Exclusivo: Hackers invadiram sistema de combustível nos EUA; Irã é suspeito

Category: GERAL,MUNDO,TECNOLOGIA e CIÊNCIA
escrito por Maria Luiza | 16 de maio de 2026

Autoridades dos Estados Unidos suspeitam que hackers do Irã estejam por trás de uma série de invasões a sistemas que monitoram a quantidade de combustível em tanques de armazenamento que abastecem postos de gasolina em diversos estados, de acordo com múltiplas fontes a par da atividade.

Os hackers □□exploraram sistemas de medição automática de tanques (ATG, na sigla em inglês) que estavam online e desprotegidos por senhas, permitindo, em alguns casos, manipular as leituras exibidas nos tanques, mas não os níveis reais de combustível, disseram as fontes.

Não se sabe se as invasões cibernéticas causaram danos físicos, mas as violações levantaram preocupações de segurança, pois o acesso a um sistema ATG poderia, em teoria, permitir que um hacker fizesse um vazamento de gás passar despercebido, de acordo com especialistas e autoridades americanas.

As fontes a par da investigação disseram que o histórico do Irã de atacar sistemas de tanques de combustível é um dos motivos pelos quais o país é o principal suspeito.

No entanto, as fontes alertaram que o governo americano pode

não conseguir determinar definitivamente quem foi o responsável devido à falta de evidências deixadas pelos hackers.

Se o envolvimento do Irã for confirmado, este será o caso mais recente de Teerã ameaçando infraestruturas críticas em território americano, que permanecem fora do alcance de drones e mísseis iranianos.

Isso também poderia levantar uma questão politicamente sensível para o governo de Donald Trump, chamando ainda mais atenção para o aumento dos preços da gasolina causado pela guerra.

Uma pesquisa recente apontou que 75% dos adultos americanos entrevistados avaliam que a guerra com o Irã teve um efeito negativo em suas finanças.

A campanha de hackers também serve de alerta para muitos operadores de infraestrutura crítica nos EUA que têm lutado para proteger seus sistemas, apesar de anos de recomendações federais.

Grupos de hackers iranianos há muito tempo buscam alvos fáceis – sistemas de computador críticos dos EUA que interagem com instalações de petróleo e gás e sistemas de água, por exemplo.

Após o ataque do Hamas a Israel em 7 de outubro de 2023, autoridades americanas culparam hackers afiliados à Guarda Revolucionária Islâmica do Irã por uma série de ataques a empresas de serviços públicos de água nos EUA, que exibiram mensagens anti-Israel em equipamentos usados □□para controlar a pressão da água.

Pesquisadores de segurança cibernética vêm alertando sobre os ATGs expostos à internet há mais de uma década. Em 2015, a empresa de segurança Trend Micro colocou sistemas ATG simulados online para verificar que tipo de hackers os atacariam. Um grupo pró-Irã surgiu rapidamente.

Um relatório de 2021 da Sky News citou documentos internos da Guarda Revolucionária Islâmica que apontavam os ATGs como um alvo potencial para um ataque cibernético disruptivo a postos de gasolina.

Operações cibernéticas do Irã estão “acelerando”

As agências de inteligência americanas consideram as capacidades cibernéticas do Irã inferiores às da China ou da Rússia. Mas uma série de ataques oportunistas a importantes ativos americanos durante a guerra sugere que o Irã é um adversário capaz – e imprevisível.

Desde o início da guerra, no final de fevereiro, hackers ligados a Teerã causaram interrupções em diversas instalações de petróleo, gás e água nos EUA, atrasos no transporte de materiais da Stryker, uma importante fabricante americana de dispositivos médicos, e vazaram os e-mails privados do diretor do FBI, Kash Patel.

Organizações e cidadãos israelenses também têm sido alvos frequentes dos hackers iranianos durante a guerra, enquanto os militares dos EUA e de Israel têm usado operações cibernéticas para tornar seus ataques físicos mais letais.

A atividade cibernética do Irã durante a guerra mostrou “um aumento significativo na escala, velocidade e integração entre operações cibernéticas e campanhas psicológicas”, disse Yossi Karadi, chefe da Diretoria Nacional de Cibersegurança de Israel.

Em março, as Forças de Defesa de Israel alegaram ter atacado um complexo que abrigava o “quartel-general de guerra cibernética” do Irã. Não está claro quantos ciberoperadores iranianos, se houver algum, foram mortos nesse ataque.

Karadi não comentou o assunto, pontuando que sua agência se

limita à defesa cibernética.

“Dito isso, de uma perspectiva defensiva, nos últimos meses, estamos observando alguma degradação em partes da atividade cibernética hostil. A questão fundamental é que os agentes iranianos estão sob pressão e estão tentando atacar onde quer que encontrem uma brecha no ciberespaço”, destacou.

