CERT-MU

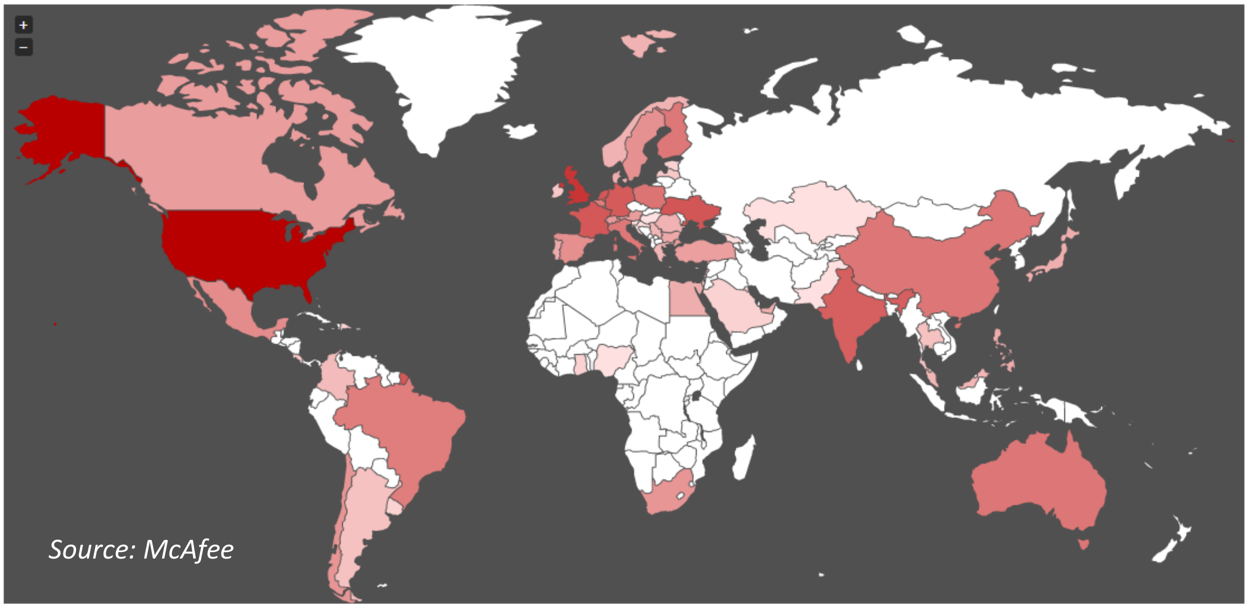
THE PETYA CYBER ATTACK

Whitepaper

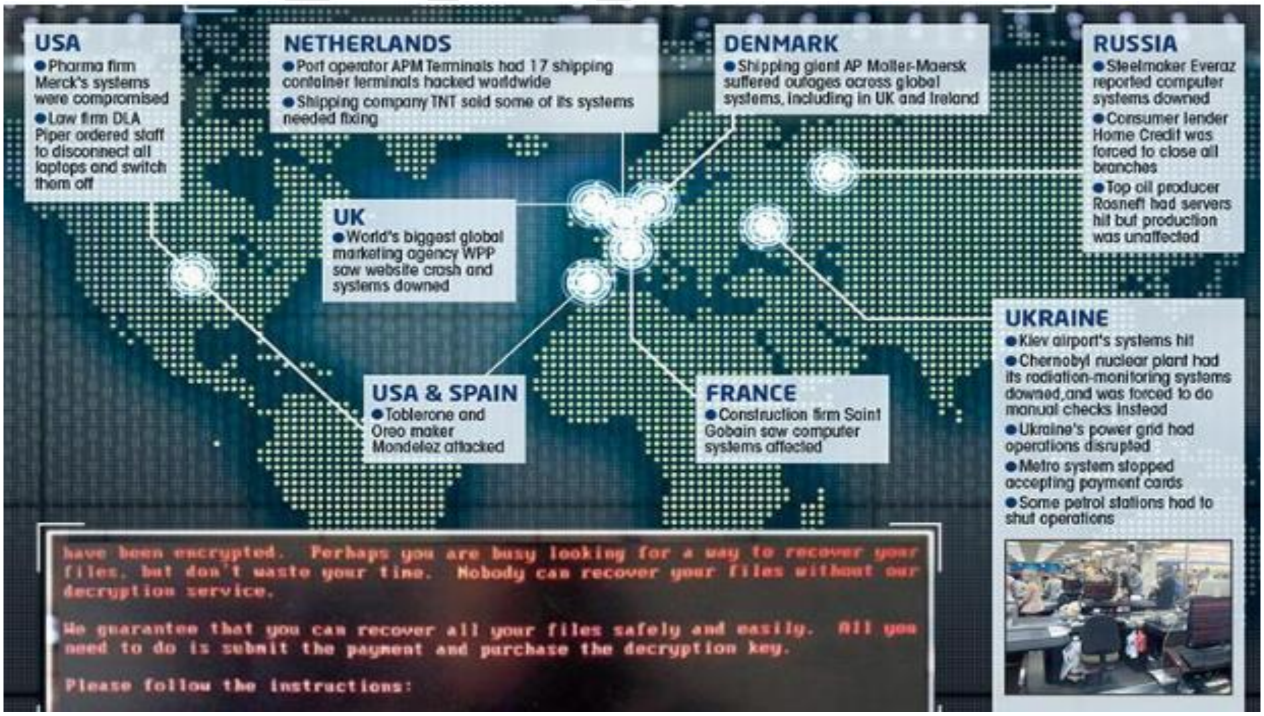
Prepared By CERT-MU

June 2017

THE PETYA GLOBAL CYBER ATTACK



Source: McAfee



USA
- Pharma firm Merck's systems were compromised
- Law firm DLA Piper ordered staff to disconnect all laptops and switch them off

NETHERLANDS
- Port operator APM Terminals had 17 shipping container terminals hacked worldwide
- Shipping company TNT said some of its systems needed fixing

DENMARK
- Shipping giant AP Moller-Maersk suffered outages across global systems, including in UK and Ireland

RUSSIA
- Steelmaker Everaz reported computer systems downed
- Consumer lender Home Credit was forced to close all branches
- Top oil producer Rosneft had servers hit but production was unaffected

UK
- World's biggest global marketing agency WPP saw website crash and systems downed

USA & SPAIN
- Toblerone and Oreo maker Mondelez attacked

FRANCE
- Construction firm Saint Gobain saw computer systems affected

UKRAINE
- Kiev airport's systems hit
- Chernobyl nuclear plant had its radiation-monitoring systems downed,and was forced to do manual checks instead
- Ukraine's power grid had operations disrupted
- Metro system stopped accepting payment cards
- Some petrol stations had to shut operations

```
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

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

Please follow the instructions:
```

Maps showing Petya Infections around the world

CONTENTS

1.0 INTRODUCTION

The world has witnessed another major cyber-attack known as “Petya” since Tuesday 27th June 2017. The malware is a new variant of the Petya Crypto Ransomware which firstly made its apparition in March 2016. The malware is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry Ransomware exploited in May 2017 and uses the same NSA EternalBlue Exploit. The exploit, known as “Eternal Blue,” was released online in April 2017 in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

The first infections began spreading across Europe, most particularly in Ukraine, where more than 12,500 machines encountered the threat. Then infections were observed in another 64 countries, including Belgium, Brazil, Germany, Russia, India and the United States. Many critical systems, organisations, airports, banks and Government departments were affected.

Petya is a ransomware family that works by modifying the Window’s system’s Master Boot Record (MBR), causing the system to crash. When the user reboots their PC, the modified MBR prevents Windows from loading and instead displays an ASCII Ransom note demanding payment of US $300 in Bitcoin from the victim to retrieve their individual decryption key

The threat is still under active investigation; the situation may change as we learn more. CERT-MU will continue to actively monitor and analyze this situation for new developments and respond accordingly.

2.0 AFFECTED SYSTEMS

Windows XP through 8.1 (Windows 10 is not vulnerable)

Microsoft released a patch MS17-010 (ETERNALBLUE) on 14 March. More information about the patch is available on:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Microsoft released a patch for the older unsupported Windows versions on 12 May, which can be found on:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

3.0 MALWARE NAMES

The malware first made its apparition in March 2016. The new variant which appeared in June 2017 has been named as follows:

- Petya
- Petna
- PetrWrap
- NotPetya

4.0 TECHNICAL ANALYSIS OF THE ATTACK

4.1 Distribution of the Petya Malware

An attack against the update mechanism of a third-party Ukrainian accounting software product called M.E. Doc appears to have been the initial vector.

The malware has been distributed via phishing e-mails.

