Lazarus: History of mysterious group behind infamous cyber attacks

medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c

Threat Intel November 16, 2017

Threat

Threat Intel

May 25, 2017

.

7 min read

The Lazarus group made headlines this week when Symantec researchers found strong evidence linking it to the WannaCry ransomware attacks that crippled computers all over the world earlier this month.

The group first came to broad international attention when it was implicated in the attacks on Sony in 2014, but it has been in operation since at least 2009.

History of attacks

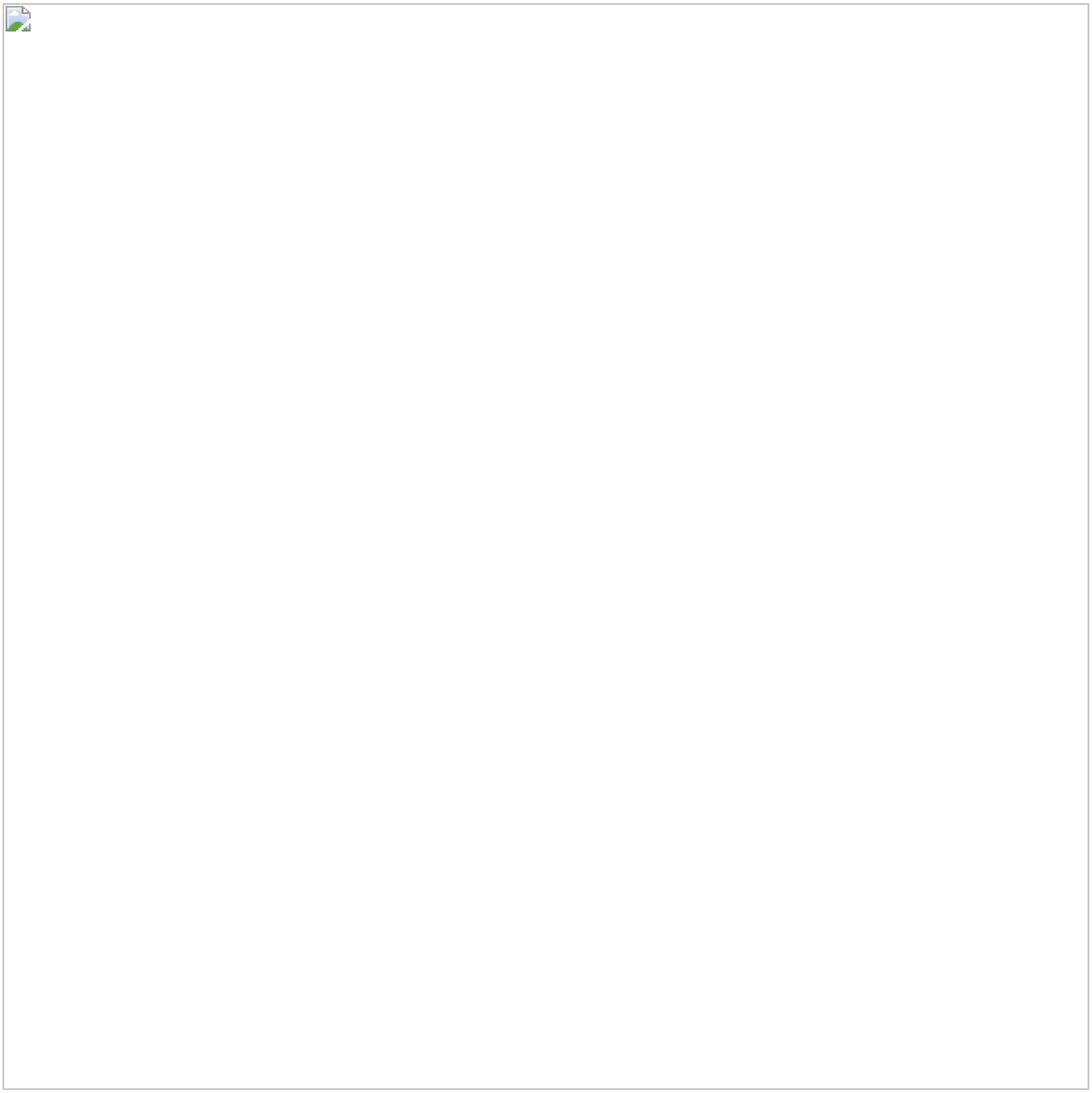
2009: Attacks on organizations in the U.S. and South Korea

