PetrWrap: Disk encrypting ransomware

A new variant of Petya ransomware, also known as Petrwrap, is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry ransomware abused using EternalBlue exploit.

Working

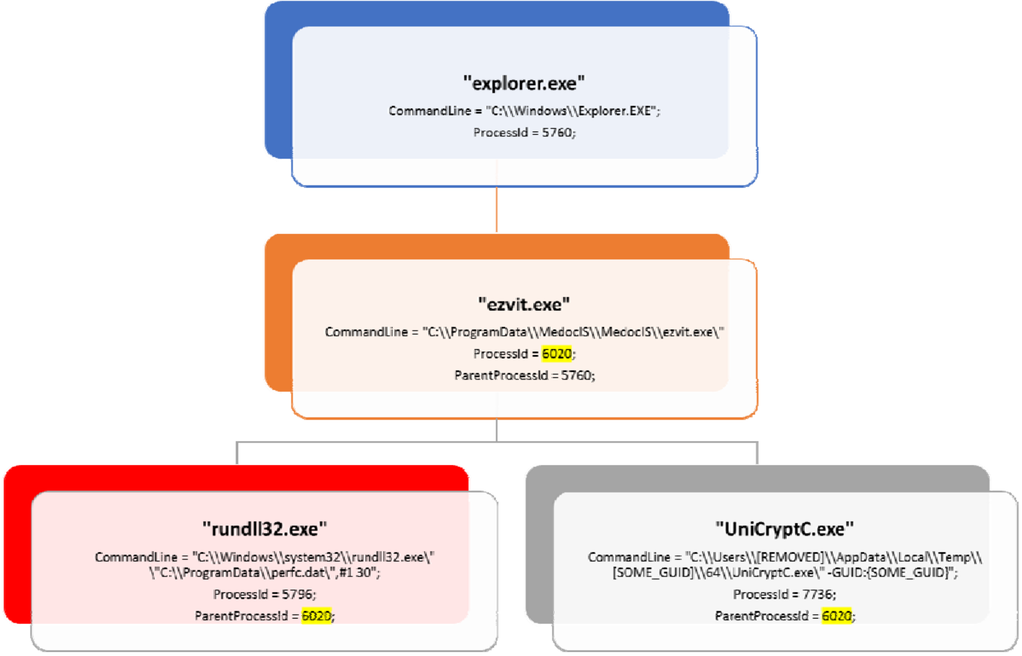
Petya is a nasty piece of ransomware and works very differently from any other ransomware malware. Unlike other traditional ransomware, Petya does not encrypt files on a targeted system one by one. Instead, Petya reboots victims computers and encrypts the hard drive's master file table (MFT) and renders 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. Petya ransomware replaces the computer's MBR with its own malicious code that displays the ransom note and leaves computers unable to boot.

Delivery and Installation

Initial infection appears to involve a software supply-chain threat involving the Ukrainian company M.E.Doc, which develops tax accounting software, MEDoc. Microsoft has evidence that a few active infections of the ransomware initially started from the legitimate MEDoc updater process.

The execution chain leading to the ransomware installation is represented in the diagram below and essentially confirms that EzVit.exe process from MEDoc, for unknown reasons, at some moment executed the following command-line:

```
C:\\Windows\\system32\\rundll32.exe\” \”C:\\ProgramData\\perfc.dat\”,#1 30
```



"explorer.exe"

CommandLine = "C:\\Windows\\Explorer.EXE";
ProcessId = 5760;

"ezvit.exe"

CommandLine = "C:\\ProgramData\\MedocIS\\MedocIS\\ezvit.exe\"
ProcessId = 6020;
ParentProcessId = 5760;

"rundll32.exe"

CommandLine = "C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30";
ProcessId = 5796;
ParentProcessId = 6020;

"UniCryptC.exe"

CommandLine = "C:\\Users\\[REMOVED]\\AppData\\Local\\Temp\\[SOME_GUID]\\64\\UniCryptC.exe\" -GUID:{SOME_GUID}";
ProcessId = 7736;
ParentProcessId = 6020;

Technical Details

- This ransomware's initial entry into the system involves the use of the PsExec tool, an official Microsoft utility used to run processes on remote systems.
- It also comes through spear phishing emails, it is reported to be generated from wowsmith123456@posteo.net
- It also uses the EternalBlue exploit–previously used in the WannaCry attack–that targets a vulnerability in Server Message Block (SMB) v1.
- Once on a system, this Petya variant uses the *rundll32.exe* process to run itself.
- The actual encryption is then carried out by a file named *perfc.dat*, located in the Windows folder.
- This ransomware then adds a scheduled task, which reboots the system after at least an hour. Meanwhile, the Master Boot Record (MBR) is also modified so that the encryptor will carry out the encryption and the appropriate ransom note will be displayed.

