No Hard Evidence that North Korea Hacked Sony

by Kim Zetter via rees - Wired *Friday, Dec 19 2014, 9:23am*
international / prose / post

> I suppose it is to be expected that the mass murdering criminal bastards that control the USA are again pumping propaganda regarding a hack of the Sony corporation, an exercise no doubt to compromise and justify a possible future target. The informed are in 'yawn' territory, however, the *Wired* article is worth a read as it is one of the few specialised sources that explains to lay people that the US line is a media beat-up based on extremely weak real evidence.

Story follows:

The Evidence That North Korea Hacked Sony Is Flimsy

Today Sony canceled the premiere of “The Interview” and its entire Christmas-Day release of the movie because of fears that terrorists might attack theaters showing the film.

The actions show just how much power the attackers behind the Sony hack have amassed in a short time. But who exactly are they?

1 The New York Times reported this evening that North Korea is “centrally involved” in the hack, citing unnamed U.S. intelligence officials. It’s unclear from the Times report what “centrally involved” means and whether the intelligence officials are saying the hackers were state-sponsored or actually agents of the state. The Times also notes that “It is not clear how the United States came to its determination that the North Korean regime played a central role in the Sony attacks.” The public evidence pointing at the Hermit Kingdom is flimsy.

Other theories of attribution focus on hacktivists—motivated by ideology, politics or something else—or disgruntled insiders who stole the data on their own or assisted outsiders in gaining access to it. Recently, the finger has pointed at China.

In the service of unraveling the attribution mess, we examined the known evidence for and against North Korea.

Attribution Is Difficult If Not Impossible

First off, we have to say that attribution in breaches is difficult. Assertions about who is behind any

attack should be treated with a hefty dose of skepticism. Skilled hackers use proxy machines and false IP addresses to cover their tracks or plant false clues inside their malware to throw investigators off their trail. When hackers are identified and apprehended, it's generally because they've made mistakes or because a cohort got arrested and turned informant.

Nation-state attacks often can be distinguished by their level of sophistication and modus operandi, but attribution is no less difficult. It's easy for attackers to plant false flags that point to North Korea or another nation as the culprit. And even when an attack appears to be nation-state, it can be difficult to know if the hackers are mercenaries acting alone or with state sponsorship—some hackers work freelance and get paid by a state only when they get access to an important system or useful intelligence; others work directly for a state or military. Then there are hacktivists, who can be confused with state actors because their geopolitical interests and motives jibe with a state's interests.

Distinguishing between all of these can be impossible unless you're an intelligence agency like the NSA, with vast reach into computers around the world, and can uncover evidence about attribution in ways that law enforcement agents legally cannot.

So let's look at what's known.

Sony and FBI Deny Connection to North Korea

First of all, Sony and the FBI have announced that they've found no evidence so far to tie North Korea to the attack. 2 New reports, however, indicate that intelligence officials who are not permitted to speak on the record have concluded that the North Koreans are behind the hack. But they have provided no evidence to support this and without knowing even what agency the officials belong to, it's difficult to know what to make of the claim. And we should point out that intelligence agencies and government officials have jumped to hasty conclusions or misled the public in the past because it was politically expedient.

Nation-state attacks aren't generally as noisy, or announce themselves with an image of a blazing skeleton posted to infected computers, as occurred in the Sony hack. Nor do they use a catchy nom-de-hack like Guardians of Peace to identify themselves. Nation-state attackers also generally don't chastise their victims for having poor security, as purported members of GOP have done in media interviews. Nor do such attacks involve posts of stolen data to Pastebin—the unofficial cloud repository of hackers—where sensitive company files belonging to Sony have been leaked. These are all hallmarks of hacktivists—groups like Anonymous and LulzSec, who thrive on targeting large corporations for ideological reasons or just the lulz, or by hackers sympathetic to a political cause.

Despite all of this, media outlets won't let the North Korea narrative go and don't seem to want to consider other options. If there's anything years of Law and Order reruns should tell us, it's that focusing on a single suspect can lead to exclusionary bias where clues that contradict the favored theory get ignored.

The Interview a Red Herring?

Initial and hasty media reports about the attackers pointed to cyberwarriors from North Korea, bent on seeking revenge for the Sony movie The Interview. This was based on a complaint North Korea made to the United Nations last July about the Seth Rogen and James Franco flick, which was originally slated to be released in October before being changed to Christmas Day. North Korea's UN ambassador said the comedy, about a TV host and his producer who get embroiled in an ill-

conceived CIA plot to assassinate North Korean President Kim Jong-un, was an act of war that promoted terrorism against North Korea.

“To allow the production and distribution of such a film on the assassination of an incumbent head of a sovereign state should be regarded as the most undisguised sponsoring of terrorism as well as an act of war,” UN ambassador Ja Song Nam wrote the UN secretary general in a letter. “The United States authorities should take immediate and appropriate actions to ban the production and distribution of the aforementioned film; otherwise, it will be fully responsible for encouraging and sponsoring terrorism.”

In other statements, North Korea threatened a “resolute and merciless” response if the U.S. didn’t ban the film.

But in their initial public statement, whoever hacked Sony made no mention of North Korea or the film. And in an email sent to Sony by the hackers, found in documents they leaked, there is also no mention of North Korea or the film. The email was sent to Sony executives on Nov. 21, a few days before the hack went public. Addressed to Sony Pictures CEO Michael Lynton, Chairwoman Amy Pascal and other executives, it appears to be an attempt at extortion, not an expression of political outrage or a threat of war.

“[M]onetary compensation we want,” the email read. “Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You’d better behave wisely.”

