SECURITY REPORT

NOTPETYA RANSOMWARE

AVIRAL RAJPUT

A00258751

Table of Contents

NotPetya Virus

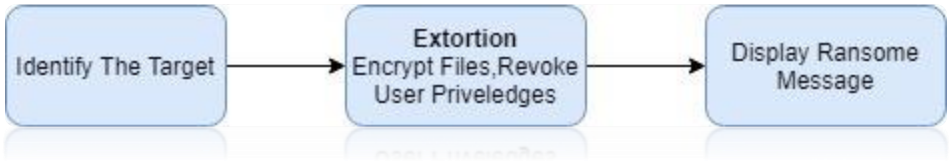
Software Engineering Year 4, Athlone Institute of Technology, Athlone, Ireland
A00258751@student.ait.ie

Introduction

On the day of 28th June 2017 when Ukraine was celebrating constitution day they were unaware about what was coming to them. On that evening Ukraine lost 50 Million in terms of destruction of data. Organizations and agencies hit by NotPetya ransomware were not only limited to geographic borders of Ukraine, it affected many European Countries and US. Ukraine being the ground zero for NotPetya, it targeted Ukraine's central bank, municipal metro, a state telecom and Kiev's Boryspil Airport. Conditions with Chernobyl nuclear site were so disturbed that they had to switch to manual radiation motoring. Russia's state oil company was compromised due to NotPetya and faced major issues. In US, number of hospitals were affected and 'Merck' a pharmaceutical company and 'DLA Piper' a law firm from US faced major losses.

What Is a Ransomware?

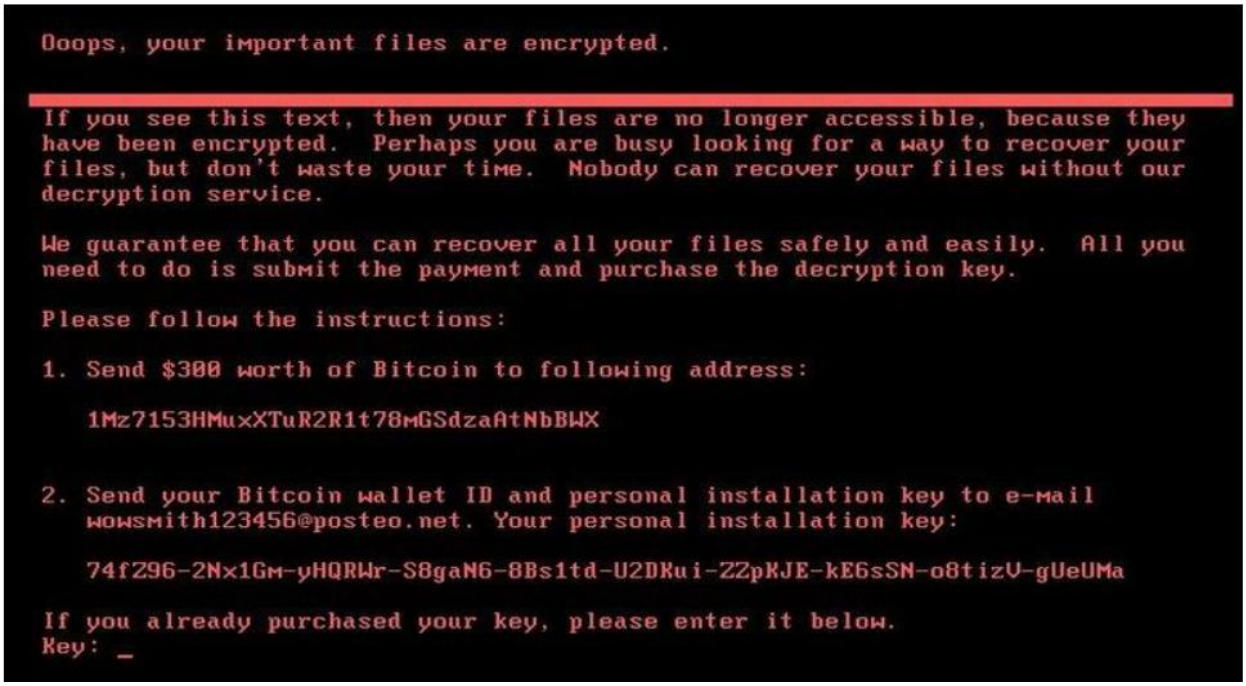
Ransomware is assembled from two words ransom and malware. "A ransomware is a kind of malware which demands a payment in exchange for a stolen functionality" [10].Most ransomwares encrypt the files on the system for blackmail purpose. Blackmailing in terms to data. Where the attacker steals the data from user and demand a ransom (Asset in exchange in terms of Money, Bitcoin Generally) to return the data. Ransomwares have been into eyes from a long time and used as the medium of mass destruction of data in terms of information technologies.



1. Identify The Target: Identifying what has to be encrypted, as a user is more concerned about personal files like photos, documents, and document files i.e. .pdf, .zip, .rar rather than any dll file that's on the system.
2. Extortion: Depending upon the frim and how readily the firm is willing to pay ransom attackers infect the system, i.e. Government agencies need data to keep it confidential and readily available. Attacker take the advantage of these situations to blackmail the user.
3. Ransome: The aim behind all this is money, Attacker leave a message with contact via email or other services to communicate with the user.

NotPetya

NotPetya From the family of ransomware got its name from derived from close relative **Petya** an encryption ransomware that was created to attack Microsoft windows based computer systems. Petya attacks and infects the MBR (Master Boot Loader) of the windows system to execute the payload and then encrypts the hard drive's file system table. When Encrypted displays a message to user demanding payment in bitcoins to buy the key to access the data again.
NotPetya though have many common features of Petya but NotPetya is termed as fastest spread virus of the History.
"Petya generates a 16-byte key and uses the Salsa20 cipher to encrypt the MFT of the NTFS partitions found on local drives. To make decryption possible only by its operators, it uses the Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithm with the curve secp192k1 and a public key is embedded Into Petya's body," said Kaspersky [1] Lab researchers.



Source: Symantec

Scenario

Infector used watering hole technique to widespread NotPetya, Ukrainian website that is used throughout the country for accounting and taxation software programs called MEDoc**.** This allowed the attackers to download and execute arbitrary activities run harmful commands to exploit the system and resources.

"MEDoc is one of only two software options Ukrainian businesses have to pay their taxes, noted Lesley Carhart, an information security expert. [2]"

While MEDoc became just an initial path for attacker to get inside plenty of systems, once they

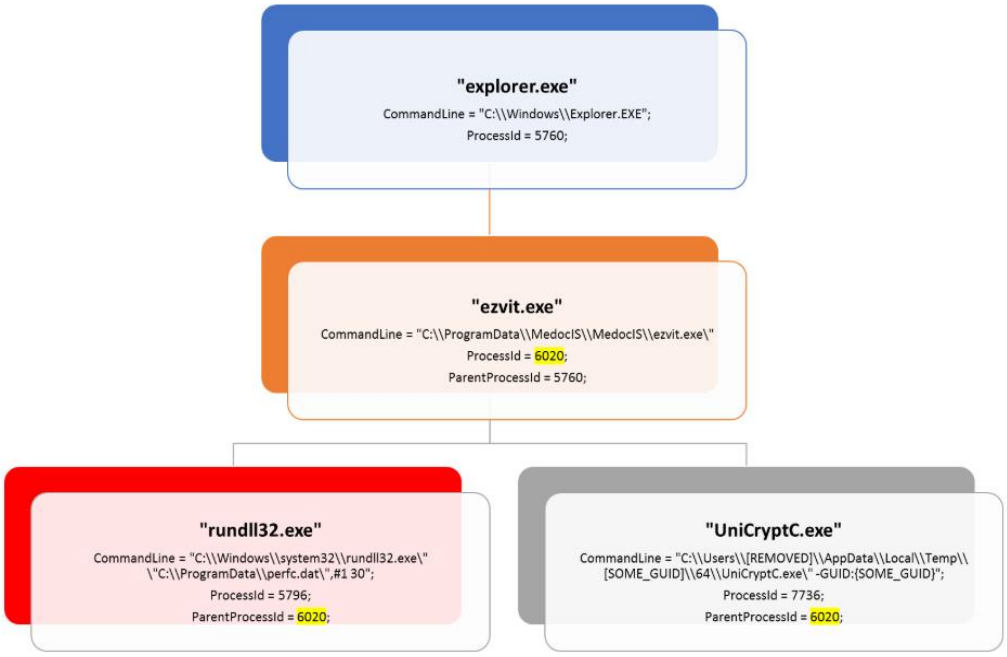
NotPetya triggers various methods to supper in the poisoned network [3] (Us-cert.gov, 2018)

