CTI Report

Not Petya

2024-02-11

Viktor Listi DVGHI22h
vili22@student.bth.se

Table Content

Introduction

The 27th of june 2017 Ukraine was hit with an attack that brought the entire country to a halt, most of the computer systems in the entire country had been hit with a devastating attack by the name of NotPetya. It is said to have been one of the most devastating cyber attacks to ever have been executed.

The following report will provide an overview of the timelines of the attack and explain what the NotPetya worm was and how it worked inorder to do the damage that it did.

Summary

The NotPetya attacks was a destructive worm that affected Ukraine among other countries on the 27th of june 2017[2]. But the planning and preparations for this attack had started at least 6 weeks before by exploiting a backdoor in one of the primary applications for tax preparation in Ukraine called M.E DOC to initially spread. Leveraging vulnerabilities in the Windows OS, the worm quickly propagated within networks, infecting connected systems and completely destroying them.

Although the attacks were theorized to only hit Ukraine the attacks managed to also hit other countries as well but 80% of the reported attacks were against Ukraine[2]. Countries such as Germany, France, Italy, Poland, the UK, the US and Russia were also hit although a press secretary from Russia stated that the attacks had caused no serious damage to Russia[x]. The worm had been made to totally destroy the systems it affected by completely encrypting the entire computer system similarly to a ransomware attack although in this case there was no plan of ever decrypting any of the systems affected. These attacks ended up totally halting daily life in Ukraine as payment systems, public transport systems, power grid systems among others were affected which effectively brought down the entire country for a period of time. In the aftermath of the attack, affected organizations struggled to contain the spread of NotPetya and restore operations as the complexity of recovering encrypted systems posed a significant challenge.

Threat Actors

Certain experts believe the NotPetya attacks to have been a politically motivated attack against Ukraine since it occured on the evening of the Ukrainian constitution day[2]. The main suspects for these attacks are believed to be Russian hackers and to be related to the ongoing conflict between these two countries as the timing of the attacks suggests a deliberate attempt to maximize the disruption caused. The correlation between this attack and Russian linked groups grows even stronger due to the multitude of previous attacks that Ukraine have faced which have been proved to be linked to Russian groups. The sophistication and scale of the NotPetya attacks indicates a well resourced and organized threat actor. As well as the attack having a purely destructive goal points to the threat actor in this case not being some random grouping but a well organized grouping with a larger goal. Later analysis of the attack has proved there was evidence of Russian presence, and an employee’s account on M.E DOC servers had been compromised. The attacks were blamed on the Russian hacking group called Sandworm within the GRU Russian military intelligence organization by researchers and several government entities.[2]

Methodology and Vulnerabilities

The NotPetya attacks used many different tools and vulnerabilities when initiating their attack, in this part of the report these will be explained and how they worked in the bigger picture.

Petya

Petya is a type of ransomware malware that was first used in 2016[2]. The malware attacks the system by executing a payload that encrypts the entire Master File Table (MFT) and Master Boot Record (MBR) of a system. Unlike other ransomware methods, Petya does not encrypt individual files but the entire system structure as a whole making the system unusable. It then requests the target to pay a sum of money in order to get the system decrypted and usable again.

EthernalBlue

EthernalBlue is a tool initially developed by the U.S National Security Agency (NSA) that was leaked after a hacker group called Shadow Brokers attacked the NSA on April 14 2017[3]. EthernalBlue exploits a vulnerability in Microsoft's server message protocol which enables remote code execution effectively allowing the attacks to infiltrate vulnerable systems without any user interaction. Microsoft released a patch for this issue just a month after the leak but many systems remained unprotected which later led to the possibility of the NotPetya attack.

Mimikatz

Mimikatz is a powerful exploitation tool which exploits a flaw in the Windows OS where both an encrypted version of users passwords and the key to decipher were extractable from the Local Security Authority Subsystem Service (LSASS) which effectively gave all the required passwords to control a system to whoever wanted them.

