KIM ZETTER SECURITY 02.12.16 9:00 AM

EVIDENCE SUGGESTS THE SONY HACKERS ARE ALIVE AND WELL AND STILL HACKING

Researchers Juan Andrés Guerrero-Saade (L) of Kaspersky Lab and Jaime Blasco of AlienVault Labs, speaking at the Kaspersky Security Analyst Summit in Spain. KIM ZETTER

TENERIFE, SPAIN—THE MASSIVE hack against Sony in late 2014 was sudden and loud. The perpetrators made themselves known four days before Thanksgiving with a red skull emblazoned on computer screens

company-wide and an ominous warning that they were about to spill Sony secrets.

A few days later they began to leak what they claimed was more than 100 terabytes of stolen data, including damaging emails and sensitive employee data. The scorched earth attack left Sony crippled for months after the attackers also destroyed data and systems on their way out the digital door, rendering some Sony servers inoperable in a move that cost the company an estimated $35 million in IT infrastructure repairs.

But a month later, after the US government blamed North Korea for the hack and some observers began calling the breach an act of terrorism, the attackers suddenly went silent. Or did they?

According to new data released this week by Juan Andrés Guerrero-Saade, senior security researcher with Kaspersky Lab's Global Research and Analysis Team, and Jaime Blasco who heads the Lab Intelligence and Research team at AlienVault Labs, the hackers behind the Sony breach are alive and well...and still hacking. Or at least evidence uncovered from hacks of various entities after the Sony breach, including South Korea's nuclear power plant operator and Samsung in South Korea, suggests this later activity has ties to the Sony case.

"[T]hey didn't disappear...not at all," Guerrero-Saade said during a presentation with Blasco this week at the Kaspersky Security Analyst Summit in Spain.

If true, it would mean the hackers who demonstrated an "extremely high" level of sophistication in the Sony attack have been dropping digital breadcrumbs for at least the last year, crumbs that researchers can now use to map their activity and see where they've been. The clues include—to name a few—re-used code, passwords, and obfuscation methods, as well as a hardcoded user agent list that showed up repeatedly in attacks, always with Mozilla consistently misspelled as "Mozillar."

They're thinking about publishing a paper describing their work, but likely won't reveal all the tricks they used to tie the hacks and malware families together, since they don't want to tip off the attackers to all the ways they can now be tracked.

How They Tracked the Hackers

They began their investigation with samples of the Destover malware—the destructive component that was responsible for overwriting the master boot record and other critical data on hacked Sony computers—and used them and other data to produce a "taxonomy" of related attacks.

They wrote a series of so-called YARA rules based on tiny similarities and quirks that stood out in the Sony samples and the attackers' techniques, which made them think that if they ever saw those quirks again, it would likely be in a breach conducted by the same guys. YARA is a tool for uncovering malicious files or patterns of suspicious activity on systems or networks that share similarities. YARA rules—essentially search strings—help analysts find, group, and categorize related malware samples and draw connections between them in order to build malware families and uncover groups of attacks that might otherwise go unnoticed.

Over the course of more than a year, they collected 400 to 500 malware samples used in attacks now believed to be related, as well as other digital footprints left behind by the group or groups of hackers behind the attacks. The method even allowed them to find related malware that had never been publicly reported by other security researchers before. "I think we've gotten quite accurate and good at finding the work of

these guys," Guerrero-Saade said about the attackers.

The YARA rules showed that the attackers were repeatedly using a lot of the same code, techniques and practices. But the tipping point came when they found a dropper used repeatedly in a number of attacks. Droppers are exploits that, when triggered, drop or install malware onto a victim's system. Often the dropper comes in the form of a phishing email with a malicious attachment; when the user clicks on the attachment, the dropper kicks into action and installs some malware.

In this case, they found several versions of the same dropper that was responsible for depositing several different families of malware that they initially believed were related, but couldn't verify until now. What tied them together was the fact that in each case the resource where the dropper's payload was hidden was protected with a unique password that was the same across all droppers used with different families of malware. The attackers were using the embedded password as an anti-analysis technique to prevent antivirus scanners and other automated security tools from executing the malicious file in order to examine it. Although the malware could use the password to launch the executable, automated tools could not see it and use it to launch the file.

Another clue that ended up being a Rosetta stone for the researchers involved a technique the attackers repeatedly used to automatically delete traces of their activity on victim machines. Although the attackers erased a lot of their tracks to thwart forensic investigators, they used a .BAT file—which got created on hacked systems on the fly—to do this. The file itself didn't remain on systems, but evidence of its creation and use did, so the researchers were able to look for these.

Other telling evidence that linked malware families and attacks was a custom list of sandboxes the malware was looking for. Sandboxes are virtual environments that are boxed off on a system so that any malware that tries to execute on them won't harm the system or network. Antivirus and other security products set up sandbox environments to automatically execute malware and study its behavior. The host names identifying some of these sandboxes can be found online. The attackers apparently drew up part of their list from this publicly available information, and if their malware encountered a system with a host name on their sandbox list, the malware avoided infecting that system. But their list also included names of sandboxes that are not publicly known.

