CHARLES DHARAPAK/AP

DMITRY ASTAKHOV/REUTERS–20/12/2023

TRONGNGUYEN - STOCK.ADOBE.COM

No sentido horário, acusados de ataque hacker; Xi em reunião em Pequim; rede elétrica no Texas

Ele afirmou que estrategistas militares falam em sincronizar ataques aéreos e de mísseis com interrupções de redes de comando e controle, infraestruturas críticas, redes de satélites e sistemas de logística militar.

Eles falaram sobre essas ferramentas aplicando-as em invasões anfíbias, afirmou. "São coisas que eles claramente consideram muito relevantes em um cenário, apesar de não dizerem explicitamente, que é assim que tomarão Taiwan", disse McReynolds.

Esta operação é diferente da primeira incursão chinesa em infraestruturas críticas. Em 2012, a empresa canadense Telvent, cujo software operava remotamente grandes gasodutos na América do Norte, notificou os clientes que um hacker sofisticado tinha invadido seus firewalls e roubado dados relacionados a controles de sistemas industriais. A firma de cibersegurança Mandiant constatou que a invasão foi realizada por um prolífico grupo hacker do ELP, chamado Unit 61398. Cinco membros do grupo foram indiciados em 2014 por hackear empresas americanas.

Na época, o governo americano não tinha certeza se o objetivo da China era coletar inteligência ou se preposicionar para causar perturbações. Hoje, com base em informações de inteligência e no fato das empresas e instalações afetadas terem poucos dados de inteligência de valor político e econômico, as autoridades americanas afirmam ser evidente que a única razão para invadi-las era ser capaz de conduzir ações de interferência ou destruição posteriormente.

O pesquisador de ameaças Jonathan Condra, da empresa de segurança Recorded Future – que em meados do ano descobriu o Tufão Volt inserida na rede de de eletricidade do Texas – afirmou que o nível de sigilo em que os chineses conduziram os ataque indica que eles não queriam que os EUA soubessem de suas capacidades. "Os hackers trabalharam muito mais furtivamente do que se quisessem ser pegos", afirmou.

O governo americano busca há muito melhorar a coordenação com o setor privado, que é dono da maior parte da infraestrutura crítica do país, e empresas de tecnologia capazes de detectar ciberataques. Empresas como Microsoft compartilham dados de forma anônima a respeito das táticas dos adversários, indicadores de que um sistema foi comprometido e mitigações, como explicouGoldstein, do Cisa. Geralmente, essas empresas não percebem a presença dos hackers dentro das redes dos clientes, mas a detectam por meio de comunicações com os servidores que os hackers usam para direcionar os ataques.

Em alguns casos, as próprias vítimas buscam assistência da Cisa. Em outros, afirmou Goldstein, o Cisa é alertado por um software ou fornecedor de rede de comunicação a respeito de uma vítima, e o governo tem de buscar uma ordem judicial para obrigar o fornecedor a revelar a identidade da vítima.

Em maio, a Microsoft afirmou que encontrou um Tufão Volt infiltrado em infraestruturas críticas em Guam e outras partes, listando uma série de setores. As vítimas incluíam empresas de telecomunicações, de acordo com fontes familiarizadas com o assunto. Os ataques de hackers foram preocupantes, afirmaram analistas, porque Guam é o território americano mais próximo ao contestado Estreito de Taiwan.

As invasões em setores como sistemas hídricos e redes de eletricidade ocorrem enquanto o governo Biden busca fortalecer a capacidade da indústria de se defender, aplicando uma série de regras obrigatórias de cibersegurança. Em 2021, o governo americano publicou as primeiras regulações de Washington sobre cibersegurança em tubulações de petróleo e gás natural. Em março, a Agência de Proteção Ambiental (EPA) anunciou um requerimento para que os Estados relatem ameaças cibernéticas em suas auditorias de sistemas públicos de abastecimento de água. Pouco depois, contudo, três Estados abriram processos contra o governo federal na Justiça, acusando-o de exceder poderes regulatórios.

"A China está sentada sobre uma pilha de vulnerabilidades estratégicas ou falhas de segurança não reveladas que o país pode usar em ataques furtivos. É uma luta por nossa infraestrutura crítica. Temos de dificultar as coisas para eles"

Morgan Adamski
Diretor do Centro de Colaboração em Cibersegurança da Agência de Segurança Nacional (NSA)

PROTEÇÃO. A EPA retirou a regra e pediu para o Congresso produzir a regulação. Enquanto isso, a agência depende dos Estados relatarem as ameaças voluntariamente. uma análise conjunta publicada em maio, a aliança em inteligência Cinco Olhos, um acordo que reúne EUA, Reino Unido, Canadá, Austrália e Nova Zelândia, ofereceu orientações sobre como caçar invasores. Um dos desafios é a tática hacker de evitar detecção de firewalls e outras defesas usando ferramentas legitimamente, para que a presença dos hackers se mescle à atividade normal da rede. A técnica é chamada "viver da terra".

"Os dois desafios mais difíceis com essas técnicas é determinar que um comprometimento ocorreu; e então, uma vez que a invasão é detectada, é difícil ter certeza de que o perpetrador foi expulso", afirmou Adamski, da NSA, cujo Centro de Colaboração em Cibersegurança trabalha em coordenação com o setor privado.

A NSA e outras agências recomendam redefinições massivas de senhas e melhor monitoramento de contas que tenham privilégios de rede elevados. Elas também pediram às empresas para exigir mais formas seguras de autenticação multifator, como tokens de hardware, em vez de depender de mensagens de texto para os telefones dos usuários, que podem ser interceptadas por governos estrangeiros.

NOVOS ALVOS. Apesar da segurança incrementada após a revelação de maio, os hackers persistiram, buscando novos alvos. Em agosto, segundo a Recorded Future, os hackers tentaram fazer conexões a partir de infraestruturas que tinham sido usadas pelo Tufão Volt para domínios ou subdomínios de internet usados pela Comissão de Serviços Públicos e pelo Conselho de Segurança Elétrica do Texas, que opera a rede de transmissão de eletricidade no Estado. Apesar de não haver nenhuma evidência de as tentativas de invasão do sistema terem sido bem-sucedidas, o esforço evidencia o tipo de alvo que interessa aos militares chineses. As duas agências texanas recusaram-se a responder perguntas sobre os incidentes.

O Conselho de Segurança Elétrica afirmou que trabalha proximamente com agências federais e grupos da indústria e que usa sistemas redundantes e controles de acesso como parte de uma "defesa em camadas".

Nas semanas que antecederam a reunião entre Biden e Xi, no mês passado, autoridades da NSA repetiram chamados em conferências da indústria para que o setor privado compartilhe informações sobre tentativas de invasões hacker. A NSA pode vigiar as redes dos adversários no exterior, enquanto as empresas americanas conseguem observar as redes corporativas dentro do país. Juntos, a indústria e o governo podem conseguir obter uma percepção mais completa sobre objetivos, táticas e motivações dos adversários dos EUA, afirmam autoridades americanas.

"A China está sentada sobre uma pilha de vulnerabilidades estratégicas, ou falhas de segurança não reveladas que o país pode usar em ataques furtivos", afirmou Adamski no mês passado na conferência CyberWarCon, em Washington. "É uma luta por nossa infraestrutura crítica. Temos de dificultar as coisas para eles."

O tópico das intrusões cibernéticas da China em infraestruturas críticas figurou numa lista proposta de temas a serem levantados no encontro de Biden com Xi, de acordo com fontes familiarizadas com o assunto, mas não foi abordado nas quatro horas de reunião. ● TRADUÇÃO DE GUILHERME RUSSO