In fact, it is possible that Lazarus was active as far back as 2007, but it first came to widespread attention in 2009, when a series of attacks starting on July 4 that year impacted several government, financial, and media websites in both the U.S. and South Korea. The attacks began in the U.S. on its independence day, and targeted institutions including the White House and the Pentagon. Later that week the websites of major government, financial, and media organizations in South Korea were hit.

These attacks were distributed denial of service (DDoS) attacks that aimed to take websites offline. The attackers used the Dozer malware (Trojan.Dozer) to carry out these attacks. The attacks, while disruptive, were relatively unsophisticated, but over the years Lazarus has refined its methods to carry out more sophisticated attacks. However, as can be seen in the WannaCry attacks to which it has been linked, it can still be prone to sloppiness.

2011: South Korean organizations targeted again

In 2011, organizations in South Korea were yet again targeted by DDoS attacks. Similar to 2009, a number of government and private websites were targeted, this time using a tool called Trojan.Koredos. This attack was unusual for a DDoS attack because it did not use a command and control (C&C) server; the commands were hidden inside the threat itself. The use of a tactic like this indicated a growth in sophistication from the group compared to the 2009 attacks. Symantec research into this threat also found that, as well as carrying out a DDoS attack, if the infected computers were not cleared of this Trojan the master boot record (MBR) of some of them would be destroyed within 10 days.



South Korea’s capital Seoul. South Korean organizations have been frequently targeted by Lazarus.

2013: Attacks become more destructive

In 2013, a destructive attack against banks and local broadcasting organizations in South Korea was reported. The attack defaced the website of a Korean ISP and also crippled servers belonging to a number of organizations. The websites of the companies affected went down in this attack, with a number of the organizations affected having the hard drives of many of their computers wiped. Wiping malware called Jokra (Trojan.Jokra) was used in this attack, which a group called ‘WhoIs’ originally claimed credit for in a message posted on computers during the attacks. However, Symantec and other security researchers believe that the Lazarus group was behind this attack, as well as the two previously mentioned attacks in 2011 and 2009.

Also in 2013, researchers spotted a piece of malware called Castov (Downloader.Castov and Infostealer.Castov) targeting South Korean financial institutions and their customers. In these attacks, which are also believed to originate from Lazarus, Castov was used to steal passwords, account details, and digital certificates from the computers it infected. Castov (Trojan.Castov) was also used in further DDoS attacks against South Korean targets in June 2013.

The Sony attacks

It was the attack on the computer systems of Sony Pictures Entertainment (SPE) in 2014 that brought the Lazarus group to widespread attention.

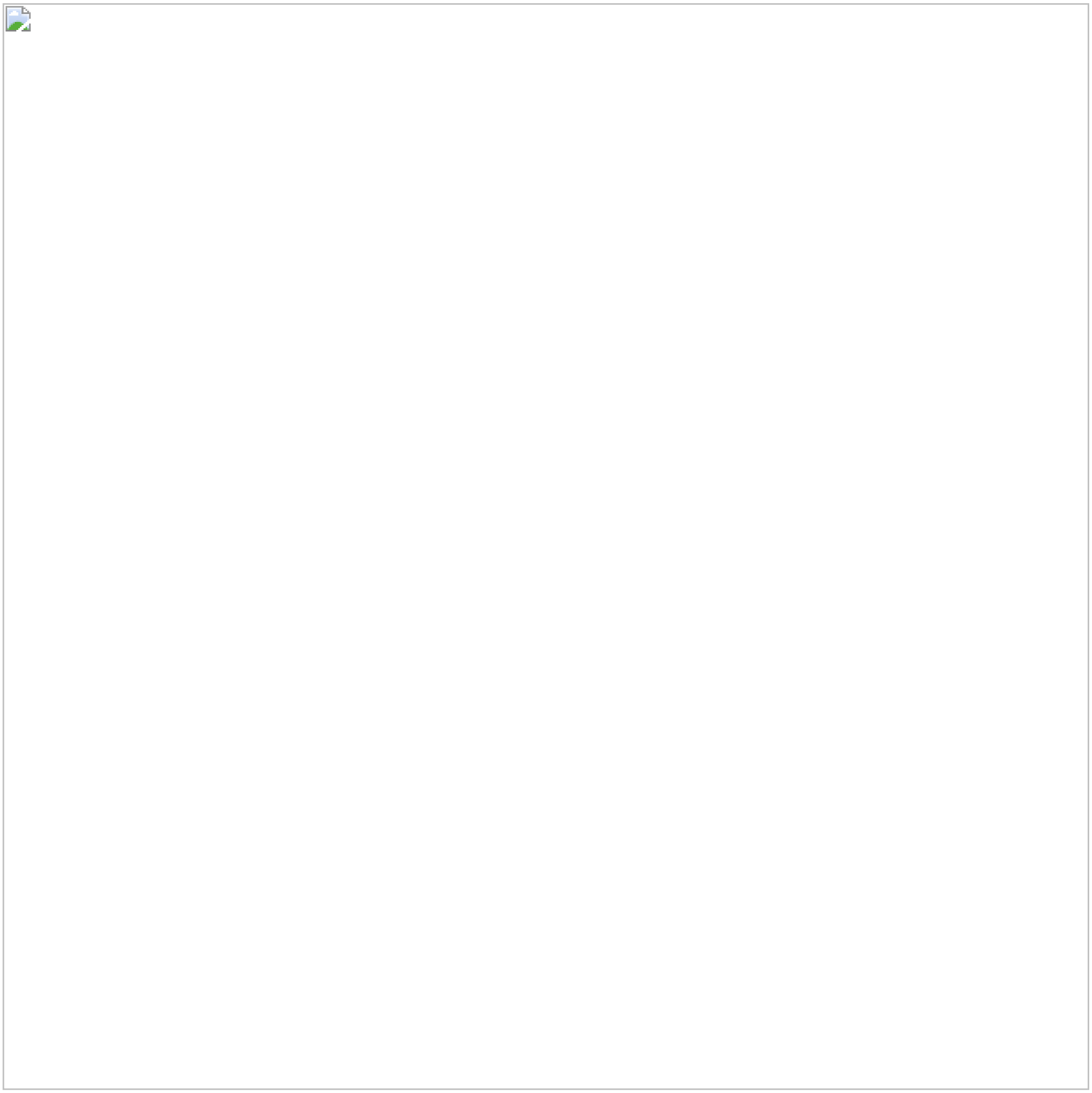
The attack on Sony Pictures became public knowledge on November 24, 2014, when Sony employees turned on their computers to be greeted with the sight of a neon red skeleton and the words “Hacked by GOP”, which stood for “Guardians of the Peace”. The message also threatened to release data later that day if an unspecified request was not met. Over the following weeks, huge swathes of information stolen from Sony were released, including: personal information about employees and their families; email correspondence between employees at the company; information about company salaries, unreleased Sony films, and other information.

Much of the leaked information, particularly some of the email correspondence between executives at the company, received a lot of coverage in the media and caused embarrassment for the company.

It’s not clear how long the hackers were on Sony’s systems before they released this information, but given how much data was obtained it is likely they maintained a presence for a few months at least.

As well as leaking this vast trove of data, the attackers also destroyed many computers in the organization using malware identified as Backdoor.Destover. Destover is a particularly destructive malware that can completely wipe infected systems. It was the subject of an FBI Flash Warning at the time. Flash Warnings are confidential alerts sent to businesses thought to be at risk from attackers. It is possible to configure Destover to only target computers in one particular organization, which is likely to have been the case in the Sony attack. Some of the tools and techniques used by Destover allowed researchers to link it to the previously mentioned 2013 attacks carried out against targets in South Korea, indicating the same group was responsible for both these attacks.

