Army Vision: By 2028, a world-class Army that is a source of national pride.

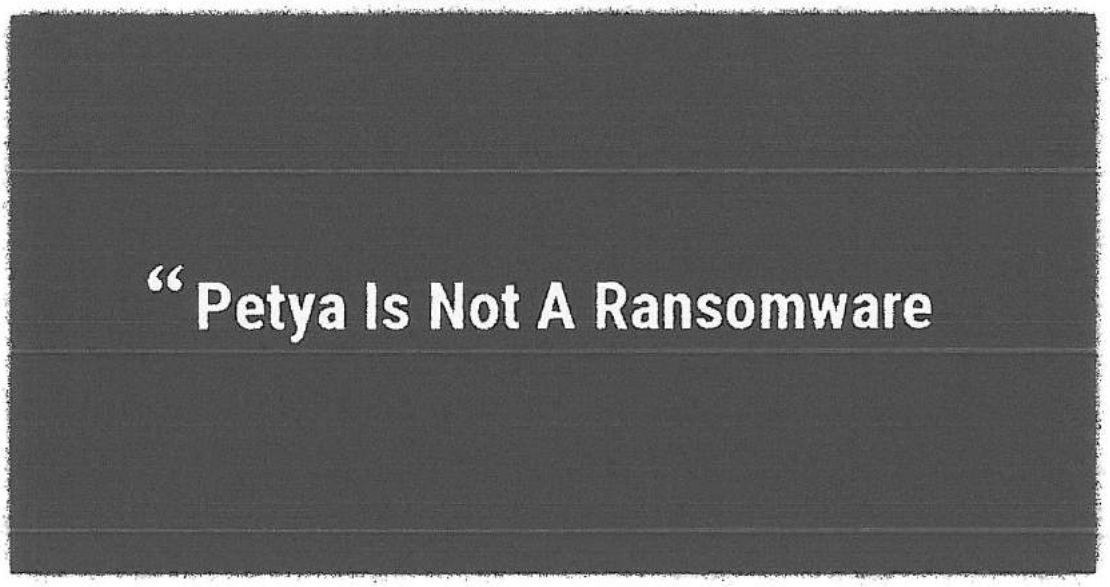
HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 14 July 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-27

Turns Out New Petya is Not a Ransomware,
It's a Destructive Wiper Malware



Tuesday's devastating global malware outbreak was not due to any ransomware infection. The Petya ransomware attacks that began infecting computers in several countries, including Russia, Ukraine, France, India and the United States on Tuesday and demands $300 ransom was not designed with the intention of restoring the computers at all. According to a new analysis, the virus was designed to look like ransomware but was wiper malware that wipes computers outright, destroying all records from the targeted systems. Comae Technologies Founder Matt Suiche, who closely looked the operation of the malware, said after analyzing the virus, known as Petya, his team found that it was a "**Wiper malware**," not ransomware.

Security experts even believe the real attack has been disguised to divert world's attention from a state-sponsored attack on Ukraine to a malware outbreak.

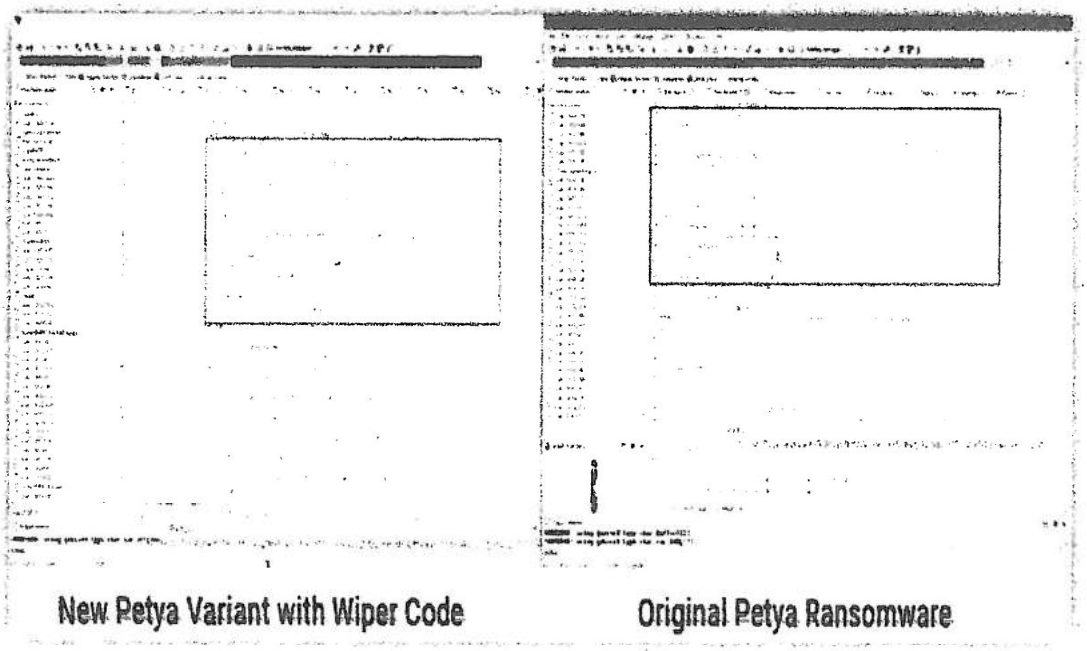
"They believe the ransomware was, in fact, a lure to control the media narrative, especially after the WannaCry incident, to attract the attention on some mysterious hacker group rather than a national state attacker," Suiche writes.

