FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft

fbi.gov/news/press-releases/fbi-confirms-lazarus-group-apt38-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft

Washington, D.C.

The FBI continues to combat malicious cyber activity, including the threat posed by the Democratic People's Republic of Korea (DPRK) to the U.S. and our private sector partners. Through our investigation, we were able to confirm that the Lazarus Group (also known as APT38), cyber actors associated with the DPRK, are responsible for the theft of $100 million of virtual currency from Harmony's Horizon bridge reported on June 24, 2022.

FBI Los Angeles and FBI Charlotte—in coordination with the FBI's Cyber Division, the United States Attorney's Office for the Central District of California, the United States Attorney's Office for the District of Columbia, the National Cryptocurrency Enforcement Team, the National Security Division's Counterintelligence and Export Control Section, and the FBI's Virtual Assets Unit—continue to identify and disrupt North Korea's theft and laundering of virtual currency, which is used to support North Korea's ballistic missile and Weapons of Mass Destruction programs.

On Friday, January 13, 2023, North Korean cyber actors used RAILGUN, a privacy protocol, to launder over $60 million worth of ethereum (ETH) stolen during the June 2022 heist. A portion of this stolen ethereum was subsequently sent to several virtual asset service providers and converted to bitcoin (BTC).

A portion of these funds were frozen, in coordination with some of the virtual asset service providers. The remaining bitcoin subsequently moved to the following addresses:

- 1BK769SseNefb6fe9QuFEi8W4KGbtP8gi3
- 15FcqYRbwh2JsRUyBjvZ4jJ2XAD3pycGch
- 1HwSof6jnbMFpfrRRa2jvydYdopkkGB4Sn
- 15emeZ7buVegqhYh9PekH7cwFEJcCeVNpS
- 3MSbCJCYtx5sj1nkzD4AMEhhvvviXBc8XJ
- 17Z79rZpkk8kUiJseg5aELwYKaoLnirMUn
- bc1qp2vvntdedxw4xwtyd4y3gc2t9ufk6pwz2ga4ge
- 3P9WebHkiDxCi8LDXiRQp8atNEagcQeRA3
- 37fnBxofDeph2fpBZxZKypNkwdXAt9nT6F
- 185NxhFAmKZrdwn9rVga3kqbvDP4FkbTNw
- 12283Cq1pJ3f1gXwqi6K3bRf5LZb8Bkm6g

The FBI, in conjunction with the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Treasury Department, previously published a joint Cybersecurity Advisory describing a malware campaign dubbed "TraderTraitor" that the DPRK used in the Harmony intrusion.

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 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.