# **Petya / NotPetya** Malware Recovery Advisory

This document provides a quick overview of the Petya / Non Petya ransomware and provides preventive measures as well as recovery guidance.

## Overview

On 27th June, 2017, a new worm like ransomware called Petya / NotPetya has affected organizations around the world. After the infection the malware, using the password harvesting utility, ETERNALBLUE exploit and ETERNALROMANCE exploit, infects all computers on the local network. Despite the fact that Petya / NotPetya virus actively uses these two exploits to infect as many computers as possible, it does not spread through the Internet, it hits computers only on the local network (where the virus first penetrated).

Petya / NotPetya encrypts entire hard drive, by encrypting the system volume, Master File Table and Master Boot Record, Petya / NotPetya prevents the system from booting normally and hooks it into Petya's own bootloader with the ransom note displayed on the screen. **This prevents attempts at file recovery using standard forensic techniques such as booting to a LiveCD or other OS.**

After infection Petya demands approximately 300$USD in bitcoins in order to decrypt the files. After transferring the bitcoins an email has to be sent to the hacker providing wallet's address so that the hacker can verify the transaction and respond with the decryption keys. However, **since the hackers email address has apparently been taken down, paying the ransom in order to decrypt the files is currently not possible.**

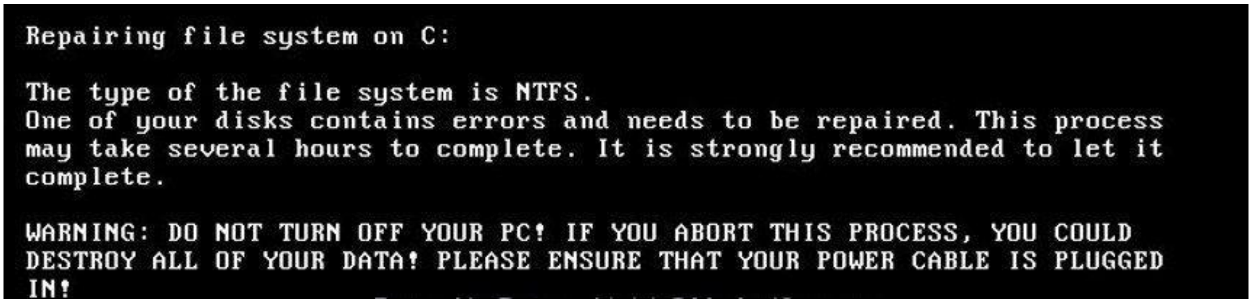
## How it infects?

Microsoft has stated in their latest blog post that at least some of the infections were started from Ukrainian Accounting software MeDoc's legitimate update process.

The ransomware spreading functionality is composed of multiple methods responsible for:

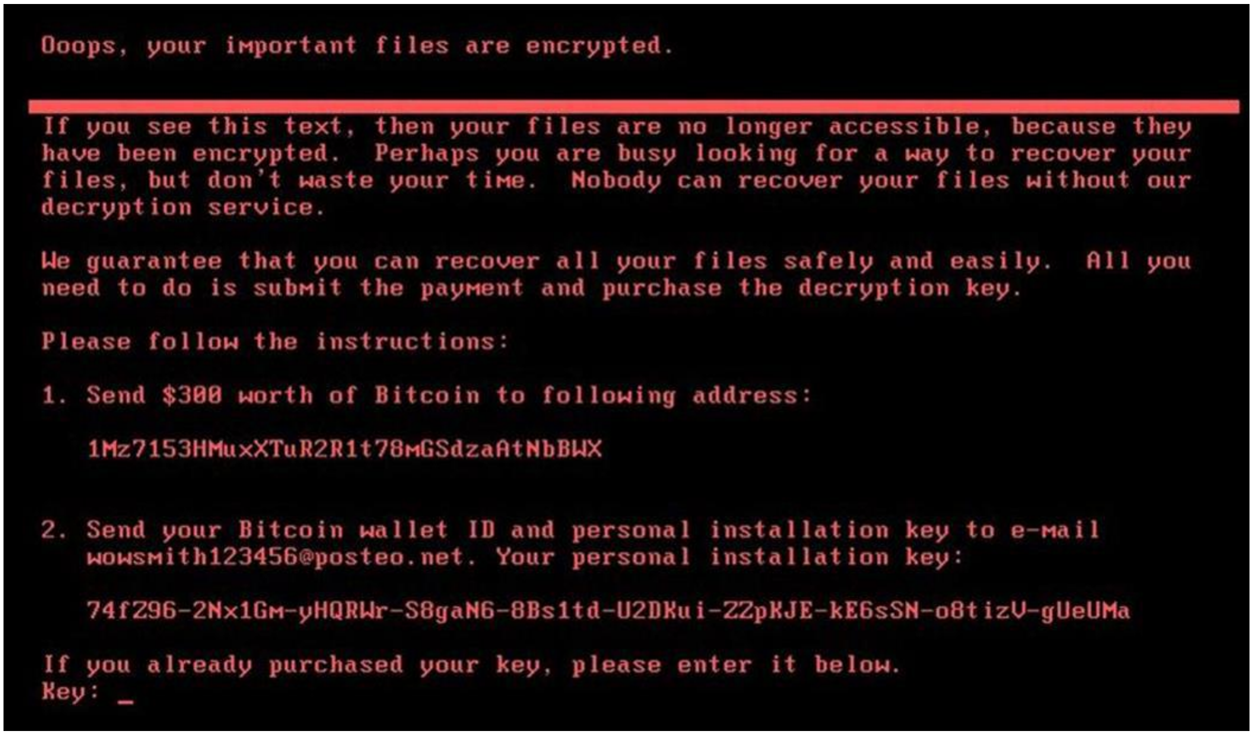
- Stealing credentials or re-using existing active sessions
- Using file-shares to transfer the malicious file across machines on the same network
- Using existing legitimate functionalities to execute the payload or abusing SMB vulnerabilities for unpatched machines

