Afiliados ao Exército de Libertação Popular invadiram sistemas de órgãos críticos do país

Infraestrutura dos EUA sob mira de hackers chineses

ELLEN NAKASHIMA
JOSEPH MENN
THE WASHINGTON POST

Pentágono
Congresso aprova orçamento de Defesa de US$ 886 bilhões que inclui o desenvolvimento de programas de vigilância eletrônica

As Forças Armadas da China estão incrementando sua capacidade de perturbar infraestruturas críticas dos Estados Unidos, incluindo serviços de fornecimento de energia e água, assim como sistemas de comunicações e transportes, de acordo com autoridades americanas e responsáveis por segurança na indústria.

Hackers afiliados ao Exército de Libertação Popular (ELP) invadiram sistemas computacionais de aproximadamente uma dúzia de entidades críticas ao longo do ano passado, afirmam os especialistas. As invasões são parte de um esforço mais amplo de desenvolver maneiras de semear pânico e caos ou perturbar logísticas na eventualidade de um conflito EUA-China no Pacífico, afirmaram eles.

Entre os alvos estiveram uma instalação hídrica no Havaí, um grande porto na Costa Oeste e pelo menos uma rede de tubulações de petróleo e gás natural, segundo relataram ao *Washington Post* pessoas familiarizadas com os incidentes. Os hackers também tentaram invadir o operador do sistema de eletricidade do Texas, que opera independentemente das redes de transmissão do restante do país.

Várias entidades fora dos EUA, incluindo empresas de eletricidade, também foram vítimas dos hackers, afirmaram as fontes, que falaram sob condição de anonimato em razão da sensibilidade do tema.

Nenhuma invasão afetou sistemas de controle industrial que operam bombas, motores ou outro tipo de função crítica, nem causou nenhuma perturbação, afirmaram autoridades americanas. Mas elas disseram que a atenção ao Havaí, lar da Frota do Pacífico dos EUA, e a pelo menos um porto, assim como a centros de logística, sugere que os militares chineses querem a capacidade de complicar esforços americanos para enviar soldados e equipamentos para a região se um conflito sobre Taiwan irromper.

Esses detalhes, revelados com exclusividade, ajudam a compor uma visão de uma campanha cibernética apelidada de Tufão Volt, detectada pela primeira vez cerca de um ano atrás pelo governo americano, conforme EUA e China enfrentam dificuldades para estabilizar uma relação que passa pelo período de maior antagonismo em décadas.

Os comandantes militares chineses recusaram-se por mais de um ano a conversar com comandantes americanos, mesmo em casos cada vez mais comuns no Pacífico Ocidental em que caças de combate chineses quase interceptaram aviões-espiões dos EUA. Os presidentes de EUA, Joe Biden, e China, Xi Jinping, concordaram em restaurar esses canais de comunicação em novembro.

"Está muito claro que as tentativas chinesas de comprometer infraestruturas críticas são, em parte, para se pré-posicionar para mostrar serem capazes de perturbar ou destruir aquelas infraestruturas críticas na eventualidade de um conflito, ou até para evitar que Washington seja capaz de projetar poder na Ásia ou para provocar caos social dentro dos EUA – para afetar nossa tomada de decisão numa crise", afirmou o diretor executivo da Agência de Cibersegurança e Infraestrutura (Cisa) do Departamento de Segurança Interna, Brandon Wales. "É uma mudança significativa em relação à atividade cibernética da China de sete a dez anos atrás, que tinha foco principalmente em espionagem política e econômica."

Esquema de ataque
Detalhes revelados ajudam a compor uma visão de uma campanha cibernética apelidada de Tufão Volt

O diretor do Centro de Colaboração em Cibersegurança da Agência de Segurança Nacional (NSA), Morgan Adamski, confirmou por e-mail que a atividade Tufão Volt "parece ter foco em alvos dentro da região do Indo-Pacífico, a incluir o Havaí".

MÉTODOS. Os hackers mascaram seus rastros realizando seus ataques por meio de dispositivos inofensivos, como roteadores de residências ou empresas, antes de alcançar suas vítimas, afirmaram autoridades. Um objetivo crítico foi roubar credenciais de funcionários que eles poderiam usar para retornar, disfarçados de usuários normais. Mas alguns de seus métodos de entrada não foram determinados.

Os hackers buscam uma maneira de entrar nos sistemas e ficar dentro sem ser detectados, afirmou o pesquisador Joe McReynolds, que estuda segurança chinesa na Fundação Jamestown, um instituto de análise com foco em questões de segurança. "Você está tentando construir túneis de acesso à infraestrutura de seu inimigo para poder usar posteriormente para atacar. Até lá, fica em espera, faz reconhecimentos, aprende como entrar em sistemas de controle industrial, em empresas mais importantes ou alvos de nível mais alto. E um dia, se vier a ordem de cima, você passa do modo de reconhecimento para o modo de ataque."

As revelações do *Post* reforçam as constatações da análise anual de ameaças do Escritório da Diretora de Inteligência Nacional, que alertaram, em fevereiro, que a China "quase certamente é capaz" de lançar ciberataques que perturbariam infraestruturas críticas nos EUA, incluindo tubulações de petróleo e gás natural e sistemas ferroviários.

"Se Pequim temesse que um grande conflito com os EUA era iminente, quase certamente consideraria praticar operações cibernéticas agressivas contra infraestruturas domésticas críticas e ativos americanos em todo o mundo", afirmou a análise.

Algumas das vítimas do Tufão Volt foram empresas e organizações menores, de setores variados e "não necessariamente que tivesse conexão imediata e relevante com algum serviço crítico do qual os americanos possam depender", afirmou o diretor executivo da Cisa, Eric Goldstein. Pode ter havido uma "mira oportunista com base nos locais em que eles conseguem acesso" – como uma maneira de obter um ponto de apoio numa cadeia de fornecimento na esperança de um dia alcançar clientes mais importantes, afirmou ele.

Oficiais militares chineses descreveram em documentos internos como poderiam usar ferramentas cibernéticas ou "guerra de redes" em um conflito, afirmou McReynolds, que analisou parte dos registros.