Written by Ben Lee

Malware Analysis Report - NotPetya

2022-23-01

EXECUTIVE SUMMARY

NotPetya is a malware that was discovered on June 17th 2017. It targeted many Windows Operating Systems using a SMB exploit named 'Eternal Blue' originally created by the National Security Agency (NSA). It encrypted data within compromised systems acting similar to a ransomware, displaying messages to send bitcoin for keys to decrypt the data. However, it also destroyed hard disks of such systems so data would be non-recoverable, leading the malware to be known as a form of wiper malware.

This malware analysis report will go over the threat intelligence motivations behind NotPetya, some capabilities that I have deduced from analyzing the malware and at the end of the report, provide recommendations for mitigating and preventing the malware from spreading.

TABLE OF CONTENTS

MITRE ATT&CK MATRIX

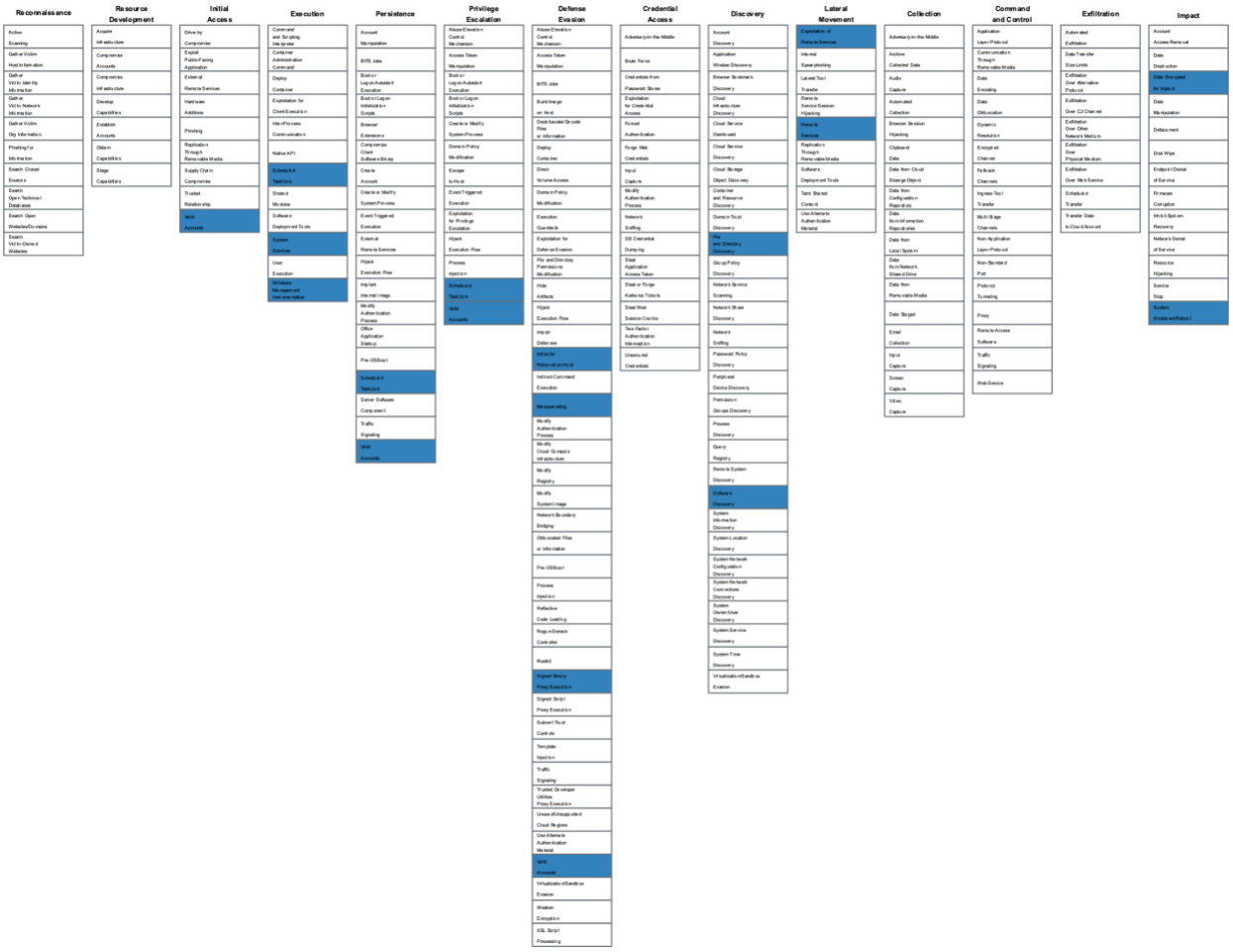

Figure 1.1 – MITRE ATT&CK Navigator

Technique ID	Tactic Name	Technique Name	Description
T1486	Impact	Data Encrypted for Impact	NotPetya encrypts user files and disk structures such as the MBR with 2048-bit RSA key and generated AES-128 bit key.
T1210	Lateral Movement	Exploitation of Remote Services	NotPetya uses two SMB exploits Eternal Blue and Eternal Romance to spread to other systems on a network.
T1083	Discovery	File and Directory Discovery	NotPetya searches for files with the correct file extensions prior to encryption
T1036	Defense Evasion	Masquerading	Notpetya drops a file named dllhost.dat for remote execution
T1021.002	Lateral Movement	Remote Services: SMB/ Windows Admin Shares	NotPetya uses dllhost.dat to access the network and for remote execution on a system
T1063.005	Execution, Persistence, Privilege Escalation	Scheduled Task/Job: Scheduled Task	Notpetya creates a scheduled task to reboot the system an hour after initial infection
T1070.001	Defense Evasion	Indicator Removal on Host: Clear Windows Event logs	Notpetya uses wevtutil command to clear Windows Event Logs
T1218.011	Defense Evasion	Signed Binary Proxy Execution: Rundll32	Notpetya uses rundll32.exe to install itself on a system via wmic
T1518.001	Discovery	Software Discovery: Security Software Discovery	Notpetya searches for specific antivirus programs and checks if they are running on an infected machine
T1569.002	Execution	System Services: Service Execution	Notpetya uses dllhost.dat for executing commands
T1529	Impact	System Shutdown/Reboot	Notpetya shutdown/reboots system after one hour of initial infection
T1078.003	Defense Evasion, Persistence, Privilege escalation, Initial Access	Valid Accounts: Local Accounts	Notpetya uses user credentials via wmic to spread itself to remote systems
T1047	Execution	Windows Management Instruction	Notpetya uses wmic to execute malicious commands and propagate itself across a network

