**Crimes na Web: BlackHole mira usuários Windows no Brasil**

A Kaspersky Lab identificou a chegada de uma nova modalidade de cibercrime no Brasil. Os cibercriminosos passaram a adotar o uso de exploit kits, pacotes de códigos maliciosos prontos e negociados entre cibercriminosos com o intuito de automatizar ataques através da navegação web. O escolhido foi o BlackHole, criado e largamente utilizado entre cibercriminosos do leste europeu. Ele foi encontrado em um ataque recente, visando distribuir trojans bancários.

O BlackHole explora falhas de segurança em softwares populares e assim potencializa o número de novas vítimas e de computadores infectados. Esse fato revela a existência de negociações comerciais, até então desconhecidas, entre cibercriminosos brasileiros e do leste europeu.

Em muitos casos, os valores envolvidos podem ser bastante elevados: uma cópia da última versão do BlackHole custa em média U$ 2.500,00 (dois mil e quinhentos dólares). Os desenvolvedores também alugam ou vendem versões pré-pagas do kit – o aluguel pode sair por U$ 50,00 (cinquenta dólares) por dia de uso.

De acordo com a análise da Kaspersky Lab, o BlackHole agora está sendo usado em ataques no país para promover a instalação de trojans bancários e, dessa forma, roubar usuários dos serviços de internet banking.

Esta prática deixa os usuários expostos a mais riscos enquanto navegam, com maior possibilidade de infecção sem que percebam o ataque, geralmente bem elaborados e com baixa taxa de detecção e bloqueio pelas soluções de segurança mais usadas.

Segundo Fabio Assolini, analista de malware da Kaspersky no Brasil, “o uso de exploit kits por cibercriminosos brasileiros nos indica que mais usuários estarão em risco, elevando os ataques a outro patamar e potencializando a distribuição de trojans bancários”.

**Táticas dos cibercriminosos com o BackHole**

No Brasil, os ataques usando Blackhole são criados quando os usuários são estimulados pela curiosidade. Um exemplo recentemente identificado foi a técnica de engenharia social, que não é nova, convidando o usuário a clicar e assistir um suposto vídeo da “Juju Panicat”.

Ao clicar no link do vídeo, os usuários foram redirecionados para uma página maliciosa hospedada no domínio co.cc, onde os códigos do exploit kit estavam prontos para entrarem em ação, sem que haja nenhuma outra ação do usuário.

A Kaspersly Lab teve acesso ao painel de controle do caso analisado: no momento da análise, 905 computadores estavam infectados, 378 destes no Brasil. Em um único dia o cibercriminoso infectou 171 pessoas. Usuários de Internet Explorer e Windows XP (que ainda são bastante

usados no Brasil) foram os maiores infectados. Percentualmente, menos de 5% dos usuários do Google Chrome que foram expostos ao golpe foram infectados, contra 23% do Internet Explorer.

**Fonte: Convergência Digital. [Portal]. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31804&sid=18>. Acesso em: 17 set. 2012.**

A utilização deste artigo é exclusiva para fins educacionais.