



By: The Editorial Board

Binance suspects the biggest cryptocurrency theft began on an engineer's computer



On 29 October, assets worth approximately \$6.3 billion were transferred from **Binance** digital wallets in the largest cryptocurrency theft ever recorded. The exchange stated that the probable origin of the attack was a compromised computer belonging to one of its engineers.

TRM Labs, which tracks the movement of stolen funds, attributed the operation to the North Korean group TraderTraitor with a high degree of confidence. The **identity of the perpetrators** has not yet been confirmed by state investigative bodies.

The day before the attack, the US Treasury Department imposed sanctions on a new group of individuals and a company that enable North Korean developers to work for foreign firms under false identities and transfer their earnings through Russia.

Investigations have not yet linked the two operations, but a series of earlier attacks shows how the authorisations of employees and their suppliers can translate into access to financial systems worth billions of dollars, while regular payments to undercover workers represent another source of funding for North Korean state organisations.

For exchanges that hold billions of dollars in other people's assets, indemnifying users cannot be the limit of their responsibility. Previous attacks highlight the need for tighter, independently audited controls over the people and programmes that authorise transactions.

Four attacks, access already granted

In May 2024, \$308 million was stolen from the Japanese exchange DMM. According to a **joint investigation** by the FBI and Japanese police, the attacker posed as a recruiter on LinkedIn and sent a malicious recruitment task to a Gincio developer.

When the employee ran the code, the

attackers obtained his login credentials and likely altered the legitimate money transfer account details.

The following February, about \$1.5 billion disappeared from the Bybit exchange. The **FBI** attributed responsibility to the same TraderTraitor group. An investigation by the provider Safe{Wallet} determined that the attackers had previously compromised its developer's computer and then modified the website used by Bybit employees to approve transactions.

Bybit staff saw what appeared to be a regular transaction and approved an action that allowed the attackers to take over the wallet.

In April this year, about \$292 million was stolen from the KelpDAO system, which facilitates the transfer of digital assets between networks.

According to **LayerZero's report**, which KelpDAO disputes in the section addressing responsibility for system tuning, attackers associated with TraderTraitor gained access through a LayerZero developer and then altered the data used to approve transfers between networks.

Multiple signatures and additional checks do not protect assets when they all rely on the same compromised data source

LayerZero claims that the vulnerability arose from KelpDAO's decision to rely on a single verifier, while KelpDAO counters that this was the default setting offered by the supplier. In both accounts, one compromised check was enough to lose the assets.

Binance currently suspects that the attackers gained access via an engineer's official laptop. The exchange states that there is no evidence that the digital codes, without which money cannot be withdrawn from its accounts, were stolen.

Analysts at the US company TRM Labs

determined that the attack was prepared at least a day and a half earlier. According to their findings, Binance's system itself approved 50 accounts that the attackers had set up in advance.

One of these accounts effectively handed control over to the attackers, so they also took the money that arrived in that account after the initial emptying.

Funds were simultaneously leaving 10 different networks, with regular approvals from the exchange, so TRM Labs suspects that the attackers took control of the internal system through which Binance approves payments.

The fact that the secret keys were not stolen says little about whether the money was protected. In the case of KelpDAO, according to LayerZero's report, the keys remained intact and a legitimate system signed a certificate based on falsified data.

Multiple signatures and additional checks do not protect assets when they all rely on the same compromised data source.

The first three cases were established by investigations, and Binance's case now appears to follow the same pattern according to preliminary findings: money disappears when a system without independent verification does what a single broadly authorised access point instructs it to do.

Time needed to freeze funds

After the Binance attack, there was a race between the perpetrators moving the assets and the companies able to block certain digital currencies.

According to TRM's data from the early morning of 30 October, Tether, the issuer of the dollar-pegged digital currency USDT, had frozen about \$1.77 billion, and Circle, the issuer of USDC, had frozen about \$825 million.

Other issuers and managers of certain networks blocked additional amounts, so TRM

estimated the total frozen at about \$2.7 billion.

Binance, in a later statement, put the figure at approximately \$3 billion.

Issuers of USDT and USDC can block transfers of funds from tagged addresses, whereas Bitcoin and Ether have no central issuer capable of imposing such a ban.

Binance has promised compensation from the SAFU fund, worth around \$1 billion, and from company funds

At the time of its assessment, TRM was tracking more than 420,000 units of Ether and 18,270 bitcoins, with a total value of about \$2.4 billion.

Those assets can be tracked and potentially seized when they reach intermediaries that cooperate with the authorities, but their movement cannot simply be stopped by a single company's decision.

According to TRM, the attackers sold approximately \$325 million in USDT for Ether at a price more than 10% below market solely to move the funds before they were frozen.

The stolen assets amounted to just over 4% of the roughly \$144 billion that Binance held for users before the attack, but that figure does not show how much of the exchange's own funds it had to use to cover the loss.

Binance has promised compensation from the SAFU fund, worth around \$1 billion, and from company funds. The final loss will also depend on how many frozen assets are recovered.

Revenues flowing to the military industry

An eleven-nation multilateral **sanctions monitoring team** found that North Korean hackers stole at least \$2.84 billion in cryptocurrency between early 2024 and

September 2025.

The value of Bitcoin and Ether that TRM tracked to the perpetrators in the immediate aftermath of the latest attack approached the amount stolen over the preceding 21-month period.

In 2023, US Deputy National Security Adviser Anne Neuberger estimated that approximately half of North Korea's missile programme was financed through cyber attacks and cryptocurrency theft.

In a 2025 report, the multilateral team estimated that cryptocurrency thefts in 2024 accounted for about a third of North Korea's foreign exchange earnings, valuing the assets at the time of theft.

North Korea also earns money through programmers, employed by foreign companies under false identities, who work from home. This income is smaller than the proceeds from theft but arrives regularly, every month.

The company believes it has an employee in the US but is in fact paying a salary to someone working for Pyongyang

On 13 October, the FBI warned that North Korean networks were paying intermediaries in the US for this work. When a company sends a laptop to a new employee's home address, the intermediary takes it, turns it on at home and allows the North Korean programmer to work on it remotely.

Intermediaries sometimes attend job interviews themselves instead of the actual candidate. The company thus believes it has an employee in the US but is in fact paying a salary to someone working for Pyongyang.

The internal workings of such a scheme are illustrated by the case of John Allen Kerl, an employee of a US military contractor who was granted access to top-secret information. On 28 October, he pleaded guilty in court to employment fraud.

According to court documents, he allowed foreigners to apply for remote jobs under his and other people's names, kept at home the laptops that companies sent to new employees, and used them to enable work from abroad.

In this way, nine job offers were obtained. Kerl's defence claims that he did not know that North Korea might be behind the scheme, but he admitted participating in the fraud.

Russia after the shutdown of the UN Panel of Experts

Money earned by North Korean developers is often transferred in cryptocurrencies, as these are harder to track. For it to be spent, someone must exchange it for dollars, roubles or other currencies. American sanctions announced on 28 October indicate that this work is carried out in part by people in Russia.

According to the **US Treasury Department**, since 2024 a Russian national has exchanged about \$3.5 million worth of cryptocurrencies for a North Korean company that employs such developers. Another has carried out similar work worth more than \$3 million for North Korean officials since early 2025.



Russia used its veto in the UN Security Council to block the extension of the mandate of the Panel of Experts, a group of independent specialists that had been investigating how Pyongyang circumvents sanctions

The sanctions also reveal that **North Korea** has its own base in Russia for such programmers. An organisation controlled by Pyongyang

operates in Vladivostok, where six developers have earned more than \$750,000 since the start of 2025. North Koreans who lead teams of these workers in Russia have also been sanctioned.

All this is happening in a country that, in 2024, shut down the main international monitoring of sanctions against North Korea.

Russia then used its veto in the UN Security Council to block the extension of the mandate of the Panel of Experts, a group of independent specialists that for years had been investigating how Pyongyang circumvents sanctions and reporting to the United Nations.

The sanctions remained in place, but without a body to detect violations. Eleven countries, including the US, Japan and South Korea, subsequently set up their own monitoring team, but its reports do not carry the weight of UN documents.

While North Korean organisations can open a new centre in Russia to replace each one that closes, sanctions on individual intermediaries will have only a limited effect.

Large exchanges must be held accountable as financial institutions

A trading platform that holds tens of billions of dollars of other people's assets should not be able to rely on a promise that it will have enough money to pay for the next attack.

Large cryptocurrency platforms should be subject to mandatory independent audits of payment approval systems, clear separation of powers, specific controls over supplier access and direct management accountability for identified failures.

The rigour of such **supervision** must be commensurate with the scale of the assets they safeguard, as with other key financial institutions.

Some of these obligations already exist in the European Union. From January 2025, the Digital Operational Resilience Act (DORA) will require authorised cryptoasset service providers to manage technological risk, report incidents and monitor suppliers, while the Markets in Crypto-Assets (MiCA) regulation will make cryptoasset custodians liable to clients for losses caused by incidents attributable to them.

It is not clear which of these obligations applied to the affected Binance business, who supervised their fulfilment or how, and that is exactly what the regulators and the exchange owe the public after such a loss.

Determining the origin of the attack and closing individual accounts will not be enough

At the same time, countries need to cut off intermediary networks in Russia and identify new channels before profits reach end users.

Determining the origin of the attack and closing individual accounts will not be enough if companies can continue to approve transactions and work with intermediaries in the same way, running the same business under different names.

Following DMM, Bybit and KelpDAO, more should be demanded of Binance than compensation and a statement that the vulnerability has been fixed.

The exchange must publish its findings on which powers were abused and which controls were absent or failed, and an independent audit must confirm that these failings have been eliminated.

If oversight continues to rely on exchanges' own statements, the next group of attackers will again look for the person or supplier whose authority opens the way to money, and users will still bear the risk, regardless of whether the largest exchange subsequently indemnifies them.