CIBERSEGURANÇA

Investigação do Citizen Lab confirmou primeiro uso de propagandas na internet para invadir dispositivos. Técnica foi usada contra 45 computadores da emissora Al Jazeera, entre 2024 e 2025. Ataque é silencioso e não depende da interação do alvo

Anúncio vira brecha virtual

» PEDRO JOSÉ BORGES SILVA

Uma investigação do Citizen Lab, no último mês, identificou, pela primeira vez, o uso de uma técnica de espionagem digital que utiliza a infraestrutura de publicidade programática para distribuir programas espiões sem que a vítima precise clicar em links ou interagir com anúncios, batizada de AdFection.

O método foi utilizado, segundo o Citizen Lab, para invadir computadores da emissora Al Jazeera. A exploração dessa estrutura de publicidade se insere em um mercado de tecnologias de vigilância que gera preocupação pelo uso contra ativistas , jornalistas e alvos de interesse político.

Quando um usuário acessa uma página, ocorre um leilão automatizado, conhecido como Real-Time Bidding (RTB), que define qual publicidade será exibida. Segundo as informações levantadas, empresas envolvidas na operação conseguiam inserir códigos JavaScript nos espaços publicitários, utilizando a estrutura de plataformas legítimas para alcançar os dispositivos dos usuários.

Depois da exibição, o código coleta informações técnicas do aparelho, como endereço IP e sistema operacional, para definir se o equipamento invadido é um alvo em potencial.

A partir dessa confirmação, a cadeia de ataque utiliza falhas de segurança para contornar mecanismos de proteção, como a sandbox do navegador, e instalar o spyware.

Entre as empresas relacionadas à estrutura está a Discover-Tech, responsável pela plataforma Controlium, utilizada para operacionalizar campanhas de publicidade. A investigação também identificou conexões entre a Discover-Tech e empresas de espionagem digital, como a israelense Candiru, agora chamada Integrity Labs, conhecida pelo desenvolvimento do spyware Devil's Tongue, ou Arwen.

Pesquisadores analisaram cerca de 4 bilhões de registros de lances publicitários. A estrutura teria alcançado mais de 120 mil sites e 75 mil aplicativos para Android e iOS, incluindo páginas de grande acesso, como *The New York Times*, BBC e Yahoo, além de aplicativos como Truecaller, Snap VPN e jogos para dispositivos móveis.

O ecossistema identificado inclui, ainda, vínculos com a Intellexa, grupo associado ao desenvolvimento e à comercialização do spyware Predator, além de empresas como Bindecy e Intelos, relacionadas a pesquisas de vulnerabilidades, exploração de falhas em navegadores e coleta de dados para vigilância. Os levantamentos também mencionam Eric Banoun, veterano do setor de operações cibernéticas em Israel, que teria integrado o conselho de administração da Discover-Tech.

Vigilância

Um dos casos concretos identificados pelo Citizen Lab envolve um jornalista da emissora Al Jazeera. Durante a análise do dispositivo, pesquisadores recuperaram um arquivo com extensão .dll, utilizado no sistema Windows, que indicaria a presença de uma versão atualizada da cadeia de ataque associada à Candiru.

Segundo o relatório, pelo menos 45 dispositivos da Al Jazeera foram alvos da operação. A emissora informou que identificou atividades suspeitas nos dispositivos de jornalistas e procurou o Citizen Lab para investigar o caso.

Antes da investigação, apesar das denúncias, não havia comprovação de que esses sistemas eram utilizados para infectar dispositivos de civis. A descoberta, no entanto, indica que essas ferramentas podem ir além do monitoramento de autoridades governamentais e pessoas classificadas como "terroristas", alcançando também jornalistas e ativistas.

Para a advogada Ludmila Filizola, especialista em Direito Digital e Novas Tecnologias e diretora jurídica e de operações do escritório M.Puppe & Associados, a principal questão jurídica da AdFection está no uso de uma arquitetura válida para monitorar e infectar dispositivos sem o conhecimento dos usuários.

"Do ponto de vista jurídico, a questão muda de patamar quando há acesso não autorizado ao dispositivo, coleta clandestina de informações ou instalação de software com finalidade de vigilância. A partir daí, já podemos estar diante de crimes como invasão de dispositivo e, dependendo do caso, interceptação ilegal de comunicações", explica.

O fato de o ataque ocorrer sem interação da vítima apenas agrava essa avaliação, e mostra como a invasão pode ser silenciosa.

Filizola também aponta limites legais para a comercialização e o uso de ferramentas de espionagem digital, mesmo se usado para governos e órgãos de inteligência. "Uma contratação pública ou uma justificativa genérica de segurança nacional não autoriza qualquer forma de monitoramento", afirma a advogada.

Marcelo Cassal Jr./Agência Brasil



Publicidade pode ser utilizada para instalar spywares sem que o usuário precise clicar nem baixar nada

Binance retoma saques

A Binance retomou ontem a primeira fase de saques, entre 3h e 6h de Brasília, após o ataque hacker que levou à suspensão temporária do serviço. Segundo a plataforma, os depósitos seguem abertos e não foram afetados.

Em atualização publicada no site oficial, a corretora afirmou que adotou medidas de precaução para proteger a plataforma, realizou avaliações de segurança e trabalhou para verificar a prontidão dos serviços impactados. A reabertura, segundo a Binance, ocorrerá de forma progressiva, com novas redes e ativos adicionados à medida que os testes de estabilidade e segurança forem concluídos.