- *PsExec - a legitimate Windows administration tool*

- *WMI - Windows Management Instrumentation, a legitimate Windows component*
- *EternalBlue - the same Windows SMBv1 exploit used by WannaCry*
- *EternalRomance - another Windows SMBv1 exploit ".*

In simple words, NotPetya encrypts the user's data files with a 128 bit key that is generated dynamically and created the unique ID of the user. While, there were both an encrypted key and a unique id it's still unclear if there was any relationship between them which suggest even if the demand are met there is no assurance that the files will be decrypted again.

C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30



The same update vector was also mentioned by the Ukraine Cyber Police in a public list of indicators of compromise (IOCs) , which includes the MEDoc updater.

NotPetya implemented an amended ***Mimikatz*** *version* to get the user credentials from windows system. Then With the help of WMIC (Windows Management Instrument Command Line) tool or the Microsoft SysInternals utility, psexec.exe access other systems that are present in the network.

Another Way of penetration was the use to EternalBlue exploit tool that aimed at the system that were running on older version of SMBv1 which was vulnerable. Here the virus attempts to identify other nodes present in the network by running a poisoned DHCP (Dynamic host configuration protocol) with IP to physical address mapping table.

It will then run a scan on all the system present in the network, identifies the system with exploitable SMB versions (old version- Not Patched) and installs the ransomware on them and repeats the cycle again.

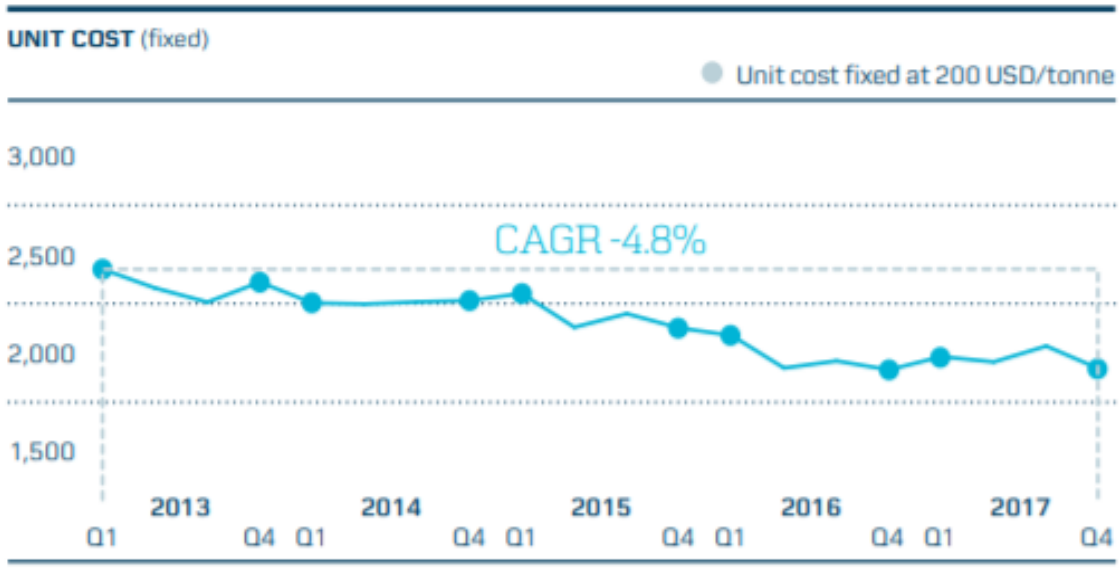
NotPetya used 128 bit AES (Advanced Encryption Standard) algorithm during runtime. The ransomware then creates a text file in system installation directory with a static bitcoin location and unique key intended for the infected system to be used while making the payment in bitcoin. It modifies the MBR (Master Boot Loader) that enables the encryption of MFT (Master File Table) and original MBR along with it and then reboots the system.