To make matters confusing, however, the email wasn’t signed by GOP or Guardians of Peace, who have taken credit for the hack, but by “God’sApstls,” a reference that also appeared in one of the malicious files used in the Sony hack.

A person purporting to be a Guardians of Peace spokesperson then emphasized again, in an interview with CSO Online published Dec. 1, that they are “an international organization … not under direction of any state.” The GOP’s members include, they wrote, “famous figures in the politics and society from several nations such as United States, United Kingdom and France.”

The person also said the Seth Rogen film was not the motive for the hack, but that the film was problematic nonetheless in that it exemplified Sony’s greed and fed political turmoil in the region:

“Our aim is not at the film The Interview as Sony Pictures suggests,” the person told CSO Online. “But it is widely reported as if our activity is related to The Interview. This shows how dangerous film The Interview is. The Interview is very dangerous enough to cause a massive hack attack. Sony Pictures produced the film harming the regional peace and security and violating human rights for money. The news with The Interview fully acquaints us with the crimes of Sony Pictures. Like this, their activity is contrary to our philosophy. We struggle to fight against such greed of Sony Pictures.”

It was only on December 8, after a week of media stories connecting North Korea and the Sony film to the hack, that the attackers made their first reference to the film in one of their public announcements. But they continued to trounce the theory that North Korea was behind their actions, and they denied ownership of an email sent to Sony staffers after the hack, threatening them and their families with harm if they didn’t denounce their employer.

At this point, it’s quite possible the media are guilty of inspiring the hacker’s narrative, since it was only after news reports tying the attack to the Sony film that GOP began condemning the movie in

public statements. This week the hackers have pounced on that narrative, using it to escalate the stakes by making oblique terrorist threats against the film's New York premiere and theaters scheduled to screen it Christmas day. Even if members of GOP lack the means or intent to pull off a terrorist attack on their own, they've now created an open invitation for opportunistic attackers to do so in their name—in essence, escalating their crimes and influence to a level no other hackers have achieved to date.

So why do some people continue to claim that North Korea is the culprit? There are two forensic discoveries that fuel this assertion, but they are flimsy.

Evidence: Malicious Files Point to Possible Korean Speakers

Four files that researchers have examined, which appear to be connected to the hack, seem to have been compiled on a machine that was using the Korean language. This refers to the encoding language on a computer; computer users can configure the encoding language so that content on their machine renders in a language they speak. But an attacker can set the language on a compilation machine to any language they want and, researchers note, can even manipulate information about the encoded language after a file is compiled to throw investigators off.

Evidence: Files Show Up In Other Hacks

The Sony attackers didn't just siphon data from the studio's networks, they also used a wiper component to destroy data. To do the wiping, they used a driver from a commercially-available product that had been used by other attackers before. The product, called RawDisk, uses drivers that allow administrators to securely delete data from hard drives or for forensic purposes to access memory.

The same product was used in similarly destructive attacks that hit Saudi Arabia and South Korea. Since some people have claimed those were both nation-state attacks—U.S. officials blamed Iran for the Saudi Arabia attack; South Korea blamed China and North Korea for its attack—people assume the Sony hack is also a nation-state attack. But the evidence pointing to those other attacks as nation-state attacks is also flimsy.

The 2012 attack in Saudi Arabia, dubbed Shamoon, wiped data from about 30,000 computers belonging to Saudi Aramco, the state-owned oil conglomerate. Although U.S. officials blamed Iran for it, researchers found that malware used in the attack contained sloppy code riddled with errors and attributed it to hacktivists with political motives rather than a nation-state. The malware displayed part of an image of a burning U.S. flag on infected machines before they were wiped. What's more, a group calling itself the Cutting Sword of Justice took credit for the hack. "This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression," they wrote in a Pastebin post. "We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression."

That sounds like a call to recruit other like-minded activists who might also be opposed to, say, a "criminal" company like Sony.

Last year, a similarly destructive attack, dubbed Dark Seoul by researchers, struck computers at banks and media companies in South Korea. The attack used a logic bomb, set to go off at a specific time, that wiped computers in a coordinated fashion. The attack wiped the hard drives and master boot records of computers at three banks and two media companies simultaneously, reportedly

putting some ATMs out of operation and preventing South Koreans from withdrawing cash from them. As with the Sony and Saudi Aramco hacks, the attackers used a RawDisk driver for their attack. They also left an image of a skull on the web site of the South Korean president's office. And an IP address used for one of the attackers' command-and-control servers matches an IP address the Sony hackers used for one of their command servers.

South Korea alternately blamed North Korea for the attack as well as China—since an IP address in China appeared to be part of the campaign. Officials later retracted the allegations.

The same group behind this attack are said to be behind other attacks in South Korea that occurred on the anniversary of the Korean War.

OK, So Who Hacked Sony?

Regardless of whether the Sony, Saudi Aramco and South Korea attacks are related, the evidence indicating they're nation-state attacks is circumstantial. And all of the same evidence could easily point to hacktivists. Our money is on the latter.

This is likely a group of various actors who coalesce and disperse, as the Anonymous hackers did, based on their common interests. But even with that said, there is another possibility with regard to the Sony hack: that the studio's networks weren't invaded by a single group but by many, some with political interests at heart and others bent on extortion. Therefore, we can't rule out the possibility that nation-state attackers were also in Sony's network or that a nation like North Korea was supportive of some of these hackers, since they shared similar anger over Sony. Another interesting scenario was recently posited by Deadline, suggesting that China may have initiated a breach at Sony during business negotiations with the studio last year, before handing off control to freelance hackers.

http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/
