Petya (Petwrap) Ransomware Attack

Medium of Infection
• Phishing, Spam

Exploits Vulnerabilities
• MS17-010(EternalBlue) (probable)

Analysis
Petya lands on infected systems via email spam, in the form of boobytrapped Office documents. These documents contain the Petya installer, which then runs the SMB worm and spreads to new computers. It encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer. It is currently called as Petwrap, and is spreading rapidly with the help of same Windows SMBv1 vulnerability that helped the WannaCry ransomware. • **PetrWrap** This Ransomware has evolved and last known variant called PetrWrap seen in March 2017. The Ransomware comes with a package. When the executable file launches, the malicious packer's code begins to work – it unpacks the malicious DLL Setup.dll into a newly designated RAM area, and then passes control to it. The cybercriminals used an implementation of cryptographic algorithms available in the public library mbedtls (formerly polarssl). Setup.dll is not saved to the hard drive as a separate file, but always remains in the RAM.

At a higher degree of abstraction, the actions of Setup.dll come down to the following:

- ✓ Re-write the boot record on the hard drive with its own malicious loader;
- ✓ Generate a key, infection ID and other auxiliary information, and save them to the hard drive;
- ✓ Cause a system abort and reboot, thereby passing control to the malicious loader.

Now let's look into the detail of how all of this is implemented in the Trojan? But before that, we need to define the terminologies used.

Hard disk sector – the minimum addressable unit of a hard drive, typically 512 bytes.

Master boot record (MBR) – the code and the data written to Sector 0. After hardware is initialized, this code is used to boot the PC. Also, this sector contains the hard disks' partition table. A disk partitioned with MBR may have up to four primary partitions, and the maximum partition size is ~2.2 TB.

GUID Partition Table (GPT) – a more modern standard of hard drive layout. It supports up to 128 partitions, each up to 9.4 ZB in size (1 ZB = 1021 bytes.)

While infecting an MBR disk, Setup.dll performs the following actions:

- ✓ Encrypts sector 0 (the original code and the MBR data) with the simple operation XOR 0x37 (ASCII '7') and writes the result to sector 56;
- ✓ Encrypts sectors 1-33 with the same operation XOR 0x37;
- ✓ Generates configuration data for the malicious loader and writes them to sector 54;
- ✓ Creates the verification sector 55 populated with the repeating byte 0x37;
- ✓ Copies the disk's NT signature and the partition table saved from the original MBR into its own first-level loader; writes first-level malicious code to sector 0 of the disk, and writes second-level code to sectors 34-50 (referred to here as the malicious loader);
- ✓ Calls the function NtRaiseHardError, which causes the operating system to crash (BSOD – the 'blue screen of death')

This Modus operandi was used in original Petya.

- **Petwrap**

PetrWrap implementation uses cryptographic routines from OpenSSL (whereas Petya used the mbedtls library) and proceeds as follows:

- ✓ The Trojan contains an embedded public key master_pub (which is a point on the curve prime192v1 and is again different from the one chosen by Petya);
- ✓ During each infection PetrWrap generates a new pair of session keys ec_session_priv + ec_session_pub;
- ✓ Computes ecdh_shared_digest = SHA512(ECDH(master_pub, ec_session_priv));
- ✓ 'Intercepts' the salsa key generated by Petya and encrypts it using ecdh_shared_digest (there are number of semi-useless manipulations which comes down to essentially encrypting the salsa key with AES-256 using different parts of ecdh_shared_digest as the key and IV);
- ✓ Constructs user_id which is a string representation that contains the encrypted salsa key and the ec_session_pub;
- ✓ Passes this user_id to Petya, which uses it as if it was its own data (puts it into the configuration for the bootloader to be shown to the user after the PC reboot)

PetrWrap hooks two procedures in Petya which we will call petya_infect and petya_generate_config and replaces them with its own procedures dubbed wrap_infect and wrap_generate_config.

wrap_infect implements the following functionality:

- ✓ Saves the salsa key generated by Petya for further use;
- ✓ Patches the Petya bootloader code and ransom text in order to skip the flashing skull animation and to wipe all mention of Petya in the ransom message;
- ✓ Passes execution to the original petya_infect procedure.

wrap_generate_config in turn does the following:

- ✓ Calls the original petya_generate_config procedure;
- ✓ Generates the user_id string according to the algorithm described in the previous paragraph;
- ✓ Replaces Petya's id string with this newly generated user_id.

- **PetWrap**

PetWrap seems to install itself to the disk's master boot record (MBR) like a bootkit. But instead of covert actions, it displays a red screen with instructions on how to restore the system. Going after the MFT is a fast attack that takes far less time than encrypting data files, but the overall affect is the same – the data becomes inaccessible.

Which is similar to other variants.

Clears the windows event log using Wevtutil - Writes a message to the raw disk partition - Shuts down the machine - Leverages PsExec to spread. PsExec is dropped as dllhost.dat Example note: If you see this text, then your files are no longer accessible, because they have been encrypted.

As we are awaiting additional information.

Mitigation
• Apply Microsoft Patch MS17-010 (CVE-2017-0144) • Enable Snort Rules 42329-42332, 42340, 41978 • SMB publically accessible via the internet (ports 139, 445). Should immediately block inbound traffic. • Educate users should not open unexpected attachments. • Ensure all your computers are up to date with Microsoft patches. • Keep backup of the Data. • Avoid enabling macro's for Microsoft word for known files. • Employ content scanning and filtering on your mail servers.

Detection(IOCs)
As it initially clears windows audit Logs, check for audit log and clear logs. **Domains** • wowsmith123456@posteo.net **File Paths** • dllhost.dat **Hashes** • 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a7454 • 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d2 • 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b10

References	
BleepingComputer	https://www.bleepingcomputer.com/news/security/wannacry-d-j-vu-petya-ransomware-outbreak-wreaking-havoc-across-the-globe/
InfoSecurity	https://www.infosecurity-magazine.com/news/ukraine-businesses-petya-ransomware/
ArsTechnica	https://otx.alienvault.com/pulse/5952575d39091b762f50e8fa/ https://otx.alienvault.com/pulse/5952674095270e2d0f055eaf/ https://otx.alienvault.com/pulse/59525e7a95270e240c055ead/
hromadske.ua	https://hromadske.ua/posts/ukrposhtu-ukrenerho-ta-banky-atakuvav-podibnyi-do-wannacry-virus