

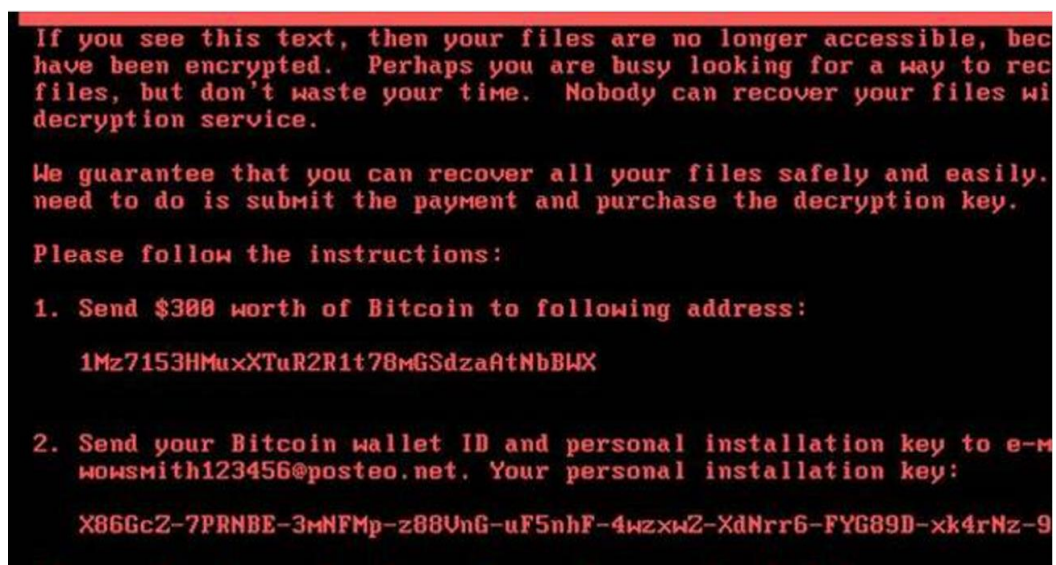


INTEZER

Analysis of
NotPetya Ransomware

Overview

A malware, referred to as NotPetya, hit organizations in Europe and the world yesterday. It was originally misclassified as previous ransomware, Petya and PetrWrap. NotPetya had shut down many systems in large organizations including the Cadbury chocolate factory in Australia, supermarkets in the Ukraine, India's largest container port, and more. It is not yet known the total amount of computers and organizations that have been harmed thus far. However, it can be said that instead of the typical ransomware that are designed to make money, NotPetya was designed to inflict severe damage. All of our customers were protected from the attack before inception, since it was detected by Intezer's Code Intelligence™ technology.



** Example screenshot of a computer infected with NotPetya*

Spreading Across Organizations

As per what's known today, in order to get into the organization, the threat actor used malicious documents with a vulnerability known as CVE-2017-0199 and also through a software supply chain attack.

After infiltrating an organization, the ransomware quickly spreads within the network using EternalBlue, an exploit leaked from the NSA. EternalBlue exploits a vulnerability in the Server Message Block (SMB) protocol used by Microsoft. In the beginning of May, the same exploit was used to spread WannaCry, another recent malware that hit more than 230,000 computers in 150 countries.

