Era da ciberguerra começou e envolve países e empresas
Michael Riley e Ashlee Vance

Nas primeiras horas da manhã de 24 de maio, um ladrão armado, com o rosto encoberto por uma máscara de esquiar, invadiu os escritórios da Nicira Net-works, uma empresa iniciante do Vale do Silício instalada em um dos incontáveis prédios de arquitetura indefinível na Highway 101. Ele passou pelas escrivaninhas repletas de computadores portáteis e dirigiu-se diretamente à mesa de um dos principais engenheiros da empresa. O assaltante parecia saber exatamente o que queria: um computador volumoso, que armazenava o código-fonte da Nicira. Pegou a máquina e fugiu. Toda a operação durou cinco minutos, como mostrou um vídeo capturado pela minicâmera do computador de um dos funcionários.

O sargento Dave Flohr, da polícia de Palo Alto, decreveu o caso como um típico roubo de computador no Vale do Silício. "Há montes de idiotas por aí que pegam o que podem e saem", diz.

Duas fontes próximas à empresa, no entanto, dizem suspeitar, assim como investigadores federais encarregados do caso, de algo mais sinistro: um assalto profissional, realizado por alguém com laços com a China ou a Rússia. O ladrão não queria um computador que pudesse vender na Craigslist, empresa popular de anúncios classificados. Queria as ideias de Nicira.

O que antes era domínio de Hollywood tornou-se real: ladrões de alta tecnologia e vírus que derrubam usinas
O roubo de propriedade intelectual está longe de ser algo inédito no Vale do Silício. Na maioria das vezes, se trata de uma invasão digital de redes por hackers em busca de algum produto muito usado. Neste caso, houve uma invasão física, por um ladrão armado que estava atrás de uma tecnologia secreta, que ainda nem está no mercado.

A Nicira passou os últimos quatro anos desenvolvendo silenciosamente um programa de infraestrutura de computação para centros de dados. De acordo com site da empresa, os fundadores da Nicira vieram dos departamentos de ciência da computação das universidades de Stanford da Califórnia, em Berkeley.

A empresa conta com grandes investidores em capital de risco, como a Andreessen Horowitz e New Enterprise Associates. A Nicira também pediu verbas para o Departamento de Defesa dos Estados Unidos, para trabalhar em tecnologias de rede para uso militar. Representantes da Nicira não quiseram comentar o assunto para este artigo. (A Bloomberg LP, dona da Bloomberg Businessweek, é investidora na Andreessen Horowitz).

Os que estão a par do roubo se recusam a falar publicamente. Atribuem a relutância a ordens dos investigadores federais. De forma reservada, mostram preocupações em comum: a ciberespionagem e os ataques de hackers ligados a países parecem estar aumentando em frequência e gravidade. O que outrora parecia domínio de Hollywood - assaltantes de alta tecnologia armados e vírus de internet que derrubam usinas elétricas - tornou-se real. Eles temem que os conflitos on-line e os incidentes de espionagem estejam aumentando venham a se transformar em uma disputa cruel e perturbadora, envolvendo governos, empresas e hackers altamente avançados e fora de alcance.

A nova era da "Code War" (Guerra de Códigos, que em inglês soa semelhante a Guerra Fria) não se tem superpotências encarando-se para ver quem pisca primeiro. Lembra mais a Europa de 1938, quando o continente era um caos e um conflito mundial parecia inevitável.

Os ciberataques costumavam ser mantidos em silêncio. Muitas vezes, passavam despercebidos por muito tempo depois do ataque, e países ou empresas atingidos normalmente não falavam sobre o assunto. Isso mudou à medida que um fluxo constante de incursões mais descaradas começou a ser exposto.

Os alvos mais atraentes nesta guerra são civis. "Nada é mais revelador da derrota do que uma cidade faminta"

Em 2010, por exemplo, a Google acusou a China de espionar funcionários e clientes da empresa. Na ocasião, informou que pelo menos outras 20 empresas foram vítimas do mesmo ataque, apelidado de Operação Aurora pela empresa de segurança em computação McAfee. Entre as vítimas também estavam Adobe Systems, Juniper Networks e Morgan Stanley.

