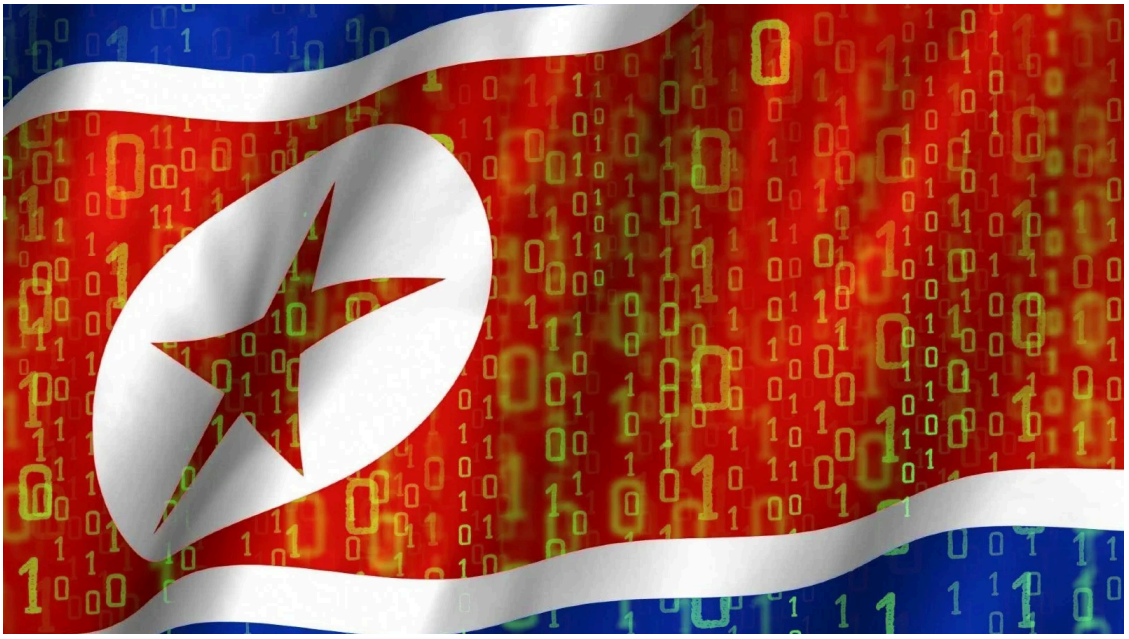
FBI links largest crypto hack ever to North Korean hackers

By Sergiu Gatlan

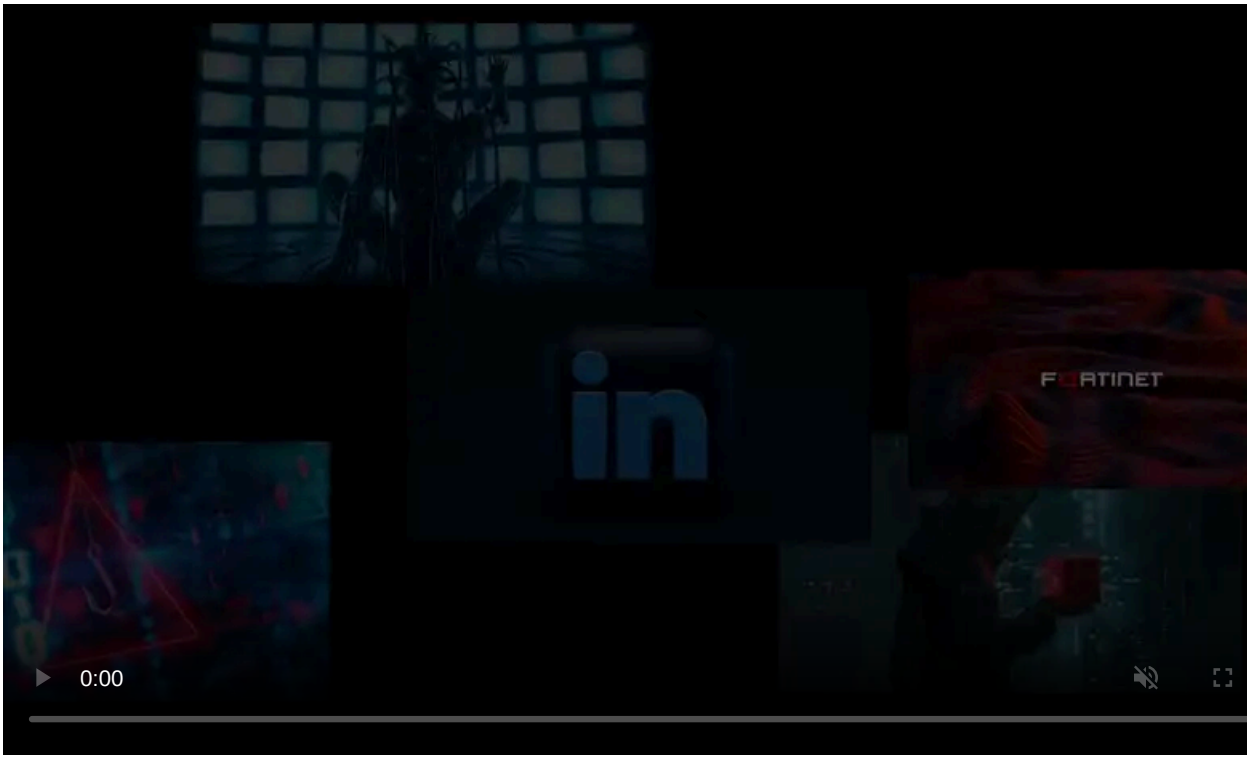
Published: 2022-04-14 · Archived: 2026-04-05 20:16:02 UTC

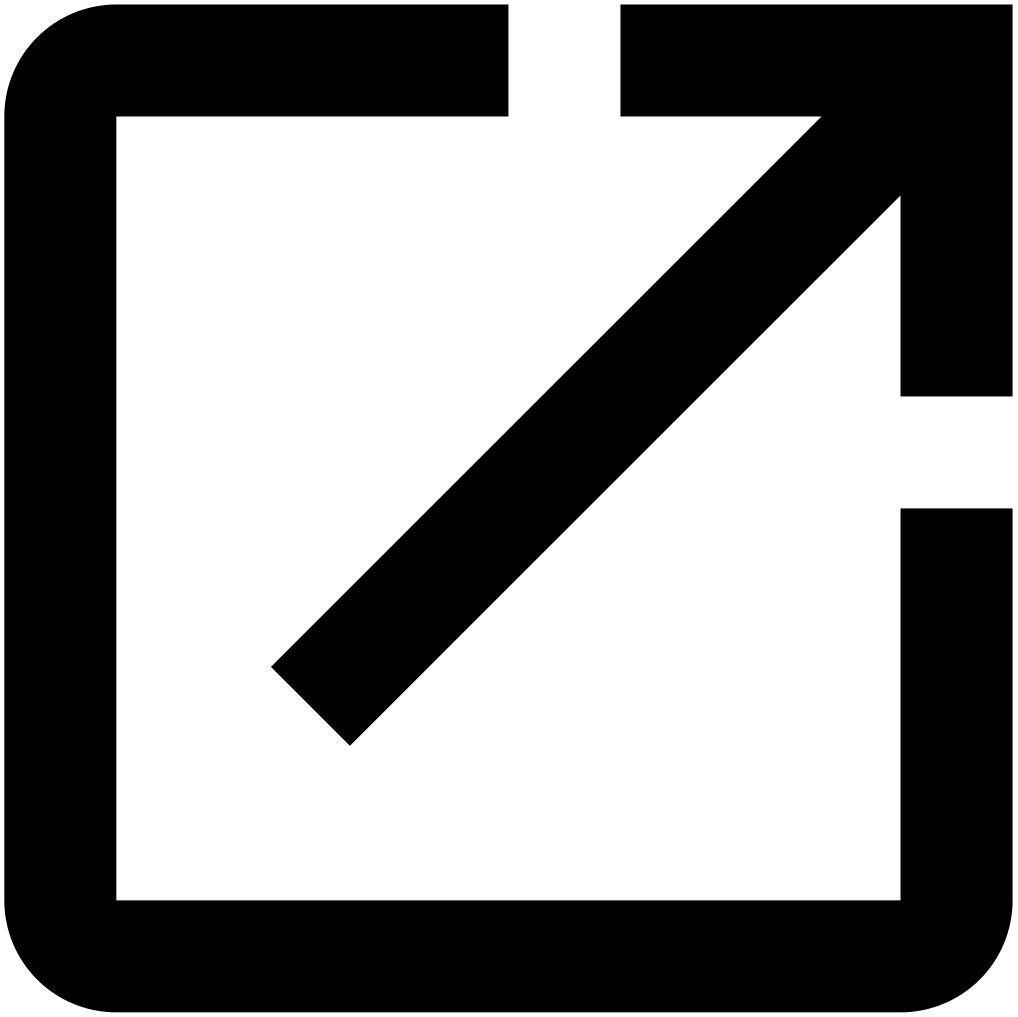


The Treasury Department's Office of Foreign Assets Control (OFAC) has sanctioned the address that received the cryptocurrency stolen in the largest cryptocurrency hack ever, the hack of Axie Infinity's Ronin network bridge.

The Federal Bureau of Investigation (FBI) said two North Korean hacking groups, Lazarus and BlueNorOff (aka APT38), were behind last month's Ronin hack.

"Through our investigation, we were able to confirm Lazarus Group and APT38, cyber actors associated with the DPRK, are responsible for the theft of $620 million in Ethereum reported on March 29th," the FBI said.


0:00



"The FBI, in coordination with Treasury and other U.S. Government partners, will continue to expose and combat the DPRK's use of illicit activities — including cybercrime and cryptocurrency theft — to generate revenue for the regime."

ETH address linked to Lazarus Group

Blockchain data platform Chainalysis first spotted that a new ETH address added by OFAC to the SDN list as part of a Lazarus Group update was also used in March to collect the ETH and USDC tokens stolen in the Ronin hack.

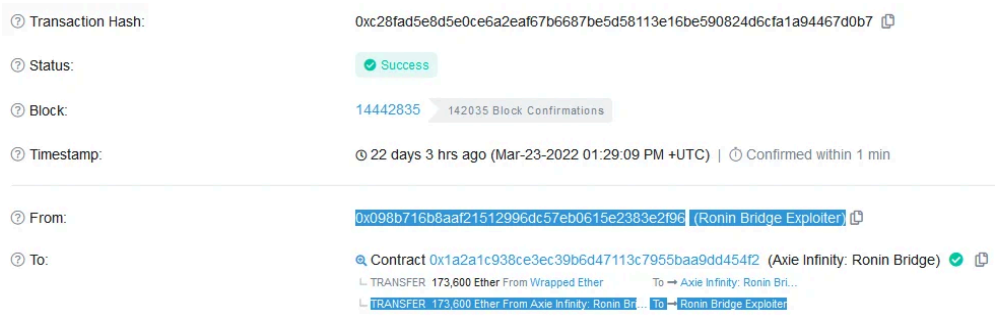
Ronin is an Ethereum sidechain developed by Sky Mavis to enable transactions for the Axie Infinity game, acting as a bridge for transferring ERC-20 tokens between the Ronin and Ethereum blockchains.

On March 29, Sky Mavis disclosed that the Ronin bridge was hacked, with 173,600 Ethereum and 25.5M USDC tokens stolen in two transactions [1 and 2], worth over $617 million.

Sky Mavis also published an update to their initial blog post disclosing the attack, saying the FBI now attributes the attack to the North Korean-backed Lazarus Group hacking group.

"Today, the FBI attributed North Korea based Lazarus Group to the Ronin Validator Security Breach," Sky Mavis said today.

"The US Government, specifically the Treasury Department, has sanctioned the address that received the stolen funds."



173,600 Ether transferred to Lazarus-controlled wallet (BleepingComputer)

This attack is the largest crypto hack in history, with the previous most significant theft of cryptocurrency being the $611 million Poly Network hack from August 2021.

"Today, OFAC added a new ETH address to Lazarus Group's SDN entry as an identifier: 0x098B716B8Aaf21512996dC57EB0615e2383E2f96," Chainalysis revealed in a Twitter thread on Thursday.

"That address was involved in the Ronin hack, having received 173,600 ETH and 25.5 million USDC from the Ronin Bridge smart contract during the attack."

Notorious North Korean threat group

The Lazarus Group (tracked as HIDDEN COBRA by the United States Intelligence Community) is a North Korean military hacking group active for more than a decade, since at least 2009.

Its operators are linked to multiple high-profile hacks, including the 2017 global WannaCry ransomware campaign and attacks against Sony Films and various banks worldwide.

Google also spotted the Lazarus Group's attempts to target security researchers in January 2021 and March 2021 as part of complex social engineering attacks.

They were also observed using the ThreatNeedle backdoor and the MATA malware framework against defense industry entities from over a dozen countries in cyber-espionage campaigns starting with early 2020.

The US Treasury sanctioned three DPRK-sponsored hacking groups (Lazarus, Bluenoroff, and Andariel) in September 2019.

The US government also offers a reward of up to $5 million for tips on the DPRK hackers' malicious activity to help identify or locate them.

Update: Added FBI statement.

Source: https://www.bleepingcomputer.com/news/security/fbi-links-largest-crypto-hack-ever-to-north-korean-hackers/