An Analysis of the Petya Ransomware Project Proposal

Song Yang (sea.yang@rutgers.edu)
Xin Yang (xin.yang@rutgers.edu)
Zhuohang Li (zl299@scarletmail.rutgers.edu)

February 8, 2018

1 Introduction

We are going to run our project on the Petya malware. It is going to be a course report, but we will still make it professional. Back to 2015, Ukraine power government suffered a hack because of a malware attack, which caused some Ukraine cities out of power for hours before Christmas.

2 Malware Description

2.1 Basic Information

Petya is a famous ransomware family first found in 2016. In 2017, a variant of Petya family which was 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 going to study the most original one, which is called exactly Petya. Petya is the first malware that can blackmail and change the master boot record(MBR) at the same time and targets on computers running Microsoft Windows.

2.2 Attack Methods

Petya was propagated through email at the very beginning. The attackers send malicious emails with faked files as attachments[2] and mislead users to download the attachments such as a resume pdf file. After the user opens the file, Petya will be activated and run. 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 stop Windows from rebooting, meanwhile, it will encrypt the whole file system and blackmail the users for

Bitcoins worth three hundred dollars to decrypt the file system. If the user failed to pay the ransom, the requirement would be doubled. Also during the encrypting process, Petya will pretend to be fixing hard disk issues and tell users this progress might take hours, during this period of time, until the whole system is locked, Petya would reboot again and show the real face asking for ransom, asking users to download Tor Browser, which is a tool to get access to the dark web[4]. Then users are asked to follow the instructions on the screen to visit the dark website and pay for decryption, the only way provided by Petya author to decrypt is to type the purchased decryption code. Also, in the background, Petya would scan the local area network, which is also an important method for propagation.

Comparing with the recent blackmail virus - WannaCry, they show similar features. As they both require Bitcoins to unlock computers, and they took use of the same security vulnerability named EternalBlue. Although WannaCry is threatening enough to urge users to install the patch, there are still many people with outdated computers from government and educational institutions got hacked. Not as widely as WannaCry, Petya, according to public report, attacked targets including Ukraine government and media, Russia Central Bank, some European business company and certain companies in America.[5]

The very source of this Petya attack is the email. The update service of MeDoc is hijacked, the hackers use this as a security case or mask of the virus. Emails were sent with an attachment of document from an unknown user. The document is actually a mask of plenty payloads. Petya is really smart, it will hide after it has successfully installed on the computer, and run a private tiny system to keep its own data. In case of the static scan from antivirus software, Petya uninstalls the main body of itself and only left parts of scripts.

2.3 Global Influence and Damage

The danger of Petya is that it will directly lock and encrypt the whole hard disk[6], rather than just encrypt several types of files as what other traditional ransomware would do. Petya changes the original MBR, so it took over the boot order and theres no way to reboot into Windows. Also after being infected by Petya, if there are other computers in local area network(LAN), those computers can be infected too.

The initial version of Petya began to spread in March of 2016. It is sent to the victims computer attached to an email pretending to be a job applicants resume. The package contains an executable file, with PDF somewhere in the file name. The plan is to get you to click on that file and to subsequently agree to the Windows User Access Control warning that tells you that the executable is going to make changes to your computer. Petya is different from other popular ransomware because instead of encrypting files one by one, it denies access to the full system by attacking the low-level structure of the disk. The writer of Petya created not only their own bootloader but also a 32-sector-long kernel[7].

In June of 2017, a new variant of Petya began spreading rapidly. Within 3 months, it has already influenced most of Europe countries, including Ukraine, Russia, England, France, and India. The government, bank, electrical supply system, communication system and companies are suffered from varying degrees of damage. Over 80 percent infected computers are in Ukraine. The countrys government, banks, top energy companies, airports, and metro

system have all reported hits on their systems. Even the nuclear power plant is hit by this attack.[8] According to online sources, nearly 150 organizations have been affected in Ukraine and under 50 in the US. As the government and banks declared after being attacked, the trend is well under control.

Also as a result of this event, the digital currency is heavily influenced, the rate of Bitcoin to dollars dropped to the lowest point since 2000.

As Microsoft explained, Petya is a malware with a high level of complexity, but the number of victims is way much 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 cant say this malware can be perfectly intercepted under Windows 10 because the defense methods can only reduce the chance of being attacked. Microsoft has released a patch to fix the vulnerability about remote debug code.[9]

3 Project Motivation

Petya is one of the most influential malware in recent years. The modified version of it caused huge damage worldwide. It has several features:

- Petya targets Windows-based systems, which meets the course requirement since our virtual machine is based on Windows XP. Moreover, due to the fact that Microsoft has already fully stopped the support for XP while there are still massive users using Windows XP, studying Petya could be of practical use.
- This malware is attached to an email with disguised PDF at the early time. This is a common way for malware to spread themselves nowadays. Therefore we believe analyzing this can make us more experienced when dealing with other malware that shares the same feature.
- Petya uses the local area network to searching for local IPs to infect other computers in the same network, which is hard to detect on a large scale of users. And it only takes little time to destroy the whole system. This is the point that makes Petya extremely threatening to group users like companies and government.
- Petya uses the local area network to searching for local IPs to infect other computers in the same network, which is hard to detect on a large scale of users. And it only takes little time to destroy the whole system. This is the point that makes Petya extremely threatening to group users like companies and government.
- Users are forced to pay three hundred dollar-worth Bitcoins and email to the writer as ransom. This is becoming the stock-in-trade of modern cybercriminals.
- Petya exploits the EternalBlue exploit that also used by the WannaCry ransomware.
- We are quite interested in what the program Petya is designed for, and all the steps that can cheat the users along with antivirus software.

- Petya can enhance its permission. Wed like to find out how it works and how to avoid this.
- Petya uses a fake chkdsk program to hide the process that encrypting documents.

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] Quora N0.a2ce54846eb0, 2017, https://www.forbes.com/sites/quora/2017/07/05/how-similar-are-wannacry-and-petya-ransomware/.

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

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

[8] Keith Clollins, 2017, https://qz.com/1015755/ukraine-cyber-attack-the-petyapetrwrap-ransomware-with-similarities-to-wannacry-is-now-going-global/.

[9] Market Realist, 2018, https://marketrealist.com/2017/07/what-microsoft-has-to-say-about-petya.