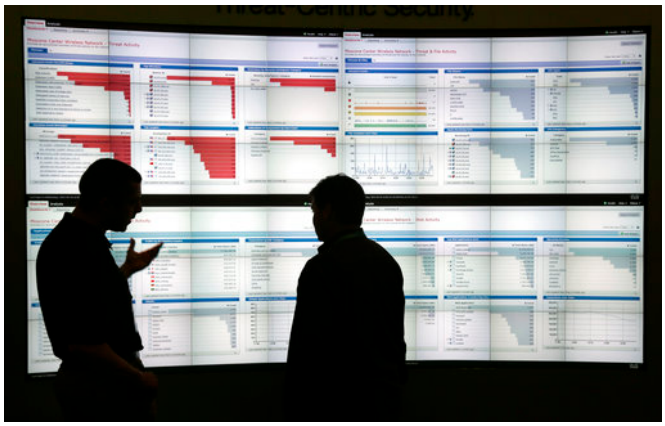
Experts see possible North Korea links to global cyberattack

16 May 2017, by Youkyung Lee



In this Wednesday, April 22, 2015, file photo, Stijn Vanveerdeghem, left, an engineer with Cisco, shows graphics with live wireless traffic to FedEx employee Barry Poole during the RSA Conference in San Francisco, where threat analysts, security vendors and corporate IT administrators gathered to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. As the Friday, May 12, 2017, global cyberextortion attack that held people's computer files hostage slows, authorities are working to catch the crooks behind it, which is a difficult task that involves searching for digital clues and following the money. (AP Photo/Marcio Jose Sanchez, File)

Cybersecurity experts are pointing to circumstantial evidence that North Korea may be behind the global "ransomware" attack: the way the hackers took hostage computers and servers across the world was similar to previous cyberattacks attributed to North Korea.

Simon Choi, a director at South Korean anti-virus software company Hauri Inc. who has analyzed North Korean malware since 2008 and advises the government, said Tuesday that the North is no newcomer to the world of bitcoins. It has been mining the digital currency using malicious computer programs since as early as 2013, he said.

In the attack, hackers demand payment from victims in bitcoins to regain access to their encrypted computers. The malware has scrambled data at hospitals, factories, government agencies, banks and other businesses since Friday, but an expected second-wave outbreak largely failed to materialize after the weekend, in part because security researchers had already defanged it .

Choi is one of a number of researchers around the world who have suggested a possible link between the "ransomware" known as WannaCry and hackers linked to North Korea. Researchers at Symantec and Kaspersky Lab have found similarities between WannaCry and previous attacks blamed on North Korea.

While Choi's speculation may deepen suspicions that the nuclear-armed state is responsible, the evidence is still far from conclusive. Authorities are working to catch the extortionists behind the global cyberattack, searching for digital clues and following the money.

"We are talking about a possibility, not that this was done by North Korea," Choi said.

ABOUT THAT NORTH KOREA LINK

WannaCry paralyzed computers running mostly older versions of Microsoft Windows in some 150 countries. It encrypted users' computer files and displayed a message demanding $300 to $600 worth of the digital currency bitcoin to release them; failure to pay would leave the data scrambled and likely beyond repair .

The hackers appeared to have taken control of computers and servers around the world by sending a type of malicious code known as a worm to file-sharing protocols. The worms quickly scanned computers with vulnerability, in this case

the older versions of Microsoft Windows, and used those computers as hackers' command and control centers.

This method, which allows quick and massive infections of computers with security weaknesses, has been found in previously known North Korean cyberattacks, including the Sony hack in 2014 blamed on North Korea.

"Since a July 2009 cyberattack by North Korea, they used the same method," Choi said. "It's not unique in North Korea but it's also not a very common method."

Choi also cited an accidental communication he had last year with a hacker traced to a North Korean internet address who admitted development of ransomware.

South Korea was mostly spared from the latest ransomware attack, partly because constant threats from the North have made the government and companies careful about always updating their software.

South Korea has been a frequent target of cyberattacks that it traced to its northern neighbor. Some high-profile attacks between 2009 and 2013 shut down government websites, banking systems and paralyzed broadcasters.

On Monday, the Russian security firm Kaspersky Lab said portions of the WannaCry program use the same code as malware previously distributed by the Lazarus Group, a hacker collective behind the 2014 Sony hack.

But it's possible the code was simply copied from the Lazarus malware without any other direct connection. Kaspersky said "further research can be crucial to connecting the dots."

Another security company, Symantec, has also found similarities between WannaCry and Lazarus tools, and said it's "continuing to investigate for stronger connections."

If North Korea, believed to be training cyber warriors at schools, is indeed responsible for the latest attack, Choi said the world should stop underestimating its capabilities and work together to think of a new way to respond to cyber threats, such as having China pull the plug on North Korea's internet.

"We have underestimated North Korea so far that since North Korea is poor, it wouldn't have any technologies. But North Korea has been preparing cyber skills for more than 10 years and its skill is significant. We should never underestimate it," Choi said.

FOLLOW THE MONEY

Researchers might find some additional clues in the bitcoin accounts accepting the ransom payments. There have been three accounts identified so far, and there's no indication yet that the criminals have touched the funds.

Although bitcoin is anonymized, researchers can watch it flow from user to user. So investigators can follow the transactions until an anonymous account matches with a real person, said Steve Grobman, chief technology officer with the California security company McAfee.

But that technique is no sure bet. There are ways to convert bitcoins into cash on the sly through third parties. And even finding a real person might be no help if they're in a jurisdiction that won't cooperate.

TELL-TALE SIGNS

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington, said U.S. investigators are collecting forensic information—such as internet addresses, samples of malware or information the culprits might have inadvertently left on computers—that could be matched with the handiwork of known hackers.

Investigators might also be able to extract some information about the attacker from a previously hidden internet address connected to WannaCry's "kill switch." That switch was essentially a beacon sending the message "hey, I'm infected" to the hidden address, Weaver said.

That means the very first attempts to reach that address, which might have been recorded by spy agencies such as the NSA or Russian intelligence, could lead to "patient zero"—the first computer infected with WannaCry. That, in turn, might further narrow the focus on possible suspects.

THE PLAYERS

Forensics, though, will only get investigators so far. One challenge will be sharing intelligence in real time to move as quickly as the criminals—a tricky feat when some of the major nations involved, such as the U.S. and Russia, distrust each other.

Even if the perpetrators can be identified, bringing them to justice could be another matter. They might be hiding out in countries that wouldn't be willing to extradite suspects for prosecution, said Robert Cattanach, a former U.S. Justice Department attorney and an expert on cybersecurity.

On the other hand, the WannaCry attack hit—and annoyed—many countries. Russia was among the hardest hit, and Britain among the most high-profile, and both have "some pretty good investigative capabilities," Cattanach said.

Anick Jesdanun and Barbary Ortutay in New York, Lori Hinnant in Paris and Deb Riechmann in Washington contributed to this story.

APA citation: Experts see possible North Korea links to global cyberattack (2017, May 16) retrieved 27 January 2022 from https://phys.org/news/2017-05-experts-north-korea-links-global.html