GlobalResearch
Center for Research on Globalization

“The Interview”: Who Was Behind the Cyberattack on Sony?

By Gregory Elich

Global Research, December 31, 2014
Counterpunch

Region: Asia
In-depth Report: NORTH KOREA

The cyberattack on Sony Pictures unleashed a torrent of alarmist media reports, evoking the image of North Korean perfidy. Within a month, the FBI issued a statement declaring the North Korean government “responsible for these actions.” Amid the media frenzy, several senators and congresspersons called for tough action. Arizona Senator John McCain blustered, “It’s a new form of warfare that we’re involved in, and we need to react and react vigorously.” President Barack Obama announced his administration planned to review the possibility of placing North Korea on the list of states sponsoring terrorism, a move that would further tighten the already harsh sanctions on North Korea. “They caused a lot of damage, and we will respond,” Obama warned darkly. “We will respond proportionally, and we’ll respond in a place and time and manner that we choose.”

In the rush to judgment, few were asking for evidence, and none was provided. Computer security analysts, however, were vocal in their skepticism.

In its statement, the FBI offered only a few comments to back its attribution of North Korean responsibility. “Technical analysis of the data deletion malware used in the attack revealed links to other malware that the FBI knows North Korean actors previously developed,” it reported, including “similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.” The FBI went on to mention that the IP addresses used in the Sony hack were associated with “known North Korean infrastructure.” Tools used in the attack “have similarities to a cyberattack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.”

The major problem with the evidence offered by the FBI is that it is self-referential, all of it pointing back to the 2013 attack on South Korean banks and media that was carried out by the DarkSeoul gang. At that time, without supplying any supporting evidence, the United States accused North Korea of being behind DarkSeoul. In effect, the FBI argues that because the U.S. spread the rumor of North Korean involvement in the earlier attack, and some of the code is related, this proves that North Korea is also responsible for the Sony hack. One rumor points to another rumor as ‘proof,’ rendering the argument meaningless.

The logical fallacies are many. To date, no investigation has uncovered the identity of DarkSeoul, and nothing is known about the group. The linking of DarkSeoul to North Korea is purely speculative. “One point that can’t be said enough,” emphasizes Risk Based Security, “is that ‘attribution is hard’ given the nature of computer intrusions and how hard it is to ultimately trace an attack back to a given individual or group. Past attacks on Sony have not been solved, even years later. The idea that a mere two weeks into the investigation and there is positive attribution, enough to call this an act of war, seems dangerous and questionable.”

Consider some of the other flaws in the FBI’s statement. The IP addresses that were hard-coded in the malware used in the Sony hack belonged to servers located in Thailand, Poland, Italy, Bolivia, Singapore, Cypress, and the United States. The FBI implies that only the Democratic People’s Republic of Korea (DPRK – the formal name for North Korea) could have used these servers. The Thai port is a proxy that is commonly used in sending spam and malware. The same is true of the Polish and Italian servers. All of the servers used in the Sony attack have been previously compromised and are among the many computers that are widely known and used by hackers and spam distributors. Anyone with the knowhow can use them.

Whether or not these machines were used is another matter. Hackers often use proxy machines with phony IP addresses to mislead investigators. No hackers use their own computers to launch an attack. Vulnerable systems are hijacked in order to route traffic. For the FBI to point to IP addresses either reveals a fundamental misunderstanding of cybersecurity or a cynical attempt to deliberately mislead the public.

The Sony hack also bears similarities with the 2012 Shamoon cyberattack on computers belonging to Saudi Aramco. Those responsible for that attack have never been identified either, although the United States accused Iran without providing any evidence. Using the FBI’s logic, one could just as easily argue that the Sony hack was the work of Iran. One groundless accusation is used to buttress another. As evidentiary matter, it is worthless. It should also be recalled that in 1998, the United States blamed Iraq for the Solar Sunrise hack into Defense Department computers, only for it be ultimately revealed that it was the act of a few teenagers.

Nor do the similarities in code between the Sony hack and the earlier Shamoon and DarkSeoul attacks indicate a shared responsibility. Malware is freely available on the black market. Hackers operate by purchasing or borrowing, and then tweaking commonly available software, including both illegal and legal components. Code is shared among hackers on forums, and malware is assembled by linking various elements together.

One of the components used in the Sony cyberattack was the RawDisk library from EldoS, a commercial application that allows direct access to Windows hardware bypassing security. Anyone can legally purchase this software. There is nothing to tie it to the DPRK.

“There’s a lot of malware that’s shared between different groups, and all malware is built on top of older malware,” reports Brian Martin of Risk Based Security. “They’re also built on top of hacking tools. For example, you’ll find lots of malware that uses pieces of code from popular tools like Nmap. Does that mean that the guy who wrote Nmap is a malware author? No. Does it mean he works for North Korea? No.”

