informática

CORREIO BRAZILIENSE

Brasília, terça-feira, 12 de abril de 2005
Editor: Renato Ferraz//renato.ferraz@correioweb.com.br
e-mail: informatica@correioweb.com.br
Tel: 214 1184

CRIME VIRTUAL
E CASTIGO REAL

INDÚSTRIA DE SOFTWARES PIRATAS INCLUI CÓDIGOS MALICIOSOS NAS CÓPIAS BRASILIENSES DE UM DOS ANTIVÍRUS MAIS POPULARES, O NORTON

LUIZ HENRIQUE QUEMEL
ESPECIAL PARA O **CORREIO**

Quando você compra um antivírus top de linha, segue corretamente cada passo da instalação e faz todas as atualizações necessárias na internet, você parte do pressuposto que sua máquina vai estar protegida contra qualquer ameaça virtual, mesmo que o software seja pirata. Afinal, é apenas uma cópia do original. Certo? Estaria se não fosse o fato de quem fez as cópias ter modificado "geneticamente" o programa e inserido um cavalo de tróia que abre não só um buraco, mas uma verdadeira cratera no seu sistema. Até agora foram encontradas cópias corrompidas em Brasília, Goiânia, Rio de Janeiro, Belo Horizonte, Recife, Porto Alegre, São Paulo, Curitiba e Belém.

Foi isso que aconteceu com as cópias piratas testadas pelo **Correio** do Norton System Works (NSW), Norton Internet Security (NIS) e Norton Antivírus (NAV) 2005. Repetimos: somente as cópias piratas apresentaram o código malicioso. O alerta foi dado depois que a coluna InfoAjuda recebeu dezenas de reclamações sobre o mal funcionamento desses softwares. E todas tinham algo em comum — mesmo com o firewall e o antivírus instalados e devidamente atualizados, o comportamento da máquina era estranho. Lentidão, demora em abrir páginas e, após certo tempo, um arquivo vital para o sistema operacional era apagado.

Durante três meses os programas foram investigados. O que foi descoberto foi um misto de cultura pirata e crime informático. De dez dúvidas que chegam à coluna, sete são relacionadas às pragas virtuais e, dentre elas, cinco são relativas a programas gratuitos que não funcionam. A queixa dos leitores era justamente que, uma cópia paga (R$ 10), mesmo que pirata, acumulava problemas diversos. Vale observar que quem vende o software falsificado também ignora o fato de o programa ter falhas de segurança. A origem do problema está em quem copiou o programa e introduziu o cavalo de tróia antes de repassar o software para o comércio.

O *Informática* visitou diversos leitores e pôde constatar que, em todos os casos de comportamento estranho da máquina, o problema tinha origem na mesma cópia batizada dos produtos da Symantec. Partindo desse ponto, três amostras (NSW, NIS e NAV 2005) de diversos pontos de venda foram recolhidas, totalizando 21 cópias dos produtos. Na análise do código dos programas, todas as amostras tinham origem em uma única matriz "geneticamente" modificada e pronta para deixar o computador aberto ao roubo de informações.

O usuário nem imaginaria que ao adquirir esses produtos estava na verdade facilitando o trabalho dos crackers. Ou que ao instalar a versão pirata abriria uma porta ou serviço para que remotamente as informações fossem coletas. Foi o que aconteceu com Carlos*, 38 anos, eletrotécnico. "Eu utilizava a versão 2003, mas ela expirou e um colega me emprestou a versão 2005. Deu tanto problema que eu tive que desinstalar o programa", conta. A maioria dos usuários não teve a sorte de, mesmo sem saber do perigo, cortar o mal pela raiz.

O golpe

Quando o CD é inserido no PC, a primeira coisa que ele faz é garantir que a máquina seja devidamente configurada para que o cavalo de tróia se estabeleça como uma aplicação válida. Nesse momento é carregado para a memória o programa SHEL.EXE, que cuida de mudar as páginas e, em algumas versões, incluir um DNS (servidor responsável por pesquisar e encontrar as páginas da internet) falso no arquivo LMHOST.SAM. Em caso de o usuário digitar o site do Banco do Brasil, por exemplo, ele será direcionado para um site igual ao do banco, mas na verdade falso (*phishing scam*).

O segundo passo seria registrar o aplicativo AUTODATA.EXE, contendo o código malicioso, como um programa válido, permitindo dessa forma que o firewall e o antivírus o identificassem como uma aplicação válida. Muitos leitores se irritaram e creditaram a falha aos fabricantes, quando o responsável por abrir a porta, deixar o bandido entrar e depois fechá-la foi o próprio usuário.

A última providência era deixar que os programas fossem carregados na memória e permitissem o monitoramento da máquina. São eles os arquivos WINHLP16.EXE e WINIT.EXE, gravados no Registro. Se o usuário já tem instalado outro produto, como o AVG ou McAfee, essa operação é abortada. No entanto, existe um programa que continua ativo. O KEYGEN.EXE serve para gerar a chave de ativação do software pirata, onde é solicitada uma contra-senha.

Para identificar como eles agem, foi deixado, durante 83 dias, um servidor *honeypot* (armadilha contra crackers) monitorado pelos bandidos (na verdade eram os piratas cibernéticos que estavam sendo vigiados). E enviadas uma conta bancária e senhas falsas.

Logo depois de inserir os dados da conta no sistema, a janela do navegador informou que o arquivo WINHLP16.EXE havia provocado um erro. A máquina foi reiniciada e, após o boot, apareceu a mensagem fatal: "arquivo NTLDR faltando...tecle CTRL+ALT+DEL". Logo em seguida, os piratas cibernéticos recebiam as informações necessárias para destruir a máquina do usuário. Fica a dica: compre sempre produtos originais.

*** NOME FICTÍCIO**

LEIA MAIS SOBRE O RISCO DOS SOFTWARES PIRATAS NA
PÁGINA 3