Topiary e WhiteKidney e fiquei tomando notas em tempo real; mais tarde, baixei o arquivo de áudio. Descrevi a transmissão do programa *NBC Nightly News* com Michael Isikoff após assistir ao vídeo on-line. A observação de que os "ossos" de Brown "doeram" por causa da abstinência de Suboxone, juntamente com o ponto sobre sua recaída em Nova York em abril de 2011, foram provenientes de minha entrevista por telefone com Brown. Alguns detalhes extras sobre a Operação Metal Gear e suas pesquisas foram originados em parte do Project PM wiki de Brown, http://wiki.echelon2.org/; em parte, do site do Metal Gear, http://opmetalgear.zxq.net/, antes de ficar fora de uso; e em parte do site da empreiteira Booz Allen Hamilton.

Descrições da opinião geral entre Anons em relação a Brown foram originadas das discussões com um punhado de Anons, inclusive William, bem como de minha observação de comentários relevantes no IRC AnonOps. Brown pensou ter visto uma ligação no interesse da HBGary na licitação de um contrato para vender às forças armadas dos EUA software de gestão de pessoal, tecnologia que essencialmente permitia ao usuário espionar os outros por meio da internet e das mídias sociais.

Detalhes sobre o jovem apelidado de OpLeakS e sua oferta de informações aparentemente explosivas sobre o Bank of America foram provenientes de entrevistas com Brown e Topiary, com dados adicionais provenientes do bankofamericasuck.com, da conta de OpLeakS no Twitter e de várias notícias veiculadas sobre a matéria. E-mails publicados no site de OpLeakS mostravam claramente o nome do funcionário demitido pelo Bank of America que estava "vazando" as informações: Brian Penny.

Ao utilizar o termo "grupo de hacker nerds", Topiary estava se referindo aos grupos de hacker das décadas de 1980 e 1990, alguns dos quais utilizavam imagens de caveira sobre ossos cruzados e geralmente se levavam demasiado a sério.

No Anonymous, não era incomum saltar de uma operação para outra, refletindo às vezes a limitada capacidade de atenção de seus grupos e asseclas. Paralelamente à Operação Metal Gear, havia a Operação Wisconsin, a Operação Eternal Ruin e operações com foco na Líbia e na Itália, cada qual contando com

cerca de duas a doze pessoas envolvidas. No início de 2011, a versão original da Operação Vingança, lançada contra empresas de direitos autorais, voltou para o segundo round, alvejando mais sites relacionados com direitos autorais. Topiary observou, no entanto, que seus proponentes continuavam a mudar de alvo – por exemplo, eles escolhiam o agcom.it como alvo, provocando o disparo de algumas pessoas contra o site, mas fracassavam na intenção de criar ímpeto suficiente para derrubá-lo, fornecendo aos demais um motivo para passar para outra coisa. A troca constante de alvos é uma das razões cruciais para a Operação Vingança ter minguado para cerca de cinquenta pessoas em outubro de 2010 e quase definhar – até o WikiLeaks aparecer meio por acaso e milhares de pessoas de repente embarcarem na operação.

Capítulo 14: Backtrace ataca Os parágrafos introdutórios deste capítulo são provenientes de entrevistas com Jennifer Emick, com alguns dados extras – incluindo o nome do seu grupo no Skype, o Treehouse – vindo de blogs relacionados ao Anonymous.

Dados sobre as prisões na Holanda e na Grã-Bretanha baseiam-se em diversos noticiários da grande mídia. A Polícia Metropolitana do Reino Unido anunciou em 27 de janeiro que havia prendido cinco pessoas em batidas matinais por todo o país. De acordo com um relatório no The TechHerald da época, os suspeitos supostamente foram rastreados com “pouco mais do que os registros do servidor e confirmação de seu provedor de acesso”.

Descrições

do

que

Emick

estava

encontrando

no

DigitalGangster.com baseiam-se originalmente em informações de Emick corroboradas por minhas próprias observações do site, especialmente na seção

“About”. Também entrevistei uma participante do fórum apelidada de Jess, amiga íntima da mulher de 23 anos de Seattle que frequentava o fórum e atendia pelo nome de Kayla, cujo nome verdadeiro é Kayla Anderson. Jess confirmou que a mulher não é a mesma Kayla do LulzSec, embora ela e sua amiga se julgassem conhecidas do hacker de codinome Xyrix. Provavelmente era uma coincidência, ela acrescentou, que Xyrix estivesse ligado a uma Kayla de DigitalGangster.com e à Kayla do LulzSec. Emick duvidou desse relato quando eu o transmiti a ela em novembro de 2011, e acreditava que havia uma conexão entre as duas Kaylas.

Nesse meio-tempo, aliás, Corey “Xyrix” Barnhill negou ser Kayla, tanto por meio de comentários em notícias on-line sobre Kayla quanto em e-mails enviados diretamente a mim. A Kayla do AnonOps também me disse, junto com alguns membros do Anonymous, que deixou correr o boato de que ela era Xyrix, porque ajudava a ocultar sua verdadeira identidade.

As descrições sobre YTCracker e a história sobre a hackeagem do DigitalGangster.com tiveram como fonte entrevistas por telefone com o próprio Bryce “YTCracker” Case, além minhas observações sobre a mensagem de deface postada em seu site quando Corey “Xyrix” Barnhill, Mike “Virus” Nieves e Justin “Null” Perras tinham, de acordo com Case, alterado o DigitalGangster.com para apontar contra seus próprios servidores.

Durante minha própria observação do DigitalGangster.com, vislumbrei posts anunciando empregos que exigiam como requisitos a habilidade de hackear sites por meio de injeção de SQL, roubar bancos de dados de nomes e endereços de e-mail ou apenas roubar endereços e enviá-los para os spammers. Um banco de dados com senhas valia mais, já que os spammers poderia depois enviar spam a partir de endereços legítimos.

Ocasionalmente um tópico começava com um post procurando “freelancers” capazes de programar em C, Objective-C, C#, VB, Java e JavaScript. Um post de junho de 2010 tinha o título “DGs [*Digital Gangsters*] in Washington? Be my mail man in the middle”, seguido de: “Aqui está como funciona. Uma entrega é enviada ao seu endereço, você abre o pacote remover item, reenvia o item para mim em um novo destinatário com um falso endereço de retorno.

Quando o item chegar, você é pago. Interessado?”.

A descrição de Jin-Soo Byun originou-se de entrevistas com Jennifer Emick e Laurelai Bailey; a observação de que Aaron Barr estava ajudando a investigação dela baseou-se numa entrevista com Barr. O detalhe sobre Emick ter configurado a investigação inicial da Backtrace sobre o Anonymous e, em seguida, rastreado "Hector Montsegur" (sic) provém de entrevistas com Emick.

Descrições de alguns defaces de Sabu vêm de capturas de tela fornecidas por ele mesmo e também a partir de um post de blog feito por Le Researcher, ativista antiAnonymous que trabalha com Emick. Outro grupo que inclui Kelly Hallissey, usuária de longa data do EFnet, afirma ter doxeado Sabu em dezembro de 2010 e passado seus dados à Backtrace Security em fevereiro de 2011.

Emick nega isso.

A declaração de Sabu de que ele ia "pegar o carro, ir até a casa [de Laurelai] e perturbá-lo" baseou-se no testemunho de Topiary.

As origens da palavra backtrace apontam para uma das operações mais notória já conduzidas pelo 4chan e pelo Anonymous.

Começou em julho de 2010, quando os usuários do painel *b* do 4chan começaram a trollar uma menina de onze anos de idade chamada Jessica Leonhardt. On-line, ela era conhecida como Jessi Slaughter e se tornou uma pequena "e-celebrity" após carregar vídeos de si mesma em um site chamado StickyDrama. Quando outros usuários do StickyDrama começaram a fazer bullying com Slaughter, ela filmou uma série de revides chorosos, incluindo um em que seu pai bigodudo poderia ser visto por trás de seu ombro com o dedo em riste na direção da câmera e gritando: "Seu bando de punks mentirosos e inúteis! E eu sei de onde vocês vêm! Porque eu fiz um BACKTRACE!". A reprimenda gerou diversos bordões e memes na internet, inclusive "backtrace", "Ya done goofed" e "As consequências jamais serão as mesmas!". Em fevereiro de 2011, Jessi Slaughter tinha sido colocada sob proteção policial e ingressado em uma instituição psiquiátrica. No agosto seguinte, o pai dela morreu de ataque cardíaco, aos 53 anos de idade.

