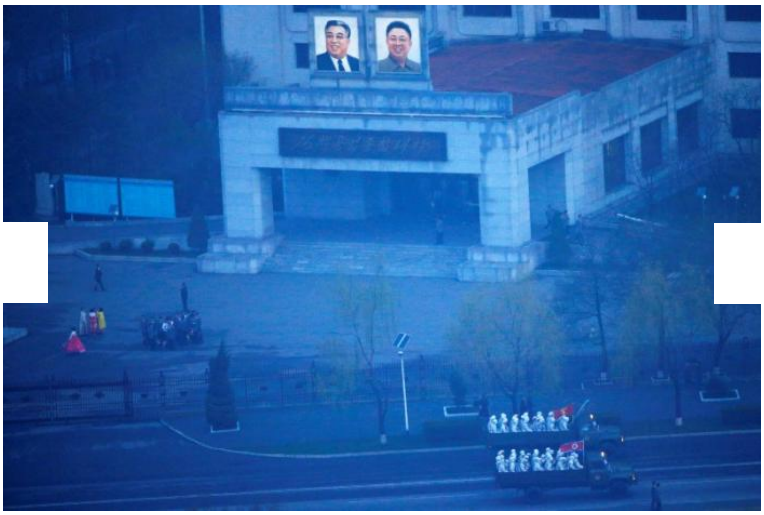
CYBER RISK | Mon May 22, 2017 | 11:34am EDT

Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West



FILE PHOTO: Military trucks carry soldiers through central Pyongyang before sunset April 15, 2017. REUTERS/Damir Sagolj/File Photo

TRENDING **STORIES**

1 U.S. warship drill meant to defy China's claim over artificial island - officials

2 Trump directly scolds NATO allies, says they owe 'massive' sums

3 Trump, Macron engage in a little handshake diplomacy

4 Trump condemns leaks after UK police stop sharing attack information

5 GM is accused in lawsuit of cheating on diesel truck emissions

By **Ju-min Park** and **James Pearson** | SEOUL

North Korea's main spy agency has a special cell called Unit 180 that is likely to have launched some of its most daring and successful cyber attacks, according to defectors, officials and internet security experts.

North Korea has been blamed in recent years for a series of online attacks, mostly on financial networks, in the United States, South Korea and over a dozen other countries.

Cyber security researchers have also said they have found technical evidence that could link North Korea with the global WannaCry "ransomware" cyber attack that infected more than 300,000 computers in 150 countries this month. Pyongyang has called the allegation "ridiculous".

The crux of the allegations against North Korea is its connection to a hacking group called Lazarus that is linked to last year's $81 million cyber heist at the Bangladesh central bank and the 2014 attack on Sony's Hollywood studio. The U.S. government has blamed North Korea for the Sony hack and some U.S. officials have said prosecutors are building a case against Pyongyang in the Bangladesh Bank theft.

No conclusive proof has been provided and no criminal charges have yet been filed. North Korea has also denied being behind the Sony and banking attacks.

North Korea is one of the most closed countries in the world and any details of its clandestine operations are difficult to obtain. But experts who study the reclusive country and defectors who have ended up in South Korea or the West have provided some clues.

Kim Heung-kwang, a former computer science professor in North Korea who defected to the South in 2004 and still has sources inside North Korea, said Pyongyang's cyber attacks aimed at raising cash are likely organized by Unit 180, a part of the Reconnaissance General Bureau (RGB), its main overseas intelligence agency.

"Unit 180 is engaged in hacking financial institutions (by) breaching and withdrawing

PICTURES

money out of bank accounts," Kim told Reuters. He has previously said that some of his former students have joined North Korea's Strategic Cyber Command, its cyber-army.

"The hackers go overseas to find somewhere with better internet services than North Korea so as not to leave a trace," Kim added. He said it was likely they went under the cover of being employees of trading firms, overseas branches of North Korean companies, or joint ventures in China or Southeast Asia.

James Lewis, a North Korea expert at the Washington-based Center for Strategic and International Studies, said Pyongyang first used hacking as a tool for espionage and then political harassment against South Korean and U.S. targets.

"They changed after Sony by using hacking to support criminal activities to generate hard currency for the regime," he said.

