North Korea, cyberattacks and 'Lazarus': What we really know

June 2 2017, by Eric Talmadge

In this Monday, May 15, 2017, file photo, employees watch electronic boards monitoring possible ransomware cyberattacks at the Korea Internet and Security Agency in Seoul, South Korea. Beyond the frequently used shorthand that North Korea was behind the "WannaCry" ransomware attack lies a more complicated and enlightening story: the rise of an infamous group of workaholic hackers, collectively known as "Lazarus," who may be using secret lairs in northeast China and have created a virtual "malware factory" that could wreak a lot more havoc in the future. (Yun Dong-jin/Yonhap via AP, File)

With the dust now settling after "WannaCry", the biggest ransomware attack in history, cybersecurity experts are taking a deep dive into how it was carried out, what can be done to protect computers from future breaches and, trickiest of all, who is really to blame.

For many, it seems that last question has already been solved: It was North Korea.

But beyond the frequently used shorthand that North Korea was likely behind the attack lies a more complicated—and enlightening—story: the rise of an infamous group of workaholic hackers, collectively known as "Lazarus," who may be using secret lairs in northeast China and have created a virtual "malware factory" that could wreak a lot more havoc in the future.

Big caveat here: Lazarus doesn't reveal much about itself. What little is known about the group is speculative.

Nevertheless, extensive forensic research into its activities dating back almost a decade paints a fascinating, if chilling, picture of a hacker collective that is mercenary, tenacious and motivated by what appears to be a mixture of political and financial objectives.

Their fingerprints are all over WannaCry.

So who, then, are they?

___

OPERATION BLOCKBUSTER

On Dec. 19, 2014, just one month after a devastating hack hobbled Sony Pictures Entertainment, the FBI's field office in San Diego issued a press

release stating North Korea was the culprit and saying such cyberattacks pose "one of the gravest national security dangers" to the United States.

"The destructive nature of this attack, coupled with its coercive nature, sets it apart," the statement said. "North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior."

The FBI listed similarities in specific lines of code, encryption algorithms, data deletion methods and compromised networks for its determination. It said there was a significant overlap between the infrastructure used in the attack and other cyberactivity it had previously linked directly to North Korea, including several internet protocol addresses hardcoded into the data deletion malware.

Its claim that North Korea was to blame has since been widely disputed.

In an attempt to analyze the Sony Hack, an industry consortium led by Novetta launched "Operation Blockbuster," which in 2016 released the most detailed public report to date on the attack. Its findings lined up with the FBI's conclusion that the tactics, tools and capabilities strongly indicated the work of a "structured, resourced and motivated organization," but said its analysis could not support the direct attribution of a nation-state.

Instead, it determined the attack "was carried out by a single group, or potentially very closely linked groups, sharing technical resources, infrastructure and even tasking."

It named the group Lazarus.

Operation Blockbuster traced the first inklings of Lazarus activity to

2009, or possibly to 2007, with large-scale denial of service attacks on U.S. and South Korean websites. That was followed by the "Operation Troy" cyberespionage campaign that lasted from 2009 to 2013; "Ten Days of Rain," which used compromised computers for denial of service attacks on South Korean media and financial institutions and U.S. military facilities; and "DarkSeoul," an attack on South Korean broadcasting companies and banks.

"This is a determined adversary with the resources to develop unique, mission-oriented malware tools," the 100-page report concluded.

In this Monday, May 15, 2017, file photo, a customer walks by the notice that reads: "Due to ransomware affection, we are unable to screen advertisement. Beyond the frequently used shorthand that North Korea was behind the "WannaCry" ransomware attack lies a more complicated and enlightening story: the rise of an infamous group of workaholic hackers, collectively known as "Lazarus," who may be using secret lairs in northeast China and have created a

virtual "malware factory" that could wreak a lot more havoc in the future. (AP Photo/Lee Jin-man, File)

NORTH KOREAN HACKERS OR CYBER-MERCENARIES?

Researchers at cybersecurity giant Kaspersky Labs, which also participated in Operation Blockbuster, analyzed timestamps on accounts suspected of being linked to Lazarus to create a profile of its hackers.