Robert Graham of Errata Security regards the evidence offered by the FBI as “complete nonsense. It sounds like they’ve decided on a conclusion and are trying to make the evidence fit.” Graham adds: “There is nothing unique in the software. We know that hackers share malware on forums. Every hacker in the world has all the source code available.”

Trojan-Destover, the malware used in the Sony cyberattack, included at least six components utilized earlier by Shamoon and DarkSeoul. “Even in such damaging scenarios, the cyber attacker’s tools are reused,” points out Sariel Moshe of CyActive. “For them, if it worked once, tweak it a bit and it will work again. The attack on Sony demonstrates quite clearly that this method works quite well." Indeed, while Shamoon and DarkSeoul are the most commonly mentioned predecessors to the Sony hack, it is thought that this software has been used on several occasions in the past against multiple targets.

The software utilized in the Sony cyberattack is atypical for a nation state. "It's a night and day difference in quality," says Craig Williams of Cisco's Talos Security Intelligence and Research Group. "The code is simplistic, not very complex, and not very obfuscated."

Four files used in the attack were compiled on a machine set to the Korean language. That fact proves nothing, notes computer security analyst Chris Davis. "That is pretty weak evidence. I could compile malware code that used Afrikaans and where the timestamp matched JoBerg in about five seconds." Any reasonably competent hacker would change the language setting in order to misdirect investigators. Had North Korean conducted this attack, it certainly would have taken the basic step of changing the language setting on the machine used to compile code.

What about North Korean resentment over Sony Picture's tasteless lowbrow comedy, *The Interview*, which portrays the assassination of DPRK leader Kim Jong-un? It is doubtful that Americans would find themselves any more amused by a foreign comedy on the subject of killing a U.S. president than the North Koreans are by *The Interview*.

Among the emails leaked by the cyberattack on Sony was a message from Bruce Bennett of the Rand Corporation. Bennett was a consultant on the film and opposed toning down the film's ending. "I have been clear that the assassination of Kim Jong-un is the most likely path to a collapse of the North Korean government," he wrote, adding that DVD leaks of the film into North Korea "will start some real thinking." In another message, Sony CEO Michael Lynton responded: "Bruce – Spoke to someone very senior in State (confidentially). He agreed with everything you have been saying. Everything." Lynton was also communicating with Robert King, U.S. Special Envoy for North Korean Human Rights Issues in regard to the film.

The Western media portray North Korean reaction to *The Interview* as overly sensitive and irrational, while U.S. officials and a Rand Corporation consultant saw the film as having the potential to inspire the real-life assassination of Kim Jong-un. The scene of Kim's assassination was not intended merely for so-called 'entertainment.'

The mass media raced to attribute the Sony hack to the DPRK, based on its reaction to the Sony film. A closer look at the cyberattack reveals a more likely culprit, however. The group taking responsibility for the hack calls itself 'Guardians of Peace', and in one of the malware files the alternate name of 'God'sApstls' is also used. In the initial attack, no reference was made to the film, nor was it mentioned in subsequent emails the attackers sent to Sony. Instead, the hackers attempted to extort money: "Monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as whole."

In an interview with CSO Online, a person represented as belonging to Guardians of Peace said the group is "an international organization…not under the direction of any state," and included members from several nations. "Our aim is not at the film *The Interview* as Sony Pictures suggests," the hacker wrote, but mentioned that the release of a film that had the potential of threatening peace was an example of the "greed of Sony Pictures."

For two weeks following the cyberattack, the media harped on the subject of North Korean culpability. Only after that point did the Guardians of Peace (GOP) make its first public reference to *The Interview*, denying any connection with the DPRK. Yet another week passed before the GOP denounced the movie and threatened to attack theaters showing the film.

It appears that the narrative of North Korean involvement repeated ad nauseam by the media and the U.S. government presented a gift to the hackers too tempting to pass up. The GOP played to the dominant theme and succeeded in solidifying the tendency to blame the DPRK, with the effect of ensuring that no investigation would pursue the group.

For its part, the Obama Administration chose to seize the opportunity to bolster its anti-North Korea policy in preference over tracking down the culprits.

There are strong indications that the cyberattack involved one or more disgruntled Sony employees or ex-employees, probably working together with experienced hackers. The malware used against Sony had been modified to include hard-coded file paths and server names. System administrator user names and passwords were also hard-coded. Only someone having full access with system administrator privileges to Sony's computer network could have obtained this information.

The GOP could have hacked into the Sony system months beforehand in order to gather that data. But it is more likely that someone with knowledge of Sony's network configuration provided the information. Arguing against the possibility that critical information had been siphoned beforehand through a hack, cybersecurity expert Hemanshu Nigam observes, "If terabytes of data left the Sony networks, their network detection systems would have noticed easily. It would also take months for a hacker to figure out the topography of the Sony networks to know where critical assets are stored and to have access to the decryption keys needed to open up the screeners that have been leaked."