"So far, it's worked as well or better as drugs, counterfeiting, smuggling – all their usual tricks," Lewis said.

COST-EFFECTIVE, DENIABLE

The U.S. Department of Defense said in a report submitted to Congress last year that North Korea likely "views cyber as a cost-effective, asymmetric, deniable tool that it can employ with little risk from reprisal attacks, in part because its networks are largely separated from the Internet".

"It is likely to use Internet infrastructure from third-party nations," the report said.

South Korean officials say they have considerable evidence of North Korea's cyber warfare operations.

"North Korea is carrying out cyber attacks through third countries to cover up the origin of the attacks and using their information and communication technology infrastructure," Ahn Chong-ghee, South Korea's vice foreign minister, told Reuters in written comments.

Besides the Bangladesh Bank heist, he said Pyongyang was also suspected in attacks on banks in the Philippines, Vietnam and Poland.

In June last year, police said the North hacked into more than 140,000 computers at 160 South Korean companies and government agencies, planting malicious code as part of a long-term plan to lay the groundwork for a massive cyber attack on its rival.

North Korea was also suspected of staging cyber attacks against the South Korean nuclear reactor operator in 2014, although it denied any involvement.

That attack was conducted from a base in China, according to Simon Choi, a senior security researcher at Seoul-based anti-virus company Hauri Inc.

"They operate there so that regardless of what kind of project they do, they have Chinese IP addresses," said Choi, who has conducted extensive research into North Korea's hacking capabilities.

MALAYSIA LINK

Malaysia has also been a base for North Korean cyber operations, according to Yoo Dong-ryul, a former South Korean police researcher who studied North Korean espionage techniques for 25 years.

"They work in trading or IT programming companies on the surface," Yoo told Reuters. "Some of them run websites and sell game and gambling programs".

Two IT firms in Malaysia have links to North Korea's RGB spy agency, according to a Reuters investigation this year, although there was no suggestion either of them was involved in hacking.

ALSO IN CYBER RISK

Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings

Wikipedia can pursue NSA surveillance lawsuit: U.S. appeals court

Survivors of Manchester attack

SPONSORED **TOPICS**

Michael Madden, a U.S.-based expert on the North Korean leadership, said Unit 180 was one of many elite cyber warfare groups in the North Korean intelligence community.

"The personnel are recruited from senior middle schools and receive advanced training at some elite training institutions," Madden told Reuters.

"They have a certain amount of autonomy in their missions and tasking as well," he said, adding that they could be operating from hotels in China or Eastern Europe.

In the United States, officials said there was no conclusive evidence that North Korea was behind the WannaCry ransomware, but that was no reason to be complacent.

"Whether or not they are directly involved with ransomware doesn't change the fact that they are a real cyber threat," said a senior administration official, who spoke on condition of anonymity.

Dmitri Alperovitch, co-founder of prominent U.S. security firm CrowdStrike Inc, added: "Their capabilities have improved steadily over time, and we consider them to be a threat actor that is capable of inflicting significant damage on U.S. private or government networks."

(To view a graphic on 'Don't click: The ransomware WannaCry worm' click here)

(Additional reporting by David Brunnstrom in Washington, Joseph Menn in San Francisco,; Rozanna Latiff and Tom Allard in Kuala Lumpur; Editing by Raju Gopalakrishnan)

NEXT IN CYBER RISK

Newly discovered vulnerability raises fears of another WannaCry

SINGAPORE A newly found flaw in widely used networking software leaves tens of thousands of computers potentially vulnerable to an attack similar to that caused by WannaCry, which infected more than 300,000 computers worldwide, cybersecurity researchers said on Thursday.

Former CIA chief says he warned Moscow over election hacking

WASHINGTON Former CIA Director John Brennan said on Tuesday it became clear last summer that Russia was attempting to interfere in the U.S. presidential election, and that he warned the head of Russia's FSB security service that such interference would hurt U.S. ties.

MORE FROM **REUTERS**

SPONSORED **CONTENT**

FROM AROUND THE **WEB**

Promoted by Revcontent

Follow Reuters:

Subscribe: **Feeds** | **Newsletters** | **Podcasts** | **Apps**

Reuters News Agency | **Brand Attribution Guidelines** | **Careers**