They surmised the attackers are probably located in a time zone eight or nine hours ahead of Greenwich Mean Time—which would include China, Malaysia and parts of Indonesia, among other places—because they seem to start working at around midnight GMT and break for lunch three hours later.

They even claimed the hackers get roughly 6-7 hours of sleep per night.

"This indicates a very hard-working team, possibly more hard working than any other Advanced Persistent Threat group we've analyzed," it said. It also said the reference sample of suspected Lazarus activity indicated at least one resource in the Korean language on a majority of the computers being used.

"The group rapidly develops, mutates and evolves malware through the extensive use of a 'malware factory,'" said James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, a Washington-based think tank. "Essentially, it is believed that they subcontract or outsource the rapid development of new malware and malware variants to numerous external threat actors."

Scott said any connections between Lazarus and North Korea remain unclear, but four possibilities exist:

— Lazarus is affiliated with North Korea;

— it is an independent side operation of persons affiliated with North Korea;

— it is entirely independent of North Korea;

— it is a cyber-mercenary collective that occasionally works on behalf of North Korea.

"There is no conclusive evidence that Lazarus is state-sponsored," Scott said, adding that it has instead "always exhibited the characteristics of a well-resourced and organized cybercriminal or cyber-mercenary collective."

Jon Condra, director of Asia-Pacific research at the cybersecurity firm Flashpoint, cautiously noted the theory that at least some Lazarus Group hackers are likely working out of China and that they may include North Koreans. Flashpoint analyzed the WannaCry ransom notes posted in 28 languages and determined all but three were created using translation software—suggesting its authors include human members who are native in Chinese and fluent but not perfect in English.

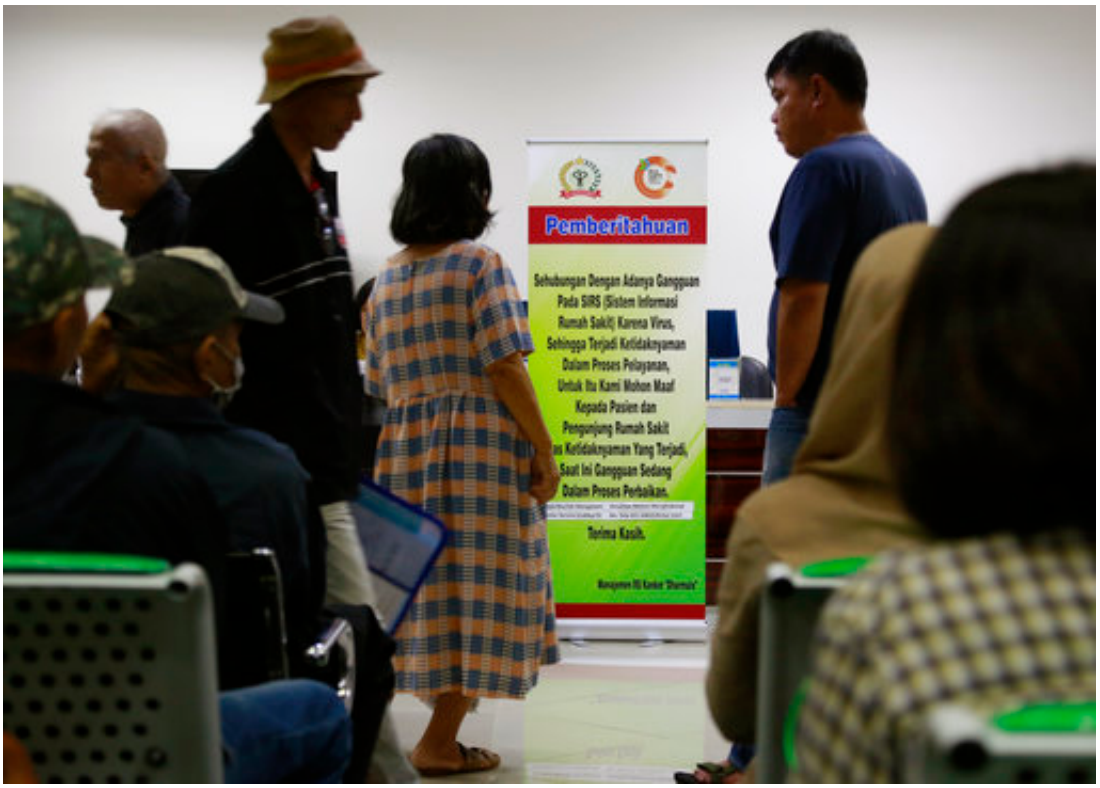
"It is widely believed that at least some North Korean hacking units operate out of Northeastern China—the city of Shenyang, in particular—but hard evidence is scant," he said. "It is entirely possible that the Lazarus Group is not entirely made up of North Korean actors, but may also have Chinese members."

