New American

Written by **C. Mitchell Shaw** on February 16, 2015

Published in the February 16, 2015 issue of the New American magazine. Vol. 31, No. 04

FBI Wrong on Sony Hack

After Sony Pictures was the victim of a sophisticated cyberattack just before Thanksgiving, they and the FBI were quick to point the finger of blame at North Korea, saying the attack was perpetrated in retaliation for the film *The Interview*. The media was quick to jump on the bandwagon and considered it a forgone conclusion that Pyongyang was behind what is almost certainly the largest data breach ever experienced by an American company. But many cybersecurity experts are saying that the available evidence doesn't support that conclusion. The evidence points, instead, to a hacktivist group calling itself "Guardians of Peace," which first attempted extortion, then when that failed, began a rolling release of Sony's data to the media and the web. The information that was leaked to news services and the Internet included personnel files, salaries and salary negotiations, employee Social Security numbers, unreleased scripts, and several movies (four of which had not even been shown in theaters yet).

After the FBI determined that North Korea was responsible, President Obama publicly accused Pyongyang and threatened a "proportional response." The first part of that, said the president, would be strict financial sanctions against the communist nation, made under authority he granted himself via an executive order. In a statement from the White House, Treasury Secretary Jacob Lew said:

> Today's actions are driven by our commitment to hold North Korea accountable for its destructive and destabilizing conduct. Even as the FBI continues its investigation into the cyber-attack against Sony Pictures Entertainment, these steps underscore that we will employ a broad set of tools to defend U.S. businesses and citizens, and to respond to attempts to undermine our values or threaten the national security of the United States. The actions taken today under the authority of the President's new Executive Order will further isolate key North Korean entities and disrupt the activities of close to a dozen critical North Korean operatives. We will continue to use this broad and powerful tool to expose the activities of North Korean government officials and entities.

FBI's Cursory Investigation

Much of the evidence that the FBI and Sony Pictures relies upon for their assertion that North Korea was involved has been called "flimsy" by the private-sector experts who have looked at it and other evidence. It also appears that the FBI has overlooked evidence that would be more valuable in determining the actual perpetrators. For instance, the FBI made much of the Korean programming language used in the intrusion into Sony's servers — though it is well known that hackers often use a variety of programming languages to disguise themselves and their locations — while not considering how the hackers knew exactly where to look for the data they stole. That data was stored on servers at Sony, and the hackers knew the names and passwords of those servers and hard coded that information into the malware they used in the attack. That knowledge indicates that someone inside Sony was involved in the breach.

As Kurt Stammberger, senior vice president of the computer security company Norse, told CBS News, "We are very confident that this was not an attack master-minded by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history…. Sony was not just hacked, this is a company that was essentially nuked from the inside." Stammberger is not alone in his thinking. Marc Rogers, who is a security researcher at the cloud security firm CloudFlare and also serves as director of security operations for the annual hacker convention DefCon, agrees. In a post for the Daily Beast, Rogers wrote, "Essentially, we are being left in a position where we are expected to just take agency promises at face value. In the current climate, that is a big ask." He also said that considering that Sony was planning to lay off a fairly large number of employees, "You don't have to stretch the imagination too far to consider that a disgruntled Sony employee might be at the heart of it all."

Though Norse had no involvement in the official Sony investigation, the company conducted its own inquiry into the matter. Whereas the FBI started with the presupposition that North Korea was behind the intrusion, Norse began with the knowledge that hacks of this nature usually involve current or former employees who are disgruntled. In an interesting turn of events, Norse used much of the leaked data from Sony to conduct its investigation. Poring over personnel files and other internal documents, Stammberger's team identified several current and former employees who might have been involved in the hack and subsequent leaks. Following web traffic, social media posts, and Internet Relay Chat (IRC) communications, they narrowed their investigation down to one woman, whom they identify only as "Lena," who had both motive and opportunity. She was an employee of Sony Pictures for 10 years before being laid off in May 2014. During her time at Sony, she was in a position that gave her access to the information used in the intrusion. And finally, she has ties to Guardians of Peace. "This woman was in precisely the right position and had the deep technical background she would need to locate the specific servers that were compromised," Stammberger said.

For their part, the FBI claims to have tracked some of the computers used to route the malware that devastated Sony's systems. The agency claims that these are the same computers used in attacks on banking and media institutions in South Korea last year. Those attacks are believed to have been North Korean in origin. But just because something is believed does not mean it is proven. The FBI is building presupposition upon presupposition. Even if North Korea were responsible for the attacks in South Korea last year, the fact that some of the same web servers routed traffic in both attacks is nothing like proof that the same persons are responsible for both attacks. Web traffic gets routed and re-routed to

different servers all the time. Hackers use tools such as TOR (anonymity software) and proxies not only to disguise their IP addresses, but also to route their traffic through servers that will disguise their location. The murky world of hacking is, after all, murky.

FBI Director James Comey has also said that part of what made the agency's job of tracking the malware back to North Korea possible was that on several occasions the hackers "got sloppy. Several times, either because they forgot or they had a technical problem, they connected directly, and we could see them. And we could see that the IP addresses that were being used … were coming from IPs that were exclusively used by the North Koreans," but that they seem to have immediately noticed their blunder and "shut it off very quickly" so as to avoid further detection. As if a group of hackers able to succeed in a hack of this size, scope, and sophistication would likely make a rookie mistake like that. And make it not once, but "several times." Marc Rogers expressed his doubt as well: "These guys literally burnt Sony down to hide their tracks and they staged everything pretty methodically. It would surprise me that somebody like that would make such a huge mistake to forget to use a proxy." It is far more likely that these "mistakes" were deliberate ruses. As Stammberger points out, "When we run all those leads to ground they turn out to be decoys or red herrings."

The Electronic Trail

Stammberger believes that the FBI was premature in placing blame on North Korea. "When the FBI made the announcement so soon after the initial hack was unveiled, everyone in the [cyber]intelligence community kind of raised their eyebrows at it, because it's really hard to pin this on anyone within days of the attack." Attribution is hard to determine in hacking cases. Most hacks are only ever attributed after someone or some group claims responsibility. In this case that is exactly what happened. Guardians of Peace immediately claimed responsibility.

When employees of Sony Pictures attempted to log on to their computers on November 24, they were greeted with an ominous message on their monitors: "Hacked by #GOP" — which included a graphic of a skeleton and several accusations against Sony Pictures, as well as threats that they would begin leaking the nearly 100 terabytes of data they had stolen. The message alluded to demands they had made that had not been met, leading many to speculate about what those demands might have been. The message read:

> We've already warned you, and this is just a beginning. We continue till our request be met. We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world. Determine what will you do till November the 24th, 11:00 PM(GMT). Post an email address and the following sentence on your twitter and facebook, and we'll contact the email address.

Thanks a lot to God'sApstls [sic] contributing your great effort to peace of the world. And even if you just try to seek out who we are, all of your data will be released at once.

The initials GOP refer to the hacktivist group Guardians of Peace. They appear to also use the name "God'sApstls." The group then used some of the stolen files to gain access to Twitter accounts belonging to Sony Pictures, using those Twitter accounts to publicly attack the company with statements about their business practices. Sony regained control of those accounts almost immediately.

As to the nature of the demands Sony was supposed to meet to avoid the leaking of troves of data, the best disclosure of that came out when the data was leaked. Part of that data was the e-mails of corporate executives. One of those e-mails, dated November 21, was addressed to executives at Sony Pictures, including CEO Michael Lynton and Chairwoman Amy Pascal. The e-mail hints at previous communications and demands that Sony pay extortion or suffer the consequences, "Monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole."

While Guardians of Peace/"God'sApstls" have claimed responsibility, North Korea has consistently denied any involvement in the cyberattack, even while saying it was a "righteous act." North Korea prides itself on not backing down in the face of Western pressure. It is unlikely that the Hermit Kingdom would deny something so grandiose if, indeed, it were responsible. Why not flout the hacking prowess of their elite geeks and put the West on notice?

The Interview Connection

Guardians of Peace has consistently denied being aligned with Pyongyang. They have also denied that *The Interview* was the motive for their assault on Sony Pictures. In a public statement the group said,

> We are an international organization including famous figures in the politics and society from several nations such as United States, United Kingdom and France. We are not under direction of any state. Our aim is not at the film The Interview as Sony Pictures suggests. But it is widely reported as if our activity is related to The Interview. This shows how dangerous film The Interview is. The Interview is very dangerous enough to cause a massive hack attack. Sony Pictures produced the film harming the regional peace and security and violating human rights for money. The news with The Interview fully acquaints us with the crimes of Sony Pictures. Like this, their activity is contrary to our philosophy. We struggle to fight against such greed of Sony Pictures.

The above statement, made one week after the attack that crippled Sony's systems, was the first mention of *The Interview* made by the hackers. Only after repeated speculation that the film was the motivation behind the attack did the hackers attempt to capitalize on the notoriety of the film. Three weeks after the attack, Guardians of Peace issued a threat to theaters that planned to show *The Interview* and the patrons who would go to see it. The threat made references to 9/11 and frightened theater owners sufficiently to cause them to refuse showing the film. The message, which was posted on Internet bulletin boards, said:

> Warning We will clearly show it to you at the very time and places "The Interview" be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time. (If your house is nearby, you'd better leave.) Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment. All the world will denounce the SONY. More to come…

The threat was hollow. The Department of Homeland Security issued a statement saying, "There is no

credible intelligence to indicate an active plot against movie theaters within the United States." After Sony worked out deals to show the film in about 500 theaters and via On Demand and streaming services, no terrorist attacks took place.

While it is unlikely that Guardians of Peace or "God'sApstls" really has famous members from the "politics and society" of several nations, it is obvious that English is not the primary language of this group. When linguists studied the e-mails and online messages of the group, they determined that there is little likelihood that whoever wrote the messages is North Korean. Computational linguists at cybersecurity firm Taia Global have determined, from the messages they analyzed, that "Korea[n] is still a possibility, but it's much less likely than Russia[n]." They made their determination based on the phrasing of the messages compared to the way different social groups speak.

One big question that has not been answered by those claiming that North Korea is behind the cyberattack on Sony Pictures Entertainment is why North Korea would go to all this trouble to stop this particular film. After all, in the recent past, there have been other movies that have cast North Korea in a very negative light and fed the perception that the totalitarian regime significantly threatens U.S. national security. Both the 2012 remake of *Red Dawn* and the 2013 film *Olympus Has Fallen* were critical of North Korea and showed the nation being defeated by the United States. Neither film resulted in attacks from North Korea against the film companies or anyone else involved.

The FBI is standing by its story. Having been presented with the fullness of Norse's investigation and briefed by investigators from the company, a spokeswoman for the agency said, "The FBI has concluded the government of North Korea is responsible for the theft and destruction of data on the network of Sony Pictures Entertainment. Attribution to North Korea is based on intelligence from the FBI, the U.S. intelligence community, DHS, foreign partners and the private sector. There is no credible information to indicate that any other individual is responsible for this cyber incident."

It appears that the FBI has its narrative, and anything that doesn't fit that narrative is dismissed without any serious consideration, even if it is presented by experts in the field. Cybersecurity expert Bruce Schneier said it best when he said that the evidence cited by the FBI is the type that is "easy to fake, and it's even easier to interpret it incorrectly."

Did We Know What They Know?

The FBI also now claims that as early as 2010 the NSA began installing an "early warning radar" system of secretive software that is hidden in the infrastructure of North Korea's Internet traffic to allow the agency to monitor and backtrack traffic from the despotic nation. They say this is their "smoking gun" proof that North Korea was responsible for the cyberattack on Sony Pictures. According to a report by the *New York Times*, the NSA monitored "spear phishing" attacks on Sony, which they claim originated in North Korea. Spear phishing is an attack using targeted e-mail that does not appear to be spam. When the unsuspecting victim clicks on a link in the e-mail, the link installs malicious computer code that infects the system. The FBI is claiming that a systems administrator at Sony fell prey to spear phishing, and North Korean hackers stole this person's login credentials, allowing them full access to the network. The hackers then spent two months — from the middle of September 2014 to the middle of November 2014 — mapping the network and preparing the hack before ex-filtrating 100 terabytes of data over Sony's Internet connection. This scenario requires that some serious questions be asked and answered.

Written by **C. Mitchell Shaw** on February 16, 2015

Published in the February 16, 2015 issue of the New American magazine. Vol. 31, No. 04

Holes in the story: The NSA claims to be able to monitor and backtrack traffic coming from Kim Jong-un's regime. If so, why did the agency not prevent the attack? *(Photo credit: AP Images)*

What is the likelihood that a professional network administrator — the very person responsible for assuring that others abide by carefully planned protocols for protecting system integrity — would not only fall for such a tactic, but remain totally unaware of it as his network is mapped and attacked?

How did the hackers plan and execute something of this magnitude in just two months, considering that experts agree it would take much longer — possibly even years?

How was 100 terabytes of data ex-filtrated over Sony's Internet connection without someone noticing anomalies in the network traffic?

Why did the NSA miss the attack and only notice it after the fact?

Until these questions can be adequately addressed, the FBI's claim seems just a little too convenient. Given the choice between those claims and the logical, reasonable, technologically sound answers offered by private-sector cybersecurity experts, the choice seems clear — especially considering that the motivation of those private-sector experts is to expose the hackers and their methods and to prevent future attacks of this type, while the FBI appears to be politically motivated.

Written by **C. Mitchell Shaw** on February 16, 2015
Published in the February 16, 2015 issue of the New American magazine. Vol. 31, No. 04