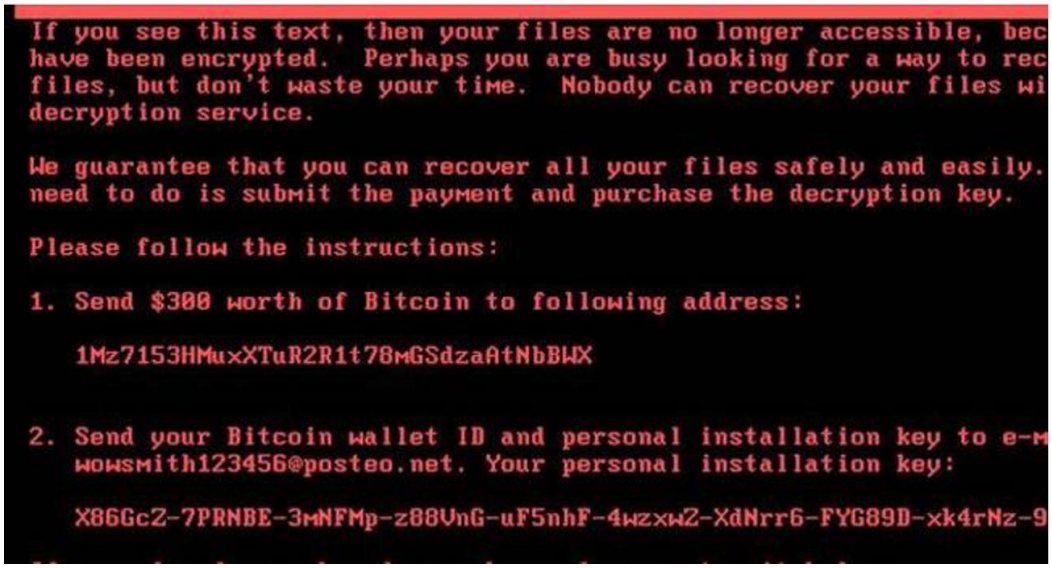
INTEZER

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.

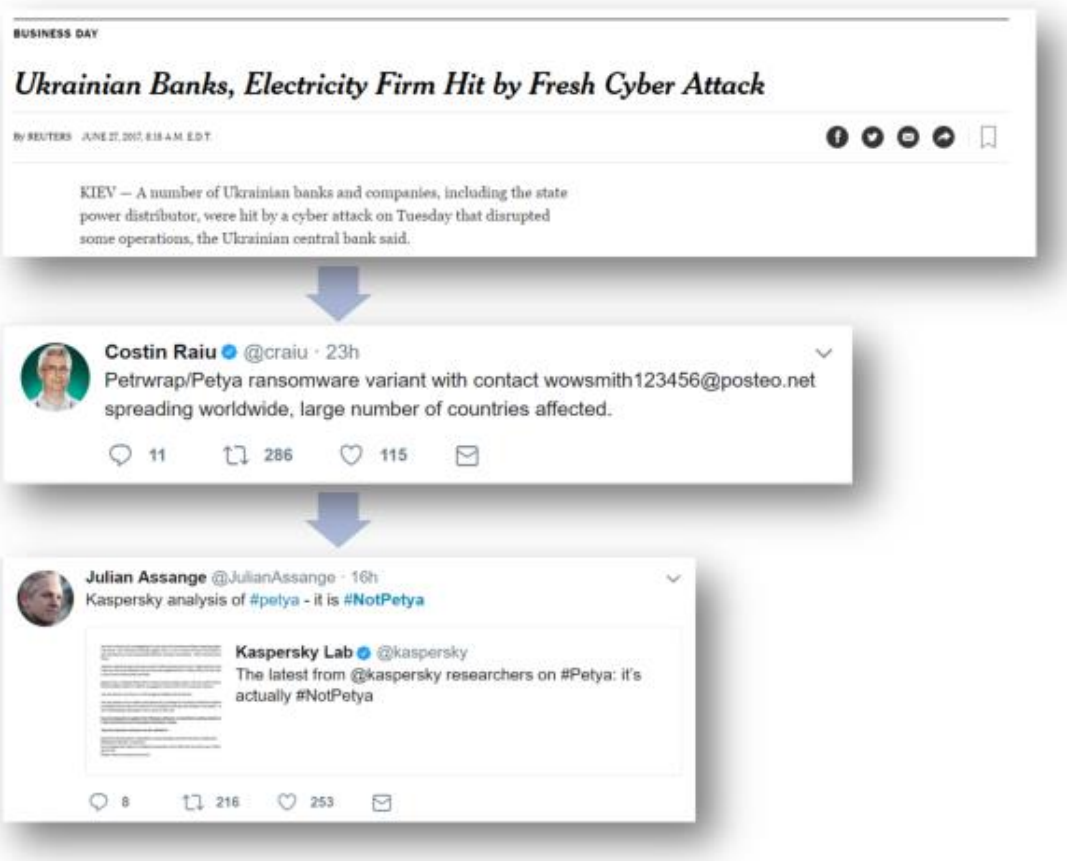
Intezer has published another report you are welcome to request related to WannaCry and its attribution to the Lazarus group, an alleged cyber unit of North Korea. You can also read a more technical analysis of this exploit under the vulnerability catalog name CVE-2017-0144.