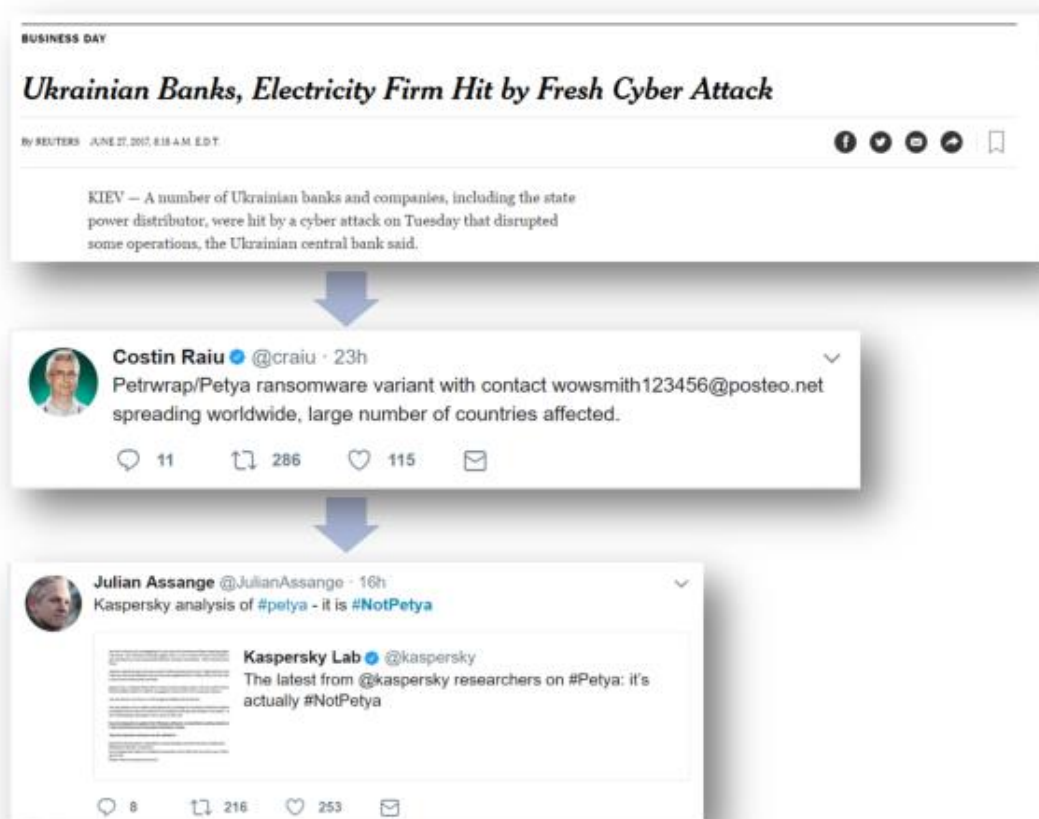
Intezer has published another report you are welcome to request related to WannaCry and its attribution to the Lazarus group, an alleged cyber unit of North Korea. You can also read a more technical analysis of this exploit under the vulnerability catalog name CVE-2017-0144.

