Malware no Peru indica tendência inédita de ciberespionagem na América Latina
Adriele Marchesini

Malware Medre, direcionado a roubar arquivos de Autocad, mostra que ataques oportunistas dão espaço para invasões corporativas direcionadas na região

Um alerta no Peru chama a atenção para a segurança da informação na região da América Latina como um todo: um caso direcionado de espionagem industrial por meio de uma invasão do tipo Advanced Persistent Threat (ou ameaça avançada e persistente, da sigla em inglês) roubou dez mil projetos de Autocad peruanos. É preciso entender, por isso vale a repetição, que os focos eram extremamente claros: projetos de Autocad e o Peru. "Esta foi a primeira vez que vimos algo neste nível na América Latina", contou Raphael Labaca, especialista em educação e pesquisa do laboratório de segurança da Eset na América Latina.

"Não podemos dizer que existe uma forte tendência de APT, mas este é o único caso em que um malware foi feito especificamente para uma empresa", continuou Labaca. Segundo o executivo, o Brasil também registra casos esparsos, mas nada ainda com força o suficiente ou em frequência de ocorrências que possa configurar um auge da ameaça. "Não posso dizer que a AL está em um auge de ataques direcionados, nem posso falar que espionagem representa uma porcentagem específica dos casos na região. O que posso afirmar é que estamos vendo casos que nunca havíamos visto", garantiu.

Para explicar esse foco, Labaca detalhou que a maior parte dos projetos roubados pelo Medre eram de empresas peruanas em mais de 90% das ocorrências. Uma parcela menor acabou por atingir outros países, como Equador, Colômbia, Estados Unidos e até mesmo Brasil (a menor proporção de todas), mas isso foi causado muito mais pela propagação incontrolável – característica típica dos vírus (humanos ou de computador) - do que por objetivo.

De qualquer forma, o especialista explicou que oportunismo, ainda, é o principal meio utilizado pelos cibercriminosos para roupas suas vítimas. As ameaças específicas são outro nível do malware, com mais assertividade e maior retorno do "investimento". No caso do troias ou botnets, por exemplo, a ideia é alcançar o máximo número de usuários, porque a "receita" obtida pela ação é de valor reduzido. É no volume que se ganha.

Ainda segundo Labaca, explicar roubo de dados por espionagem é algo difícil. Diferentemente de um bem, quando um hacker rouba um arquivo, ele não desaparece da máquina da vítima – ele é copiado para em outro servidor. Além disso, não sai dinheiro da conta-corrente da empresa e, com isso, a compreensão do risco torna-se muito menor neste caso.

APTs

As APTs não são uma novidade no mercado de segurança da informação. Diferente dos malwares comuns, esses programas têm objetivos específicos e extremamente direcionados. Seriam uma evolução dos vírus convencionais, com foco no corporativo. Impossível não levar em consideração o Stuxnet (ameaça voltada para paralisar o enriquecimento de urânio no Irã) e Flame (voltado para máquinas Windows também no Irã) ,e outros exemplos.

Talvez não tão repercutido são operações como a Aurora, que de dezembro de 2010 a janeiro de 2011 buscou promover ações contra a Adobe, Google, Juniper, entre outras, explorando a vulnerabilidade de dia zero no Microsoft Internet Explorer. O processo era de direcionar usuários a sites maliciosos e instalar cavalos de Troia e ferramentas de acesso remoto, como forma de roubar documentos confidenciais.

Outro exemplo foi o Shady Rat, que teve duração de cinco anos e afetou 14 geografias do mundo. Diversos países foram alvo, tanto corporações públicas quanto privadas e, no total, foram 72 empresas comprometidas e 32 tipos de organizações.

Fonte: Information Week [Portal]. Disponível em: <http://informationweek.itweb.com.br/10997/malware-no-peru-indica-tendencia-inedita-de-ciberespionagem-na-america-latina/>. Acesso em: 19 out. 2012.