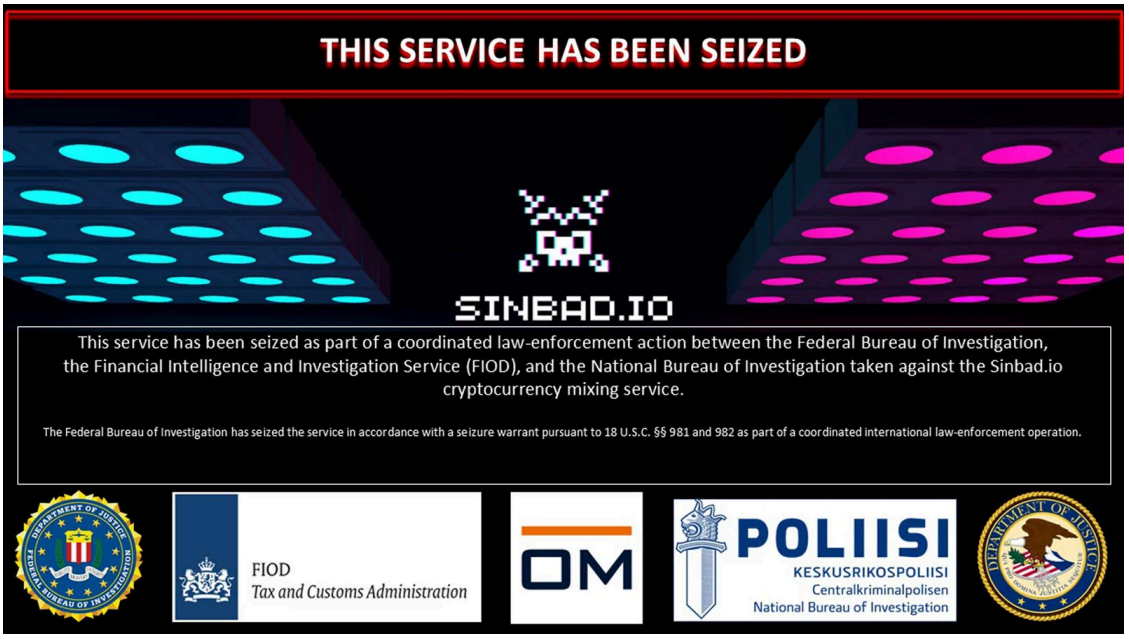
US seizes Sinbad crypto mixer used by North Korean Lazarus hackers

