Who hacked Sony becomes Internet's new mystery

December 24 2014, byTami Abdollah

In this Dec. 22, 2014, file photo, a South Korean army soldier walks near a TV screen showing an advertisement of Sony Picture's "The Interview," at the Seoul Railway Station in Seoul, South Korea. It seems everyone has a theory about who really hacked Sony Pictures Entertainment Inc. Despite President Barack Obama's conclusion that North Korea was the culprit, the Internet's newest game of whodunit continues. Top theories include disgruntled Sony insiders, hired hackers, other foreign governments or Internet hooligans. Even some experts are undecided, with questions about why the communist state would steal and leak gigabytes of data, email threats to some Sony employees and their families then threaten moviegoers who planned to watch "The Interview" on Christmas. (AP Photo/Ahn Young-joon)

Everyone has a theory about who really hacked Sony Pictures Entertainment Inc.

Despite President Barack Obama's conclusion that North Korea was the culprit, the Internet's newest game of whodunit continues. Top theories include disgruntled Sony insiders, hired hackers, other foreign governments or Internet hooligans. Even some experts are undecided, with questions about why the communist state would steal and leak gigabytes of data, email threats to some Sony employees and their families and then threaten moviegoers who planned to watch "The Interview" on Christmas.

"Somebody's done it. And right now this knowledge is known to God and whoever did it," said Martin Libicki, a cyber security expert at RAND in Arlington, Virginia, who thinks it probably was North Korea. "So we gather up a lot of evidence, and the evidence that the FBI has shown so far doesn't allow one to distinguish between somebody who is North Korea and somebody who wants to look like North Korea."

Perhaps the only point of agreement among those guessing is that even the most dramatic cybercrimes can be really, really hard to solve convincingly. When corporations are breached, investigators seldom focus on attributing the crime because their priority is assessing damage and preventing it from happening again.

"Attribution is a very hard game to play," said Mike Fey, president of security company Blue Coat Systems Inc. and former chief technology officer at McAfee Inc. "Like any criminal activity, how they get away with it is a very early step in the planning process, and framing another organization or individual is a great way to get away with something.

Fey added: "If they're smart enough and capable enough to commit a high profile attack, they're very often smart enough and capable enough

to masquerade as someone else. It can be very difficult to find that true smoking gun."

In a report earlier this month, Fey's company described a malicious software tool called Inception, in which attackers suggested a link to China, used home routers in South Korea, included comments in Hindi, with text in Arabic, the words "God_Save_The_Queen" in another string, and used other techniques to show links to the United States, Ukraine or Russia.

This Dec. 19, 2014, file photo shows an exterior view of the Sony Pictures Studios building is seen in Culver City, Calif. It seems everyone has a theory about who really hacked Sony Pictures Entertainment Inc. Despite President Barack Obama's conclusion that North Korea was the culprit, the Internet's newest game of whodunit continues. Top theories include disgruntled Sony insiders, hired hackers, other foreign governments or Internet hooligans. Even some experts are undecided, with questions about why the communist state

would steal and leak gigabytes of data, email threats to some Sony employees and their families then threaten moviegoers who planned to watch "The Interview" on Christmas. (AP Photo/Damian Dovarganes)

Unlike crimes in the physical world, forensic investigators in the cyber world can't dust for fingerprints or corroborate evidence by interviewing suspects. In prior closed-book cases, cyber criminals caught bragging online were only charged after evidence was found on their hard drives.

"The NSA (National Security Agency) has penetrated a lot of computers, but until Ed Snowden came around, nobody was certain because the NSA has the world's best operational security. They know how to cover their tracks and fingerprints very well," Libicki said.

After Sony was hacked, investigators analyzed network logs, the hacking tool and the remains of their crippled network. The investigation began after the attackers announced themselves and wiped the systems by crippling Sony's hard drives. Security professionals discovered that the hackers had been conducting surveillance on it since the spring. And if not for the theatrics of the Guardians of Peace, as the hackers call themselves, the breach could have easily continued for months without knowledge of the compromise.

Because North Korea is so isolated and its Internet infrastructure is not directly connected to the outside world, it's more difficult to trace attacks originating there. North Korea has vehemently denied that it was responsible for the attack.

To complicate matters, roughly 10 percent of home computers are compromised by hackers, allowing their use to conduct attacks on others, said Clifford Neuman, a director of the University of Southern

California Center for Computer Systems Security. These compromised machines become networks of computers controlled remotely by hackers and borrowed or rented in an underground economy.

Botnets "could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks or disrupt access to critical national infrastructure," Gordon Snow, then-assistant director of the FBI's cyber division, told a Senate panel in 2011.

The FBI worked with other U.S. agencies, including the National Security Agency, on the Sony investigation to trace the attacks. The FBI said clues included similarities to other tools developed by North Korea in specific lines of computer code, encryption algorithms and data deletion methods. It also discovered that computer Internet addresses known to be operated by North Korea were communicating directly with other computers used to deploy and control the hacking tools and collect the stolen Sony files.

The FBI said some of its evidence against North Korea was so sensitive it couldn't be revealed. Neuman said that could include reviewing evidence of communications or even recorded conversations between suspected hackers before or during the breach and subsequent leaks of Sony's confidential business information.

"Attribution to any high degree of certainty will always be impossible," said Chris Finan, a former White House cyber security adviser. "At some point these are always judgment calls. You can do things like corroborate using intelligence sources and methods. But ultimately you're still looking at a pool of evidence and you're drawing a conclusion."

Even knowing North Korea was involved doesn't mean others weren't, too.

"It's very difficult to understand the chain of command in something like this," Fey said. "Is this a hacking-for-hire scenario? Is it truly delivered by an organization? Or, is it possible there's some alternate nefarious plot under way none of us understand yet."

He later added: "One last idea. What if all this is just a movie-goer (who) can't stand the idea of another Seth Rogen movie?"