Reverse Engineering the Behaviour of NotPetya Ransomware

R Lakshmi Prasanna Sai, T. Pavan Kumar

Abstract—Recently Ransomware attack had a great impact on several sectors like, Banking & finance, Insurance, Healthcare, utility and energy, Manufacturing, Education, Public and Government sectors etc. One of the prominent type of ransomware that effected several computers across the world, including Ukraine, France, Russia, and England which hit the big time in 2017, however its effect still persists in 2018, and is referred to as NotPetya. This is destructive because it combines regular ransomware behaviour with stealthy transmission technquies. NotPetya encrypts the files and also master boot loader (MBR) which intercepts the booting process with a ransom note. Eventhough by paying the ransom, the data couldn't have been recovered from the machine. This paper gives comprehensive technical analysis and reverse engineering of NotPetya ransomware.

Keywords—Ransom, Ransomware, NotPetya, Encryption, Reverse Engineering.

I. INTRODUCTION

Ransomware is one of the biggest threats in the Digital world. It is a type of malware that encrypts all the files or documents on the PC and it has the capability to spread across the netwok. Victim's can only get back to their files only if they pay ransom to the attacker. Data from the stastics shows that Public/Private sector is not immune to attack. Most of the attacks are targeting Financial services, Education, IT/Telecoms, Power grids, Oil and gas, Government etc have been hit as well. All these ransomware attacks are mainly carried by using Trojan that is a malicious code is masked as a legitimate file which comes as an email attachment where the victim is tricked to open it or download it. Around from 2012, ransomware scams are growing internationally.[3] The victims who confronts with ransomware between 2016 to 2017 increased by 11.4% when compared with 2015-16. The average ransom is up to $1,000. Adding strength to the effect, about 20% of the victim's who have paid the ransom demands, never retrived their files back from effect. They disconnected with the network without providing decryption key. About 72% of the infected companies lost there access to data for two to three days which is a great loss to the revenue. [5] In the first six months of 2018 there have been 181.5 million ransomware attacks[4]. According to Kaspersky, for every 40 seconds, a company gets shot by a ransomware.[6]

In the ransomware families one of the devasting type of ransomware is NotPetya which is currently spreading across the world which stood top second in its effect. According to reports it first originated from Russia and Ukraine, but now reached to U.S, the U.K, Denmark, Poland, Italy, India, Japan, Germany, France. In other words, it's almost everywhere in the world. The “NotPetya” attacks is similar to the very recent WannaCry ransomware which uses NSA exploit EternalBlue for spreading through network. But in addition to this, NotPetya uses multiple propogation techniques to spread through the computers. It includes Credential stealer to grab passwords and PsExec which use those collected usernames and passwords to gain access to other systems that are connected in that domain in the same network.[7] It is not usual type of ransomware because instead of directly encrypting the victim’s files, it encrypts the MFT(Master File Table) which holds the information related to the file names, size and location on the physical drive. Prior encrypting MFT, it replaces MBR(Master Boor Record), which stores the code that intiates the OS bootloader and replaces it with malicious code that displays the ransom note with instructions. So it stops the system from booting and displays the ransom note whenever the system is started.[8]

So, to analyze the functionality of malware we need to reverse engineer it. Reverse Engineering is a challenging task for the malware analyst. Reverse Engineering invovles mainly two important techniques for analysis of malware they are static and dynamic analysis. Static analysis is done without running the the malware, so it is much safer than dynamic analysis. Whereas in dynamic analysis the malware is executed in sepereate/isolated environment to examine its behaviour[9]. Most of the literatures are based on static analysis or dynamic analysis. Whereas my work will collectively represents static, dynamic and characterstics of NotPetya malware. This paper will cover in-depth technical analysis of NotPetya, which is structured as follows: Sec. 2 describes how NotPetya spreads. In Sec. 3 Flow of the malware execution in secured environment. In Sec. 4 reports static and dynamic analysis results done with malware. Sec. 5 Summarises the related work. Sec. 6 Concludes.

II. RELATED WORK

NotPetya malware combines ransomware functionality with an ability to propogate itself in network. This is intially identified on the systems running a document management software that is M.E.Doc. This software is mostly used for tax and payroll accounting. Based on analysing the M.E.Doc software, and from reports by anti-virus companies, it was

Revised Manuscript Received on March 08, 2019.

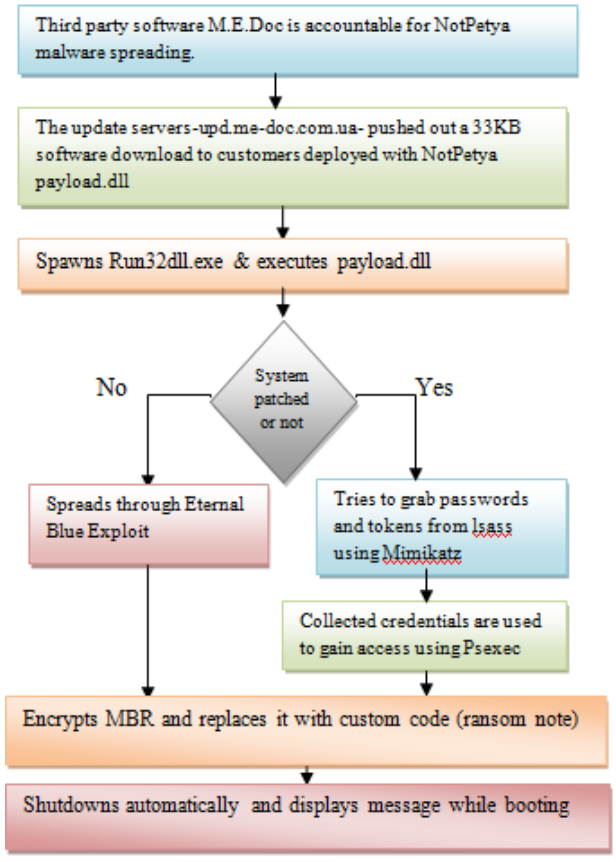
R Lakshmi Prasanna Sai, M.Tech Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India. (laxmiprasannasai@hotmail.com)

Dr.T. Pavan Kumar, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India. (pavanakumat_ist@kluniversity.in)

first deployed as a software update. And it started distrubuting though network slowly. It combines traditional ransomware with propogating through network functionality[10].

The system infected with NotPetya has three methods of spreading as discussed in the flowchart,

1. Remote exploit (EternalBlue, EternalRomance) for MS17-010.
2. Windows Management Instrumentation(WMI).
3. The psexec tool.



Flow of NotPetya ransomware

It spreads to Windows Operating Sytem through several methods. One of the prominent way is SMB service exploit (EternalBlue) which is previously exploited by WannaCry. It is the same vulnerability reported by Microsoft as MS17-010. It also uses Mimikatz, a technique to collect the credentials from the windows lsass (Local Security Authority Subsystem Service). The collected credentials are used to make an attempt to compromise other systems by using Microsoft tools, PsExec and Windows Management Instrumentation (WMI). Not Petya malware uses MS17-010 vulnerability to infect the unpatched systems. It uses PsExec and WMI tools to exploit the patched systems by extracting credentials from infected system's lsass process to gain access to systems [10][11].

Then it overwrites the MFT table and replaces the MBR with hostile code which prevents system from booting and displays the ransom demanding note. The encryption algorithms used by this ransomware are 128-bit AES in CBC mode and 2048-bit RSA to encrypt files. The ransom note demands $300 USD for each infected machine, and established Bitcoin workflow with the email address(wowsmith123456@posteo.net <mailto:wowsmith123456@posteo.net>). According to research reports, there are no such evidences of providing decryption keys by the attackers for recovering files after payment.

So to analyze the actual infection that is caused by the malware, Reverse Engineering is prefered. As discussed there are two methods for analysing a malware. They are static and dynamic analysis which are once again divided into two sub parts.

1.1 Static Analysis

1.1.1 Basic Static Analysis

It will help to make sure that the file is malicious or not. It is mainly used to know the functionality of the malware because it is a process of investigating the executable file without viewing the actual code. It is a straightforward process and very quick, but it is mostly uneffective against sophisticated malware.

1.1.2 Advanced Static Analysis

Advanced static analysis, is looking at the program's instructions to know the fuctionality of malware by loading the PE file into a disassembler. Disassembler will tell exactly what the program does by executing the instructions through CPU. It is a deeper learning process than basic static analysis and requires knowledge to understand the assembly-level code and also windows OS concepts.

1.2 Dynamic Analysis

1.2.1 Basic Dynamic Analysis

It involves running the malware on the system and noticing its behaviour in order to remove the infection. But to run the malware a separate environment must be setted up that will decrease the risk of damage to system and also to network. Like Basic Static analysis, it can be performed without having deep programming knowledge. But through this approach they may miss the important functionality.

1.2.2 Advanced Dynamic Analysis

It involves running the malware using debugger to examine the internal state of the executable. This technique provides an appropriate way to know the behaviour of malware functionality. This technique will be most useful to obtain information that is difficult to gather from other techniques.

III. MALWARE ANALYSIS & RESULTS

- 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745----------**Main DLL**
  - 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f---------- **(embedded 64-bit credential dumper)**
  - eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998---------- **(embedded 32-bit credential dumper)**
  - f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5----------

embedded psexec.exe (not harmful).

The above are the hash values of the analyzed samples. First one is the Main dll which contains the code of the EternalBlue and EternalRomance exploit. Second and third is the 32-bit and 64-bit embedded credential dumper similar to Mimikatz. The last one is the Sysinternals PsExec.exe file which is used to gain remote access to other systems for spreading the infection. Further technical analysis is done in the below sections accordingly.

Basic Static Analysis

The sample that is used for basic static analysis is 32-bit DLL with an unnamed export as in Fig 1. It is not packed, as shown in fig 2. As shown in fig 3, the resource section contains four obfuscated binaries. In those binaries, one is PsExec utility, two are 32-bit and 64-bit credential harvesters and the fourth one is a component of exploit (Eternal Blue).

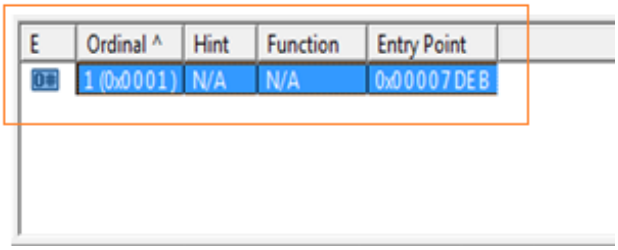


Figure 1

Figure 2

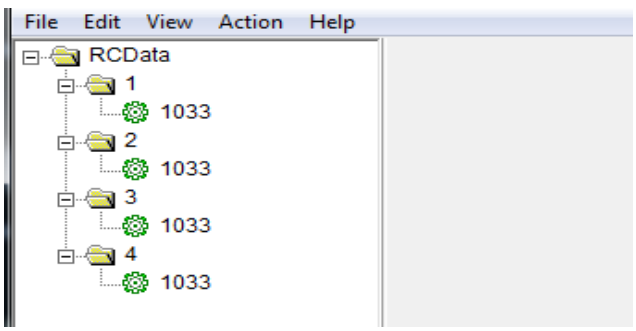


Figure 3

In this work, I have developed a tool named Basic Static analysis Report, which gives the information in the file. It displays the details like MD5, SHA1, PE file entropy, list of sections in the PE file, windows functions that are used by malware. Tool has the capability to show entropy of a given sample. It may detect the type of malware family according to the given yara rules. It also generates results according to the malware behavior as shown in Fig 4.

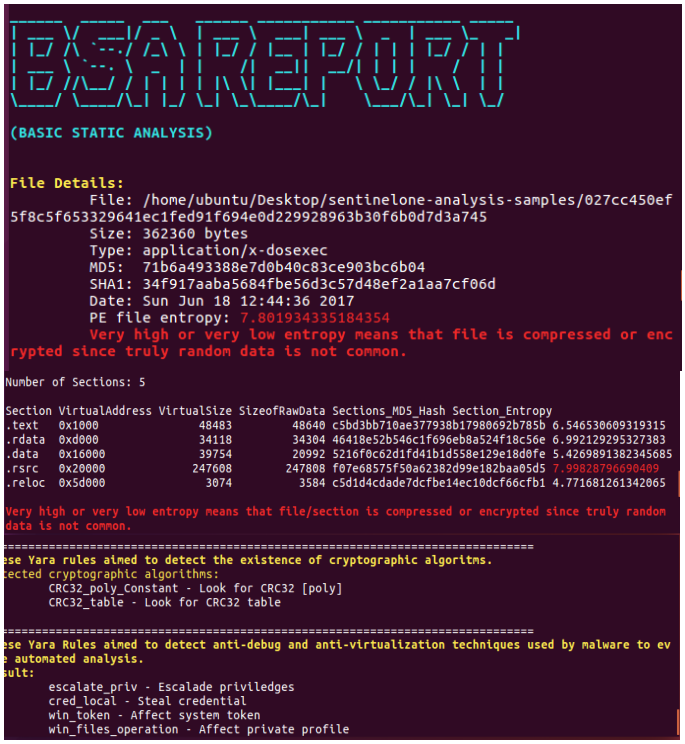


Figure 4

Basic Dynamic Analysis

In this analysis, the sample is executed in a safe or isolated environment. The file that is dropped by the malware is as follows:

- C:\Windows\perfc.dat

Whenever the sample gets installed, it will check whether the main dll is present in "C:\Windows" directory. This technique is commonly used to thwart the analysis efforts.

- *C:\Windows\System32\rundll32 perfc.dat, #1*

So, through Process Monitor we can check the processes that are created by the malware, shown in Fig 5. A temp file named 3FC0.tmp is created in the %temp% folder which is 32-bit or 64-bit credential harvester. It drops the file **C:\Windows\dllhost.dat**, a copy of the PsExec, which allows execution of process remotely. And also copies itself in to the memory and free the original one, removing the lock of the file on the disk.

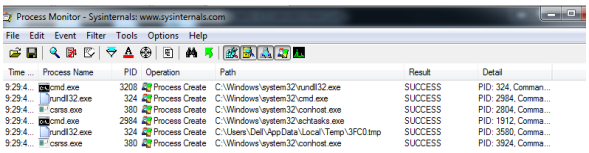


Figure 5

As shown in Fig 6, the files that are created by the malware after execution are dllhost.dat and also perfc.

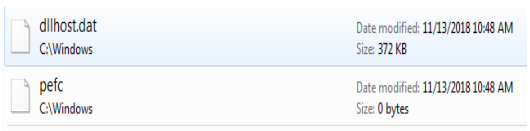


Figure 6

As shown in Fig 7, the result obtained by regshot helps to view the changes in the registry values after running the malware. It lists the number of modified keys, newly added keys and the total number of changes done in the registry.

```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2018/11/12 09:32:44 , 2018/11/12 09:33:59
Computer: WIN-K3LMKMB0VRM , WIN-K3LMKMB0VRM
Username: Dell , Dell
----------------------------------
Keys added: 14
----------------------------------
----------------------------------
Values added: 54
----------------------------------
----------------------------------
Total changes: 93
----------------------------------
```

Figure 7

Advanced Static Analysis

Here, we need to disassemble the code of malware to know its functionality. As shown in the Fig 8, it is the main EternalBlue exploit code i.e., core_MS17_010. If the exploit condition exits, the actual code is called in order to gain remote code execution abilities on victim computers.

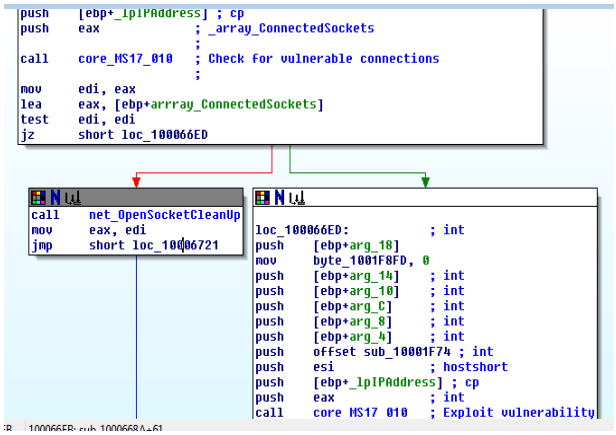


Figure 8

The process of exploitation starts from core_MS17_010 (sub_10005A7E).It sets up connections to vulnerable victims and then calls sub_10003CA0 which is responsible for decrypting and delivering payloads to victims. In exploit, the construction of payload is finished by decrypting and adding two packed resources to the malware's resource section.

Fig 9 represents the flow of decrypting EternalBlue packers packed in malware's resource section.

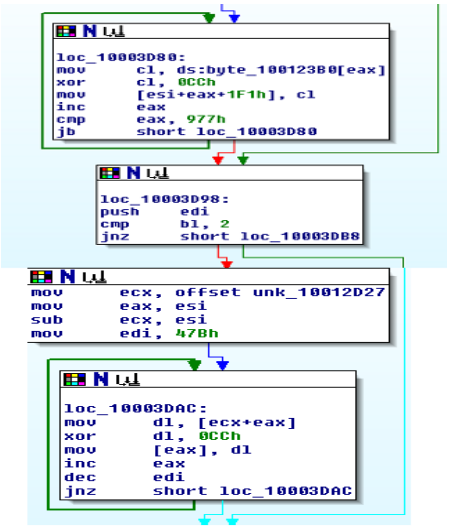


Figure 9

In the Fig 10, we can see how the previously constructed packet is delivered through the open socket.

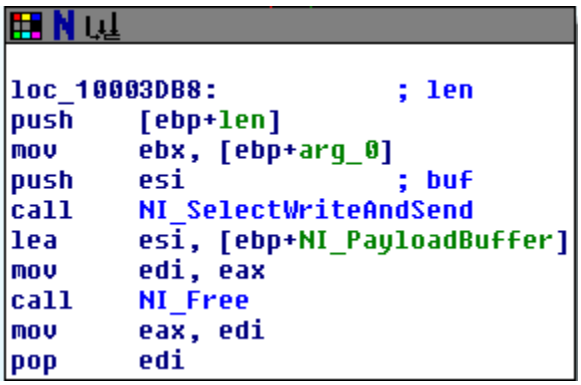


Figure 10

Advanced Dynamic Analysis

In this we use OllyDbg to debug the malware for knowing its internal functionality. For patched systems to spread the malware, a copy of windows sysinternals PsExec tool is written to %WinDir%\dllhost.dat. It uses the tool for gaining access to remote system to run malware on it with the following command.

- *Psexec -accepteula -s -d c:\windows\system32\rundll32.exe "C:\Windows\<filename>", #1*

Figure 11

If the connection is successful, it checks whether the system is already infected or not. If it is not infected, it uses PsExec and WMIC to spread the infection which is shown as follows:

- C:\windows\system32\wbem\wmic.exe /node:"<node>" /user:"<user>" /password:"<password>" process call create "C:\Windows\System32\rundll32.exe "C:\Windows\<file>\", #1

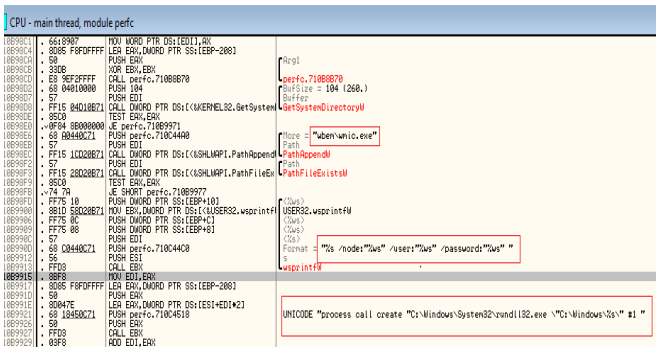


Figure 12

NotPetya engages the following method to reboot the system so that MFT encryptor code loads in the boot loader and displays the ransom note.

It schedules shutdown through cmd with the following command as shown in Fig 13.

- */c schtasks /Create/SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <HH:MM>*

/r → reboot after shutdown

/f → forces running applications to close

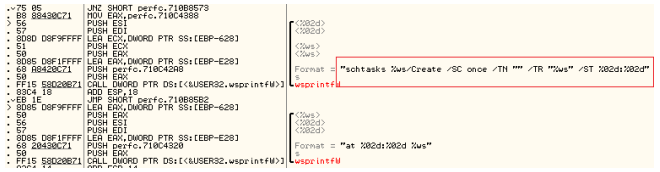
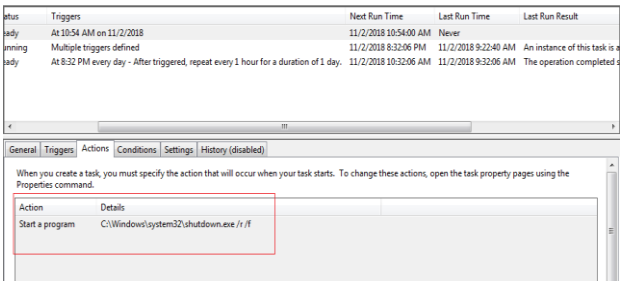


Figure 13



Scheduled shutdown in system

At last, after encrypting MBR and replacing MFT, it restarts at a particular time scheduled by malware and displays the message shown in the Fig 14.

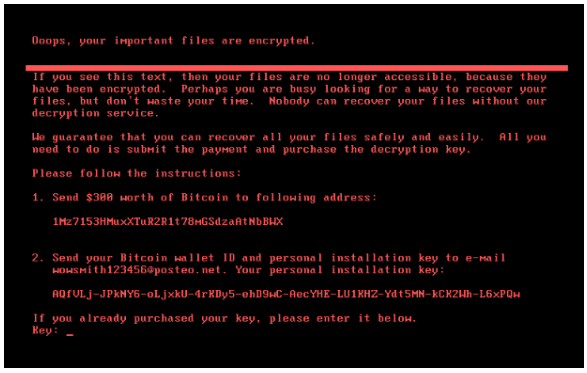


Figure 14

IV. CONCLUSION

By analyzing the NotPetya Ransomware, we have found many important factors like encryption mechanism used by the malware, the types of files it will effect, the network connection that is established for transmitting payload to exploit vulnerabilities in the network system, the registry changes performed by the malware and the new process created by it.

To safeguard from this type of ransomware we always have to maintain a backup copy of the data. Place the firewall for filtering malicious traffic and make sure that the installed softwares are up to date by patching it regularly.

Further analysis is carried on different kinds of rasnomware and the signature needs to be added to the antivirus database so that they can be blocked whenever they are detected in any of the system.

V. ACKNOWLEDGMENT

This work is supported by the Department of Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

REFERENCES

1. DAN DAHLBERG "ransomware cyber attacks " blog on Bitsight
2. Online "Ransomware" wikipedia
3. Online "New Internet Scam" news on FBI 2012
4. "sonicwall cyber threat report" article on helpnet security 2018
5. Phillip Long "5 Ransomware Statistics Every Business Owner Needs to Know" blog on BIS
6. "Attacks on Business Now Equal One Every 40 Seconds" press release on kaspersky lab 2016
7. Online "Petya" wikipedia
8. Lucian Constantin "Petya ransomware is now double the trouble" article on network world
9. Syarif Yusirwan S, Yudi Prayudi, Imam Riadi "Implementation of Malware Analysis using Static and
10. Dynamic Analysis Method" International Journal of Computer Applications (0975 – 8887)Volume 117 – No. 6, 2015
11. Falcon Intelligence Team "fast spreading petrwrap ransomware attack combines eternalblue exploit credential stealing" blog on CrowdStrike "malware analysis basics static analysis" InfoSec Resources