ENTREVISTA

4

Guerra ciberespacial

A internet é um barril de pólvora

RESUMO CEO da maior empresa de antivírus do mundo alerta para a guerra cibernética atualmente em curso, capaz de derrubar serviços hospitalares, energéticos etc., e preconiza a criação de uma entidade global de segurança cibernética, como a Agência Internacional de Energia Atômica, para arbitrar as regras do jogo.

MARCELO NINIO
tradução **PAULO MIGLIACCI**

EUGENE KASPERSKY ERA funcionário do Ministério da Defesa da então União Soviética, em 1989, quando seu computador corporativo foi infectado pelo vírus Cascade. A dor de cabeça despertou o interesse do jovem russo para esses programas maliciosos. Em 1997, deixou o emprego no governo e fundou a Kaspersky Lab.

Autodenominada a maior desenvolvedora de softwares de proteção de computadores do mundo, a companhia diz que seus produtos contra "malwares" —códigos maliciosos encontrados, por exemplo, na internet, tais como "worms" e cavalos de troia— têm mais de 300 milhões de usuários.

Foi a Kaspersky Lab que, em 2009, detectou quase por acaso o vírus Flame, que infectou a rede das centrífugas de urânio no Irã. Em junho, o jornal "Washington Post" revelou, citando fontes anônimas, que os EUA e Israel desenvolveram o vírus para prejudicar o programa nuclear iraniano.

Em entrevista à **Folha**, concedida por e-mail, Kaspersky, 46, prevê um "armagedon cibernético", uma guerra on-line capaz de pôr abaixo serviços essenciais, como eletricidade, hospitais e aeroportos, e propõe a criação urgente de uma organização internacional de segurança cibernética.

★

Folha — O sr. poderia explicar o que é o vírus Flame e como foi detectado? Por quanto tempo operou e que danos ainda pode causar?

Eugene Kaspersky — O Flame foi identificado por especialistas no Kaspersky Lab depois que a União Internacional de Telecomunicações [agência da ONU especializada na área] nos procurou para ajudar a identificar um "malware" que apagava informações importantes em todo o Oriente Médio.

Quando saímos em busca daquele código —conhecido como Wiper—, descobrimos um novo "malware", o worm.win32.flame. Os criadores do Flame mudaram as datas de criação dos arquivos para impedir que os investigadores descobrissem quando foram criados. Tinham datas como 1992, 1994, 1995, mas eram datas falsas.

Descobrimos que um módulo da versão do [virus do tipo "worm"] Stuxnet, o "Resource 207", que começou a circular no começo de 2009, era um "plug-in" [programa auxiliar] do Flame. Ou seja, quando o Stuxnet foi criado, a plataforma Flame já existia e o código-fonte de pelo menos um módulo do Flame foi usado no Stuxnet.

Em 2010, o módulo "plug-in" do Flame foi removido do Stuxnet e substituído por outros, que exploravam novas vulnerabilidades. De acordo com nossos dados, havia uso do Flame em agosto de 2010. Outros apontam circulação do Flame já em fevereiro ou março de 2010. É possível que antes disso existisse uma versão anterior.

Em uma conferência sobre guerra cibernética, no começo de junho, em Tel Aviv, o sr. fez um alerta sobre os riscos de terrorismo digital, afirmando que ele poderia causar "o fim do mundo como o conhecemos". O que isso significa?

A evolução do "armagedon cibernético" vem seguindo a trajetória prevista. A internet não é mais um local para conhecer pessoas. Agora ela afeta as nossas vidas diretamente, por ser usada em todos os serviços vitais, como aeroportos, hospitais, bancos, polícia etc.

A infraestrutura de todo o planeta depende da internet. Não é mais brincadeira de criança. Alguém pode pregar uma peça inofensiva que pode ter consequências desastrosas. No futuro, poderemos ter falta de luz ou paralisações em hospitais por causa de algum "malware" aleatório ou, pior, em decorrência de um ato deliberado de guerra cibernética.