NotPetya Analysis

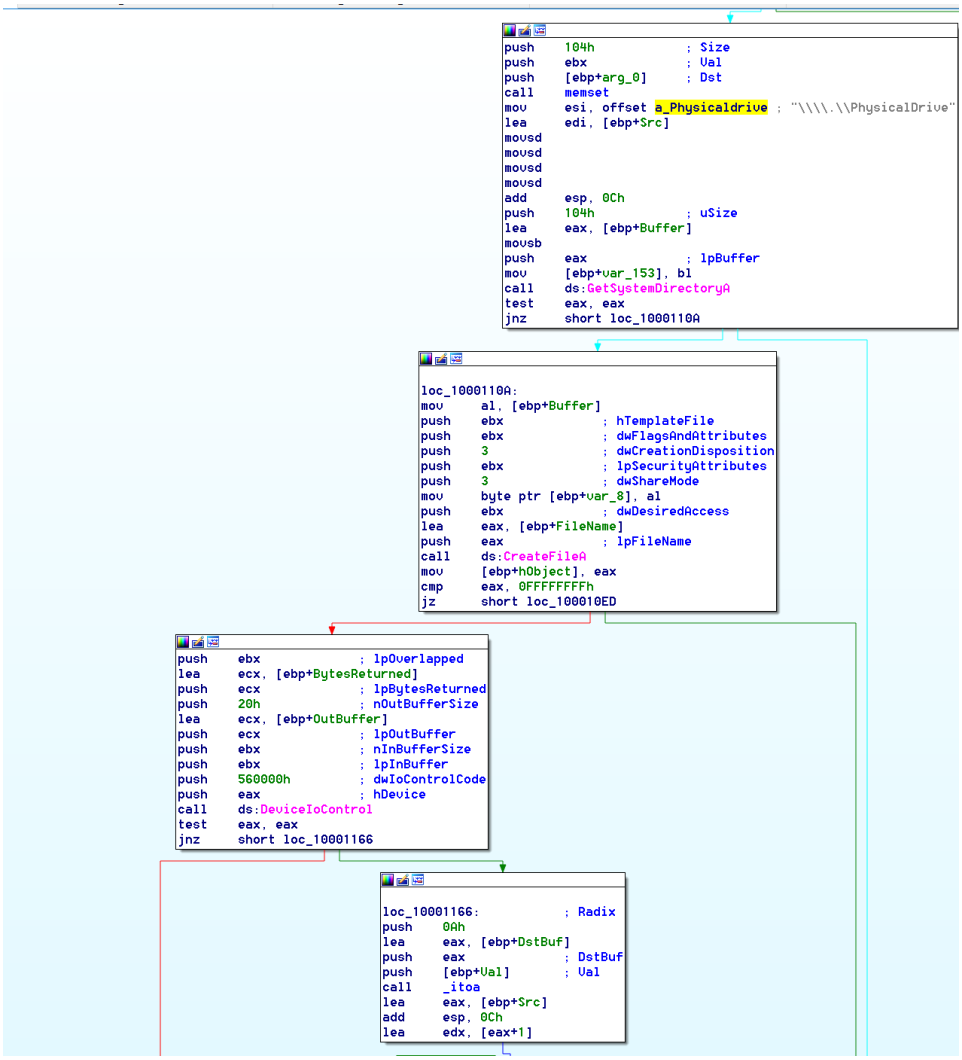
NotPetya first originated in the Ukraine by hijacking a tax accounting software, MEDoc, and it's updating process. The malicious module then gets loaded into memory with the proper parameters to start the infection process.

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.

