Studies: Cyberspying targeted SKorea, US military

July 8 2013, by Martha Mendoza

In this July 3, 2013 photo, Chris Palm, director of corporate communications, runs a demonstration of global computer virus activity inside the war room at the McAfee headquarters in Santa Clara, Calif. The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years. Researchers at the McAfee Labs said the malware was designed to find and upload information referring to U.S. forces in South Korea, joint exercises or even the word "secret." (AP Photo/Marcio Jose Sanchez)

The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years.

The identities of the hackers, and the value of any information they have acquired, are not known to U.S. and South Korean researchers who have studied line after line of computer code. But they do not dispute South Korean claims that North Korea is responsible, and other experts say the links to military spying add fuel to Seoul's allegations.

Researchers at Santa Clara, California-based McAfee Labs said the malware was designed to find and upload information referring to U.S. forces in South Korea, joint exercises or even the word "secret."

McAfee said versions of the malware have infected many websites in an ongoing attack that it calls Operation Troy because the code is peppered with references to the ancient city. McAfee said that in 2009, malware was implanted into a social media website used by military personnel in South Korea.

"This goes deeper than anyone had understood to date, and it's not just attacks: It's military espionage," said Ryan Sherstobitoff, a senior threat researcher at McAfee who gave The Associated Press a report that the company is releasing later this week. He analyzed code samples shared by U.S. government partners and private customers.

McAfee found versions of the keyword-searching malware dating to 2009. A South Korean cybersecurity researcher, Simon Choi, found versions of the code as early as 2007, with keyword-searching capabilities added in 2008. It was made by the same people who have also launched prior cyberattacks in South Korea over the last several

years, Choi said.

Versions of the code may still be trying to glean military secrets from infected computers. Sherstobitoff said the same coded fingerprints were found on an attack June 25—the anniversary of the start of the 1950-53 Korean War—in which websites for South Korea's president and prime minister were attacked. A day later the Pentagon said it was investigating reports that personal information about thousands of U.S. troops in South Korea had been posted online.

Sherstobitoff began his investigation after the March 20 cyberattack, known as the Dark Seoul Incident. It wiped clean tens of thousands of hard drives, including those belonging to three television networks and three banks in South Korea, disabling ATMs and other bank services. South Korea says no military computers were affected by Dark Seoul.

The code used in the shutdown is different from that used to hunt for military secrets, but they share so many characteristics that Sherstobitoff and Choi believe they were made by the same people.

Sherstobitoff said those responsible for the spying had infected computers by "spear phishing"—targeted attacks that trick users into giving up sensitive information by posing as a trusted entity. The hackers hijacked about a dozen obscure Korean-language religious, social and shopping websites to make it easier to pull secrets from infected computers without being detected.

The McAfee expert said the hackers have targeted government networks with military information for at least four years, using code that automatically searched infected computers for dozens of military terms in Korean, including "U.S. Army," "secret," "Joint Chiefs of Staff" and "Operation Key Resolve," an annual military exercise held by U.S. Forces Korea and the South Korean military.

The report does not identify the government networks that were targeted, but it does mention that in 2009, the code was used to infect a social media site used by military personnel living in South Korea. McAfee did not name the military social media site, nor release what language it is in, at the request of U.S. authorities who cited security issues. South Korea has a military force of 639,000 people, and the U.S. has 28,500 military personnel based in the country.

McAfee also said it listed only some of the keywords the malware searched for in its report. It said it withheld many other keywords that indicated the targeting of classified material, at the request of U.S. officials, due to the sensitivity of releasing specific names and programs.

"These included names of individuals, base locations, weapons systems and assets," said Sherstobitoff.

Choi, who works for a South Korean cybersecurity company, has made similar discoveries through IssueMakersLab, a research group he and other "white-hat" hackers created.

In this Friday, July 5, 2013 photo, a man walks by a sign at Cyber Terror Response Center of National Police Agency in Seoul, South Korea. The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years. (AP Photo/Lee Jin-man)

Results of a report Choi produced were published in April by Boan News, a Seoul-based website focused on South Korean security issues, but they did not get broad attention. That report included many search terms not included in the McAfee report, including the English-language equivalents of Korean keywords.

Both McAfee and IssueMakersLab found that any documents, reports and even PowerPoint files with military keywords on infected computers would have been copied and sent back to the attackers.

The attackers are also able to erase hard drives en masse by uploading malware and sending remote-control commands, which is what happened March 20.

Before that attack, hackers had been sending spy malware on domestic networks for months, giving them the ability to gather information about how their internal servers work, what websites the users visit and which computers are responsible for security, the researchers found. This information would have been crucial for planning the coordinated attacks on banks and TV networks.

Anti-virus software and safe practices such as avoiding links and attachments on suspicious emails can prevent computers from getting infected, but the March attack shows how difficult this can be to accomplish on a broad scale. Ironically, some of the malicious codes used were disguised as an anti-virus product from Ahnlab Inc., South Korea's largest anti-virus maker, said McAfee.

