ZLAB

Malware Analysis Report: NotPetya

Malware Analysts:
Antonio Pirozzi
Antonio Farina
Luigi Martire
Table of Contents

Introduction .............................................................................................................................................. 3
Basic static Analysis ................................................................................................................................. 4
Behavioural Analysis ................................................................................................................................. 5
Advanced static analysis ............................................................................................................................ 10
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     | 34f917aaba5684fbe56d3c57d48ef2a1aa7c06d |
| SHA-256   | 027cc450ef58c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 |
| File size | 353 KB |

*Table 1 - Generic Info about NotPetya*

Sections

<table>
<thead>
<tr>
<th>Name</th>
<th>Virtual address</th>
<th>Virtual size</th>
<th>Raw size</th>
<th>Entropy</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>4096</td>
<td>48483</td>
<td>48640</td>
<td>6.55</td>
<td>c6bd3bb710ae7773b3b1790592b7f8b</td>
</tr>
<tr>
<td>.rdata</td>
<td>53248</td>
<td>34118</td>
<td>34304</td>
<td>6.99</td>
<td>46410e52b546c1696e8af524f10c56e</td>
</tr>
<tr>
<td>.data</td>
<td>90112</td>
<td>39754</td>
<td>20992</td>
<td>5.43</td>
<td>52160c62d1df1b1d5e2e9e286e789f</td>
</tr>
<tr>
<td>.rsrc</td>
<td>131072</td>
<td>247508</td>
<td>247508</td>
<td>8.00</td>
<td>1f07e685750a23b32d9e182baa06d5</td>
</tr>
<tr>
<td>.reloc</td>
<td>380528</td>
<td>3074</td>
<td>3584</td>
<td>4.77</td>
<td>c5d1d4dcade7dcbf1e4c10dc66dbf1</td>
</tr>
</tbody>
</table>

*Table 2 - Info about NotPetya's Sections*

Relevant Strings

```plaintext
\PhysicalDrive0
123456789ABCD\EFGHJKLMNQPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
1Mz7153HMuxXTuR2R1t78mGSDzAAtNBWX
Your personal installation key: wowsmith123456[dot]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:
```

CSE CyberSec Enterprise SPA  
Via Giovanni Paisiello 416, Rome, Italy 00198, Italy  
Email: info@csecybsec.com  
Website: www.csecybsec.com
Send $300 worth of Bitcoin to following address:

NtRaiseHardError
255.255.255.255

These strings are the most relevant in the malware dll. There are two strings, “wowsmith123456[at]posteo[dot]net” and “1Mz7153HMuxXTuR2R1t78mGSdzatNbBWX” 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”.

![NotPetya Privileges Table]

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:

![NotPetya performed actions before reboot Diagram]

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.

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:

   ".

   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.

![Figure 4 - Execution of custom Mimikatz contained in a temporary file](image)

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.

![Figure 5 - Request-Response between two machines with NetBios protocol](image)

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.

![Figure 6 - Example of communication between the infected host and another host on the network](image)

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.

CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com
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.

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.
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.

Figure 9 - Disk layout before and after the infection

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:

![Figure 11 - Creation of command to run tmp file](image)

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

![Figure 12 - Generation of command line for PsExec running](image)

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.
Figure 13 - Network discovery