North Koreans finish initial laundering stage after more than $1 billion stolen from Bybit

By Jonathan Greig

Published: 2025-03-04 · Archived: 2026-04-05 12:49:35 UTC

The suspected North Korean hackers behind the theft of more than $1 billion from crypto platform Bybit have completed the initial stage of laundering the funds.

Experts from multiple blockchain security companies said Monday that the hackers were able to move all of the stolen ETH coins to new addresses — the first step taken before the funds can be laundered further.

Ari Redbord, a senior official at TRM Labs, told Recorded Future News that the laundering process relied heavily on decentralized finance (DeFi) tools that helped obscure the origins of the stolen assets.

“This rapid and methodical operation indicates an unprecedented level of operational efficiency, posing serious challenges for investigators,” Redbord said.

Last week, the FBI attributed the attack on Bybit to a well-known North Korean group known as TraderTraitor or Lazarus, and urged the cryptocurrency community to help contain the $1.4 billion in cryptocurrency stolen from the exchange.

“TraderTraitor actors are proceeding rapidly and have converted some of the stolen assets to Bitcoin and other virtual assets dispersed across thousands of addresses on multiple blockchains,” the FBI alert said. “It is expected these assets will be further laundered and eventually converted to fiat currency.”

At the time of the FBI advisory, TRM Labs said about $400 million had been laundered.

‘Scale and velocity’

Experts at another blockchain security firm, Elliptic, said the North Korean group was forced to pause the laundering process on Friday because the service they were using, eXch, couldn’t handle the volume of transactions. eXch does not use a “Know Your Customer” (KYC) protocol, meaning no proof of identity is required.

The laundering resumed on Saturday and allegedly accelerated.

“This rapid laundering suggests that North Korea has either expanded its money laundering infrastructure or that underground financial networks, particularly in China, have enhanced their capacity to absorb and process illicit funds,” Redbord said.

“The scale and velocity of this operation present new challenges for investigators, as traditional anti-money laundering mechanisms struggle to keep pace with the high volume of illicit transactions.”

TRM Labs has tracked previous thefts by North Korean actors and found a similar playbook, where the hackers use DeFi platforms to convert funds into Bitcoin before using mixers to obfuscate the source of the cryptocurrency.

Nick Carlsen, TRM Labs' North Korean expert and a former FBI official, said the Bybit attack "indicates that the regime is intensifying its 'flood the zone' technique — overwhelming compliance teams, blockchain analysts, and law enforcement agencies with rapid, high-frequency transactions across multiple platforms, thereby complicating tracking efforts."

The Dubai-based Bybit has launched a recovery bounty program and offered 10% of the recovered funds to anyone who helps in tracing and freezing the stolen cryptocurrency.

As of Thursday, 12 "hunters" had been awarded about $4.2 million so far and CEO Ben Zhou released a preliminary report on the incident from incident response company Sygnia and financial security firm Verichains.

TRM Labs said about 77% of the funds are still traceable and they are working alongside other blockchain security funds to help stop the money from being laundered further. The FBI in its advisory urged DeFi services and other entities to block transactions with or derived from addresses used by TraderTraitor actors.

The Bybit attack is the largest crypto hack of all time, far surpassing previous headline-grabbing thefts of more than $600 million from DeFi platforms like Ronin Network and Poly Network.

North Korea's Lazarus Group has stolen billions worth of cryptocurrency over the last 9 years, with blockchain monitoring firm Chainalysis saying hacking groups connected to North Korea's government stole $1.34 billion worth of cryptocurrency across 47 incidents in 2024.

Correction: A previous version of this article misspelled the company name Sygnia.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
