



# Sony attackers thought to be behind multiple large attacks

Security researchers have found similarities in malware and attack methods and now know what digital breadcrumbs to follow



InfoWorld | Feb 12, 2016

Regardless of whether you think the attack against Sony in late 2014 was committed by North Koreans in order to stop a movie, there is new evidence that links the perpetrators to several other large attacks, including the phishing campaign using Samsung's messenger app My Single Messenger.

The attackers -- still at large -- breached Sony's networks, stole massive amounts of data, publicly dumped emails and sensitive employee data, and damaged systems badly enough that it cost Sony an estimated \$35 million in IT repairs. After the U.S. government and other experts pointed fingers at North Korea, the attackers ceased their public taunting and disappeared from sight.

**[ Watch out for 11 signs you've been hacked -- and learn how to fight back, in InfoWorld's PDF special report. | Discover how to secure your systems with InfoWorld's Security newsletter. ]**

While there was a lot of attention on trying to figure out who was behind the attack, very few in the security industry looked at what happened afterward.

"[The attackers] didn't disappear ... not at all," said Juan Andrés Guerrero-Saade, senior security researcher with Kaspersky Lab's Global Research and Analysis Team.

The group behind the Sony attack can be linked to several other acts of cyber espionage and malware attacks, a few going back to 2013, according to new data released at the Kaspersky Security Analyst Summit by Guerrero-Saade and Jaime Blasco, who heads the Lab Intelligence and Research team at AlienVault Labs.

They found that even though the attackers changed their methods and malware to avoid detection, a lot stayed the same -- such as passwords and code blocks -- which defenders can use to track them.

Guerrero-Saade and Blasco combined what they knew about the group's techniques and analyzed Destover -- the malware used in the Sony attack, which overwrote the master boot record and other critical data on infected systems -- to develop a "taxonomy" that could be used to identify similar attacks. They found quirks, such as code snippets that were reused across different malware samples, the same password reused in different parts of the attack, and similar obfuscation methods used to hide their activities. The group also repeatedly used a hardcoded user agent list where it consistently misspelled Mozilla as "Mozillar," for example.

Guerrero-Saade and Blasco felt that the patterns were unique enough that if they recurred in other attacks it would be a strong indicator the same group was behind them.

The researchers were "overwhelmed with the amount of malware" they uncovered, Guerrero-Saade said.

## **Yara connects the dots**

They developed Yara rules based on these quirks and found 400 to 500 malware samples used in different attacks. Yara helps analysts uncover malicious files or patterns of suspicious activity on systems or networks by searching for specific strings. Analysts can write rules to find, group, and categorize related files so that they can find connections between different attacks.

During their "Yara hunting spree," Guerrero-Saade and Blasco were able to link malware samples uncovered in 2013 from the Operation Troy campaign (also known as DarkSeoul or Silent Chollima) to samples associated with Hangman (also known as Volgmer or TEMP.Hermit) discovered in 2014. They were also able to link these samples to the malware used in WildPositron and Duuzer, uncovered in 2015, and uncovered links to more recent campaigns, including New Troy.dll/AIMRAT, Sonlog/SSPPMID, SpaSPE, Hangman\_Samsung/mySingleMessenger.

Hangman\_Samsung is the widely reported campaign that targeted Samsung's companywide messenger app, My Single Messenger, on Samsung's My Single intranet. Guerrero-Saade and Blasco found that their Yara rules were specific enough that it had

actually detected malware samples a few days before the campaign had been publicized. This was "an indication of how well we've honed in on the [hackers'] toolkit," Guerrero-Saade said.

The attackers also explicitly targeted zero-day vulnerabilities in Hangul, a South Korean word processing program used widely within the South Korean government. It was used in a spear-phishing campaign to target someone working in South Korea's nuclear industry back in September 2015. At the time, FireEye attributed the attacks to North Korean actors.

"I think we've gotten quite accurate and good at finding the work of these guys," Guerrero-Saade said.

## **Attackers left behind clues**

Guerrero-Saade and Blasco's Yara rules showed that these attackers were reusing the tools, techniques, and practices (TTPs), which led them to find previously unknown malware samples as well as links to existing attacks.

The rules led the researchers to several versions of a dropper -- a malicious executable that installs additional malware onto the victim's computer -- that had been previously used by different malware families. Researchers had long suspected the malware families were related, but didn't have any evidence linking them. Guerrero-Saade and Blasco found the definitive link: the dropper used the same embedded password in each of the campaigns.

The attackers dynamically created .BAT files on victims' systems to erase their activities and make it hard for security teams to piece together what they'd done. While they deleted the .BAT files themselves, the machines still had evidence the files had been created and used, which was a clue for forensics investigators.

The malware also profiled the system for specific sandboxes and to stop executing if it found any of those environments on the targeted system. There were 30 to 40 sandboxes on the list, and while most were widely known ones such as Adobe's sandbox, a few weren't public knowledge. The antisandbox "was a huge red flag," Blasco said.

The attackers several times mistakenly left traces of Korean in the files when compiling their code.

Guerrero-Saade and Blasco found the attackers did not rely on sinkholes or domain-based campaigns. The attacks frequently used hacked infrastructure, such as those consisting of compromised home routers on DSL networks. The attackers were also using SSL to secure malware communications with the command-and-control servers. While the use of SSL is

increasingly becoming common among different crews, Blasco said the combination of these four techniques would be a strong indicator this was the work of the same group that was behind the Sony attack.

## Defenders know what to look for

It is possible the similarities in malware and attack methods could be an indicator of extensive code-sharing between multiple groups. There are some disparities in attack methods -- such as the type of tools used to wipe systems after they are done -- which lend credence to the multiple group theory, but there are too many overlaps in code and similarities in the infrastructure used, Blasco said.

While the attackers appear to be focusing on South Korean targets, Guerrero-Saade and Blasco warned their malware sample size was still too small to definitively say the attackers are not looking at other victims around the world. Further analysis could find other victims in other countries, which could mean the North Koreans weren't behind the attacks after all.

"At [Kaspersky] we do not do attribution," Guerrero-Saade said. People are "very opinionated about what happened with Sony," but their research focused on cluster of activity that appears to be related without entering the realm of speculation.

Regardless of who the attackers may be, they are leaving enough digital breadcrumbs behind that security defenders can start looking for them to detect if their systems have been breached. While attack groups frequently change their methods, especially after researchers discover them, it is unlikely they will abandon all of the tools and techniques they are using.

"They would have to dump the entire codebase," Guerrero-Saade said.



**Fahmida Y. Rashid** — *Senior Writer*

Fahmida Y. Rashid is a senior writer at InfoWorld, whose coverage focuses on information security.




➤ **From CIO: 8 Free Online Courses to Grow Your Tech Skills**

 **View Comments**

## YOU MIGHT LIKE

---

Promoted Links by Taboola 

### ~~The Most Exciting MMORPG You've Ever Played. Don't miss this!~~

Sparta Online Games



Don Gates

You Had

[Sign In](#) | [Register](#)

### The 10 Most Popular European Cars in the U.S. - Carophile

Carophile

### The Ultimate Way to Get Cheap Hotel Rooms

Hotel Bargains

### Two Superpowers We Wish We Had

Melinda Gates

### Pirates: Finally a Free and Addictive Strategy Game!

Pirates - Online Game

### A huge Navy destroyer looks like a small boat on radar

### SpaceX rocket sticks landing, makes history

### How to buy a laptop in 2016: Everything you need to know

### How to Set Up and Optimize a Nexus Player [Tutorial]

Intel

