GBBC JUST THE FACTS

Published October 30, 2026

GBBC is a non-profit focusing on education, partnerships and standards for the blockchain and digital assets community. GBBC does not lobby.

INDUSTRY WORKING TO RECOVER ASSETS LOST IN BINANCE HACK

On October 29, 2026, Binance was hacked resulting in $6B+ being withdrawn across 10 blockchains. The industry response was immediate, with approximately ~$3B has been frozen on-chain.

The attack started late in the evening in UTC time zones and continued through the night. Binance has indicated that the attack was carried out using **compromised laptop** belonging to a DevOps engineers. **Reporting** from Elliptic indicates that Binance has uncovered additional points of breach. Attackers are said to have gained access to a service container and submitted **unauthorized withdrawal transactions**.

ABOUT THE HACK

The hack was triggered at 20:20 UTC when a new wallet was funded through Tornado Cash (similar to the ByBit hack). The attacker sent one transaction with 50 authorization signatures. One worked and using EIP-7702, control of the 'Binance 14' wallet was handed to a **smart contract**. The contract swept the wallet and **transferred out 167,464 ETH, 1.6B USDT and 60+ tokens**. Other Binance wallets were attacked with loses mounting to **$6.3B**. The attackers subsequently:

- Used UniswapX and intent-based contracts (where users describes a desired outcome and constrains and the contract executes) to sell USDT to professional fillers and market makers.
- Borrowing techniques as a second attacker wallet supplied 60 million USDT on Aave V3 Ethereum Core as collateral and **borrowed 19,762 WETH** (USD$44.6m) against it, moving funds out at a 10% loss. Aave subsequently froze the affected markets.



*Source: **Elliptic***

Blockchain intelligence firms **reported** that the following methods were also used to move value:

- JustLend lending protocol received **300M USDT** from a wallet on TRON
- A chain of hop wallets (intermediate wallets) move a further **200M USDT**
- Decentralized exchanges were used to sell **48M RLUSD** from a wallet which had passed through two hops
- A peel chain was used to split **18,270 BTC** from an attacker address into round **1,000 BTC** and **100 BTC** pieces inside the same block

Additionally, **Chainalysis** identified:

- Commingling of funds with funds stolen in the Bitget exploit
- Use of automation allowing for thousands of transactions in a short period to hide the flow of funds indicative of a programmatic process with wallet addresses receiving 1 TRX, followed by additional funds which are then forwarded to other addresses

GBBC JUST THE FACTS

Published October 30, 2026

GBBC is a non-profit focusing on education, partnerships and standards for the blockchain and digital assets community. GBBC does not lobby.

LINKS TO NORTH KOREA

Blockchain intelligence firms have warned that **North Korea** is likely behind the attack, with one firm identifying **TraderTraitor** (linked to the **Lazarus Group**) as the group responsible. TraderTraitor was previously linked to the USD$1.5B ByBit hack in February 2025.

TraderTraitor has previously been the subject of a **cybersecurity advisory**, which highlighted that the group engaged in activities targeting individuals often working in IT operations or administration of software development through social engineering / spearfishing attacks.

The "term TraderTraitor describes a series of malicious applications written using cross-platform JavaScript code with the Node.js runtime environment using the Electron framework."

The attack came one day after the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) **sanctioned** 10 individuals and one entity for their roles in Democratic People's Republic of Korea (DPRK) government-run information technology (IT) worker schemes. This has not been officially confirmed by government officials.

BINANCE RESPONSE

Binance has indicated it "will cover all losses from the SAFU fund and the company's funds" and that they will "publish an updated Proof of Reserves once the remediation is complete." Binance has also **announced** the following measures:

- Temporary suspension of deposits and withdrawals while security checks are completed
- Revoking the affected address authorisation
- **Rebuilding** and testing the withdrawal service by Sunday
- Full security review across the entire company
- Share proof of reserves by Monday
- Engaging law enforcement and blockchain intelligence partners and issuers to trace and recover funds

INDUSTRY RESPONSE

The industry responded withing minutes, with stablecoin issuers, blockchain infrastructure and blockchain intelligence firms working to trace and **freeze** assets in collaboration with law enforcement authorities.

- Tether and Circle froze USDT (USD$1.77bn) and USDC (USD$825M) in their main receiver wallets shortly after the initial attack. Later attacks either landed in the frozen wallets or were also frozen in coordination with law enforcement.
- Ripple froze the wallet holding stolen RLUSD ((USD$40.5m).
- World Liberty Financial froze USD in the main receiving wallet (USD$27.8m).
- Arbitrum Security Council forced transfers out of the attackers Arbitrum ETH ($74.6m) wallet to prevent access. This occurred within 4 hours of the initial attack.

Blockchain intelligence firms have been sharing intelligence publicly, and likely with law enforcement partners. Further public-private coordination is needed.

It has been **reported** that the UK's Financial Conduct Authority has contact Binance to understand the wider implications of the hack and in the U.S., the FBI and the U.S. Secret Service are working with Binance to recovered stolen assets.

Centralized exchanges, decentralized exchanges, OTCs, banks, foreign exchange houses, FinTechs and payment service providers should continue to monitor the situation in the coming months as $3.3bn remains at large and will likely be cleaned through the international financial system.