North Korea accused of orchestrating $100 million Harmony crypto hack

By Jonathan Greig

Published: 2023-01-12 · Archived: 2026-04-05 16:32:20 UTC

Hackers connected to a prolific North Korea military-backed group have been accused of orchestrating the recent $100 million hack of blockchain company Harmony.

Researchers with blockchain analysis company Elliptic said the incident — and the way the money was being laundered — resembled the way North Korea's Lazarus Group operates. The researchers said they do not yet have concrete evidence linking the North Korean military to the hack.

On June 24, $100 million worth of Ether, Tether (USDT), Wrapped Bitcoin (WBTC) and BNB was stolen from Harmony, a platform that helps people send cryptocurrency, stablecoins and NFTs between different blockchains like Ethereum and Binance Smart Chain. The stolen funds were converted into 85,837 ETH through decentralized exchange Uniswap.

Since the incident, the hackers have laundered about $39 million worth of cryptocurrency through Tornado Cash – a cryptocurrency mixing service that is typically used by cybercriminals.

> 1/ We are aware the hacker has begun to move funds through Tornado Cash. The team is working with two highly reputable blockchain tracing and analysis partners, and collaborating with the FBI as part of an investigation into this criminal act.
>
> — Harmony (@harmonyprotocol) June 28, 2022

Elliptic researchers said they believe North Korea is behind the hack because of their consistent interest in attacking DeFi services such as cross-chain bridges like Harmony. A cross-chain bridge – also known as a blockchain bridge – allows people to transfer tokens, assets, smart contract instructions and data between blockchains.

They have become a ripe target for hackers in recent months and exploits in bridges have led to millions of dollars in losses.

“The theft was perpetrated by compromising the cryptographic keys of a multi-signature wallet – likely through a social engineering attack on Harmony team members. Such techniques have frequently been used by the Lazarus Group,” Elliptic explained in a blog.

“Lazarus Group tends to focus on APAC-based targets, perhaps for language reasons. Although Harmony is based in the US, many of the core team have links to the APAC region.”

Elliptic added that the regularity of the deposits into Tornado over extended periods of time suggests that an automated process is being used. Their researchers have seen a similar laundering process with the cryptocurrency stolen from Ronin Network, which was attributed to Lazarus.

The researchers also noted that the short periods during which the stolen funds stop being moved out of Tornado cash are consistent with nighttime hours in the Asia-Pacific region.

> #PeckShieldAlert ~18k $ETH (~22m) into 0x1e...6430 from @harmonyprotocol exploiters pic.twitter.com/NN4j5Korsz
>
> — PeckShieldAlert (@PeckShieldAlert) June 27, 2022

Harmony initially said it was working with the FBI on addressing the hack and has offered the hackers a $10 million bug bounty in exchange for a return of the stolen funds. It does not appear that offer has been accepted based on the laundering patterns connected to the stolen cryptocurrency.

Blockchain bridge attacks have become increasingly common over the last year. In addition to the Ronin hack in March, a hacker abused a vulnerability in the Wormhole cryptocurrency platform in February to steal an estimated $322 million worth of Ether currency.

A week before the Wormhole hack, a similar attack took place against another blockchain bridge when a hacker stole $80 million from Qubit Finance.

The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Treasury, and the FBI issued a joint advisory in April describing a North Korean state-sponsored hacking campaign that has been associated with cryptocurrency heists since at least 2020.

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.
