North Korean hackers linked to $1.5 billion ByBit crypto heist

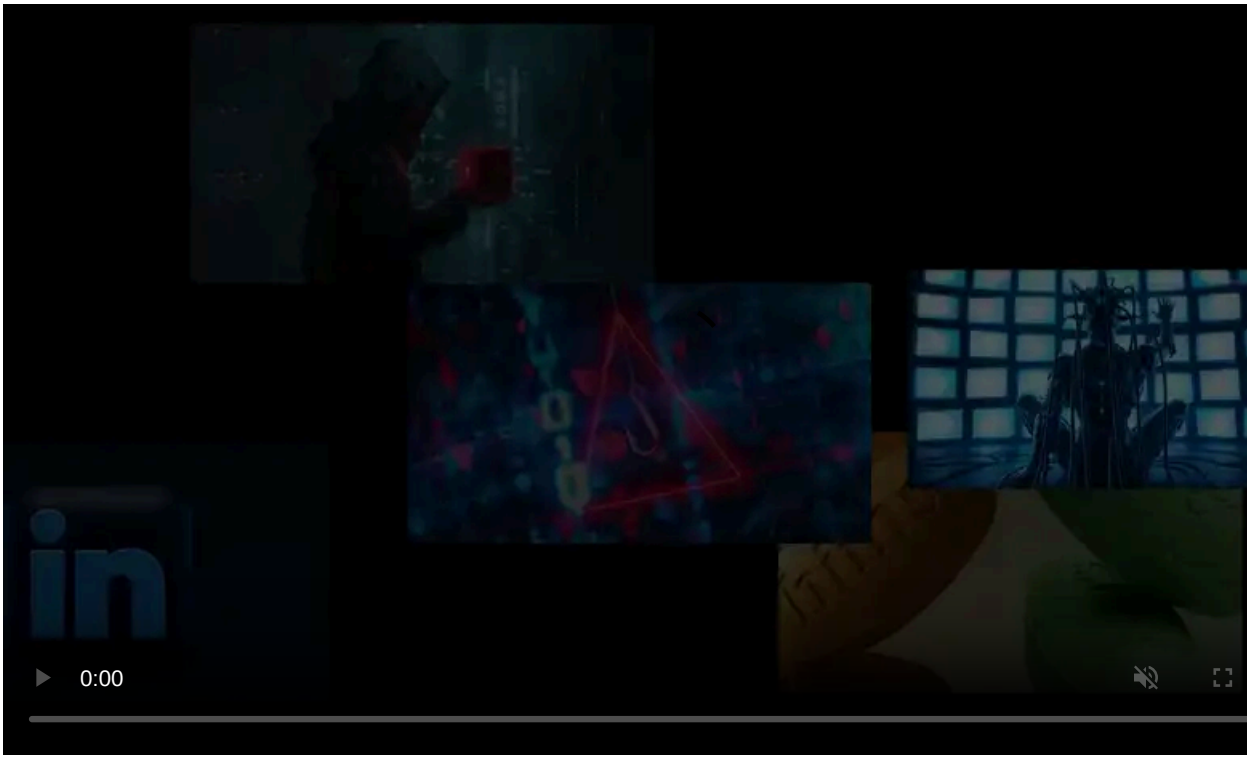
By Sergiu Gatlan

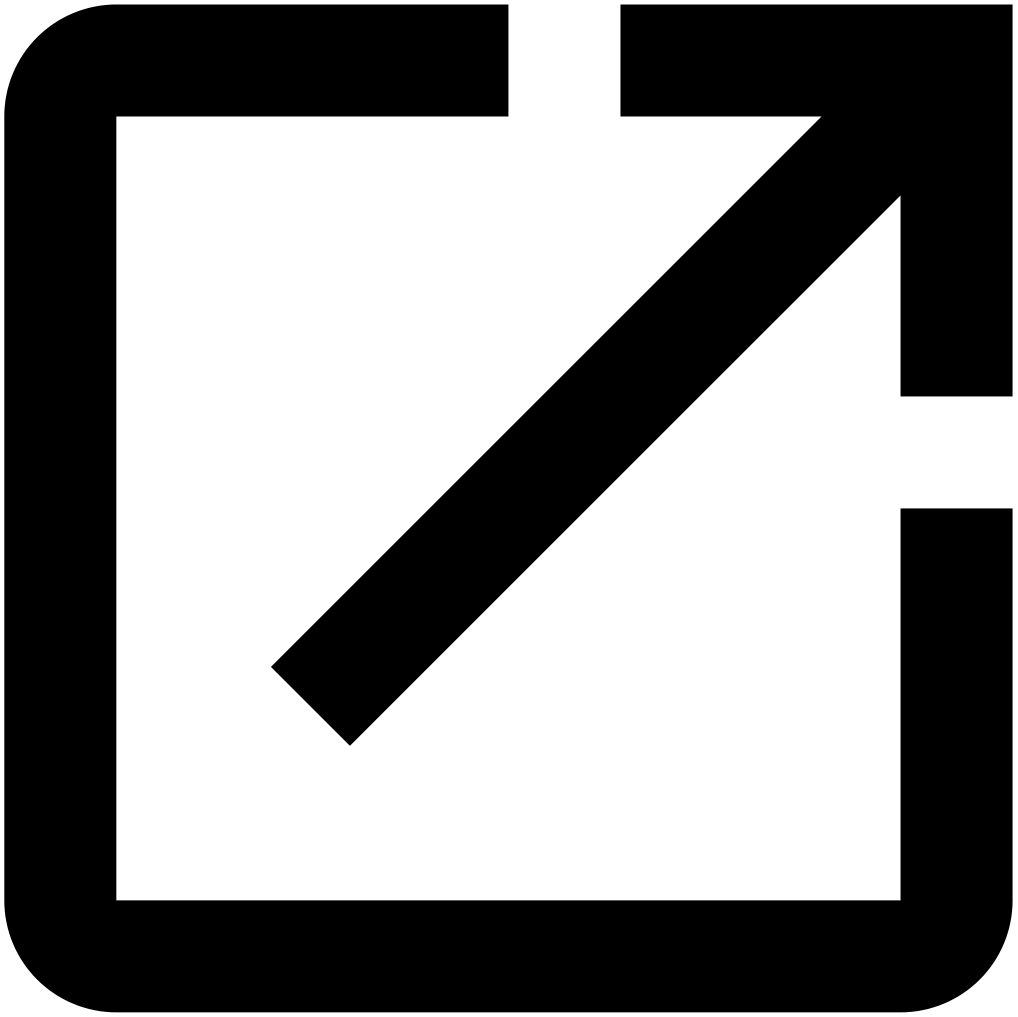
Published: 2025-02-24 · Archived: 2026-04-05 16:49:56 UTC

Over the weekend, blockchain security companies and experts have linked North Korea's Lazarus hacking group to the theft of over $1.5 billion from cryptocurrency exchange Bybit.

In what is now considered the largest crypto heist in history, the attackers intercepted a planned transfer of funds from one of Bybit's cold wallets into a hot wallet, redirecting the crypto assets to a blockchain address under their control.

"On February 21, 2025, at approximately 12:30 PM UTC , Bybit detected unauthorized activity within one of our Ethereum (ETH) Cold Wallets during a routine transfer process. The transfer was part of a scheduled move of ETH from our ETH Multisig Cold Wallet to our Hot Wallet," Bybit explained in a post-mortem published on Friday.


0:00



"Unfortunately, the transaction was manipulated by a sophisticated attack that altered the smart contract logic and masked the signing interface, enabling the attacker to gain control of the ETH Cold Wallet. As a result, over 400,000 ETH and stETH worth more than $1.5 billion were transferred to an unidentified address."