O diálogo entre Topiary, Kayla, Tflow e AVunit, começando com a citação "Todos eles pensam que sou Xyrix!", tem como fonte o debate entre eles realizado em 21 de março de 2011, no canal de IRC privado chamado Seduce. A essa altura, Topiary havia me apresentado a Kayla (com quem eu já havia me

comunicado por email) e foi nessa sala que falei pela primeira vez com AVunit, Tflow e Sabu. A partir daí, organizei entrevistas separadas com cada um deles. O grupo já estava se comunicando uns com os outros em seu próprio canal exclusivo, e o #seduce foi criado com a finalidade de falar comigo e fornecer depoimentos para este livro. O nome Seduce veio da revelação, no final de fevereiro, no registro do bate-papo do #HQ, de que Kayla estaria falando comigo; ela brincou que “Ela escreveu coisas boas sobre nós até agora... ela falou com Topiary. Acho que ele a deixou seduzida”. Mais tarde, ao mudar para um servidor de IRC diferente, o grupo criaria outro canal, chamado #charmy, também para falar exclusivamente comigo. Mais tarde me disseram que Sabu era extremamente cauteloso em falar comigo no canal #seduce em março, e eu observei que ele raramente aparecia na sala ou inventava desculpas para sair. Em 13 de abril de 2011, no entanto, realizamos nossa primeira entrevista real via IRC, e ele se tornou mais comunicativo.

Não está claro se “Christopher Ellison”, o nome associado com AVunit no documento final da Backtrace, estava correto ou não.

Não foi noticiado pela imprensa nem por comunicados da polícia a prisão de alguém conectado ao apelido, e não havia qualquer informação sobre o paradeiro do AVunit real até meados de abril de 2012.

O estudo de François Paget foi publicado em 21 de outubro de 2011, num post de blog da McAfee intitulado “The Rise and Fall of Anonymous”.

O dado sobre o FBI ter entrado em contato Jennifer Emick vem de conversas com Emick. O ponto adicional de que o FBI precisava esperar para confirmar a identidade de Sabu e reunir provas para ameaçá-lo com uma sentença longa baseou-se na reportagem do FoxNews.com, intitulada “Infamous International Hacking Group LulzSec Brought Down by Own Leader”, publicada em 6 de março de 2012.

Laurelai Bailey não tinha sido a única responsável pelo vazamento dos registros.

Menos

prejudicial,

porém

igualmente

constrangedor, foi o vazamento do jornalista de televisão e web freelancer Matthew Keys, que obtivera acesso ao #InternetFeds desde dezembro de 2010 até 6 de janeiro de 2011, quando ele foi banido após membros do canal suspeitarem de ele ter vazado informações ao *The Guardian*. Mais tarde, Sabu alegou que Keys fornecera acesso de administrador ao sistema de publicação on-line do Tribune, seu antigo empregador, em troca da oportunidade de "passear em nosso canal". Keys nega isso.

Uma nota sobre a criação de canais de IRC: geralmente a pessoa que tem a ideia para um canal é quem o cria. Os criadores podem tornar os canais mais seguros pela adição de comandos como +isPu e +k para obter mais controle de quem entra. Às vezes, porém, a melhor maneira de tornar um canal seguro é configurá-lo completamente aberto, sem nenhuma política de convite, e ficar alternando entre diferentes canais a cada um ou dois dias. Tornar um canal "apenas com convite" é "o mesmo que segurar uma bandeira vermelha na frente de um touro", de acordo com AVunit, acrescentando que por esse motivo ele e sua equipe evitavam políticas de apenas com convite. Para encontrar uns aos outros, membros da equipe usavam consultas normais de IRC, verificavam qual canal estava ativo ou apenas digitavam no canal relevante de IRC e retomavam a discussão.

É interessante notar que a própria Backtrace foi objeto de numerosos episódios de doxeagem. Pelo menos desde março de 2011 em diante, alguns adeptos do Anonymous revelaram a identidade dos membros do grupo Backtrace: Jennifer Emick, Byun Jin-Soo e John Rubenstein, publicando seus endereços, números de telefone, alguns dados sobre suas famílias e outros perfis on-line na ferramenta de web Pastebin.

Capítulo 15: Dando um tempo As descrições dos "três modos de responder a uma doxeagem"

foram derivadas de minhas conversas com Topiary e minhas observações sobre o modo com que os asseclas dos Anonymous, como Ryan Cleary, reagiam ao ter suas verdadeiras identidades reveladas. Mais dados sobre o "drama" no Anonymous e a cultura desenvolvida pela confusão de canais no IRC foram provenientes de minhas conversas com membros do grupos e de minhas próprias observações. Os detalhes sobre a ideia de Aaron Barr de penetrar em canais de

codificação privada, bem como a descrição neste capítulo de “No”, baseiam-se em depoimentos de Topiary. Os dados sobre a batida do FBI na casa de Renee Haefer foram provenientes de uma entrevista que Haefer deu ao Gawker para uma reportagem on-line intitulada “An Interview with a Target of the FBI’s Anonymous Probe”, publicada em 11 de fevereiro de 2011. Dados sobre os cinco britânicos presos em 27 de janeiro são provenientes de um comunicado oficial da polícia metropolitana e de notícias veiculadas na mídia.

Os parágrafos detalhando a retirada elaborada de Topiary foram provenientes de entrevistas com ele. Editei substancialmente o registro falsificado para fins de concisão; o registro mencionava que o roteador sem fio de Topiary havia sido deixado ligado. Isso tinha o objetivo de causar ainda mais confusão entre as centenas de usuários habituais do AnonOps, pois os roteadores eram o primeiro item a ser procurado em uma batida policial. A artimanha se mostrou quase sofisticada demais. Uma amiga on-line ficou tão apavorada que tentou entrar em contato com a então namorada de Topiary, uma garota canadense que ele havia conhecido on-line três anos antes. De modo problemático, essa amiga então deixou escapar a outros sobre a existência da namorada de Topiary. Até então, ele havia tentado isolá-la de suas atividades com o Anonymous, de modo que ela não ficasse vinculada como coconspiradora se ele fosse preso. Para corrigir esse problema, ele escreveu outra mensagem falsificada, dessa vez como se fosse a namorada, insinuando que ela subitamente estava com ciúmes da amiga preocupada. A sugestão distraiu o suficiente a moça, que não suspeitou da verdade: que Topiary não tinha sido preso, mas estava dando um tempo do Anonymous.

Citações do comunicado de imprensa do Anonymous dirigido à Sony foram originadas do próprio comunicado de imprensa, ainda disponível em AnonNews.org. Dados sobre o envolvimento de William na OpSony provêm de entrevistas com ele. William também me mandou via e-mail um link sobre parte do trabalho da SonyRecon, inclusive dados do diretor executivo da Sony, Howard Stringer, como seu endereço antigo e atual em Nova York, o nome de sua esposa, os nomes de seus filhos e o nome da antiga escola de seu filho. O post ainda está on-line em JustPaste.

Os dados sobre o processo da Sony contra George Hotz vêm de vários relatos da grande imprensa.

“Irritando milhões de gamers mundo afora” é a minha interpretação de miríade

de comentários indignados em fóruns de gamers, assim como no site oficial da PlayStation Network, que contém declarações mostrando que a PSN é utilizada por dezenas de milhões de pessoas.

A carta de oito páginas da Sony para a Câmara dos Deputados dos EUA, datada de 3 de maio de 2011, está visível no Flickr.

A publicação de 653 apelidos e endereços IP no AnonOps foi colada em um documento público on-line, que eu vi e que foi trazido à luz por vários repórteres, inclusive por Andy Greenberg, da *Forbes*. Seu artigo "Mutiny Within Anonymous May Have Exposed Hackers' IP Addresses" foi publicado em 9 de maio de 2011. Concluí que o "AnonOps IRC se tornou uma cidade fantasma" com base em minhas próprias observações e nas observações de Topiary sobre a rede. A declaração de vários operadores

de

AnonOps

que

estavam

"profundamente entristecidos com esse drama" foi publicada e republicada em vários blogs. O post original também mencionava que o AnonOps iria "protagonizar um retorno e voltar com força máxima". Ryan Cleary, o responsável pelo do vazamento do IP, deu uma entrevista para o blog de tecnologia thinq_ dizendo que os operadores por trás do AnonOps tinham "sede de publicidade" e "começaram a se engajar em operações apenas para ganhar as manchetes" e "alimentar seus próprios egos". Conforme o blog thinq_, Ryan teria dito: "Eles só gostam de ver as coisas destruídas".