Joel F. Brenner, chefe de contrainteligência dos EUA até 2009, diz que a mesma operação que desencadeou a Aurora teve muitas outras vítimas ao longo dos anos. "Seria aceitável dizer que pelo menos 2 mil empresas foram atingidas", diz Brenner. "E esse número está mais para o lado conservador", afirma.

Dezenas de outros nomes, como a Lockheed Martin, a Intel, o Ministério da Defesa da Índia, o Fundo Monetário Internacional (FMI) e o Pacific Northwest National Laboratory, sofreram ataques similares. Neste ano, hackers invadiram as redes de computador da RSA, uma empresa de segurança que protege computadores de outras empresas. Eles roubaram alguns dos códigos de computador mais valiosos do mundo, os algoritmos das fichas SecureID, da RSA, produtos usados por agências do governo dos EUA, fornecedores militares e grande bancos para impedir invasões de computadores. É como invadir um chaveiro altamente protegido e roubar a chave mestra que abre os cofres de todos os cassinos na Las Vegas Strip.

No mês de julho, o Pentágono revelou que também havia sido "hackeado". Mais de 24 mil arquivos foram roubados dos computadores de um fornecedor militar, não identificado, por "invasores estrangeiros".

O mais famoso incidente de ciberguerra até agora, cujos detalhes tiveram maior divulgação, envolveu o vírus Stuxnet. Em 2010, o Stuxnet - cuja existência foi noticiada em primeira mão pelo blog de segurança de Brian Krebs - apareceu em dezenas de países, tendo como alvo o que se conhece como controladores lógicos programáveis, que são computadores industriais do tamanho de um maço de cigarro, presentes em quase tudo.

O Stuxnet foi projetado para atingir apenas um tipo: os controladores de processamento de combustível de urânio em uma instalação nuclear do Irã.

As pessoas que analisaram o ataque acham que alguém conectou um "pen drive" carregado com o Stuxnet em algum computador pessoal com Windows conectado às centrífugas, localizadas dentro de um refúgio. O vírus deu a ordem para o equipamento girar com velocidade exagerada, o que o acabou destruindo.

Enquanto tudo isso acontecia, o Stuxnet manteve-se escondido dos técnicos iranianos. O vírus desarmou os alarmes e inseriu falsos informes de funcionários, assegurando que as centrífugas estavam funcionando bem.

O Stuxnet atrasou o programa nuclear iraniano por meses. Não comprometeu apenas bases de dados, como a maioria dos vírus de computador: destruiu algo físico. "O Stuxnet foi o equivalente a uma arma balística de alta potência", diz Ed Jaehne, estrategista-chefe da KEYW, empresa de segurança de computadores, em Maryland, que vem apresentando grande crescimento.

Quando os pesquisadores dissecaram a tecnologia e buscaram os motivos, alguns apontaram para os EUA ou Israel como o local mais provável de origem.

A investigação sobre o Stuxnet não era necessariamente de muita ajuda: se há uma característica distintiva dos ataques na Guerra dos Códigos é que a tecnologia envolvida está em constante mutação. Os ciberarmamentos parecem estar entrando na era dourada de progresso acelerado - uma nova corrida armamentista. O desafio em Washington, no Vale do Silício e por todo o mundo é desenvolver ferramentas digitais tanto para a espionagem como para a destruição.

Os alvos mais atraentes nesta guerra são civis - redes elétricas, sistemas de distribuição de alimentos e qualquer infraestrutura básica que rode em computadores. "Esse negócio é mais cinético do que os armamentos nucleares", diz Dave Aitel, fundador da Immunite, uma empresa de segurança em computadores, em Miami Beach, usando um termo militar que designa poder de destruição no mundo real. "Nada é mais revelador de que você perdeu do que uma cidade faminta."

Os ciberarmamentos existem há vários anos, em sua maior parte nas agências de inteligência nacionais e militares. Especialistas em segurança confirmaram que trabalhos da Northrop Grumman, Raytheon e General Dynamics, potências da indústria militar tradicional, estão ajudando o governo dos EUA a desenvolver formas de espiar ou desativar redes de computadores de outros países.

O setor, no entanto, começou a mudar em torno a 2005, quando o Pentágono começou a dar mais ênfase ao desenvolvimento específico de ferramentas de hackers com fins militares.