THREAT INTEL INSIGHTS

TARGETS

The malware has spread and infected numerous systems around the globe mainly in the countries of Ukraine, Russia and East Europe. The majority of its infections are however situated in Ukraine, affecting multiple Ukrainian businesses, state-enterprises, banks, transport and metro systems.

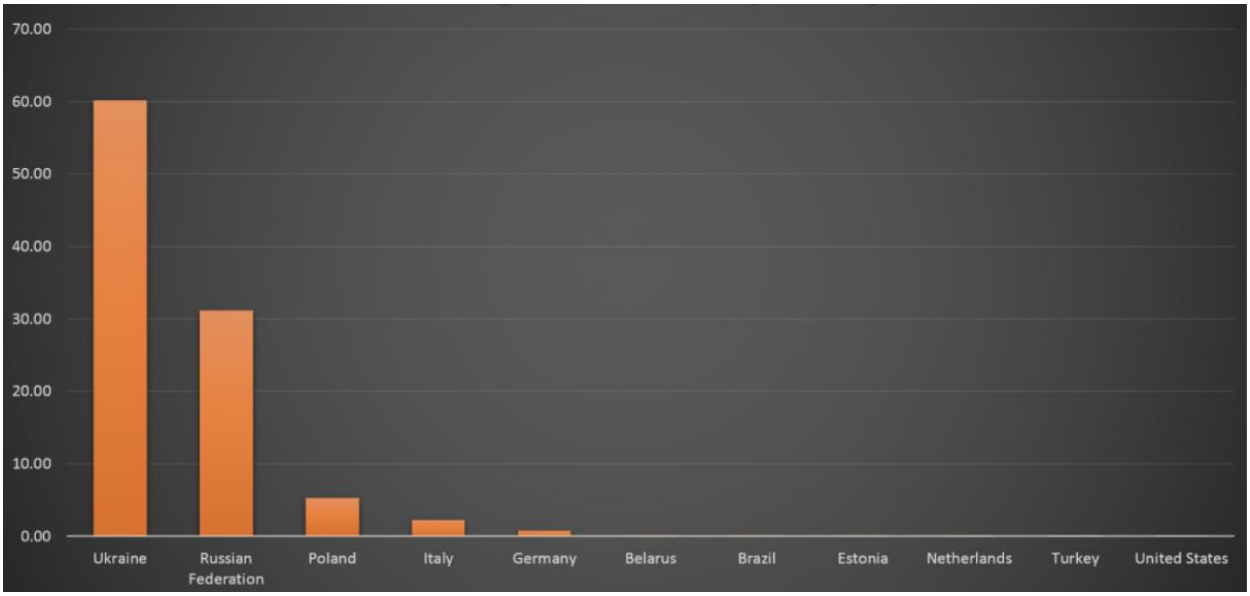

Figure 2.1 – Percentage of NotPetya Infections per country

MOTIVATIONS

The threat actors created an initial infection vector through the exploitation of an update procedure for a third-party Ukrainian software product named 'MEDoc'. MEDoc is a software mainly used for tax accounting purposes in multiple Ukrainian businesses and government, financial and energy sectors. We can safely say that the main motivation of the threat actors were to disrupt, hinder and sabotage multiple Ukrainian organizations and infrastructure to harm Ukraine's economy.

ATTRIBUTIONS

The US government has attributed NotPetya to APT Sandworm, a Russian-tied intelligence and cyber warfare group funded by the Russian Intelligence Directorate (GRU). Ukraine has been in conflict with Russia for a long time due to political trade deals with the European Union and from the Russian annexation of Crimea from Ukraine starting in 2014.

TECHNICAL ANALYSIS

MAIN COMPONENT: DROPPER

The malicious sample, not_petya.exe acts as dropper through a compromised update of the tax accounting software 'MEDoc' used by many Ukraine organisations. It has a multitude of features after the initial infection vector including privilege escalation, network enumeration and propagation, encryption and MBR overwrite, forced system-shutdown and performing anti-analysis techniques to make the malware harder to detect and analyze.

Filename	MD5	PE Timestamp	Size (in Bytes)	Description
not_petya.exe	71b6a493388e7d0b40c83ce903bc6b04	2017-06-18 07:14:36 UTC	362360 bytes	Dropper, Trojan-Ransom.Win32.ExPetr.gen, Form of Wiper Malware, Main Installer

EXPLOITS/VUNLERABILITIES AND LATERAL MOVEMENT

CVE Number	Type	Description
CVE-2017-0144	Remote Code Execution	This exploit is known as 'Eternal Blue'. It exploits Microsoft's implementation of the SMBv1 protocol allowing the execution of arbitrary code remotely.
CVE-2017-0145	Remote Code Execution	This exploit is known as 'Eternal Romance'. It exploits Microsoft's implementation of the SMBv1 protocol allowing the execution of arbitrary code remotely.

The malware exploits the following vulnerabilities **CVE-2017-0144 and CVE-2017-0145** also known as **'Eternal Blue'** and '**Eternal Romance'**. These CVE's both exploit Microsoft's implementation of the SMBv1 protocol enabling a threat actor to generate SMBv1 packets to trigger the vulnerability and allow the execution of arbitrary code, spreading to unpatched machines and networks.

The Eternal Blue vulnerability allows an inter-process communication share (**IPC$**) to perform a null session connection by default. This special share is created by the Windows Server Service and allows the connection to be established by anonymous users/login. NotPetya exploits this vulnerability allowing SMB packets over TCP connection to open the null session in the **IPC$** share allowing threat actors to perform network enumeration and to propagate the malware.

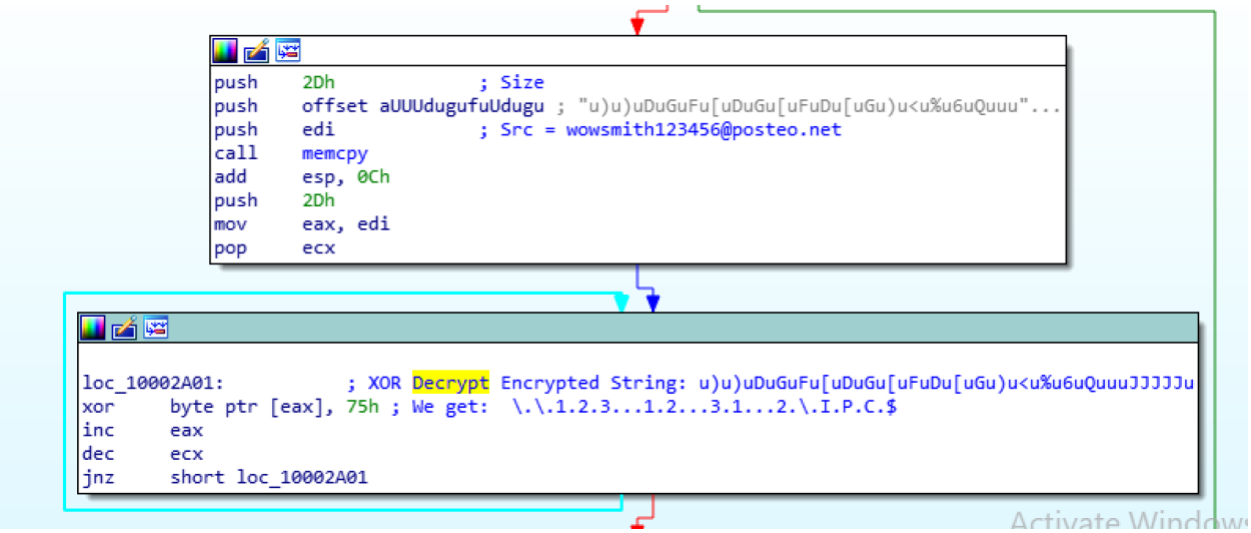

Figure 3.1 – IPC$ Functionality seen within NotPetya

PRIVILEGE ESCALATION

The malware first attempts to find and store how long it has been since the system has started in milliseconds via the **GetTickCount** API. The malware then tries to gain more privileges within the operating system through the following table:

Privilege	Description
SeShutdownPrivilege	Allows the ability to shut-down the system
SeDebugPrivilege	Allows the ability to debug or adjust memory of a program/process
SeTcbPrivilege	Allows user to access higher privileges of the Operating Subsystem

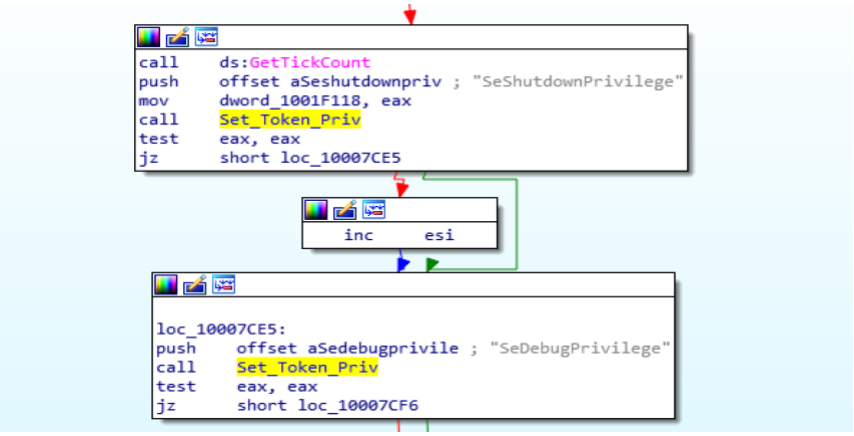

Figure 4.1 – Showcasing GetTickCount, SeShutdownPrivilege, SeDebugPrivilege

It rewrites the DesiredAccess to TOKEN_ADJUST_PRIVILEGES for these privileges via the API's **OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges.**

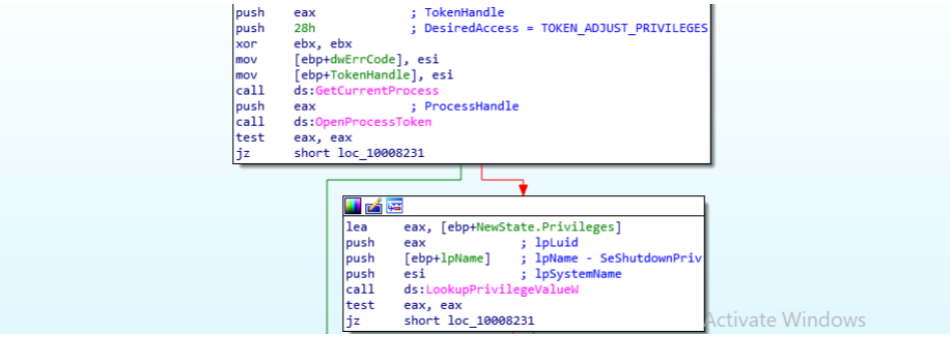

Figure 4.2 – Showcasing DesiredAccess = TOKEN_ADJUST_PRIVILEGES

Once the malware gains all privileges, it is able to propagate more of its functions via the SMB Eternal Blue exploit, force shutdown and reboot the infected machine via the **SeShutdownPrivilege** level and encrypt and overwrite data in hard-drives making them unusable via **SeDebugPrivilege** and **SeTcbPrivilege**.

NETWORK ENUMERATION

The malware attempts to gather network and computer information on an infected machine such as IP addresses, subnet-masks, computer name and computer version by creating a thread via the **CreateThread** API and executing it to see if the malware can connect to SMB port 445.

Interesting API's invoked by the malware that allow network enumeration are as follows:

API	Description
GetIPNetTable	Retrieve IPv4 to physical address mapping table
GetExtendedTCPTable	Retrieves a table that contains a list of TCP endpoints
NetServerEnum	List Servers visible in a domain
NetServerGetInfo	Retrieves configuration information for a server
WnetOpenEnumW/WnetEnumResourceW	Enumerate for network resources and connections
GetAdapterInfo	Retrieve Adapter/IP information from local machine

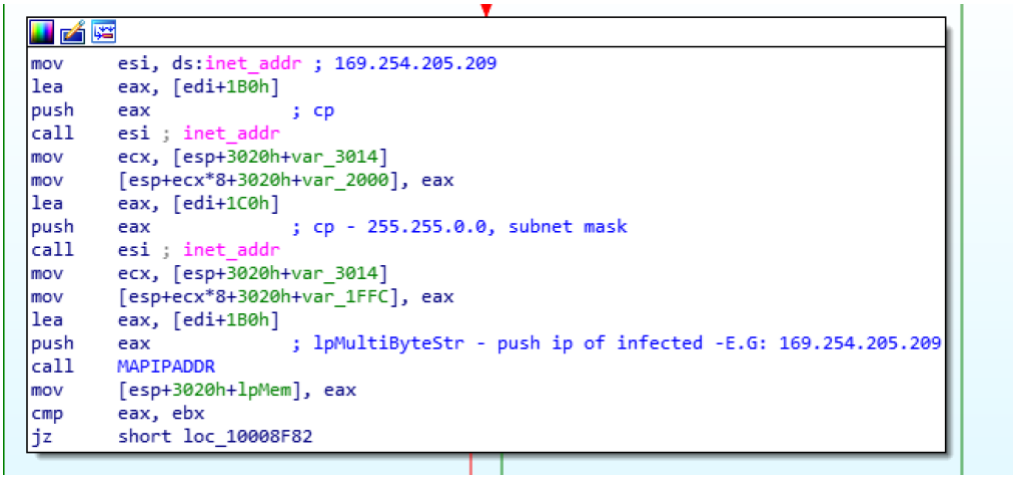

Figure 5.1 – Showcasing IP, Subnet mask Collection

If the malware is able to gather information about a machine or server, it will use DHCP for enumeration to get the IP addresses of infected machines and uses SMB from the Eternal Blue exploit to connect to more hosts.

It does this through the following API's:

API	Description
DhcpEnumSubnets	Return enumerated list of subnets from DHCP server
DhcpGetSubnetInfo	Returns information on a specific subnet
DhcpEnumSubnetClients	Returns an enumerated list of clients with served IP addresses in the specified subnet

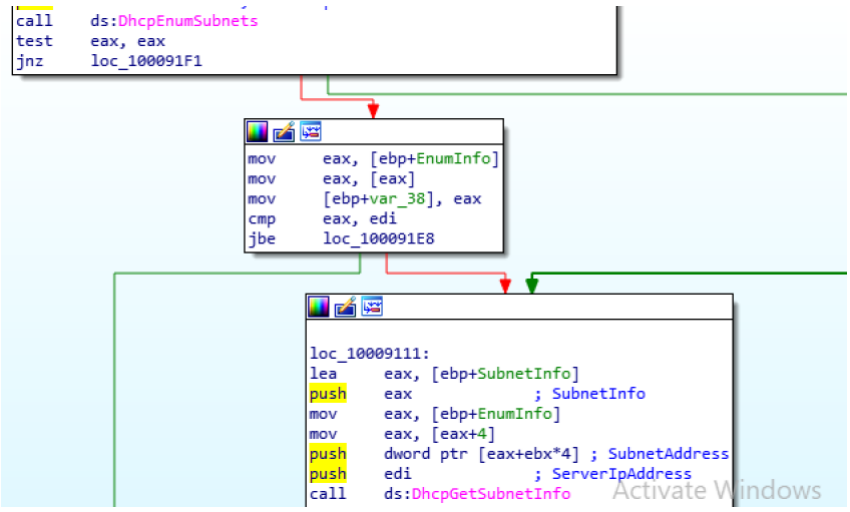

Figure 5.2 – Showcasing DhcpEnumSubnets, DhcpGetSubnetInfo

RESOURCES ANALYSIS AND EXAMINATION

Notpetya contains several resources which we can extract via Resource-Hacker. A table of the resources can be seen below:

Resource	MD5 .bin Hash of resources
R1	5273A3494495F2278D4415B999DEBEC3
R2	FFE1EE50B87D6C569C92E3D847F2FB9A
R3	779D952F314C92881ABFC4980A7269EA
R4	F56FE3B66610DEA29473D997792F1AC6

The malware checks if the infected machine is a 32-bit or 64-bit system via **IsWow64Process**. If the machine is 32-bit the malware will use **Resource 1**, if it is 64-bit the malware will use **Resource 2.** It will unlock the RT_RCDATA in memory and creates a new file [**x].tmp** in the Appdata %Temp% Path.

Example: **C:\Users\User\Appdata\Local\Temp\D0A6.tmp**

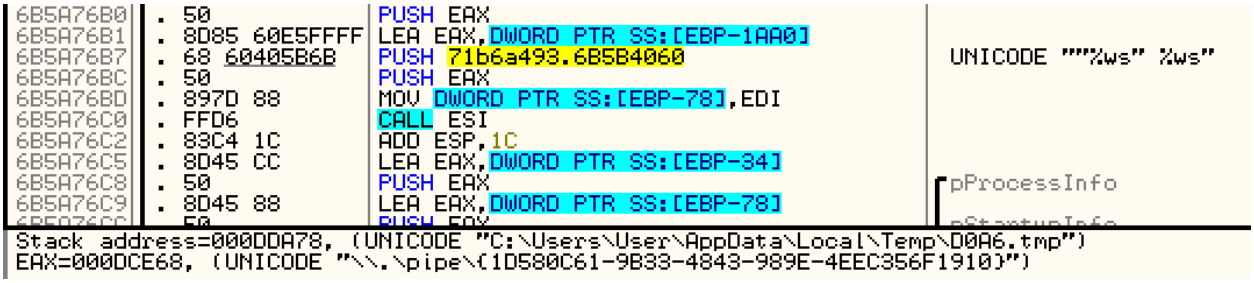

Figure 6.1 – Showcasing creation of new .tmp file and GUID

The malware will then create a unique GUID for the **[x].tmp** File and writes the resource to it, executing the resource as a new process with the argument **\\.\pipe\{GUID}** to obtain user credentials**.** Once complete, the malware will delete the **[x].tmp** file by calling to the API **DeleteFileW.**

The malware also uses **Resource 3** in another function, unlocking the RT_RCDATA in memory and writes the resource to a new file called **dllhost.dat** in the **C:\Windows** path.

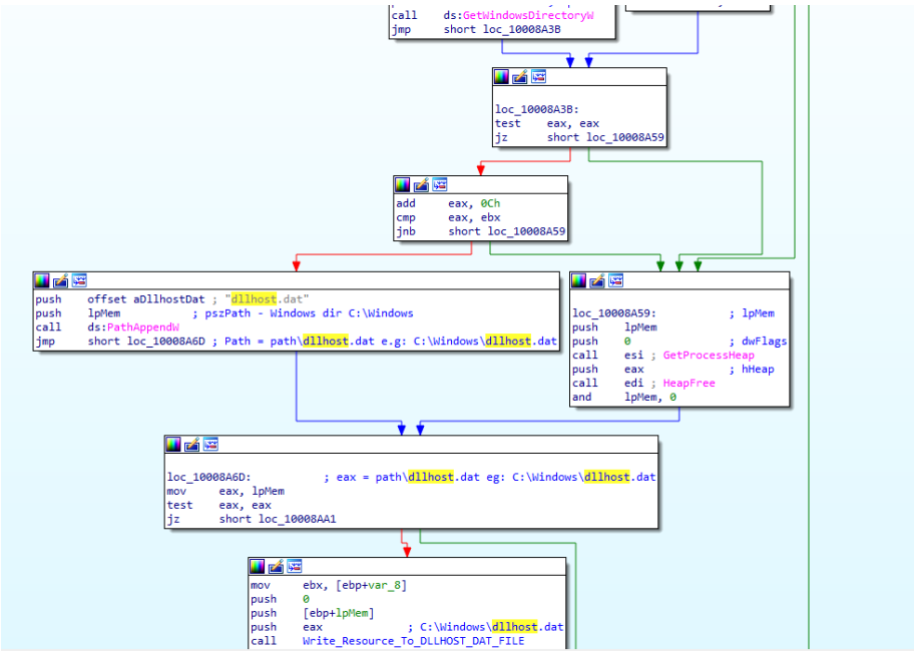

Figure 6.2 – Resource 3 Dllhost.dat creation

Resource 4 is a resource used to exploit the EternalBlue vulnerability via SMB.

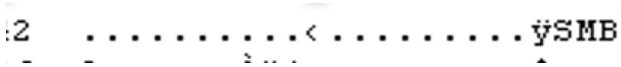

Figure 6.3 – Resource4 SMB Payload

REMOTE EXECUTION

The malware uses the following command for remote execution on the infected machine:

Command Name
C:\Windows\dllhost.dat \\<Host> -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\Filename",#1

Command	Purpose of the command
schtasks	Main command used to schedule tasks periodically at a specific time. Able to create, delete, modify, start/stop scheduled tasks
Host	Targeted Host/Machine
-accepteula	Suppresses license dialog display
-s	Run remote process in system
-d	Don't wait for application/process termination
Filename	Filename dropped by malware, usually perfc.dat

#1	Export Ordinal Value

WMIC or the Windows Management Instrumentation Command-Line is also used for remote execution on the infected machine. It uses a username and password combination to spread to other machines via stolen credentials or user token impersonation.

