South Korea Sanctions Pyongyang Hackers

By Jayant Chakravarti

Archived: 2026-04-05 18:41:59 UTC

Blockchain & Cryptocurrency , Cryptocurrency Fraud , Fraud Management & Cybercrime

Seoul Cracks Down on North Korea's Flourishing Cryptocurrency Theft Industry (@JayJay_Tech) • February 13, 2023

North Korean leader Kim Jong-un watches a missile demonstration in August 2019. (Photo: Korean Central News Agency)

South Korea sanctioned four North Korean individuals and seven organizations for conducting illegal cyber activities to finance the totalitarian regime's nuclear and missile development programs.

See Also: Revolutionizing Cross-Border Transactions with Permissioned DeFi

Seoul accused the individuals and institutions of stealing virtual currency, conducting ransomware attacks and obtaining IT work at front companies using fake documents to raise funds.

Among the individuals is Park Jin-Hyok, an alleged member of Reconnaissance General Bureau, North Korea's military intelligence agency. Park is already named in a U.S. federal indictment for allegedly participating in a campaign to steal more than $1.3 billion of money and cryptocurrency from financial institutions and companies worldwide.

The United States also charged Park for carrying out the global WannaCry 2.0 ransomware attacks, an $81 million heist from Bangladesh Bank in 2016, and numerous other attacks.

Seoul also sanctioned Jo Myong Rae, the head of the Computer Technology Research Institute, and Chosun Expo Joint Venture, a front company with offices in China and North Korea. The sanctions list also blacklists state hacking groups such as Lazarus, Bluenoroff and Andariel, and the state Technical Reconnaissance Bureau.

The government said the targeted sanctions against North Korean entities to prevent cryptocurrency theft were a long time in the making. It established in August 2022 a working group with the U.S. to discuss potential sanctions against North Korean hackers and conducted a joint symposium with the U.S. in November to share information with the private sector about North Korea's hacking techniques.

South Korea also established a National Cyber Security Cooperation Center in November 2022 to enable joint response of public and private sectors against North Korea's cyberattacks. Seoul also partnered with domestic and foreign cryptocurrency exchanges to freeze stolen funds, identify crypto wallet addresses used by hackers and established a procedure to record senders and recipients for all crypto transactions. It has now listed eight virtual asset wallet addresses associated with Lazarus.

Stolen cryptocurrency has become a principle source of hard currency for North Korea. The country exported just $82 million worth of goods and services in 2021, but its hackers stole over $1.2 billion in cryptocurrency since 2017. Blockchain analysis firm Chainalysis says North Korean cybercriminals had "a banner year in 2021," stealing about $400 million worth of digital assets.

The FBI last year blamed Lazarus for stealing $620 million in ethereum from online game Axie Infinity. It also said last week that Lazarus stole $100 million worth of ethereum from Harmony Horizon, a cross-chain bridge for ethereum.