By Lawrence Abrams

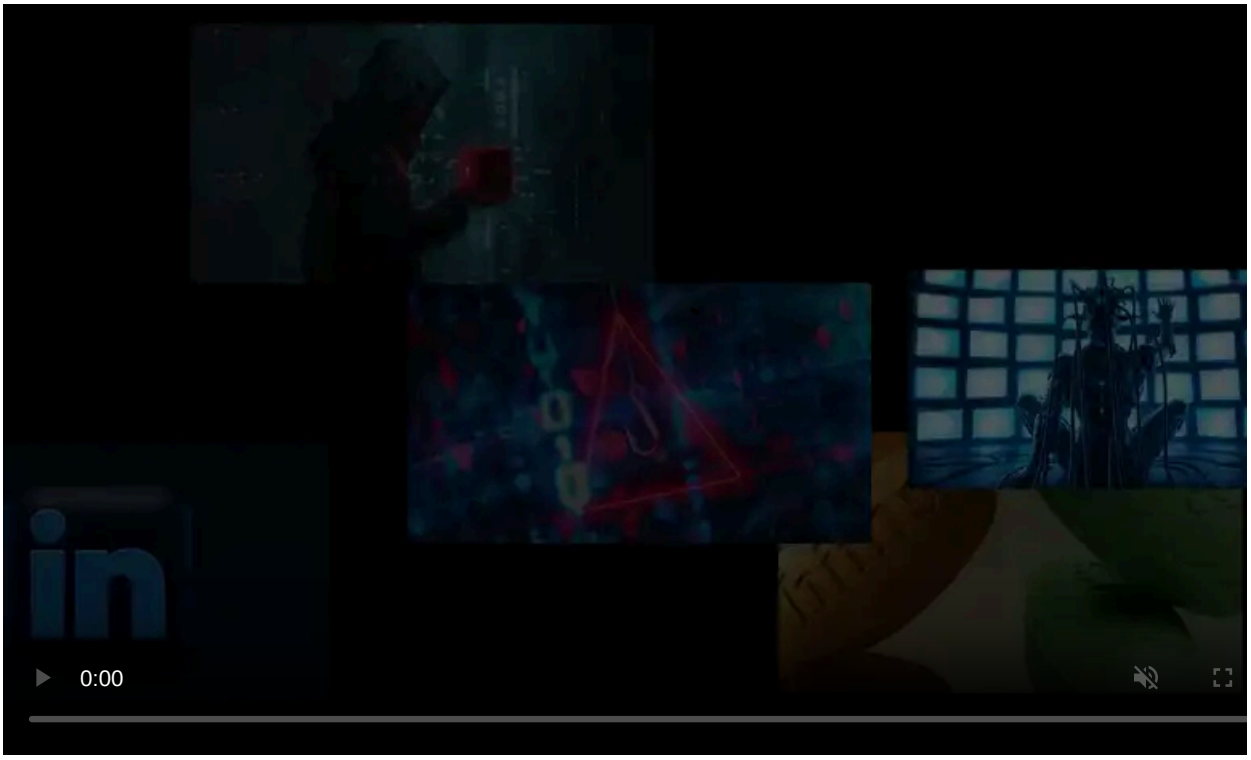
Published: 2023-11-29 · Archived: 2026-04-05 15:28:34 UTC

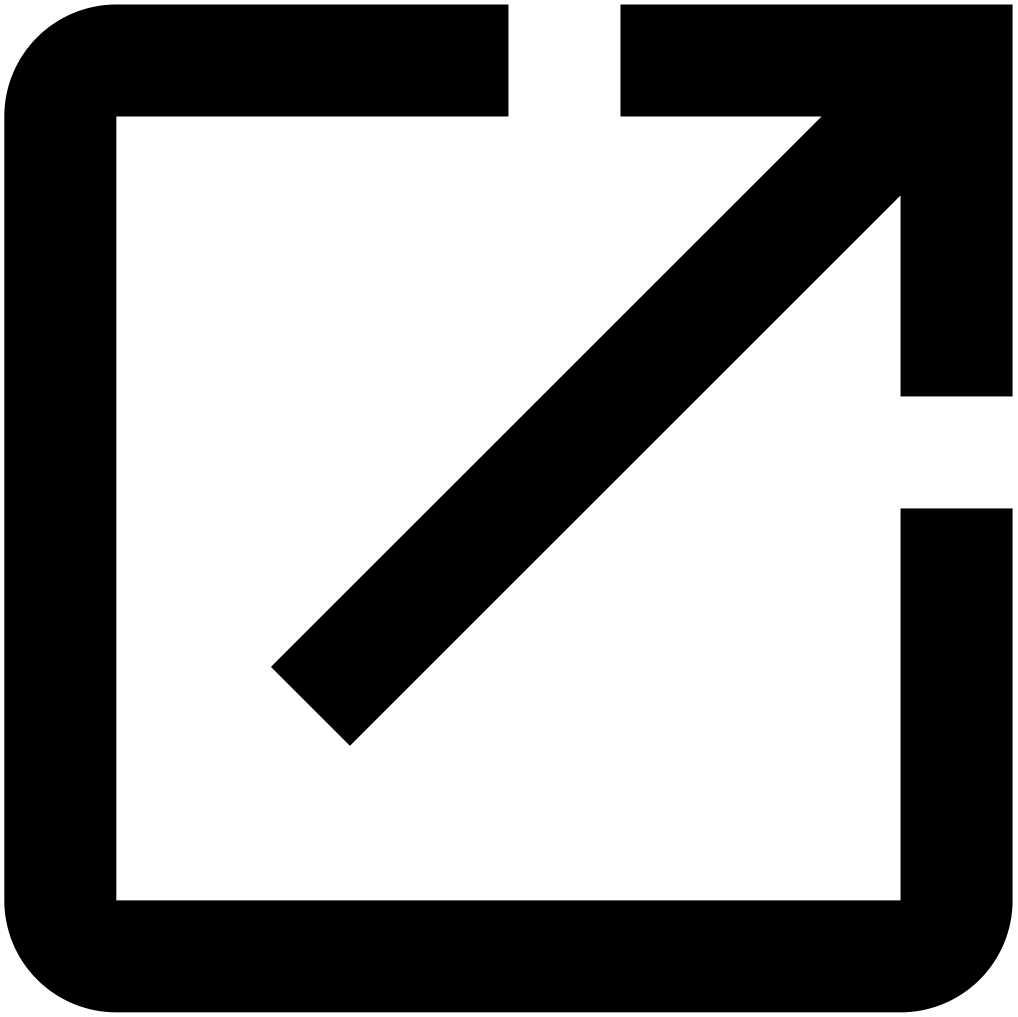


The U.S. Department of the Treasury has sanctioned the Sinbad cryptocurrency mixing service for its use as a money-laundering tool by the North Korean Lazarus hacking group.

A cryptocurrency mixer is a server that allows people to deposit crypto, which is mixed among many different wallet addresses to help prevent it from being accurately traced.

The mixing service takes a commission from the crypto deposited, and after it is "mixed," it will send it to another wallet address owned by the customer.


0:00



Today, the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned Sinbad.io (Sinbad) for its alleged use by North Korean hackers who have performed large-scale crypto heists, leading to hundreds of millions of dollars in losses.

"Sinbad has processed millions of dollars' worth of virtual currency from Lazarus Group heists, including the Horizon Bridge and Axie Infinity heists," reads a Department of Treasury press statement.

"Sinbad is also used by cybercriminals to obfuscate transactions linked to malign activities such as sanctions evasion, drug trafficking, the purchase of child sexual abuse materials, and additional illicit sales on darknet marketplaces."

Lazarus is a notorious North Korean hacking group known for its phishing attacks, fake employee recruitments, and exploiting blockchain vulnerabilities to steal millions in crypto, including $620 million from Axie Infinity, $100 million from Harmony Horizon, the Atomic Wallet hacks, and $37 million from CoinsPaid.

The F.B.I. says that North Korea uses this stolen money to fund the country's operations.

According to the Treasury Department, Sinbad was used to mix most of the stolen funds from the Atomic Wallet, Axie Infinity, and Horizon hacks.

In addition to sanctioning the crypto mixer, the domain for the Sinbad website has been seized in an international law enforcement operation conducted by the U.S., Netherlands, and Poland.

"This service has been seized as part of a coordinated law-enforcement action between the Federal Bureau of Investigation, the Financial Intelligence and Investigation Service (FIOD), and the National Bureau of Investigation taken against the Sinbad.io cryptocurrency mixing service," reads the seizure message on Sinbad[.]io.

"The Federal Bureau of Investigation has seized the service in accordance with a seizure warrant pursuant to 18 U.S.C. 981 and 982 as part of a coordinated international law-enforcement operation."

In addition to the clearweb site shown above, the Tor site for Sinbad is no longer operational. This indicates that the servers for the mixing service were seized by law enforcement as well.

OFAC previously sanctioned North Korean hacking groups, including Lazarus, in 2019. In 2022, OFAC sanctioned the Tornado Cash mixer for its use by North Korean hackers to launder stolen funds.
