FBI Identifies Cryptocurrency Funds Stolen by DPRK

fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk

The FBI is warning cryptocurrency companies of recent blockchain activity connected to the theft of hundreds of millions of dollars in cryptocurrency. Over the last 24 hours, the FBI tracked cryptocurrency stolen by the Democratic People's Republic of Korea (DPRK) TraderTraitor-affiliated actors (also known as Lazarus Group and APT38). The FBI believes the DPRK may attempt to cash out the bitcoin worth more than $40 million.

The FBI investigation found the TraderTraitor-affiliated actors moved approximately 1,580 bitcoin from several cryptocurrency heists and are currently holding those funds in following bitcoin addresses:

- 3LU8wRu4ZnXP4UM8Yo6kkTiGHM9BubgyiG
- 39idqitN9tYNmq3wYanwg3MitFB5TZCjWu
- 3AAUBbKJorvNhEUFhKnep9YTwmZECxE4Nk
- 3PjNaSeP8GzLjGeu51JR19Q2Lu8W2Te9oc
- 3NbdrezMzAVVfXv5MTQJn4hWqKhYCTCJoB
- 34VXKa5upLWVYMXmgid6bFM4BaQXHxSUoL

The DPRK TraderTraitor-affiliated actors were responsible for several high-profile international cryptocurrency heists to include the $60 million theft of virtual currency from Alphapo on June 22, 2023; the $37 million theft of virtual currency from CoinsPaid on June

22, 2023; and the $100 million theft of virtual currency from Atomic Wallet on June 2, 2023. The FBI previously provided information on their attacks against Harmony's Horizon bridge and Sky Mavis' Ronin Bridge, and provided a Cybersecurity Advisory on TraderTraitor. In addition, the U.S. Department of Treasury's Office of Foreign Assets Control sanctioned the Lazarus Group in 2019.

Private sector entities should examine the blockchain data associated with these addresses and be vigilant in guarding against transactions directly with, or derived from, the addresses. The FBI will continue to expose and combat the DPRK's use of illicit activities—including cybercrime and virtual currency theft—to generate revenue for the regime. If you have any information to provide, please contact your local FBI field office or the FBI's Internet Crime Complaint Center at ic3.gov.