MUNDO • GUERRA NA UCRÂNIA

Ucrânia convocou 'exército de TI' contra ações cibernéticas russas, mas Moscou ainda não usou seu potencial na guerra atual

Recursos de defesa dos ucranianos foram reforçados e sujeitos a ataques desde 2014, e autoridades prometem reagir a possíveis agressões de Moscou contra seus sistemas

Filipe Barini
13/03/2022 - 05:30 / Atualizado em 13/03/2022 - 15:50

Tela de computador infectado com o vírus que "sequestra" arquivos, como o NotPetya, em 2017 Foto: Simon Dawson / Bloomberg

Horas antes de as tropas russas começarem a invasão da Ucrânia, dezenas de sites de instituições e bancos ucranianos ficaram inacessíveis, no que autoridades locais e serviços de monitoramento digital afirmaram ser um ataque contra o país — o terceiro do tipo neste ano.

"Um outro ataque DDoS contra nosso Estado começou", disse no Telegram, em 24 de fevereiro, o ministro da Transformação Digital ucraniano, Mykhailo Fedorov, usando a sigla em inglês para "ataque distribuído de negação de serviço", quando uma ação coordenada, com várias máquinas, derruba um determinado sistema. Naquele mesmo dia, empresas de segurança digital, como a Symantec, apontaram que computadores na Ucrânia também eram alvo de um "software malicioso" (malware) responsável por apagar dados de máquinas infectadas.

Entenda: Para analista, cálculo errado pode explicar silêncio cibernético russo

Ao lado dos sinais de uma invasão convencional, havia o temor em Kiev de que o ataque militar seria acompanhado por ações contra sistemas estratégicos da Ucrânia, incluindo redes de transmissão de energia. Afinal, desde 2014, quando a Euromaidan depôs o presidente pró-Moscou Viktor Yanukovych e um governo

anti-Rússia chegou ao poder, ciberataques de grandes proporções são uma rotina.

Antes do conflito: Após fracasso de negociações entre Rússia e Otan, Ucrânia sofre ataque hacker e sites do governo saem do ar

Como parte dos planos de defesa, agora com foco no atual conflito e na possibilidade de uso de um "arsenal digital", o governo da Ucrânia, que já vinha convocando voluntários de todo o mundo para o front, fez um apelo também a hackers e especialistas em segurança. "Estamos criando um exército de TI (Tecnologia de Informação). Precisamos de talentos digitais", escreveu o ministro Fedorov no Twitter, no dia 26 de fevereiro. "Haverá tarefas para todos. Continuaremos a lutar no front cibernético."

Hoje, há cerca de 35 mil inscritos no canal de Telegram usado para a convocação, mas não se sabe exatamente quantos são "soldados" ou quantos são jornalistas, pesquisadores ou apenas curiosos. A maior parte das tarefas é defensiva, mas existe a possibilidade de serem usados em ações ofensivas contra a Rússia.

— A questão aqui é que estamos sob ataque, e jamais reagimos. Só nos defendemos. Então, pela primeira vez, vamos tentar mostrar para eles [russos] como é a sensação de ter sua infraestrutura atacada, quando é não poder usar

cartões bancários ou serviços do governo — disse Oleksandr Bornyakov, vice-ministro de Tranformação Digital, ao site TechCrunch.

Novo 'campo de combate': Hackers assumem posição central na estratégia de grandes potências

Apesar das grandes expectativas, especialistas ouvidos pelo GLOBO são um pouco mais céticos quanto à “tropa digital”.

— Os impactos desse grupo ainda não podem ser verificados, mas é provável que, dentro de um conflito armado, suas operações sejam, na melhor das hipóteses, insignificantes — disse Lukasz Olejnik, pesquisador independente de cibersegurança e ex-consultor da Cruz Vermelha em Genebra.

Stuart Madnick, professor de Tecnologia da Informação na Escola Sloan de Gestão no Instituto de Tecnologia de Massachusetts, por sua vez, lembra que nem sempre são necessários tantos recursos, técnicos e humanos, para uma operação do tipo.

— Não sei o quão eficazes eles são, mas você não precisa de muita gente para provocar estragos. Não falei com eles e não sei o que têm em mãos. Mas acredito que há um aspecto de relações públicas em ter tanta gente de fora vindo para te ajudar — disse ao GLOBO.

Alerta: EUA, UE e Otan acusam China de hackear servidor da Microsoft em campanha global de ciberataques

Ainda não foi possível verificar em grande escala as capacidades do "Exército de TI" ucraniano: ao contrário do que se previa, a Rússia tem evitado repetir ações passadas contra a Ucrânia. Em 2015 e 2016, ataques derrubaram os sistemas de transmissão de energia, deixando milhares de pessoas sem luz, inclusive em Kiev.

— Neste conflito, não tivemos ciberataques de grande impacto. Eles não estão sendo aplicados, talvez com a exceção dos efeitos de alguns malwares de destruição de dados provocando problemas em sistemas de controle de fronteiras — aponta Lukasz Olejnik. — Como o elemento cibernético será usado vai depender de como o conflito se desenrolar no futuro. Ciberataques de impacto não podem ser afastados, mas eles não são uma certeza. Tudo depende dos objetivos de seus autores.

