WannaCry 'Highly Likely' Work of North Korean-linked Hackers, Symantec Says

By Ionut Arghire

Published: 2017-05-23 · Archived: 2026-04-06 00:53:49 UTC

North Korea-linked Lazarus Hacking Group is "Highly Likely" to be Responsible for the Global "WannaCry" Ransomware Attack, Symantec Says

Analysis of the tools and infrastructure used in the WannaCry ransomware attacks reveal a tight connection between the threat and the North Korean hacking group Lazarus, Symantec claims.

The global outbreak on May 12 drew the world's attention to WannaCry, but the threat had been active before that, the security researchers say. Over 400,000 machines have been hit by WannaCry to date, although not all had been infected, courtesy of a kill-switch domain registered shortly after the attack began.

The first WannaCry variant, however, emerged in February, and security researchers already discovered a possible tie between it and the Lazarus group, although some suggested such a connection was far-fetched.

North Korea has denied involvement in the ransomware outbreak.

The Lazarus group (also known as BlueNoroff) was previously associated with a number of devastating attacks, including the Sony Pictures hack in 2014 and the $81 million cyber heist from Bangladesh's account at the New York Federal Reserve Bank in 2016. Recently, Kaspersky suggested that the group could be the most serious threat to banks.

Symantec now says that tools previously associated with the group were found on computers infected with WannaCry. Before the May 12 attack, the ransomware was used in a small number of targeted campaigns in

February, March, and April, and the variants are almost identical, save for the method of propagation (the recent version uses the NSA-linked EternalBlue exploit).

According to Symantec, these attacks show "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 behind the spread of WannaCry."

Despite that, however, "the WannaCry attacks do not bear the hallmarks of a nation-state campaign but are more typical of a cybercrime campaign," the security researchers admit. Prior to the May 12 campaign, WannaCry was using stolen credentials to spread across infected networks and didn't employ the leaked EternalBlue exploit.

After the first WannaCry attack in February, experts discovered three pieces of malware linked to Lazarus on the victim's network, including the Volgmer Trojan and two variants of the Destover backdoor (the disk-wiping tool used in the Sony Pictures attacks).

Moreover, the researchers discovered that WannaCry used the Alphanc Trojan for distribution in the March and April attacks, and that this malicious program is a modified version of the Lazarus-linked Duuzer backdoor.

Symantec also found the Bravonc backdoor, which has similar code obfuscation as WannaCry and Fakepude info-stealer (also linked to Lazarus), and the Bravonc Trojan, which used the same IP addresses for command and control (C&C) as Duuzer and Destover, both linked to Lazarus.

Finally, there is the shared code between the previous WannaCry ransomware version and the Lazarus-linked Contopee backdoor.

The February WannaCry attack hit a single organization but compromised over 100 computers within two minutes after the initial infection. A variant of the Mimikatz password-dumping tool was used for compromise, with a second tool used to copy and execute WannaCry on other network computers using the stolen passwords.

In addition to these tools, the security researchers found five other pieces of malware on a second computer on the victim's network, and three of them were linked to Lazarus: Volgmer and the two variants of Destover.

A new sample of WannaCry emerged in late March, and five organizations were infected with it. The Alphanc and Bravonc backdoors were employed in these attacks, with the former used to drop WannaCry onto the compromised computers of at least two victims. Alphanc is believed to be an evolution of Duuzer, a sub-family of the Destover wiping tool used in the Sony attacks.

These attacks hit organizations spanning a range of sectors and geographies, but Symantec found evidence of the tools used in the February attacks on the computers compromised in March and April as well.

The Bravonc Trojan was used to deliver WannaCry to the computers of at least two other victims, the security researchers say. The malware connects to a C&C server hosted at the same IP address as the IP address used by Destover and Duuzer samples, and which was also referred to in a Blue Coat report last year.

"The incorporation of EternalBlue transformed WannaCry from a dangerous threat that could only be used in a limited number of targeted attacks to one of the most virulent strains of malware seen in recent years. It caused

widespread disruption, both to organizations infected and to organizations forced to take computers offline for software updates," Symantec explained.

The security firm also notes that the passwords used to encrypt the ZIP files embedded in the WannaCry dropper are similar across versions ("wcry@123", "wcry@2016", and "WNcry@2ol7") suggesting they come from the same actor. Further, the use of a small number of Bitcoin addresses in the initial version and its limited spread indicates that it wasn't a ransomware family shared across cybercrime groups.

"Aside from commonalities in the tools used to spread WannaCry, there are also a number of links between WannaCry itself and Lazarus. The ransomware shares some code with Backdoor.Contopee, malware that has previously been linked to Lazarus. One v
ariant of Contopee uses a custom SSL implementation, with an identical cipher suite, which is also used by WannaCry. The cipher suite in both samples has the same set of 75 different ciphers to choose from (as opposed to OpenSSL where there are over 300)," Symantec says.

The small number of earlier WannaCry attacks provides sufficient evidence to link the ransomware to Lazarus, Symantec says, given the significant use of tools, code, and infrastructures previously associated with the group. The company also notes that leak of the EternalBlue exploit was what turned the malware into a far more potent threat than it would have been if it continued to use own tools.

Related: North Korea Denies Role in Global Cyberattack

Related: WannaCry Does Not Fit North Korea's Style, Interests: Experts

Realted: North Korea Possibly Behind WannaCry Ransomware Attacks

---