

# A rede em pé de guerra

Hackers armados com softwares cada vez mais sofisticados ameaçam infraestruturas nacionais, transformando a internet em um campo de batalha cujas regras os países ainda estão longe de definir

Igor Zolnerkevic ●

Você pode achar que não tem nada a ver com os conflitos nas ex-repúblicas soviéticas ou com a crise em torno da tentativa do Irã de produzir armas nucleares, mas seu computador pode lhe contradizer. Milhões de máquinas em todo o planeta vêm cada vez mais servindo como instrumento de uma guerra que ocorre literalmente em campo mundial: a internet.

Organizações criminosas, revolucionárias e serviços secretos nacionais têm se valido de ferramentas como as “botnets” (rede de milhões de computadores “zumbis” controlados remotamente por hackers, sem que os usuários percebam – veja a ilustração na pág. 30) ou sofisticados vírus de computador para desenvolver ataques que podem tornar a guerra cibernética tão ou mais feroz e eficaz que a feita por tanques e mísseis.

O assunto não é exatamente novo para os entendidos, mas veio à tona quando, no final de 2010, a imprensa dedicou manchetes aos eventos que se seguiram à divulgação na internet de mensagens confidenciais entre embaixadas norte-americanas pela organização não governamental Wikileaks.

Um deles foi um conflito entre hackers contra e pró a organização. Os primeiros



tiraram o site temporariamente do ar, usando botnets para sobrecarregá-lo com um número impossível de pedidos de acesso, uma tática conhecida como DDoS (negação de serviço distribuída, em inglês). Em resposta, seus partidários usaram a mesma tática contra sites das empresas Mastercard, Paypal e Visa, que haviam recusado seus serviços ao Wikileaks.

O ataque DDoS é a ferramenta mais comum desses conflitos e foi usado no que vem sendo chamado por alguns de “primeira guerra cibernética”. Em meados de 2007, em resposta à remoção de um memorial de guerra soviético em Talin, capital da Estônia, hackers derrubaram por três semanas os sites do parlamento, de ministérios, de partidos políticos, de bancos e de jornais.

A Estônia acusou o governo russo de orquestrar os ataques, argumentando que a magnitude e a organização dos ataques só seria possível com apoio estatal. A Rússia negou envolvimento. E embora alguns dos DDoS tenham partido de máquinas de instituições públicas russas, nada foi provado.

O conflito inspirou a criação pela Otan de um centro de defesa cibernética em Talin, em 2008, bem como a criação de “comandos cibernéticos” nas forças armadas de alguns países. Em 2009, o Pentá-

gono criou o Comando Cibernético dos EUA, para defender as redes militares e governamentais do país. No mesmo ano, foi criado o Centro de Comunicações e Guerra Eletrônica do Exército Brasileiro (CCOMGEX). Junto a terra, mar, ar e espaço orbital, a internet se tornou o quinto domínio da guerra.

## Ganhos estratégicos

“A internet é um novo meio de guerra, que abre dimensões que precisam ser pensadas e analisadas com muito cuidado”, afirma Héctor Saint-Pierre, especialista em segurança internacional e professor da Faculdade de Ciências Humanas e Sociais da Unesp em Franca.

Uma dessas dimensões é o uso da rede para atingir ganhos políticos e estratégicos, como evitar um conflito armado. Foi o que ocorreu no México, em 1998, quando o exército avançava para a província de Chiapas, esperando liquidar guerrilheiros do movimento zapatista. Os guerrilheiros, então, organizaram protestos on-line, convidando internautas a acessarem sem parar sites como o da bolsa de valores mexicana em uma espécie de DDoS voluntário. A repercussão foi tanta que levou a uma votação no congresso norte-americano suspendendo qualquer

ajuda financeira ao México enquanto o governo não interrompesse a ofensiva.

A expectativa dos especialistas é que daqui para a frente todo conflito armado seja acompanhado de escaramuças eletrônicas. Em meados de janeiro, quando fechávamos esta edição, o conflito cibernético do momento era uma revolta popular na Tunísia. Nas ruas, pessoas morriam em protestos, acusando o governo de corrupção e censura. Na internet, líderes da oposição tinham suas contas de e-mail e perfis no Facebook roubados, enquanto sites do governo sofriam ataques DDoS.