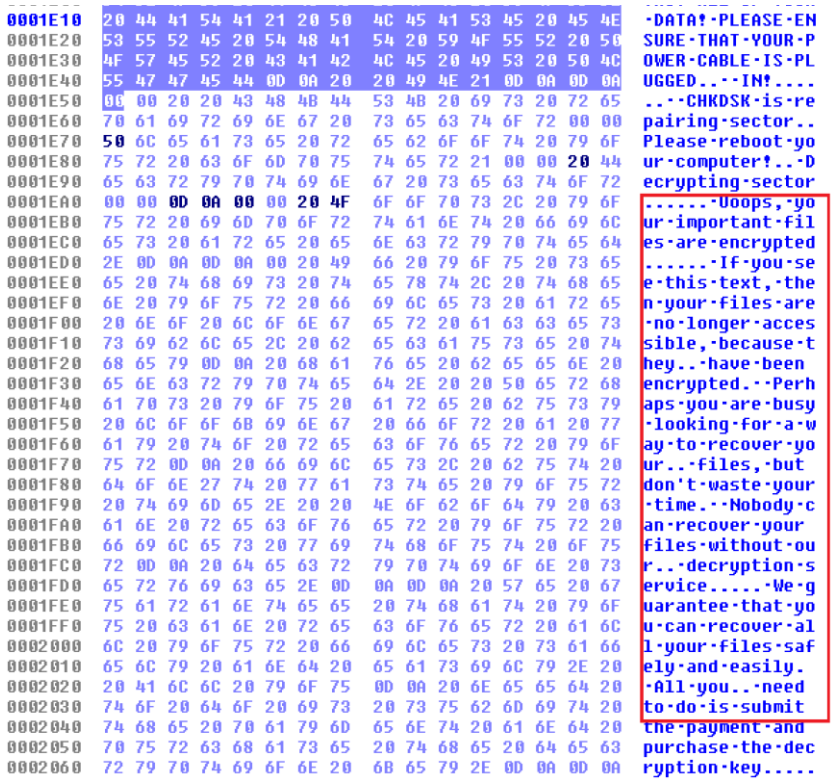
Upon further analysis of the code, it appears to be a threat actor that mimicked the previous Petya ransomware.



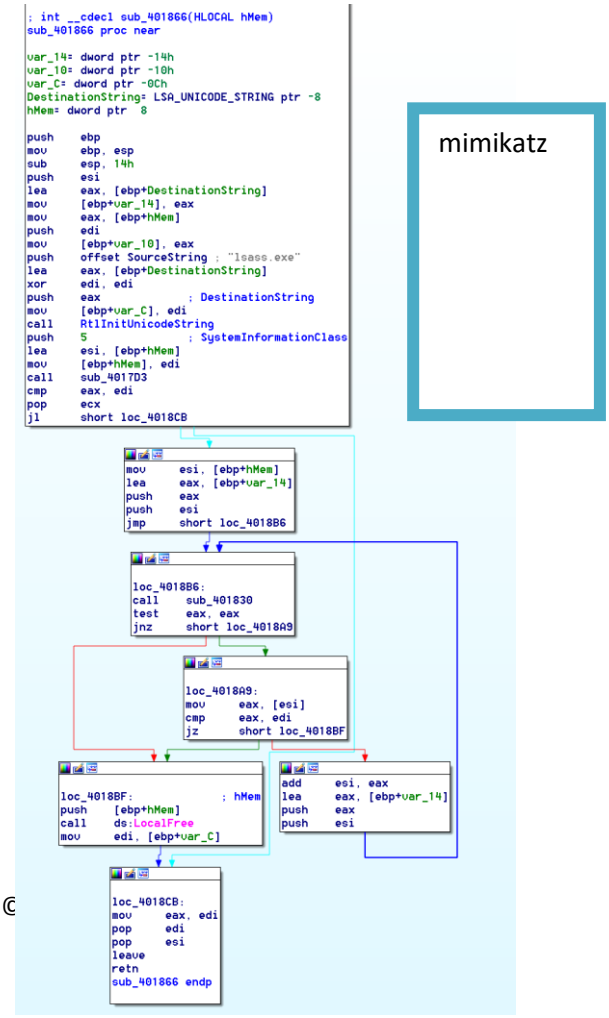
After the ransomware is loaded, it will infect the Master Boot Record of the hard drive with code to display the ransom message and encrypt the drive.

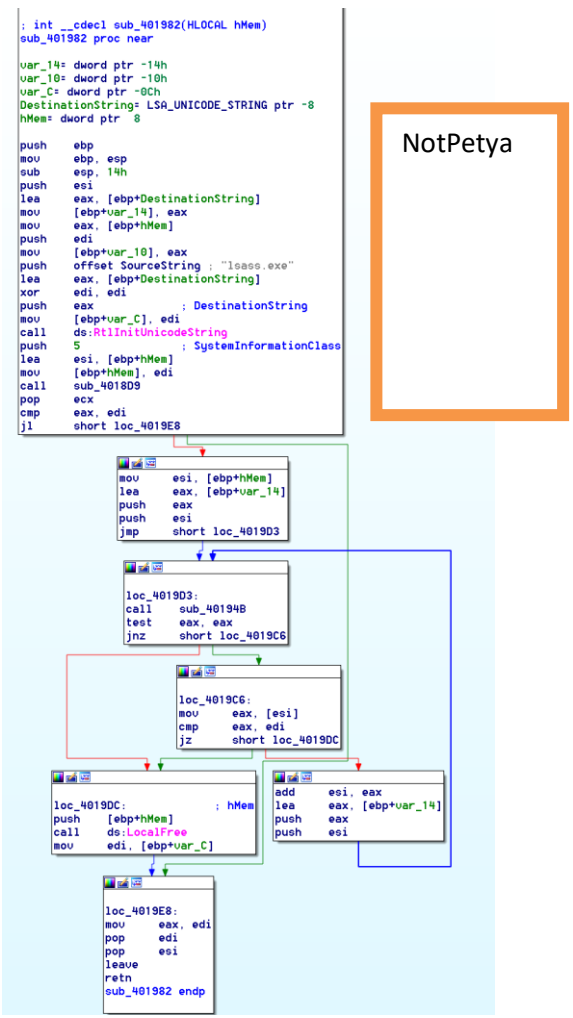


Below, you can see some of the code and data that is written to the MBR to display the ransom messages.

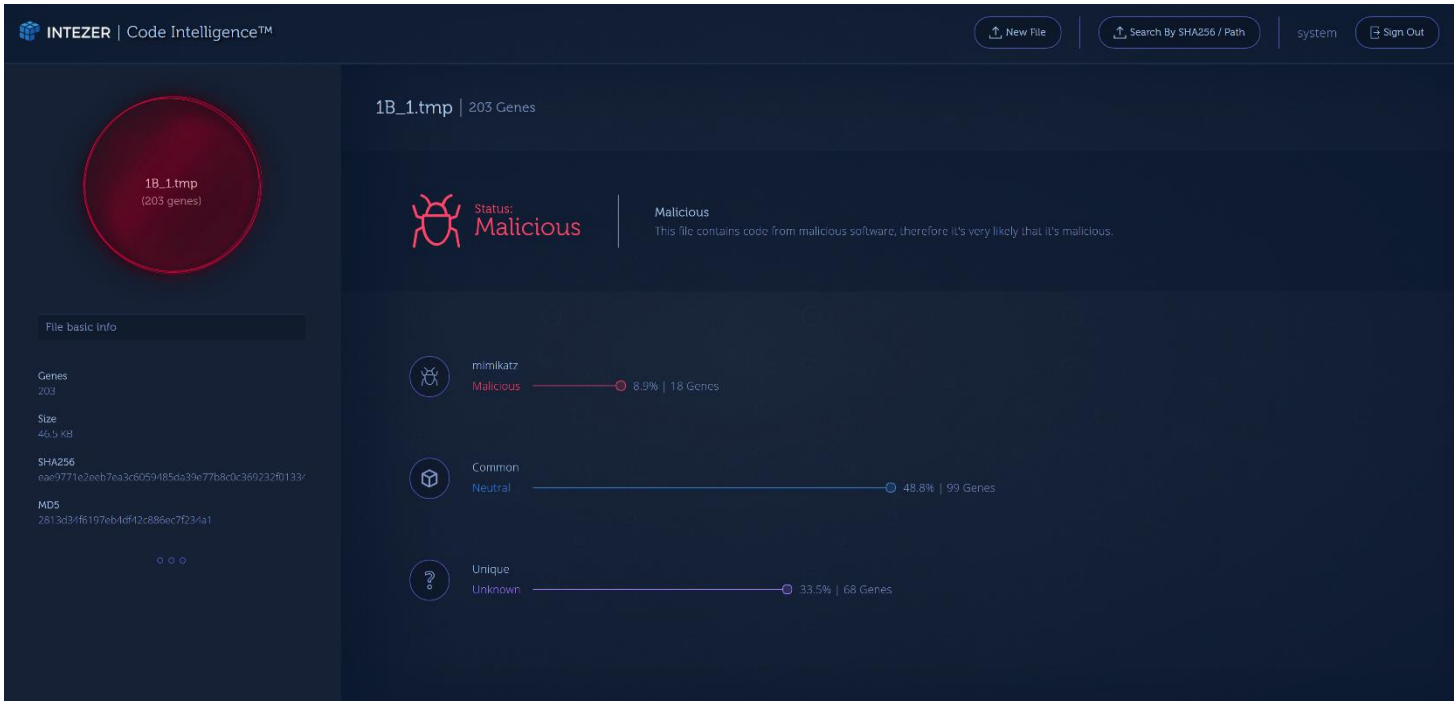


After writing code to the MBR, another file is dropped to the disk. This file is a worm that attempts to spread across the network via WMIC or a copy of PSExec that is also dropped to the disk and attempts to steal the network administrator credentials using code from a known open source credential stealing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





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/b100339590b27cffacd8eab488c82c0d