US sanctions crypto mixer Tornado Cash used by North Korean hackers

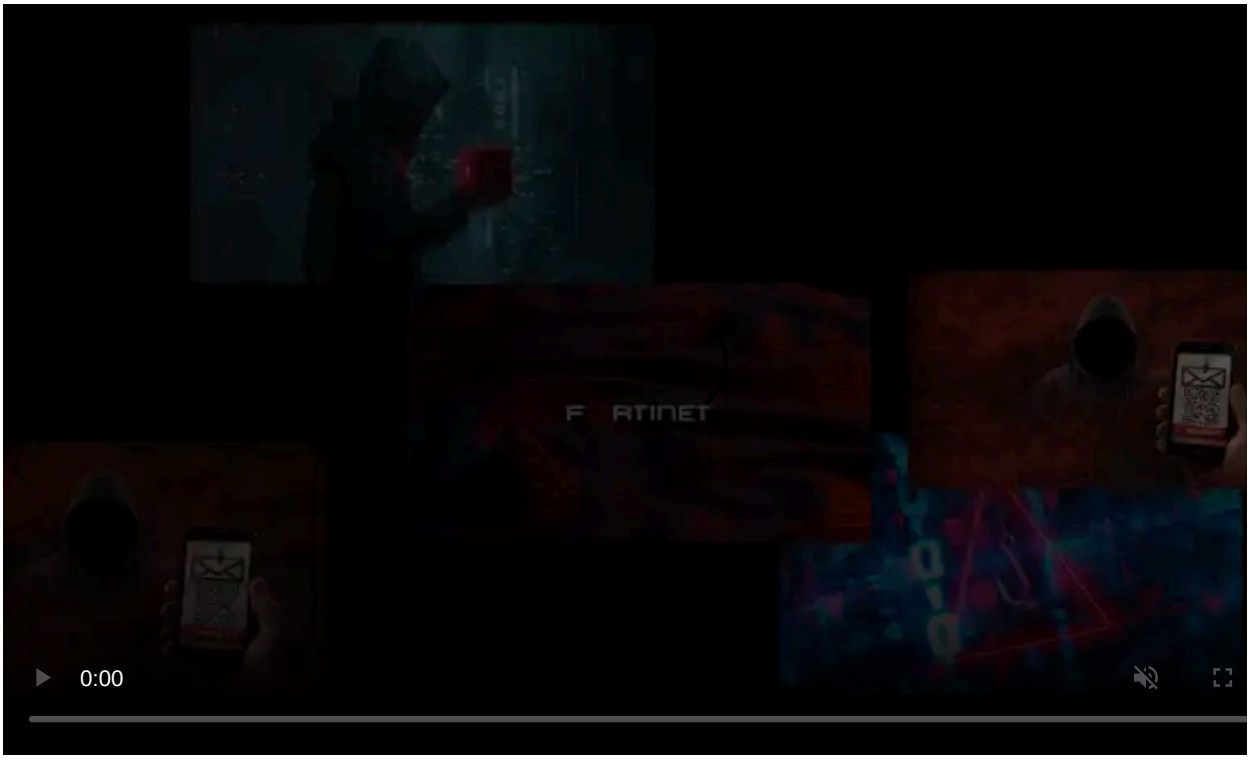
By Sergiu Gatlan

Published: 2022-08-08 · Archived: 2026-04-05 21:19:45 UTC

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash today, a decentralized cryptocurrency mixer service used to launder more than $7 billion since its creation in 2019.

The North Korean-backed APT Lazarus Group also used the crypto mixer to launder approximately $455 million stolen in the largest known cryptocurrency heist ever.

This was part of the total bounty collected following that attack since Lazarus stole $620 million worth of Ethereum after hacking Axie Infinity's Ronin network bridge in April.


F RTINET
0:00

Tornado Cash was also used to launder over $96 million after the June Harmony Bridge hack (out of $100 million stolen) and at least $7.8 million from the August Nomad Heist (out of $150 million stolen).

This crypto mixer was also used to make it harder to trace stolen funds after hacking blockchain music platform Audius, the Beanstalk DeFi platform, and the decentralized cryptocurrency exchange Uniswap, as well as in the Arbix Finance exit scam.

"Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States," said Brian E. Nelson, the Under Secretary of the Treasury for Terrorism and Financial Intelligence.

"Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks."

Not the first crypto mixer sanction by Treasury

U.S. Treasury has also sanctioned cryptocurrency mixer Blender.io in May, a service the Lazarus hacking group also used to launder cryptocurrency stolen after hacking the Ronin bridge.

The Financial Crimes Enforcement Network (FinCEN) also issued the first-ever civil money penalty against Larry Dean Harmon in October 2020, the founder and operator of the Helix and Coin Ninja mixer services, for violations of the Bank Secrecy Act (BSA) and its implementing regulations.

FinCEN revealed at the time that the most significant volume of cryptocurrency laundered using the Helix tumbler came from dark web illegal markets, including AlphaBay, Dream Mark, Agora Market, Nucleus, and several others.

"Virtual currency mixers that assist criminals are a threat to U.S. national security. Treasury will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financing risks in the virtual currency ecosystem," OFAC added today.

"As today's action demonstrates, mixers should in general be considered as high-risk by virtual currency firms, which should only process transactions if they have appropriate controls in place to prevent mixers from being used to launder illicit proceeds."

Source: https://www.bleepingcomputer.com/news/security/us-sanctions-crypto-mixer-tornado-cash-used-by-north-korean-hackers/