Além dos ataques propriamente ditos, outra estratégia de guerra que ganha nova dimensão com a internet é a espionagem. Um dos documentos vazados pelo Wikileaks, por exemplo, sugere que hackers a mando do governo chinês tenham diversas vezes invadido computadores do governo e de empresas norte-americanas, copiado informações secretas. Possivelmente, os EUA fizeram o mesmo com a China. “É bem sabido que todos os governos têm uma agenda secreta de análise das infraestruturas de outras nações”, diz Adriano Cansian, cientista da computação do Instituto de Biociências, Letras e Ciências Exatas da Unesp, em São José do Rio Preto (SP).

De acordo com Claudia Canongia, asses-

sora técnica do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República, a cada hora a rede governamental sofre em média duas mil tentativas de roubo de informação.

#### Salto no nível de alerta

Mas se as ameaças de DDoS e de espionagem cibernética assustam, elas nem se comparam ao poder do Stuxnet, considerado “engenheiro”, “uma obra de arte”, por Cansian: “Fez a gente saltar de nível de alerta”. Trata-se de um worm (vírus que não precisa se ligar a um arquivo para se propagar) que, entre 2009 e 2010, infectou pelo menos cem mil computadores em todo o mundo, mais da metade no Irã, disseminando-se pela internet ou por dispositivos com entradas do tipo USB (como pen drives).

As principais empresas do ramo de segurança computacional mobilizaram-se para analisar seu código, e seus relatórios sugeriram que o Stuxnet tinha um objetivo bem específico. A intenção de seus criadores seria espalhar o worm pelo mundo na esperança de que infectasse o computador pessoal de um funcionário da fábrica de enriquecimento de urânio em Natanz, no Irã.

Com sorte, esse funcionário conectaria via USB seu notebook ao computador de controle e automação industrial da fábrica. O Stuxnet, então, entraria em ação, variando a velocidade das centrífugas enriquecedoras de urânio sem que os operadores percebessem. Com as máquinas avariadas ou destruídas, o programa nuclear do país seria atrasado em anos.

Se esse era mesmo o objetivo da missão, parece que ela foi bem-sucedida. O governo iraniano confirmou que teve problemas com o Stuxnet em Natanz e que a produção da fábrica caiu.

Uma análise da empresa Symantec concluiu que, para desenvolver o Stuxnet, foi preciso uma equipe de dez pessoas trabalhando por seis meses, com acesso a quatro falhas de segurança do sistema operacional Windows 7 – que ninguém mais conhecia até o momento (a Microsoft já as corrigiu). Obter informações sobre falhas

## Receita para uma botnet

Espalhando programas maliciosos (malwares) pela internet, hackers criam redes de milhões de computadores “zumbis”, as chamadas botnets



inéditas, chamadas de “vulnerabilidades de dia zero”, chega a custar centenas de milhares de dólares no mercado negro.

A equipe tinha de ter ainda acesso a um programa caríssimo para controle e automação industrial produzido pela empresa alemã Siemens, além de saber detalhes sobre as peças do maquinário da fábrica em Natanz. Todos esses recursos levam a crer que o Stuxnet seja um projeto estatal. Especialistas sugerem que os EUA e Israel sejam os responsáveis, embora as duas nações neguem qualquer envolvimento com o worm.

O temor é que o Stuxnet seja apenas o primeiro de uma nova geração de malwares capazes de danificar infraestruturas críticas: usinas hidrelétricas, nucleares, a rede de distribuição de energia elétrica, indústrias químicas, o sistema financeiro e, é claro, a própria internet. E considerando o caso iraniano, pondera Cansian, o ataque com um programa malicioso tão sofisticado acaba sendo mais eficiente que jogar um míssil diretamente sobre a

fábrica. Além de correr o risco de errar o alvo, a arma é muito mais cara.

