How the Lazarus Group is stepping up crypto hacks and changing its tactics

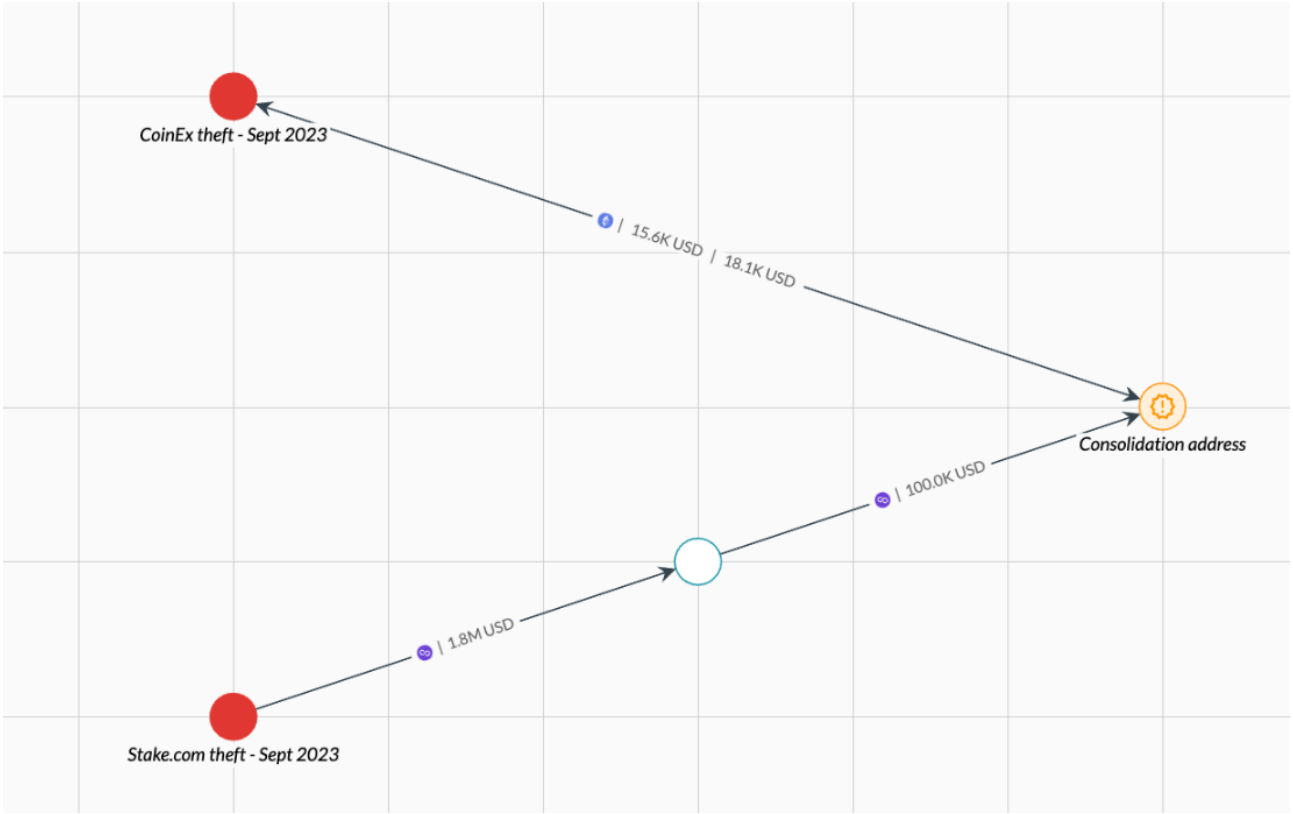
By Elliptic Research

Archived: 2026-04-06 02:58:27 UTC

The Lazarus Group – North Korea's elite hacking organization – appears to have recently ramped up its operations, conducting a confirmed four attacks against crypto entities since June 3rd.

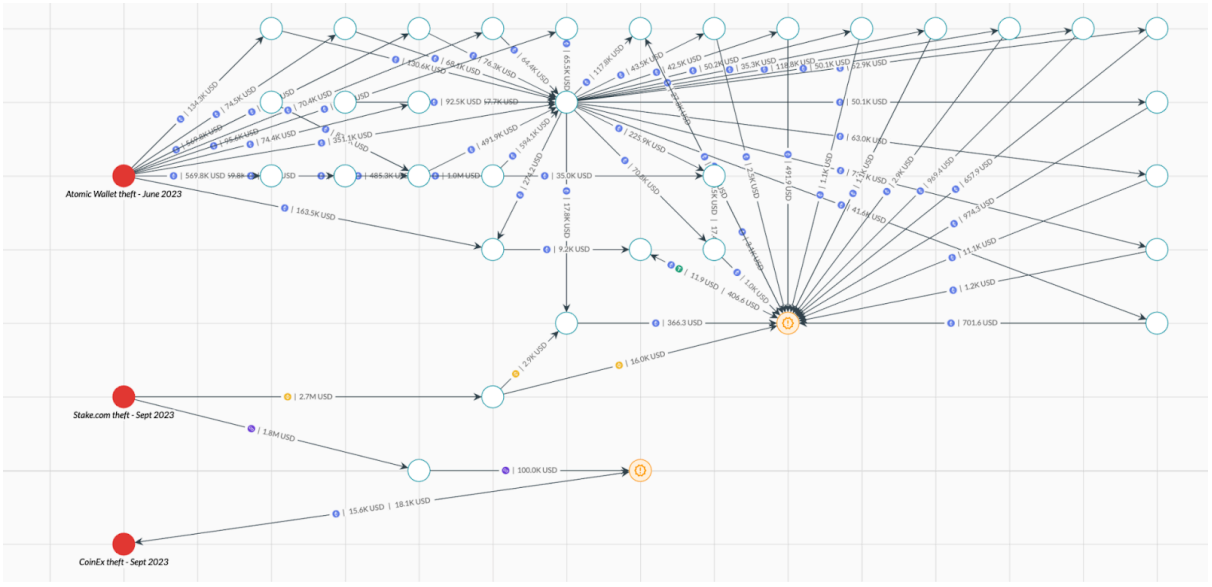
Now, they are suspected of carrying out a fifth attack, this time targeting the crypto exchange CoinEx on September 12th. In response to this, the company has released several tweets indicating that suspicious wallet addresses are still being identified, and therefore the total value of stolen funds is not yet known, however it is currently believed to be around $54 million.