Aftermath: Destruction caused by NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

FedEx Owned European subsidiary company TNT Express a company that provides delivery services was also affected by NotPetya Due to MEDoc as they have their services in Ukraine. Financial reports published by the company depicts the serious damages that been held in many cases. There are certain chances that the data lost in attack could never be recovered, Says Report [4]. *Financial Loss:* $400,000,000 through European subsidiary TNT Express.

Danish business conglomerate Maersk evaluated in their financial reports [5] that the losses occurred due to Cyber-attack were as high as $300 million. The conglomerate attributes to cyber-attack for the loss in revenue in the third quarter of 2017.



Unit cost at fixed bunker price was 0.2% above 2016, as 2017 was impacted by contingencies, a cyber-attack and lower headhaul utilisation. Unit cost was at its lowest for the year in Q4 2017, with volume recovery following a challenging Q3 2017 impacted by the cyber-attack.

Pharmaceutical company Merck CFO Robert Davis said [6] that NotPetya had "negatively impacted third-quarter results, including an unfavorable revenue impact of approximately $135 million from lost sales and approximately $175 million in cost". Confirming the financial announcements, Merck admitted that virus had disturbed the jobs carried in various sectors including manufacturing and sales as major.

Reckitt Benckiser, the British consumer goods Company said the attack interrupted its manufacturing unit and product distribution cycle. With the lost or track with goods generated company concluded it will suffer huge revenue loss due to cyber-attack. Financial Loss: $129,000,000.

Nuance Communications Voice and language solutions financial reports (Nuance Communications, 2017) [7] concluded the difference of GAAP and Non GAAP revenue from the third quarter estimate before the cyber-attack took place. Nuance estimates reveals the GAAP revenue of $501.6 million and non GAAP revenue of $511 million if the cyber-attack would have not been taken place. Which incase generated the loss to revenue with GAAP revenue of $486.2 million and non-GAAP revenue of $495.6 million in the third quarter

Mondelez International, Estimated a loss of over $150 million in terms of lost sales and other expenses to recover the data and make system fully functional. Financial unit, sales and distribution were the major parts affected by the attack. Company reflected that the attack brought net loss of 2.3% on revenue growth as the result of incident. *Mondelez said [8]. "The malware affected a significant portion of the company's global Windows-based applications and its sales, distribution and financial networks across the company".*

Saint-Gobain [9] (SAINT-GOBAIN, 2017) French construction giant confirmed in their report the attack led to downtime of information systems and disruption of supply chain which were restored on July 10. The cyber-attack led to loss of $258 million on sales and $76 million on operating income in the first half of 2017. Total losses are expected to rise to $387 million.

How to Stay Protected From NotPetya?

The first assumed plan before any ransomware attack is to leverage the working of the user's system either by corrupting the system or bringing it down temporarily, the virus can be spread by phishing emails or by simply poisoning the DNS. NotPetya was able to infect the systems that had older version of windows running on them.

Mentioned below the following ways to in which we can prevent NotPetya Ransomware

- Arm the system with a good intrusion detections and prevention system with personalized settings native to systems environment and for personal use keep an anti-virus.
- Avoid installing/downloading or opening of any unknown attachments from untrusted sources.