“Cabe a cada país definir urgentemente suas ações para mitigar ameaças e riscos de ataques cibernéticos”, comenta Raphael Mandarino, diretor do DSIC. Essas ações vão desde a simples verificação de presença de malwares (programas maliciosos como o Stuxnet) em pen drives de funcionários a uma decisão mais ampla sobre com quais outros computadores as máquinas que controlam infraestruturas devem ou não se conectar.

Ano passado, o DSIC publicou um livro propondo esquemas para a segurança das infraestruturas críticas da informação nacionais. Segundo Claudia, o Ministério do Planejamento já mostrou interesse em implementar o guia na Infovia – rede de banda larga em construção que pretende interconectar toda a administração pública federal brasileira.

Paralelamente ao esforço de proteger as redes, especialistas vêm se dedicando a monitorar o que os hackers andam

aprontando, na tentativa de melhorar a atuação dos antivírus.

#### Hackeando os hackers

Uma das linhas de frente é tentar identificar a origem dos vírus. Segundo André Grégio, pesquisador do Centro de Tecnologia da Informação Renato Archer, do Ministério da Ciência e Tecnologia, há tantos circulando na internet porque muitos são feitos com base em “kits faça-você-mesmo”. Baratos e fáceis de usar, eles permitem que criminosos sem conhecimento técnico realizem esses golpes. “Muitos malwares de roubo de senhas bancárias são provenientes do mesmo kit”, diz.

Junto com Cansian, da Unesp, Paulo de Geus, da Unicamp, e Rafael Santos, do Inpe, Grégio mantém uma rede de “honeypots” (literalmente, potes de mel) – computadores ligados à internet sem nenhuma defesa. A análise de como um malware interage com os honeypots revela, por exemplo, se o programa é um exemplar da “escola” chinesa ou da russa.

Latina, provavelmente sem que ninguém da instituição soubesse de nada.

Em seu laboratório, Cansian e seus alunos criam detectores de ataques a grandes redes, justamente para impedir que algo semelhante aconteça na Unesp. São programas que percebem em segundos se a passagem de dados pela rede continua normal ou passou a apresentar um comportamento suspeito.

Porém, por mais que as ferramentas de defesa se emparelhem com as de ataque, os hackers geralmente saem-se melhor ao explorar o elo fraco da cadeia de segurança: o usuário comum. Segundo Cansian, a maioria das pessoas tem um “comportamento promiscuo” na rede mundial, “cliqueando em tudo”, usando senhas fáceis de decifrar, além de revelarem informações comprometedoras em redes sociais.

Outro fator que provavelmente contribuiu para a disseminação de vírus e afins é que ainda falta no mundo uma legislação para definir o que são exatamente esses crimes e qual a punição para quem os cometer.

Uma tentativa nesse sentido surgiu no ano passado, durante um encontro em Salvador promovido pelo Escritório das Nações Unidas sobre Drogas e Crime (UNODC, em inglês). Lá ficou decidida a criação de um grupo de trabalho específico com o objetivo de produzir uma convenção global de combate a crimes cibernéticos. O grupo é liderado por Julio Cezar Zelner Gonçalves, embaixador brasileiro em Viena (Áustria), onde fica a sede do UNODC.

Não se espera, entretanto, que tal acordo saia tão cedo. “Ajustar os termos para que se adequem às legislações de todos os países membros da ONU não é tarefa simples”, diz Raphael Mandarino. Um dos entraves para um acordo global é que não há acordo sobre a definição de crime cibernético.

Em países de regime totalitário, uma campanha política por meio de blogs é vista em pé de igualdade com ataques DDoS. Mandarino acredita que as posições tanto das democracias ocidentais quanto dos demais países precisarão ser revisadas. “Ironicamente, a questão suscitada pelo Wikileaks pode acelerar o entendimento”, sugere.

O Stuxnet talvez seja o programa malicioso mais sofisticado já desenvolvido. Analistas de segurança temem que ele seja apenas o primeiro de uma nova geração capaz de danificar infraestruturas críticas como usinas hidrelétricas, o sistema financeiro e a própria internet