Nações se aprontam para guerras cibernéticas
Bruno Romani

Supervírus no Irã reforça preocupações de governos e empresas globais

Inimigos "sem rosto" colocam em risco infraestrutura mundial; rede militar dos Estados Unidos já foi violada

O mundo se está a beira de uma guerra. Mas, em vez de bombas e explosões, o caos virá por meio de apagões no sistema elétrico e colapso nas comunicações. A causa para tudo isso: um potente vírus de computador.

O conceito de guerra cibernética, ataques à infraestrutura do Estado por meio de computadores, soa como script de filme, mas governos, empresas e agências de inteligência demonstram preocupação. "A ameaça é real e digna de atenção", disse na semana passada Iain Lobban, diretor da GCHQ, agência britânica de espionagem eletrônica.

O medo de uma ciberguerra ganhou força com a descoberta do Stuxnet, um malware do tipo worm que infectou milhares de máquinas no Irã, na Indonésia e na Índia.

O que chamou a atenção na praga era que ela tinha como alvo sistemas de controle utilizados em processos industriais, como os de usinas de energia. Ele explorava pelo menos três vulnerabilidades no Windows do tipo "dia zero", aquelas ainda não descobertas por desenvolvedores - número inédito de falhas para a mesma praga. E também tinha duas certificações de segurança, que no mercado negro podem custar US$ 500 mil.

Dada a complexidade da praga, especialistas acreditam que ela tenha sido concebida pelo governo de um país. Empresas que analisaram o código do Stuxnet dizem que ele não visava ganhos financeiros ou roubo de dados. Ele teria sido criado para sabotar e o alvo seria o programa nuclear iraniano.

Teerã já disse ter prendido "espiões" e acusa o Ocidente.

SEM ROSTO

Uma das grandes dificuldades de ataques pela rede é que o inimigo não tem rosto. É possível identificar no código do malware sua origem, mas, diz Roel Schouwenberg, analista da Kaspersky, muitas vezes sinais falsos são plantados com a intenção de confundir. "O mais prudente é ignorá-los", diz ele.

Mesmo pragas potentes, como o Stuxnet, porém, dependem de formas simples para atingir o alvo com sucesso. Segundo os especialistas ouvidos pela Folha, pen drives e laptops contamindos são mais perigosos do que ataques feitos pela rede.

Em 2008, a maior falha da história na rede militar dos EUA foi causada por um pen drive. O vice-secretário de defesa do país, William J. Lynn III, disse que o malware queria roubar informações.

Fonte: Folha de S.Paulo, São Paulo, 20 out. 2010, Tec, p. F4.