Eu vi a doxeagem sobre Ryan quando o arquivo foi publicado a primeira vez on-line. Ele incluía seu endereço real em Wickford, Essex, seu número de telefone celular e os nomes e as idades de seus pais. A página dos dox dizia que Ryan tinha sido "dominado"

por Evo, acrescentando: "Quem é o 'bicho de estimação' agora, vadia?". O documento também dava "hurras", ou saudações, a Sabu, Kayla, Owen, #krack e a todos do AnonOps.

A afirmação de que o Anonymous “estava começando a parecer uma piada” vem de minhas próprias observações, bem como de discussões com os seguidores.

Capítulo 16: Papo sobre uma revolução Em sua maioria, os dados e as descrições deste capítulo derivam de entrevistas com Topiary e Sabu ao longo de vários meses, incluindo entrevistas via Internet Relay Chat, discussões por telefone e encontros presenciais.

A questão sobre o prefeito de Nova York, Rudy Giuliani, ter aumentado a força policial da cidade para 40 mil integrantes foi corroborada pela ata de 11 de abril de 2000, da Câmara de Vereadores, e por notícias veiculadas na imprensa.

Os detalhes sobre o COINTELPRO foram corroborados por informações do próprio site do FBI, que afirma que o projeto foi “justamente criticado pelo Congresso e o povo americano por cercear direitos da primeira emenda e por outros motivos”.

Consulte http://vault.fbi.gov/cointel-pro.

O ponto de que Kayla, Tflow e AVunit tinham “dado um tempo”

antes da formação do LulzSec foi corroborado por Sabu e pelo menos por outro adepto do LulzSec.

A citação “As hackeagens mais profissionais e de alto nível nunca são detectadas” vem de uma entrevista com um hacker sectário do Anonymous que preferiu não ser identificado.

Capítulo 17: Lulz Security A maioria dos dados neste capítulo foi proveniente de entrevistas com Topiary, Sabu e Kayla. Dados adicionais, inclusive o diálogo de Pwnsauce, baseiam-se na minha observação das discussões entre Topiary, Kayla, Tflow, AVunit e Pwnsauce no canal de IRC

#charmy, criado para discussões que eu poderia reproduzir neste livro. Também realizei entrevistas com alguns do grupo, tais como Pwnsauce, neste canal.

A afirmação de que “demorou uma semana para os administradores de TI da Fox detectarem a invasão” baseou-se em entrevistas no #charmy.

Em relação à conta original do LulzSec no Twitter, @LulzLeaks: a conta original

que contém esse primeiro tweet ainda está on-line.

Eu corroborei que o LulzSec havia realmente postado um banco de dados de possíveis competidores do The X Factor conversando com um porta-voz da Fox cerca de vinte e quatro horas após o anúncio da hackeagem. Também vi o banco de dados publicado no Pastebin.

Capítulo 18: A ressurreição de Topiary e Tupac Dados sobre a hackeagem da PBS foram provenientes de entrevistas com os hackers envolvidos, bem como de um post que Topiary publicou no Pastebin com detalhes sobre que tipo de ferramentas, como a Havij, o grupo havia usado. De acordo com um artigo de março de 2012 no darkreading.com, a ferramenta "predileta dos hacktivistas" foi criada por hackers iranianos, e seu nome vem da palavra persa para "cenoura", também um apelido para o órgão sexual masculino.

A afirmação de que "o pessoal na sala de bate-papo #anonleaks do IRC AnonOps surtou" quando Topiary postou algo em sua conta pessoal no Twitter baseou-se em entrevistas com Topiary após ele ter visitado a rede de bate-papo.

Capítulo 19: Guerra hacker Concernente ao aumento no tráfego do Pastebin, os controladores do site mais tarde demonstrariam seu apreço pelo LulzSec por retweetar o anúncio de 13 de julho de 2011 do @LulzSec de que "Se o @pastebin atingir 75 mil seguidores, vamos nos envolver numa misteriosa operação que irá causar o caos". (Esse foi um dos raros tweets do @LulzSec depois que o grupo acabou oficialmente.) Horas mais tarde, @Pastebin tweetou: "O nº de seguidores do @pastebin está crescendo muito rapidamente desde que o @lulzsec passou a nos enviar seu amor", seguido de: "A loucura do Twitter continua graças ao @lulzsec". Nesse mesmo dia, Topiary trocou e-mails com o proprietário do Pastebin, Jeroen Vader, empresário holandês de 28 anos de idade, a quem Topiary solicitou um ícone "exclusivo de coroa verde" ao lado de sua conta pessoal "Topiary" no Pastebin, o qual, quando realçado, também dissesse "CEO no consumo de tortas". Vader concordou, dizendo: "Deixa comigo; vou lhe conseguir uma coroa muito especial. Muito obrigado por confiar no Pastebin com suas publicações 'especiais'". As publicações do LulzSec e do Anonymous no Pastebin estão entre os posts com maior tráfego, juntamente com a derradeira publicação do LulzSec, "50 Days of Lulz", de 25 de junho de 2011, que alcançou 411.354 visualizações de página, registradas em 3 de abril de 2012. (O Pastebin hospeda anúncios em seu site, por isso o tráfego extra deve ter contribuído com seu lucro.) Ironicamente, Vader afirmou no início de abril de

2012 que ele iria contratar mais pessoal para ajudar a policiar “informações confidenciais” postadas no site, de acordo com a BBC News.

Dados sobre o ponto de encontro do The Jester no 2600 e sobre as outras pessoas que o frequentavam têm como fonte os registros de bate-papo vazados do canal #pure-elite do LulzSec, as entrevistas com Topiary e minhas próprias observações da rede de IRC 2600.

Os itens sobre as origens de 2600: The Hacker Quarterly baseiam-se em diversos artigos da web, incluindo a reportagem de capa da PCWorld, “Hacking’s History”, publicada em 10 de abril de 2001.

As informações sobre a criação de um segundo escalão de asseclas do LulzSec têm como base conversas com Topiary e Sabu. O

detalhe sobre o Antisec e seus adeptos originais abrangendo “algumas centenas de hackers habilidosos” foi originário de minhas conversas com Andrew “weev” Auernheimer, hacker nos primeiros dias do movimento Antisec, e em vários artigos na web, incluindo a reportagem de 2002 da *Wired,* intitulada “White-Hat Hate Crimes on the Rise”.

Os apelidos de “membros do segundo escalão” do LulzSec, tais como Neuron e M_nerva, baseiam-se nos registros de bate-papo do #pure-elite, inicialmente vazados on-line via Pastebin, em 5 de junho de 2011, no post intitulado “LulzSec Private Log”. Os logs foram republicados pelo *The Guardian* três semanas mais tarde, em 25 de junho, atraindo ainda mais atenção dos principais órgãos de comunicação. As fontes das descrições adicionais sobre a sala, seus membros e o contexto de suas discussões são entrevistas com Topiary e com outro hacker, que preferiu não ser identificado.

O detalhe de que Adrian Lamo foi diagnosticado com síndrome de Asperger é originário do artigo da *Wired*, intitulado “Ex-Hacker Adrian Lamo Institutionalized, Diagnosed with Síndrome de Asperger”, publicado em 20 de maio de 2010.

Capítulo 20: Mais Sony, mais hackers Quanto ao LulzSec e à Sony: uns dias antes do ataque contra a PBS, o LulzSec já tinha publicado dois bancos de dados com informações internas do site da Sony Japan. A ação não causou rebuliço, pois Topiary simplesmente tinha colado endereços da web específicos, vulneráveis a hackeagem por simples injeção de SQL.

Um

deles,

por

exemplo,

era

assim:

http://www.sonymusic.co.jp/bv/cromagnons/track.php?

item=7419. Topiary anunciou os achados num comunicado de imprensa, dizendo a outros hackers: “Dois outros bancos de dados hospedados nesta boxxy box. Vá atrás deles se quiser”. Ele acrescentou que as “entranhas” eram “saborosas, mas não muito empolgantes”. Detalhes sobre a maneira com que a cúpula e o segundo escalão do LulzSec se reuniam e exploravam vulnerabilidades cibernéticas no âmbito da rede da Sony e em outros lugares foram provenientes de discussões com Topiary e também com Sabu e Kayla. O diálogo entre os hackers também se originou de entrevistas com o trio. A maioria dos dados que o LulzSec roubou da Sony veio dos sites SonyPictures.com, SonyBMG.nl e SonyBMG.bg – mas 95% dos tesouros vieram da SonyPictures.

Descrições sobre o estilo de redação de Topiary são baseadas nas minhas próprias observações dos comunicados de imprensa que ele escreveu e da conta do Twitter controlada por ele.

O contexto da extensão dos ataques cibernéticos contra a Sony teve como fonte o site de segurança cibernética attrition.org e seu artigo “Absolute Sownage: A Concise History of Recent Sony Attacks”. Inclui provavelmente o mais abrangente resumo de ataques cibernéticos contra empresa realizados entre os meses de abril e de julho de 2011.

Os boatos sobre a hackeagem da Play Station Network, envolvendo um empregado despedido e a venda de um banco de dados por US$ 200 mil, baseiam-se em reportagens da imprensa e em uma fonte interna do Anonymous que prefere não ser identificada. Não está claro se os hackers da PSN tinham vendido tudo num mercado de carders (fraudadores de cartões) ou em lotes. Mas

em certos mercados on-line era possível fazer mil dólares vendendo um banco de dados de seis anos de idade contendo os nomes de 300 mil usuários – em geral, o preço no mercado dependia da idade do banco de dados, de acordo com pessoas familiarizadas com o assunto. Isso significava que mais de 100 milhões de recentes logins da Sony facilmente alcançariam valores de dezenas de milhares de dólares. Um artigo da *Reuters*, de 23 de junho de 2011, citou uma ação judicial contra a Sony alegando que a empresa tinha despedido funcionários da unidade responsável pela segurança de rede duas semanas antes de ocorrer a falha de segurança, e que, embora a empresa "gastasse prodigamente" em segurança para proteger seus próprios dados corporativos, não conseguia fazer o mesmo pelos dados de seus clientes. A ação, movida em um tribunal distrital dos EUA, citava uma "testemunha confidencial".

Detalhes sobre o modo como o LulzSec atacou Karim Hijazi provêm de entrevistas com Topiary e Kayla, bem como de registros de bate-papo publicados pelo LulzSec e por Hijazi.

Informações adicionais provêm de entrevistas por telefone com Hijazi nos dias após seu ataque ser anunciado e de entrevistas com seu porta-voz de imprensa.

Dados sobre o grupo de hackeagem ~el8 foram originados de seus quatro e-zines, que permanecem disponíveis on-line, e do artigo de 2002 da *Wired*, intitulada "Hate White-Hat Crimes on the Rise".

Detalhes sobre a divulgação de Andrew "weev" Auernheimer de uma falha de segurança para os usuários de iPad no site do AT&T

foram provenientes de entrevistas com Auernheimer, da reportagem do *Gawker*, intitulada "Apple's Worst Security Breach: 114,000 iPad Owners Exposed", de 9 de junho de 2010, e do artigo do CNET, "AT&T iPad Site Hacker to Fight on in Court", publicado em 12 de setembro de 2011. Em julho de 2011, um grande júri federal em Newark, Nova Jersey, indiciou Auernheimer em uma acusação de conspiração para ganhar acesso a computadores e uma acusação de roubo de identidade. A partir de setembro de 2011 até meados de abril de 2012, ele estava solto sob fiança e declaradamente proibido de usar IRC ou confraternizar com pessoas de seu grupo hacker.

A afirmação de que o IRC AnonOps estava "uma confusão, todos com os nervos à flor da pele" se baseia em minhas próprias observações da rede de bate-papo e

em entrevistas com Topiary.

A afirmação de que alguns chapéus brancos “secretamente desejavam participar da diversão” origina-se de minhas observações dos comentários feitos por especialistas em segurança de chapéu branco em blogs e no Twitter, que muitas vezes professavam admiração pelo LulzSec e expressavam gratidão, pois o grupo havia demonstrado a necessidade da profissão de segurança em internet. Um bom exemplo é o artigo do especialista em segurança australiano Patrick Gray, em seu blog risky.biz, intitulado “Why We Secretly Love LulzSec”, postado em 8

de junho de 2011. O post rapidamente viralizou no Twitter.

Sobre o ataque de DDoS de Ryan contra o canal de IRC público do LulzSec – ele ficou enviando a mesma mensagem para todos os operadores no canal de IRC.

Capítulo 21: Estresse e traição Dados sobre a operação paralela de Kayla foram provenientes de entrevistas com Kayla e Topiary, enquanto o diálogo neste capítulo se baseou nos registros vazados do #pure-elite. Contexto adicional sobre a hackeagem da Infragard, as discussões no #pure-elite e as doações no Bitcoin vem de entrevistas com os membros fundadores do LulzSec. Alguns diálogos, tais como a reação à doação de US$ 7800 via BitCoin, também foram provenientes de entrevistas.

O informe preliminar da OTAN sobre o Anonymous pode ser encontrado no site da organização, no endereço http://www.nato-pa.int/default.asp?SHORTCUT=2443. Foi mencionado a primeira vez em blogs de tecnologia, tais como o thinq_, no início de junho.

O código de exclusão rm -rf/* é bem conhecido entre os trolls da web, que em certa época tinham o hábito de dizer aos usuários de Mac e Linux para digitar o código em sua cópia do Terminal, o aplicativo que permite aos usuários interagir com seus computadores usando uma interface de linha de comando. Isso pode conduzir os usuários a inadvertidamente apagar seus discos rígidos. De acordo com KnowYourMeme.com, o esquema de trollagem contra os usuários de PC vem sendo aplicado desde o início dos anos 2000, mas tornou-se popular com sua divulgação no 4chan por volta de 2006. Usuários do *b* postavam panfletos digitais ou iniciavam tópicos de discussão dizendo, por exemplo, que a

Microsoft tinha incluído uma pasta chamada system32 em todos os PCs e que essa pasta continha 32 gigabytes de “porcarias”. Eles acrescentavam que a empresa fizera isso para vender mais software de limpeza de sistema, e que a maneira de se vingar da gananciosa Microsoft seria excluir o arquivo. Claro que isso era uma completa inverdade.

Eis uma tradução do código UNIX rm -rf/*: “rm” é o comando curto para remover; em seguida, um espaço em branco indica o final do comando. O “-” começa as opções, com “r” significando “recursivamente excluir todos os diretórios” e “f” significando “ignorar permissões de arquivo”. “/ *” significa que tudo após a raiz da árvore (“/”) deve ser afetado. O comando inteiro significa “remover tudo à força”.

A afirmação de que “muitas agências de notícias adotaram esse ponto de vista” – o de que o LulzSec tinha hackeado a Infragard em resposta ao anúncio do Pentágono – baseou-se em diversos artigos veiculados na mídia. Entre eles está a reportagem do digitaltrends.com, “LulzSec Hacks FBI Affiliate, Infragard”.

Detalhes sobre a prisão de Sabu foram originados em parte de reportagens da Fox News, inclusive a intitulada “Infamous International Hacking Group LulzSec Brought Down by Own Leader”, e em parte de uma entrevista com uma fonte anônima que teve acesso a informações sobre a prisão e a investigação do FBI. Dados adicionais sobre a prisão do Sabu e seu comparecimento mais tarde perante o tribunal em uma audiência secreta são explicados no Capítulo 26.

Dados sobre o tweet promocional da Cisco, aparecendo nas buscas pelo LulzSec no Twitter, foram originados de minhas próprias observações e corroborados pelo porta-voz da Cisco, John Earnhardt, que alegou que o LulzSec era um “termo de interesse”

na indústria de segurança. Um dia depois de eu escrever na *Forbes* um post de blog sobre o lance publicitário intitulado “How Cisco Is Capitalizing on LulzSec Hackers’ Popularity”, publicado em 15 de junho de 2011, a promoção desapareceu.