All of these tools together is what builds up the NotPetya worm. Now the question arises, how do all these fall together? It is very simple, firstly a system gets infected with the worm, it then deploys the Mimikatz tool to gather password information which it can later use on other systems. When it has gathered the information it executes the Petya encryption on the system and carries on jumping from system to system and gathering more information as it goes. Sometimes the worm will encounter a system it cannot infect, then it would deploy the EternalBlue tool to attack that system and continue its rapid spread. The worm was so effective that it was uncontrollable and an attack that was meant to just attack Ukraine quickly spread out of the borders and attacked other countries as well.

Timeline of attack[5]

- June 27, 2017 (05:00-06:00 EDT) - First signs of a digital attack campaign emerge on Twitter with tweets of reports indicating attacks on an electric power supplier.
- June 27, 2017 (08:00 EDT) - Threat intelligence provider Symantec Security confirms that Petya is responsible for the attacks, as well as it using EternalBlue.
- June 27, 2017 (10:00 EDT) - Kaspersky Lab tweets that the ransomware attack is not a variant of Petya but a completely new attack. They also reveal that the attack has affected approximately 2000 organizations.
- June 27, 2017 (12:00 EDT) - M.E DOC is confirmed to have been used as an infection vector for the attack.
- June 27, 2017 (13:00 EDT) - Security researchers begin to share ways in order to prevent the ransomware.
- June 28, 2017 (05:00 EDT) - Confirmations that people who have paid NotPetya are not getting their files back are being circulated on twitter.

Indicators of Compromise

- File integrity, hash values[6]
    - 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
    - 9717cfdc2d023812dbc84a941674eb23a2a8ef06
    - 38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
    - 56c03d8e43f50568741704aee482704a4f5005ad
- Commands[6]
    - Scheduled reboots
    - schtasks /Create /SC once /TN “” /TR “\shutdown.exe /r /f” /ST
    - cmd.exe /c schtasks /RU “SYSTEM” /Create /SC once /TN “” /TR “C:\Windows\system32\shutdown.exe /r /f” /ST
    - \”C:\\Windows\\System32\\rundll32.exe \\\”C:\\Windows\\perfc.dat\\\” #1
- Network[6]
    - tcp port 139
    - tcp port 445

Mitigation

There are many steps we can take in order to mitigate the NotPetya attack, methods for which and how they help prevent will be explained in the following.

- **Shutting down infected device**[7] - The encryption process could be stopped by shutting down the device when the check disk screen appears.
- **Creation of read-only files**[7] **-** Creation of read-only files called *perfc* and *perfc.dat* in the Windows installation directory could prevent the execution of NotPetya.
- **Patch of vulnerabilities**[7] **-** Installation of patches for the vulnerabilities to EternalBlue were released in 2017 March before the NotPetya attacks, these patches could help prevent the attack.

Sources

[1] ‘Mimikatz’ (18 December 2023 08:18 UTC). Wikipedia. https://en.wikipedia.org/wiki/Mimikatz (Accessed: 11 February 2024).

[2] ‘Petya (Malware Family)’ (18 December 2023 21:19 UTC). Wikipedia. https://en.wikipedia.org/wiki/Petya_(malware_family) (Accessed: 11 February 2024)

[3] ‘EternalBlue’. (10 January 2024 04:00 UTC). Wikipedia. https://en.wikipedia.org/wiki/EternalBlue (Accessed: 11 February 2024).

[4] Porsklev, Markus, (30 June 2020) ‘Notpetya och Ukraina’, *Nätets mörka sida.* [Podcast]. https://podme.com/se/natets-morka-sida/404233 (Accessed: 11 February 2024)

[5] ‘NotPetya: Timeline of a ransomworm’ (28 June 2017). Tripwire. https://www.tripwire.com/state-of-security/notpetya-timeline-of-a-ransomworm (Accessed: 11 February 2024)

[6] ‘Petya/NotPetya Ransomware’ (29 June 2017). Logpoint. https://www.logpoint.com/en/blog/petya-notpetya-ransomware/ (Accessed: 11 February 2024)

[7] ‘Email breach chronicles: The NotPetya catastrophe - global havoc in 2017’ (27 November 2023). Zoho. https://www.zoho.com/workplace/articles/notpetya-cyberattack.html (Accessed: 11 February 2024)