On infecting a computer with admin privilege, this malware forces the computer to reboot after it rewrites the MBR (Master Boot Record) with a custom boot loader, and on booting it encrypts the user files and MFT (Master File Table) and shows a ransom note.



```
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!
```

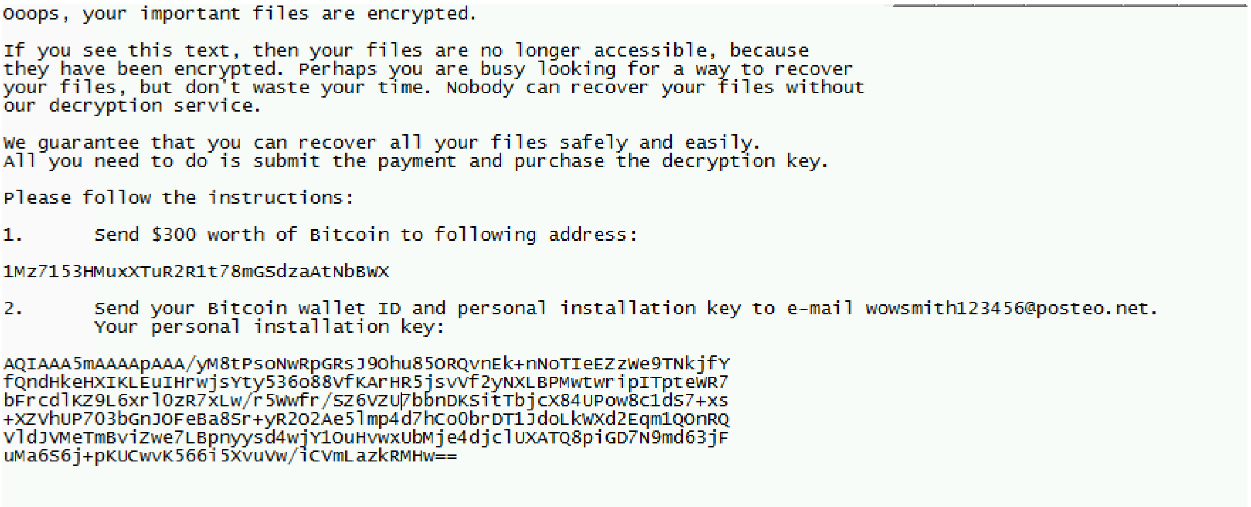
When this process is complete, the following message is displayed to the user.



```
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:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

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

**On infecting a computer without admin privilege**, this ransomware attempts to encrypt all user files with commonly known extensions in all folders in all fixed drives, except for C:\Windows. Unlike most other ransomware, this threat does not append a new file name extension to encrypted files. Instead, it overwrites the said files.

After completing its encryption routine, this ransomware drops a text file called README.TXT with the following text:



```
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:

AQIAAA5mAAAApAAA/yM8tPsoNwRpGRsJ9Ohu85ORQvnEk+nNoTIeEZzWe9TNkjfY
fQndHkeHXIKLEuIHrwjsYty536o88VfKArHR5jsvVf2yNXLBPMwtwripITpteWR7
bFrcdlKZ9L6xrl0zR7xLw/r5Wwfr/SZ6VZU7bbnDKSitTbjcX84UPow8c1dS7+xs
+XZVhUP7O3bGnJOFeBa8Sr+yR2O2Ae5lmp4d7hCoObrDT1JdoLkWXd2Eqm1QOnRQ
VldJVMeTmBviZwe7LBpnyysd4wjY1OuHvwxUbMje4djclUXATQ8piGD7N9md63jF
uMa6S6j+pKUCwvK566i5XvuVw/iCVmLazkRMHw==
```

## Prevention

This ransomware also clears the System, Setup, Security, Application event logs and deletes NTFS journal info.

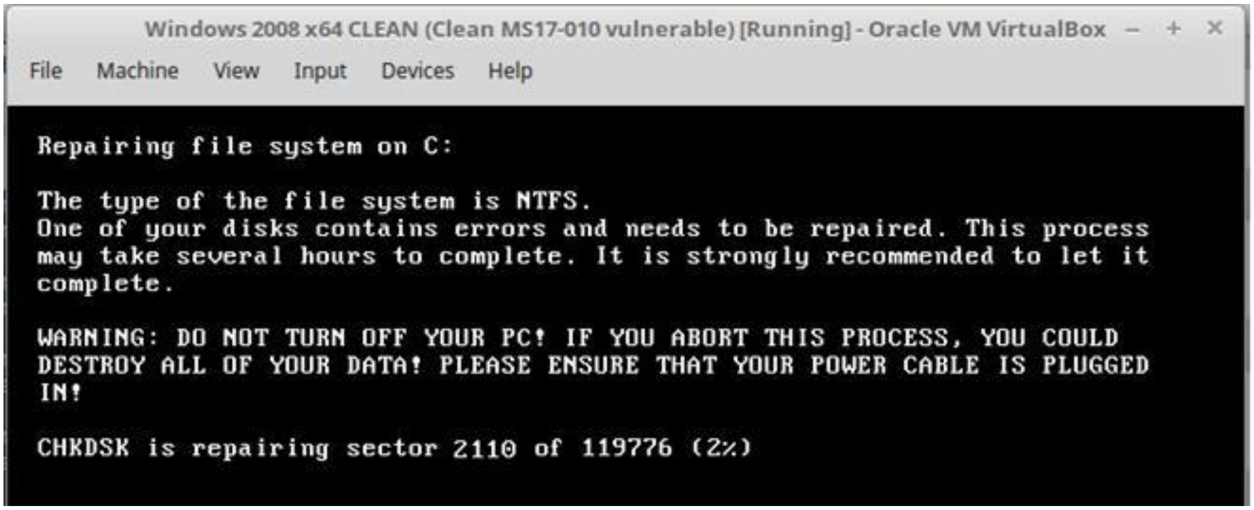
- Patching the computer with security update MS17-010 as soon as possible. Until the patch is applied, following are the possible workarounds to reduce the attack surface:
    - Disable SMBv1 with the steps documented at Microsoft Knowledge Base Article 2696547 and as recommended previously
    - Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445 and 139
    - Disable remote WMI and file sharing for a very short time period while you assess the impact and apply definition updates.
- Consistent and up-to-date system backups are critical to recovering from a ransomware infection.
- Keeping your systems patched and upgrading legacy systems will also go a long way toward preventing infection to begin with.
- Don't enable macros in document attachments received via email
- Be cautious about unsolicited attachments
- Don't give yourself more login power than you need

Microsoft patched the vulnerabilities back in March in the MS17-010 bulletin. In the wake of WannaCry, Microsoft later released patches for even legacy Windows operating systems like Windows XP.

## Recovery

The encryption process uses a dual AES-128 and RSA-2048 standard encryption model.

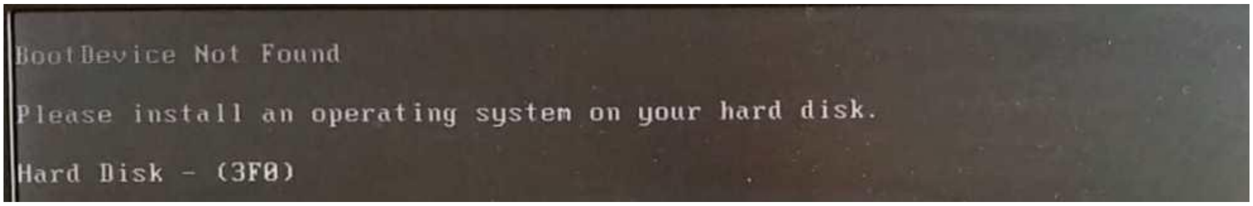
**Scenario 1**: After system reboot, if the following screen appears: IMMEDIATELY PULL OUT THE PLUG/POWER OFF/REMOVE BATTERY.


Windows 2008 x64 CLEAN (Clean MS17-010 vulnerable) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help

