NETWORK SECURE

RELATORIO GERENCIAL

BUG RCE NO RDP

Possível Ataque Ransomware

NETWORK SECURE

SOLUÇÕES

SERVIÇOS ESPECIALIZADOS

- Análise de risco
- Análise de vulnerabilidade
- Política de segurança da informação
- Auditoria em segurança da informação
- Perícia forense computacional
- Projetos de segurança da informação
- Implantação de soluções e produtos
- Plano de continuidade de negócios
- Classificação da informação

MSSP

(Provedor de Serviço Gerenciado de Segurança da Informação)

Monitoramento

- Dashboard em tempo real de utilização e eventos
- Relatórios periódicos e customizáveis

SUPORTE

- Suporte especializado
- SLA 2H, 4H e 8H
- Suporte Nível 2 ou Superior
- RMA local de equipamentos

GERENCIAMENTO

- Gerenciamento centralizado e/ou compartilhado
- Gerenciamento de mudança e configuração

- Antimalware
- Análise de vulnerabilidade
- Controle de acesso web
- Controle de dispositivos (pen drive, modem/3G, wifi e etc)
- Firewall / UTM / NGFW
- IPS (intrusion prevetion system / sistema de detecção de instrusos)
- Anti spam
- Autenticação forte
- Balanceamento de carga
- Controle de conteúdo e cache web
- Criptografia
- DLP
- NAC / EVAS
- Otimização de wan
- Segurança para virtualização
- Visibilidade / monitoramento
- Wireless / wifi
- CGNAT
- Vídeo monitoramento

NOSSOS PARCEIROS

KASPERSKY lab · FORTINET · IBM Security · BLUE COAT · Extreme networks · ForeScout · CISCO · PRTG NETWORK MONITOR · JUNIPER NETWORKS · A10

QUEM SOMOS

Fundada em 2002, a **NETWORK SECURE** é uma empresa especializada em Segurança da Informação e vem se aprimorando na utilização de técnicas e metodologias de segurança com profissionais certificados para garantir sucesso aos projetos de seus clientes. O método e organização do trabalho no atendimento aos clientes são personalizados para garantir a satisfação, qualidade dos serviços e resultados esperados. Para isso, a empresa conta com uma equipe de profissionais altamente capacitados e com experiência em Tecnologia e Segurança da Informação.

VISÃO

Ser a melhor empresa de serviços e de soluções em Segurança da Informação do Brasil, oferecendo aos nossos clientes: Parceria, Gestão, Resultados e Inovação.

