Evidence points to North Korea in CoinEx cryptocurrency hack, analysts say

By Joe Warminsky

Published: 2023-09-15 · Archived: 2026-04-05 22:29:44 UTC

Experts at the cryptocurrency-tracking company Elliptic say North Korean hackers are the prime suspects in the theft of $31 million in cryptocurrency from the CoinEx exchange reported earlier this week.

The analysts compared transactions intended to hide funds taken in the CoinEx heist with the aftermath of attacks on online casino Stake.com and cryptocurrency wallet service Atomic Wallet. Both of those were linked to Lazarus Group, a North Korean government operation that U.S. authorities have accused of helping fund the country's illicit weapons programs.

"Elliptic analysis confirms that some of the funds stolen from CoinEx were sent to an address which was used by the Lazarus group to launder funds stolen from Stake.com, albeit on a different blockchain," the company said Friday.

The CoinEx funds traveled through the Ethereum blockchain and then were "sent back to an address known to be controlled by the CoinEx hacker," Elliptic said.

"Elliptic has observed this mixing of funds from separate hacks before from Lazarus, most recently when funds stolen from Stake.com overlapped with funds stolen from Atomic Wallet," the analysts said.

"In light of this blockchain activity, and in the absence of information suggesting the CoinEx hack was conducted by any other threat group, Elliptic agrees that Lazarus Group should be suspected for the theft of funds from CoinEx," the company said.

The CoinEx hack would represent just a fraction of the cryptocurrency thefts recently attributed to North Korea. Researchers at cryptocurrency-tracking company Chainalysis said Thursday that the value of stolen cryptocurrency associated with the country "currently exceeds $340.4 million this year," and was $1.65 billion in 2022.

The challenge for cybercriminals, as always, is to find ways to obfuscate their actions, given that blockchain transactions are publicly trackable. The report from Chainalysis emphasized that North Korean groups "are increasing their use of Russia-based exchanges known to launder illicit crypto assets."

Chainalysis specifically pointed to a different web of transactions related to an attack on Harmony, a company that provides a platform for trading different kinds of digital assets. Funds taken in that case traveled through an unspecified Russian exchange. Evidence shows that North Korean groups have used that pathway for money laundering since 2021, Chainalysis said.

Lazarus also appears to be focusing its attention on certain targets lately, too, Elliptic said. Including the CoinEx theft, in the past few months four of the five thefts attributed to Lazarus have been “centralized” cryptocurrency platforms, meaning they’re controlled by a single entity. Decentralized finance (DeFi) services, by contrast, distribute authority among different nodes.

Elliptic said there could be several reasons for the shift: DeFi services likely have improved security in recent years, “thus reducing the scope for hackers to identify and exploit vulnerabilities.” Centralized exchanges, meanwhile, are more susceptible to social-engineering attacks — a favorite tactic of Lazarus — because they have bigger workforces and centralized IT services.

No previous article

No new articles

Joe Warminsky

is the news editor for Recorded Future News. He has three decades of experience as an editor and writer in the Washington, D.C., area. He previously he helped lead CyberScoop for more than five years. Prior to that, he was a digital editor at WAMU 88.5, the NPR affiliate in Washington, and he spent more than a decade editing coverage of Congress for CQ Roll Call.
