WannaCry Shares Code with Lazarus APT Samples

by Michael Mimoso   May 16, 2017 , 11:45 am

As the first inkling of attribution emerged in the WannaCry ransomware outbreak, researchers found another attack using the same leaked NSA attack tools to spread the Adylkuzz cryptocurrency miner.

Kafeine, a well-known exploit researcher who works for Proofpoint, said Monday that this attack could be greater in scale than WannaCry, which spread worldwide on Friday infecting Windows machines still unpatched against the SMBv1 vulnerabilities exploited by the NSA's EternalBlue exploit and DoublePulsar rootkit and backdoor. Once Adylkuzz infects a machine, it mines the open source Monero cryptocurrency, which goes to great lengths to obfuscate its blockchain information, making it a challenge to trace activity.

Related Posts

Next NSA Exploit Payload Could be Much Worse Than WannaCry

May 17, 2017 , 1:19 pm
Kafeine said the Adylkuzz attacks pre-date WannaCry with the first samples going back to April 24. More than 20 virtual private servers are scanning the internet for targets running port 445 exposed, the same port used by SMB traffic when connected to the internet, and the same port abused by EternalBlue and DoublePulsar.

“Upon successful exploitation via EternalBlue, machines are infected with DoublePulsar. The DoublePulsar backdoor then downloads and runs Adylkuzz from another host,” Kafeine said. “Once running, Adylkuzz will first stop any potential instances of itself already running and block SMB communication to avoid further infection. It then determines the public IP address of the victim and download the mining instructions, cryptominer, and cleanup tools.”

In the meantime on Monday afternoon, Google researcher Neel Mehta, the same researcher who discovered the Heartbleed vulnerability in 2014, posted a tweet indicating a connection between WannaCry and the Lazarus APT. Lazarus is alleged to be behind the 2016 SWIFT attacks in Bangladesh and a number of other incursions against other banks, casinos and cryptocurrency operations.

Mehta’s tweet shows a code array shared between a Lazarus sample from February 2015 and an early version of WannaCry that surfaced in February of this year.

Since then, researchers at Kaspersky Lab, Symantec and Comae Technologies Matt Suiche have confirmed the similarities, adding fuel to the possible connection between North Korea and the current ransomware outbreak.
Lazarus’ history is a notorious one, starting with the 2014 Sony hack, which it is alleged to have pulled off. The group stole and leaked movie scripts, sensitive corporate emails and much more private data from the company, and also used wiper malware to damage internal workstations at Sony Pictures Entertainment.

Last year’s massive heist starting at the Bangladesh Bank abused the organization’s connection to the SWIFT network to make close to a $1 billion in fraudulent transactions. All but $80 million had been recovered once the attack was made public.

At this year’s Kaspersky Lab Security Analyst Summit, researchers from Kaspersky, BAE Systems and SWIFT talked shared more details about Lazarus’ activities, including a group within the APT it called Bluenoroff dedicated to stealing money in order to fund Lazarus’ activities.

They’ve hardly been as successful generating the same revenue with WannaCry, which at last count has collected 40 Bitcoin, which translates to about $71,000 USD.

“For now, more research is required into older versions of Wannacry,” Kaspersky Lab said in a report published Monday. “We believe this might hold the key to solve some of the mysteries around this attack. One thing is for sure — Neel Mehta’s discovery is the most significant clue to date regarding the origins of Wannacry.”

A request made to Google to speak with Mehta was declined.

“Nothing to add beyond Neel’s tweet,” a Google spokesperson told Threatpost.
While researchers admit the evidence is hardly definitive, this would be the first publicly known tools stolen from one nation-state to be used on such a scale.

“The attribution to Lazarus Group would make sense regarding their narrative which in the past was dominated by infiltrating financial institutions in the goal of stealing money,” Suiche said in a report published Monday. “If validated, this means the latest iteration of WannaCry would in fact be the first nation state powered ransomware. This would also mean that a foreign hostile nation would have leveraged lost offensive capabilities from Equation Group to create global chaos.”

Kaspersky Lab also said the likelihood of this being a false flag operations is “improbable;” Kaspersky researchers have published several reports in the past 18 months on APTs and false flags.

“In theory anything is possible, considering the 2015 backdoor code might have been copied by the Wannacry sample from February 2017. However, this code appears to have been removed from later versions,” Kaspersky Lab said. “The February 2017 sample appears to be a very early variant of the Wannacry encryptor. We believe a theory a false flag although possible, is improbable.”

Kaspersky Lab’s Juan Andres Guerrero Saade and Matt Suiche will co-host a webinar on the possible Lazarus connection Wednesday at 10 a.m. Eastern. Register here.
Next NSA Exploit Payload Could be Much Worse Than WannaCry

by Michael Mimoso

Researchers urge Windows admins to apply MS17-010 before the next attack using the EternalBlue NSA exploit deploys a worse payload than WannaCry ransomware.

Read more...

ShadowBrokers Planning Monthly Exploit, Data Dump Service

by Michael Mimoso

The latest rant from the ShadowBrokers ends with news of a subscription service starting in June that will leak exploits and stolen data to paying customers.

Read more...

WikiLeaks Reveals Two CIA Malware Frameworks

by Tom Spring

WikiLeaks released details on what it claims are two frameworks for malware samples dubbed AfterMindnight and Assassin, both allegedly developed by the US Central Intelligence Agency.
Top Stories

OpenVPN Audits Yield Mixed Bag
May 15, 2017, 5:12 pm

Apple Patches Pwn2Own Vulnerabilities in Safari, macOS, iOS
May 16, 2017, 1:56 pm

WikiLeaks Reveals Two CIA Malware Frameworks
May 16, 2017, 6:39 am

Fuze Patches Bug That Exposed Recordings of Private Business Meetings
May 2, 2017, 9:05 am

ShadowBrokers Planning Monthly Exploit, Data Dump Service
May 16, 2017, 8:30 am

Vanilla Forums Open Source Software Vulnerable to RCE, Host Header Injection Vulnerability
May 11, 2017, 4:39 pm

Microsoft Makes it Official, Cuts off SHA-1 Support in IE, Edge
The Final Say

From Kaspersky Blogs

They Asked Me… Everything!

Hi folks! Yesterday, I hosted an ‘Ask Me Anything’ (AMA) on Reddit. I wanted to take a moment to thank the attendees for all of their questions – especially the challenging ones. So here g...

Read more...

WannaCry and Lazarus Group – the missing link?

Moments ago, Neel Mehta, a researcher at Google posted a mysterious message on Twitter. The cryptic message in fact refers to similarity between samples that have shared code between themselves. The t...

Read more...
WannaCry: On screens everywhere!

Embedded systems demand special protection from infections similar to WannaCry.

Read more…

Kaspersky Academy attended MIT (IC)3 Annual Conference

72 guests, among them a global security lead Gordon Morrison, attended the MIT (IC)3 Annual Conference to share the latest insights into the industry. Educational programs manager Christel Gampig-Avil...

Read more…

Threatpost | The first stop for security news