A mudança na política militar permitiu o nascimento de uma série de pequenos, mas avançados, "negociantes de ciberarmamentos" de ataque. A maioria são empresas "obscuras" que camuflam o financiamento governamental e trabalham em projetos confidenciais. "Há cinco anos, ocorreu uma explosão", diz Kevin G. Coleman, ex-estrategista-chefe da Netscape e autor de "The Cyber Commander's eHandbook", um guia que pode ser baixado da internet. "Simplesmente, entraram em cena pessoas com capacidades ofensivas."

Dois dos principais armamentos no arsenal dos guerreiros virtuais são os "botnets" e "exploits". Um botnet é um grupo de dezenas ou até centenas de milhares de computadores sendo comandados sem o conhecimento de seus donos. Para criar esses exércitos involuntários, os hackers passam anos infectando os computadores das pessoas com códigos maliciosos (vírus de computador de autopropagação), que ficam escondidos e preparam o computador para receber ordens. Quando ativado, um botnet pode derrubar redes ao bombardeá-las com lixo digital. Também pode ajudar a espionar e, se necessário, a sabotar um grande número de máquinas.

Um "exploit", no sentido usado pelos hackers para a palavra, é um programa que explora as vulnerabilidades de outros programas de amplo uso, como o Windows, da Microsoft, ou das milhões de linhas de códigos que controlam servidores de rede. Os hackers usam os exploits para entrar e inserir um vírus ou outros conteúdos destrutivos. Algumas dessas brechas são bem conhecidas, embora os fornecedores de software possam levar meses ou até anos para criar soluções para elas.

Os exploits mais importantes são aqueles desconhecidos de todos até a primeira vez em que são usados. São chamados de "exploits dia zero" (o dia em que o ataque é descoberto seria o "dia um"). Nos subterrâneos do mundo dos hackers, em bate-papos on-line apenas para convidados nos quais são negociados produtos ilegais, um exploit dia zero para uma rede com Windows pode ser vendido por até US$ 250 mil. O Stuxnet usou quatro exploits dia zero de alta complexidade, o que o torna uma grande estrela nos círculos de hackers.

O guia de Coleman lista cerca de 40 tipos de ataques possíveis com botnets e exploits. O número 38 é o assassinato. Assim como o Stuxnet deixou a centrífuga girando fora de controle, um vírus de computador pode desativar uma terapia intravenosa ou o sistema de oxigênio controlados por computadores em algum hospital, antes de a equipe médica tomar conhecimento de que há algo errado.

Número 39: hackear carros. Os carros estão repletos de computadores, que controlam freios, câmbio, motor e praticamente tudo. Controle esses sistemas e você pode controlar o veículo - e provocar uma batida, se quiser.

Soa absurdo? Em 2010, pesquisadores da Rutgers University hackearam os computadores de um carro que estava a quase 100 quilômetros por hora, por meio do sistema sem fio usado para monitorar a pressão dos pneus.

Não está claro se o governo dos EUA já usou alguma dessas técnicas. "Somos capazes de fazer coisas que ainda não decidimos se são o melhor a fazer", diz o general Michael V. Hayden, ex-diretor da CIA.

O que diferencia um ataque normal de hacker de um do Pentágono neste contexto não é a imponência de poder, mas a destreza com que o invasor pode infiltrar-se em uma rede, esconder seu material e, depois, desaparecer.

Na Coreia do Sul, um vírus de computador iniciou em março um ataque de dez dias, tomando o controle de milhares de computadores de estudantes, trabalhadores e donos de lojas. As máquinas, então, bombardearam sites militares e governamentais com um grande tráfego incessante, derrubando redes ou inabilitando-as parcialmente. O ataque destruiu milhares de computadores e custou centenas de horas de trabalho para atenuar os problemas. Segundo a empresa de segurança McAfee, no entanto, o verdadeiro objetivo provavelmente era testar as defesas digitais sul-coreanas, sugerindo que há mais por vir.

