Atalhos perigosos na internet
Ataide de Almeida Jr.

Sabe quando você precisa passar um site para alguém ou compartilhar um link no Twitter, mas o endereço é muito grande ou complicado? Esses problemas foram resolvidos com encurtadores de URL, com nomes e siglas cada vez menores: bit.ly, ow.ly, e por aí vai. No entanto, por trás desses úteis atalhos de internet podem se esconder spams, vírus e outros males às contas virtuais.

Por sua extensa utilização em redes sociais, os encurtadores de URL se tornaram um dos métodos preferidos dos cibercriminosos, segundo o Relatório do Panorama de Ameças, publicado pela BitDefender. Pelo levantamento, os atalhos são eficientes, pois os usuários não conseguem ver o destino real por trás do link.

Um dos maiores perigos desses endereços desconhecidos é a chance de eles direcionarem os visitantes para um malware. ,,Diante disso, os cibercriminosos podem assumir o controle dos seus sistemas por meio da exploração de vulnerabilidades existentes no software e terem acesso a informações confidenciais, como dados bancários", explica Daniel Parra, gerente de marketing e relações públicas da BitDefender no Brasil.

Com a crescente adesão dos internautas às redes sociais, a tendência é de que os encurtadores sejam cada vez mais utilizados. Segundo Parra, o melhor jeito de prevenir o roubo de dados é simples. ,,Ter cuidado ao clicar em um link encurtado, principalmente se for de alguém desconhecido. Também deve-se usar a regra de ouro para baixar aplicativos na internet: usar somente o fabricante oficial". Utilizar serviços de encurtamento que verifiquem a natureza do conteúdo por trás do link, como o recém-anunciado goo.gl, do Google, ou o saf.li, também é recomendado.

SPAM

No mês passado, um encurtador de URL foi o método utilizado para a disseminação na rede social Twitter de um spam com uma notícia sobre um suposto acidente sofrido por Pe Lanza, vocalista da banda Restart. Os usuários que clicaram no link acionaram um script que fazia seus perfis postarem automaticamente a mensagem em seus perfis, o que gerou uma avalanche de mensagens falsas no microblog.

O funcionário público Leonardo Mendes, 27 anos, foi um dos que clicaram no link naquele dia, e acabou sofrendo com uma série de outros spams em seu perfil. Ele conta que não percebeu o spam porque pensava que era uma brincadeira, já que várias pessoas estavam tuitando rapidamente a mensagem. ,,No e-mail, quando alguém que você não conhece manda uma mensagem, você consegue perceber, mas no Twitter foi uma surpresa", recorda.

Após ver que seu perfil começou a disparar a mensagem, ele imediatamente tomou providências de segurança. ,,Na hora, limpei o cache (do navegador), a memória e, assim que percebi que era vírus, alterei a senha do meu perfil". Ele relata que o problema normalizou após ter alterado boa parte de suas senhas.

O script foi elaborado pelo usuário @Joseph_Felix, que, após disseminar a falsa notícia, assumiu a autoria do ataque e disse ter descoberto uma falha de segurança. O script não infectava o computador nem os perfis, mas utilizava os cookies de autenticação para publicar mensagens involutariamente nos perfis de quem clicou no link.

Logo após a onda de spams, Felix explicou que o spam foi criado com a intenção de alertar a rede de microblog. ,,Gostaria de pedir desculpas aos que foram pegos pelo bug. Fiz isso com a intenção de espalhar e mostrar para o Twitter, sendo que tendo reportado, nada foi corrigido", tuitou. Após o incidente, @Joseph_Felix teve sua conta suspensa.

Na última semana, o Google decidiu entrar na batalha dos encurtadores de URLs com o endereço http://goo.gl/. Antes disponível dentro apenas de aplicações da empresa, o serviço

está disponível para todos os usuários. Além de encurtar endereços, a página oferece estatísticas sobre a quantidade de cliques e alertas se o endereço apontar para um site suspeito de abrigar spam, phishing ou malware.

A busca de hackers com experiência

Parece estranho pensar em ter no quadro de funcionários da empresa uma pessoa que pode invadir sistemas, roubar dados confidenciais e alterar páginas da internet. No entanto, a procura pelos hackers está em franca ascensão puxados pela expansão desse mercado. De acordo com a consultoria Infonetics Research, a área de segurança da informação registrou um crescimento de 119% no primeiro trimestre deste ano em relação ao mesmo período de 2009. A empresa prevê ainda que até 2014 o setor possa se expandir oito vezes mais. É claro que os conhecimentos desses especialistas serão voltados para identificar falhas de segurança antes que outros indivíduos mal intencionados as descubram.

O trabalho na área de segurança pode compensar pelo salário ? em média, R$ 4 mil ?, mas também pode levar muitas horas para ser feito. Segundo o consultor e pesquisador em segurança da informação, Ulisses Castro, da Conviso IT Security, em média, um projeto leva 40 horas para ser concluído. Trabalhos mais complexos podem durar até 320 horas. “Para detectar as falhas são feitas varreduras, utilizando ferramentas que automatizam o processo de detecção e assinaturas de ataques conhecidos. Porém, o teste não fica completo se não houver uma análise minuciosa e manual de todos os pontos de entrada de dados da aplicação", explica Castro.

Além desses pedidos, as empresas pedem aos hackers para checar o perímetro de segurança de determinado projeto. “Para o consultor não é fornecido nenhuma informação além do nome do alvo chamado de teste de intrusão `black box'. A partir daí, ele tem que pensar e agir como um cracker e precisa realizar os ataques utilizando desde técnicas que envolvem os testes nas aplicações até os de engenharia social onde é colocada à prova a política de segurança da empresa", aponta.

Para o consultor, entrar no mercado de trabalho dos hackers do bem exige conhecimento. ,,Os requisitos para ser um profissional de segurança é ter a habilidade de enxergar e analisar de um ponto de vista que ninguém nunca imaginou, conseguir ver as coisas como um cracker sem ser um e conhecer diversas técnicas de teste". Para ajudar quem já atua na área, Castro criou um blog (http://ulissescastro.com) com informações técnicas e dicas.

CURSOS

Empresas que oferecem cursos de segurança da informação perceberam a demanda por esses profissionais e montaram cursos para torná-los hackers do bem. “Apesar de ainda estarmos na retaguarda em relação a alguns países do primeiro mundo que já contam com leis na área de segurança desde a década de 1990, começamos a dar mais importância a isso agora. As empresas passaram a contratar bastante. O único problema é que os salários do Brasil com relação ao resto do mundo ainda estão muito desiguais", diz Luiz Vieira, professor de cursos de segurança da 4Linux (http:\\www.4linux.com.br).

Fonte: Jornal do Commercio, Rio de Janeiro, 19 out. 2010, Seudinheiro, p. B-8.