**NotPetya tactical report**

**Identification**:

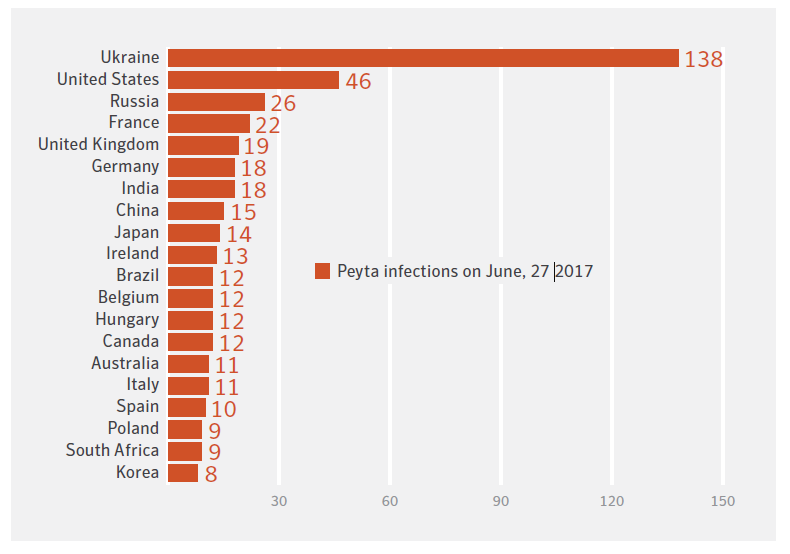
|  |  |
| --- | --- |
| **Vendor** | **Detection** |
| Symantec | Ransom.Petya |
| Kaspersky | HEUR:Trojan-Ransom.Win32.ExPetr.gen |
| Microsoft | Ransom:Win32/Petya.B!rsm |

The following table contains a list of artifacts that had been analyzed within this document.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PE timestamp** | **Md5** | **Size in bytes** | **File name** | **Description** |
| 2017/06/18 Sun 07:14:36 UTC | 71b6a493388e7d0b40c83ce903bc6b04 | 362,360 | petwrap.exe | Installer+ main functionality |

**Prevalence:**

Ransomware called Notpetya that affected thousands of computers in worldwide 2016 and 2017.the purpose of Notpetya is to encrypt hard drive of computer. And display message that needs amount of bitcoin to get a key and restore your encrypted data.it spreads to thousands of computers because of Eternal Blue exploit which developed by National Security Agency (NSA).



As shown in figure the most affected country is Ukraine. Petya affected several Ukrainian ministries, banks, metro systems and state-owned enterprises.

**Who is Responsible?**

According to statements of Ukrainian authorities, American Michael and CIA .Russia is responsible for this attack.

**Infection vector:**

* **Exploitation kit**

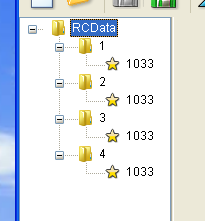
|  |  |
| --- | --- |
| **CVE** | **Exploit description** |
| CVE-2017-0199 | Remote code execution |
| CVE-2017-0143 | Remote code execution |
| CVE-2017-0144 | Remote code execution |

NotPetya ransomware first utilizes CVE-2017-0199, vulnerability in Microsoft Office that enables attacker to control pc then download ransomware, then spreads via ETERNALBLUE (CVE-2017-0143, CVE-2017-0144).

**Resource section:**

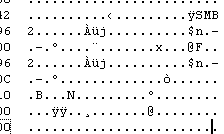
As we shown in figure NotPetya has resource section called RCDATA and this section contains 4 resources.

|  |  |  |
| --- | --- | --- |
| **Resource** | **File Name** | **Hash** |
| **R1** | perfc.dat | 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1 |
| **R2** | PsExec\_198.exe | f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 |
| **R3** | aa.exe | 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f |



**Note:**

Resource 4 will contain eternal blue exploit as shown in figure.

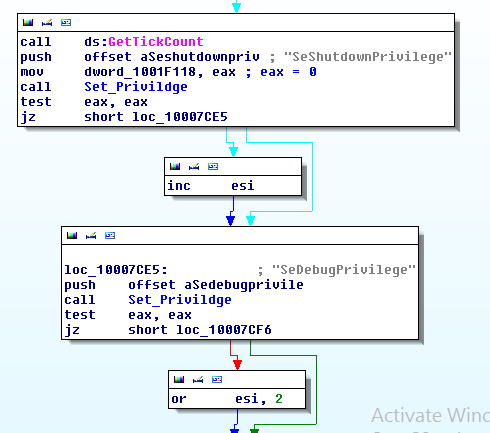


**Privilege escalation:**

At first ransomware tries to gain more privileges like

1. SeDebugPrivilege
2. SeTcbPrivilege
3. SeShutdownPrivilege

The reason of that is to access operating system components and shutdown pc.



