Cavalos de Tróia

1. Saiba o que são os cavalos de Tróia

Cavalos de Tróia são programas que vem escondidos dentro de outros sem que o usuário saiba de sua existência. Eles podem permitir que outra pessoa obtenha controle sobre a máquina de um internauta conectado à Internet.

Atualmente, o recursos tem sido amplamente utilizado para invadir máquinas conectadas à Internet. A tática é simples: mandar um programa qualquer (protetores de tela ou animações engraçadinhas, por exemplo), que na verdade contém inserido um outro que dá ao hacker acesso remoto à máquina onde o cavalo de Tróia foi instalado. Esses softwares são verdadeiras portas de acesso ao conteúdo do computador.

Os Cavalos de Tróia permitem que outra pessoa obtenha controle sobre a máquina do usuário, através do protocolo TCP/IP da Internet. Testes demonstraram que o administrador remoto é capaz de acessar dados e efetuar tarefas com mais eficiência do que o próprio usuário que está em frente à máquina.

2. Conheça os programas Back Orifice, Netbus, Sockets de Tróie e outros

Entre os principais troianos estão o Back Orifice (BO), que se instala em micros que rodam o Windows 95/98, o NetBus, capaz de rodar também no Windows NT, o Master's Paradise 98 e o Sockets de Troie (ST). Todos apresentam características semelhantes: permitem administração remota, revelam as senhas contidas no sistema operacional do usuário e mostram em tempo real tudo aquilo que é digitado.

3. Dicas para evitar a invasão de seu micro

- **Proteja e troque a sua senha**

O controle deve começar pela identidade digital do usuário. User e senha são identificações particulares que merecem o máximo cuidado e sigilo. Com certeza, ninguém gostaria de compartilhar a sua senha bancária ou o número do seu cartão de crédito com mais alguém. O mesmo deve acontecer com a sua senha de acesso.

A troca periódica da senha é um bom começo para quem não quer dar chance ao azar. A maioria dos provedores de acesso oferece esse serviço online. Para maior segurança, o usuário deve utilizar senhas relativamente complexas. No mínimo, utilize uma senha alfanumérica com 6 caracteres. Mantenha o hábito de conferir o extrato detalhado da utilização da sua conta de acesso. Ao notar qualquer alteração no número de horas utilizadas, entre em contato com administração do seu provedor.

Isso evita alguns problemas, mas não funciona se o seu computador já tiver um cavalo de Tróia instalado. Isso porque alguns desses programas permitem ao hacker roubar a sua senha do seu próprio micro. Nesse caso, é necessário desinstalar o troiano de sua máquina, antes de mais nada. Para saber se há algum cavalo de Tróia instalado em sua máquina, você precisa de um programa detector.

- **Não execute programas de origem duvidosa**

Antes de mais nada, para evitar que a sua máquina seja vítima de um ataque deste tipo, recomendamos que você pense duas vezes entes de rodar qualquer arquivo executável (qq_coisa.exe) encontrado na rede ou recebido por e-mail. Mesmo que você receba um executável de um conhecido ou amigo, procure saber antes a procedência do mesmo.

- **Seja cauteloso com o IRC e ICQ**

Muitos dos programas de IRC tem bugs conhecidos que permitem aos usuarios enviar executáveis para outros, em certas circunstâncias. Não aceite programas (jogos, screensavers etc.) recebidos

via IRC porque não há como saber quem o está enviando, e também nunca se deve deixar o IRC aceitando automaticamente transmissões de arquivos ou executando scripts. As mesmas precauções valem para o ICQ. Não acredite em noticias recebidas ao acaso dizendo coisas como "use este programa para atualizar seu ICQ" ou "rode este patch para proteger seu Explorer" etc. Se receber algo assim, confira sempre as notícias no site do fabricante do software em questão.

- **Atualize o seu navegador periodicamente**
Além da troca de senha, o usuário precisa manter seus softwares sempre atualizados. Tanto o navegador da Netscape quanto o da Microsoft (Internet Explorer) já apresentaram bugs de segurança em quase todas as suas versões. Tão logo estes bugs são descobertos, as respectivas fabricantes oferecem patches de correção para os problemas. Visitas regulares ao site da fabricante do seu navegador preferido o ajudarão na coleta de informações sobre os bugs e suas respectivas correções.

4. Copie programas para se defender

Para evitar que a sua máquina seja vítima do ataque de um hacker utilize um Firewall,