North Korea-linked hackers 'highly likely' behind WannaCry: Symantec

May 23 2017

North Korea has angrily dismissed reports linking it to the ransomware that crippled hundreds of thousands of computers

The Lazarus hacking group, widely believed to be connected to North Korea, is "highly likely" responsible for the WannaCry global cyberattack that hit earlier this month, US anti-virus firm Symantec said.

North Korea has angrily dismissed earlier reports linking its isolated

regime to the worm that crippled hundreds of thousands of computers, demanding payment in Bitcoin to return control to users.

But Symantec said the ransomware had many of the hallmarks of other Lazarus attacks, including the 2014 strike on Sony Pictures and a multimillion-dollar theft from the Bangladesh Central Bank.

Without mentioning the group's links to North Korea, it said that prior to the global outbreak on May 12, an earlier version of WannaCry was used in a small number of attacks in the previous three months.

"Analysis... revealed substantial commonalities in the tools, techniques, and infrastructure used by the attackers and those seen in previous Lazarus attacks, making it highly likely that Lazarus was behind the spread of WannaCry."

Up to 300,000 computers in 150 countries were hit by the WannaCry worm, which seizes systems and demands payment in Bitcoin to return control to users.

Banks, hospitals and state agencies were among the victims of the hackers who exploited vulnerabilities in older versions of Microsoft computer operating systems.

Staff monitor the spread of ransomware cyber-attacks at the Korea Internet and Security Agency in Seoul

The North last week vehemently denied the claims, notably but not exclusively advanced by South Korean experts, and hit back to accuse its opponents of spreading propaganda.

Experts say the North appears to have stepped up cyber-attacks in recent years in a bid to earn hard foreign currency in the face of United Nations sanctions imposed over its nuclear and missile programmes.

Symantec said that despite the links to Lazarus, "the WannaCry attacks do not bear the hallmarks of a nation-state campaign but are more typical of a cyber crime campaign."

In November 2014, Sony Pictures Entertainment became the target of

the biggest cyberattack in US corporate history, linked to its release of North Korea satire "The Interview".

Washington blamed Pyongyang for the attack, a claim it denied—though it had strongly condemned the film, which features a fictional CIA plot to assassinate leader Kim Jong-Un

Seoul internet security firm Hauri, known for its vast troves of data on Pyongyang's hacking activities, has been warning of ransomware attacks since last year.

Researchers in the US, Russia and Israel have also pointed to a potential North Korean link—but it is notoriously hard to attribute cyberattacks.

Google researcher Neel Mehta has also shown similarities between WannaCry and code used by the Lazarus hacking group, widely believed to be connected to Pyongyang.