Armagedon: *as disputas do ciberespaço não se restringem aos jogos eletrônicos. Elas podem trazer consequências econômicas e políticas imprevisíveis*

GUERRA VIRTUAL

A BATALHA CIBERNÉTICA, QUE MOBILIZA POTÊNCIAS DO PORTE DE CHINA E EUA, PÕE EM RISCO REDES DE ENERGIA ELÉTRICA E ATÉ USINAS NUCLEARES. COMO O BRASIL ESTÁ SE PROTEGENDO E DE QUE MODO ISSO AFETA AS EMPRESAS

João VARELLA e Cristiano ZAIA

Um grupo de cientistas nucleares do governo iraniano teve uma surpresa ao chegar para o trabalho, numa manhã do mês passado. Um vírus de computador havia se infiltrado nas máquinas que controlam fábricas de enriquecimento de urânio e desligaram todo o sistema. Não bastasse isso, o vírus fez uma peraltice: quando acessados, os PCs dos cientistas tocaram a barulhenta *Thunderstruck*, um dos hits da banda de rock australiana AC/DC. E no volume máximo. "Violamos todas as regras, fizemos todos de bobos", diz a letra da música. À parte esse aspecto pitoresco, o episódio aumentou a tensão na

FOTO: COLIN ANDERSON

região, que pode dar início à primeira ciberguerra mundial. O caso foi divulgado por Mikko Hypponen, diretor global de pesquisas da empresa de segurança virtual F-Secure, da Finlândia, que soube da história por um funcionário iraniano de uma das usinas nucleares do país. Segundo Hypponen, esse é apenas mais um exemplo de uma nova face da geopolítica: o uso estratégico da computação como arma na batalha entre países. "Testemunharemos uma revolução focada em combates cibernéticos", disse Hypponen à DINHEIRO.

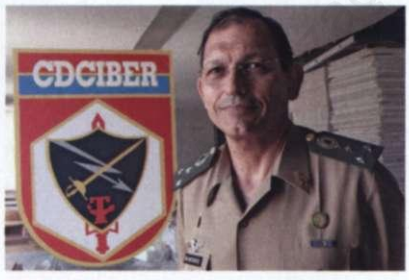
À primeira vista, a declaração soa alarmista. **Há indícios suficientes, no entanto, que demonstram que as principais potências mundiais, como EUA e China, já estão mobilizadas em torno do tema, capaz de provocar estragos na economia mundial.** Isso porque, como a infraestrutura básica dos países hoje é controlada por meio de computadores, um ataque virtual é capaz de prejudicar empresas e populações. Os principais focos de tensão estão no Exterior, mas o Brasil não está imune. Há três anos, 18 Estados foram afetados por um blecaute, que, ao que parece, foi provocado por um ataque hacker. É por essas e outras que o País acaba de inaugurar um Centro de Defesa Cibernética, mantido pelo Ministério da Defesa.

Por se tratar de sistemas interligados, todos os países devem a partir de agora manter estratégias contra ataques virtuais. É evidente, porém, que algumas regiões são mais propensas a iniciar um conflito virtual. É o caso do Irã, que reúne um exército de hackers desde que foi vítima do complexo vírus Stuxnet, descoberto em junho de 2010, usado para prejudicar as centrais nucleares do país. O código fez com que as centrífugas fossem acionadas acima da velocidade normal, resultando em estragos e queda na produção. Feito um míssil cujos danos vão além dos alvos planejados, o Stuxnet se espalhou e atingiu computadores de outros países, como Indonésia e Paquistão. Sofisticado, ele explorou quatro vulnerabilidades "dia zero", que são brechas desconhecidas antes do ataque, sem dar tempo para a vítima se preparar.

Grupos de hackers raramente usam mais de uma lacuna em um vírus. "A intenção do hacker comum é mostrar a vulnerabilidade, para depois vender o segredo no mercado", afirma José Antunes, gerente de engenharia de sistemas da McAfee. A conclusão a que diversos analistas chegaram foi de que somente um Estado com investimentos parrudos em tecnologia poderia criar essa arma. A imprensa americana denunciou que os Estados Unidos e Israel criaram o Stuxnet como parte da operação "Olympic Games", iniciada durante a administração de George Bush, em 2008, e mantida por Barack Obama. "Os Estados Unidos vão responder a ataques no ciberespaço como fariam a qualquer ameaça ao país", disse Obama em um discurso proferido em 2009.

Oficialmente, o Pentágono, que tem um chefe da segurança virtual, o general

Defesa: Obama diz que EUA responderão a ataques, embora o Pentágono, cujo chefe de seguranca virtual é o general Keith Alexander, não tenha regras definidas para o assunto



Proteção: o general José Carlos dos Santos afirma que centro cibernético vai defender redes de infraestrutura

PROTEJA SUA EMPRESA

CUIDADOS SIMPLES PODEM AJUDAR UMA COMPANHIA A EVITAR AS AMEAÇAS VIRTUAIS

- Quando possível, use **versões de 64 bits** do sistema operacional, que são mais resistentes a ataques
- Mantenha todos os **programas** usados na empresa **atualizados**
- Instale e **faça averiguações rotineiras** em todos os terminais da empresa de um programa de segurança reconhecido no mercado
- Feche qualquer **ponto vulnerável da rede** (por exemplo: um computador mais antigo ligado à intranet)
- Crie a cultura da **computação segura na empresa**: os funcionários devem ter cuidado ao abrir anexos de remetentes desconhecidos, não publicar informações de uso interno nas redes sociais e usar senhas complexas
- Tenha um **controle de acesso às informações** da organização de acordo com o grau hierárquico do colaborador

Fonte: Kaspersky / McAfee / ITS

FOTOS: CHUCK KENNEDY, AP PHOTO/JEFF CHIU, RODRIGO PAIVA/FOLHAPRESS, AP PHOTO/DAN BALILTY

Blecaute hacker: a emissora americana de tevê CBS creditou um apagão que afetou São Paulo e mais 17 Estados, em 2009, a ataques virtuais ao sistema energético do Brasil

Keith Alexander, ainda não conta com regras sobre como e quando reagir a um ciberataque. É por isso que o Congresso americano deve votar leis específicas sobre o assunto, ainda neste ano. Em meio a esse contexto cibernético, quem pode sofrer são as empresas. Obama disse estimar que as companhias dos EUA perderam US$ 1 trilhão em roubo de propriedade intelectual via ambientes digitais, em um ano.

Outra questão que vai nortear a política americana é o fato de os serviços de infraestrutura básica serem automatizados e, portanto, suscetíveis a ataques. Isso o Brasil já sentiu na pele. Em 2009, a rede americana CBS afirmou que dois blecautes no País - no Espírito Santo e Rio de Janeiro - foram provocados por hackers. O governo negou a informação. Porém, alguns dias depois, 18 Estados brasileiros sofreram outro apagão, o que reforçou as suspeitas.

Na esfera federal, tanto o Exército quanto a Polícia Federal têm órgãos dedicados a proteger o País de ataques cibernéticos. As duas instituições inauguraram seus centros para cuidar do assunto somente em junho deste ano, em preparação para a Rio+20. **O Centro de Defesa Cibernética (CDCiber), do Exército, cujos profissionais estão em fase de treinamento, tem a meta de investir R$ 400 milhões até 2015, com expectativa de R$100 milhões esperano.** Sua primeira missão foi monitorar, em parceria com a PF e o Serviço Federal de Processamento de Dados (Serpro), a estrutura de rede usada na Rio+20. Ainda em fase de implantação, o centro busca preparar o Brasil para se proteger de ataques a infraestruturas de energia, água e telecomunicações. "A preocupação é incrementar a segurança das nossas redes corporativas, caso das Forças Armadas, e das redes operacionais, como serviços públicos", afirma o general José Carlos dos Santos, chefe do CDCiber. "Até 2030, temos uma previsão de investir R$ 2,3 bilhões no centro."

No caso da Polícia Federal, o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos dispõe de um orçamento de R$ 10 milhões para aquisição de hardware e software e capacitação de profissionais. O primeiro teste da PF nessa área também foi a Rio+20. Segundo o chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, delegado Carlos Eduardo Sobral, a principal preocupação da PF tem sido coibir ataques a serviços de utilidade pública, como bancos públicos. "Nossa maior preocupação deixou de ser o combate à pedofilia ou pornografia infantil", diz Sobral. "Nosso foco agora é proteger informações do governo."

Os cuidados que o Brasil e outros países começam a tomar na área de segurança virtual costumam mirar o inimigo externo. As ameaças virtuais, porém, não necessariamente vêm de fora. Em 2002, a petrolífera venezuelana PDVSA foi alvo de uma greve. Parte dos funcionários tentou manter a operação, mas foi inútil: o sistema de TI estava sob controle da antiga diretoria, opositora do governo Hugo Chávez. Assim, a produção foi reduzida em mais de três milhões de barris por dia, afetando o preço mundial da commodity. O perito brasileiro de crimes virtuais Ricardo Theil, hoje consultor do Instituto de Tecnologia de Software (ITS), atuou no caso e afirma que a sabotagem digital vista na PDVSA pode acontecer com qualquer corporação. "Uma companhia pode tirar uma concorrente do mercado com um ataque que afete sua produção", afirma Theil. Ainda assim, a maior parte das companhias não adota medidas para evitar os ataques. "Um funcionário insatisfeito também pode comprometer a segurança de toda a empresa, sem contar as ameaças que surgem diariamente."

"É PRECISO ESTABELECER AS REGRAS DO JOGO"

Eugene Kaspersky é presidente da empresa que leva seu sobrenome, uma das mais conhecidas na área de segurança virtual. Voz ativa no alerta sobre as ameaças entre países, ele defende a criação de uma Organização Internacional da Cibersegurança.

Deveria haver regras para o uso de ciberarmas?

O que podemos fazer é estabelecer as regras do jogo para o campo de batalha virtual, regular o uso de ciberarmas. Penso que uma Organização Internacional da Cibersegurança deveria ser criada. Ela agiria como uma plataforma global independente para a cooperação internacional.

Quem apoiaria o órgão?

Os mais vulneráveis, como países com uso intenso de internet, deveriam ser os primeiros. Não surpreendentemente, descobri que pessoas que discutem essa questão há bastante tempo partilham de minha opinião, incluindo Michael V. Hayden [general americano e ex-diretor da CIA], Neelie Kroes [vice-presidente para assuntos digitais da Comissão Europeia] e Giampaolo Di Paola [ministro da Defesa da Itália]. Porém, não é fácil colocar essa ideia em prática. A sociedade ainda considera os computadores e a internet como brinquedos virtuais.

Ação global: Eugene Kaspersky propõe a criação de um órgão internacional para regular a questão da cibersegurança

Fonte: Istoé Dinheiro, São Paulo, ano 15, n. 775, p. 44-47, 15 ago. 2012.