World Socialist Web Site wsws.org

Cybersecurity investigators raise doubts about North Korean responsibility for Sony hack

Niles Williamson
31 December 2014

On Monday, researchers from the Norse cybersecurity firm provided the FBI with evidence discovered in the course of their independent investigation into the hack of Sony Pictures Entertainment which allegedly points towards a small group of individuals including a disgruntled former employee and away from North Korea.

A group known as Guardians of Peace has claimed responsibility for the hacking attack and issued threats against theaters which were to screen “The Interview,” a comedy about the assassination of the North Korean leader, Kim Jong Un. In the face of the threats, Sony initially pulled the film from theaters throughout the US, but has since made the movie available online and in a limited number of theaters.

Pyongyang has officially denied any involvement in the hacking attack, and an offer by the regime to assist in any investigation into the leaks was rebuffed by the United States.

Kurt Stammberger, a senior vice president at Norse, told the *Security Ledger* that the company’s investigation uncovered six individuals directly involved in the hack including a former Sony employee who had been employed by the company for ten years before being laid off in May. The other suspects identified included two other individuals in the United States, one in Canada, one in Singapore, and a final suspect in Thailand.

Starting with the assumption that the attack was an inside job, the Norse researchers utilized leaked Human Resources data to identify recently laid-off Sony employees with the technical skills necessary to carry out the hack. They identified one possible suspect and followed her activity online, where they noted that she had made disgruntled posts on social media about Sony and the layoffs.

The Norse investigators also recorded conversations related to the Sony hacking attack on IRC (internet relay channel) forums where hackers communicate with each other online. The investigators were able to connect an individual involved in the IRC conversations with the former employee and a server on which one of the earliest known iterations of the malware used in the attack was assembled in July.

Norse’s allegations of an insider attack directly contradict the claims of the US government, which has explicitly blamed North Korea for the hack of Sony’s server network which resulted in the leaking of sensitive employee information and embarrassing emails from top executives.

The FBI released a statement on December 19 explicitly blaming the North Korean government for the hack. The agency claimed that its analysis of the malware used in the Sony attack “revealed links to other malware that the FBI knows North Korean actors previously developed.”

The statement also pointed to an overlap in the internet protocol addresses utilized in the attack and attacks previously connected to the North Korean government. It also claimed to have found similarities in the tools used in the Sony attack and attacks last year on South Korean banks and media firms.

The same day, President Barack Obama, in his final press conference of the year, blamed North Korea for the attack and promised that the US would carry out a “proportionate response” against the country “at the time and place of our choosing.”

Last Monday, several days after Obama’s warning, North Korea lost its connection to the Internet for several hours possibly as the result of a US cyber-attack. North Korean internet and mobile 3G network service went down again for several hours on Saturday.

The evidence put forward by the US government has been scrutinized by a number of internet security experts who argue that the government has not yet provided enough evidence to convincingly support its contention of North Korea’s responsibility.

Marc Rogers, principal security researcher for mobile security company CloudFlare, wrote in *The Daily Beast* that the evidence was “weak” and “flimsy.” He pointed to the fact that the malware shared source code with previous attacks is not unusual as hackers sell malware, and source codes often leak online.

Rogers noted that all but one of the IP addresses used in the attacks were public proxies utilized in prior malware attacks. Hackers often route their attacks through public proxies to avoid being traced back to their real IP address, meaning that it cannot be known exactly where the Sony attack originated.

According to Rogers, hard-coded paths and passwords in the malware indicated that whoever wrote the code had detailed knowledge of Sony’s servers and access to crucial passwords, things to which it would be much easier for someone on the inside to gain access.

Bruce Schneier, chief technology officer at Co3 Systems, writing in *The Atlantic*, expressed his deep skepticism about the evidence provided by the US government. According to Schneier, the evidence put forward by the FBI was “easy to fake, and it’s even easier to interpret it incorrectly.” He also pointed out that Korean language in the malware code would indicate Korean origin but would not directly implicate North Korea.

A linguistic analysis of online messages put out by Guardians of Peace published last week by the cybersecurity consultancy group Taia Global concluded that the nationality of the authors was most likely Russia and possibly, but not likely, Korean.