GlobalResearch
Center for Research on Globalization

Sony Hack Was an Inside Job; North Korea Scapegoated as Distraction Strategy

By J. D. Heyes
Global Research, December 31, 2014
Natural News

Theme: Intelligence, Media Disinformation

Did the FBI get it wrong when identifying who, or what entity, was responsible for the recent hack of Sony Pictures Entertainment?

Yes, according to cyber security experts who now say there is plenty of evidence suggesting that the hack was an *inside job*.

As reported December 30 by the *New York Post*, American cyber security firms have said they have concrete evidence that a former Sony worker helped to hack Sony Pictures computer system, and that the cyber attack was not masterminded by North Korean cyber terrorists.

The paper noted in online editions:

One leading cybersecurity firm, Norse Corp., said [*Dec. 29*] *it has narrowed its list of suspects to a group of six people — including at least one Sony veteran with the necessary technical background to carry out the attack, according to reports.*

That comes in direct conflict with earlier claims by the nation's top federal law enforcement agency, which blamed the cyber attack on North Korea within days of it making headlines. The announcement by the FBI had a direct financial effect on Sony; the company decided to delay a planned Christmas Day release of its latest film, *The Interview*, a spoof about two reality TV figures landing an interview with North Korean leader Kim Jong Un, only to be recruited by the CIA to assassinate him.

FBI is holding firm to its conclusions

The FBI's claims appeared early on to make sense, given the vanity of the young North Korea leader. But, alas, it appears as though that claim is falling apart.

Kurt Stammberger, senior vice president at Norse Corp., a cybersecurity firm, now says that he used Sony's leaked human-resources documents to cross-reference information with communications on hacker chat rooms, as well as the firm's own network of web sensors, to conclude that North Korea was not responsible for the hack.

"When the FBI made this announcement, just a few days after the attack was made public, it raised eyebrows in the community because it's hard to do that kind of an attribution that quickly — it's almost unheard of," Stammberger told *Bloomberg News*. "All the leads that we did turn up that had a Korean connection turned out to be dead ends."

Politico Pro reported that FBI agents investigating the hack have been briefed by Norse. Stammberger said after the meeting the agency was "very open and grateful for our data and assistance" but would not share any of its data and findings with his cybersecurity firm, though that was what the company expected.

The federal agency is standing firm in its determination of guilt.

"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," a spokeswoman said in a statement to *Politico Pro*. "There is no credible information to indicate that any other individual is responsible for this cyber incident."

"Strong evidence of an inside job"

The virus linked to the Sony attack was coded in a Korean language environment, reports have said. The *Post* added that the malware virus is similar to one that targeted South Korean banks and media companies in 2013. However, that's not enough to just link it to North Korea, according to Trend Micro, a software development firm, *Bloomberg News* reported.

The malware in question is available on the black market and can be used without a great amount of technical know-how.

"A lot of malware is kind of like a Roomba — it shuffles around the computer network, bumps into furniture and goes in spirals and looks for things kind of randomly," Stammberger told *Bloomberg*.

"This was much more like a cruise missile," he added. "This malware had specific server addresses, user IDs, passwords and credentials, it had certificates. This stuff was incredibly targeted. That is a very strong signal that an insider was involved."

Sources:

http://nypost.com

http://www.politico.com

http://www.bloomberg.com

Articles by: J. D. Heyes