A ameaça dos espiões digitais na China
Nicole Perlroth

Viagem corporativa ao país exige 'operação de guerra' para evitar roubo de informações

Quando Kenneth G. Lieberthal, membro da Brookings Institution e especialista em assuntos ligados à China, viajou para esse país, seguiu uma rotina que parece típica de um filme de espionagem.

Ele deixou seu celular e o laptop em casa e levou consigo aparelhos emprestados, cujo conteúdo foi eliminado antes de ele partir dos Estados Unidos e apagado em seu retorno. Na China, Kenneth desabilitou o Bluetooth e o wi-fi, e jamais deixou o celular longe da sua vista. Nas reuniões, não só desligava seu telefone, mas também removia a bateria do aparelho, por temor de que o seu microfone pudesse ser ligado remotamente.

Ele se conectava à internet somente por meio de um canal codificado com senha protegida e a operação de copiar e colar a senha era realizada a partir de um pen drive. Jamais digitava sua senha diretamente porque, segundo disse, "os chineses são muito bons na instalação de software para acessar registros chave no seu laptop".

Padrão. O que outrora poderia parecer um comportamento paranoico hoje é o procedimento operacional padrão para funcionários de agências do governo americano, grupos de pesquisa e companhias que realizam negócios na China e na Rússia - como Google, o Departamento de Estado ou a McAfee, a empresa gigante no setor de segurança na internet. A espionagem digital nesses países é uma ameaça real e crescente - para obter informações confidenciais do governo ou segredos empresariais.

"Se uma companhia tem uma propriedade intelectual importante em que os chineses e russos estão interessados e você vai a um desses países com dispositivos móveis, eles conseguem penetrar nos aparelhos", disse Joel F. Brenner, antigo agente do serviço de inteligência americano.

O roubo de segredos comerciais por muito tempo foi trabalho dos chamados "insiders" - espiões corporativos ou funcionários contrariados com sua empresa. Mas hoje é mais fácil roubar informação remotamente por causa da internet, da proliferação dos smartphones e o hábito dos empregados de conectar seus aparelhos pessoais às redes corporativas e carregar informações de propriedade da empresa. O modus operandi preferido dos hackers, segundo especialistas em segurança, é entrar nos aparelhos portáteis dos funcionários e então invadir as redes da empresa e roubar segredos sem deixar nenhum vestígio.

Os alvos dos ataques destes ciberpiratas não gostam de abordar o problema e as estatísticas são escassas. Muitas das invasões não são informadas, dizem os especialistas em segurança, porque as empresas vítimas temem que a divulgação do fato possa afetar o preço das suas ações, ou porque algumas nunca tomam conhecimento da pirataria em si.

Incidente. Mas a envergadura do problema é ilustrada por um incidente ocorrido na Câmara de Comércio americana em 2010. A Câmara não sabia que ela e várias organizações associadas eram vítimas de um roubo cibernético há meses, até o FBI informar que um grupo que servidores na China estava roubando informações de quatro executivos da Câmara que iam com frequência ao país. Na época em que a Câmara resolveu checar a rede, os hackers tinham invadido seus computadores e roubado e-mails por seis semanas. Mais tarde foi descoberto que a impressora de um escritório e até o termostato em um dos apartamentos usados por funcionários tinham comunicação com um endereço de internet na China.

A Câmara não informou como os hackers se infiltraram nos seus sistemas, mas a primeira medida que adotou após o ataque foi proibir os funcionários de levarem aparelhos quando viajassem para "determinados "especialmente a China", disse um porta-voz.

O fato, disse Jacob Olcott, especialista em segurança na internet na Harbor Consulting, é que os aparelhos levados para a China eram pirateados. "Todos sabem que, se você vai realizar negócios na China, no século 21, não deve levar nada consigo."

As embaixadas da China e da Rússia em Washington não responderam aos vários pedidos para comentar o assunto. Mas depois que o Google acusou hackers chineses de invadirem seu sistema em 2010, as autoridades do país emitiram comunicado dizendo que "a China está comprometida em proteger os direitos e interesses legítimos das empresas estrangeiras em nosso país".

Mas especialistas em segurança e autoridades dos Estados Unidos e autoridades dizem que a preocupação é crescente com as invasões de hackers nas redes de empresas.

Em depoimento à comissão de inteligência do Senado, James R. Clapper, diretor da inteligência nacional, alertou sobre o roubo de segredos comerciais por "entidades" dentro da China e da Rússia. Mas Mike McConnell, ex-diretor da agência e hoje consultor, disse em entrevista que, "examinando sistemas informatizados importantes - no Congresso, no Departamento da Defesa, aeroespacial, empresas com segredos comerciais valiosos -, não encontramos uma ameaça persistente avançada".

Fonte: O Estado de S. Paulo, São Paulo, 12 fev. 2012, Economia & Negócios, p. B15.