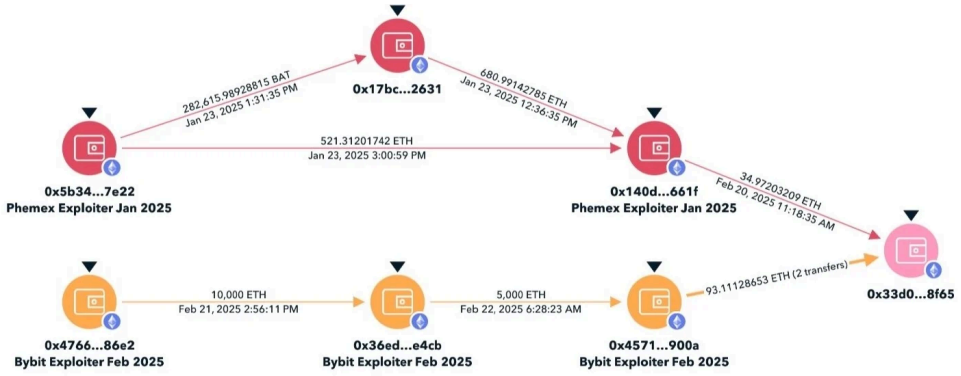
While this led to the theft of over $1.5 billion worth of ETH and stETH, Bybit said its services were largely unaffected despite a massive wave of 580,000 withdrawal requests after the incident was disclosed. It also added that all other cold wallets and assets remained secure.

The crypto exchange has since restored its ETH reserves, and the company's CEO says that Bybit is solvent even if the lost assets will not be fully recovered.

Bybit crypto-heist linked to Lazarus hackers

Since the attack, crypto fraud investigator ZachXBT has discovered links between the Bybit hackers and the infamous North Korean Lazarus threat group after the attackers sent stolen Bybit funds to an Ethereum address previously used in the Phemex, BingX, and Poloniex hacks.

"Today when laundering funds for the Bybit Hack the Poloniex hack was also linked on-chain in consolidation address 0x15ec," ZachXBT said. "This now shows the same entity is tied to four different hacks (Bybit, Poloniex, Phemex, BingX)."



Phemex/Bybit overlap (ZachXBT)

The researcher also said the threat actors launched and traded Pump Fun meme coins to launder the stolen cryptocurrency, with funds from the Bybit hack reaching more than 920 blockchain addresses. ZachXBT also claimed the Lazarus hackers are laundering ETH stolen from Bybit Hack using eXch (a centralized mixer) and bridging funds to Bitcoin via Chainflip.

"The eXch team accidentally sent 34 ETH ($96K) to the hot wallet of another exchange after laundering $35M+ for Lazarus Group from the Bybit hack today," they said.

ZachXBT's findings were confirmed by blockchain intelligence company TRM Labs, which determined with "high confidence" that the North Korean hackers were behind the Bybit hack "based on substantial overlaps observed between addresses controlled by the Bybit hackers and those linked to prior North Korean thefts."

Blockchain analysis company Elliptic said the Lazarus hackers have already moved the stolen funds through large numbers of cryptocurrency wallets to conceal the assets' actual origin and slow down tracing attempts.

"One exchange in particular, eXch appears to have knowingly laundered tens of millions of dollars worth of the stolen assets, despite calls from Bybit to halt this," Elliptic co-founder and chief scientist Tom Robinson told BleepingComputer. "The stolen assets are mostly being converted to Bitcoin - if previous laundering patterns are followed, we may expect to see the use of bitcoin mixers next - to attempt to hide the money trail."

However, eXch has denied laundering funds stolen from Bybit, saying that "eXch is NOT laundering money for Lazarus/DPRK" and that "the insignificant portion of funds from the ByBit hack eventually entered our address [..] was an isolated case and the only part processed by our exchange, fees from which we will be donated for the public good."

In December, blockchain analysis company Chainalysis said North Korean hackers stole $1.34 billion in 47 crypto heists in 2024, breaking their previous record of $1.1 billion from 2022.

In a single attack in March 2022, two North Korean hacking groups (Lazarus and BlueNorOff) stole $620 million in cryptocurrency (173,600 Ethereum and 25.5M USDC tokens) from Axie Infinity's Ronin network bridge.

"North Korea-linked actors have stolen over $6 billion in cryptoassets since 2017, with the proceeds reportedly spent on the country's ballistic missile program," Elliptic said today.
