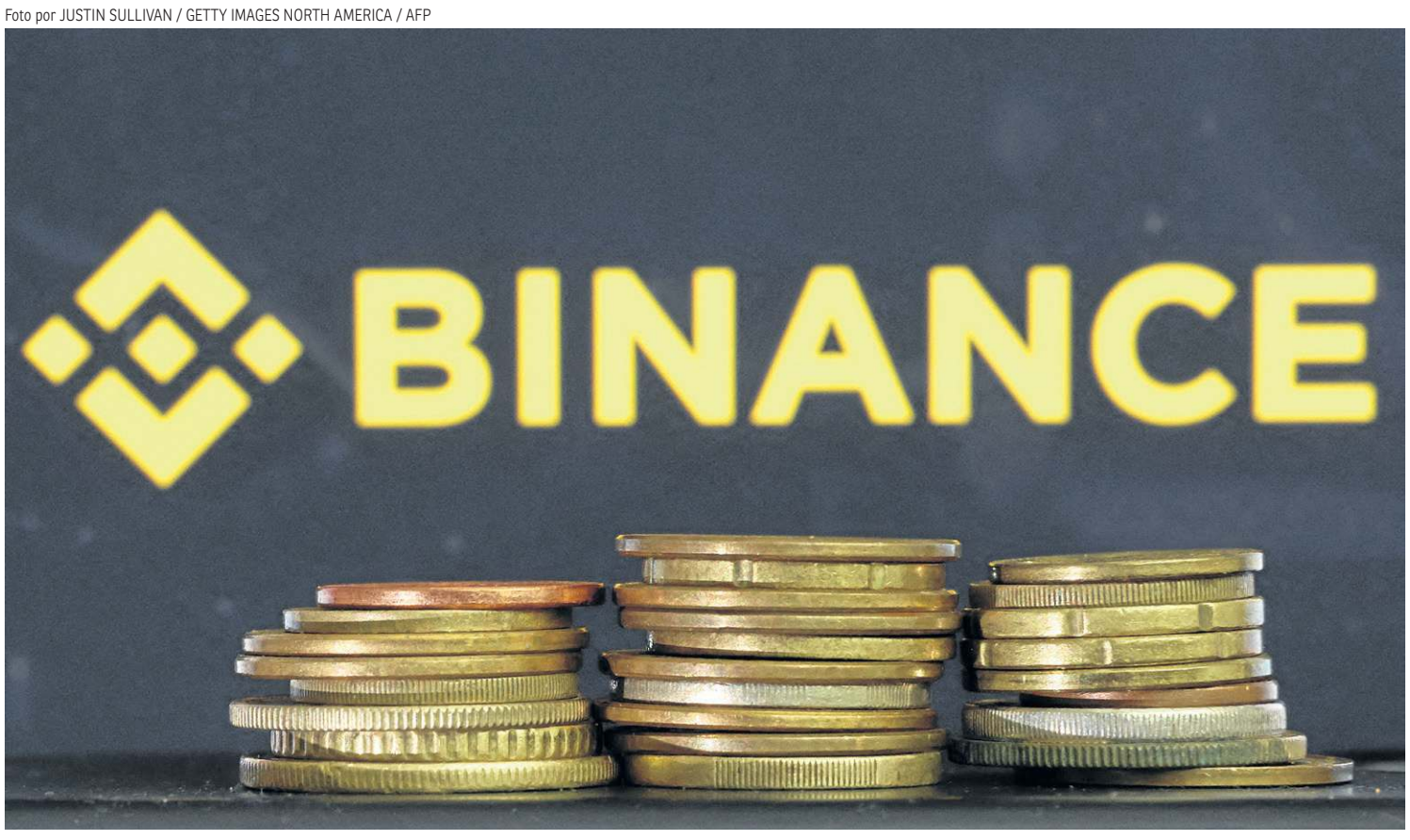
MERCADO FINANCEIRO

Hacker desvia R$ 33 bi em cripto

Ação dos criminosos é considerada o maior roubo da história dos ativos digitais. Invasão teria começado por um laptop

» PEDRO JOSÉ BORGES

Foto por JUSTIN SULLIVAN / GETTY IMAGES NORTH AMERICA / AFP



Após o ataque, a chinesa Binance informou que conseguiu congelar aproximadamente US$ 3 bilhões, o equivalente a cerca de R$ 16,2 bilhões

A corretora de criptomoedas Binance sofreu um ataque hacker que resultou no desvio de US$ 6,3 bilhões (cerca de R$ 33.8 bilhões) em ativos digitais na última quinta-feira. Considerado o maior roubo da história do mercado de criptomoedas, o episódio teve a maior parte das movimentações concentrada em aproximadamente 20 minutos e superou em mais de quatro vezes o recorde anterior, registrado no ataque de US$ 1,5 bilhão à Bybit, em 2025.

