North Korean hackers extorted health care organizations to fund further cyberattacks, US and South Korea say

By Sean Lyngaas, CNN
Updated 2039 GMT (0439 HKT) February 9, 2023

Washington (CNN) North Korean government-backed hackers have conducted ransomware attacks on health care providers and other key sectors in the US and South Korea and used the proceeds to fund further cyberattacks on government agencies in Washington and Seoul, US and South Korean officials warned Thursday.

Some of those follow-on hacks have specifically targeted Pentagon networks and US defense contractors, according to the advisory from US and South Korean intelligence and security agencies.

It's the latest in a drumbeat of warnings from US officials that North Korea is adopting cybercriminal tactics to fund dictator Kim Jong Un's ambitions, including the regime's pursuit of nuclear weapons.

The statement from the US Federal Bureau of Investigation, US National Security Agency, South Korean National Intelligence Service and others does not mention Kim's weapons programs, but US officials have previously warned that a portion of the money Pyongyang steals through hacking can go to weapons development.

North Korea's use of stolen cryptocurrency to fund its weapons programs is part of the regular set of intelligence products presented to President Joe Biden, a senior administration official told CNN this week.

"They need money, so they're going to keep being creative," the official said. "I don't think the North Koreans are ever going to stop looking for illicit ways to glean funds because it's an authoritarian regime ... under heavy sanctions."

The news comes as North Korea displayed nearly a dozen advanced intercontinental ballistic missiles at a nighttime military parade on Wednesday.

The new US-South Korea advisory did not identify hospitals that the North Korean hackers had allegedly victimized. The Justice Department has previously accused Pyongyang-backed hackers of hitting a medical center in Kansas in 2021, encrypting computer systems the facility relied on to operate key equipment, and another medical provider in Colorado.

The advisory follows a similar warning from US agencies in July that North Korean hackers had used ransomware to disrupt services at health organizations for "prolonged periods."

In the statement released Thursday, US and South Korean officials accused North Korean hackers of taking pains to try to hide their identities -- even posing as a notorious Russian ransomware gang. The North Koreans are also emulating non-state criminals in dumping online the private data of victims who do not pay, officials said.

The hackers have used a popular software used in small and medium-sized hospitals in South Korea to spread their malicious code with the aim of locking up computers, according to the advisory.

In addition to hacking, suspected North Koreans have posed as other nationalities to apply for work at IT firms and send money back to Pyongyang, US agencies have publicly warned. A CNN investigation found at least one cryptocurrency entrepreneur who unwittingly paid a North Korean tech worker tens of thousands of dollars.