Em publicação no X, após a reabertura, a companhia disse ter registrado uma saída de US$ 3,64 bilhões, o que representa 2,1% dos US$ 171 bilhões em ativos totais. "Após um pico inicial, os volumes de retirada diminuíram e estão se estabilizando conforme o esperado", afirmou.

A corretora afirmou, ainda, que, no início do processo, pode haver atrasos e tempos maiores de processamento devido ao volume de tráfego e recomendou que usuários tentem novamente em caso de falha, por ser uma retomada em fases.

A Binance reiterou que os recursos dos usuários "permanecem seguros" e disse que a empresa vai absorver o impacto financeiro dos fundos roubados. A plataforma afirmou ter coberto cerca de 95% do valor impactado, ante 90% na atualização anterior, e que os 5% restantes envolvem tokens menos líquidos.(**Com informações da Agência Estado**)

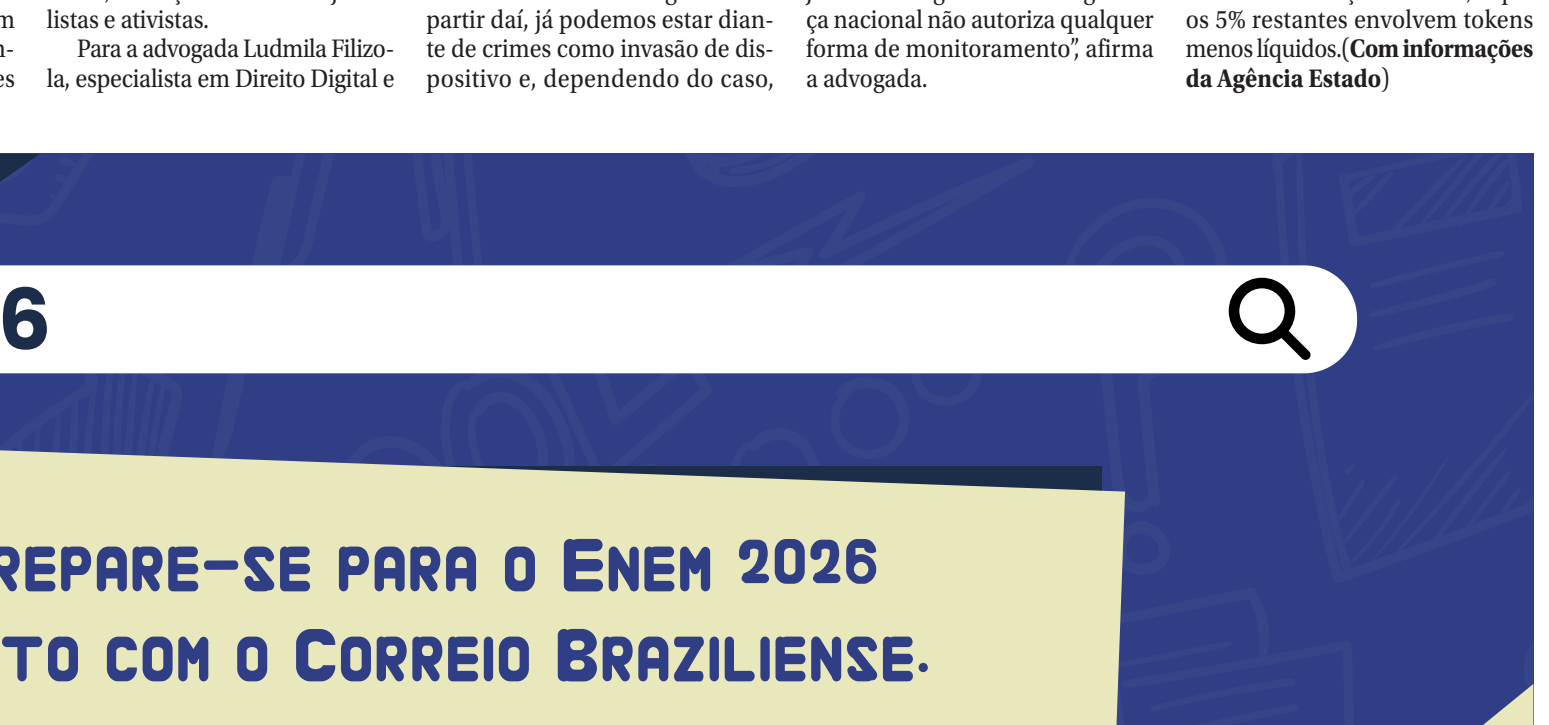
ENEM 2026

PREPARE-SE PARA O ENEM 2026 JUNTO COM O CORREIO BRAZILIENSE.

O Correio Braziliense, com o apoio do Bernoulli Educação, está preparando conteúdos exclusivos para ajudar você na preparação para o ENEM 2026.

Serão materiais, dicas e orientações pensados para fortalecer seus estudos, aumentar sua confiança e contribuir para um bom desempenho nas provas.

Acesse e saiba mais:



Apoio: Bernoulli A referência em Enem do Brasil | CORREIO BRAZILIENSE

Promoção: Clube FM 105.5 | TV BRASÍLIA