O mais provável é que Joseph K. Black, fundador da empresa de segurança em TI Black & Berg, tenha simulado o ataque contra o próprio site. Essa afirmação se baseia em entrevistas com Topiary, que garantiu que ninguém do grupo havia atacado nem planejado atacar a Black & Berg, e em entrevistas com Jennifer

Emick, que passou algum tempo investigando Black. Também baseio essa conclusão em minha opinião de que Black não é uma fonte confiável. Rob Rosenberger, especialista em segurança cibernética e antivírus, escreveu uma coluna para o site SecurityCritics.org, em 15 de fevereiro de 2011, na qual ele rotula Black de “charlatão”, cujas atividades até aquele ponto já se “qualificavam como ‘comportamento antiético’ com o objetivo de autopromoção descarada”. O site de segurança cibernética attrition.org escreveu mais tarde (28 de fevereiro de 2011) um artigo condenatório sobre Black, intitulado “Joseph K. Black: Social Media Experiment Gone Horribly Wrong”, que oferecia a previsão de que Black nunca alcançaria seu declarado emprego dos sonhos “Conselheiro de segurança cibernética nacional”. O artigo postava capturas de tela da conta de Black no Twitter a partir de janeiro de 2011, incluindo tweets como “Acabei de cheirar minha 2ª fileira de coca e são apenas 4h15; UAU!”. Outro tweet, dirigido para a própria Attrition, dizia: “Vocês só tão com inveja que os Feds ainda não lhe escolheram. Babacas. Sou intocável. Tenho os Feds em meu bolso.

Tô tranquilo”. Em outubro de 2011, Black sofreu uma perseguição policial durante trinta e cinco minutos através de quatro condados dos Estados Unidos, culminando com ele saindo do carro segurando um cachorrinho e apontando o dedo para a polícia, fazendo sons de tiro. Na mesma hora ele recebeu uma carga de Taser (fonte: “Omaha Man Caught after Early Morning Pursuit”, North Platte Bulletin, 31 de outubro de 2011). Por volta do início de 2012, a Black & Berg havia fechado as portas, e Black postara uma foto de si mesmo na página da web about.me, em que ele próprio se listava como “Conselheiro das operações do Anonymous e do #Antisec”. Na foto, Black estava parado na frente de um espelho, com moletom de capuz, óculos escuros e colar dourado. Black não respondeu a uma pergunta enviada a ele por email sobre o assunto da desfiguração do seu site, nem a um pedido de entrevista. Ironicamente, apesar das provas esmagadoras de que o deface no site de Joseph K. Black tinha sido autoinfligido para fins de publicidade, promotores de Justiça britânicos mais tarde citariam o ataque a Black & Berg entre as acusações contra Jake Davis e três outros jovens ligados ao LulzSec.

Dados sobre outros grupos hacker réplicas, como LulzSec Brasil e LulzRaft, foram originados das contas dos próprios grupos no Twitter, anúncios e notícias, bem como de entrevistas com membros do LulzSec.

A declaração de Topiary, “Estou ficando muito preocupado. Talvez algumas prisões realmente aconteçam”, foi retirada de uma entrevista que ele me

concedeu.

Capítulo 22: O retorno de Ryan, o fim da razão Dados neste capítulo sobre as atividades internas do LulzSec, o diálogo sobre o desaparecimento de Sabu e as descrições de Ryan têm como fonte entrevistas com os membros fundadores do LulzSec. Dados sobre o primeiro telefonema entre Topiary e Sabu provêm de entrevistas com Topiary.

O nome David Davidson vem da comédia amplamente criticada *Fora de casa!* (Freddy Got Fingered, 2000), dirigida e estrelada por Tom Green. Muitas vezes tem sido utilizado on-line como nome de piada, mas talvez não o suficiente para ser considerado um instantâneo meme da internet.

Ryan primeiro reacendeu o seu relacionamento com os membros do LulzSec ao se oferecer para deixar o grupo sediar sua rede IRC

em seus servidores. Essa oferta foi bem-vinda, embora no fim das contas a equipe adotasse o critério de pular de um servidor a outro, pertencentes ao AnonOps e às redes de IRC públicas fornecidas pelo EFnet, Rizon e 2600.

Topiary não acreditava que os dox publicados por Evo sobre Ryan no início daquele ano fossem reais. Ele também acreditava que o verdadeiro Ryan estava relativamente seguro, já que Ryan alegava, por exemplo, que o seu vizinho recebia todas as suas encomendas, que, seja como for, eram endereçadas a um nome falso, antes de repassá-las a ele, de modo que nunca precisava revelar seu endereço verdadeiro.

O número do Google Voice 1-614-LULZSEC permanecia sempre desligado em todos os momentos e redirecionava a outro número de Google, que também estava off-line e redirecionava instantaneamente para a conta principal de Skype usada por Topiary e Ryan. Essa conta tinha sido registrada por meio de uma conta de Gmail falsa em um endereço IP aleatório.

A afirmação de que Assange “ria” consigo mesmo baseia-se em entrevistas com Topiary, que afirmou que, na primeira vez em que conversaram via IRC, Assange afirmou que ele e outros no WikiLeaks tinham “rido” ao ouvir sobre o ataque de DDoS contra a CIA.

Detalhes sobre a situação de Julian Assange em junho de 2011, incluindo sua defesa contra a extradição e o uso de uma tornozeleira eletrônica, foram

originados de várias notícias, tais como “Julian Assange Awaits High Court Ruling on Extradition”, publicada pelo *The Guardian* em 2 de novembro de 2011.

Dados sobre as discussões de IRC no âmbito do LulzSec (primeiro entre Topiary e Sabu, depois entre outros membros da equipe) foram provenientes de entrevistas com Topiary e com outro hacker associado ao LulzSec que prefere não ser identificado.

Também vi e realizei capturas de tela do vídeo de Assange filmado por q, temporariamente carregado no YouTube. O vídeo mostrava a conversa de IRC com o LulzSec e uma tomada panorâmica de Assange fitando seu laptop. O diálogo com a discussão entre Sabu e q é retirado do mesmo vídeo, que também mostrava o texto do canal de IRC de que ambos participavam naquele momento.

Fontes próximas ao WikiLeaks confirmam: no passado, q havia organizado reuniões entre Assange e outros terceiros via IRC, e a origem de q é a Islândia. A respeito do nome do arquivo RSA 128: RSA é um algoritmo criptográfico (Rivest, Shamir e Adleman). O

número 128 deve se referir ao comprimento do código ou à força da criptografia medida em bits.

Capítulo 23: Fim explosivo Dados sobre a reação do 4chan ao LulzSec foram provenientes de entrevistas com William e Topiary. De modo um tanto irônico, o LulzSecurity.com esteve a certo ponto hospedado no mesmo centro de dados que o 4chan, de acordo com Topiary.

Sobre a publicação de 62 mil e-mails e senhas, Topiary havia carregado o banco de dados uma segunda vez no site de hospedagem de arquivos MediaFire.com. Antes de ser novamente retirado, porém, usuários aleatórios tinham-no baixado quase 40

mil vezes.

Dados adicionais sobre o estímulo do LulzSec a um revival do movimento Antisec e dados sobre o relacionamento de Topiary com Ryan baseiam-se em entrevistas com Topiary; o contexto para esses dados foi fornecido por meio de entrevistas com Sabu.

Dados sobre alguém da SOCA ter enviado à Polícia Metropolitana um e-mail mencionando um ataque de DDoS têm como fonte as anotações do promotor, que foram passadas aos membros do LulzSec detidos.

Dados sobre a prisão de Ryan provêm de reportagens na imprensa, como o artigo do *Daily Mail*, intitulado "British Teenager Charged over Cyber Attack on CIA as Pirate Group Takes Revenge on 'Snitches Who Framed Him'", publicado em 22 de junho de 2011, e de entrevistas com membros do LulzSec. Logo após a detenção do Ryan, um Anon vinculado a Ryan Cleary abordou Topiary via IRC e lhe contou com absoluta seriedade que um fotógrafo do *Sun* estava planejando voar para a Holanda para tentar tirar uma foto do "verdadeiro Topiary".

Dados sobre o vazamento de dados da polícia do Arizona e a discussão entre os membros fundadores do LulzSec sobre a dissolução do grupo basearam-se em entrevistas com Topiary, com certo contexto adicional fornecido por Sabu em entrevistas posteriores.

Capítulo 24: O destino do Lulz A analogia de "homens das cavernas espalhando sangue de bisão"

nas rochas foi extraída de uma discussão com Topiary.

Dados sobre os script kiddies invadindo a conta da Fox News no Twitter baseiam-se em vários artigos veiculados na imprensa, como "Fox News Hacker Tweets Obama Dead", publicado pela BBC

News on-line em 4 de julho de 2011. A desfiguração da página da Pfizer no Facebook, assumida pelo LulzSec, baseou-se nos posts do grupo no Twitter e de minhas próprias observações posteriores da página do Facebook desfigurada. Dados sobre outros grupos de hackers de países como Filipinas, Colômbia e Brasil basearam-se em vários relatos no TheHackerNews.com.

