# US puts sanctions on N.Korea hacking groups behind major thefts

13 September 2019

The US Treasury on Friday placed sanctions on three North Korea government-sponsored hacking operations which it said were behind the theft of possibly hundreds of millions of dollars and destructive cyber-attacks on infrastructure.

The Treasury said the three groups—dubbed Lazarus Group, Bluenoroff and Andariel—were behind major thefts from financial institutions and cryptocurrency exchanges, as well as the 2018 WannaCry hack that crippled Britain's National Health Service.

All three are tied to the Reconnaissance General Bureau, Pyongyang's main intelligence bureau, and are behind numerous malicious computer viruses as well as attempts to steal billions of dollars online to fund the North Korean government, the Treasury said.

"Treasury is taking action against North Korean hacking groups that have been perpetrating cyber attacks to support illicit weapon and missile programs," said Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence.

"We will continue to enforce existing US and UN sanctions against North Korea and work with the international community to improve cybersecurity of financial networks," she said in a statement.

Created in 2007, Lazarus group has been known for years. It was behind the malicious hack of Sony Pictures in 2014, as well as the WannaCry ransomware that spread to at least 150 countries in 2017.

The most heaviest hit was Britain's public health system, with hospitals virtually shut down and thousands of patients turned away, costing the government ultimately more than $112 million.

Bluenoroff was formed specifically to obtain revenue for the North Korean government, the Treasury said.

By hijacking the global banking transfer system SWIFT, by 2018 it had made attempts online to steal more that $1.1 billion from financial institutions .

Its biggest success, together with Lazarus, was the $80 million heist from Bangladesh's central bank.

Andariel specializes in targeting businesses, government agencies and individuals. It has been known to steal bank card information and hack into ATMs, and to steal bank customer information to sell on the black market.

The Treasury said Andariel created unique malware to hack online gambling and poker sites.

The Treasury also cited online accounts to say the three groups "likely" stole $571 million in cryptocurrency from five Asian exchanges in 2017 and 2018.

The sanctions aim to lock anyone involved with the groups out of the global financial system and empower the US government to freeze any assets held under US jurisdiction.

In September 2018 the FBI charged North Korean Park Jin Hyok, allegedly a member of the Lazarus group, with conspiracy for multiple cyberattacks including the Sony Pictures attacks and the theft from the Central Bank of Bangladesh.