N.Korea-tied hackers executed $620 mn crypto heist: FBI

April 15 2022

Hackers linked to North Korea are responsible for the March 2022 theft of $620 million in ethereum, a type of cryptocurrency.

North Korean-tied hackers were responsible for a $620-million cryptocurrency heist last month targeting players of the popular Axie Infinity game, US authorities said Thursday.

The hack was one of the biggest to hit the crypto world, raising huge questions about security in an industry that only recently burst into the mainstream thanks to celebrity promotions and promises of untold wealth.

Last month's theft from the makers of Axie Infinity, a game where players can earn crypto through game play or trading their avatars, came just weeks after thieves made off with around $320 million in a similar attack.

"Through our investigations we were able to confirm Lazarus Group and APT38, cyber actors associated with (North Korea), are responsible for the theft," the FBI said in a statement.

Lazarus Group gained notoriety in 2014 when it was accused of hacking into Sony Pictures Entertainment as revenge for "The Interview," a satirical film that mocked North Korean leader Kim Jong Un.

North Korea's cyber-program dates back to at least the mid-1990s, but has since grown to a 6,000-strong cyber-warfare unit, known as Bureau 121, that operates from several countries including Belarus, China, India, Malaysia and Russia, according to a 2020 US military report.

John Bambenek, a threat analyst with digital security firm Netenrich, said North Korea is "unique" in employing groups dedicated to cryptocurrency theft.

"As North Korea is highly-sanctioned, cryptocurrency thefts are also a national security interest for them," he said.

North Korean hackers stole around $400 million-worth of cryptocurrency through cyberattacks on digital currency outlets last year, blockchain data platform Chainalysis said in January.

In the case of the Axie Infinity heist, attackers exploited weaknesses in the set-up put in place by the Vietnam-based firm behind the game, Sky Mavis.

The company had to solve a problem: the ethereum blockchain, where transactions in the ether cryptocurrency are logged, is relatively slow and expensive to use.

To allow Axie Infinity players to buy and sell at speed, the firm created an in-game currency and a sidechain with a bridge to the main ethereum blockchain.

The result was faster and cheaper—but ultimately less secure.

The attack targeting its blockchain netted 173,600 ether and $25.5 million-worth of stablecoin, a digital asset pegged to the US dollar.