Experts question North Korea role in WannaCry cyberattack

May 19 2017, by Eric Talmadge

In this Monday, May 15, 2017, file photo, employees watch electronic boards to monitor possible ransomware cyberattacks at the Korea Internet and Security Agency in Seoul, South Korea. A couple of things about the WannaCry cyberattack are now pretty certain. It was the biggest in history and it's a scary preview of things to come—we're all going to have to get used to hearing the word "ransomware." But one thing is a lot less clear: whether North Korea had anything to do with it. (Yun Dong-jin/Yonhap via AP, File)

A couple of things about the WannaCry cyberattack are certain. It was

the biggest in history and it's a scary preview of things to come—we're all going to have to get used to hearing the word "ransomware." But one thing is a lot less clear: whether North Korea had anything to do with it.

Despite bits and pieces of evidence that suggest a possible North Korea link, experts warn there is nothing conclusive yet—and a lot of reasons to be dubious. Why, for example, would Pyongyang carry out a big hack that hurt its two closest strategic partners more than anyone else? And for what appears to be a pretty measly amount of loot—as of Friday the grand total of ransom that had been paid was less than $100,000.

Within days of the attack, respected cybersecurity firms Symantec and Kaspersky Labs hinted at a North Korea link. Google researcher Neel Mehta identified coding similarities between WannaCry and malware from 2015 that was tied to the North. And the media have since spun out stories on Pyongyang's league of hackers, its past involvement in cyberattacks and its perennial search for new revenue streams, legal or shady.

But identifying hackers behind sophisticated attacks is a notoriously difficult task. Proving they are acting under the explicit orders of a nation state is even trickier.

When experts say North Korea is behind an attack, what they often mean is that Pyongyang is suspected of working with or through a group known as Lazarus. The exact nature of Lazarus is cloudy, but it is thought by some to be a mixture of North Korean hackers operating in cahoots with Chinese "cyber-mercenaries" willing to at times do Pyongyang's bidding.

Lazarus is a serious player in the cybercrime world.

It is referred to as an "advanced persistent threat" and has been fingered

in some very sophisticated operations, including an attempt to breach the security of dozens of banks this year, an attack on the Bangladesh central bank that netted $81 million last year, the 2014 Sony wiper hack and DarkSeoul, which targeted the South Korean government and businesses.

"The Lazarus Group's activity spans multiple years, going back as far as 2009," Kaspersky Labs said in a report last year. "Their focus, victimology, and guerrilla-style tactics indicate a dynamic, agile and highly malicious entity, open to data destruction in addition to conventional cyberespionage operations."

But some experts see the latest attack as an anomaly.

WannaCry infected more than 200,000 systems in more than 150 countries with demands for payments of $300 in Bitcoin per victim in exchange for the decryption of the files it had taken hostage. Victims received warnings on their computer screens that if they did not pay the ransom within three days, the demand would double. If no ransom was paid, the victim's data would be deleted.

As ransomware attacks go, that's a pretty typical setup.

In this Monday, May 15, 2017, file photo, employees watch electronic boards to monitor possible ransomware cyberattacks at the Korea Internet and Security Agency in Seoul, South Korea. A couple of things about the WannaCry cyberattack are now pretty certain. It was the biggest in history and it's a scary preview of things to come—we're all going to have to get used to hearing the word "ransomware." But one thing is a lot less clear: whether North Korea had anything to do with it. (Yun Dong-jin/Yonhap via AP, File)

But that's not—or at least hasn't been—the way North Korean hackers are believed to work.

"This is not part of the previously observed behavior of DPRK cyberwar units and hacking groups," Michael Madden, a visiting scholar at the Johns Hopkins School of Advanced International Studies and founder of North Korea Leadership Watch, said in an email to The Associated Press. "It would represent an entirely new type of cyberattack by the DPRK."

Madden said the North, officially known as the Democratic People's Republic of Korea, if it had a role at all, could have instead been involved by giving or providing parts of the packet used in the attack to another state-sponsored hacking group with whom it is in contact.

"This type of ransomware/jailbreak attack is not at all part of the M.O. of the DPRK's cyberwar units," he said. "It requires a certain level of social interaction and file storage, outside of those with other hacking groups, that DPRK hackers and cyberwar units would not engage. Basically they'd have to wait on Bitcoin transactions, store the hacked files and maintain contact with the targets of the attack."

Other cybersecurity experts question the Pyongyang angle on different grounds.

James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, a cybersecurity think tank, argues that the evidence remains "circumstantial at best," and believes WannaCry spread due to luck and negligence, not sophistication.

"While it is possible that the Lazarus group is behind the WannaCry malware, the likelihood of that attribution proving correct is dubious," he wrote in a recent blog post laying out his case. "It remains more probable that the authors of WannaCry borrowed code from Lazarus or a similar source."

Scott said he believes North Korea would likely have attacked more strategic targets—two of the hardest-hit countries, China and Russia, are the North's closest strategic allies—or tried to capture more significant profits.

Very few victims of the WannaCry attack appear to have actually paid up. As of Friday, only $91,000 had been deposited in the three Bitcoin "wallet" accounts associated with the ransom demands, according to London-based Elliptic Enterprises, which tracks illicit Bitcoin activity.

More importantly, Scott said, the rush to blame North Korea distracts from bigger issues—software vulnerabilities resulting from manufacturers' refusal to incorporate security into their software development, organizations' failure to protect their systems and client data and the responsibility of governments to "manage, secure, and disclose discovered vulnerabilities."

"Global attacks are the new normal," he wrote.