Emerging Threat – Petya Ransomware Campaign (ETR-2017-C026)

EXECUTIVE SUMMARY:

Several countries in Europe are reporting a significant ransomware campaign delivering a variant of the *Petya* ransomware. Attacks appear to be targeted at specific organizations and so far reports for Ukraine's national bank, Boryspill International Airport, Ukraine state power provider, and a Danish shipping company have been reported. Other reports of compromise are being investigated.

A ransom of $300 USD in bitcoins is demanded per infected host. The bitcoin wallet for ransom payment shows nine payments have been made so far.

The initial infection vector for the threat is email-based and has been reported by threat researchers to be a fake resume scam. Other social engineering emails targeted to the intended company may also be being used in conjunction with CVE-2017-0199 to deliver the *Petya* payload. Once the document is opened and *Petya* has been installed, the *ETERNALBLUE* exploit is allegedly used to spread inside the affected organization through exploitation of the SMBv1 protocol (MS17-010).

As this campaign progresses and more details become available, Symantec will continue to keep you updated with Threat Landscape Updates.

THREAT TECHNICAL DETAILS:

Spain, Poland, Ukraine, Russia, UK, France, and Denmark, as well as other European countries have all reported significant ransomware campaigns delivering *Petya*.

The malware appears to be introduced into the environment with phishing emails. In some cases, phishing emails were observed spoofing a job application with a link to a malicious payload hosted on Dropbox. In more recent attacks, threat researchers have reported the use of CVE-2017-0199, a vulnerability in Microsoft Office that allows attackers to execute malicious code when users are tricked into opening a malicious Word attachment.

When the target user opens the malicious document, CVE-2017-0199 is exploited to retrieve and execute the *Petya* ransomware payload. Once installed, *Peyta* encrypts certain file types:

.3ds .7z .accdb .ai .asp .aspx .avhd .back .bak .c .cfg .conf .cpp .cs .ctl .dbf .disk
.djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .kdbx .mail .mdb .msg .nrg .ora .ost
.ova .ovf .pdf .php .pmf .ppt .pptx .pst .pvi .py .pyc .rar .rtf .sln .sql .tar .vbox .vbs
.vcb .vdi .vfd .vmc .vmdk .vmsd .vmx .vsdx .vsv .work .xls .xlsx .xvd .zip

The ransomware also clears windows event logs using the following wevtutil command:

wevtutil cl Setup & wevtutil cl System & wevtutil cl Security &
wevtutil cl Application & fsutil usn deletejournal /D %c:

Due to the recent widespread infections, it is suspected that these recent variants of *Petya* incorporate a new method for network propagation.

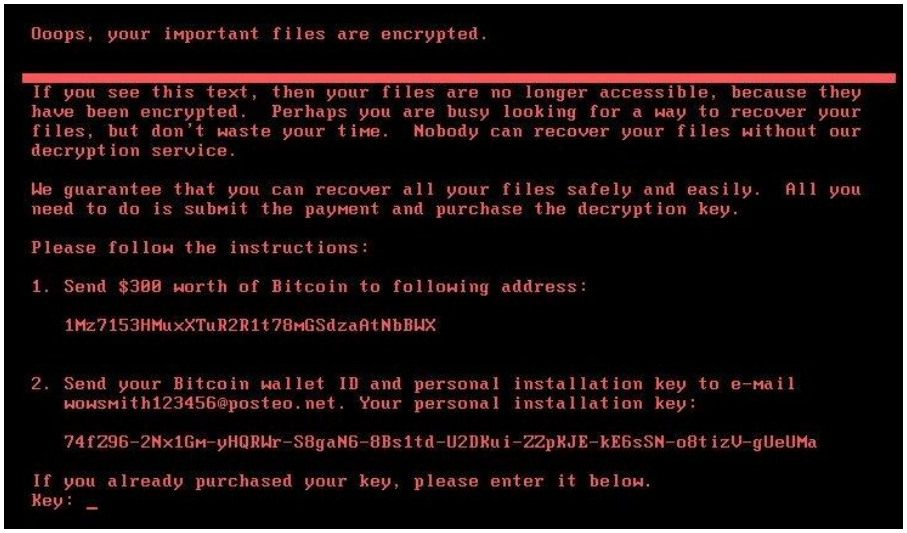
Researchers suspect that *Petya* is using MS17-010 (vulnerability in SMBv1) to propagate on the network. This is the same vulnerability that was exploited in recent Wannacry outbreaks. *Petya* also appears to leverage PSExec, a Microsoft SysInternals Suite tool that is used for remote administration, in some capacity). It is possible the malware attempts to propagate on compromised domains by leveraging compromised domain credentials and the PSExec tool, however this theory is still being investigated.

Once *Petya* completes the encryption and propagation phases, it overwrites the MBR (Master Boot Record) and causes the host to reboot via a scheduled task.

schtasks.exe /TR "%WINDIR%\system32\shutdown.exe /r /f" /ST 07:45

After the host reboots, the end user is presented with the following screen:

When the user presses any key, the following ransom message is presented:



INDICATORS OF COMPROMISE:

New Variants (SHA256):
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

Known Payload Hosting:
185.165.29[.]78/~alex/svchost.exe

Known Payment Sites:
mischapuk6hyrn72[.]onion
petya3jxfp2f7g3i[.]onion
petya3sen7dyko2n[.]onion
mischa5xyix2mrhd[.]onion/MZ2MMJ
mischapuk6hyrn72[.]onion/MZ2MMJ
petya3jxfp2f7g3i[.]onion/MZ2MMJ
petya3sen7dyko2n[.]onion/MZ2MMJ

IMPACT:

Computers infected with the Petya malware will have their files encrypted and hard drive master boot record (MBR) overwritten with the Petya bootloader. Once the server is rebooted, a fake check disk program will complete the infection rendering the server unbootable and unuseable. Overwriting the MBR can render the infected host unusable.