"[T]hat's where it gets interesting," Guerrero-Saade told WIRED. "So it looks like they're paying attention to where their malware might be automatically executed … and when they see something that's consistent with a sandbox [that's not previously known], they're adding [the host name for that sandbox] to their list of names to watch out for." Their use of this changing list is relatively new. "It's something that's popped up in the last few weeks, and it's starting to pop up with increasing frequency as they integrate it into their code," he said.

Examining these and other similarities, the researchers were able to more definitively tie multiple malware families and attacks together that had previously been believed to be related to each other and link them to the Sony hack, and they could also do this for attacks and malware that they newly uncovered that had never been reported before. They were able, for example, to tie malware samples and attacks discovered in 2013 and known variously by different security firms as Operation Troy/DarkSeoul/Silent Chollima with malware and attacks discovered in 2014 and known as Hangman/Volgmer/TEMP.Hermit and with newer malware discovered in 2015 known as WildPositron and Duuzer.

They also were able to uncover and link recent attacks conducted in 2015 and 2016. These include malware and campaigns known as New

Troy.dll/AIMRAT and Sconlog/SSPPMID, both of which were discovered in 2015, and SpaSPE and Hangman_Samsung/mySingleMessenger, discovered in 2016. Guerrero-Saade says the MySingleMessenger malware campaign represented a particular coup for them, because it showed just how on-point some of their detection methods and YARA rules were. The MySingleMessanger campaign got widely reported this year as a campaign against Samsung in South Korea. After reading stories about it in the news, they decided to use their YARA rules to see if they could uncover samples but before they could they realized their system had already picked up samples before the campaign was publicly reported.

"For us the interesting thing was just seeing it as an indication of how well we've honed in on the [hackers'] toolkit," Guerrero-Saade says. "We opened the news and saw this [hack] and then went looking [for samples].... [W]e had actually caught those samples the week before."

All of this indicates that even though the attackers are changing their malware and methods to avoid detection, they're also keeping some things the same, which the researchers are using to catch up to them.

So Just Who Are These Attackers?

The researchers shied away from directly attributing them to North Korea, but in their presentation they called the attackers they were tracking "The Interviewers," a clear reference to the Seth Rogen and James Franco comedy *The Interview*, which the US government says was the motive for North Korea to hack Sony.

In all of the campaigns Guerrero-Saade and Blasco tracked for this research, they say the adversaries appear to have focused exclusively on targets in South Korea, and they've made the mistake several times of leaving Korean language in their files when they compiled their code. In a campaign exposed last September, the attackers explicitly targeted vulnerabilities in Hangul, a word processing program made by a South Korean company and used extensively by the South Korean government.

The so-called Hangman exploit the attackers created to exploit the Hangul software was used in a spear-phishing campaign to target someone working in South Korea's nuclear industry. The attacks targeting the Hangul software have been attributed to North Korean actors by FireEye, the computer security firm that investigated the Sony hack in 2014.

The seeming focus on South Korea, and the connection to the Sony hack which has been attributed to North Korea, would seem to suggest that North Korea—South Korea's greatest enemy—is behind all of these related attacks. But Guerrero-Saade says they didn't focus on victims in this stage of their research; instead they focused on understanding the practices of the attackers first. He noted that further investigation could turn up non-South Korean targets hacked by the same group.

Could the malware samples and attacks be coming from different groups who are simply sharing code? Guerrero-Saade said, "It could be seven different crews, it could be seven guys." He said if it is a couple of groups conducting all these attacks, this could explain some disparities in operational security they find in the attacks, where some are better than others at hiding and erasing their tracks. "[I]t might explain why in some cases you see certain developments and certain awareness of security research, in other cases kind of sloppy basic anti-analysis things," he said.

But Blasco says despite these differences the attacks share too many similarities to be conducted by completely different groups. In addition to code being reused among the hacks, the attacks all use the same so-called TTPs—tools, techniques and procedures. "We thought about it,"

Blasco told WIRED. “What if [these guys] are just sharing the code with different actors? But when you mix both things [code and TTPs] it’s [all] highly related.”

Regardless of whether it’s one group behind the attacks or many related groups, the two researchers refused to enter the attribution fray.

“At [Kaspersky] we do not do attribution,” Guerrero-Saade said during their talk. “[A] lot of people were very opinionated about what happened with Sony ….[but] rather than go through any discussions [here] about attribution, we’re [just] talking about a cluster of activity that is directly related to what has already been attributed by other people. Interpret that as you will.”

Asked later if he *does* think North Korea was behind the Sony hack—and by extension is also behind the other attacks they’ve connected to it—he would say only, “If people that are uniquely positioned to do attribution say that it’s a certain thing, then it all comes down to the trust you have in that claim.”