For further distribution within the network the malware uses:

- MS17-10 vulnerability
- Remote access to WMI (Windows Management Instrumentation), command like:

  ```
  “process call create \"C:\\Windows\\System32\\rundll32.exe
  [file:///\\%22C:\Windows\perfc.dat\]\\\"C:\\Windows\\perfc.dat\\\" #1”.
  ```

- The malware also uses «PSEXEC» toolkit or some similar tool

The malware clears system logs using the following command to make further analysis more difficult:

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

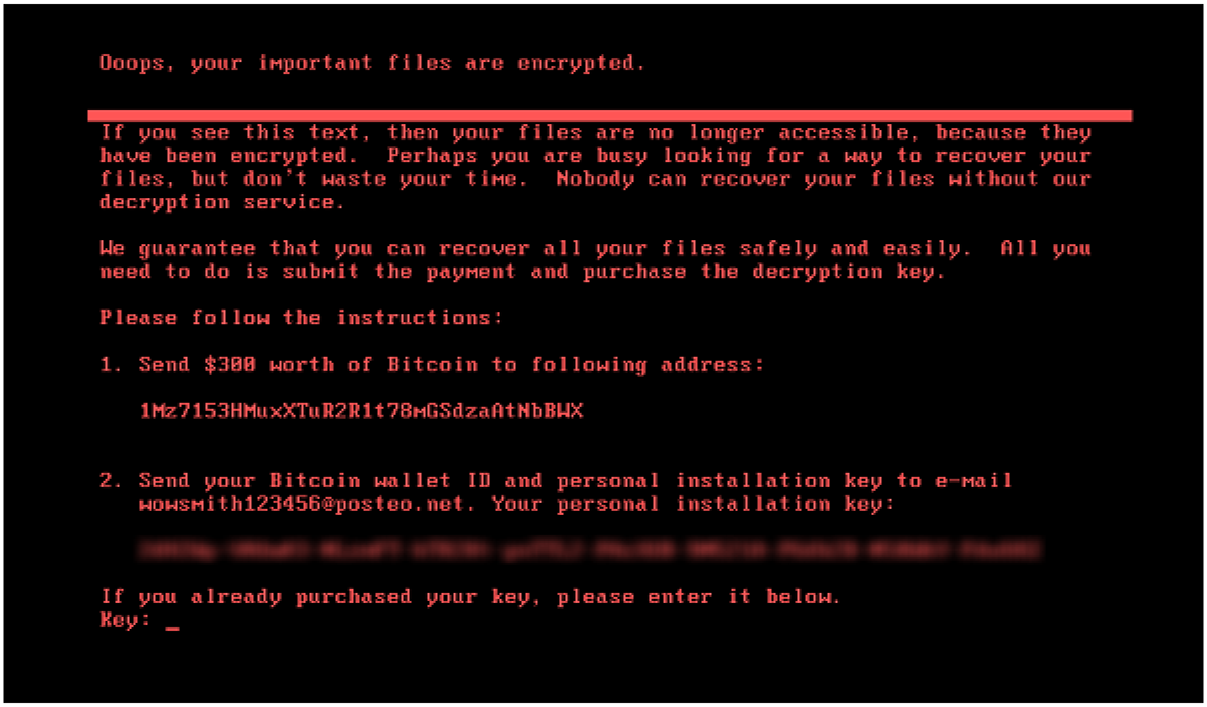
It also writes its code to Hard Drive MBR, initiates system reload and adds reload commands to Windows planner (*“schtasks”* and *“at”* commands).

4.2 Encryption

The encryption used by the malware is AES-128 with RSA. This is different from previous variants, which used SALSA20. Encryption depends on the privileges the malware has on the system such as:

- If admin rights are available, the malware will “only” encrypt the MBR and MFT.
- In case the privileges are not high enough to rewrite MBR, the files are encrypted without a system reload.

After the system is reloaded, the malware downloads its code from MBR and encrypts data on the hard drive



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

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

Please follow the instructions:

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

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   [redacted]

