North Korea's Lazarus Group Launders $900 Million in Cryptocurrency

By The Hacker News

Published: 2023-10-06 · Archived: 2026-04-06 00:55:13 UTC

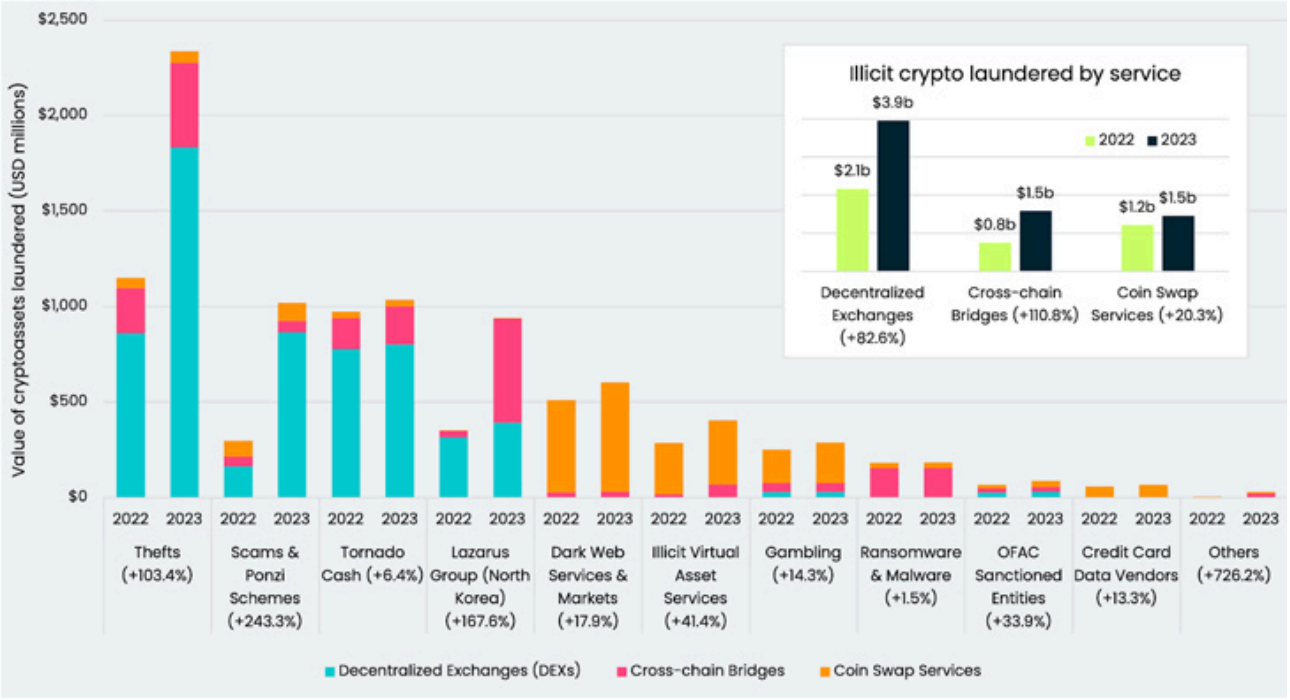
As much as $7 billion in cryptocurrency has been illicitly laundered through cross-chain crime, with the North Korea-linked Lazarus Group linked to the theft of roughly $900 million of those proceeds between July 2022 and July of this year.

"As traditional entities such as mixers continue to be subject to seizures and sanctions scrutiny, the crypto crime displacement to chain- or asset-hopping typologies is also on the rise," blockchain analytics firm Elliptic said in a new report published this week.

Cross-chain crime refers to the conversion of crypto assets from one token or blockchain to another, often in rapid succession, in an attempt to obfuscate their origin, making it a lucrative method for money laundering for crypto thefts and an alternative to traditional approaches like mixers.

According to data gathered by Elliptic, the Lazarus Group's use of cross-chain bridges contributed to a majority of the 111% increase in the proportion of funds sent via such services.

The North Korean hacking crew is estimated to have stolen nearly $240 million in cryptocurrency since June 2023, following a series of attacks targeting Atomic Wallet ($100 million), CoinsPaid ($37.3 million), Alphapo ($60 million), Stake.com ($41 million), and CoinEx ($31 million).



"The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that it performs all three pillars of cybercriminal activities: cyber espionage, cyber sabotage, and pursuit of financial gain," ESET said of the threat actor late last month.

The threat actor has also been linked to the use of Avalanche Bridge to deposit more than 9,500 bitcoin, while simultaneously employing cross-chain solutions to move some of the plundered assets.

"As is evidenced by the assets ending up on the same blockchain on numerous occasions, these transactions have no legitimate business purpose other than to obfuscate their origin," Elliptic said. "Bridging back-and-forth for the sake of obfuscation – i.e. 'chain-hopping' – is now a recognized money laundering typology."

The disclosure comes as South Korea's National Intelligence Service (NIS) has warned of North Korea attacking its shipbuilding sector since the start of the year.

"The hacking methods mainly used by North Korean hacking organizations were to occupy and bypass the PCs of IT maintenance companies, and to install malicious code after distributing phishing emails to internal employees," the agency said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
