North Korea linked to Sony hacking (Update)

December 17 2014, byEric Tucker And Ted Bridis

This photo provided by Columbia Pictures - Sony shows, Seth Rogen, center, as Aaron, and James Franco, as Dave, arriving in North Korea to a welcoming crowd in a scene from Columbia Pictures' "The Interview." (AP Photo/Columbia Pictures - Sony, Ed Araquel)

Federal investigators have now connected the hacking of Sony Pictures Entertainment Inc. to North Korea, a U.S. official said Wednesday, though it remained unclear how the federal government would respond to a break-in that exposed sensitive documents and ultimately led to terrorist threats against moviegoers.

The official, who said a more formal statement might come soon, spoke on condition of anonymity because the official was not authorized to openly discuss an ongoing criminal case. A security professional with knowledge of the breach also said investigators had strong circumstantial evidence and technical commonalities pointing to North Korea.

Until Wednesday, the Obama administration had been saying it was not immediately clear who might have been responsible for the computer break-in. North Korea has publicly denied it was involved, though it did issue a statement earlier this month describing the hack as a "righteous deed."

The unidentified hackers had demanded that Sony cancel its release of the movie "The Interview," a comedy that included a gruesome scene depicting the assassination of North Korea's leader. Sony on Wednesday canceled the Dec. 25 release, citing the threats of violence at movie theaters that planned to show the movie, and later said there were no further plans to release the film.

The disclosure about North Korea's involvement came just after Sony hired FireEye Inc.'s Mandiant forensics unit, which last year published a landmark report with evidence accusing a Chinese Army organization, Unit 61398, of hacking into more than 140 companies over the years.

Tracing the origins of hacker break-ins and identities of those responsible is exceedingly difficult and often involves surmise and circumstantial evidence, but Mandiant's work on its highly regarded China investigation provides some clues to its methods.

Investigators typically disassemble any hacking tools left behind at the crime scene and scour them for unique characteristics that might identify who built or deployed them. Hints about origin might include a tool's programming code, how or when it was activated and where in the world it transmitted any stolen materials.

In some cases, investigators will trace break-ins by hackers to "command and control" computers or web servers, and logs in those machines or information in Internet registration records might provide further clues about who is behind the hack. Sometimes, hackers using aliases are identified on social media networks or in chat rooms discussing targets or techniques.

In the Sony breach, investigators first examined the malware, or malicious software, from the cyberattack. That was key because it had many commonalities with pre-existing malware—specifically Operation Troy and DarkSeoul—used in North Korea-linked cyberattacks on South Korean media and its financial institutions in recent years, according to the security professional, who was not authorized to discuss an ongoing investigation and spoke on condition of anonymity.

Security professionals looked at the code structure, the language setting and time zone, and then looked at what infrastructure the malware was using to communicate, the professional said. In the end, a singular IP address in Bolivia seemed to match the server used in the DarkSeoul attack, while two others led to Singapore and Thailand.

Because North Korea is highly controlled in its connection to the outside world, links back to it are almost always to proxies or presumed connections to the country, the security professional said.

Beyond the technical commonalities, the professional said, the circumstantial evidence was strong, including a June declaration by the North Korean foreign ministry that the movie would be considered an "act of war."

It wasn't immediately clear how the U.S. government was preparing to respond to the Sony hack. Bernadette Meehan, National Security Council spokeswoman, said the United States was "considering a range of options."

In May, the Justice Department took the highly unusual step of announcing indictments against five Chinese military officials accused of vast cyberespionage against major American corporations. But months later, none of those defendants has been prosecuted in the United States, illustrating the challenge of using the American criminal justice system against cybercriminals operating in foreign countries.

Jonathan Zittrain, a professor of law and computer science at Harvard University, said Sony was unquestionably facing anger over the breach and the resulting disclosure of thousands of sensitive documents. But the movie studio may be able to mitigate that reaction and potential legal exposure if it's established that North Korea was behind the attack.

"If Sony can characterize this as direct interference by or at the behest of a nation-state, might that somehow earn them the kind of immunity from liability that you might see other companies getting when there's physical terrorism involved, sponsored by a state?" Zittrain said.

Citation: North Korea linked to Sony hacking (Update) (2014, December 17) retrieved 20 March 2024 from https://phys.org/news/2014-12-probe-links-nkorea-sony-hacking.html