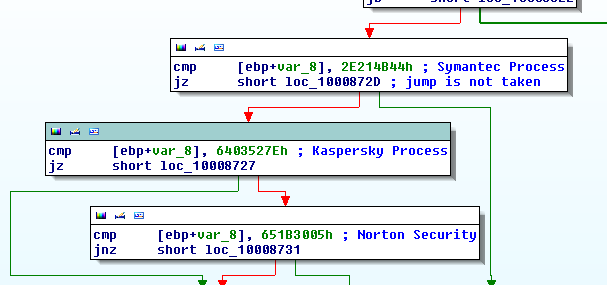
It moves current filename to this path

* C:\Windows\MalwareFilename

**Check for Processes**

Ransomware takes privileges then it lists system processes and checks for specific processes as shown in table below and figure.

|  |  |  |
| --- | --- | --- |
| **Value** | **File name** | **Product** |
| **2E214B44h** | ccSvcHst.exe | Symantec |
| **6403527Eh** | avp.exe | Kaspersky |
| **0x651B3005** | NS.exe | Norton Security |



**Destroy MBR**

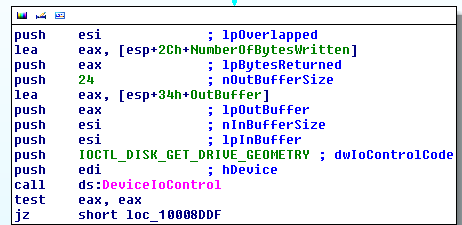
* Ransomware open c volume and call DeviceIoControl with argument “IOCTL\_DISK\_GET\_DRIVE\_GEOMETRY”to control specified volume driver then get information about physical disk and allocate 512 bytes from beginning of volume c
* It opens file called phyiscaldrive0 and writes number of bytes to it.

**Reason:**

The reason of that is to destroy partition boot record.

**Technique:**

Cavity infection.

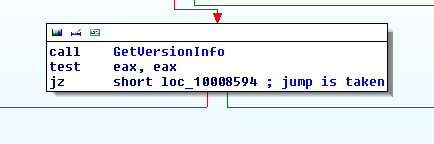


**Shutdown computer**

It gets current time and version of pc as shown in figure so depends on the version ransomware will execute on of the following command for system shutdown.

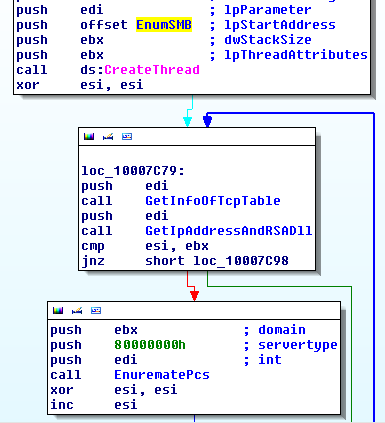
* C:\WINDOWS\system32\shutdown.exe /r /f
* schtasks /Create /SC once /TN "" /TR "C:\WINDOWS\system32\shutdown.exe /r /f" /ST <time>

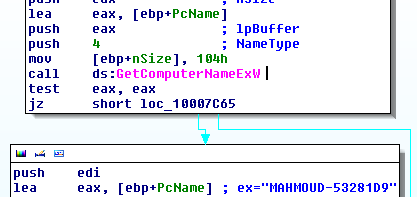
|  |  |
| --- | --- |
| **command** | **purpose** |
| schtasks | Create, delete, query, change, run, and end scheduled tasks |
| Create | Create task |
| SC once | A value that specifies the schedule frequency |
| /TN | A value that specifies a name which uniquely identifies the scheduled task |
| /TR | Run specific task ( shutwon.exe) |
| /r | Restart after shutdown |
| /f | Force to close running application |
| time | 1 hour |

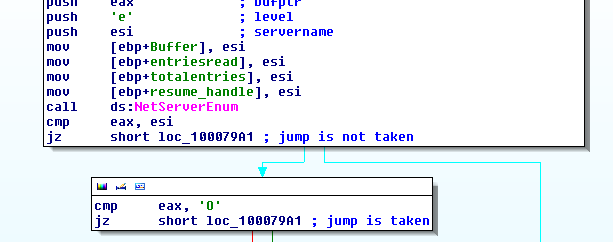


**Network enumeration:**

* It executes a thread to get computer name, ip address and subnet mask of machine.
* It checks machine is server or workstation.
* If machine is server then enumerate DHCP and get ip addresses of connected machines and use eternal blue exploit to connect to them.
* If machine is not a server so it tries to connect to other machines using eternal blue exploit.
* It executes this pervious thread at every 3 minutes.

