Cibercrime está organizado e mais profissional
Gabriela Stripoli

Assim como a TI evoluiu para ambientes e arquitetura complexos, o crime eletrônico está igualmente sofisticado

O desafio de lidar com uma TI complexa, com infraestrutura em nuvem híbrida, aplicações remotas, base de usuários móveis e análise de dados – somado à pressão por inovação – faz parte do dia a dia do CIO. A tecnologia da informação evoluiu, exigindo cada vez mais habilidades multidisciplinares do diretor de TI e uma equipe altamente especializada. Não raro, startups de negócios disruptivos têm sua base em profissionais da área.

Muitos dos melhores desses talentos, contudo, trabalham no lado do mal. Cibercriminosos também aprimoraram suas técnicas de ataque, principalmente quando o foco deles são informações corporativas. “Existe uma certa ingenuidade de empresas latino-americanas em acreditar que elas não são vítimas de APTs”, expõe o diretor da equipe de pesquisa e análise da Kaspersky Lab para América Latina, Dmitry Bestuzhev, na 3ª Cúpula Latino-americana de Analistas de Segurança, que ocorreu em agosto em Cancun, no México. Ele se refere a ameaças persistentes e direcionadas, um tipo de investida sofisticada cada vez mais presente na região.

O especialista da companhia russa de segurança é taxativo: se sua companhia foi um dos alvos de APTs, tenha certeza, houve dados roubados. É difícil sobreviver a esses ataques, pois um simples antivírus não é o suficiente se não obtiver recursos específicos de bloqueio e proteção contra exploits.

O monitoramento feito com base nos usuários de ferramentas da Kaspersky Lab dá conta de 500 mil usuários únicos para cada tipo de exploit. Elas bloqueiam 12 ameaças por segundo, ou 17.043 ataques diários.

No ranking das ameaças mais frequentes na América Latina, um script de código avançado encabeça a lista. “A maioria delas vem pela internet. Pela quantidade de usuários, somos bombardeados por ameaças virtuais”, relata Bestuzhev. É o caso do chamado ataque waterhole, com o qual cibercriminosos inserem códigos maliciosos em uma página web convencional.

Ao visitar o site, é praticamente impossível detectar a ameaça, capaz de infiltrar-se na máquina apenas por ser aberta em um navegador. Assim, criminosos chegam aos dados corporativos contando insistentemente com um comportamento simples e recorrente dos funcionários da empresa – o acesso à uma página web de notícias, ou internet banking, até mesmo sites de e-commerce. Recentemente, Apple e Facebook foram surpreendidos pela infecção.

Outra abordagem explora pontos fracos em sistemas de companhias, e alguns deles podem ser simples brechas que abrem portas para graves crises de segurança. É o exemplo do exploit Java.cve 2013-0431.gen, que se aproveita de uma vulnerabilidade do Java e já é uma das ameaças mais comuns detectadas no primeiro semestre em todo o mundo. Através dele, informações de empresas, meios de comunicação e embaixadas foram desviadas por ciberespiões. “O Brasil, logo atrás da Rússia, concentra a presença desse exploit, com taxas de êxito elevadas. Como garantir que todos os usuários de uma empresa atualizam o Java periodicamente?”, provoca Bestuzhev.

Proteção pró-ativa

Como, então, se proteger? O especialista recomenda o monitoramento da rede, o que ele garante não ser uma prática comum nas companhias latino-americanas. Sistemas de rede definida por software (SDN) começam a permitir melhor gestão, entretanto, não são bem utilizados por CIOs latino-americanos. “É preciso ter um bom sistema de gestão. Saber qual seu tráfego, analisar seu conteúdo, coisas básicas como quem está acessando a rede”,

enumera. Assim, ao menos, será possível detectar intrusos e talvez até montar emboscadas, controlando a largura de banda corporativa.

“Os ataques sofisticados têm um único tipo de objetivo: acessar um dado e roubá-lo”, resume Bestuzhev. “E culturalmente, empresas latino-americanas se concentram apenas em remediar, tomar alguma precaução quando o roubo já aconteceu, enquanto deveriam trabalhar em duas frentes: prevenir e remediar”, finaliza. No caso de APTs e roubo de dados, agir depois que o roubo aconteceu pode ser tarde demais.

Fonte: Information Week. [Portal]. Disponível em: <http://informationweek.itweb.com.br/15718/cibercrime-esta-organizado-e-mais-profissional/>. Acesso em: 1 out. 2013.