Os pesquisadores da McAfee, tentando encontrar a origem do ataque, descobriram que o vírus recebeu comandos de servidores em 26 países, incluindo Vietnã, Arábia Saudita e Emirados Árabes Unidos. Cerca de 20% dos servidores estavam nos EUA. Quando a trilha digital começava a desvendar-se, os computadores atacados foram instruídos a apagar seus códigos de software básicos, tornando-se inúteis. Os investigadores ainda tão têm certeza sobre quem lançou o ataque, mas a McAfee suspeita da Coreia do Norte.

O incidente demonstrou um dos aspectos mais assustadores da ciberguerra: a impossibilidade de rastreamento. Jaehne, da KEYW, diz que empresas iniciantes são mais apropriadas para lidar com esses ataques misteriosos de alta velocidade.

"A grande base industrial dos fornecedores militares não é conhecida por sua capacidade quanto a isso ou por sua velocidade em inovação", diz Jaehne. "Eles precisam dirigir-se a empresas menores, mais ágeis, para encontrar essa inovação."

A KEYW diz ser a única empresa com ações negociadas especializada puramente em "cibersuperioridade". Jaehne e outros executivos fundadores da empresa de Hanover, no Estado de Maryland, saíram do Northrop Grumman para criar sua empresa em 2008. A maioria dos 800 funcionários tem autorização para trabalhar em projetos secretos de agências de inteligência dos EUA, responsáveis pela maior parte da receita da empresa. Em 2010, a receita subiu 175%, de US$ 39 milhões para US$ 108 milhões. Quando perguntado sobre os tipos de munições digitais que a KEYW produz, Jaehne responde: "Não há nada que eu possa falar sobre isso."

Aitel, da Immunity, também não fala sobre os trabalhos da empresa para o governo. De acordo com uma fonte próxima à Immunity, a empresa produz "rootkits" transformados em armas: sistemas de invasão digital de grau militar usados para entrar em redes de outros países. A fonte não quis ser identificada porque o assunto é delicado. Entre os clientes, estão agências de inteligência e militares dos EUA.

O governo americano passou os últimos dois anos formalizando as suas operações e estudando a questão da guerra por computadores. Em 2009, o governo de Barack Obama anunciou a criação do U.S. Cyber Command, com sede em Fort Meade, Maryland. O presidente assinou recentemente ordens que dão aos militares aprovação total para usar armamentos digitais que possam desempenhar várias tarefas, como as de espionagem e de ataques a redes elétricas de inimigos - esses últimos exigem ordens presidenciais. É um momento de mudanças rápidas e assustadoras.

"É como nos primeiros dias do balanceamento nuclear americano-soviético", diz Clarke. "Não conhecemos as regras da estrada."

Gunter Ollmann, especialista em segurança de computadores e ex-diretor da X-Force, diz que o poder sedutor dos ciberarmamentos pode superar o medo dos governos quanto à instabilidade que seu uso possa causar. Também acredita, no entanto, que os armamentos digitais podem reduzir o risco de conflitos travados com tanques e mísseis.

O Stuxnet evitou o conflito aberto que teria se seguido a um bombardeio das instalações nucleares iranianas. Os países com arsenais digitais avançados poderiam usar a tecnologia para influenciar nações contrárias, desligando a iluminação em Caracas, por exemplo, ou inabilitando o porto da capital líbia.

"Deixa de ser uma batalha cinética e passa a ser uma guerra de cerco", diz Ollmann. "Posso controlar sua água ou sua energia a distância. E quando toda a confusão for decifrada, posso voltar a conectá-las."

Para lidar com a guerra de códigos, que implica um constante estado de ameaça, governos e empresas podem tentar desenvolver sua própria tecnologia. Mas, assim como as bombas inteligentes, caças-bombardeiros e outros instrumentos do "mundo real", as armas cibernéticas são sempre mais fáceis de ser construídas do que destruídas.

"A indústria dos hackers está muito à frente em relação à sua capacidade de implantar um grande botnet", diz Amichai Shulman, chefe de tecnologia da Imperva, empresa especializada em segurança. "Se uma nação quer lançar um ataque distribuindo algum tipo de malware, faz mais sentido para ela simplesmente alugar um botnet já existente", afirma.

Fonte: Valor Econômico, São Paulo, 2 ago. 2011, Primeiro Caderno, p. A12.

A utilização deste artigo é exclusiva para fins educacionais