Defesas

Nos últimos anos, a Ucrânia vem recebendo ajuda externa para desenvolver sua defesa, por parte de consultores independentes e do governo dos EUA, com investimentos milionários. O objetivo: preparar o país para o pior cenário possível.

Um exemplo dessa estratégia foi relatada pelo Financial Times, no começo do mês: meses antes de a guerra começar, consultores dos EUA se deslocaram rumo à Ucrânia para uma "varredura" em busca de programas maliciosos que poderiam apagar dados e sistemas inteiros.

Sistema financeiro 'paralelo': Criptomoedas ajudam a financiar grupos de apoio ao governo da Ucrânia, afirma relatório

Segundo o jornal, um dos malwares foi encontrado na empresa estatal de trens, justamente um dos principais meios usados pelos ucranianos para fugir do país. Caso tivesse sido acionado, milhares de pessoas poderiam ser impedidas de seguir viagem.

— Com certeza há tantas, tantas ações que não foram descobertas e que deixaram alguns malwares capazes de serem ativados — disse ao Financial Times V.S. Subrahmanian, professor de Ciência da Computação no Northwestern College. — É como uma bomba plantada em sua própria casa: é inócua até que seja ativada.

Não está claro por que a Rússia, que em tese tem capacidade de lançar grandes ações, ainda não utilizou maciçamente a arma cibernética.

Alguns analistas apontam para uma resposta: as forças russas menosprezaram as capacidades ucranianas, e acharam que a estratégia de "choque e pavor" não demandaria ferramentas não convencionais. Um argumento a favor dessa tese

vem dos próprios campos de batalha, com militares deixando de lado sistemas seguros de comunicação e usando celulares comuns ou rádios civis, facilmente interceptados e bloqueados.

Imagem manchada?: Rússia expõe falhas militares na Ucrânia que podem ser exploradas por adversários no futuro

Outra hipótese tem a ver com o planejamento de guerra, não apenas imediato, mas em médio e longo prazo: Stuart Madnick, do MIT, lembra que ataques de grande porte facilmente podem se espalhar por outros países, mesmo que tenham como alvo um sistema específico.

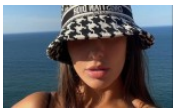
Ele cita o caso do Stuxnet, um vírus usado por EUA e Israel que em 2010 provocou estragos na central nuclear de Natanz, no Irã, mas também afetou computadores de Indonésia, Azerbaijão e dos próprios EUA. Outro exemplo é o vírus NotPetya, em 2017, que "sequestrava" computadores e sistemas e exigia um pagamento para sua liberação. A ação foi considerada a maior da História pelos EUA e atribuída à Rússia.

— O NotPetya tinha como alvo negócios ucranianos, mas alguns desses negócios eram subsidiárias de empresas multinacionais. E, assim que o vírus entrou nesses computadores, ele rapidamente se espalhou pelas redes de empresas globais, e todas tiveram suas atividades suspensas por longos períodos — afirmou o especialista.

Ainda ao falar sobre possíveis piores cenários, Mednick lembrou que, ao contrário dos combates no mundo não virtual, nem sempre é fácil descobrir de onde veio o ciberataque, o que poderia levar a conclusões erradas ou ações destinadas a responsabilizar o lado inimigo.

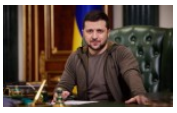
— Quando alguém dispara um canhão, você tem uma boa ideia de onde ele foi disparado. Em se tratando de um ciberataque, é muito difícil determinar isso. Um conhecido meu que trabalha com isso sempre me diz que um hacker muito bom é aquele que sabe como deixar evidências que apontem para qualquer outra pessoa — concluiu Madnick.

O GLOBO RECOMENDA



ELA
Thais Braz exibe estrias nos seios e ganha elogios em foto sem filtro: 'Uma mulher real'

POLÍTICA
Bancada invisível: saiba quem são os deputados com mais faltas sem justificativa na Câmara



MUNDO
'Entendemos que não faremos parte da Otan', diz presidente da Ucrânia

MUNDO
Jornalista ucraniana é morta junto a cinegrafista da Fox News em ataque russo

MAIS LIDAS NO GLOBO

1. **Bancada invisível: saiba quem são os deputados com mais faltas sem justificativa na Câmara**
Bruno Góes e Dimitrius Dantas

2. **Autoridades dos EUA dizem que mortes em tropas russas estão aumentando**

Do New York Times

3. **Mulher entregou Bíblia e disse que 'enxergou Deus' em morador de rua antes de ter relações com ele; marido diz que ela foi abusada**

Arthur Leal

4. **Autores de ameaças contra senadores contrários a PL das Armas são atiradores e colecionadores, diz relator**

Camila Zarur

5. **Três semanas após a Rússia invadir a Ucrânia, qual é, afinal, o número de mortos na guerra?**

Gabriel Morais

MAIS DE MUNDO

VER MAIS