Command Name
C:\WINDOWS\system32\wbem\wmic.exe /node:" " /user:" " /password:" " process call create" **C:\Windows\ \System32\ rundll32.exe "C:\Windows\Filename", #1**

Command	Purpose of the command
wmic.exe	Provides a command-line interface for administrative capabilities to query system settings, stop/start services and remotely execute scripts
/node	Server Name
/user	User Name
/password	Password of host/user
Process call create	Execute remote command

ENCRYPTION ALGORITHMS

ALGORITHMS USED: RSA AND AES

RSA is an asymmetric algorithm using public and private keys for encryption and decryption. AES is different from RSA as it is a symmetric algorithm and uses one key for encryption and decryption.

The malware first uses the Microsoft Enhanced RSA and AES Cryptographic Provider to generate an AES-128 bit key to encrypt all the files within an infected machine and its hard drive via the API **CryptGenKey**.

It searches for files to encrypt with the following file name extensions using the generated AES key to encrypt the files:

.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**	**.xcd**	**.zip**					

The malware also imports the RSA-2048 public key of the threat actor via the API **CryptImportKey** which is stored in the malware:
MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ /wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz 29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu6zfhzuts7KafP5UA8/0 Hmf5K3/F9Mf9SE68EZjK+cIiFlKeWndP0XfRCYXI9AJYCeaOu7CXF6U0AVNnNjvLeOn42LHFUK4o6JwIDAQAB

After, the AES-generated key is exported via the API **CryptExportKey** for each machine. The AES-generated key is then encrypted with the threat actors' RSA embedded public key.

When files within the infected machine are encrypted, the malware will drop a file called '**README.txt'** and writes a ransom note within it**.** It will also include the AES generated key encrypted with the threat actors RSA-2048 key as the personal installation key for that specific machine. The malware will then use the API **CryptDestroyKey** releasing the handle for the AES-128 key so it cannot be used again, making decryption of files impossible as we also do not have the private key of the threat actor to decrypt the AES-128 generated key.

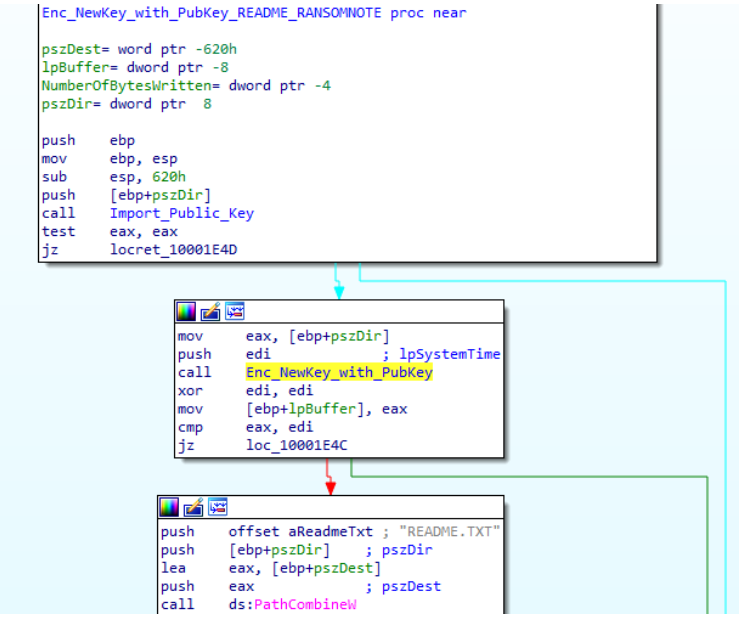

Figure 7.1 – NotPetya Imports RSA-2048 public key and encrypts AES-128 key with the public key

Figure 7.2 – NotPetya releasing handle of AES-128 key

README.txt - Notepad

File Edit Format View Help

```
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:
```

Figure 7.3 – README.txt ransom note

DESTROYING THE MASTER BOOT RECORD

The malware gets the system directory and opens the C volume on the physical drive, calling to the API **DeviceIOControl** with the IoControlCode **IOCTL_VOLUME_GET_VOLUME_DISK_CONTENTS** to gather information of the location of the volume driver.

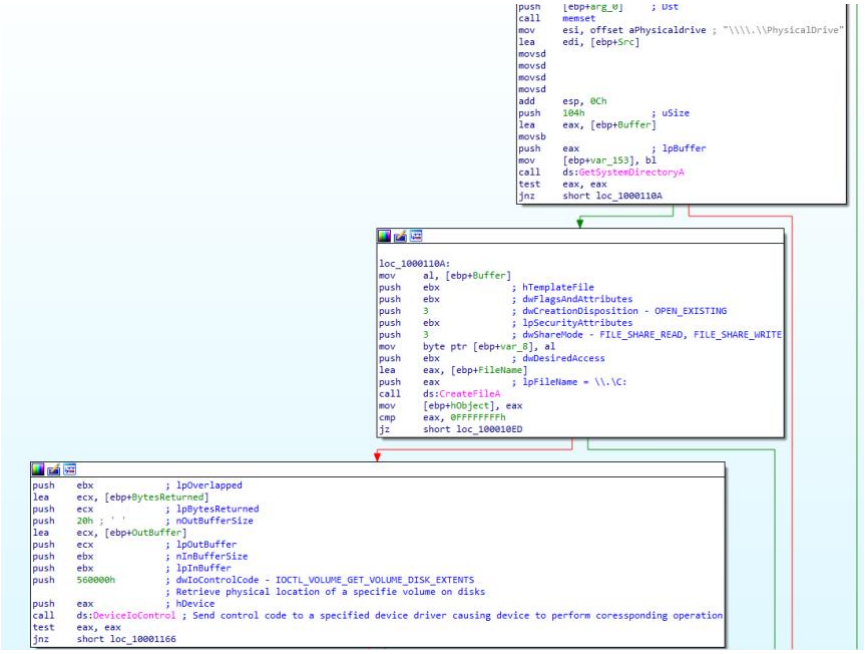

Figure 7.4 – Get System Directory, Open C Volume

It will then attempt to read the partition information such as type, size and nature of the physical disk via the IOControlCode **IOCTL_DISK_GET_PARTITION_INFO_EX** from another call to the API **DEVICEIOControl.**