```
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 2110 of 119776 (2%)
```

In this scenario there is a possibility that the files can be recovered forensically depending upon the %age of encryption completed.

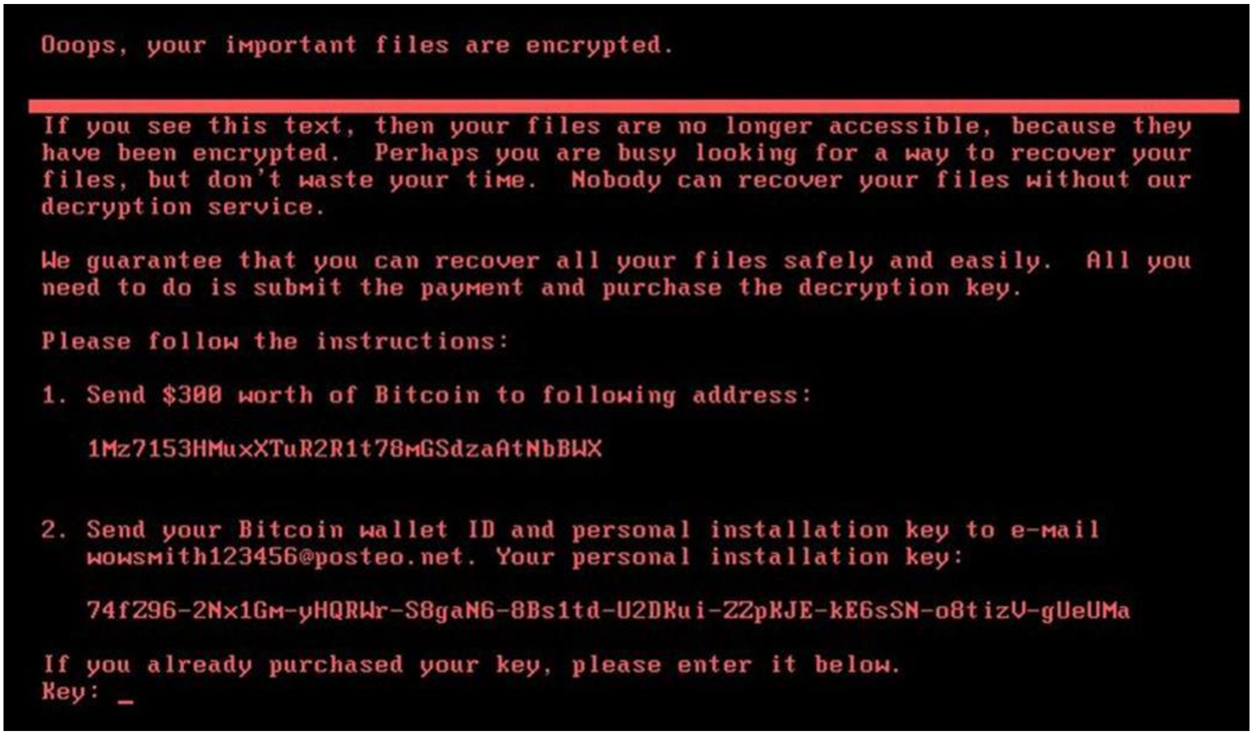
**Scenario 2**: If full disk encryption (McAfee) is enabled, then a message similar to the following will be displayed:



```
BootDevice Not Found

Please install an operating system on your hard disk.

Hard Disk - (3F0)
```

In this scenario the system has to be formatted and then data restored from a golden copy of the backup.

**Scenario 3**: Complete infection of the system (both MBR and files).



```
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:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

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

As the email of the hacker is taken down by the service provider, paying the ransom is not possible. In this scenario the system has to be formatted and data can be restored from a golden copy of the backup.

## References

- https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
- https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html
- https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Petya/NotPetya-Ransomware-Campaign/
- http://www.myantispyware.com/2017/06/28/petya-notpetya-virus/
- https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/