“Petya” Ransomware – Security Advisory

1. Executive Summary

A new variant of Petya ransomware, also known as Petwrap, is spreading rapidly due to the same Windows SMBv1 vulnerability that the WannaCry ransomware abused..It will infect MBR and on restart, it has its own low language code to encrypt MFT, which makes the drive inaccessible, Which then warns users that all their files have been encrypted with a key known only to the attacker and that they will be locked out until they pay to an anonymous party using the cryptocurrency Bitcoin.

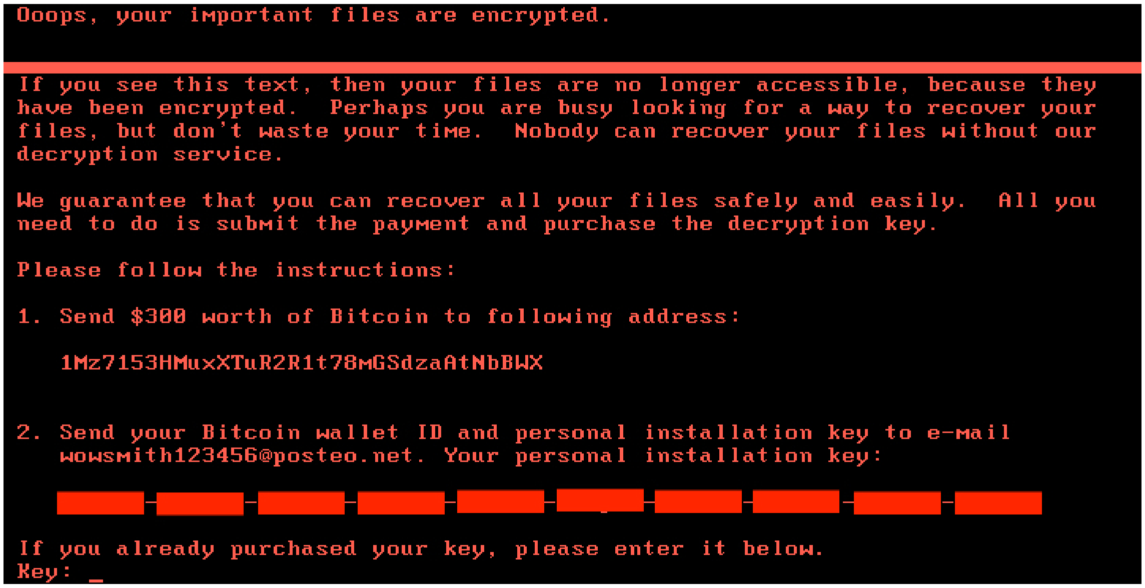
2. Introduction

Ransomware-Petya is different than regular ransomware in that upon execution, it infects low-level structure (MBR [Master Boot Record], MFT [Master File Table]) and doesn’t allow the computer to boot normally. It will infect MBR and on restart, it has its own low language code to encrypt MFT, which makes the drive inaccessible. Petya works by exploiting a vulnerability in the SMBv1 protocol to get a foothold on vulnerable machines connected online. Microsoft patched the flaw in **MS17-010**, released in March, but that doesn't mean all Windows PC owners have applied the security update.

3. Infection Vector and Analysis

It has been reported that variants of Petya ransomware with worm-like capabilities is spreading. The ransomware leverages etenalblue exploit, genuine psexec or wmic with appropriate credentials for a quick spread.

These mechanisms are used to attempt installation and execution of the dropped file "C:\Windows\perfc.dat" on other devices to spread laterally. The dropped file, if managed to get the Administrator privileges, will encrypt the Master File Tree (MFT) tables for NTFS partitions and overrides the Master Boot Record (MBR) with a custom bootloader making the system unusable. Further the malware creates a scheduled task via schtasks /at to reboot the system one hour after infection. 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: _
```

4. Indicator of Compromise (IoCs)

IOC’s are mentioned below:

Type	Details
IP	95.141.115.108
	185.165.29.78
	84.200.16.242
	111.90.139.247
DOMAIN	coffeinoffice.xyz
	french-cooking.com
	sundanders.online
URL	http[:]//french-cooking[.]com/myguy[.]exe
	http[:]//84[.]200[.]16[.]242/myguy[.]xls
	http://84[.]200[.]16[.]242/Profoma[.]xls
	http://84[.]200[.]16[.]242/Lucky[.]exe
	http://185.165.29.78/~alex/svchost.exe
sha256	02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f
	eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998
	64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
	fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47e097df04a5f7d6d206
	ee29b9c01318a1e23836b949942db14d4811246fdae2f41df9f0dcd922c63bc6
	22053C34DCD54A5E3C2C9344AB47349A702B8CFDB5796F876AEE1B075A670926
	1FE78C7159DBCB3F59FF8D410BD9191868DEA1B01EE3ECCD82BCC34A416895B5
	EEF090314FBEC77B20E2470A8318FC288B2DE19A23D069FE049F0D519D901B95
MD5	9B853B8FE232B8DED38355513CFD4F30
	CBB9927813FA027AC12D7388720D4771
	a809a63bc5e31670ff117d838522dec433f74bee
	bec678164cedea578a7aff4589018fa41551c27f
	d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
	aba7aa41057c8a6b184ba5776c20f7e8fc97c657
	0ff07caedad54c9b65e5873ac2d81b3126754aac
