GlobalResearch
Center for Research on Globalization

Sony Hack Blamed on North Korea Bears Hallmarks of U.S. Intelligence Operation

Obama administration mulling "proportional" response

By Kurt Nimmo
Global Research, December 19, 2014
Infowars 18 December 2014

Theme: Intelligence
In-depth Report: NORTH KOREA

The Obama administration considers Sony's inability to secure its computer network and allowing unknown hackers access to confidential information to be a serious breach of national security.

White House spokesman Josh Earnest did not say North Korea was responsible for the hack. Instead, the accusation was made Wednesday by an anonymous government official "who is not authorized to comment publicly."

Earnest said U.S. national security leaders "would be mindful of the fact that we need a proportional response." He was vague on what this meant.

As Paul Joseph Watson noted for Infowars.com on Thursday, there is little evidence implicating North Korea, but this has not prevented the government and the corporate media from attributing the hack to the authoritarian regime of Kim Jong-un.

For more on this, see Kim Zetter's The Evidence That North Korea Hacked Sony Is Flimsy.

U.S. Intelligence More Likely Responsible

As Marc W. Rogers noted on his security news blog on Thursday, it is unlikely North Korea is involved.

"The fact that the code was written on a PC with Korean locale & language actually makes it less likely to be North Korea," Rogers explains. "Not least because they don't speak traditional 'Korean' in North Korea, they speak their own dialect and traditional Korean is forbidden. This is one of the key things that has made communication with North Korean refugees difficult."

Additionally, the broken English used "looks deliberately bad and doesn't exhibit any of the classic comprehension mistakes you actually expect to see in 'Konglish'. i.e it reads to me like an English speaker pretending to be bad at writing English."

This would implicate U.S. or British intelligence. U.S. intelligence has, since 9/11, displayed careless and sloppy application when conducting false flag operations. The textbook example of this is the transparently bogus "intelligence" used in the effort to frame Iraq prior to the invasion of that country in 2003.

Another indicator pointing to U.S. intelligence is the familiarity with Sony's computer network. "It's clear from the hard-coded paths and passwords in the malware that whoever wrote it had extensive knowledge of Sony's internal architecture and access to key passwords," Rogers notes. "While it's plausible that an attacker could have built up this knowledge over time and then used it to make the malware, Occam's razor suggests the simpler explanation of an insider."

The attacker, however, does not necessarily have to be a Sony insider. As Edward Snowden and others have demonstrated, the NSA specializes in gaining access to computer networks and routinely penetrates the firewalls of corporate and foreign government networks.

Rogers writes the attack "suits a number of political agendas to have something that justifies sabre-rattling at North Korea, which is why I'm not that surprised to see politicians starting to point their fingers at the DPRK also."

It is true the U.S. foreign policy establishment has exploited the largely exaggerated and absurd national security threat supposedly presented by North Korea. However, they do not seriously consider it a threat and instead use it as an excuse to issue warnings to legitimize the national security state. Iran and terrorist entities, many designed by the intelligence apparatus, serve a similar purpose.

More practically, the Sony affair will be used to make the argument that cyber warfare poses an immediate threat to the national security of the United States and this threat demands a continuation and amplification of the surveillance state.

The surveillance state, however, is not turned outward, it is instead turned inward on the American people who are considered by the elite to be the true threat to their rule.

The Sony hack is not the work of an ex-Sony employee, as Rogers assumes. It is the work of the national security state and the NSA. Titillating details about movie stars and celebrities released as a result of the hack — falling on the heels of the celebrity nude photo hack earlier this year — serve the purpose of riveting the attention of the public on the affair while the government builds its case for further encroachments on their liberty.

The original source of this article is Infowars

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Kurt Nimmo

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in