A questão não é se isso vai acontecer, mas quando. Pense no blecaute na região nordeste dos EUA, em 2003, na queda do voo 5022 da Spanair, em 2008, nos aviões militares não tripulados que perderam o controle ou na escassez de banda de internet da Coreia do Sul —todos esses incidentes foram causados por surtos de vírus.

O terrorismo e a guerra cibernética se tornarão comuns? Há outros vírus como o Flame ou ainda piores?

As Forças Armadas de diversos países, como EUA, Índia, Reino Unido, Alemanha, França, China, Coreia do Sul e Coreia do Norte, estão criando unidades de guerra cibernética e armas para ela. Casos de espionagem industrial e atos de sabotagem também são de conhecimento público (vide as notícias sobre ataques patrocinados por nações, como o Stuxnet, o Duqu e, agora, o Flame).

Tudo isso é apenas a ponta do iceberg. Sempre que descobrimos um novo programa de infiltração, logo surgem as seguintes informações: o "malware" foi exposto por engano ou acidente; infestava diversas redes há algum tempo; e não temos como saber o que andou fazendo por lá. Muitas características técnicas do "malware" e a motivação de seus criadores continuam sendo um mistério.

Estamos sentados sobre um barril de pólvora. Aos poucos, os militares estão transformando a internet em um campo minado. Quanto mais se observa, mais assustadora a situação parece

Estamos sentados sobre um barril de pólvora e serrando o galho que sustenta toda a internet e, ao mesmo tempo, toda a infraestrutura do planeta. Aos poucos, os militares estão transformando a internet em um grande campo minado. Quanto mais se observa, mais assustadora a situação parece.

O sr. citou EUA, Reino Unido, Israel, China, Rússia e, possivelmente, Índia, Japão e Romênia como países capazes de desenvolver o Flame. O sr. chegou a alguma conclusão sobre a autoria do vírus?

Não existem informações no código, nem de outras fontes, que permitam vincular o Flame a um Estado-nação. Por isso, seus autores continuam desconhecidos.

O sr. disse que é necessário um esforço mundial para enfrentar o terrorismo cibernético. Como acha que isso deveria ser feito e quem deveria comandar o processo?

O mínimo que podemos fazer no momento é estabelecer as regras do jogo para o campo de batalha virtual, regulamentar o desenvolvimento e uso de armas cibernéticas, criar novas definições e ajustar as leis tradicionais de guerra.

É preciso urgentemente um equivalente cibernético da Agência Internacional de Energia Atômica, uma agência que coordene essas questões. Já existem duas organizações que anseiam por essa responsabilidade em nível mundial —a Unidade de Ação contra o Terrorismo, da ONU, e a Interpol, que planeja estabelecer, em 2014, uma divisão de policiamento cibernético sediada em Cingapura.

Também creio que alguma forma de organização internacional de segurança cibernética deveria ser criada para agir como plataforma independente para cooperação e promoção de tratados para evitar o uso de armas cibernéticas, além de regulamentar a segurança da infraestrutura essencial. Essa organização também seria responsável por investigar incidentes de ataques cibernéticos e pelo combate ao terrorismo na rede.

É claro que isso não eliminaria as armas cibernéticas, mas ao menos melhoraria a situação. As partes mais vulneráveis, ou seja, os países desenvolvidos com alto uso de internet, seriam beneficiados por uma organização como essa e, portanto, deveriam apoiá-la.

Em geral, a guerra e o terrorismo cibernéticos são percebidos como problemas por países e empresas. Que riscos os usuários comuns enfrentam? De que forma se proteger?

O alvo das armas cibernéticas recentes são organizações, ainda que as vítimas do Flame variem de indivíduos a organizações ligadas ao Estado e instituições de ensino. Ou seja, os riscos afetam a todos e significam, para governos e Forças Armadas, perda de informações sigilosas; para empresas privadas, perda de propriedade intelectual; para indivíduos, tornarem-se parte de redes de espionagem.

