FBI attributes $6.3 billion Binance theft to North Korea's TraderTraitor



The FBI says North Korean group TraderTraitor stole about $6.3 billion from Binance. Attackers reportedly entered through a compromised DevOps engineer's laptop; the FBI published 628 addresses and asked VASPs to block them.

- The FBI attributed the Binance theft, on or about October 29, 2026, to TraderTraitor, also tracked as Lazarus Group, Jade Sleet and APT38.
- Binance linked the breach to a compromised DevOps engineer's laptop that gave access to a service container and allowed unauthorized withdrawals.
- About $6.36 billion was taken across ten blockchains, most of it within 20 minutes.
- The FBI published 628 addresses (608 Ethereum, 19 Bitcoin, one Solana) and asked exchanges and other VASPs to block linked transactions.

> - Binance says it has covered about 95% of the impacted amount and that losses will not be passed to users.

The FBI has formally attributed the theft of roughly $6.3 billion from Binance to TraderTraitor, a North Korean state-sponsored group also tracked as Lazarus Group, Jade Sleet and APT38. The agency dates the theft to on or about October 29, 2026. Blockchain intelligence firms TRM Labs and Chainalysis had already pointed to the same group.

What happened

Binance previously tied the breach to a compromised DevOps engineer's laptop. That foothold gave the attackers access to a service container, from which they submitted unauthorized withdrawal transactions. About $6.36 billion left across ten blockchains, most of it in 20 minutes.

The FBI has seen the stolen assets converted mainly into Ethereum and expects further laundering through DeFi platforms and instant swap services. It, the U.S. Secret Service and IRS Criminal Investigation have asked exchanges, blockchain operators and other virtual asset service providers to block transactions tied to the laundering addresses, and the FBI released a list of 628 of them.

A familiar pattern

The source describes earlier North Korean thefts that also began with employees or developers who had access to crypto infrastructure. Methods included fake recruiters offering jobs under the 'Operation DreamJob' campaign, malicious Python code disguised as a pre-employment test, and a six-month in-person social engineering effort aimed at Drift contributors.

Binance's response

Binance said it was preparing to resume the first phase of withdrawals on November 1, between 06:00 and 09:00 UTC. It reports covering about 95% of the impacted amount, with the rest being less-liquid tokens it is still buying. It states that deposits were unaffected and that it will bear the loss.

For regulated institutions, the lesson is that privileged engineers' endpoints are a primary route to critical systems, and that attackers target people as much as software.

What to do now

1. Harden and monitor endpoints of DevOps and other privileged engineers, including controls on running unvetted code.
2. Restrict what service containers can do, and require additional approval or limits for withdrawal and payment transactions.
3. If you operate in virtual assets, add the FBI-published addresses to screening and blocking lists.

4. Brief developers and finance staff on fake recruiter approaches, unsolicited coding tests and in-person social engineering at events.
5. Review incident response and fraud playbooks for fast detection of rapid, high-value transfers.