

## SEGURANÇA

## Sob o domínio do mal

Como blindar seu PC? Leia trecho de um novo livro que propõe exatamente isso.

POR ANDRÉ MACHADO E ALEXANDRE FREIRE

Os principais problemas de segurança que acontecem nos computadores domésticos são causados, em sua maioria, pela falta de conhecimento do usuário sobre o código malicioso que prolifera por aí e sobre o próprio sistema operacional que ele usa. Ainda há muito desperpício sobre as melhores práticas e procedimentos cotidianos no computador e na navegação na internet. Na grande rede, é preciso saber mais sobre os sites visitados e os locais de onde se baixam arquivos e programas de diversos tipos. No computador, é preciso aprender a discernir os indícios de que há uma contaminação e a configurar e usar software de segurança — antivírus, firewalls pessoais, sistemas de detecção de intrusão e assim por diante.

Atualmente maioria das pessoas, está com seu computador contaminado sem saber. Mesmo profissionais experientes e acostumados a trabalhar online relatam por vezes o desvio de dinheiro após um acesso ao internet banking ou a invasão de seus computadores por um cavalo de Tróia. Isso acontece porque, por mais experientes que sejam, eles não tiveram cuidados suficientes ao manipular seus arquivos. Em suma, ninguém está livre de um ataque virtual.

#### MENTE HACKER

Como funciona a mente de um hacker? Hoje em dia, especialmente no Brasil, os principais ataques a usuários domésticos se dão por meio do phishing — a disseminação de e-mails falsos contendo um link igualmente falso, no qual a pessoa é induzida a clicar. Boa parte desses links leva, quando se acessa uma página de internet falsa, ao download de um arquivo com terminação .SCR (de "screensaver"). Geralmente, esse arquivo traz um cavalo de Tróia embutido.

Também há softwares (spywares, ou programas espíões) que ficam monitorando o internet banking do usuário, procurando verificar em que banco tem

sua conta. Cavalos de Tróia também fazem isso — alguns são programados, inclusive, para se ativar quando na barra do navegador (browser) surgir o nome de alguma instituição bancária. Uma vez ativados, esses cavalos de Tróia podem gravar tudo o que é digitado pela pessoa enquanto está fazendo sua operação bancária — login, senha, dados cadastrais, números de documentos e muito mais. Na hora em que a pessoa sai do site do banco, o código malicioso se desativa, para evitar suspeitas.

Claro, há também ataques de vírus, mas os maiores estragos e prejuízos, são causados por cavalos de Tróia e phishing. A polícia tem cada vez mais dificuldade em lidar com essas ameaças e os desvios de dinheiro crescem a cada dia. A grande motivação do hacker, hoje, é o dinheiro. (Nota da redação: a afirmação dos autores confirma a frase de Eugene Kaspersky, em entrevista à PC Magazine 14)

Um hacker do mal, por definição, é um sujeito com bons conhecimentos de programação e informática que os usa para espionagem industrial ou para lesar financeiramente pessoas, empresas ou instituições. Quem invade sites para fazer pichações virtuais,

por exemplo, nem é mais considerado hacker hoje em dia.

No Brasil, nem se trata mais de hackers ou crackers: são criminosos ou organizações criminosas que vêm atuando na área. O conhecimento de informática, nesse caso, é o mínimo possível — na verdade, com os kits de construção de códigos maliciosos dando sopa na internet, nem é preciso ter tanto conhecimento assim para operar um cavalo-de-Tróia. Os chamados "script kiddies" proliferam facilmente, seja buscando esses dados na web ou mesmo usando ferramentas de desenvolvimento encontradas em revistas com CDs vendidas em qualquer banca de jornal.

Além do phishing, os cavalos de Tróia podem vir junto com anexos em mensagens de e-mail. E os antivírus não os detectam facilmente quando já estão trabalhando dentro de um sistema operacional. Mas quais são as diferenças entre essas grandes ameaças virtuais — vírus, worms, cavalos de Tróia etc? No restante do livro, já à venda, o leitor irá conhecer as definições e prosseguir jornada pela segurança. A obra também fala das práticas comuns dos hackers, como sniffing, ataques de força bruta e outros. ☰



#### SOBRE OS AUTORES

O livro "Como Blindar seu PC" (Campus/Elsevier, R\$ 49,90) tem o objetivo de levar os conceitos e práticas de segurança para mais perto do usuário, doméstico ou um pouco mais avançado. A obra pretende levar para o dia-a-dia os conceitos já aplicados nos sistemas das empresas: garantir que as informações dos usuários estejam íntegras, disponíveis e protegidas. André Machado é repórter e colunista do jornal "O Globo" e Alexandre Freire é profissional de TI especializado em segurança da informação.