THREAT BRIEFING · 3 NOVEMBER 2026

The $6 Billion Binance Heist

How crypto exchanges are being robbed: what happened, how it worked, and how to protect yourself



ZNexora Tech Threat Briefing

In this briefing

What happened
Binance and Bitget, five weeks apart

How the attack worked
From one laptop to billions

Remediate and prevent
Steps for crypto businesses

Protect yourself
Six steps for every crypto user

$6.3B

stolen from Binance
on 29 October 2026, the largest crypto theft on record

Figures as of 3 Nov 2026

The largest crypto theft on record

Funds left Binance hot wallets on ten blockchains on the evening of 29 October 2026. The FBI attributes the theft to North Korea; North Korea denies it.

$6.36 B
moved out of Binance wallets

~20 min
for most of the transfers

10
blockchains drained

~$3B
of stolen stablecoins frozen

Sources: TRM Labs; Elliptic; Chainalysis; FBI. Estimates range from $6.3B to $6.43B.

Where the money came from

Blockchain	Reported amount stolen
Ethereum	About $3.8 billion
Bitcoin	18,270 BTC, about $1.5 billion
Tron	About $628 million, mostly USDT
XRP Ledger	About $296 million
Solana	About $96 million

Two exchanges, five weeks



24 Sep

Bitget loses $387.5 million

29 Oct

Binance drained in about 20 minutes

30 Oct

Compromised laptop named as entry point

31 Oct

FBI attributes it to North Korea

1 Nov

Withdrawals resume in phases

Chainalysis saw stolen Binance funds mix on-chain with funds stolen from Bitget.

How the attack worked



Engineer’s laptop

A DevOps laptop is compromised

Internal service

Reaches a service that submits withdrawals

Valid signatures

Hot wallets sign the transfers

EIP-7702 sweep

An Ethereum wallet runs a sweeper

Laundering

Swapped to ETH and moved on

No blockchain was broken and no private key was stolen, according to Binance.

Who is behind it



TraderTraitor (North Korea)

Named by the FBI; also tracked as Lazarus Group, Jade Sleet and APT38



Targets people, not code

Employees and developers are approached with fake jobs and malicious files



A long record

Linked to the $1.5B Bybit theft in 2025 and the Bitget theft in 2026



Denied

North Korea calls the US attribution a provocation

If you run a crypto platform: remediate now



Stop the bleeding

Pause withdrawals; isolate devices

Revoke

Delegations, approvals and credentials

Freeze and trace

Contact issuers and exchanges

Report

Preserve evidence; law enforcement

Communicate

Clear updates; proof of reserves

Speed matters: issuers froze about $3 billion of the Binance stablecoins within hours.

Prevent: seven controls for crypto businesses

- [ ] Staff devices can never reach withdrawal-signing services
- [ ] Independent policy checks on every transaction, including EIP-7702 delegations
- [ ] Multi-party approval for large or unusual withdrawals
- [ ] Hourly limits and automatic circuit breakers on hot wallets
- [ ] Most funds kept in offline cold storage
- [ ] Hardened staff devices and training on fake recruiters
- [ ] Real-time signing alerts and regular incident response exercises

Protect yourself: six steps for crypto users

Passkey or security key

Not SMS codes, for your exchange login

Withdrawal allowlist

Only pre-approved addresses can receive funds

Anti-phishing code

Recognise genuine exchange emails

Keep less on exchanges

Long-term savings in a hardware wallet

Ignore refund offers

Scammers pose as support after hacks

Never sign blindly

Beware delegation and unlimited approvals

Key takeaways

- The weakest point was one laptop and its permissions, not the blockchain.
- Businesses: separate staff devices from signing, and verify every transaction.
- Users: strong logins, less on exchanges, and treat post-hack messages as scams.

Read the full briefing at znexoratech.com