Binance ties $6.3 billion crypto theft to a compromised DevOps laptop



Binance says a compromised DevOps engineer's laptop led to unauthorized withdrawals worth about $6.3 billion. Blockchain analysts attribute the attack to North Korea's TraderTraitor; Binance has not named a group.

- Binance linked the theft of about $6.3 billion to a DevOps engineer's compromised laptop and access to a service container.
- The company says the attack was complex, not a single action, and it has found no evidence of a leaked wallet private key so far.
- TRM and Chainalysis attribute the attack to TraderTraitor, also tracked as Lazarus Group and APT38.
- About $2.7 billion has been frozen, while roughly $2.4 billion remains under the attackers' control.

> - Binance suspended deposits and withdrawals, revoked authorizations for the affected address and says it will cover all losses.

Binance has linked the theft of roughly $6.3 billion in cryptocurrency to a compromised laptop belonging to a DevOps engineer. According to the exchange, the access allowed attackers to submit unauthorized withdrawal transactions after reaching a service container. It has not yet found evidence that a wallet private key was leaked.

What Binance has said

Co-CEO Richard Teng stressed that the attacker did not simply reuse one engineer's permissions and that the operation was not a single action but a more complex process. Binance added that it has uncovered further points of breach and is still gathering facts. It has suspended deposits and withdrawals for security checks, revoked authorizations for the affected address, and is working with blockchain intelligence partners and law enforcement. It says it will cover all losses from its SAFU fund and company funds, and will publish an updated Proof of Reserves once remediation is complete.

Attribution and recovery

Binance has not named a threat actor. TRM attributed the attack to TraderTraitor, a North Korean state-backed unit also tracked as Lazarus Group and APT38, and Chainalysis said it confirmed this with a high degree of confidence. TRM reports that about $6.36 billion moved out of wallets on ten blockchains, mostly within about 20 minutes, making it the largest crypto theft on record.

Stablecoin issuers and a network security council have frozen about $2.7 billion. TRM says the attacker sold USDT to market makers and borrowed ETH against USDT, and now holds assets worth about $2.4 billion that no issuer can freeze.

Why it matters

The reported entry point was an engineer's endpoint, not a flaw in the exchange's core platform. Regulated institutions should review how developer and administrator devices connect to production services.

What to do now

1. Review how developer and DevOps laptops reach production containers and services, and restrict that access to what is necessary.
2. Apply endpoint protection, full-disk encryption and device compliance checks to all privileged engineering devices.
3. Require multi-party approval and independent controls for high-value transactions so one compromised endpoint cannot authorize them.

4. Audit container and service credentials, rotate secrets, and monitor for unusual withdrawal or transfer activity.
5. Test incident response and crypto or asset-freeze escalation procedures, including contacts with law enforcement and partners.