AFFECTED SOFTWARE:

Microsoft Windows OS-based systems.

SYMANTEC MSS SOC DETECTION CAPABILITIES:

For customers with our IDS/IPS Security Management services, vendor signatures will be deployed automatically, but enabled only where it is recommended by the vendor. Customers who would like to adjust their IDS/IPS policy outside the standard vendor policy should contact MSS to discuss their requirements. MSS can be reached by requesting help via phone, e-mail, chat, or by visiting the MSS portal at https://mss.symantec.com.

For customers with monitor-only IDS/IPS devices, Symantec MSS stands ready to provide security monitoring once your IDS/IPS vendor releases signatures and those signatures are enabled on your monitored devices.

Vendor Detection

- **Symantec Endpoint Protection**
  OS Attack: Microsoft SMB MS17-010 Disclosure Attempt attack.

- **Symantec AV**
  Ransom.Petya

- **CheckPoint**
  Microsoft Windows SMB Information Disclosure (MS17-0101: CVE-2017-0147), Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143), Microsoft Windows SMB2 Tree Connect Denial of Service (MS17-010: CVE-2017-0016)

- **Intrushield**
  NETBIOS-SS: MS17-010 SMB Remote Code Execution (Eternal Tools and WannaCry Ransomware)-0x43c0bd00, UDS-NETBIOS-SS: MS17-010 EternalBlue SMB Remote Code Execution-0x43c0bb00

- **ISS**
  SMB_EternalBlue_Implant_CnC

- **Snort**
  ET EXPLOIT Possible ETERNALBLUE MS17 010 Echo Request (set), ET EXPLOIT Possible ETERNALBLUE MS17 010 Echo Response, ET EXPLOIT Possible ETERNALBLUE MS17 010 Heap Spray, MALWARE-CNC Win.Trojan.Eternalblue variant echo request

- **Trend Micro**
  Ransom_PETYA.SM1, Ransom_PETYA.SM2, W2KM_PETYA.L, W2KM_PETYA.M

- **McAfee**
  Ransom-Petya

- **Microsoft SCEP**
  Ransom:Win32/Petya.A

This list represents a snapshot of current detection. Symantec MSS stands ready to provide security monitoring once additional vendors or additional detection is identified and enabled on your monitored devices. As threats evolve, detection for those threats can and will evolve as well.

MITIGATION STRATEGIES AND RECOMMENDATIONS:

Threat Specific Mitigating Guidelines

- Petya uses low-level disk manipulation rather than encrypting files one at a time.
- Try to not reboot servers infected by the Petya malware and take a disk image if possible.
- The primary infection vector is email-based so reviewing phishing scams and reporting of infections with employees is crucial.

RECOMMENDED BEST PRACTICES:

Symantec recommends that all customers follow IT security best practices. These will help mitigate the initial infection vectors used by most malware, as well as prevent or slow the spread of secondary infections.

Minimum Recommended Best Practices Include:

- Disable default user accounts
- Educate users to avoid following links to untrusted sites.
- Always execute browsing software with the least privileges possible
- Turn on Data Execution Prevention (DEP) for systems that support it
- Maintain a regular patch and update cycle for OS and installed software
- For additional details please reference: http://technet.microsoft.com/en-us/library/dd277328.aspx

REFERENCES:

For additional information related to this threat/vulnerability please reference the following links:

- **Ukraine's Ukrenergo says hit by cyber attack, power supplies unaffected**
  http://uk.reuters.com/article/ukraine-cyber-attacks-ukrenergo-idUKS8N1EA05J

- **Ukraine central bank says local banks, companies hit by new cyber attacks**
  http://www.nasdaq.com/article/ukraine-central-bank-says-local-banks-companies-hit-by-new-cyber-attacks-20170627-00291

- **Petya – Taking Ransomware To The Low Level**
  https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

- **Un neuevo ataque de 'ransomware' paraliza grandes empresas en todo el mundo**
  http://www.elconfidencial.com/tecnologia/2017-06-27/ataque-ransomware-dla-piper-wannacry_1405839/

- **AD maakt gebruik van cookies**
  http://www.ad.nl/rotterdam/grote-hack-bij-maersk-legt-rotterdamse-containerterminal-plat~a60dd307/

- **Энергетические компании и банки Украины атаковал аналог WannaCry**
  https://tjournal.ru/45795-energeticheskie-kompanii-i-banki-ukraini-atakoval-analog-wannacry

Thank you for choosing Symantec as your Managed Security Services Provider. Should you have any questions or feedback, please contact your Services Manager, or the Analysis Team can be reached by requesting help via phone, email, chat, or by visiting the MSS portal at https://mss.symantec.com.

Global Client Services Team
Symantec Managed Security Services
MSS Portal: https://mss.symantec.com
MSS Blog: http://www.symantec.com/connect/symantec-blogs/cyber-security-services

Need Help Responding to a Security Incident?
Contact Symantec Managed Security Services, part of our Cyber Security Services that include Incident Response Services and DeepSight Intelligence services.
Email: incidentresponse@symantec.com
US Incident Response Hotline: (855) 378-0073
UK Incident Response Hotline: +44 (0) 800 917 2793
Australia Incident Response Hotline: +61 1800 481 774
Singapore Incident Response Hotline: +65 800 1206718
Japan Incident Response Hotline: +81 0066 33 813303
For Information: http://go.symantec.com/incidentresponse