Uso de malware por órgãos de segurança supõe crimes do bem

No mundo sombrio da espionagem cibernética, órgãos de segurança de muitos países, patrocinados por seus governos, consideram a internet uma zona de guerra. Empregam grupos de hackers altamente profissionais, especializados em "ataque persistente avançado" (APT – advanced persistent attack) para lançar campanhas de espionagem e sabotagem.

Para isso, usam ferramentas criminosas, como *malwares* (software de espionagem), para invadir computadores e quaisquer dispositivos móveis de criminosos e inimigos. Mas também instalam *malwares* em dispositivos eletrônicos de cidadãos comuns e de empresas insuspeitas. Utilizam meios ilegítimos, que "justificam" com fins legítimos: o de combater o crime e garantir a segurança nacional. É como se um crime pudesse ser juridicamente legítimo.

Para o especialista em ataques cibernéticos Eugene Kaspersky, CEO da *Kaspersky Lab*, empresa que investigou os ataques cibernéticos mais complexos e sofisticados já conhecidos, como o *Stuxnet*, *Flame*, *Red October e Regin* e que opera com a Interpol e a Europol, esse é um mal que precisa ser cortado pela raiz, antes que seja tarde demais. Ele escreveu para a revista *Forbes* que, se a sociedade deixar aceitar esse delito oficial, outros crimes oficiais seguirão a mesma trilha.

Grupos governamentais e grupos criminosos usam as mesmas ferramentas de *hacking* e as mesmas táticas cibernéticas — o pessoal "do mal", só para atos criminosos, como o de roubar identidades, dados de contas bancárias e de cartão de crédito. Mas há um terceiro grupo que entrou no jogo há algum tempo: empresas que desenvolvem software de *hacking* e prestam serviços, como um modelo de negócios legítimo e lucrativo, diz Kaspersky.

Uma dessas empresas é o *Gamma Group*, que produz uma variedade de ferramentas de software para *hacking* de PCs e dispositivos móveis, como smartphones Android e iOS. Essas ferramentas possibilitam o roubo de dados confidenciais e até mesmo assumir o controle sobre esses dispositivos.

Essas empresas declaram que só vendem seus produtos a "governos responsáveis". É claro que a definição de governos que se qualificam como "responsáveis" fica aberta a interpretações. "Teoricamente, as fabricantes de armas dos grandes países ocidentais só venderiam seus produtos para governos responsáveis. Mas elas vendem armas para quem quiser comprar, incluindo países que não se qualificam, exatamente, como baluartes da paz e da democracia. O comércio de armas é muito criticado, mas nunca deixa de acontecer", ele diz.

O uso de ferramentas de vigilância cibernética por governos e seus órgãos de segurança pode ser justificável até certo ponto, diz Kaspersky. Por exemplo, o telefone de uma pessoa suspeita de envolvimento em um crime do qual já se tem notícia pode ser grampeado, desde que a ação seja amparada por um mandado judicial válido. Computadores de criminosos e arquivos podem ser confiscados para a produção de provas. "Assim, qual é o problema de se usar ferramentas sofisticadas para invadir computadores remotamente, com a devida supervisão? Há problemas", ele afirma.

Em primeiro lugar, ferramentas de vigilância são softwares chamados de *malware* (contração das palavras “malicious” e “software”). *Malwares* usados por governos agem exatamente como os usados por criminosos: invadem furtivamente dispositivos eletrônicos e roubam dados de todos os tipos. A única diferença é que os órgãos de segurança e de espionagem lhes atribuem uma característica de legitimidade, porque é fácil vender a ideia de que isso é feito “para salvar vidas” — uma explicação corriqueira do governo americano, por exemplo.

Em segundo lugar, a tentativa de legitimar o uso de *malware* é inaceitável porque implica engodo. A vítima tem de ser induzida a erro. Isto é, a fazer uma ação, como abrir um arquivo, para que seu computador seja infectado. Ou seja, o hacker tem de empregar “táticas de engenharia social” para enganar seu alvo e fazê-lo abrir um arquivo malicioso ou uma página da internet maliciosa.

Por exemplo: há algum tempo, o *Gamma Group* disfarçou seu módulo de instalação de *spyware* como o navegador Firefox. Só abandonou essa prática depois que a Mozilla, desenvolvedora do Firefox, ameaçou processá-la.

Outro método popular de infectar computadores visados é fazer o *hacking* de páginas legítimas da Internet e adicionar a elas algum código malicioso — é o já conhecido “ataque *watering hole*”. Assim ocorre no mundo virtual o que poderia acontecer no mundo real, se a polícia entrasse furtivamente na propriedade de qualquer cidadão insuspeito, roubasse pertences da pessoa e danificasse seus bens. “Isso é o que acontece nos ataques “*watering hole*” e outros ataques cibernéticos”, diz Kaspersky.

A questão fundamental é que a utilização de *malware* é ilegal. Mesmo para uma operação de busca e apreensão cotidiana o juiz tem de ser convencido a expedir um mandado. Porém, a supervisão judicial de operações no domínio cibernético ainda está em sua infância — se é que existe na maioria dos países. Assim, a criação e a utilização de programas maliciosos deveriam, teoricamente, ser punidos como um delito, não importa se as razões sejam “legítimas” ou não. A não ser que existam crimes legítimos.

Finalmente, um *malware* é um software facilmente copiado, alerta Kaspersky. Qualquer *malware*, tal como qualquer software não malicioso, é essencialmente um código de computação apenas. Se qualquer engenheiro de software se apodera desse código, ele pode replicá-lo facilmente. Dessa forma, *malwares* criados por empresas que servem governos ou por hackers profissionais próprios podem, facilmente, cair nas mãos de criminosos cibernéticos. Um mesmo cidadão, que respeita as leis, pode ser atacado por algum órgão de segurança ou por um criminoso, com o uso do mesmo malware.

Para Kaspersky, termos utilizados pelos órgãos de segurança e hackers oficiais, como “malware legítimo” ou “segurança ofensiva” são “oximoros” — ou paradoxos — e preocupantemente “antiutópicos”. Lembram, ele diz, os paradoxos do escritor George Orwell, como “guerra é paz” e “liberdade é escravidão”.

“A segurança da sociedade não vai melhorar se os órgãos de segurança continuarem agindo sem supervisão judicial e sem basear suas ações em legislação que as suporte”, ele afirma. Porém, é difícil imaginar uma legislação que dê legitimidade ao uso de *malwares*. “Não soa realística a aprovação de leis que possam legitimar, por exemplo, a prática de arrombamento, fraude ou assalto pela polícia, mesmo que seja para um bom propósito”, diz Kaspersky.

Date Created
23/12/2014