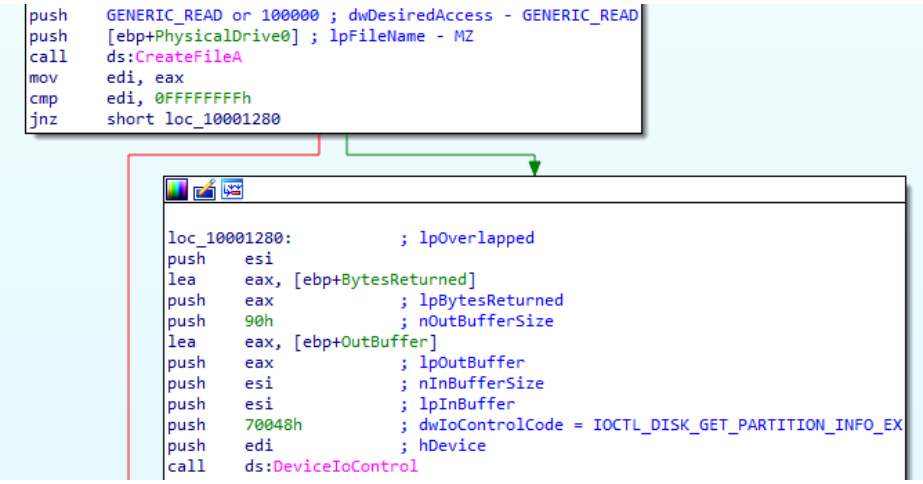

Figure 7.5 – Read Partition Information

To modify the MBR it will start calling to a function with the API's **CryptAcquireContextA** to handle the cryptographic service provider and **CryptGenRandom** to write an array of random bytes to read/write sectors within the disk.

The malware then tries to overwrite and modify certain sectors within the Master Boot Record by using the API **DeviceIoControl** with the IoControlCode **IOCTL_DISK_GET_DRIVE_GEOMETRY** to control the volume driver and creates a file named **PhysicalDrive0**, writing bytes within it to destroy the Master Boot Record and make it

unrepairable. Once completed, the malware also uses the IoControlCode **FSCTL_DISMOUNT_VOLUME** to dismount the volume after modifying the Master Boot Record.

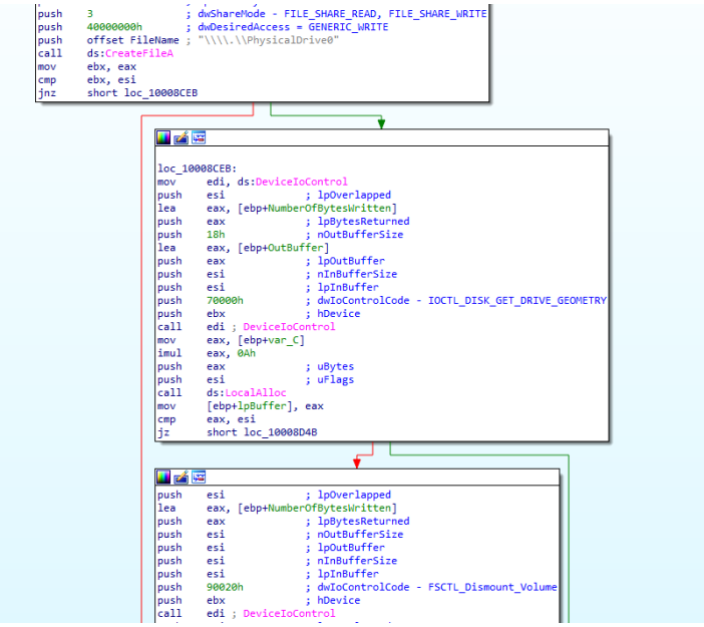

Figure 7.6 – Modify MBR and Dismount Volume

FORCED SYSTEM SHUTDOWN AND ANTI-ANALYSIS

FORCED SYSTEM SHUTDOWN

The malware gets the current time and version of an infected machine via the API's **GetLocalTime** and **GetTickCount.** It will use the following command via **cmd.exe** to schedule a system shutdown/reboot of up to 60 minutes from the current time the malware was executed on the machine:

Command Name
schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <time>

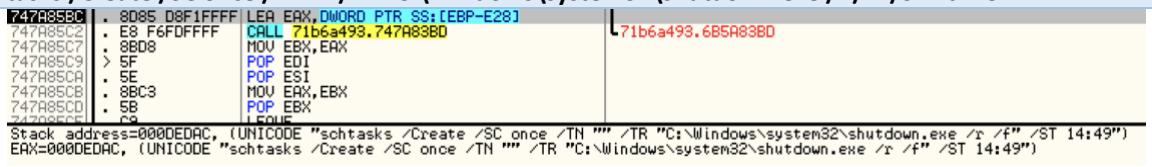

Figure 6.1 – Showcasing the schtasks command in Ollydbg

Command	Purpose of the command
schtasks	Main command used to schedule tasks periodically at a specific time. Able to create, delete, modify, start/stop scheduled tasks
/Create	Create scheduled task
/SC once	Specify schedule frequency
/TN	Value that specifies the task name, uniquely identifying the scheduled task

/TR	Runs the specific task
/r	Reboot after shutdown
/f	Force applications that are running to close
<time>	The time the scheduled task will execute (1 hour)

ANTI-ANALYSIS

The malware also tries to make it harder for analysts and users to find out what is happening on an infected machine by clearing event logs before a forceful shutdown/reboot process. It uses the following command via **cmd.exe** to clear the logs within the system:

Command Name
wevtutil cl Setup & wevtutil cl System & wevutil cl Security & wevutil cl Application & fsutil usn deletejournal /D %C

Command	Purpose of the command
wevutil setup **wevutil system** **wevutil security**	Clear the event logs of application setup logs, system logs and security logs
fsutil usn delete journal	The USN journal contains all information of all changes within a volume. This command will delete the journal
/D	Disable active USN change journal
%c	Volume path

ANTI-REVERSING TECHNIQUES

ANTI-ANTIVIRUS CHECKING

Notpetya has a form of anti-virus checking, examining anti-virus software within a system. If any of these processes are found, certain functionality of the malware such as encryption or network propagation via the SMB EternalBlue exploit may not occur.