A declaração de que havia mais de seiscentas pessoas na sala de bate-papo do AnonOps #Antisec após a dissolução do LulzSec vem de minhas próprias observações como usuária da rede de IRC.

A declaração de Sabu, "Estou fazendo o mesmo trabalho, só que mais revolucionário", baseou-se em minha entrevista com Sabu via IRC.

Dados sobre o "afastamento" de Topiary do Anonymous depois da dissolução do

LulzSec foram provenientes de entrevistas com ele.

A afirmação de que “vários órgãos da grande imprensa ficaram se mordendo de inveja” quanto à alegação de Sabu sobre conceder a certos órgãos de comunicação acesso aos e-mails do *News of the World* originou-se de notícias como “LulzSec Claims to Have News International E-mails”, publicada pelo *The Guardian* em 21 de julho de 2011.

O detalhe sobre o marido do Rebekah Brooks ter posto no lixo seu laptop em um saco preto baseia-se no artigo do *The Guardian*, “Police Examine Bag Found in Bin Near Rebekah Brooks’s Home”, publicado em 18 de julho de 2011.

A afirmação de que a polícia em oito países havia detido setenta e nove pessoas em conexão com as atividades realizadas sob os nomes do Anonymous e do LulzSec tem como fonte diversas notícias sobre essas detenções e um cálculo no Pastebin. Dados sobre a prisão iminente de Topiary foram obtidos a partir dele mesmo, com certos fatos, inclusive a suposta contratação de um jatinho particular, corroborados pelas notícias veiculadas, tais como a publicada no *Daily Mail* com a manchete “Autistic Shetland Teen Held over Global Internet Hacking Spree ‘Masterminded from His Bedroom’”, publicada em 31 de julho de 2011.

Parte 3

Capítulo 25: O verdadeiro Topiary Dados sobre a prisão do Topiary, incluindo descrições de seu encontro com a polícia, foram provenientes de entrevistas posteriores com Jake Davis. Os dados sobre a visita da polícia à casa da mãe de Jake, em Spalding, foram provenientes de conversas com Jennifer Davis. As descrições de Sra. Davis entrando na delegacia de polícia de Charing Cross baseiam-se em minhas próprias observações após visitar a delegacia naquele dia.

A asserção de que nas salas de bate-papo do AnonOps "corriam boatos acalorados" baseia-se em minhas próprias observações ao visitar a rede de IRC; a declaração de que Sabu estava "bastante deprimido" vem de minha entrevista com ele.

A afirmação de que o nome de Jake viera à tona na sala de bate-papo do AnonOps após um erro envolvendo sua conexão VPN

originou-se de minhas observações do banco de dados do registro da bate-papo da sala pública do AnonOps, em 8 de dezembro, em http://blyon.com/Irc/. O boato sobre o amigo dos fóruns Xbox postar "Jake de Shetland" originou-se do registro do bate-papo virtual publicado por Sabu com sua conversa com Mike "Virus"

Nieves (ver Capítulo 26) e do artigo do *Gawker*, "How a Hacker Mastermind Was Brought Down by His Love of Xbox", publicado em 16 de agosto de 2011.

Dados sobre o provedor de VPN HideMyAss acatar uma ordem do tribunal britânico para ajudar a identificar um membro do LulzSec provêm de um post de blog no site do HideMyAss com o título "LulzSec Fiasco", publicado em 23 de setembro de 2011. A empresa HideMyAss não respondeu a reiterados pedidos de entrevista e não lista um número de telefone em seu site.

O item sobre o Ministério de Segurança Nacional esperar ataques mais significativos do Anonymous tem como fonte o boletim ministerial do Centro de Integração de Comunicações e Cibersegurança Nacional e Cibersegurança Nacional, publicado em 1º de agosto de 2011.

Os dados e as descrições sobre o comparecimento de Jake Davis ao tribunal

originam-se de minhas observações enquanto participava da audiência, com contexto adicional fornecido por entrevistas posteriores com Davis.

A obra *Free Radicals: The Secret Anarchy of Science* obteve substancial aumento em sua classificação na Amazon após Jake Davis mostrar a capa do livro para as câmeras, de acordo com uma entrevista com o autor do livro, Michael Brooks.

Descrições das imagens da propaganda e cartazes digitais de Jake Davis após sua audiência no tribunal têm como fonte minhas próprias observações depois de conversar com vários sectários do Anonymous no AnonOps, um dos quais me enviou um crescente repositório dessas imagens.

Dados sobre as cartas de fãs a Jake Davis e sobre sua vida em casa provêm de entrevistas com Davis, que incluíram visitas à sua casa em Spalding, e de minha própria observação de algumas das cartas recebidas por ele.

Dados sobre o ataque executado por William e outros membros do *b* contra uma moça de dezesseis anos de idade no Facebook, chamada Selena (nome não verdadeiro), foram provenientes de entrevistas com William realizadas por e-mail e pessoalmente.

O encontro de Davis com William foi organizado por mim. Eu imaginava, há algum tempo, que seria interessante observar o que aconteceria se duas pessoas do Anonymous se encontrassem cara a cara. Também queria organizar um encontro em que um Anon e uma vítima dos Anon – por exemplo, Jake Davis e Aaron Barr – se conhecessem pessoalmente. Restrições de tempo e distância tornaram impraticável um encontro entre Barr e Davis, então a segunda melhor alternativa parecia ser uma reunião entre William e Topiary. Consultei se um estava disposto a conhecer o outro, e, após os dois concordarem, estipulei uma data em fevereiro de 2011. No dia combinado, primeiro me encontrei com William antes de viajar com ele de trem ao local do encontro com Davis.

Acompanhei os dois a um restaurante, onde conversamos enquanto almoçávamos. À medida que os dois homens debatiam o Anonymous, fiz perguntas e tomei notas.

Capítulo 26: O verdadeiro Sabu Dados sobre a cooperação do Sabu com a polícia e seus delitos fora do mundo do Anonymous e do LulzSec provêm de seu indiciamento criminal e de uma transcrição da denúncia contra ele de 5 de

agosto de 2011, no tribunal federal de primeira instância de Nova York. Contexto e descrição adicionais foram fornecidos por uma entrevista com uma fonte que teve acesso à investigação do FBI sobre Sabu, bem como por entrevistas com hackers do Anonymous que tinham trabalhado com Sabu nos meses após a dissolução do LulzSec e durante seu tempo como informante do FBI. Todas as fontes alegaram categoricamente não ter conhecimento de que Sabu era informante, embora tivessem variados graus de suspeita.

A descrição de Hector "Sabu" Monsegur baseou-se na notícia da Fox News "Infamous International Hacking Group LulzSec Brought Down by Own Leader", publicada em 6 de março de 2012, no artigo do *The New York Times* com o título "Hacker, Informant and Party Boy of the Projects", publicado em 8 de março de 2012.

Descrições adicionais de Sabu baseiam-se em minhas próprias conversas com ele on-line e por telefone, em minhas observações de sua conta no Twitter e no registro de bate-papo vazado entre Sabu e o hacker Mike "Virus" Nieves. O registro de bate-papo foi publicado no Pastebin em 16 de agosto de 2011 e intitulava-se "sabu vs vírus ou debi & loide parte 2".

Os abrangentes dox de Sabu, que dessa vez incluíam uma foto de Hector Monsegur, foram publicados por um pesquisador de segurança de chapéu cinza apelidado Le Researcher, que colou diversas capturas de tela de e-mails, mensagens de deface e posts de fóruns em http://ceaxx.wordpress.com/uncovered/.

A afirmação de que o hacktivismo é "extremamente popular no Brasil" originou-se de um relatório da Imperva intitulado "The Anatomy of an Anonymous Attack", publicado em fevereiro de 2012, bem como de minhas próprias observações sobre o número de notícias sobre ataques cibernéticos do Anonymous no Brasil.

As descrições sobre a interação e os diálogos da interação entre Sabu e sup_g, também conhecido como Jeremy Hammond, antes do ataque a Stratfor, têm como fonte o indiciamento criminal de Hector Monsegur, com contexto adicional, incluindo detalhes sobre sua ligação com o WikiLeaks, baseado em entrevistas com outros hackers que participaram do ataque contra a Stratfor.

A referência ao artigo do *The New York Times* em que o FBI negou ter "deixado

o ataque [a Stratfor] acontecer” é originária da reportagem “Inside the Stratfor Attack”, publicada no blog Bits do mencionado jornal, em 12 de março de 2012.

