Final Report of Ransomware Petya Analysis

Song Yang (sea.yang@rutgers.edu) **Xin Yang** (xin.yang@rutgers.edu)
Zhuohang Li (zhuohang.li@rutgers.edu)

April 2018

Abstract

This report describes our research on the Petya ransomware. We proposed several prevention tools to help protect the user's machine, along with one way to recover the infected machine by MBR recovery.

1 Introduction

1.1 Malware Description

1.1.1 Background Information

Petya is a famous ransomware family first found in 2016. In 2017, a variant of Petya family which is called NotPetya[1] caused a global cyber attack, and the main target is Ukraine and Russia. Since Petya family has a lot of variants, we are talking about the most original one for this project, which is called exactly Petya. Petya is the first malware that can blackmail and modify the master boot record(MBR) at the same time and targets on computers running Microsoft Windows.

1.1.2 Attack Methods

Petya propagates through email at the very beginning. The attackers send emails with attached malicious files[2] and mislead users to download the attachments, e.g., a PDF resume. After the user opens the file, Petya will be activated. As is widely known, Petya will write the code into MBR and run the payload to force the computer rebooting[3]. Then Petya would run in its own environment and encrypt the whole file system to blackmail the users for Bitcoins. During the encryption process, Petya pretends to be running a check disk command. It will reboot again and show the interface asking for ransom. Petya asks users to download the Tor Browser, which is a tool to get access to the dark web[4], to pay for the ransom. If the user failed to pay the ransom in time, the ransom will double.

1.1.3 Influence and Damage

The danger of Petya is that it will directly lock and encrypt the whole hard disk[5], rather than just encrypt several types of files. Petya changes the MBR, so it took over the bootloader and there's no way to boot back into Windows.

As Microsoft explained, Petya is a malware with a high-level complexity, but the number of victims is smaller than expected. Most of the hacked computers were running Windows 7, and Microsoft had already published a series of patches for the problem. But we still can't assume that Petya can be perfectly intercepted under Windows 10.

2 Design

2.1 Analysis

Since this malware will throw a hardware exception and turn off the machine immediately, it's hard to run the dynamic analysis. We will first run a detailed static analysis combining with available literature to figure out how the Petya damages computers, and try to find the weak points.

2.2 The Icon Protector Mechanism

The reason why users are easily deceived is that Petya is disguised as a PDF file or compressed package by using an inappropriate icon. Generally, users tend to be cautious before clicking on executable files but negligent for PDF or compressed files.

Based on the results of our analysis, we developed a tool called Icon Protector, which can prevent the users being infected by supervising the icons of specific files.

Therefore, to prevent the users from icon spoofing malware, those 'user-believed' icons should be used under supervision and should follow a strict standard. The Icon Protector should be a system level detector, which can detect icons including PDF, compressed packages, Word, PowerPoint, Excel, and folder. Executable files have to be strictly matched with its icons to remind the users.

The Icon Protector is not defined as an anti-virus software. Its responsibility is to detect recently downloaded file and make sure the file is using a correct icon, and warn users if necessary.

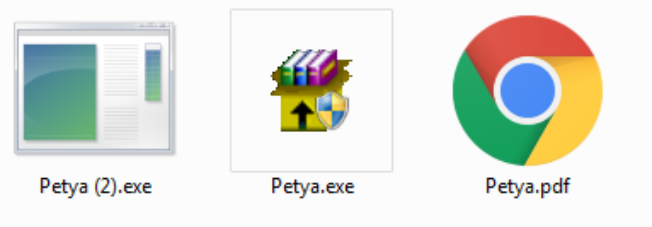

Figure 1: Petya Icons

2.3 VirusTotal Based File Scanner

The best way to keep the computer prevent safe is to prevent users from downloading malicious files, thus we came up with this more general method which calls the API from VirusTotal to scan the downloaded files, in this way the users can get the latest security information from VirusTotal and avoid being infected by known malware.

This is a basic Google Chrome plug-in that can detect downloaded files that are smaller than 10 Mb, and upload them to virustotal.com to get virus report automatically. If the report indicates that the file is malicious, the plug-in will notify the user.

2.4 MBR Recovery Methodology

The original Petya targets only at Master Boot Record(MBR) partitioned computers, UEFI + GPT partitioned computers will not be infected by this ransomware. In this consideration, we will test if it's possible to recover the system and user files by using MBR recovery in that Petya will only encrypt the MBR instead of specific types of files.

