Doubts remain on North Korea role in Sony attack (Update)

December 30 2014, by Rob Lever

Even after Washington pointed the finger at North Korea for the massive cyberattack on Sony Pictures, some experts say the evidence is far from clear cut.

President Barack Obama earlier this month took the unusual step of naming North Korea for the crippling attack, while promising that the United States would "respond proportionately" after the FBI said evidence pointed to Pyongyang.

But a number of cybersecurity specialists argue that links to North Korea are uncertain, and that some evidence leads elsewhere.

"I'm skeptical about the claim and I would be even more skeptical that the North Koreans did it on their own without help from a third party or government," said John Dickson, a former air force intelligence officer who is now a partner in the cybersecurity firm Denim Group.

The North Koreans "certainly have the will to poke us in the eye," but "don't have the critical mass skills of other nation states" to carry out an attack of this kind, Dickson told AFP.

Security technologist Bruce Schneier of Co3 Systems, also a fellow at Harvard's Berkman Center, said he also doubts the role of North Korea.

"The truth is we don't know," he said. "There are facts that are classified and not being released."

Schneier added that "even if we don't know (who is responsible), it makes sense for us to pretend we know because it serves as a warning to others."

In a blog post, Schneier said that "clues in the hackers' attack code seem to point in all directions at once... this sort of evidence is circumstantial at best. It's easy to fake, and it's even easier to interpret it incorrectly."

North Korea has been seen as the source of the malware, presumably due to anger at the cartoonish portrayal of the Pyongyang communist regime in the comedy film "The Interview."

But a linguistic-based analysis of the malware by the Israeli-based security firm Taia Global said the native language of the hackers appeared to be Russian, not Korean.

The study concluded that the software authors were not native English speakers, and that the translation errors pointed away from the Koreans.

"We tested for Korean, Mandarin Chinese, Russian and German," the report said. "Our preliminary results show that Sony's attackers were most likely Russian, possibly but not likely Korean and definitely not Mandarin Chinese or German."

Meanwhile, the politico.com website reported that the FBI was briefed Monday by the Norse cyber intelligence firm, which believes that laid-off Sony staff working in concert with hackers—not North Korea—were the culprits.

Classified intelligence

Security experts note that it is relatively easy for hackers to route their attacks through third parties to fake their location and that is nearly

impossible to conclusively show the source of an attack.

And Dickson notes that Washington is unlikely to reveal its intelligence sources in the Sony case "because the next set of attackers would change their tactics" to avoid detection.

Johannes Ullrich, dean of research at the SANS Technology Institute, said the attacks could have been carried out by independent hacker groups, possibly with help or direction from North Korea.

"Sometimes state actors use the hacker groups and stay at arm's length, but are helping these groups," he told AFP.

The free flow of information among hacker groups and rogue nations could mean multiple parties were involved, Ullrich said.

He noted that the Sony attack "did not require a high level of sophistication, but what it required was persistence, to find the weak spot to get in."

Contract hackers

Researcher Robert Graham at Errata Security said if North Korea had a role in the attacks, it may have been through outside hackers.

"North Korean hackers are trained as professional, nation state hackers," Graham said in a blog post.

"North Korea may certainly recruit foreign hackers into their teams, or contract out tasks to foreign groups, but it's unlikely their own cybersoldiers would behave in this way."

Other experts argue that the Obama administration would not publicly

name North Korea unless it had solid evidence.

"I'm amazed that people continue to have doubts," said James Lewis, a cybersecurity researcher at the Center for Strategic and International Studies. "People love conspiracy theories."

Lewis said US intelligence has the capability to locate the source of the attacks, and there is no domestic political need to blame North Korea.

"The intelligence community would never have let (Obama) stick his neck out on this unless they had a high degree of confidence about this," he said.

Paul Rosenzweig, a former US Homeland Security official who now heads a consulting group, said "it is worth considering the opposing view."

"In the post-Watergate/post-Snowden world, the (government) can no longer simply say 'trust us,'" he wrote in a post on the Lawfare blog.

"Not with the US public and not with other countries. Though the skepticism may not be warranted, it is real."

© 2014 AFP

Citation: Doubts remain on North Korea role in Sony attack (Update) (2014, December 30) retrieved 4 June 2023 from https://phys.org/news/2014-12-north-korea-role-sony.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.