Detalhes sobre Donncha “Palladium” O’Cearrbhail ter hackeado a conta do Gmail de um membro da polícia nacional irlandesa para escutar uma ligação entre o FBI e a Polícia Metropolitana têm como fonte os indiciamentos de O’Cearrbhail e Monsegur.

Dados sobre Monsegur ter se passado por agente federal ao NYPD

foram provenientes de seu indiciamento criminal.

Capítulo 27: A verdadeira Kayla, os verdadeiros Anonymous Descrições sobre Ryan Mark Ackroyd foram provenientes de minhas observações de Ackroyd em sua primeira audiência no tribunal, em 16 de março de 2012. Dados sobre a sua irmã mais nova, Kayleigh, provêm de uma busca de diretório com o nome de Ryan Ackroyd, que revelou os nomes dos pais e irmãos de Ackroyd; a descrição física de Kayleigh baseou-se em sua conta pública no Facebook, assim como as observações de que ela postou no mural do Facebook do irmão Keiron.

As datas e os detalhes básicos sobre a primeira e a segunda detenções de Ryan Ackroyd foram provenientes dos comunicados de imprensa da Polícia Metropolitana para ambos os incidentes.

Em geral, as solicitações de entrevista com a Polícia Metropolitana para obter mais detalhes sobre Ryan Ackroyd e a investigação da Met sobre o Anonymous foram negadas.

Dados sobre a reação da comunidade do Anonymous à notícia de que Sabu atuava como informante há oito meses foram provenientes de entrevistas com a acadêmica Gabriella Coleman, Jake Davis e um punhado de Anons, junto com minha observação de várias contas no Twitter, postagens de blogs e comentários em canais de IRC frequentados por sectários do Anonymous.

Glossário

4chan:

Popular painel de imagem frequentado por 22 milhões de usuários distintos por mês.

Originalmente anunciado como local para discutir animes japoneses, metamorfoseou-se num terreno de encontro para a discussão de toda sorte de tópicos, inclusive trotes on-line, ou "ataques", contra outros sites da web ou indivíduos (ver Capítulos 2 e 3). Uma de suas características essenciais é o anonimato compulsório dos usuários, que assim são capazes de postar livremente, sem inibições e sem medo de serem responsabilizados.

Anonymous: Nome que engloba grupos de pessoas que causam perturbações na internet com o objetivo de realizar trotes ou protestos. Derivado a partir do anonimato obrigatório dos usuários do painel de imagem 4chan, evoluiu ao longo dos últimos cinco anos para se tornar associado com ataques cibernéticos contra empresas e agências governamentais, atraindo grande atenção pública. Sem nenhuma estrutura clara de liderança nem regras para afiliação, existe como um grupo fluido de pessoas que seguem um vago conjunto de princípios derivados das 47 Regras da internet. A ampla coletividade assume várias aparências, dependendo de quem está adotando o nome na ocasião – por exemplo, os organizadores do projeto Chanology em 2008

(ver Capítulo 5) e os hackers do LulzSec em 2011 (ver Capítulo 17).

Antisec (Anti-Security): Movimento cibernético lançado no começo dos anos 2000, no qual hackers de chapéu preto fizeram campanha para terminar com o sistema de "divulgação integral" entre os profissionais de segurança de TI, em geral atacando esses mesmos profissionais de chapéu branco. O

LulzSec reviveu o movimento no verão de 2011, com o nebuloso objetivo de atacar agências governamentais e autoridades em um esforço às vezes superficial de expor corrupção.

***b*:**

Painel mais popular do 4chan, visitado por cerca de um terço dos usuários do site. O *b* foi originalmente anunciado pelo criador Christopher "moot" Poole como o painel "aleatório" do site. Acabou servindo de tábula rasa no qual surgiu uma série de memes criativos da internet, como Lolcats, e é amplamente considerado o local de origem da "mente colmeia" do Anonymous. Muitos asseclas dessa organização afirmam que fizeram o primeiro contato com ela por

meio do *b*. Conhecido por sua falta de moderadores.

Botnet:

Rede de computadores zumbis formada pela disseminação de vírus ou links para falsas atualizações de software. Botnets podem ser controlados por uma pessoa, capaz de comandar milhares, às vezes milhões, de computadores para executar ordens com base na web e em massa.

Chanology: Também conhecido como Projeto Chanology, consiste na série de ataques, protestos e trotes cibernéticos conduzidos por sectários do Anonymous ao longo da maior parte de 2008 contra a Igreja da Cientologia. O nome é uma mistura de “4chan” com “Scientology”.

Chapéu branco: Alguém que sabe como hackear uma rede de computadores e furtar informações, mas utiliza essa habilidade para ajudar a proteger sites e organizações.

Chapéu preto: Alguém que utiliza o conhecimento sobre programação e software para fins perniciosos, tais como fazer o deface de um site ou furtar bases de dados com informações pessoais para fins de vendê-los a outrem. Os hackers de chapéu preto também são chamados de “crackers”.

DDoS (*Distributed Denial of Service,* ou negação de serviço distribuída): Ataque contra um site ou outro recurso de rede executado por uma rede de computadores que temporariamente derruba o site sobrecarregando-o com tráfego de lixo eletrônico. O ataque pode ser executado por uma rede de voluntários por trás de cada computador (ver “LOIC”) ou por uma rede cujos computadores foram sequestrados para participar de um botnet.

Deface:

Quando utilizado como substantivo (por exemplo, “fazer um deface”), o termo se refere à imagem e ao texto publicado num site que foi invadido, anunciando que ele é um alvo e os motivos de ter sido atacado. Quando utilizado como verbo, significa vandalizar (pichar) ou desfigurar um site.

Dox:

Quando utilizado como verbo (por exemplo, “doxear”), o termo se refere ao ato

de revelar dados pessoais, como nomes, números de telefone e endereços residenciais verdadeiros, em geral por meio do Google ou de engenharia social. As informações resultantes constituem os “dox” (o termo é derivado de “docs”, forma sincopada de “documents”) da pessoa. Doxear costuma servir de ameaça no Anonymous e entre as comunidades hacker, habitadas por personalidades on-line que usam nicknames e quase nunca revelam suas identidades verdadeiras.

Encyclopedia Dramatica: Site que relata boa parte do que acontece no Anonymous, inclusive memes da internet, linguagem do 4chan e discussões on-line entre os usuários mais populares de vários blogs e redes de IRC. O site é quase uma paródia do Wikipedia; tem a mesma aparência e também é editado pelos usuários, mas seu estilo é irreverente, profano e ocasionalmente disparatado, repleto de piadas e links a outros verbetes da ED que apenas os iniciados entendem.

Engenharia social: O ato de mentir ou de falar com uma pessoa sob o disfarce de uma falsa identidade, ou sob falsos pretextos, com o objetivo de extrair informações.

Espreitar: Navegar em sites, redes de IRC ou painéis de imagem como o 4chan sem fazer postagens, em geral com a intenção de aprender sobre a cultura do site sem se expor como novo usuário.

Espreitadores, também chamados de *lurkers* ou bisbilhoteiros, podem ser declarados não bem-vindos em certas redes de IRC se nunca contribuem com os debates.

Hacker:

Termo de definição vaga que, no contexto do Anonymous, se refere a alguém com a habilidade técnica para invadir uma rede de computadores (ver “chapéu branco” e “chapéu preto”). Em linhas gerais, o termo pode se referir a um entusiasta de programação computacional ou a alguém cujo hobby consiste em brincar com sistemas internos e criar atalhos e novos sistemas.

Hacktivista: Palavra composta derivada de “hacker” e “ativista”. Descreve alguém que lança mão de ferramentas digitais para ajudar a disseminar uma mensagem política ou sociológica. Entre os métodos mais ilegais utilizados estão ataques de DDoS, desfigurações de páginas da web e vazamento de dados confidenciais.

IP (*Internet Protocol*): O endereço IP (protocolo de internet) é um número exclusivo atribuído a cada aparelho conectado a uma rede de computadores ou à internet.

IRC (*Internet Relay Chat*): Algo como “bate-papo interativo da internet”. Talvez o método de comunicação predominante entre os partidários do Anonymous, as redes de IRC oferecem o tipo de conversa textual em tempo real que os painéis de imagem não conseguem oferecer. O IRC permite aos usuários conversar uns com os outros em salas de bate-papo, ou “canais”, e existe desde o final da década de 1980. Cada rede de IRC atrai comunidades que compartilham interesses em comum, como a rede IRC AnonOps, que atrai as pessoas interessadas no Anonymous. “Operadores” da rede e do canal moderam as discussões nessas redes; esses cargos são encarados como indicador de alto status social.