McAfee said it shared its findings with U.S. authorities in Seoul who are in close collaboration with South Korean military authorities.

Tim Junio, who studies cyberattacks at Stanford University's Center for International Security and Cooperation, said the McAfee report provides "pretty compelling evidence that North Korea is responsible" for the attacks in the South by tying the series of hacks to a single source, and by showing that users of a military social media site were targeted.

There are clues in the code as well. For example, a password, used again and again over the years to unlock encrypted files, had the number 38 in it, a politically loaded figure for two countries divided on the 38th parallel, security experts said.

Pentagon spokesman Army Lt. Col. James Gregory said the Defense

Department is aware of the study and looks forward to reviewing it.

"The Defense Department takes the threat of cyber espionage and cyber security very seriously, which is why we have taken steps to increase funding to strengthen capabilities and harden networks to mitigate against the risk of cyber espionage," he said.

South Korea's Defense Ministry says its secrets are safe. Ministry spokesman Kim Min-seok said officials were unaware of McAfee's study, but added that it's technically impossible to have lost classified reports because computers with military intelligence are not connected to the Internet. When accessing the Web, military officials use different computers disconnected from the internal military server, he said.

A hack of sensitive South Korean military computers from the Internet "cannot be done," Kim said. "It's physically separated."

Sherstobitoff, however, said it can be done, though he's not sure that it has been.

In July 3, 2013 photo, a global map tracks computer virus activity at the McAfee headquarters in Santa Clara, Calif. The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years. Researchers at the McAfee Labs said the malware was designed to find and upload information referring to U.S. forces in South Korea, joint exercises or even the word "secret." (AP Photo/Marcio Jose Sanchez)

"While it is not entirely impossible to extract information from a closed network that is disconnected from the Internet, it would require some extensive planning and understanding of the internal layout to stage such an exfiltration to the external world," he said.

Kwon Seok-chul, chief executive officer of Seoul-based cyber security firm Cuvepia Inc., said recent hacking incidents suggest that hackers

may have enough skills to infiltrate into the internal servers of Korean and U.S. military. Even if two networks are separated, he said, hackers will do anything to find some point where they converge.

"It takes time, but if you find the connection, you can still get into the internal server," Kwon said.

FBI Assistant Director Richard McFeely would not comment on McAfee's findings, but said in a written statement that "such reports often give the FBI a better understanding of the evolving cyber threat."

Neither the McAfee nor the IssueMakersLab reports suggest who is responsible for the cyberattacks, but many security experts believe North Korea is the likely culprit.

South Korean authorities have blamed the North for many cyberattacks on its government and military websites and have said they linked the March 20 attacks to at least six computers located in North Korea that were used to distribute malicious codes.

In this July 3, 2013 photo, the anatomy of a cyber attack is displayed at the McAfee headquarters in Santa Clara, Calif. The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years. Researchers at the McAfee Labs said the malware was designed to find and upload information referring to U.S. forces in South Korea, joint exercises or even the word "secret." (AP Photo/Marcio Jose Sanchez)

Several calling cards were left behind after the March attack, taunting victims. Two different and previously unknown groups separately took credit: The "Whois Hacking Team" posted pictures of skulls and a warning, while the "NewRomanic Cyber Army Team" said it had leaked private information from banks and media organizations.

"Hi, Dear Friends," began one such note. "We now have a great deal of personal information in our hands."

But McAfee says that claim, and others—including tweets and online rumors claiming credit for prior attacks—were meant to mislead the public and investigators, covering up the deeper spying program.

James Lewis, a senior fellow at the Center for Strategic and International Studies, said the attack is far more skillful and took place over a much longer period than was previously thought.

"I used to joke that it's hard for the North Koreans to have a cyber army because they don't have electricity, but it looks as if the regime has been investing heavily in this," said Lewis. "Clearly this was part of a larger effort to acquire strategic military information and to influence South Korean politics."

In this March 20, 2013 photo, depositors stand in front of automated teller machines of Shinhan Bank at a subway station as the bank's computer networks was paralyzed in Seoul, South Korea. The hackers who knocked out tens of thousands of South Korean computers simultaneously this year are out to do far

more than erase hard drives, cybersecurity firms say: They also are trying to steal South Korean and U.S. military secrets with a malicious set of codes they've been sending through the Internet for years. (AP Photo/Ahn Young-joon)

North Korean leader Kim Jong Un has made computer use and the importance of developing the IT sector hallmarks of his reign, devoting significant state resources toward science and technology. Though much of the country lacks steady electricity, a massive hydroelectric power station keeps the capital—and state computer centers—humming.

North Korean officials insist the emphasis on cyberwarfare is on protecting North Korea from cyberattacks, not waging them, but there is widespread suspicion that resources are also being poured into training scores of cyberwarriors as well.

Relatively few North Koreans are allowed to access the Internet—especially when compared to the South's hyper-wired society—but it too has seen its computer systems paralyzed by cyberattacks. Pyongyang blames the U.S. and South Korea and has warned of "merciless retaliation."