If you already purchased your key, please enter it below.
Key: _
```

If the computer is shut down before the reload, MBR can be reestablished with *"bootrec /FixMbr"* command. (in Vista+, for Windows XP *"fixmbr"* can be used).

In case the privileges are not high enough to rewrite MBR, the files are encrypted without a system reload. The list of file types that are encrypted:

> *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.*

5.0 TECHNICAL ANALYSIS: IP ADDRESS AND CREDENTIAL GATHERING

Petya builds a list of IP addresses to spread to, which includes primarily addresses on the local area network (LAN) but also remote IPs. The full list is built as follows:

- All IP addresses and DHCP servers of all network adaptors
- All DHCP clients of the DHCP server if ports 445/139 are open
- All IP addresses within the subnet as defined by the subnet mask if ports 445/139 are open
- All computers you have a current open network connection with
- All computers in the ARP cache

- All resources in Active Directory
- All server and workstation resources in Network Neighborhood
- All resources in the Windows Credential Manager (including Remote Desktop Terminal Services computers)

Once the list of target computers has been identified, Petya builds out a list of user names and passwords it can use to spread to those targets. The list of user names and passwords is stored in memory. It uses two methods to gather credentials:

- Gathers user names and passwords from Windows Credential Manager
- Drops and executes a 32bit or 64bit credential dumper

6.0 WIPER V/S RANSOMWARE

As mentioned, encryption performed by Petya is twofold; firstly specific file types are encrypted in user-mode after spreading occurs and the key is encrypted with an embedded public key, Base64 encoded, and appended to the ***README.TXT*** file.

After a system reboot occurs, the infected MBR is loaded, disk encryption begins, and the ransom note is displayed to the user. The "installation key" referenced in the ransom note is a randomly generated string that is displayed to the user. A randomly generated Salsa20 key is then used for disk encryption. As there is no relationship between the “installation key” and Salsa20 key, the disk can never be decrypted. This demonstrates that Petya is more accurately a wiper rather than ransomware.

7.0 MALWARE INDICATORS

SHA256 hashes

f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 (signed PSEXEC.EXE)
64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1 (main 32-bit DLL)
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (main 32-bit DLL)
02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f (64-bit EXE)
eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998 (32-bit EXE)

Files

- c:\windows\dllhost.dat
- c:\windows\<malware_dll> (no extension)
- %TEMP%\<random name>.tmp (EXE drop)

Other indicators

- PIPE name: \\.\pipe\{df458642-df8b-4131-b02d-32064a2f4c19}

- Scheduled task running “shutdown -r -n”

8.0 COMMAND AND CONTROL SERVERS

Petya contains no Command and Control mechanisms that we know of. After a host is infected, there is no communication from the malware back to the attacker.

9.0 DETECTION OF THE MALWARE BY ANTI-VIRUS

Microsoft Windows Defender, System Center Endpoint Protection, and Forefront Endpoint Protection detect this threat family as **Ransom: Win32/Petya**.

Users should ensure that they have a definition version equal to or later than:

- Threat definition version: 1.247.197.0
- Version created on: 12:04:25 PM: Tuesday, June 27 2017
- Last Update: 12:04:25 PM: Tuesday, June 27 2017

Various anti-virus software detect the malware as:

- Trojan.Cryptolocker.AJ
- Win32/Diskcoder.C Trojan
- Ransom.Petya
- Ransom.Petya!g1

In addition, the free Microsoft Safety Scanner is designed to detect this threat as well as many others. The scanner is available on the link below:

http://www.microsoft.com/security/scanner/

10.0 CAN THE ENCRYPTED FILES BE RECOVERED?

As there is no relationship between the “installation key” and Salsa20 key, the disk can never be decrypted. Therefore files cannot be recovered as Petya is more like a wiper under the disguise of a ransomware.

11.0 RECOMMENDED STEPS FOR PREVENTION

- 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

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.

- Applocker policies to block execution of files having name perfc.dat as well as psexec.exe utility from sysinternals.

- **A quick fix** to prevent by creating the files (perfc, perfc.dll, and perfc.dat) to already exist on the Windows machine, under C:\Windows, with READONLY permissions. A brief description is here:
  https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/
  [NOTE: This is not a Kill Switch but only a vaccine with no Guarantees]

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.

- 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.

- Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys 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.

- 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.

- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.

- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- Maintain updated Antivirus software on all systems.

- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.

- Block the attachments of file types: *exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf*

- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)

- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.

- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.

- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.

- Disable remote Desktop Connections, employ least-privileged accounts.

- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems, Check regularly for the integrity of the information stored in the databases.

- Restrict users' abilities (permissions) to install and run unwanted software applications.

- Employ data-at-rest and data-in-transit encryption.

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.

- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.

- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.

- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.

- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.

- Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.

- Test your backups to ensure they work correctly upon use.

11.1 Consider implementing the following best practices:

- Segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band network management.
- Validate integrity of hardware and software.

11.2 Recommended Steps for Remediation

- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

11.3 Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software, especially free software - from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

12.0 REFERENCES

https://securelist.com/schroedingers-petya/78870/

https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/

https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/

https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/

https://blog.malwarebytes.com/cybercrime/2017/06/petya-esque-ransomware-is-spreading-across-the-world/

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

https://researchcenter.paloaltonetworks.com/2017/06/unit42-threat-brief-petya-ransomware/

https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html

http://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/

https://blogs.forcepoint.com/security-labs/d%C3%A9j%C3%A0-vu-petya-ransomware-appears-smb-propagation-capabilities

https://www.binarydefense.com/petya-ransomware-without-fluff/

https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

https://www.itnews.com.au/news/what-you-need-to-know-about-the-petya-notpetya-ransomware-466707

https://nakedsecurity.sophos.com/2017/06/27/breaking-news-what-we-know-about-the-global-ransomware-outbreak/

https://securityintelligence.com/petya-werent-expecting-this-ransomware-takes-systems-hostage-across-the-globe/

https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported

https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know

https://www.symantec.com/connect/articles/petya-ransomware-next-global-threat

The Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu