

North Korea behind \$1.5 billion crypto theft, FBI says

AFP —The US Federal Bureau of Investigation on Wednesday accused North Korea of being behind the theft of \$1.5 billion worth of digital assets last week, the largest crypto heist in history.

Dubai-based cryptocurrency exchange Bybit reported last week that it had been robbed of 400,000 in cryptocurrency Ethereum.

According to the company, attackers exploited security protocols during a transaction, enabling them to transfer the assets to an unidentified address.

On Wednesday, the US government pointed the finger at Pyongyang.

“(North Korea) was responsible for the theft of approximately \$1.5 billion USD in virtual assets from cryptocurrency exchange, Bybit,” the FBI said in a public service announcement.

The bureau said a group called TraderTraitor, also known as the Lazarus Group, was behind the theft.

It said they were “proceeding rapidly and have converted some of the stolen assets to Bitcoin and other virtual assets dispersed across thousands of addresses on multiple blockchains”.

“It is expected these assets will be further laundered and eventually converted to fiat currency,” the FBI added.

Lazarus Group gained notoriety a decade ago when it was accused of hacking into Sony Pictures as revenge for “The Interview,” a film that mocked North Korean leader Kim Jong

Un.

It was also allegedly behind the 2022 \$620 million heist of Ethereum and USD Coin from the Ronin Network in 2022, previously the biggest crypto theft in history.

And in December, the United States and Japan blamed it for the theft of cryptocurrency worth over \$300 million from the Japan-based exchange DMM Bitcoin.

North Korea's cyber-warfare program dates back to at least the mid-1990s, and the country has been dubbed "the world's most prolific cyber-thief" by a cybersecurity firm.

Pyongyang's program has grown to a 6,000-strong cyber-warfare unit known as Bureau 121 that operates from several countries, according to a 2020 US military report.

A United Nations panel on North Korea's evasion of sanctions last year estimated the nation has stolen more than \$3 billion in cryptocurrency since 2017.

Much of the hacking activity is reportedly directed by Pyongyang's Reconnaissance General Bureau, its primary foreign intelligence agency.

Money stolen helps to fund the country's nuclear weapons program, the panel said.

AFP