LOIC (*Low Orbit Ion Cannon*): Canhão de íons de órbita baixa. Originalmente criado como ferramenta de teste de estresse para servidores, este aplicativo de web de código aberto se tornou popular entre os apoiadores do Anonymous como arma digital que, se utilizada por um número suficiente de pessoas, pode executar um ataque de DDoS a um site.

Lulz:

Modificação da abreviação LOL (*Laugh Out Loud*, ou cair na gargalhada), o termo parece ter aparecido pela primeira vez numa rede de IRC em 2003 em reação a algo engraçado. Hoje se refere ao prazer sentido após realizar um trote ou uma perturbação on--line que conduz ao constrangimento de outrem.

LulzSec:

Grupo de hackers que temporariamente se desmembrou do Anonymous em meados de 2011

para realizar uma série de ataques mais concentrados, de ampla repercussão, contra empresas como Sony e agências governamentais como o FBI. Fundado por hacktivistas como Topiary e Sabu, o LulzSec tinha 6 membros principais e no máximo em torno de 12 a 24 colaboradores de segundo escalão.

Meme:

Slogan ou imagem que se torna inadvertidamente popular, graças à qualidade viral da internet, e cujo significado em geral se perde entre os usuários da web. Funcionando muitas vezes como piadas internas para os defensores do Anonymous, vários memes, tais como “over 9000” ou “delicious cake”, têm suas fontes em velhos jogos de computadores ou se originam de discussões no *b*. Outros exemplos: “rickrollear” e “pedobear”.

Moralfag:

Rótulo dispensado a qualquer usuário do 4chan ou membro do Anonymous que discorda da orientação moral de posts, imagens, métodos de trollagem, ideias, ataques ou atividades. Em geral utilizado como termo pejorativo.

Newfag: Usuário do painel *b* do site 4chan novo no local ou ignorante acerca dos costumes da comunidade.

Oldfag:

Usuário do *b* que entende os costumes da comunidade, geralmente após passar anos frequentando o site.

OP (postador/a original): Qualquer pessoa que começa um tópico de discussão em painéis de imagem. Na cultura do 4chan, o/a OP sempre é chamado de “faggot”.

Painel de imagem: Fórum de discussão on-line com diretrizes vagas no qual os usuários geralmente anexam imagens para ajudar a ilustrar seus comentários. Também conhecidos como “chans”, são fáceis de criar e manter. Certos painéis de imagem são famosos por tratar de tópicos específicos. Por exemplo, o 420chan é conhecido por sua discussão sobre entorpecentes.

Pastebin:

Site simples, mas extremamente popular, permite a qualquer um armazenar e publicar textos.

Defensores do Anonymous o utilizam de modo crescente nos últimos dois anos para publicar dados roubados, tais como e-mails e senhas confidenciais, a partir de bases de dados da web.

Também serviu de plataforma para hackers publicarem comunicados de imprensa, método utilizado pelo LulzSec, facção do Anonymous, durante sua onda de hackeagem em meados de 2011.

Regras da internet: Lista de 47 “regras” supostamente originada em uma conversa de IRC em 2006, e a partir da qual surgiu o slogan do Anonymous “Não perdoamos, não esquecemos”. As regras abrangem a etiqueta cultural em painéis de imagem como o 4chan e atitudes esperadas das comunidades on-line, como a ausência feminina.

Script:

Em computação, programa relativamente simples, muitas vezes utilizado para automatizar tarefas.

Script kiddie: Termo pejorativo que designa alguém que cultiva ambições de se tornar um hacker de chapéu preto e que lança mão de ferramentas da web bem conhecidas e disponíveis gratuitamente, ou “scripts”, para atacar redes de computadores. Em geral, script kiddies procuram ampliar seu status social entre os amigos fazendo hackeagem.

Servidor:

Computador que ajuda a processar o acesso a recursos centrais ou serviços para uma rede de outros computadores.

Shell:

Interface de software que lê e executa comandos. Em certos sites vulneráveis, um hacker pode conseguir um shell para um servidor que hospeda o site, utilizando seu painel de controle administrativo, e então o shell, como a nova interface, dá a esse hacker o controle sobre o site.

SQLi:

Injeção de SQL. Às vezes pronunciado “sequel injection”, o termo se refere ao método de obter acesso a uma base de dados vulnerável da web pela inserção de comandos especiais na própria base, às vezes por meio dos mesmos formulários da web utilizados pelos usuários normais do site. O processo é um modo de adquirir informações de uma base de dados que deveria estar oculta dos usuários

normais.

Troll:

Pessoa que no anonimato persegue ou caçoa de outro indivíduo ou grupo on-line, muitas vezes deixando comentários em fóruns de sites ou, em casos extremos, hackeando contas das mídias sociais. Quando utilizado como verbo, “trollar” também pode significar fazer circular uma mentira bem elaborada. A meta é, em última análise, irritar ou humilhar.

VPN (*virtual private network*): Rede virtual privada, rede de tecnologia que fornece acesso remoto e seguro à internet por meio de um processo conhecido como encapsulamento (tunneling). Muitas organizações utilizam VPN para permitir a seus funcionários que trabalhem a partir de casa e se conectem de modo seguro a uma rede central. Hackers e sectários do Anonymous, porém, utilizam as VPN para substituir seus verdadeiros endereços IP, possibilitando-lhes se esconder das autoridades e de outras pessoas na comunidade.

Document Outline

- Antes de você ler este livro
- ÿþP
  - O Ataque
  - William e as raízes do Anonymous
  - Todo mundo vem para cá
  - Kayla e a ascensão do Anonymous
  - Projeto Chanology
  - Guerra civil
  - FOGO FOGO FOGO
  - Tiros que saíram pela culatra
  - O revolucionário
  - Conhecendo a ninja
  - O rescaldo
- Parte 2 - Fama
  - Encontrando uma voz
  - Conspiração (que nos une)
  - Backtrace ataca
  - Dando um tempo
  - Falando sobre uma revolução
  - Lulz Security
  - A ressurreição deTopiary e Tupac
  - Guerra hacker
  - Mais Sony, mais hackers
  - Estresse e traição
  - O retorno de Ryan, o fim da razão
  - Fim explosivo
  - O destino do Lulz
- ÿþP
  - O verdadeiro Topiary
  - O verdadeiro Sabu
  - A verdadeira Kayla, os verdadeiros Anonymous
- Epílogo
- Agradecimentos
- Linha do tempo

- Notas e fontes
- Glossário

Table of Contents

Antes de você ler este livro
ÿþP
    O Ataque
    William e as raízes do Anonymous
    Todo mundo vem para cá
    Kayla e a ascensão do Anonymous
    Projeto Chanology
    Guerra civil
    FOGO FOGO FOGO
    Tiros que saíram pela culatra
    O revolucionário
    Conhecendo a ninja
    O rescaldo
O Ataque
William e as raízes do Anonymous
Todo mundo vem para cá
Kayla e a ascensão do Anonymous
Projeto Chanology
Guerra civil
FOGO FOGO FOGO
Tiros que saíram pela culatra
O revolucionário
Conhecendo a ninja
O rescaldo
Parte 2 - Fama
    Encontrando uma voz
    Conspiração (que nos une)
    Backtrace ataca
    Dando um tempo
    Falando sobre uma revolução
    Lulz Security
    A ressurreição deTopiary e Tupac
    Guerra hacker
    Mais Sony, mais hackers
    Estresse e traição

- O retorno de Ryan, o fim da razão
- Fim explosivo
- O destino do Lulz

Encontrando uma voz
Conspiração (que nos une)
Backtrace ataca
Dando um tempo
Falando sobre uma revolução
Lulz Security
A ressurreição deTopiary e Tupac
Guerra hacker
Mais Sony, mais hackers
Estresse e traição
O retorno de Ryan, o fim da razão
Fim explosivo
O destino do Lulz
ÿþP

- O verdadeiro Topiary
- O verdadeiro Sabu
- A verdadeira Kayla, os verdadeiros Anonymous

O verdadeiro Topiary
O verdadeiro Sabu
A verdadeira Kayla, os verdadeiros Anonymous
Epílogo
Agradecimentos
Linha do tempo
Notas e fontes
Glossário