This attack was hugely high profile and received vast media coverage, with some executives at Sony even stepping down in its wake.



The Sony attacks, where were widely attributed to Lazarus, made headlines.

2015: Manufacturing industry in South Korea targeted

In October 2015, Symantec found evidence that organizations in South Korea were being targeted by a number of malicious tools, including Backdoor.Duuzer, W32.Brambul, and Backdoor.Joanap. These threats all appeared to originate from the same actors and seemed to have a focus on the South Korean manufacturing industry. The aim of these attacks appeared to be to steal data and information: cyber espionage.

SWIFT attacks

A cyber attack in February 2016 resulted in $81 million being stolen from the Bangladesh Central Bank, with the figure likely to have been much higher but for a typo and the vigilance of eagle-eyed bank officials who put a stop to the fraud before any more money was stolen. It is believed the attackers originally aimed to steal $1 billion.

The money was stolen through fraudulent SWIFT transactions, though the SWIFT system itself was not compromised, and malware (Trojan.BanSwift) was used to cover the attackers' tracks. Subsequent investigations by Symantec determined that the same attackers were behind similar attacks on other banks in Asia, including Vietnam's Tien Phong Bank, which said it had intercepted a fraudulent transfer of more than $1 million in the fourth quarter of 2015.

Code sharing between the BanSwift Trojan and Backdoor.Contopee, which had previously been observed being used by Lazarus, led researchers to determine that Lazarus was also behind these attacks.

The Bangladesh bank heist was a sophisticated and complex attack. Much of the $81 million stolen in this attack remains unrecovered.

2017: Banks targeted again

In February 2017, Symantec published an investigation into watering hole attacks that had attempted to infect more than 100 organizations in 31 different countries with a previously undiscovered malware called Downloader.Ratabanka. These attacks were highly targeted, with the majority of institutions targeted being banks, with a small number of telecoms and internet firms also on the list of targets. However, there was no evidence funds were successfully stolen from any of the banks in this attack.

Researchers from Symantec were able to establish a number of links between Ratabanka and tools previously associated with Lazarus, leading them to conclude with reasonable confidence that the group was behind these attempted attacks.

WannaCry rocks the world

The WannaCry ransomware attacks have received extensive coverage since a widespread attack on May 12 caused the systems of many large organizations around the world, including the NHS in the UK, to come to a juddering halt.

Symantec discovered evidence that an earlier version of WannaCry was used in targeted attacks on enterprises in February, March, and April, but the leak of the EternalBlue exploit code by the Shadow Brokers in April was seemingly a fortuitous occurrence for the attackers that allowed them to spread the ransomware much more widely.

Analysis of the early WannaCry attacks by Symantec revealed substantial commonalities in the tools, techniques, and infrastructure used by the attackers and those seen in previous Lazarus attacks, making it highly likely that Lazarus was also behind the spread of WannaCry.

While it made a splash, certain errors in how WannaCry was deployed indicate a degree of sloppiness that may have curtailed its effectiveness. For example, while the ransomware had code to provide unique Bitcoin addresses for each victim it defaulted to hardcoded addresses as a result of a race condition bug. This meant WannaCry couldn't use unique Bitcoin addresses because of the bug so couldn't track payments. The attackers did release a variant 13 hours after the initial deployment of WannaCry with this bug fixed, but the vast majority of infections that occurred had this bug.

Much mystery still surrounds the WannaCry attack, and Lazarus itself, but given it has been active for almost a decade, this ransomware attack is unlikely to be the last we see of this audacious attack group.

Check out the Security Response and follow Threat Intel on to keep up-to-date with the latest happenings in the world of threat intelligence and cybersecurity.

Like this story? Recommend it by hitting the heart button so others on Medium see it, and follow Threat Intel on Medium for more great content.