	51eafbb626103765d3aedfd098b94d0e77de1196
	078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
	7ca37b86f4acc702f108449c391dd2485b5ca18c
	2bc182f04b935c7e358ed9c9e6df09ae6af47168
	1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
	82920a2ad0138a2a8efc744ae5849c6dde6b435d

Filename	C:\0487382a4daf8eb9660f1c67e30f8b25.hta
	petwrap.exe
	C:\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll
	Order-20062017.doc
	myguy[1].hta
	myguy.xls
	dllhost.dat
Named pipe	{df458642-df8b-4131-b02d-32064a2f4c19}
Emails	wowsmith123456@posteo.net
	wowsmith123456@posteo.net
	iva76y3pr@outlook.com
	carmellar4hegp@outlook.com
	amanda44i8sq@outlook.com

Characteristics and Symptoms:

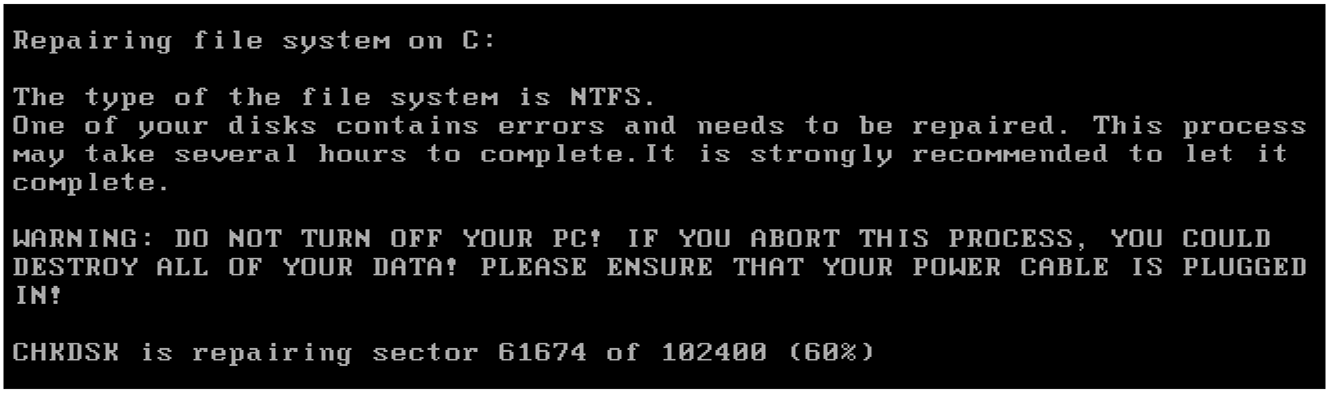
Upon execution, Ransomware-Petya will show the UAC window to gain the Administrator privilege to execute the binary. After it runs, it will keep original MBR with simple byte-wise XOR operation to sector 56 (XoR Key = 0x37).

Later, it will overwrite MBR with its own code. It also fills its own content for the next 32 sectors and will perform simple byte-wise XOR encryption to next 32 sectors (with same XoR key 0x37).

Malware keeps its 16-bit code from sector 34 to 49, which has booting image and encryption and decryption routines. In Sector 54, it will write a personal decryption code and TOR URL.

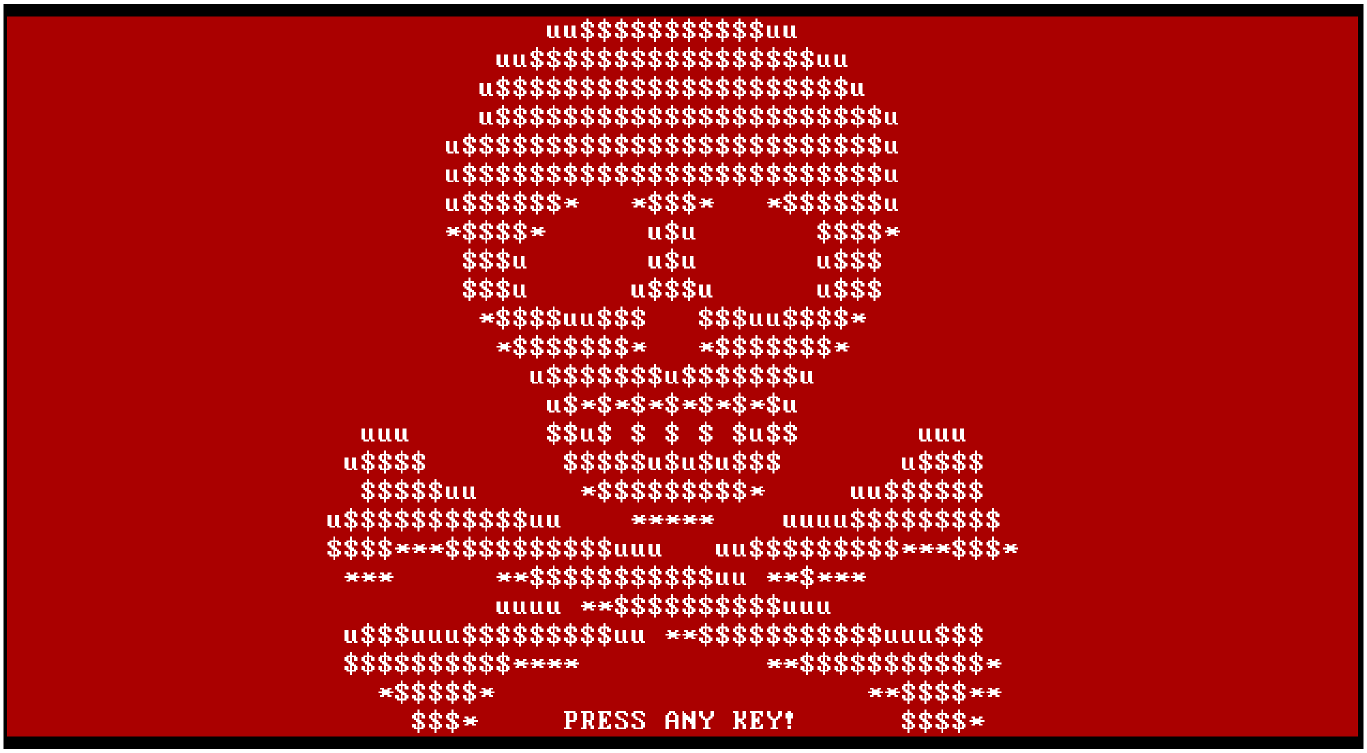
It will then adjust privilege to SeShutDownPrivilege, and use the undocumented Windows API "NtRaiseHardError" to create a blue screen to restart the infected system.

On reboot, it will show the following screen showing "chkdsk" is repairing. While showing this, it will encrypt the Master File Table.(MFT):



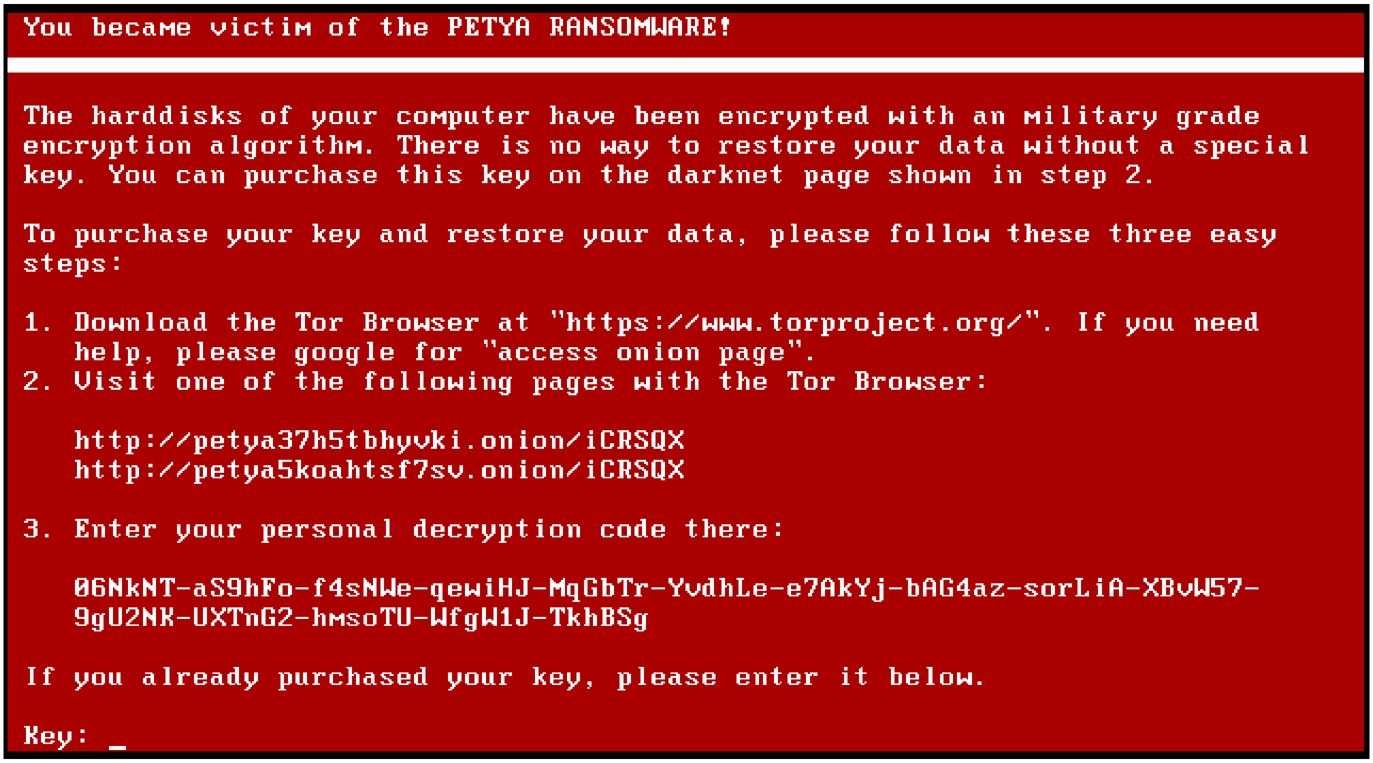
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 61674 of 102400 (60%)
```

After it encrypts MFT, it will show the red skeleton screen (Danger):



```
PRESS ANY KEY!
```

Finally, it will show TOR URLs asking for ransom for the victim machine. At this stage the malware has encrypted MFT, which makes the disk unreadable even if you access the disk from other devices.



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/iCRSQX
   http://petya5koahtsf7sv.onion/iCRSQX

3. Enter your personal decryption code there:

   06NkNT-aS9hFo-f4sNWe-qewiHJ-MqGbTr-YvdhLe-e7AkYj-bAG4az-sorLiA-XBvW57-
   9gU2NK-UXTnG2-hmsoTU-WfgW1J-TkhBSg

If you already purchased your key, please enter it below.

Key: _
```

5. Mitigation

These are following mitigation to avoid these kind of attacks,

1. 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
2. Use updated antivirus software.
3. 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.
4. Applocker policies to block execution of files having name perfc.dat as well as psexec.exe utility from sysinternals.
5. Don't 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.
6. 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.
7. 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.
8. 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.
9. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
10. Disable remote Desktop Connections, employ least-privileged accounts.

Disclaimer:-

1. These advisories are for information purpose only. We recommend you to act upon these advisories at your own discretion after conducting risk analysis in your specific environment.

2. These advisories are time sensitive in nature and may be over ridden is subsequent updates from our side as new information is received on the threats.