Written by **C. Mitchell Shaw** on January 22, 2015

NSA, FBI: "Smoking Gun" Shows North Korea Behind Sony Hack

FBI officials are now claiming that they have a smoking gun that proves it was North Korea that carried out the cyber-attack that devastated computer systems at Sony Pictures Entertainment last November and allowed hackers to steal and leak 100 terabytes of Sony's data to the Internet. As private sector cyber-security experts continue to present solid evidence that casts doubt on the FBI's claims that North Korea was behind the attack, the agency is now claiming that as early as 2010, the NSA had penetrated North Korea's Internet with an "'early warning radar" of software painstakingly hidden to monitor North Korea's activities."

The FBI says U.S. intelligence agencies used the penetration tools to monitor Internet traffic coming from North Korea and a base located in China used by North Korean hackers as the hackers attacked Sony's systems, the *New York Times* reported January 18. Of course, this penetration begs the question as to why U.S. intelligence did not detect the attack. According to anonymous sources who spoke to the *Times*, the NSA did not realize the severity of spear-phishing attacks North Korean hackers allegedly launched on Sony. (Spear-phishing is a targeted e-mail attack where the hacker sends an e-mail that looks legitimate but which contains a link that purports to be something the victim would have interest in. When the unsuspecting target clicks the link, malware is allowed to infiltrate the network, creating a back door the hackers use to come and go at will.) The sources claim that the spear-fishing attack enabled North Korean hackers to steal the login credentials of a systems administrator at Sony and that they then spent about two months planning and then executing what is probably the largest data-breach ever experienced by an American company.

There are reasons why many cyber-security experts doubt the FBI's account. For one, it requires that a professional systems administrator — the very person responsible for planning and enforcing protocols to protect the integrity of the networks at Sony — not only fall prey to a spear-fishing attack, but was then completely unaware of it as that attack was used to exfiltrate 100 terabytes of data across the network. It would be nearly unthinkable that that volume of data could be sent over the network without some type of alert being triggered. It also means that North Korea would have had to be able to receive that much data in a relatively short time frame — something experts say could not happen.

As *The New American* previously reported, Hector Monsegur, who used the name "Sabu" when he was associated with the infamous hacktivist groups Anonymous and LulzSec, explained, "It had to happen over a long period of time. You can not just exfiltrate … 100 terabytes of data in a matter of weeks. It's just not possible. It would have taken months, maybe even years to exfiltrate something like 100 terabytes of data without anyone noticing." He also claims that that much data flowing into North Korea

"would have shut down [the] North Korean Internet, completely," because of the country's Internet infrastructure.

A much more likely scenario (and one that is supported by evidence that anyone can examine for themselves) is that the hackivist group known as Guardians Of Peace, working with a disgruntled former employee of Sony, perpetrated the crippling attack on the entertainment giant. They appear to have had two purposes: extortion and revenge. The extortion — spelled out clearly in e-mails from the group to Sony executives in the weeks leading up to the attack — failed, as those executives either underestimated the hackers' abilities or figured that the destruction and pillaging would happen whether or not they paid.

The revenge was catastrophically successful. The hackers leaked everything from personnel records and sensitive e-mails to scripts for upcoming productions and several movies — some of which had not even been shown in theaters yet.

Private-sector computer security analysts presented the FBI with a trove of evidence — much of it garnered from leaked e-mails and personnel files — that point to a former employee named Lena who worked with Guardians Of Peace after she was dismissed in May 2014. The evidence shows a trail of online communications including e-mails, social media messages, and Internet Relay Chat (IRC) sessions proving her involvement with the hackitvists who claimed responsibility for the attack.

Kurt Stammberger, vice president of the computer security company Norse, and his team of investigators presented this evidence to the FBI; however, it seems to have fallen on deaf ears. A spokeswoman for the FBI stated, "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."

Many have wondered how, with so much evidence to the contrary, the FBI can make such a claim, and have suggested that the agency's decision to stick by its story is politically motivated. After the FBI determined that North Korea was responsible, President Obama publicly accused Pyongyang and threatened a "proportional response." The first part of that response, added the president, is strict financial sanctions against the communist nation, which he 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.

In one concise paragraph, the American people were told that the president had taken it upon himself "under the authority" he gave himself by an executive order to use tools that are are described as "broad and powerful" — tools he does not have the constitutional authority to use. If the attack on Sony

were shown to be simply the actions of a handful of angry nerds and one disgruntled former employee, instead of those of an emotionally unstable dictator, the premise on which he is building his "authority" would collapse like a house of cards.

Contitutionalists have noted that this looks like just another case of an overreaching president taking seriously the words of his mentor Rahm Emanuel about a previous crisis: "You never want a serious crisis to go to waste…. This crisis provides the opportunity for us to do things that you could not before."

Photo of North Korean soldiers: David Stanley