Experts see Korean parallels in Sony hack

December 4 2014, byBrandon Bailey And Youkyung Lee

In this June 25, 2013 file photo, a man walks by a gate at Cyber Terror Response Center of National Police Agency in Seoul, South Korea. Some cybersecurity experts say they've found striking similarities between the code used in the hack of Sony Pictures Entertainment and attacks blamed on North Korea which targeted South Korean companies last year. Sony has not commented on any Korean connection, except to deny a report Wednesday, Dec. 3, 2014 that it was poised to announce such a link. But three independent researchers told The Associated Press there are intriguing signs of a North Korean link to the attack, even as others warned it's difficult to make a definitive connection. (AP Photo/Lee Jin-man, File)

Some cybersecurity experts say they've found striking similarities

between the code used in the hack of Sony Pictures Entertainment and attacks blamed on North Korea which targeted South Korean companies and government agencies last year.

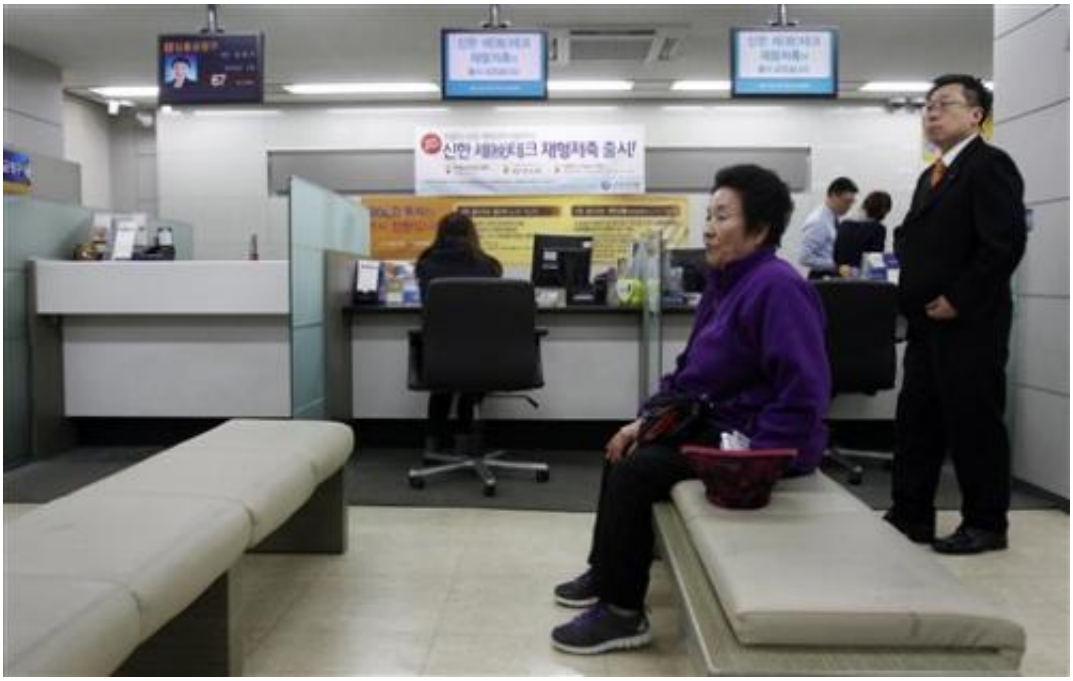
Sony is working with the FBI and Silicon Valley security firm FireEye to investigate the attacks that apparently gave access to unreleased movies as well as personnel records, technical documents and other material. It has not commented on any Korean connection, except to deny a report Wednesday that it was poised to announce such a link. The FBI and FireEye also had no comment Wednesday.

But three independent researchers told The Associated Press there are intriguing signs of a North Korean link to the attack, even as others warned it's difficult to make a definitive connection.

Analysts said they were able to examine code that was shared online after the FBI sent a flash alert to businesses this week, warning about a new threat from "destructive malware." While the FBI alert did not mention Sony Pictures by name, researchers said the alert listed Internet Protocol addresses that led them to samples of malware and references to Sony's internal network and passwords.

"We've seen it and it has a number of similarities to the attack code used in March 2013 during "Dark Seoul," said Tom Kellermann, chief cybersecurity officer for Trend Micro, a Japanese security company with operations in the United States. "Dark Seoul" refers to attacks last March and in June 2013 on South Korean companies and government servers, which the South Korean government blamed on the North.

Kellermann stopped short of saying the attack that crippled Sony's internal computer systems last week was definitely the work of North Korea. But he said, "There are strong indications of North Korean involvement. All roads lead to Rome here."



In this March 20, 2013 file photo, a customer sits in a branch of Shinhan Bank in Seoul, South Korea, after the bank's computer networks was paralyzed. Some cybersecurity experts say they've found striking similarities between the code used in the hack of Sony Pictures Entertainment and attacks blamed on North Korea which targeted South Korean companies last year. Sony has not commented on any Korean connection, except to deny a report Wednesday, Dec. 3, 2014 that it was poised to announce such a link. But three independent researchers told The Associated Press there are intriguing signs of a North Korean link to the attack, even as others warned it's difficult to make a definitive connection. (AP Photo/Ahn Young-joon, File)

Speculation about a North Korean link to the Sony hacking has centered on that country's angry denunciation of an upcoming Sony comedy film, in which two American journalists are sent to North Korea to assassinate its leader Kim Jong Un. North Korea has threatened "merciless" retaliation for the movie, saying its release would be an "act of war that we will never tolerate."

