North Korean hackers stole $400 mn in crypto in 2021: Chainalysis

14 January 2022

Pyongyang's cyberwarfare abilities first came to global prominence in 2014 when it was accused of hacking into Sony Pictures Entertainment as revenge for "The Interview", a satirical film that mocked leader Kim.

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

Pyongyang is under multiple international sanctions over its atomic bomb and ballistic missile developments but analysts say the North has also built up its cyber capabilities with an army of thousands of well-trained hackers who extract finances to fund the state's weapons programs.

In 2021, the hackers launched seven attacks on crypto platforms, extracting assets from "internet-connected 'hot' wallets" and moving them to North Korean controlled accounts, according to Chainalysis.

"Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out," Chainalysis said in a report published on its website.

"These complex tactics and techniques have led many security researchers to characterize cyber actors for the Democratic People's Republic of Korea (DPRK) as advanced persistent threats."

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

"From 2018 on, The group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million."

The hackers also target a diverse variety of cryptocurrencies, with Bitcoin, the world's largest digital currency, accounting for only a quarter of stolen assets.

"The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation," Chainalysis said.

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

The United States imposed new sanctions on North Korea this week following what Pyongyang called hypersonic missile tests on January 5 and 11.

On Friday South Korean and Japanese officials said North Korea fired an unidentified projectile eastward in its third suspected weapons test in just over a week.