Os últimos 18 meses mostraram que as operações cibernéticas do Irã, em geral, “estão se acelerando com iterações mais rápidas, perfis de hacktivistas mais complexos e, provavelmente, escalonamento impulsionado por IA para reconhecimento e phishing”, comentou Allison Wikoff, diretora da equipe de inteligência de ameaças da PwC, com mais de uma década de experiência no rastreamento de ameaças originárias do Irã.

“O que é notavelmente novo em seu manual cibernético é a rápida criação de malware ‘bom o suficiente’, incluindo os tipos destrutivos de limpeza de dados, complementada por campanhas assertivas de invasão e vazamento de informações contra a mídia, dissidentes e infraestrutura civil (americana) chave”, afirmou Wikoff.

Parte da estratégia iraniana consiste em capitalizar sobre o clima de guerra da mídia americana, que está sempre pronta para se aproveitar de alegações feitas por todos os lados.

Hackers associados ao Ministério da Inteligência e ao braço paramilitar do Irã mantêm diversas personas de “hacktivistas” por meio das quais usam o Telegram para exagerar seus feitos, publicar material roubado e lançar vídeos promocionais com músicas cativantes.

Um dos grupos, que se autodenomina Handala, em referência a um personagem de desenho animado palestino, provocou Patel enquanto alegava ter invadido os sistemas de computador “impenetráveis” do FBI. Na realidade, os hackers invadiram os e-mails antigos de Patel no Gmail.

“O fato de cada alegação do Handala causar pânico nas pessoas demonstra que a realidade operacional da ameaça que o Irã representa é algo que tanto agências governamentais quanto fornecedores parecem não conseguir articular”, disse Alex Orleans, pesquisador de segurança cibernética que rastreia hackers ligados ao Irã há anos e lidera a inteligência de ameaças na empresa de segurança Sublime Security.

Apesar da série de ataques cibernéticos realizados pelo Irã durante a guerra, Orleans apresentou dois motivos para que não tenham ocorrido mais.

“O primeiro é que o Irã parece não ter tido acesso suficiente para produzir efeitos sustentados, ou provavelmente teríamos visto mais incidentes como o Stryker”, explicou ele.

“O segundo é que o regime demonstrou claramente sua intenção de perdurar, o que desestimula ainda mais operações cibernéticas indiscriminadas”, concluiu.

“Ninguém está pagando o preço por isso”

Para algumas autoridades americanas, atuais e antigas, a natureza agressiva e imprevisível das operações cibernéticas iranianas ganha ainda mais importância às vésperas das eleições de meio de mandato.

Nas eleições de 2020, agências federais, incluindo a Agência de Segurança Cibernética e de Infraestrutura, culparam o Irã por um esquema que se passava pelo grupo de extrema-direita Proud Boys para tentar intimidar eleitores.

Durante as eleições presidenciais americanas de 2024, hackers iranianos invadiram a campanha de Trump e enviaram documentos internos para veículos de imprensa.

Agora, pela primeira vez em anos, militares e oficiais de inteligência dos EUA ainda não ativaram uma equipe especializada dedicada a detectar e frustrar ameaças

estrangeiras às eleições – uma medida que um ex-oficial do Comando Cibernético, Jason Kikta, considerou uma "negligência estratégica".

"Entre o que vimos o Irã fazer nesta guerra e o que eles fizeram em 2020, eu ficaria surpreso se eles não participassem das eleições de meio de mandato", disse Chris Krebs, que, como diretor da agência em 2020, estava ao lado do então diretor de Inteligência Nacional, John Ratcliffe, quando alertaram o público americano sobre as operações de influência iranianas e russas.

"Minha aposta é em operações de informação, não em ataques a sistemas eleitorais. É para aí que os russos e os chineses têm ido, e por um bom motivo. É barato, é fácil de escalar com IA e ninguém está pagando um preço por isso", afirmou Krebs.

Fonte: g1 e Publicado Por: Jornal Folha do Progresso 16/05/2026/06:44:40

Progresso

Apenas os administradores do grupo poderão mandar mensagens e saber quem são os integrantes da comunidade. Dessa forma, evitamos qualquer tipo de interação indevida. Sugestão de pauta enviar no e-mail:folhadoprogresso.jornal@gmail.com.

Envie vídeos, fotos e sugestões de pauta para a redação do JFP (JORNAL FOLHA DO PROGRESSO) Telefones: WhatsApp (93) 98404 6835– (93) 98117 7649.

"Informação publicada é informação pública. Porém, para chegar até você, um grupo de pessoas trabalhou para isso. Seja ético. Copiou? Informe a fonte."

Publicado por Jornal Folha do Progresso, Fone para contato 93 981177649 (Tim) WhatsApp:-93- 984046835 (Claro) -Site: www.folhadoprogresso.com.br e-mail:folhadoprogresso.jornal@gmail.com/ou e-mail: adeciopiran.blog@gmail.com

Lignosulfonato de sódio no Brasil: onde e por que ele é utilizado