In the past 104 days, Lazarus has already been identified as responsible for stealing almost $240 million in cryptoassets from Atomic Wallet ($100 million) CoinsPaid ($37.3 million), Alphapo ($60 million), and Stake.com ($41 million).



As seen in the chart above, 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. Following this, the funds were bridged to Ethereum, using a bridge previously used by Lazarus, and then sent back to an address known to be controlled by the CoinEx hacker.

Elliptic has observed this mixing of funds from separate hacks before from Lazarus, most recently when crypto was stolen from Stake.com overlapped with funds stolen from Atomic Wallet. These instances in which funds from different hacks have been consolidated are represented in the chart below in orange.



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.

Five Lazarus attacks in 104 days

In 2022, several high profile hacks were attributed to Lazarus, including the hacks of Harmony's Horizon Bridge, and Axie Infinity's Ronin Bridge, both of which occurred within the first half of last year. Between then and June of this year, no major crypto heists were publicly attributed to Lazarus. As a result, the various hacks of the last 104 days represent a step up in activity for the North Korean threat group.

- On June 3rd 2023, users of Atomic Wallet – a non-custodial decentralized cryptocurrency wallet – lost over $100 million. Elliptic attributed this hack to Lazarus on June 6th 2023, after identifying multiple factors indicating that the North Korean threat group was responsible. This attribution was later confirmed by the FBI.

- On July 22nd 2023, Lazarus gained access to hot wallets belonging to crypto payment platform CoinsPaid via a successful social engineering attack. This access allowed the attackers to create authorized requests to withdraw approximately $37.3 million in crypto assets from the platform's hot wallets. On July 26th, CoinsPaid published a report claiming Lazarus was responsible for this attack. This attribution was later

confirmed by the Federal Bureau of Investigation (FBI).

- On the same day, July 22nd, Lazarus conducted another high-profile attack, this time against centralized crypto payment provider Alphapo, stealing $60 million in cryptoassets. The attackers may have gained access through previously compromised private keys. As above, the FBI later attributed this attack to Lazarus.
- On September 4th 2023, online crypto casino Stake.com suffered an attack in which approximately $41 million in virtual currency was stolen, possibly as a result of a stolen private key. The FBI issued a press release on September 6th confirming that the Lazarus Group was behind this attack.
- Finally, on September 12th 2023, centralized crypto exchange CoinEx was the victim of a hack, in which $54 million was stolen. As detailed above, a number of factors indicate that Lazarus is responsible for this attack.

An analysis of Lazarus' latest activity suggests that since last year, it has shifted its focus from decentralized services to centralized ones. Four of the five recent hacks discussed previously are of centralized virtual asset service providers (VASPs). Centralized exchanges were previously Lazarus' target of choice prior to 2020, before the rapid rise of the decentralized finance (DeFi) ecosystem.

There are a number of possible explanations for why Lazarus' attention may have once again shifted back to centralized services.

Increased focus on security

Elliptic's previous research into DeFi hacks of 2022 found that one exploit occurred every four days, each stealing an average of $32.6 million.

Cross-chain bridges – which were a relatively new form of service in early 2022 – become some of the most frequently-hacked types of DeFi protocol. These trends have likely prompted improvements in smart contract auditing and development standards, thus reducing the scope for hackers to identify and exploit vulnerabilities.

Susceptibility to social engineering

For many of its hacks, the Lazarus Group's attack methodology of choice is social engineering. The $540 million hack of Ronin Bridge, for example, was attributed to a fake LinkedIn job offer.

Nevertheless, decentralized services often boast small workforces and – as the name suggests – are to varied extents decentralized. Hence, gaining malicious access to a developer may not necessarily equate to getting administrative access to a smart contract.

Centralized exchanges, meanwhile, will likely operate bigger workforces, thus widening the scope of possible targets. They are also likely to operate using centralized internal information technology systems, allowing Lazarus malware a greater chance to penetrate the intended functions of their business.

Elliptic will continue to monitor these incidents and update our system with new information on stolen funds.