NotPetya Analysis

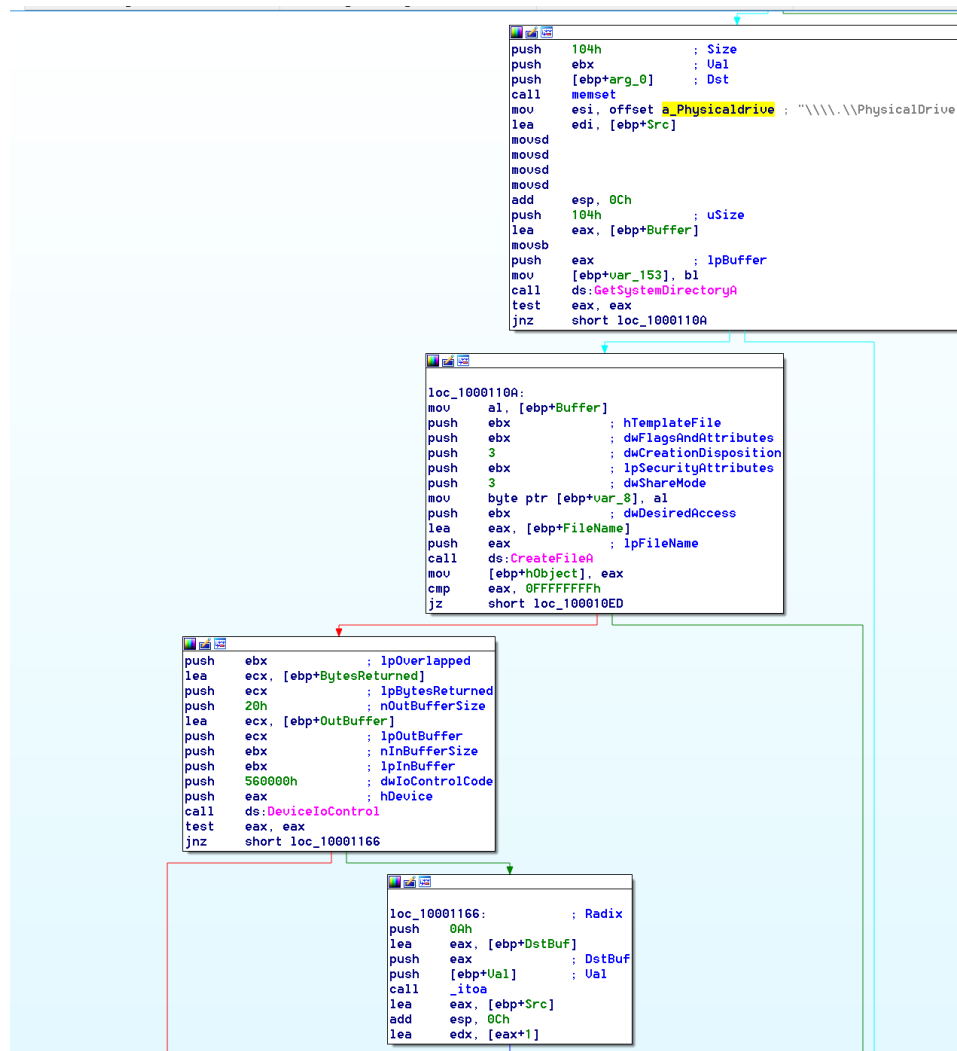
NotPetya first originated in the Ukraine by hijacking a tax accounting software, MEDoc, and its updating process. The malicious module then gets loaded into memory with the proper parameters to start the infection process.

When NotPetya first started infecting computers, the Infosec community immediately started referring to this ransomware as a newer version of Petya and PetrWrap. This is due to some of the similar behavior between NotPetya and Petya.

Upon further analysis of the code, it appears to be a threat actor that mimicked the previous Petya ransomware.



After the ransomware is loaded, it will infect the Master Boot Record of the hard drive with code to display the ransom message and encrypt the drive.



Below, you can see some of the code and data that is written to the MBR to display the ransom messages.