- Create and maintain the backups of system routinely.
- Install the latest updates of antivirus software and apply patches whenever necessary.
- Train people on soft skills of IT to realize and examine possible threats and how to deal with them.

Conclusion

NotPetya ransomware recklessly made a hassle and destroyed IT infrastructure in Ukraine and other countries. With the loss of overall more than billions NotPetya became one of the quickest spread virus witnessed till date. While Ukraine became the ground zero for NotPetya, it escalated quickly into different parts of world leaving many major business on temporary halt. Compromise in security could be seen as the result of inefficient planning and lack of infrastructure.

Regular Surveys by National Cyber Security Alliances demonstrate that many companies lack a formal set of internet protocols to be followed by employees, the statistics of these studies are unpleasant. Only around 25% business have had 3rd parties outsourced to test their systems to ensure proper working and ensure all possible security protocols are being met. Human Resource play an important role in deciding what will the impact of virus, a proper training to IT professionals could prevent or minimize the loss that could occur. Organizations could learn from the mistakes from past and try to impose the system that is robust and secure.

References

[1] Securelist.com. (2017). *PetrWrap: the new Petya-based ransomware used in targeted attacks*. [online] Available at: https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/ [Accessed 24 Mar. 2019].

[2] Washington Post. (2017). *Ukraine's ransomware attack was a ruse to hide culprit's identity*. [online] Available at: https://www.washingtonpost.com/gdpr-consent/?destination=%2fworld%2fnational-security%2fthis-weeks-global-ransomware-attack-was-a-ruse-to-deflect-attention-from-the-true-culprit-researchers-say%2f2017%2f06%2f29%2fda455a0e-5cf0-11e7-9b7d-14576dc0f39d_story.html%3futm_term%3d.a0013cfefdf1&utm_term=.32937fb40357 [Accessed 25 Mar. 2019].

[3] Us-cert.gov. (2018). *Petya Ransomware | US-CERT*. [online] Available at: https://www.us-cert.gov/ncas/alerts/TA17-181A [Accessed 26 Mar. 2019].

[4] ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934. (2017). [online] UNITED STATES: FEDEX CORPORATION. Available at: https://www.sec.gov/Archives/edgar/data/1048911/000095012317006152/fdx-10k_20170531.htm [Accessed 27 Mar. 2019].

[5] Anon, (2017). *A.P. Moller - Maersk | Annual Report 2017*. [Online] Available at: https://www.maersk.com/-/media/ml/about/sustainability/20180209-a-p-moller-maersk-annual-report.pdf [Accessed 26 Mar. 2019].

[6] TechRepublic. (2017). *NotPetya ransomware outbreak cost Merck more than $300M per quarter*. [online] Available at: https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/ [Accessed 28 Mar. 2019].

[7] Nuance Communications, I. (2017). *Nuance Announces Third Quarter 2017 Results*. [online] GlobeNewswire News Room. Available at: https://www.globenewswire.com/news-release/2017/08/08/1081816/0/en/Nuance-Announces-Third-Quarter-2017-Results.html [Accessed 28 Mar. 2019].

[8] Foodbusinessnews.net. (2017). *Mondelez not yet 'back to normal' from cyber attack*. [online] Available at: https://www.foodbusinessnews.net/articles/9725-mondelez-not-yet-back-to-normal-from-cyber-attack [Accessed 31 Mar. 2019].

[9] SAINT-GOBAIN (2017). *First-half 2017 results*. [online] Available at: https://www.saint-gobain.com/sites/sgcom.master/files/cp_va_resultats_s1_2017_t.pdf [Accessed 29 Mar. 2019].

[10] Gazet, A. (2008). Comparative analysis of various ransomware virii. *Journal in Computer Virology*, [online] 6(1), pp.77-90. Available at: https://link.springer.com/article/10.1007/s11416-008-0092-2 [Accessed 29 Mar. 2019].

[11] Microsoft Security. (2017). *New ransomware, old techniques: Petya adds worm capabilities - Microsoft Security*. [online] Available at: https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/ [Accessed 26 Mar. 2019].