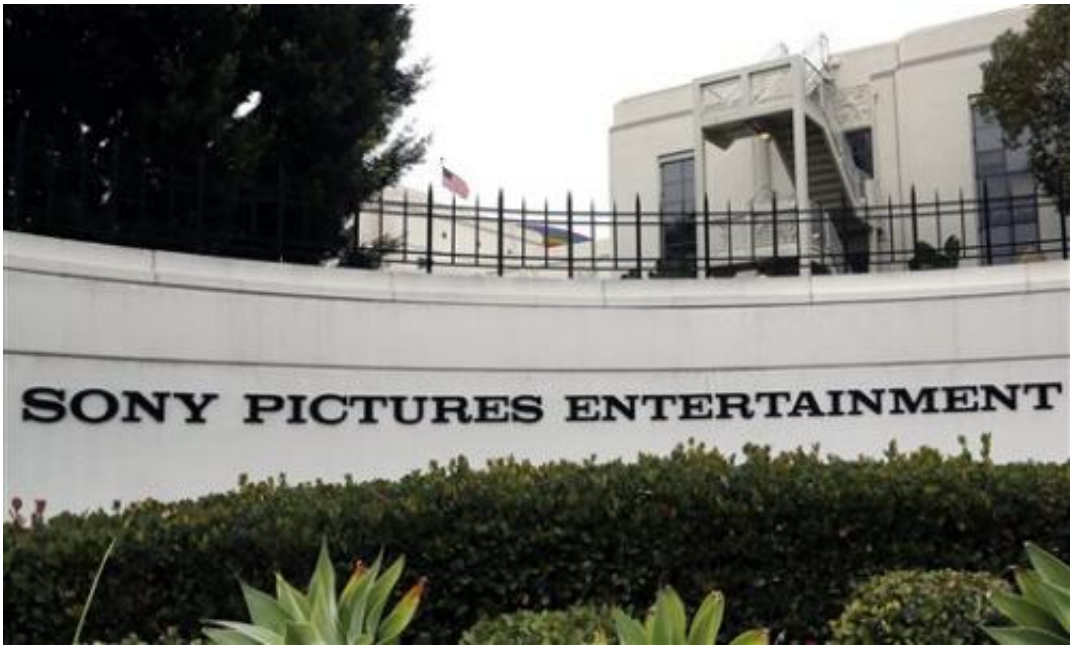
If the North Korean government were involved in the Sony hack, it would be a departure from the majority of high-profile computer hacks in recent years, which have been blamed on criminal groups seeking financial data or other valuable information. "It's a harbinger of a new era of hacking, one that's going to be far more problematic," said Kellermann.

It would also make the Sony hack the first known major North Korean cyber assault targeted outside South Korea. Seoul has recently stepped up the military's cyber warfare capabilities to better respond to what it sees as a growing cyber threat from Pyongyang.

There have been previous cyberattacks that were blamed on national governments. Bruce Schneier, a well-known cyber-security researcher and chief technology officer at Co3 Systems in Cambridge, Massachusetts, cited the so-called Stuxnet virus, which the New York Times has reported was developed by the United States and Israel to disrupt Iran's nuclear capabilities.

"Right now there is an arms race going on in cyberspace. Countries are building and stockpiling cyber weapons," Schneier said. He stressed that he had no conclusions about North Korean involvement in the Sony episode, adding that the notion of a government attack as retaliation for a movie is "just weird."

But Simon Choi, a senior security researcher at Seoul-based anti-virus company Hauri Inc., said a sample of malware from the Sony attack contained codes that were nearly the same as malware that wiped the hard drives of PCs at South Korean media companies on June 25, 2013. After an investigation, government officials attributed the attack to North Korea. "After I checked the (sample of) malware, I now see this was done by North Korea," he said.



In this Dec. 2, 2014 file photo, Sony Pictures Entertainment headquarters in Culver City, Calif. Some cybersecurity experts say they've found striking similarities between the code used in the hack of Sony Pictures Entertainment and attacks blamed on North Korea which targeted South Korean companies last year. Sony has not commented on any Korean connection, except to deny a report Wednesday, Dec. 3, 2014 that it was poised to announce such a link. But three independent researchers told The Associated Press there are intriguing signs of a North Korean link to the attack, even as others warned it's difficult to make a definitive connection. (AP Photo/Nick Ut, FIle)

Another similarity, Choi said, was that the Sony hackers left a screen image of a skull and messages that included links to the data that hackers grabbed from Sony's servers.

"That layout is exactly same with the screen image left on the Chung Wa Dae website when it was hacked on June 25," Choi said referring to the 2013 cyberattack on the South Korean presidential office. While it's not difficult to copy such a layout, Choi said it's highly unusual for hackers

to leave messages and links in that way.

In another intriguing development, Trend Micro analysts found indications that the Sony malware was created by someone using Korean-language programming tools, said Kellermann. He also said the hackers routed the attack through servers in Thailand, Italy and other countries, but researchers believe this was done to disguise the true source.

Experts at another security firm, AlienVault of San Mateo, California, reported similar findings, including evidence of Korean-language tools in the Sony malware. But the hackers could have used those tools to throw investigators off track, said AlienVault lab director Jaime Blasco. "In this world, you can fake everything, so it's really difficult to say" where the code originated.

Blasco said one thing is certain: "From the samples we obtained, we can say the attackers knew the Internal network of Sony." He said the malware contained coded names of Sony servers, user names and passwords.