Army Vision: By 2028, a world-class Army that is a source of national pride.

Is Petya Ransomware Faulty or Over-Smart?

Petya is a nasty piece of malware that, unlike other traditional ransomware, does not encrypt files on a targeted system one by one. Instead, Petya reboots victims computers and encrypts the hard drive's master file table (MFT) and renders the master boot record (MBR) inoperable, restricting access to the full system by seizing information about file names, sizes, and location on the physical disk.

Then Petya ransomware takes an encrypted copy of MBR and replaces it with its own malicious code that displays a ransom note, leaving computers unable to boot.



New Petya Variant with Wiper Code | Original Petya Ransomware

However, this new variant of Petya does not keep a copy of replaced MBR, mistakenly or purposely, leaving infected computers unbootable even if victims get the decryption keys. Also, after infecting one machine, the Petya ransomware scans the local network and quickly infects all other machines (even fully-patched) on the same network, using EternalBlue SMB exploit, WMIC and PSEXEC tools.

Don't Pay Ransom; You Wouldn't Get Your Files Back

So far, nearly 45 victims have already paid total $10,500 in Bitcoins in hope to get their locked files back, but unfortunately, they would not. It's because the email address, which was being set-up by the attackers to communicate with victims and send decryption keys, was suspended by the German provider shortly after the outbreak. Meaning, even if victims do pay the ransom, they will never recover their files. Kaspersky researchers also said same.

"The analysis indicates there is little hope for victims to recover their data. The have analyzed the high-level code of the encryption routine, and they have figured out that after disk encryption, the threat actor could not decrypt victims' disks," the security firm said.

"To decrypt a victim's disk threat actors need the installation ID. In previous versions of 'similar' ransomware like Petya/Mischa/GoldenEye this installation ID contained the information necessary for key recovery."

If claims made by the researcher is correct that the new variant of Petya is a destructive malware designed to shut down and disrupt services around the world, the malware has successfully done its job. However, it is still speculation, but the virus primarily and massively targeted multiple entities in Ukraine, including the country's local metro, Kiev's Boryspil airport, electricity supplier, the central bank, and the state telecom. Other countries infected by the Petya virus included Russia, France, Spain, India, China, the United States, Brazil, Chile, Argentina, Turkey and South Korea.

How Did Petya get into the Computers in the First Place?

According to research conducted by Talos Intelligence, little-known Ukrainian firm MeDoc is likely the primary source of the yesterday's global ransomware outbreak. Researchers said the virus has possibly been spread through a malicious software update to a Ukrainian tax accounting system called MeDoc, though MeDoc has denied the allegations in a lengthy Facebook post.

"At the time of updating the program, the system could not be infected with the virus directly from the update file," translated version of MeDoc post reads. "They can argue that users of the MEDoc system can not infect their PC with viruses at the time of updating the program."

However, several security researchers and even Microsoft agreed with Talo's finding, saying MeDoc was breached and the virus was spread via updates.

Reference:

This was cross posted from:
http://thehackernews.com/2017/06/petya-ransomware-wiper-malware.html

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: MAJ GIL P TARIO II (SC) PA – Acting Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-7982005. Email: tariogp@army.mil.ph.