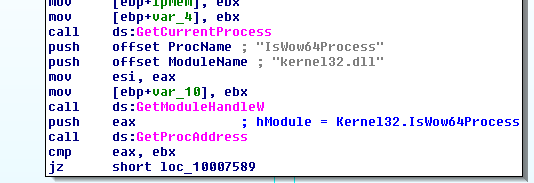






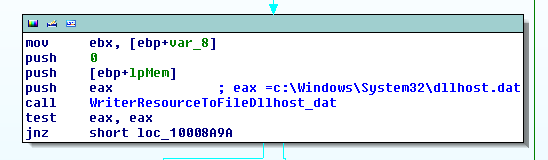
**Find suitable resource**:

* It checks current machine is 32 or 64 bit using IsWow64Process.
* If machine is 32 bit then it will unlock resource from section RT\_RCDATA in memory and this resource is copy of ransomware to execute it to remote machines.
* It creates file in this path C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\B0.tmp with random name and writes resource to it.
* It creates GUID to B0.temp file and writes resource to it.
* It executes B0.temp with argument \\.\pipe\{GUID}.
* It deletes file B0.temp.



**Another Resource**:

* It unlocks another resource from section RT\_RCDATA in memory.
* It creates new file called dllhost.dat and writes resource to it and resource is copy of ransomware.



**Remote Execution &Enumerate Resource**:

* It enumerates all network resource.
* It connects to server using default credentials and writes itself using following command:

\\ServerName\\admin$\RansomwareName

* It enumerates wmic.exe and executes it.
* It executes command to remote machine.

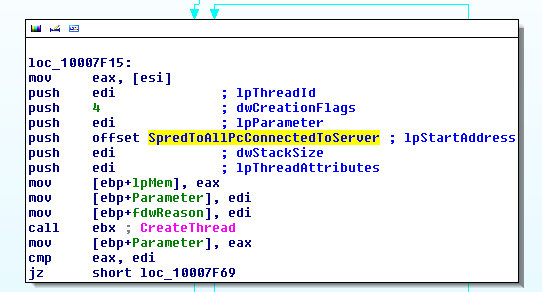
<Host>\\ -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\Filename", #1

|  |  |
| --- | --- |
| **Command** | **Purpose** |
| <Host> | Target machine |
| -accepteula | This suppresses the display of the license dialog |
| -s | Run remote process in the SYSTEM |
| -d | Don’t wait for the application to terminate |
| Filename | Rasomware |
| #1 | Export ordinal value |

* It enumerates TERMSRV.dll and executes another command.

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

|  |  |
| --- | --- |
| **Command** | **Purpose** |
| wmic.exe | command-line utility to make administrate task |
| node | Server name |
| user | User name |
| password | Password of user |
| process call create | Execute remote command |



**Encryption**:

* It gets available drivers and determines this driver is disk is removable, fixed, CD-ROM, RAM disk, or network drive.
* It generates Key using Microsoft Enhanced RSA and AES Cryptographic Provider. Let’s name it key (gen).
* It searches for specified types of files as shown in table.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | mai | l.mdb | msg |
| nrg | ora | ost | pv | ova | ovf | pdf | php | pmf | ppt |
| pptx | pst | i.pk | .pyc | .rar | .rtf | .sln | .sql | .tar | .vbox |
| .vbs | .vcb | .vdi | .vfd | .vmc | .vmd | .k | .vmsd | .vmx | .vsdx |
| .vsv | .work | .xls | .xlsx | xvd | .zip |

* It starts encrypting files using Key(gen).
* It import public key which is stored in ransomware.
* Public key = MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu6zfhzuts7KafP5UA8/0Hmf5K3/F9Mf9SE68EZjK+cIiFlKeWndP0XfRCYXI9AJYCeaOu7CXF6U0AVNnNjvLeOn42LHFUK4o6JwIDAQAB
* After ransomware finished encryption then it encrypt Key (gen) with public key and send new key to attacker.

**Decryption Possible?**

We couldn’t decrypt files because we only know public key but we don’t know key (gen).

