Participação de hackers russos nas eleições dos EUA acende alerta

Finalmente, o presidente eleito dos EUA, Donald Trump, admitiu, nesta quarta-feira (11/1), que a Rússia invadiu os computadores do Comitê Democrata que geriu a campanha de Hillary Clinton. A seu estilo, Trump contra-atacou: a culpa foi de Hillary. Nisso ele tem razão. Como disse, o Comitê Democrata não fez nada para bloquear ataques cibernéticos a seus computadores. O Comitê Republicano tomou providências para não sofrer tais ataques.

Para o consolo de povos mais descuidados, os últimos anos da era cibernética provaram um fato que poucos se deram conta: americanos só fecham a porta depois de roubados. Por descuido dos mais altos escalões do Partido Democrata, os russos conseguiram interferir nas eleições presidenciais dos EUA e, possivelmente, mudar o resultado das eleições. Em três estados, a diferença de votos, em favor de Trump, foi de cerca de apenas 40 mil votos.

Trump só admitiu que a Rússia invadiu os computadores dos democratas porque dirigentes dos três principais órgãos de segurança do país — CNA (Agência Nacional de Segurança), CIA e FBI — lhe entregaram um relatório e lhe disseram, pessoalmente, a verdade. Mas ele declarou, publicamente, que não há prova de que a invasão influenciou as eleições, porque as máquinas eleitorais não foram atacadas.

De qualquer forma, ele decidiu, como anunciou, fechar as portas: convocou os seis melhores especialistas em segurança cibernética do mundo, todos americanos, segundo ele, para impedir que o país volte a ter sua privacidade em risco. A segurança cibernética passou a ser prioridade nos EUA.

Segundo o *Legaltech News*, os escritórios de advocacia americanos fazem a mesma coisa: só montam um sistema para impedir invasão de seus computadores depois que foram atacados e sofreram prejuízos consideráveis. Provavelmente esse descuido não é exclusividade dos americanos.

Em um artigo para a *Legaltech News*, o copresidente do grupo especializado em segurança de dados e privacidade Morrison & Foerster, Andrew Serwin, especialista em segurança cibernética, governança da informação, privacidade e compartilhamento da informação, ofereceu três observações para a consideração dos advogados. São elas:

1. Os *hackers* não mais objetivam apenas dados de consumidores.
Ataques cibernéticos dirigidos apenas a pessoas, para roubar dados que dão acesso a contas bancárias, cartões de crédito etc., fazem parte da história. Hoje os *hackers* visam dados de empresas, dentro de um processo de espionagem industrial, governos, escritórios de advocacia e outras organizações.

O interesse nos escritórios de advocacia é grande. A última novidade em termos de crimes cibernéticos é o uso de um *malware* chamado *ransomware*. Uma vez instalado em um sistema de computação do escritório, o *hacker* "sequestra" dados e documentos e só os libera mediante o pagamento de um resgate. Bancas americanas já pagaram milhões de dólares para obter seus documentos e outros dados de volta.

Outro crime cibernético comum é o de invasão de documentos de escritórios envolvidos em processos de fusão e aquisição, em que os *hackers* se beneficiam das informações obtidas para comprar e vender

valores mobiliários das empresas envolvidas, obtendo um grande lucro em pouco tempo. Os *hackers* pegos nos EUA estão sendo processados por *insider trading* baseado em *hacking*, uma vez que usaram informações privilegiadas (mesmo que roubadas) para obter lucro fácil, em detrimento dos demais investidores.

Mesmo que o ataque cibernético não objetive o dinheiro fácil, ele pode causar grandes problemas aos escritórios. Exemplo disso foi o que aconteceu com a banca panamenha Mossack Fonseca, da qual os *hackers* roubaram documentos de mais de 214 mil entidades *offshore* e gerou o escândalo conhecido como "Panama Papers". Os papéis foram entregues por um "delator" a um jornal alemão, mas a banca sustenta que eles foram obtidos através de *hacking*.

2. Serviços à venda
Os *hackers* inventaram um novo "modelo de negócios", bastante simples aliás, para ganhar dinheiro fácil: criar *malwares* fáceis de usar e vendê-los a pessoas interessadas em invadir computadores alheios. O *malware* ganhou um nome próprio: "*weaponized malware*" (*malware* para ser usado como arma por um cliente que quer atacar alguém que ele conhece ou uma organização desafeta).

Em essência, o nome também indica que alguns *hackers* se transformaram em "traficantes de armas cibernéticas", que permitem a criminosos sem competência tecnológica fazer seus próprios ataques cibernéticos. Para um escritório de advocacia, isso significa que não é preciso que um *hacker* competente esteja interessado em seus documentos. Basta que a outra parte, que luta contra seu cliente nos tribunais, decida acessar os documentos do escritório.

3. Crime cibernético organizado
Escritórios de advocacia, como outras organizações, às vezes não são visados apenas por um *hacker*, isoladamente. Já há casos registrados de crime organizado, com a participação de vários *hackers* — ou de uma quadrilha —, que trocam informações para obter dados e depois usá-los ou vendê-los. Essa prática é chamada de "*asymmetric threat*" (ameaça assimétrica).

De acordo com *Legaltech News*, os *hackers* estão ficando mais sofisticados e mais perigosos, a exploração "comercial" das invasões está se desenvolvendo a cada dia e, por isso, os escritórios de advocacia também têm de tornar a segurança cibernética uma prioridade.

Date Created
12/01/2017