3 Implementations

Since Petya aims at the bottom level, we can hardly make any remedy after the system reboots. It's better to prevent rather than to recover. In this case, we proposed several measures to defense against Petya and other similar malware based on the analysis. Also, we developed an MBR recovery method to stop the infection.

3.1 Petya Analysis

3.1.1 Infection Routine

Petya targets Windows OS and is mainly distributed by social engineering. It is disguised as a job application letter containing a hyperlink to a Dropbox storage location or a faked resume file. The malware itself is a self-extracting executable file, named as the applicant's resume with a photo of the applicant.[6]

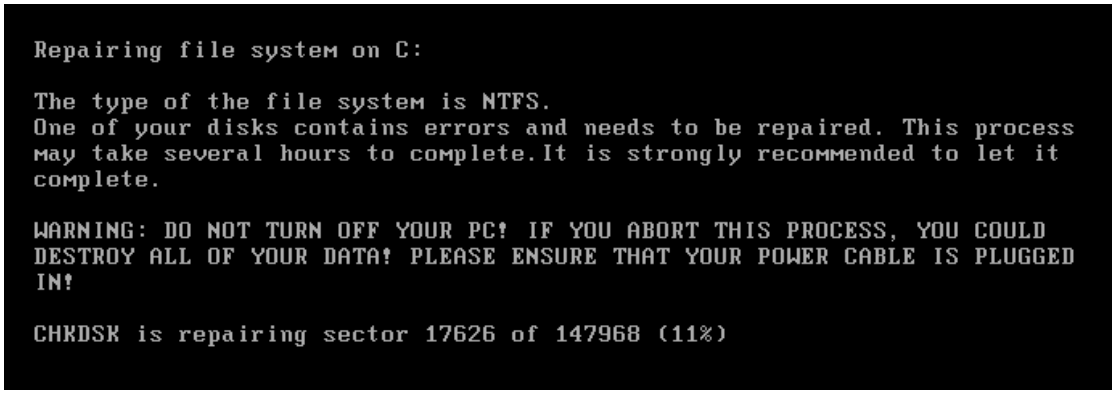

Figure 2: Screen after reboot

Figure 3: Ransom information

3.1.2 Infection Symptoms

After double clicking on this executable file, the victim's machine will crash with a blue screen of death (BSOD) and reboot. After the system restarts, it will show a screen claiming to be running a disk check command CHKDSK. The progress of the so-called disk check is actually the progress of encrypting the file system. Then after the next reboot, a flashing skull will be displayed. By far all of the files on disk will be no longer accessible from the user, even attempting to restart into the safe mode will also fail[7]. Petya will ask the victim to pay ransom on the dark web for decryption[8]. Comparing with other ransomware like WannaCry, which encrypt victim's important files on disk, Petya goes much further to encrypt the entire disk rather than specific files.

3.1.3 Internet Behavior Detection

In order to find out indicators of Petya's Internet behaviors, we use VirtualBox to build an internal LAN environment without access to the Internet as shown in Figure 4. We set up three virtual machines, VM 1 (IP:192.168.0.10), VM 2 (IP:192.168.0.12) and VM 3 (IP: 192.168.0.14), and get them connected to each other. VM 2 is set up as the host. VM 3 is for detecting how the TCP streams go from the infected computer to the host. So it has to be fully protected. We are using Windows 7 (64 bit) as the testing OS.

This original version does not have any indicators of launching Internet attacks. Wireshark cannot receive any package sent from the virtual machine infected by Petya.

Other than the original version of Petya, we also tested the updated variants on our platform. We found a latest variant with worm features, which can send a copy of Petya after it runs, right before the system shut down. The worm will scan the whole internal network and form a list and finally broadcast its copy.

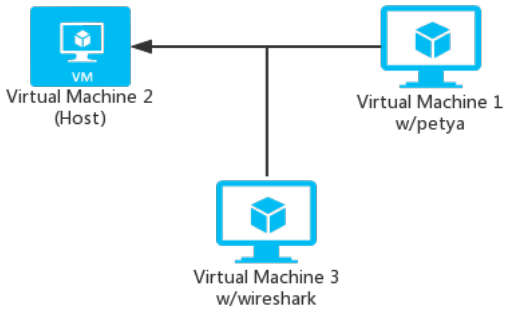

Figure 4: Network Setup

3.1.4 Static Analysis

When we load the Petya into IDA Pro, we can see the code starts from .text:00401000, and it uses CreateFile and DeviceIoControl. According to MSDN, CreateFile returns a handle that can be used to access the file or device for various types of I/O depending on the file or device and the flags and attributes specified, and DeviceIoControl sends a control code directly to a specified device driver, causing the corresponding device to perform the corresponding operation. [9] Therefore we can infer that the program is trying to scan the disks. No further information we can get. The program is actually packed/encrypted with FUD/crypter, which is a pretty strong packer. The malware also disguises itself as a Win32 program, but in fact, it extracts all malicious codes to memory[10].

The malware also contains a lot of misleading strings to prevent people from figuring its actual purpose. Since it's had to get true malware program and assembly languages, we tried to start up a local debugger, but unfortunately, it's hard to locate actual breakpoint that can stop the programming form restarting the computer. We failed to get the dump file of memory, cause it seems that after programs loaded to memory, it runs at once like another thread and out of control from IDA pro. So we guess that the function that causes system reboot is exactly loaded into memory.

3.1.5 Encrption Methodology

Petya is based on a variant of 'Salsa20', which is a symmetric encryption algorithm built on a pseudorandom function based on add-rotate-xor operations. Salsa20 takes a 16-byte or 32-byte key, and 8-byte initialization vector(IV), the number of calculation rounds, and a less than 2 ^ 70 bytes long message as input.The output ciphertext is encrypted data with the same length of the input message. For standard Salsa algorithm, the data is little-endian and the input key should be not less than 16 bytes. However, the valid key in Petya is only 8 bytes long. The key to be input in the terminal by the user is constructed by separating the original key with letter 'x'. Petya will take this key and after doing a series of calculations, compare the results with the data stored in sector 55. If the two data matches, Petya will take this as a valid key. Although Petya allocates 8 bytes memory in sector 54 offset 33 to store the IV, only the lower bits of the two DWORD is used. The data structure Petya uses to do the calculation is as shown in Figure 6. Petya is doing 10 rounds of calculation, each with a row round and a column round. Salsa algorithm takes the calculation result and does a bitwise xor operation with the original text to get the encrypted data. Petya is doing xor with 0x37 and stores the result in the corresponding driver sector.

Figure 5: calling I/O function

```
petya_matrix struct {
        Const0  uint16
        Key0    uint16
        Key2    uint16
        Key4    uint16
        Key6    uint16
        Const2  uint16
        Nounce0 uint16
        Nounce2 uint16
        Counter uint32
        Const4  uint16
        Key8    uint16
        Key10   uint16
        Key12   uint16
        Key14   uint16
        Const6  uint16
}
```

Figure 6: Encryption Data

3.2 The Icon Protector

The icon protector is based on the file scan. The program first scans the recently downloaded files and detect the file type. File suffix names including .rar, .zip, .exe, .pdf, .doc, .xls will be checked. After the scan, files whose actual type does not match its extension will be moved to a folder with a warning icon.

3.3 VirusTotal Based File Scanner

The VirusTotal file scanner is a chrome plug-in. When files are downloaded by Chrome, it will call chrome.downloads plug-in API to monitor the downloading event and get the downloaded file resource, then upload the downloaded file to Virus Total using an open source interface. The Chrome plug-in also provides a method to get the icon of the file, which is 'chrome.downloads.getFileIcon', which can also be used to get the suitability between given extension name and actual file type.

VirusTotal API

```
var virustotal = require('virustotal.js');
virustotal.setKey('API-KEY');
virustotal.getFileReport('downloadedFile.exe', function (err, res) {
        if (err) {
                console.error(err);
                return;
        }
        console.log(res);
});
```

3.4 MBR Recovery Methodology

Since Petya will do severe damage to the file system table, we will launch this malware on a virtual machine. First, we set our virtual machine in VirtualBox as Microsoft Windows XP 32 bit, with no anti-virus software, partitioned by MBR. We kept the virtual optical disk drive and loaded the .iso file for Windows XP installation and recovery. Then we cut off all other connections to the virtual machine to isolate this environment. We will try to use the MBR recovery tools coming with the official installation disk.

After double-clicking on the Petya executable we downloaded, the virtual machine suddenly shut down as a hardware error, this might be shown as a blue screen error on a normal machine. Then it goes into the boot device selection interface. To avoid further damage, we directly enter the Windows XP installation CD. By far we avoided the damage that Petya would do to our file table, only the MBR section and several following unimportant parts are modified. At the main interface of installation CD, we press R to enter recovery mode and select the operating system that we would like to recover. After a few steps, we arrive at the recovery mode command line interface. Here we use the official command "fixmbr", after the confirmation, there will be a message showing that MBR is overwritten successfully. We then enter "exit" to restart. We found that we can directly enter the Windows XP as usual without seeing the Petya interface, which means we have successfully overwritten the malicious code stored in MBR section. Meanwhile, all files are normal as usual, without being encrypted.

Then we tried to recover MBR after the Petya completely executed. In this condition, we can clear the Petya ransom interface by using "fixmbr" command, but the system still failed to boot in that the Master File Table is destroyed while the fake CHKDSK interface is displaying.[7] So we tried to use third-party tools to enter a temporary PE system booting from a live CD or USB, then use disk tools trying to recover the system. However, if the malicious codes have been executed, it's not likely to recover the whole system even if we rebuild the MBR bootloader, but it's still possible for some third-party disk software to recover some of the files.

In our experience, it's still possible to recover the whole file system without paying the ransom, but it would need professional knowledge about lost data recovery and experiences about recovering the MBR and MFT.

4 Results

4.1 The Icon Protector

The program scan a specific folder or files, using an open source File scanner to ensure every file is using an appropriate icon according to its extension as shown in Figure 7.

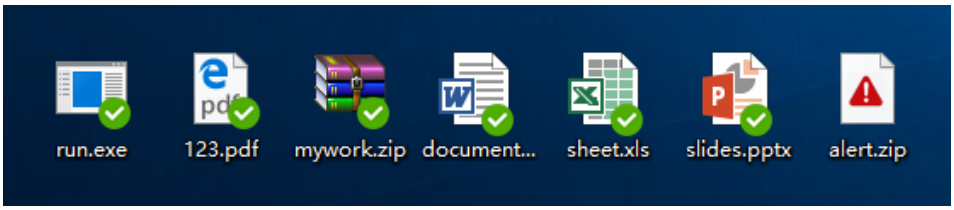

Figure 7: Icon protection

4.2 VirusTotal Based File Scanner

With the download checker, after user downloaded the attachment from email website in Chrome, as long as the viruses spread through email attachments is confirmed by virustotal.com, the user will be announced whether this file is secure or not.8

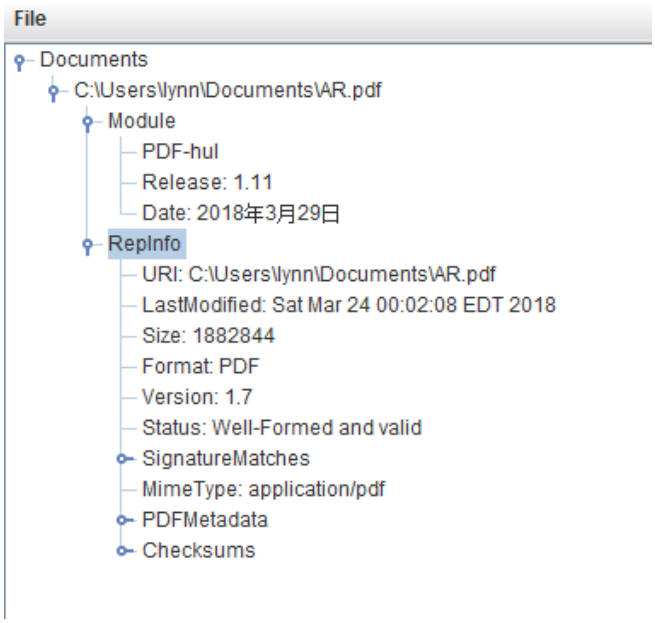

Figure 8: Open Source Jhove

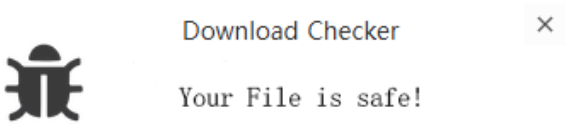

Figure 9: Download Checker Safe Announcement

4.3 Defense Mechanism Based on MBR Recovery

From our experiments, we can see that ransomware like Petya, which targets MBR partitioned machines and only encrypts the MBR section instead of specific files can be easily recovered at the

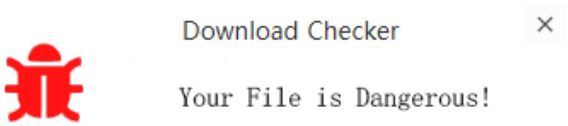

Figure 10: Download Checker Dangerous Announcement

first stage after infected. We can prevent further steps from happening before the malware does harm to other parts by launching MBR rebuild or overwrite. Advanced methodologies are that we can backup the MBR and MFT regularly, and if any modification towards these parts detected, a recovery boot item will be added and users can automatically enter the recovery stage before the malware execute other malicious codes. In this way, we can stop the malware at the first time and help protect users from losing data.

4.4 Decryption Tool

Based on the previous discussion about the encryption process, there are two ways to generate the password without paying the ransom.

Comparing to the original Salsa20 algorithm, Petya's encryption algorithm is largely simplified by replacing DWORD with WORD. Therefore, one way to decrypt is brute force. [11] gives a solution to take the 512 bytes data in sector 55(0x37) offset 0, and the 8 bytes data starting at sector 54(0x36) offset 33(0x21), which is the IV and do the calculation to get the personal code.

Given the fact that the malware author has released his master key on July 5th, 2017 and the personal code is generated by encrypting the decryption password with ECIES scheme, another way to decrypt is to use the decryption code along with the master key to get your personal key[12].

5 Conclusion

From the several basic methods we proposed, we can help to protect the users from the source, i.e., we can stop the users from downloading or opening a malicious file.

The detection of Petya is hard, but it has several common features which most malware would have, e.g., using an inappropriate icon. Our methods are not complicated but are effective for malware with this features.

The recovery of encrypted files are extremely difficult, but we can find the way to recover MBR before Petya destroy the whole file system and avoid the loss of data. And with the decryption key provided by the writer, we can recover the files with the help of third-party tools available on the Internet.

The advice given by NJCCIC is to install patches in time, and stop using outdated software and discontinue the use of unsupported/EoL software or hosts, update anti-virus software with the latest definitions and set it to automatically update. We should also run all software as a non-privileged user to diminish the effects of a successful attack. Applying the Principle of Least Privilege to all systems and services is a good way to prevent ourselves from this kind of attack.[7]

6 Contribution

Song Yang: I worked on the background analysis, and the analysis of Internet attack indicator of Petay, and find out the icon protector and file scanner defense mechanisms, and implemented these defense applications.
Xin Yang: I did the background research, proposed and implemented the MBR recovery method, also did the paper writing, and assisted the research on other defense mechanisms.
Zhuohang Li: I did the infection research, literature review, proposed and implement decryption methods and assisted on analysis and defense mechanisms.

References

[1] Wikipedia, 2018. https://en.wikipedia.org/wiki/Petya_(malware).

[2] Josh Fruhlinger, 2017. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

[3] Symantec Security Response Team, 2017. https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

[4] Paul Ducklin, nakedsecurity by sophos, 2016. https://nakedsecurity.sophos.com/2016/04/04/new-ransomware-with-an-old-trick-petya-parties-like-its-1989/.

[5] Stefano Mereghetti, 2017. https://smeretech.com/en/petya-ransomware/.

[6] Petya crypto-ransomware overwrites mbr to lock users out of their computers. https://blog.trendmicro.com/trendlabs-security-intelligence/petya-crypto-ransomware-overwrites-mbr-lock-users-computers/. [Accessed: 2016-03-15].

[7] Petya. https://www.cyber.nj.gov/threat-profiles/ransomware-variants/petya. [Accessed: 2016-12-7].

[8] Ransomware petya encrypts hard drives. https://www.gdatasoftware.com/blog/2016/03/28213-ransomware-petya-encrypts-hard-drives?type=0. [Accessed: 2016-03-24].

[9] Deviceiocontrol function. https://msdn.microsoft.com/en-us/library/windows/desktop/aa363216(v=vs.85).aspx.

[10] Petya – taking ransomware to the low level. https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/. [Posted: April 1, 2016].

[11] hack-petya. https://github.com/leo-stone/hack-petya.

[12] petya recovery. https://github.com/hasherezade/petya_recovery.