The malware first takes a snapshot of all current processes and threads within a system via the API **CreateToolhelp32Snapshot** with the dwFlags parameter being TH32CS_SNAPALL**.** It will search for antivirus processes via the API's **Process32FirstW** and **Process32NextW** until it finds an AV executable. If none of the AV executables are found, the malware will run normally.

The Antivirus software that NotPetya checks are seen in the table below:

Hash	AV Software Name	Executable
0x2E214B44	Kaspersky Antivirus	avp.exe
0x6403527E	Symantec Antivirus	ccSvcHst.exe
0x651B3005	Norton Security Antivirus	NS.exe

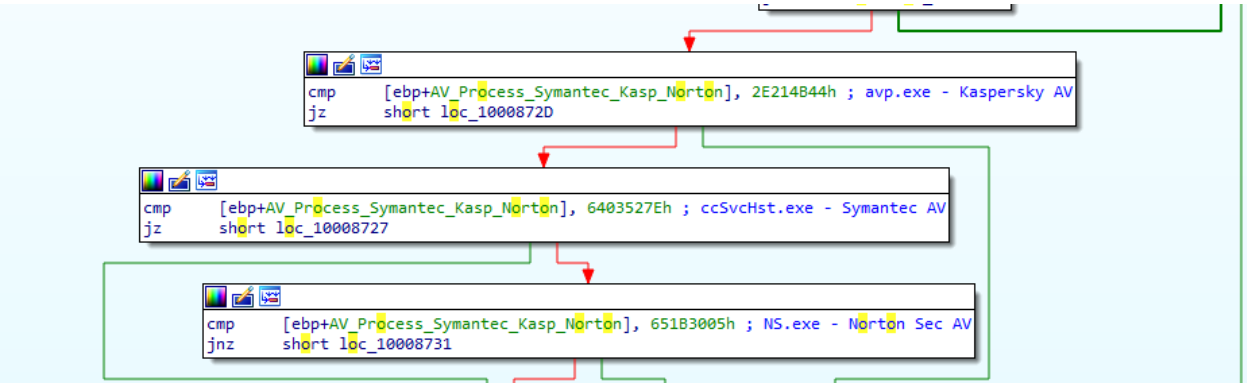

Figure 8.1 – NotPetya Checks the following AV products

RECOMMENDED ACTIONS

There are a multitude of ways we can prevent and mitigate NotPetya from spreading to other networks and machines.

- Install the Windows Security Update and patch **MS17-010** which fixes both the Eternal Blue and Eternal Romance vulnerabilities
- Disable **SMBv1** if your machine currently does not need to use it.
- Have an antivirus/anti-malware solution which can help prevent malicious executables from executing
- Implement a firewall rule to block SMB traffic on port 445
- If you are in a large organization, backup your data or implement a DRP (Disaster Recovery Plan) or disaster recovery sites (Cold, Warm, Hot sites) in order to backup and restore data when needed.

CONCLUSION

NotPetya is a malicious malware that is incredibly complex and was used to successfully target multiple Ukrainian organisations and businesses.

It tries to gain higher privileges within an infected hosts system scanning for user credentials and network information. It uses network propagation to spread to other hosts via the Eternal Blue and Eternal Romance SMB vulnerabilities. Furthermore, it uses encryption algorithms to encrypt data within drives, but also overwrites the master boot record to make system recovery nigh impossible. NotPetya as a result, is a form of wiper malware masking itself as a type of ransomware.

I hope you enjoyed reading this report. Feedback is greatly appreciated.

YARA SIGNATURE

```
rule Notpetya

{

        meta:

                description = "Yara Rule for Notpetya"

                author = "Ben Lee"

                date = "2022-23-01"

                hash = "71b6a493388e7d0b40c83ce903bc6b04"



        strings:

                $s1 = "CryptDestroyKey" fullword ascii

                $s2 = "wowsmith123456@posteo.net"

                $s3 =
".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." fullword wide

                $s4 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu6zfhzuts7KafP5UA8/0Hmf5K3/F9Mf9SE68EZjK+cIiFlKeWndP0XfRCYXI9AJYCeaOu7CXF6U0AVNnNjvLeOn42LHFUK4o6JwIDAQAB"
fullword wide

                $s5 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii

                $s6 = "Send your Bitcoin wallet ID and personal installation key to e-mail" fullword wide



        condition:

                (uint16(0) == 0x5a4d) and (filesize< 400000) and (all of them)

}
```

REFERENCES

- https://www.justice.gov/opa/press-release/file/1328521/download
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
- https://blog.3or.de/reverse-engineering-nopetyawiper-pt-1.html
- https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/inter-process-communication-share-null-session#:~:text=KB%20number%3A%203034016-,About%20IPC%24%20share,domain%20accounts%20and%20network%20shares.&text=Then%20it%20makes%20sure%20that,the%20specified%20users%20or%20groups.
- https://attack.mitre.org