0001E10	20 44 41 54 41 21 20 50	4C 45 41 53 45 20 45 4E	-DATA! PLEASE EN
0001E20	53 55 52 45 20 54 48 41	54 20 59 4F 55 52 20 50	SURE THAT YOUR P
0001E30	4F 57 45 52 20 43 41 42	4C 45 20 49 53 20 50 4C	OWER CABLE IS PL
0001E40	55 47 47 45 44 00 0A 20	20 49 4E 21 00 0A 00 0A	UGGED... IN!
0001E50	00 00 20 20 43 48 48 44	53 48 20 69 73 20 72 65	...CHKDSK is re
0001E60	70 61 69 72 69 6E 67 20	73 65 63 74 6F 72 00 00	pairing sector..
0001E70	50 6C 65 61 73 65 20 72	65 62 6F 6F 74 20 79 6F	Please reboot yo
0001E80	75 72 20 63 6F 6D 70 75	74 65 72 21 00 00 20 44	ur computer!...D
0001E90	65 63 72 79 70 74 69 6E	67 20 73 65 63 74 6F 72	ecrypting sector
0001EA0	00 00 0A 00 00 20 4F	6F 6F 70 73 2C 20 79 6FOops, yo
0001EB0	75 72 20 69 6D 70 6F 72	74 61 6E 74 20 66 69 6C	ur important fil
0001EC0	65 73 20 61 72 65 20 65	6E 63 72 79 70 74 65 64	es are encrypted
0001ED0	2E 00 0A 00 00 20 49	66 20 79 6F 75 20 73 65If you se
0001EE0	65 20 74 68 69 73 20 74	65 78 74 2C 20 74 68 65	e this text, the
0001EF0	6E 20 79 6F 75 72 20 66	69 6C 65 73 20 61 72 65	n your files are
0001F00	20 6E 6F 20 6C 6F 6E 67	65 72 20 61 63 63 65 73	no longer acces
0001F10	73 69 62 6C 65 2C 20 62	65 63 61 75 73 65 20 74	sible, because t
0001F20	68 65 79 00 0A 20 68 61	76 65 20 62 65 65 6E 20	hey..have been
0001F30	65 6E 63 72 79 70 74 65	64 2E 20 20 50 65 72 68	encrypted...Perh
0001F40	61 70 73 20 79 6F 75 20	61 72 65 20 62 75 73 79	aps you are bus
0001F50	20 6C 6F 6F 68 69 6E 67	20 66 6F 72 20 61 20 77	looking for a w
0001F60	61 79 20 74 6F 20 72 65	63 6F 76 65 72 20 79 6F	ay to recover y
0001F70	75 72 00 0A 20 66 69 6C	65 73 2C 20 62 75 74 20	ur...files, but
0001F80	64 6F 6E 27 74 20 77 61	73 74 65 20 79 6F 75 72	don't waste you
0001F90	20 74 69 6D 65 2E 20 20	4E 6F 62 6F 64 79 20 63	time...Nobody c
0001FA0	61 6E 20 72 65 63 6F 76	65 72 20 79 6F 75 72 20	an recover your
0001FB0	66 69 6C 65 73 20 77 69	74 68 6F 75 74 20 6F 75	files without ou
0001FC0	72 00 0A 20 64 65 63 72	79 70 74 69 6F 6E 20 73	r...decryption s
0001FD0	65 72 76 69 63 65 2E 00	0A 00 0A 20 57 65 20 67	ervice.....We g
0001FE0	75 61 72 61 6E 74 65 65	20 74 68 61 74 20 79 6F	uarantee that yo
0001FF0	75 20 63 61 6E 20 72 65	63 6F 76 65 72 20 61 6C	u can recover al
0002000	6C 20 79 6F 75 72 20 66	69 6C 65 73 20 73 61 66	l your files saf
0002010	65 6C 79 20 61 6E 64 20	65 61 73 69 6C 79 2E 20	ely and easily.
0002020	20 41 6C 6C 20 79 6F 75	00 0A 20 6E 65 65 64 20	All you..need
0002030	74 6F 20 64 6F 20 69 73	20 73 75 62 6D 69 74 20	to do is submit
0002040	74 68 65 20 70 61 79 6D	65 6E 74 20 61 6E 64 20	the payment and
0002050	70 75 72 63 68 61 73 65	20 74 68 65 20 64 65 63	purchase the dec
0002060	72 79 70 74 69 6F 6E 20	68 65 79 2E 00 0A 00 0A	ryption key.....

After writing code to the MBR, another file is dropped to the disk. This file is a worm that attempts to spread across the network via WMIC or a copy of PSEXec that is also dropped to the disk and attempts to steal the network administrator credentials using code from a known open source credential stealing tool called “mimikatz.”