Even that, he added, is speculative: "We really do not have a clear

picture of the composition of the Lazarus Group."

___

AN EVER-MORPHING ADVERSARY



In this Monday, May 5, 2017, file photo, patients wait near a banner informing about a delay in service due to a cyberattack at the Dharmais Cancer Hospital in Jakarta, Indonesia, Monday, May 15, 2017. Beyond the frequently used shorthand that North Korea was behind the "WannaCry" ransomware attack lies a more complicated and enlightening story: the rise of an infamous group of workaholic hackers, collectively known as "Lazarus," who may be using secret lairs in northeast China and have created a virtual "malware factory" that could wreak a lot more havoc in the future. (AP Photo/Dita Alangkara, File)

Kaspersky took another look into Lazarus after the attempted heist of $900 million from the central bank of Bangladesh in February last year. It found Lazarus is both accelerating its activities and morphing rapidly.

According to Kaspersky, the Lazarus Group now has its own cybercrime subgroup, dubbed BlueNoroff, to help finance its operations through attacks on banks, casinos, financial institutions and traders.

"The scale of Lazarus operations is shocking," its report said. "It's something that requires strict organization and control at all stages of the operation. ... Such a process requires a lot of money to keep running the business."

The disruptive and "asymmetric" nature of cyber warfare clearly makes it a weapon North Korea can be assumed to want to exploit against its much more powerful adversaries in a military conflict.

Cybercrime would also seem to be extremely attractive to North Korea.

It's hard to trace, can be done on the cheap and, for those who can master the technological expertise, the opportunities seem to be everywhere. It would also seem to be a less risky means of procuring illicit income than other activities the North Korean regime has been accused of in the past, like drug trafficking and counterfeiting U.S. $100 bills.

Washington, Seoul and defectors from North Korea all claim the North is working hard to train an army of cyber warriors, mainly within its primary intelligence agency, the Reconnaissance General Bureau. South Korea said North Korea's cyber army consisted of 6,800 hackers in 2015.

But independent experts tend not to take such claims too literally.

Scott and Condra caution that much of what is reported about North Korea's cyber army comes from defectors or rival governments with a spin motive and is amplified by partisan or attention-seeking media. Defectors' insights are valuable, yes. But even if they're not politically motivated, they are limited by the scope of their access and inside knowledge—and are usually significantly out of date.

___

STILL-MISSING LINKS

The U.S. government has not blamed WannaCry on North Korea.

"We know North Korea possesses the capability of doing this kind of thing but we are still assessing what the source is," National Intelligence Director Dan Coats told a congressional hearing last week. Coats added, however, that cyberattacks are possibly "the most significant threat to the United States at this time."

Pinning a cybercrime to a cybercriminal is a Sisyphean task. A known group might claim responsibility. It might use a traceable internet protocol address, or a unique code. Its methods and tools may reveal a pattern. Often, it will do all of the above and more in an attempt to lead investigators down a false path.

Determining the role of a nation-state can be even more difficult.

Some campaigns that have been attributed to the Lazarus Group suggest a lower-skilled adversary than one might expect from one with full state backing—a factor that Beau Woods, the deputy director of the Cyber Statecraft Initiative at the Atlantic Council, says is indicative of "a blurred line" between state and non-state actors.

"Many countries allow, or at least tolerate, non-state actors that are doing things that are ideologically aligned," he said. "With North Korea, it appears to be the case that they rely very heavily on this kind of criminal element-amateurs-professionals. It's a predominance of question marks."

"The big lesson we learned from WannaCry, no matter who did it, is just how vulnerable, prone and exposed some of our critical pieces of infrastructure are," he said. "When the stakes are so high, we owe it more diligence than what we have seen so far."