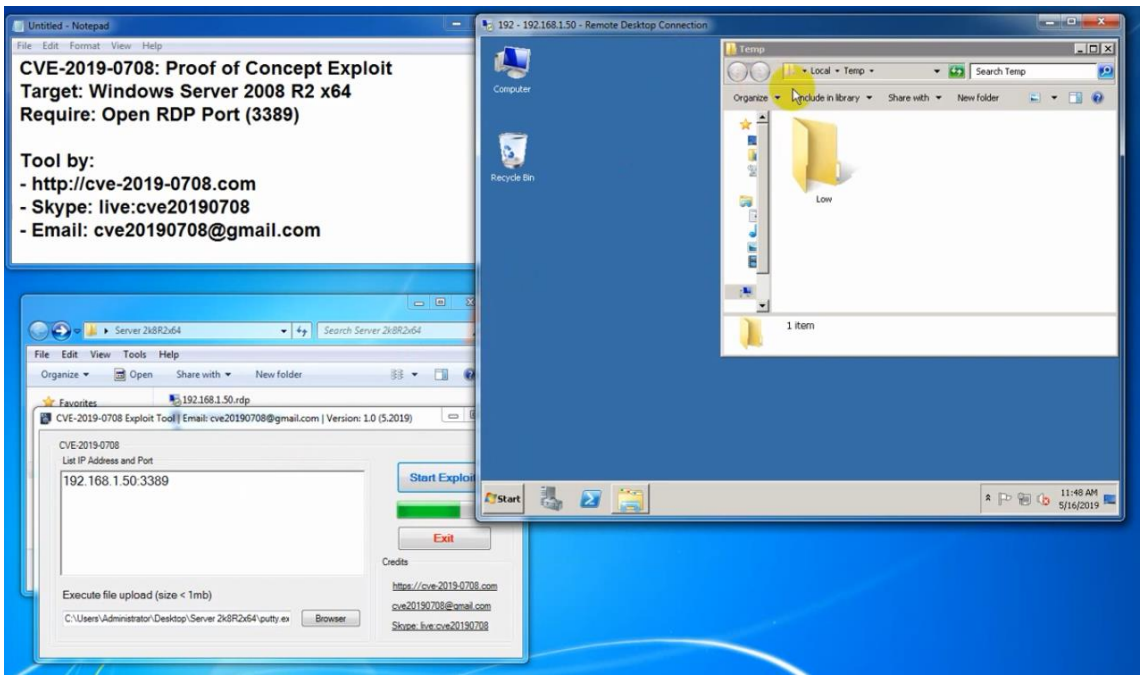
MISSÃO

Oferecer e promover serviços, soluções inovadoras e confiáveis em tecnologia e segurança da informação, para os setores público e privado, potencializando suas atividades por meio de:

- Produtos e serviços inovadores;
- Soluções líderes de mercado;
- Foco nos resultados;
- Profissionais especializados em constante capacitação;
- Buscando valorização e desenvolvimento pessoal e profissional de cada colaborador e parceiro.

Versão			
#	**Data**	**Revisão / Descrição**	**Autor**
1.0	17/05/2019	Criação do documento	Hamir Campos Analista de Segurança Senior **Network Secure**

Bug RCE no protocolo RDP permite que hackers executem ataque WannaCry em 3 milhões de endpoints vulneráveis



Uma vulnerabilidade crítica de execução remota nos serviços de área de trabalho remota da Microsoft permite que os invasores comprometam o sistema vulnerável com o malware do nível WannaCry.

A Microsoft corrigiu recentemente essa vulnerabilidade de RCE nos Serviços de Área de Trabalho Remota – anteriormente conhecida como Serviços de Terminal, e afetou parte da versão antiga do Windows.

Um ataque WannaCry foi um dos notórios ataques cibernéticos nesta década e fechou milhões de computadores em todo o mundo, explorando a vulnerabilidade no protocolo RDP.

Nesse caso, o protocolo RDP (Remote Desktop Protocol) em si não é vulnerável, mas os invasores precisam executar a pré-autenticação e não exigem interação do usuário.

Esta vulnerabilidade não tinha nenhuma exploração neste momento, mas, no futuro, um invasor criará um malware que explora essa vulnerabilidade de maneira semelhante ao ataque WannaCry.

Os sistemas de suporte vulneráveis incluem o Windows 7, o Windows Server 2008 R2 e o Windows Server 2008, além de versões de suporte do Windows 2003 e do Windows XP.

Inicialmente, um invasor não autenticado enviará a solicitação mal-intencionada especialmente criada aos sistemas vulneráveis depois que estabelecerem uma conexão por meio do RDP.

Segundo a Microsoft , essa vulnerabilidade é um pré-autenticação e não requer interação do usuário. Um invasor que explora com êxito essa vulnerabilidade pode executar um código arbitrário no sistema de destino. Um invasor pode então instalar programas; visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário.

Um pesquisador independente, Kevin Beaumont, disse que, com base no mecanismo de busca Shodan, cerca de 3 milhões de endpoints RDP estão diretamente expostos à Internet.

Esse tipo de ataque já está sendo comercializado na internet livremente, conforme demonstrado o vídeo abaixo:

https://youtu.be/SCsJ9Uq3POk

"Há mitigação parcial nos sistemas afetados que possuem o NLA (Network Level Authentication) ativado. Os sistemas afetados são mitigados contra malware "wormable" ou ameaças avançadas de malware que podem explorar a vulnerabilidade, já que a NLA exige autenticação antes que a vulnerabilidade possa ser acionada ", informou a Microsoft .

De acordo com Simon Pope, diretor de resposta a incidentes, o Microsoft Security Response Center (MSRC) "Clientes que executam o Windows 8 e o Windows 10 não são afetados por essa vulnerabilidade".

Recomendações:

- Remover todo e qualquer acesso de servidores aberto diretamente na internet pelo protocolo RDP, independe de porta padrão ou customizada
- Utilizar VPN para estabelecer uma conexão segura e acessar o sistema

Referencias

https://www.cvedetails.com/cve/CVE-2019-0708/