As investigações preliminares indicam que a invasão começou com o comprometimento do laptop de um engenheiro da área de DevOps da empresa. A partir do equipamento, os criminosos teriam conseguido acessar um ambiente interno de serviços e autorizar transações de saque. O co CEO da Binance, Richard Teng, afirmou que a operação não foi resultado de uma ação simples nem dependeu exclusivamente das permissões de um funcionário.

Até o momento, não há indicação de que as chaves privadas das carteiras da plataforma tenham sido comprometidas. O episódio aponta para uma mudança na estratégia dos criminosos, que teriam explorado sistemas internos e acessos de pessoas autorizadas a movimentar os recursos, em vez de atacar diretamente as chaves que protegem os ativos.

Para Matheus Puppe, advogado, mestre e doutorando em Direito Digital pela Universidade de Frankfurt e consultor da Comissão Especial de Direito Digital da Câmara dos Deputados, é necessário diferenciar uma falha na infraestrutura operacional de uma vulnerabilidade na própria tecnologia blockchain.

"Precisamos fazer uma distinção importante: até o momento, não há indicação de que a tecnologia blockchain tenha sido comprometida. O que temos é um possível comprometimento da infraestrutura operacional de uma empresa que custodia e movimenta bilhões de dólares em ativos digitais", explica.

O especialista avalia que o caso demonstra como a segurança de grandes instituições financeiras depende não apenas de mecanismos de criptografia, mas também do controle de credenciais, equipamentos e acessos privilegiados. Segundo ele, criminosos podem explorar vulnerabilidades humanas e operacionais sem precisar romper diretamente as tecnologias de proteção dos ativos.

"O maior erro seria acreditar que segurança cibernética se resolve apenas com criptografia avançada ou sistemas tecnologicamente sofisticados. Muitas vezes, os criminosos não precisam quebrar a tecnologia. Basta comprometer as pessoas, as credenciais ou os sistemas que possuem autorização para operá-la", conta.

Puppe também destacou que práticas como engenharia social, phishing e comprometimento de equipamentos representam ameaças para organizações de diferentes portes, inclusive instituições financeiras com estruturas avançadas de segurança.

Empresas de inteligência e análise de blockchain, como Chainalysis, TRM Labs e Check Point, apontaram, com alto grau de confiança, uma possível participação do grupo TraderTraitor, associado ao Lazarus Group e ligado ao governo da Coreia do Norte. A Binance, no entanto, ainda não confirmou oficialmente a autoria do ataque.

Foram identificadas semelhanças entre a operação e outros roubos atribuídos a grupos norte-coreanos, como o ataque à Bybit, em 2025, e à Bitget, em setembro de 2026. Agências ocidentais apontam que operações desse tipo são utilizadas pelo regime norte-coreano para financiar programas nucleares e de desenvolvimento de mísseis.

A Binance informou que trabalha com autoridades internacionais, entre elas o FBI e o Serviço Secreto dos Estados Unidos, para investigar o caso e rastrear os recursos desviados.

Após o ataque, a Binance e empresas parceiras do setor conseguiram localizar e congelar aproximadamente US$ 3 bilhões, o equivalente a cerca de R$ 16,2 bilhões. Entre as companhias que atuaram no bloqueio estão emissoras de stablecoins, criptomoedas cujo valor é vinculado a ativos de referência, como o dólar.

A Tether congelou cerca de US$ 1,57 bilhão, enquanto a Circle bloqueou mais de US$ 800 milhões. A Ripple também informou o congelamento de aproximadamente US$ 200 milhões. A World Liberty Financial, empresa de criptomoedas ligada à família do presidente dos Estados Unidos, Donald Trump, também teria auxiliado nas medidas.

A notícia provocou queda nos principais ativos digitais ontem. O Bitcoin recuou mais de 5% e chegou a US$ 75.5, menor cotação em seis semanas. O Ether também perdeu mais de 5%, negociado a US$ 2.2, enquanto o BNB, token associado à Binance, caiu 6%, para US$ 700.

Fundada na China, em 2017, a Binance é uma das maiores plataformas de negociação de criptomoedas do mundo. A empresa reúne mais de 300 milhões de usuários registrados e mantém sob custódia mais de US$ 160 bilhões em ativos digitais. O ataque amplia a preocupação sobre os riscos de segurança em plataformas que concentram grandes volumes de recursos e dependem de sistemas internos para autorizar movimentações financeiras.