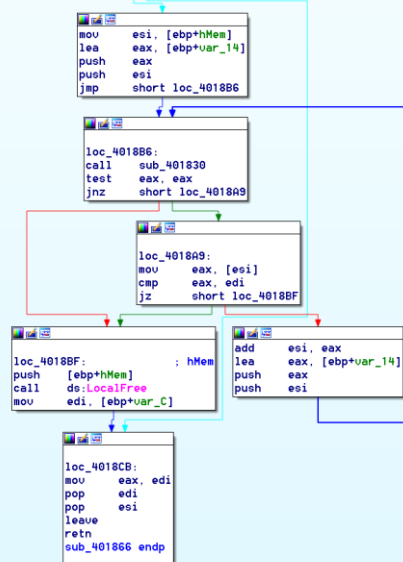
```

: int __cdecl sub_401866(HLOCAL hMem)
sub_401866 proc near
var_14= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
DestinationString= LSA_UNICODE_STRING ptr -8
hMem= dword ptr 8

push ebp
mov ebp, esp
sub esp, 14h
push esi
lea eax, [ebp+DestinationString]
mov [ebp+var_14], eax
mov [ebp+hMem], eax
push edi
mov [ebp+var_10], eax
push offset SourceString : "lsass.exe"
lea eax, [ebp+DestinationString]
xor edi, edi
push eax
mov [ebp+var_C], edi
call RtlInitUnicodeString
push 5
lea esi, [ebp+hMem]
mov [ebp+hMem], edi
call sub_4017D3
cmp eax, edi
pop ecx
jnl short loc_4018CB

```

mimikatz



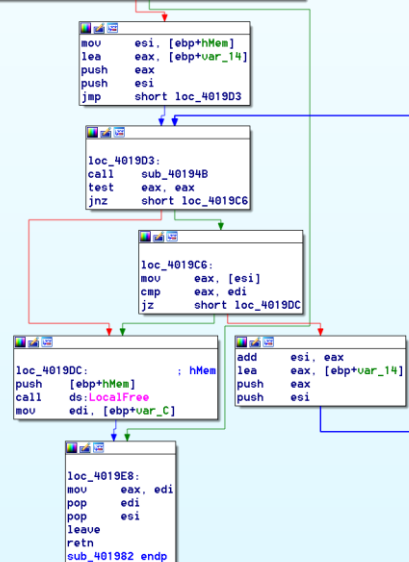
```

: int __cdecl sub_401982(HLOCAL hMem)
sub_401982 proc near
var_14= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
DestinationString= LSA_UNICODE_STRING ptr -8
hMem= dword ptr 8

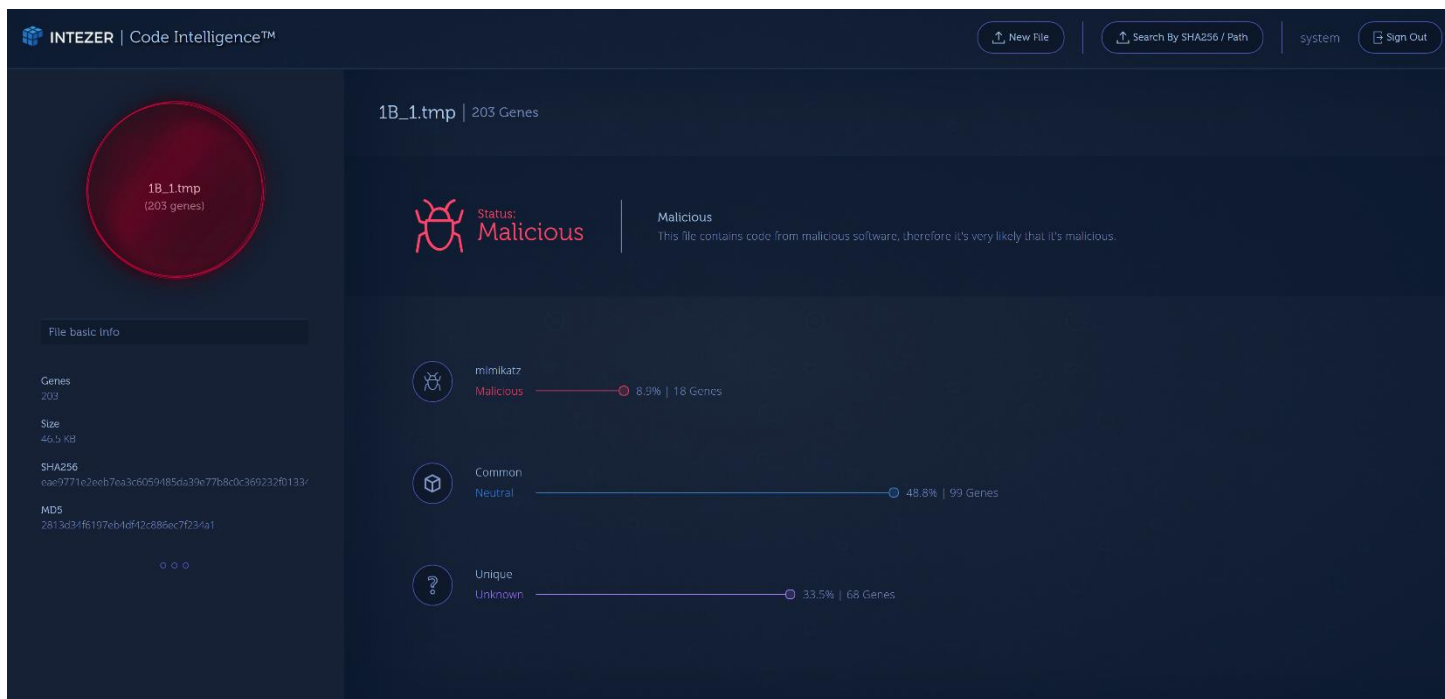
push ebp
mov ebp, esp
sub esp, 14h
push esi
lea eax, [ebp+DestinationString]
mov [ebp+var_14], eax
mov [ebp+hMem], eax
push edi
mov [ebp+var_10], eax
push offset SourceString : "lsass.exe"
lea eax, [ebp+DestinationString]
xor edi, edi
push eax
mov [ebp+var_C], edi
call ds:RtlInitUnicodeString
push 5
lea esi, [ebp+hMem]
mov [ebp+hMem], edi
call sub_4018D9
pop ecx
cmp eax, edi
jnl short loc_4019E8

