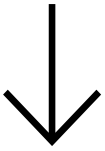
North Korean hackers return to Tornado Cash despite sanctions

By Elliptic Research

Archived: 2026-04-05 17:09:42 UTC



- **$112.5 million was stolen from exchange HTX and its HECO cross-chain bridge in November 2023 - Elliptic has attributed this hack to North Korea's Lazarus Group**
- **Since March 13 2024, over $100 million from this hack has been laundered through Tornado Cash**
- **Lazarus turned to Sinbad.io as its mixer of choice following sanctions on Tornado Cash in August 2022, but this service was seized by US authorities in November 2023**

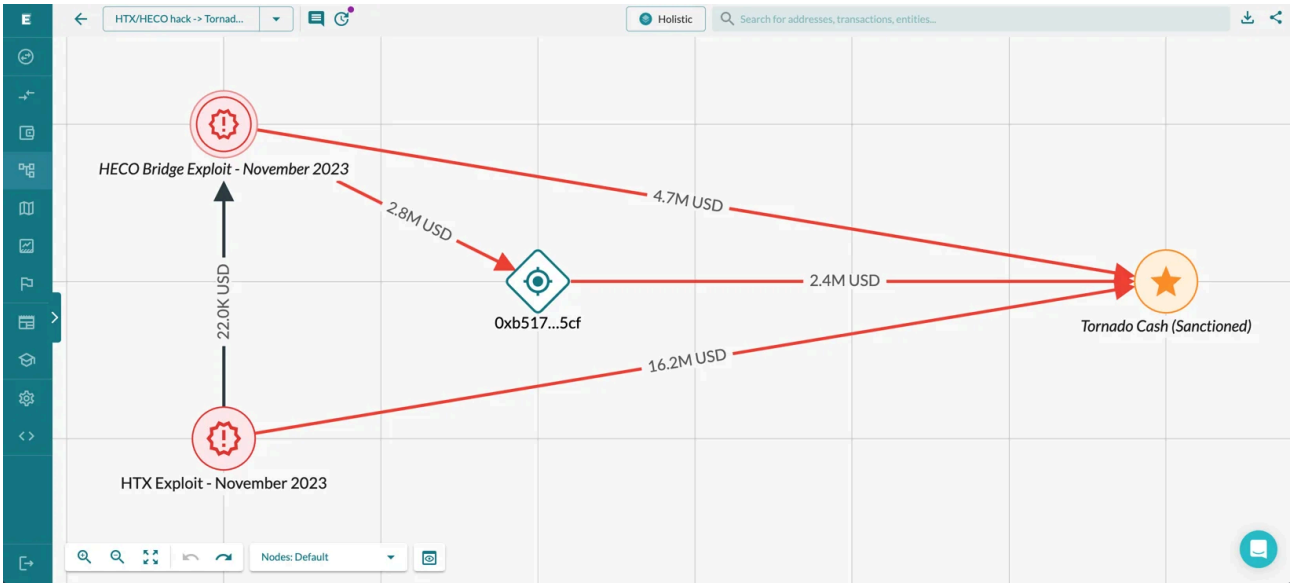
In November 2023, $112.5 million in cryptocurrency was stolen from crypto exchange HTX and its cross-chain bridge, known as HECO Bridge. Elliptic and others have attributed this theft to North Korea's Lazarus group, based on various attributes of the hack and the subsequent movement of funds.

Following common crypto-laundering patterns, the stolen tokens were immediately swapped for ETH, using decentralized exchanges. The stolen funds then lay dormant until March 13 2024, when the stolen cryptoassets began to be sent through Tornado Cash.

Tornado cash is a decentralized, smart contract-based mixer. It was sanctioned by the U.S. Treasury in August 2022, for its role in laundering $455 million from Lazarus Group crypto hacks. In response, Lazarus Group stopped using Tornado Cash, relying instead on using cross-chain bridges and the Bitcoin based mixer, Sinbad.io.

But in November 2023 Sinbad.io was itself seized by U.S. authorities, eliminating another mixing option.

However, Tornado Cash continues to operate despite sanctions. The mixer operates through smart contracts running on decentralized blockchains, so it cannot be seized and shut down in the same way that centralized mixers such as Sinbad.io have been.



A screenshot from Elliptic Investigator, showing the primary flow of funds from the HTX/HECO Bridge hacker wallet to Tornado Cash, as of March 15, 2024. (Not all transaction flows are displayed)

Lazarus Group now appear to have returned to using Tornado Cash as a way to launder funds at scale and obfuscate their transaction trail.

Since March 13 2024, more than $100 million in ETH from the HTX/HECO thefts has been laundered through Tornado Cash,.

This change in behavior and return to the use of Tornado Cash likely reflects the limited number of large-scale mixers now operating, thanks to law enforcement takedowns of services such as Sinbad.io and Blender.io.

Crypto exchanges and other financial institutions should use tools such as Elliptic's crypto transaction and wallet screening solutions to ensure that they do not engage in transactions with sanctioned actors such as Tornado Cash and Lazarus Group. Contact us to learn more.

This article has been updated to reflect the latest movements of funds into Tornado Cash and to correct the amount stolen from HTX and HECO Bridge.