#CYBERSECURITY #HACKS AND CRACKS #KASPERSKY #NORTH KOREA #SONY HACK

MORE SECURITY

SECURITY

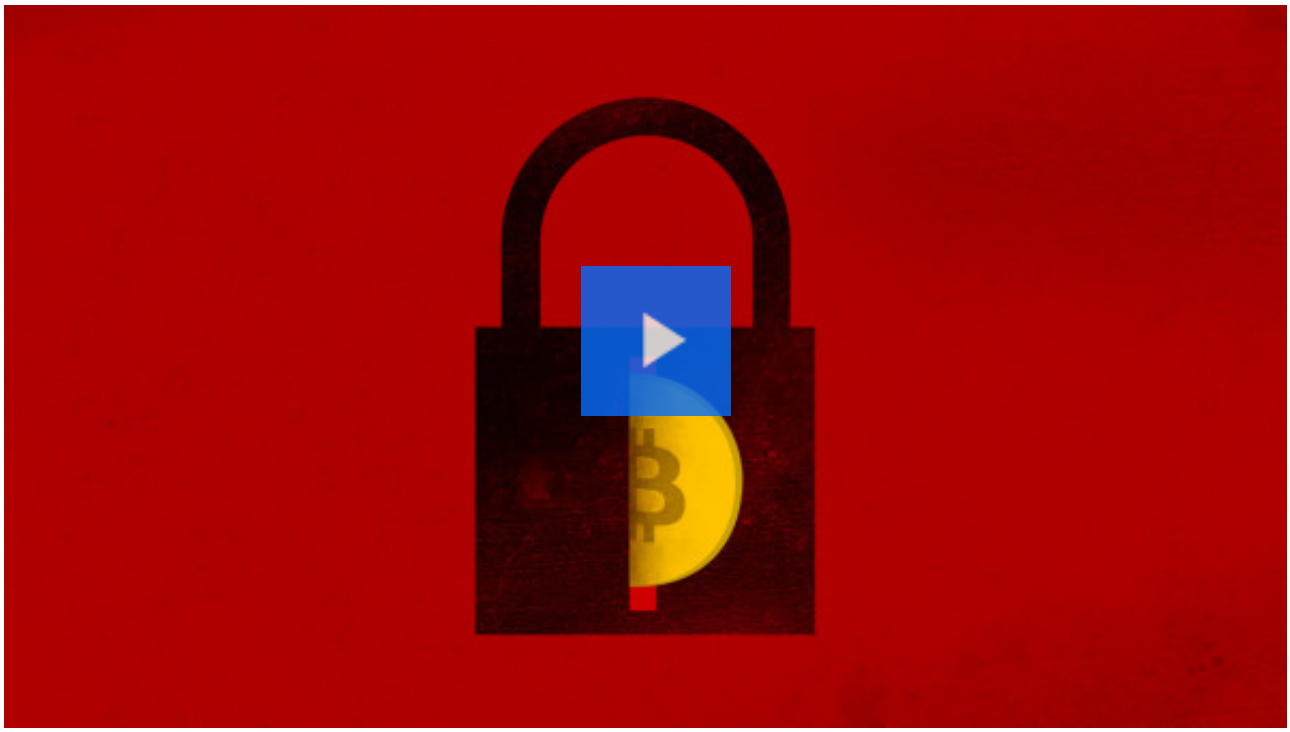
Security News This Week: The Government Wants to Listen In on Your Smart Home

2 DAYS

PSA

Don't Set Your iPhone Back to 1970, No Matter What

02.12.16



CYBERCRIME

Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise

09.17.15

SECURITY

New Bill Aims to Stop State-Level Decryption Before It Starts

02.10.16

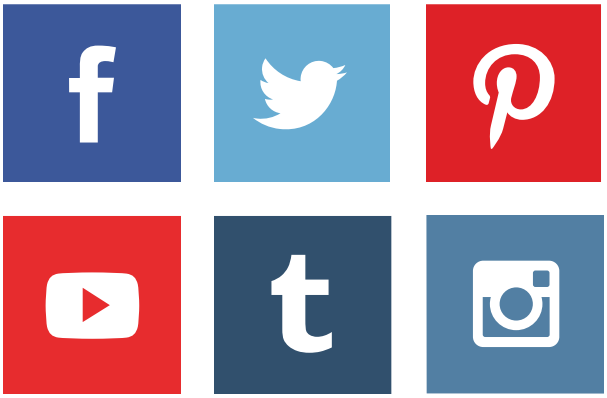
WIRED OPINION

Obama's Cybersecurity Plan is Meant to Secure His Legacy

02.10.16

WE RECOMMEND

WIRED



SUBSCRIBE	ADVERTISE
SITE MAP	PRESS CENTER
FAQ	CUSTOMER CARE
CONTACT US	NEWSLETTER
WIRED STAFF	JOBS
RSS	