# FBI links North Korean hackers to $1.5 billion cryptocurrency heist



The FBI has formally linked a significant cryptocurrency heist to North Korean hackers, describing it as one of the largest publicly acknowledged thefts in the sector's history, with a value estimated at approximately $1.5 billion. This incident occurred earlier this month when the attackers targeted Bybit, one of the most prominent cryptocurrency exchanges globally, based in Dubai.

In an online public service announcement released late Wednesday, the FBI stated its belief that hackers associated with the North Korean government, referred to as the "TraderTraitor" group and the "Lazarus Group," were behind the substantial theft. The Bureau detailed that the criminals achieved this via the distribution of altered cryptocurrency trading applications embedded with malware, which facilitated the theft of digital currency.

Notably, the FBI indicated that the hackers have acted quickly to convert some of the stolen ethereum into Bitcoin and other virtual assets, systematically dispersing these across numerous addresses on multiple blockchains. The Bureau anticipates that these assets will undergo further laundering efforts before eventually being converted into fiat currency.

Reports underscore that North Korea has amassed an estimated $1.2 billion from cryptocurrency thefts and various virtual assets in the last five years, as per South Korea’s spy agency. These stolen funds serve as a vital source of foreign currency, helping to support North Korea's struggling economy and its controversial nuclear weapons programme, especially amid stringent U.N. sanctions and the nation’s strict border closures during the ongoing COVID-19 pandemic.

In parallel, a panel of U.N. experts is reportedly investigating 58 suspected cyberattacks attributed to North Korea between 2017 and 2023, with claims that around $3 billion has been looted to allegedly back the advancement of the country's weapons of mass destruction initiatives.

Ben Zhou, co-founder and CEO of Bybit, acknowledged the FBI's announcement through a post on the social media platform X, linking to a website that offers bounties up to $140 million for information relating to the tracking and freezing of the stolen cryptocurrency. He noted that a routine transfer of ethereum from a "cold" or offline wallet was reportedly "manipulated" by the attacker, who redirected the funds to an unidentified address.

Manuel Villegas, an analyst at Julius Baer, elaborated that the hack was executed with a high degree of sophistication, targeting cold wallets through a "blind signing" exploit. This method involved the creation of a deceptive interface that closely resembled the trusted trading platform, thereby misleading users.

Blockchain analytics firm Certik defined the recent theft as "the largest breach" in the history of blockchain transactions. In the aftermath of the hack, overall cryptocurrency prices have experienced a decline, with market sentiment shaken despite previous bullish trends following the election of U.S. President Donald Trump. For instance, Bitcoin, which had surpassed $100,000 a month ago, fell to over $82,000 per coin on Thursday.

The implications of the theft are vast, as Villegas cautioned that it poses significant challenges for Bybit's customers and is likely to attract increased regulatory scrutiny moving forward.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.bleepingcomputer.com/news/security/fbi-confirms-lazarus-hackers-were-behind-15b-bybit-crypto-heist/> - This article confirms the FBI's attribution of the $1.5 billion Bybit crypto heist to North Korean hackers, specifically the Lazarus Group. It details how the hackers intercepted a scheduled transfer of funds and redirected them to their control.
* <https://www.ic3.gov/PSA/2025/PSA250226> - This FBI public service announcement confirms North Korea's involvement in the theft of approximately $1.5 billion from Bybit and notes the rapid conversion of stolen assets into Bitcoin and other virtual currencies.
* <https://www.voanews.com/a/north-korea-behind-1-5-billion-crypto-theft-fbi-says/7989814.html> - This article reports on the FBI's accusation that North Korea was behind the $1.5 billion crypto theft from Bybit, attributing it to the Lazarus Group. It also mentions North Korea's history of cyber warfare.
* <https://www.noahwire.com> - This is the source article that discusses the FBI's formal linking of the cryptocurrency heist to North Korean hackers and provides additional context on the implications and methods used in the hack.
* <https://www.chainalysis.com/> - Chainalysis is a blockchain analysis company that tracks cryptocurrency transactions and could provide insights into North Korea's cryptocurrency thefts and laundering efforts, though specific details on this incident are not directly linked here.