- A fake CHKDSK notice is initially displayed; this is when the encryption is carried out. Unusually for ransomware, it does not change the extensions of any encrypted files.
- More than 60+ file extensions are targeted for encryption; it is worth noting that the file extensions targeted are focused on file types used in enterprise settings; images and video files (targeted by other ransomware attacks) are notably absent.

Further Propagation

The malware has four mechanisms used to propagate once a device is infected:

- EternalBlue - the same exploit used by WannaCry.
- EternalRomance - a second exploit for CVE-2017-0145
- Psexec - a legitimate Windows administration tool.
- WMI - Windows Management Instrumentation, a legitimate Windows component

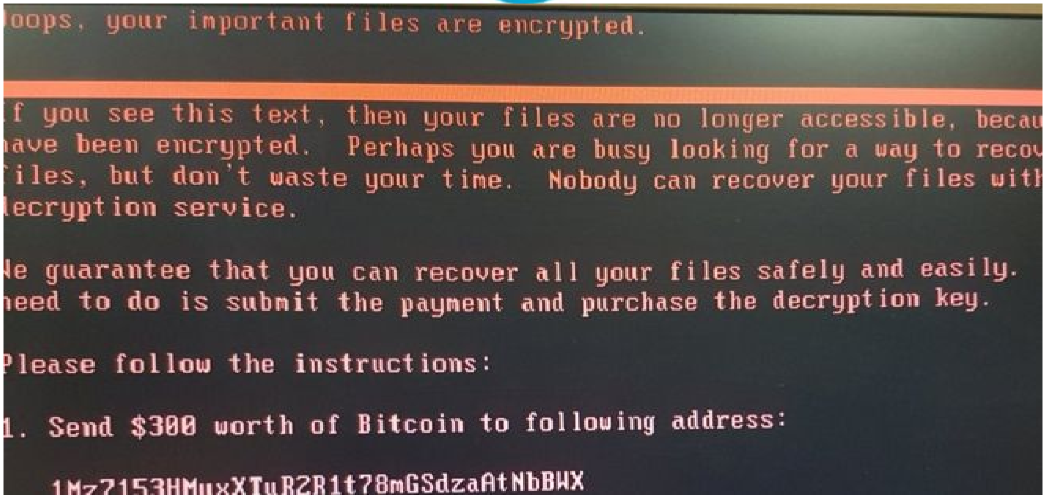
Global Impact

Petya ransomware has already infected IT systems in various countries:

- Russia: State-owned oil giant Rosneft
- Ukraine: Ukrainian state electricity suppliers: Kyivenergo and Ukrenergo, National Bank of Ukraine (NBU) and Oschadbank, Ukrainian telecommunication operators: Kyivstar, LifeCell, Ukrtelecom.
- US: Pharma Giant Merck
- UK: Britain's WPP, the world's biggest advertising agency
- IT systems of Shipping giant A.P. Moller-Maersk impacted at multiple locations and business units.
- India: Jawaharlal Nehru Port Trust (JNPT)

Ransom Amount

The ransomware displays a text, demanding $300 worth of Bitcoins



```
oops, your important files are encrypted.

f you see this text, then your files are no longer accessible, becau
ave been encrypted.  Perhaps you are busy looking for a way to recov
iles, but don't waste your time.  Nobody can recover your files with
ecryption service.

e guarantee that you can recover all your files safely and easily.
eed to do is submit the payment and purchase the decryption key.

lease follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
```

Kill-Switch for Petya ransomware

PT Security, a UK-based cyber security company and Amit Serper from Cybereason, have discovered a Kill-Switch for Petya ransomware. According to a tweet, company has advised users to create a file i.e. "C:\Windows\perfc" to prevent ransomware infection.

Preventive Actions to be taken

1. Block source/destination E-mail addresses:
   - wowsmith123456@posteo.net
   - iva76y3pr@outlook.com
   - carmellar4hegp@outlook.com
   - amanda44i8sq@outlook.com

   To safeguard against any ransomware infection, users should always be suspicious of unwanted files and documents sent over an email and should never click on links inside them unless verifying the source.

2. Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.

3. Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.

4. Block domains:
   - http://mischapuk6hyrn72.onion/
   - http://petya3jxfp2f7g3i.onion/
   - http://petya3sen7dyko2n.onion/
   - http://mischa5xyix2mrhd.onion/MZ2MMJ
   - http://mischapuk6hyrn72.onion/MZ2MMJ
   - http://petya3jxfp2f7g3i.onion/MZ2MMJ
   - http://petya3sen7dyko2n.onion/MZ2MMJ
   - http://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin
   - COFFEINOFFICE.XYZ
   - http://french-cooking.com/

5. Block IPs:
   - 95.141.115.108
   - 185.165.29.78
   - 84.200.16.242
   - 111.90.139.247

6. Apply patches against EternalBlue (MS17-010)

7. Disable SMBv1

8. Filter inbound connections on ports TCP 445 and 139 coming from untrusted networks

9. Disable WMIC

Since Petya Ransomware is also taking advantage of WMIC and PSEXEC tools to infect fully-patched Windows computers, users are also advised to disable WMIC (Windows Management Instrumentation Command-line).

10. Update Anti-Virus

    Use a good and effective anti-virus security suite on your system, and keep it up-to-date.

11. Keep a good back-up routine in place that makes their copies to an external storage device that isn't always connected to your PC.

12. Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application

13. Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA%, %PROGRAMDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations. Enforce application whitelisting on all endpoint workstations

14. Disable Macros in MS office products.

15. Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.

16. Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.

17. Update Snort IDS rules:

- alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool"; flow: to_server, established; content: "|FF|SMB2|00 00 00 00|"; depth: 9; offset: 4; byte_test: 2, >, 0x0008, 52, relative, little; pcre: "/\xFFSMB2\x00\x00\x00\x00.{52}(?:\x04|\x09|\x0A|\x0B|\x0C|\x0E|\x11)\x00/"; flowbits: set, SMB.Trans2.SubCommand.Unimplemented; reference: url, msdn.microsoft.com/en-us/library/ee441654.aspx; classtype: attempted-admin; sid: 10001254; rev: 2;)

- alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] ETERNALBLUE (WannaCry, Petya) SMB MS Windows RCE"; flow: to_server, established; content: "|FF|SMB3|00 00 00 00|"; depth: 9; offset: 4; flowbits: isset, SMB.Trans2.SubCommand.Unimplemented.Code0E; threshold: type limit, track by_src, seconds 60, count 1; reference: cve, 2017-0144; classtype: attempted-admin; sid: 10001255; rev: 3;)

- alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Trans2 Sub-Command 0x0E. Likely ETERNALBLUE (WannaCry, Petya) tool"; flow: to_server, established; content: "|FF|SMB2|00 00 00 00|"; depth: 9; offset: 4; content: "|0E 00|"; distance: 52; within: 2; flowbits: set, SMB.Trans2.SubCommand.Unimplemented.Code0E; reference: url, msdn.microsoft.com/en-us/library/ee441654.aspx; classtype: attempted-admin; sid: 10001256; rev: 2;)

- alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Petya ransomware perfc.dat component"; flow: to_server, established, no_stream; content: "|fe 53 4d 42|"; offset: 4; depth: 4; content: "|05 00|"; offset: 16; depth: 2; byte_jump: 2, 112, little, from_beginning, post_offset 4; content: "|70 00 65 00 72 00 66 00 63 00 2e 00 64 00 61 00 74 00|"; distance:0; classtype:suspicious-filename-detect; sid: 10001443; rev: 1;)

- alert tcp any any -> $HOME_NET 445 (msg:"[PT Open] SMB2 Create PSEXESVC.EXE"; flow:to_server, established, no_stream; content: "|fe 53 4d 42|"; offset: 4; depth: 4; content: "|05 00|"; offset: 16; depth: 2; byte_jump: 2, 112, little, from_beginning, post_offset 4; content:"|50 00 53 00 45 00 58 00 45 00 53 00 56 00 43 00 2e 00 45 00 58 00 45|"; distance:0; classtype:suspicious-filename-detect; sid: 10001444; rev:1;)

References

1. https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759
2. http://thehackernews.com/2017/06/petya-ransomware-attack.html
3. http://seckurity.com/2017/06/everything-technical-about-the-new-ransomware-petya/
4. https://twitter.com/PTsecurity_UK/status/879779707075665922
5. https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/