**Command:**

* **It executes this command**

**wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejourna**

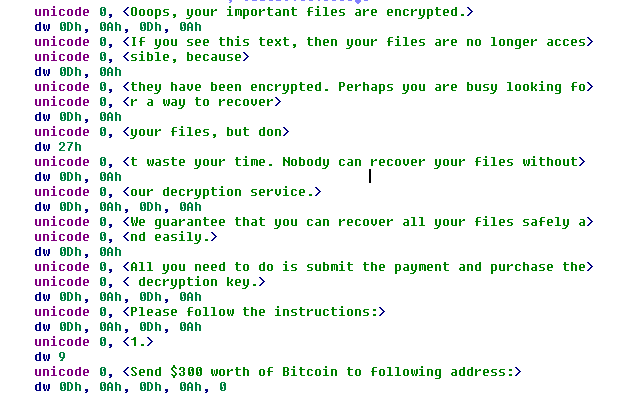
**Reason?**

|  |  |
| --- | --- |
| **command** | **purpose** |
| **& wevtutil cl System**  **& wevtutil cl Security**  **& wevtutil cl Application** | **Clear event log** |
| **& fsutil usn deletejourna** | **The USN change journal is a database of all changes made to files on a volume** |

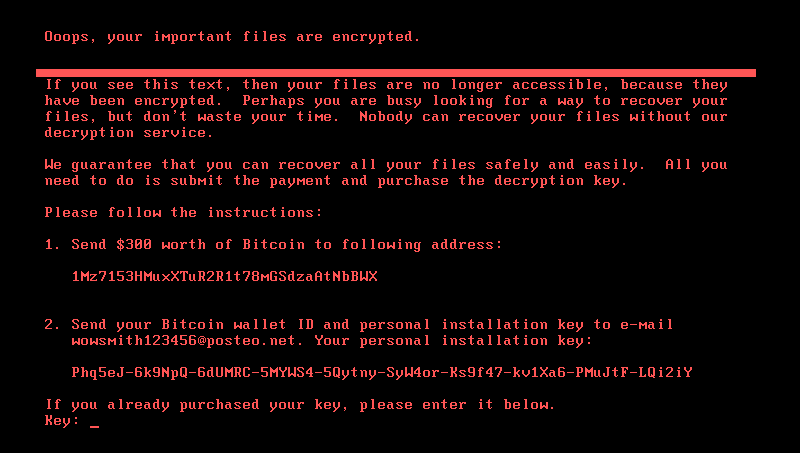
**Ransomware Notes**:

It creates file called “README.TXT”.

It writes to file these strings as shown in figure



* Then it repeats stage of Remote Execution, Enumerates resources and tries to connect to machines in network using Eternal Blue exploit.
* It finally forces system to shut down and shows this figure below.



**Summary:**

**NotPetya ransomware is self-propagation ransomware that spreads regarding to Eternal Blue exploits. So once NotPetya infects machine it tries to do some activities like enumerating server, connecting machines with it, encrypting MBR and other files with random key , destroying key and finally shutting down machine and rebooting it.it needs a payment about 300$ to specific address to restore your encrypted files.**

**Yara Signature:**

/\*

Yara Rule Set

Author: Mahmoud Elmenshawy

Date:2019-07-1

Identifier: NotPetya

This rule to detect file petwrap.exe and other copies of file

\*/

private rule IsPE

{condition:

// MZ signature at offset 0 and ...

uint16(0) == 0x5A4D and

// ... PE signature at offset stored in MZ header at 0x3C

uint32(uint32(0x3C)) == 0x00004550}

rule NotPetya{

meta:

Author = "Mahmoud Elmenshawy"

Description = " NotPetya Rule for detecting Installer "

MD5 = "71b6a493388e7d0b40c83ce903bc6b04"

strings:

$x1 ="\\.\PhysicalDrive"

$x2 ="1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX"

$x3 ="wowsmith123456@posteo.net"

$x4 ="Ooops, your important files are encrypted"

$x5 ="Send $300 worth of Bitcoin to following addres"

$x6 ="MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu6zfhzuts7KafP5UA8/0Hmf5K3/F9Mf9SE68EZjK+cIiFlKeWndP0XfRCYXI9AJYCeaOu7CXF6U0AVNnNjvLeOn42LHFUK4o6JwIDAQAB"

$x7 ="TERMSRV"

$x8 ="shutdown.exe /r /f"

$x9 ="wbem\wmic.exe"

$x10 = ".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"

condition:

3 of them and IsPE

}

**MITIGATION AND PREVENTION:**

* There are several ways customers can mitigate and prevent NotPetya from impacting your environment.
* First and foremost, we strongly recommend that customers who have NOT yet already applied MS17-010 to go do so immediately. Given the severity of the vulnerability and the widely available tools that exploit it, leaving this vulnerability unpatched is unwise.
* Ensure you have anti-malware software deployed on your systems that can detect and block the execution of known malicious executable.
* Implement a disaster recovery plan that includes backing up and restoring data from backup devices that are kept offline. Adversaries frequently target backup mechanisms to limit the possibilities a user may be able to restore their files without paying the ransom.
* Disable SMBv1, if possible, on networks and move to a more updated version of SMB. (SMBv2 was introduced with Microsoft Vista)
* Organizing your networks in a number of well-defined logical segments, and allowing access to network assets only to those users and systems within a segment may help with containing outbreaks of self-spreading worms such as NotPetya.