```

NotPetya



As can be seen in the screenshot of the Code Intelligence™ web service, we find gene connections in this sample to the credential stealer mimikatz. (MD5: 2813d34f6197eb4df42c886ec7f234a1)



After the network credentials have been stolen and the ransomware has spread, it will begin to encrypt the files on disk that end in the following extensions:

.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 then proceeds to restart your computer. Next, the user will be presented with a fake screen saying chkdsk is repairing the sectors on your hard drive. In this time, the ransomware is encrypting the entire MFT. After the encryption is complete, the user is then presented with a new message with instructions to send about \$300 worth of Bitcoin to unlock the computer.

Summary

The behavior of NotPetya is similar to that of the previous Petya ransomware, but we can see, according to our Code Intelligence™ technology, that the code is completely different. Either this is a new threat actor or the author of the malware has redone the code from scratch.

Our customers are and were protected from the NotPetya malware, since like almost any other malware, it reuses code from previous malware or hack tools.

Jay Rosenberg

Senior Security Researcher

jay@intezer.com

Intezer Labs

Indicators of Compromise

File MD5s

- 71b6a493388e7d0b40c83ce903bc6b04
- e285b6ce047015943e685e6638bd837e
- 7e37ab34ecdcc3e77e24522ddfd4852d
- 2813d34f6197eb4df42c886ec7f234a1
- 0df7179693755b810403a972f4466afb
- 42b2ff216d14c2c8387c8eabfb1ab7d0
- e595c02185d8e12be347915865270cca

Tool

Since only the main module of the ransomware was available, the initialization function had to be reverse engineered to call it with the correct parameters. The following link is to some code that will allow a researcher to load the module for analysis.

<https://gist.github.com/jayint3z3r/b100339590b27cfffacd8eab488c82c0d>