The most likely motivation for the attack was revenge on the part of current or former Sony employees. "My money is on a disgruntled (possibly ex) employee of Sony," Marc Rogers of CloudFlare wrote. "Whoever did this is in it for the revenge. The info and access they had could have easily been used to cash out, yet, instead, they are making every effort to burn Sony down. Just think what they could have done with passwords to all of Sony's financial accounts."

Nation states never conduct such noisy hacking operations. Their goal is to quietly infiltrate a system and obtain information without detection. Sony had no data that would have been of interest to a nation state. Computer security blogger The Grugq wrote, "I can't see the DPRK putting this sort of valuable resource onto what is essentially a petty attack against a company that has no strategic value."

It would have been reckless for a North Korean team to draw attention to itself. Cybersecurity specialist Chris Davis says, "All the activity that was reported screams Script Kiddie to me. Not advanced state-sponsored attack." Davis adds, "Well, the stupid skeleton pic they splashed on all the screens on the workstations inside Sony…is not something a state-sponsored attack would do…Would ANY self-respecting state-sponsored actor use something as dumb as that?" The consensus among cybersecurity experts is clear, Davis argues. "The prevalent theory I am seeing in the closed security mailing lists is an internet group of laid off Sony employees."

Following his cybersecurity firm's investigation, Kurt Stammberger of Norse echoes that view. "Sony was not just hacked. This is a company that was essentially nuked from the inside. 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."

"What is striking here is how well they knew to exploit Sony's vulnerabilities," reports Nimrod Kozlovski of JVP Labs. "The malware itself is not creative or new; there are plenty of actors that could have manifested this particular attack." The hackers "knew more about the company, Sony, and its vulnerabilities than they knew, or needed to know, about hacking."

As an indication of the hacker's real motivation, it should be noted that the first communications focused on a different issue than the Sony film. The content of an email sent by the GOP to the IDG News Service refers to Sony's restructuring, in which thousands of employees lost their jobs: "Sony and Sony Pictures have made terrible racial discrimination and human rights violation, indiscriminate tyranny and restructuring in recent years. It has brought damage to a lot of people, some of whom are among us. Nowadays, Sony Pictures is about to prey on the weak with a plan of another indiscriminate restructuring for their own benefits. This became a decisive motive for our action." In an email to *The Verge*, the GOP wrote, "We want equality. Sony doesn't…We worked with other staff with similar interests to get in."

Seeking to diffuse tensions, North Korea proposed to conduct a joint investigation with the United States into the Sony cyberattack. Predictably, the United States quickly rebuffed the offer. National Security Council spokesman Mark Stroh arrogantly responded, "If the North Korean government wants to help, they can admit their culpability and compensate Sony for the damages this attack caused." North Korea can hardly be expected to accept blame for an act it did not commit. But getting to the truth of the matter was the farthest thing from the Obama Administration's mind. Similarly, U.S. officials are ignoring requests from cybersecurity experts to be allowed to analyze the Destover code. "They're worried we'll prove them wrong," Robert Graham concludes.

The Obama Administration's outrage over the Sony attack contains more than a small measure of hypocrisy. It was the United States that launched the Stuxnet attack that destroyed many of Iran's nuclear centrifuges. According to a *Washington Post* article published in 2013, the United States conducted 231 cyber operations throughout the world two years before. The National Security Agency, as is now well known, regularly hacks into computer networks, scooping up vast amounts of data. The GENIE program, the Post reported, was projected to have broken into and installed implants in 85,000 computers by the end of 2013. It was reported that GENIE's next phase would implement an automated system that could install "potentially millions of implants" for gathering data "and active attack." According to former deputy of defense secretary William J. Lynn III, "The policy debate has moved so that offensive options are more prominent now."

Contrast the mild treatment the media gave to the recent large-scale hacks into Target, Home Depot and JP Morgan, in which millions of credit cards and personal information were stolen, with the coverage of the cyberattack on Sony Pictures. It is impossible to avoid the conclusion that political considerations are driving the media furor over the latter case.

After six years in office, the Obama Administration has yet to engage in dialogue or diplomacy with North Korea. It prefers to maintain a wall of hostility, blocking any prospect of progress or understanding between the two nations.

Already, North Korean websites have been targeted by persistent denial of service operations. Whether the attacks were launched by a U.S. government cyber team or independent hackers inspired by media reports is not known. In any case, President Obama has already promised to take unspecified action against the DPRK. Actual responsibility for the Sony attack is irrelevant. Backed by media cheerleading, U.S officials are using the cyberattack as a pretext to ratchet up pressure on North Korea. Any action the Obama Administration takes is likely to trigger a response, and we could enter a dangerous feedback loop of action/counteraction.

Gregory Elich is on the Board of Directors of the Jasenovac Research Institute and the Advisory Board of the Korea Policy Institute. He is a member of the Committee to Defend Democracy in South Korea and a columnist for Voice of the People. He is also one of the co-authors ofKilling Democracy: CIA and Pentagon Operations in the Post-Soviet Period, published in the Russian language.

The original source of this article is Counterpunch

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Gregory Elich

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 print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca