Progress Report of Ransomware Petya Analysis

Song Yang Xin Yang Zhuohang Li

March 2018

Abstract

This is the second module from our research project for course *Malware Analysis & Reverse Engineering*. In this module, we will provide a review of the past work on the analysis of Petya and sum up the methodology to analyze such ransomware.

1 Review of Literature

This section presents previous analysis report on Petya. Petya is a malware first discovered in March 2016. Petya prevents the victim from accessing his files by encrypting the hard drive and asks the victim to pay the ransom by Bitcoin to unlock. Petya is the first ransomware that infects the lower level structure of the victim machine.

1.1 Infection Routine

Petya targets Windows OS and is mainly distributed via email. It is disguised as a job application letter from an applicant that is seeking a job within the victim's company. It contains a hyperlink to a Dropbox storage location. Under this Dropbox folder, as shown in Figure 1, there are a self-extracting executable file, named to be the applicant's CV, and a photo of the applicant. If the user downloads and run that executable file, it would start extracting and unleash a Trojan to the system[3].

1.2 Infection Symptoms

After double clicking on this executable file, the victim machine will crash with a blue screen of death (BSOD) and reboot. As the system restarts it will show a screen as Figure 2. It claims to run a system check program namely CHKDSK, but it actually has already started encrypting. Then after the next reboot, a flashing ASCII skull as shown in Figure 3 will be displayed on the screen when the victim is finally aware that something is wrong. By now all of the files on disk will be no longer accessible from the user, even attempt to restart in safe mode will fail[2]. As shown in Figure 4, Petya asks the victim to go to the deep website and

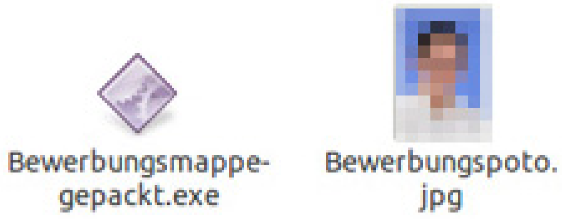
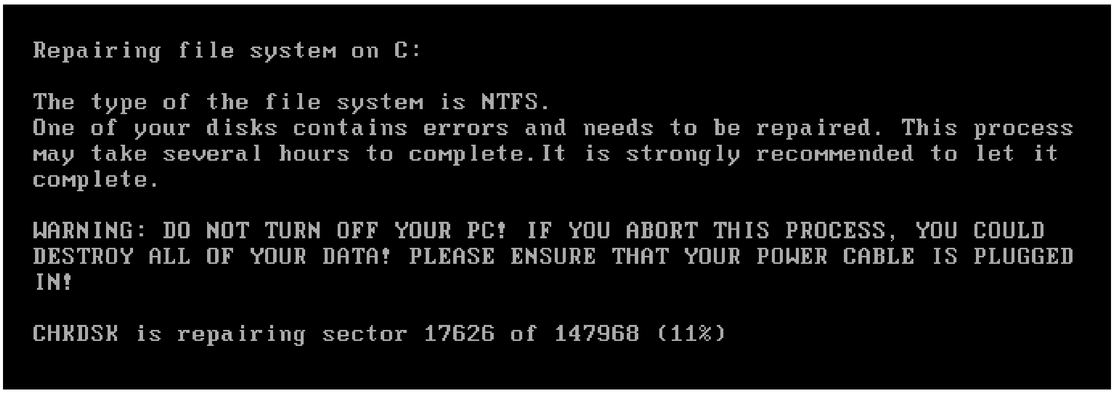
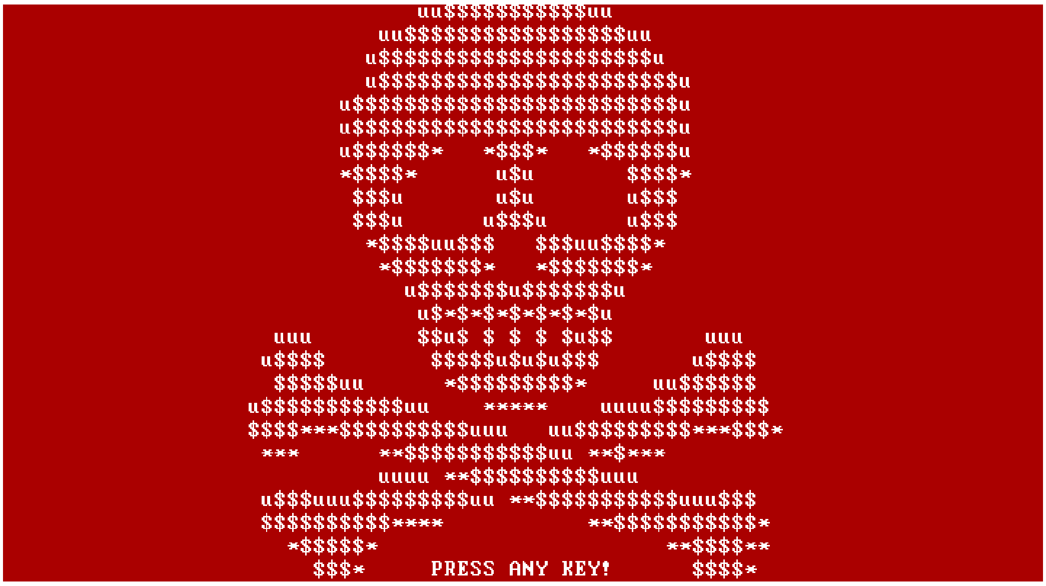


Figure 1: Contant of Dropbox Folder



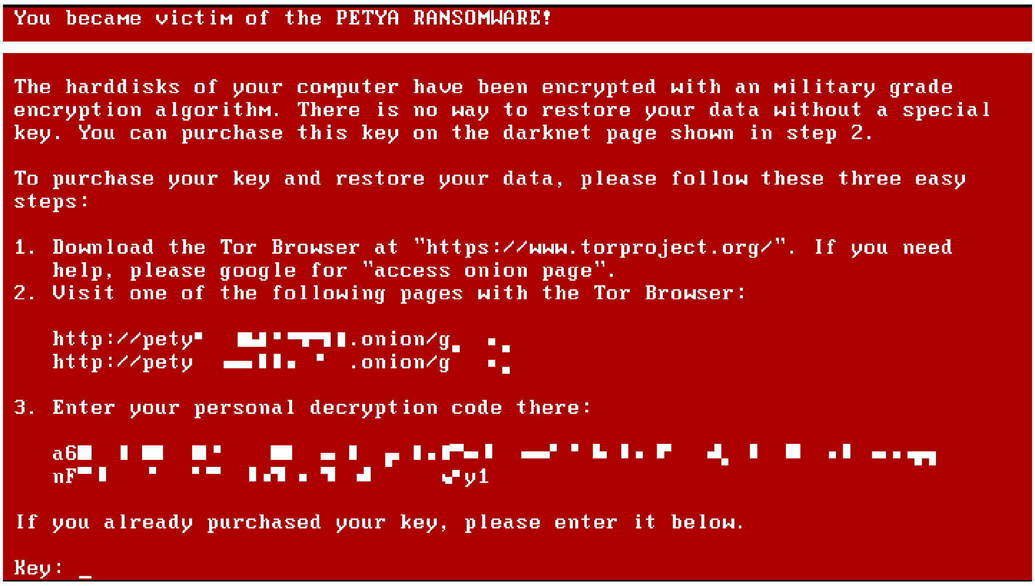
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 17626 of 147968 (11%)
```

Figure 2: Screen after reboot



```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$$*    uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

Figure 3: Petya's red-skull-and-crossbones warning



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://pety[redacted].onion/g[redacted]
   http://pety[redacted].onion/g[redacted]

3. Enter your personal decryption code there:

   a6[redacted]
   nF[redacted]y1

If you already purchased your key, please enter it below.

Key: _
```

Figure 4: Ransom information

pay ransom to decrypt[6]. Compared with other ransomware, for example, WannaCry, which encrypt victim's important files on disk, Petya goes a step further to encrypt the entire disk instead and it works before the system boots.

1.3 Behavior Pattern

Previous reports unveil that Petya has the following behavior pattern after execution:

- **Overwrite MBR:** Master boot record (MBR) is the first section of a partitioned storage device. MBR holds the information that how the logical partitions are organized in that region. Moreover, it also contains executable code that loads the installed in the operation system. Comparing with encrypting all files on disk which would cost a lot of time, this makes Petya works in a more efficient way and the OS will remain inaccessible even if the victim reinstall the OS. Modifying MBR requires permission from the administrator, that's the reason why there are a pop-up windows requests for administrator privilege when the user executes the fake CV file in the first place. Other ransomware usually encrypts files directly to avoid requesting for special privileges[7]. In this stage, Petya also generates a set of crypto keys, including a 16-byte key for disk encryption and an Elliptic Curve key. At this point, the special ”decryption key” is also prepared. Disk encryption key and the decryption code is stored in the disk for later use. After all this, it will shut down the machine without waning to boot the MBR code[4].
- **Encrypt MFT** In this stage, Petya will first check if the overwrite to the MBR is successfully completed. If so, Petya then begins enumerating the drive's Master File Table (MFT) records, as the same time display the screen as shown in Figure 2 to masquerading as a legitimate file repair application [1]. MST is the file system used by Windows OS.After this stage, the file system will become completely unreadable.
- **Demand Ransom** Display the horrifying Petya logo and then gives all the instructions the victim need to finish the payment through provided a link in order to decrypt their disk. Generally speaking, hackers do care about user experience, but in Petya, long personal decryption code and locking the whole system make more victims choose to wipe the data rather than paying them.

2 Methodology

The infection of Petya is a disaster and many security organizations have released their own Petya recovery tools, but they are only for the afterward. The currently available given advice for prevention is to install the patches in time. Our idea is to provide a tool which can both help prevent the Petya and recover if infected regardless of the partition table format and operating system version with a forward-looking partition table backup and recovery mechanism.

2.1 Prevention

Petya is exploiting the EternalBlue vulnerability, hence we would study the features of it and help users take necessary steps to prevent from being infected.

Multiple operations are available and the most important one is to install the patches. Also according to the available analysis[5], a vaccine can be taken to stop the infection, which is creating a perfc.bat file manually. Raising the level of UAC and turn of auto reboot after system failure can also help prevent the Petya enter the second stage.

The most deadly feature of Petya is that it will encrypt the MBR partition table and make the whole disk unreadable. What we are trying to do is develop our own prevention method to backup the partition table in case it's changed by malware.

2.2 Recovery

As Petya is targeting on Windows systems which have a version lower than Windows 10 with MBR partition table, most recovery tools and official decryption can successfully recover the encrypted disk when the victim is using an MBR partitioned machine.

As to recent machines which have UEFI plus GPT boot mechanism, the most origin Petya won't work, but for recent variants, the recovery tools might fail as Petya variants will destroy the GPT part instead of MBR. Our novelty is to target the encryption of the partition table and try to find out a proper way which can help recover the victims regardless of which partition table is used. To make this recovery tool long lasting and more widely used. We will also study how to backup the MBR or GPT partition table and recover if infected by other malware with the similar mechanism.

Our methodologies will be based on the analysis and understanding of how the partition table is encrypted and recovered and the solutions from third-party security organizations. We will develop a complete solution for both prevention and recovery, which is targeted on Petya but still might work for future malware's attack.

References

[1] Decrypting the petya ransomware. https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/. [Accessed: 2016-04-11].

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

[3] 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].

[4] Petya: Disk encrypting ransomware. https://labsblog.f-secure.com/2016/04/01/petya-disk-encrypting-ransomware/. [Accessed: 2016-05-03].

[5] 'petya' ransomware attack: what is it and how can it be stopped? https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how. [Accessed: 2017-06-28].

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

[7] The petya ransomware just got a whole lot worse. https://www.pcworld.com/article/3070374/security/petya-ransomware-is-now-double-the-trouble.html. [Accessed: 2016-03-13].