A proteção contra essas ameaças é praticamente impossível para um usuário comum de computador. Mas existem alguns conselhos que podem melhorar a segurança das máquinas. Entre elas, usar um sistema operacional moderno como o Windows 7 ou o Mac OS X; quando possível, utilizar a versão em 64 bits do sistema, porque é mais resistente a ataques de "malwares"; manter atualizados tanto o sistema operacional quanto os softwares criados por terceiros; instalar e manter um pacote de segurança operacional decente; tomar cuidado ao abrir anexos de fontes desconhecidas, evitar divulgar informações pessoais em redes sociais e usar senhas fortes.

O sr. se espantou com o filme "Duro de Matar 4.0", que aborda um ataque cibernético massivo aos EUA. O sr. se preocupa mais com o fato de o tabu sobre terrorismo cibernético ser exposto ou por ele ter sobrevivido por tanto tempo?

As ameaças de terrorismo cibernético e de guerra cibernética começaram a ser encaradas com seriedade no começo da década de 2000, mas foram pouco debatidas em público. Até que "Duro de Matar 4.0" foi lançado, em 2007.

Era fácil zombar do tema do filme, mas fiquei assustado. Na Kaspersky Lab, nós víamos o lado sério, porque entendíamos que nada impede que um cenário como aquele aconteça na vida real.

Depois de assistir ao filme, comecei a falar e a fazer alertas sobre o terrorismo cibernético, que se provaram precisos: a ameaça é real, não exagerei em nada.

O que um país emergente como o Brasil pode fazer para se proteger contra o terrorismo cibernético?

Desdobramentos recentes, como Stuxnet, Duqu e Flame, demonstraram que mesmo sistemas supostamente seguros de infraestrutura industrial podem ser atacados. É quase impossível se proteger contra um ataque como esse. Seria preciso reescrever todo o software de sistemas vitais para protegê-los. Mas isso exigiria muito tempo e dinheiro, e temo que nenhum país possa investir um orçamento dessa ordem na proteção à tecnologia de informação.

O caminho é criar, como falei, uma organização internacional que controle as armas no ciberespaço. Ela adotaria estruturas semelhantes às de segurança nuclear de que dispomos, mas aplicadas ao ciberespaço. O ideal seria proclamar a internet uma zona desmilitarizada. Mas não estou seguro de que o desarmamento seja possível.

A oportunidade já foi perdida, os investimentos foram realizados, as armas foram criadas e a paranoia já existe. Mas os países precisam ao menos chegar a um acordo sobre regras e controles quanto às armas cibernéticas.

Há quem diga que seus alertas são exagerados e o acuse de possível conflito de interesse. Como o sr. responde a elas?

É justo dizer que sou meio paranoico e que não penso muito antes de me pronunciar sobre meu medo de futuras catástrofes na internet ou sobre a cobiça e a degeneração dos vilões cibernéticos e a imensa ameaça que representam.

Mas basta que você se atenha aos fatos que expus acima. Os incidentes de espionagem industrial e os atos de sabotagem não são fantasias. Diversos países estão criando unidades especiais de guerra cibernética e isso não ocorre sem propósito. Devido à minha tendência a falar abertamente, sempre sou acusado de causar medo. Mas não me incomodo, ainda que as acusações sejam tolas.

Vou continuar dizendo o que precisa ser dito sem me importar com as críticas.

Depois de assistir a "Duro de Matar 4.0", comecei a falar e a fazer alertas sobre o terrorismo cibernético, que se provaram muito precisos: a ameaça é real e não exagerei em nada

No futuro, poderemos ter falta de eletricidade ou paralisações em hospitais por causa de um "malware" aleatório ou, pior, em função de um ato deliberado de guerra cibernética

CLAUDIUS | *cartum*