COMP 7003
Assignment 1

Analysis of the NotPetya Malware

Daryush Balsara
A01265967
Sept, 10 2024

Executive Summary

The NotPetya attack emerged in June of 2017. It masqueraded as a ransomware but caused irreversible damage to targets. It was made to cause widespread damage instead of extorting money for financial profit. It used a vulnerability known as MS EternalBlue which was a backdoor in Microsoft's SMB protocol. NotPetya spread throughout multiple networks as a worm infecting and encrypting multiple organizations systems.

The attack was mainly meant for organizations in Ukraine but because of a network's interconnectivity that spread far beyond Ukraine and affected organizations internationally. It rendered mission critical data inaccessible by heavily encrypting/overwriting files and the master boot record which led to most systems being inoperable for quite some time, which led to financial loss and disruptions to the affected organizations.

Nowadays, it is seen to be a state sponsored attack by Russia which served as either a demonstration of their cyber power or a geopolitical move attributed to the war on Ukraine. The attack showed us the vulnerabilities in many networks which led to the need to improve our global security standards to keep up with the ever evolving landscape of cybersecurity.

Introduction

In 2016, the world first encountered Petya, a ransomware strain designed to encrypt a target's files and demand a ransom for their decryption. It encrypted files on infected systems and demanded a ransom payment in Bitcoin for decryption. However, in 2017, a new and more destructive variant emerged, which bore a striking resemblance to Petya but was later identified as NotPetya by Kaspersky. Unlike its predecessor, NotPetya was engineered not just to demand ransom but to cause irreversible data destruction. This devastating attack primarily targeted Ukrainian businesses and government servers, affecting at least 2,000 organizations. While the exact motives behind NotPetya remain unclear, with theories ranging from showcasing cyber capabilities to geopolitical maneuvering, its impact was profound, highlighting the growing sophistication and potential for destruction in modern cyber warfare. The NotPetya cyberattack serves as a critical case study in modern cybersecurity threats, illustrating the intersection of geopolitics and digital warfare, and emphasizing the urgent need for organizations to prioritize resilience against emerging cyber risks.

Technical Analysis

To fully understand the impact and development of NotPetya, we must trace its origins back to its precursors and the evolving landscape of cyber threats that paved the way for its creation. EternalBlue is the name of an exploit developed by the NSA (National Security Agency) which allowed a threat actor to gain access to multiple computers on a network. The NSA kept this vulnerability hidden from Microsoft for many years until in 2017 they discovered that it had been stolen by a hacker group that went by the name of Shadow Brokers. The NSA had known about this exploit for over five years but did not inform Microsoft until it was discovered by the hacker group called the Shadow Brokers.

After the hackers exfiltrated the EternalBlue exploit, they initially attempted to find a buyer but were unsuccessful. Ultimately, they released it to the public on April 14, 2017. EternalBlue is an exploit that was based on Microsoft’s implementation of SMBv1 (Server Message Block Version 1). This protocol was used to provide shared access to files printers and serial ports on a network. It allowed software and users to access remote servers and resources. SMB is mainly client to client based. On May 12 2017, one month after the initial release WannaCry, a malware, used the EternalBlue exploit that the NSA developed to attack computers. It acted like ransomware but was a worm therefore, it encrypted data and asked for a ransom payment in the form of bitcoin. Microsoft had actually developed and released a security patch a month before May 2017, but many organizations had not applied these patches or had devices that were past their end of life allowing WannaCry to be executed.

One month after the WannaCry attack, the NotPetya malware was deployed, marking a significant escalation in the severity and sophistication of global cyber threats. It initially started to spread through a bad update in the Ukrainian tax software called MeDoc. This software was mainly used by the government and businesses. When the attackers gained control of the MeDoc update server, they began spreading illegitimate updates which were then sent to the users of the tax software who were connected to the server. The malicious update had the NotPetya executable payload so when users installed the newest update of the existing software they got the NotPetya malware installed on their devices. Once installed the malware would execute its own code by modifying the existing system configurations. The primary propagation method included using Microsoft’s SMBv1 to spread laterally across the network. This method was successful because of the users trust in the automated update server by sending legitimate updates and bypassing traditional security measures that would be able to detect a threat such as this one. The affected systems would lose all access to the master boot record which would be heavily encrypted by the malware.

To minimize the risk of an attack like NotPetya occurring in the future, we can implement several measures such as: Segmenting different regions of the network which is helpful in a situation like this as it isolates the devices that are affected by this malware which would help slow the lateral movements and would stop it from coming into contact with any critical devices. The segmentation would also help reduce the amount of systems the malware can jump to. You could implement some kind of user access control in between the segments such as critical components and infrastructure which would make it harder for NotPetya to get to these systems even if other parts of the network are infected. In this case you could implement a way to monitor each segment of the network and that way you can target certain devices that might get or have malware in the future. The long term impact of NotPetya is that it is known for its destructiveness and the fact that even though it acted like Petya which was ransomware it was actually a worm that could move laterally through the networks. It was known as a cyber activity which is considered to be an act of war. After this attack many organizations changed their implementation of network security by segmenting, creating more robust firewall rules, deploying security patches, setting access control rules and other strategies to help secure their network. Many organizations have responded by enhancing their security practices, including implementing more rigorous patch management processes, improving network segmentation, and deploying advanced intrusion detection and prevention systems. These measures aim to limit the spread of malware and reduce the likelihood of similar attacks succeeding in the future. The attack's impact on essential services demonstrated that cyber threats could translate into real-world consequences, affecting power grids, transportation systems, financial institutions and many more. This underscores the importance of integrating cybersecurity measures with physical security protocols and ensuring that IT environments are protected against sophisticated cyber threats.

The NotPetya attack did a lot of damage and had big implications in the world of cybersecurity and state sponsored cyber attacks. NotPetya is known as one of the most damaging security threats in the past couple of years. It revealed the critical need for a unified approach to security. The attack demonstrated how security vulnerabilities in different parts of the world can spread globally and impact organizations across different sectors. The interconnectedness of systems shows the need for cooperation from organizations globally and to further develop the global security policies to help foster information sharing, creating frameworks for incident response and to standardize best practices to help defend against attacks like this in the future. There were many ethical implications of this attack as it was linked to state sponsored actors. This raised questions about the ethics of cyber warfare. The introduction of cyber attacks like NotPetya introduces the complexities regarding accountability in responses. Since the cybersecurity field is always growing and evolving organizations need to keep themselves updated on the newest security practices on how to handle cyber attacks like this one and to prevent minimal losses in future attacks while keeping collateral damage to a minimum. There should be rules in place to govern how a nation can use cyber warfare going forward.

NotPetya also caused the insurance industry to transform how it looks at cyber attacks. The insurers need to determine how to provide coverage for these attacks. The ambiguity of NotPetya complicates policy and makes it harder to access the liability. Insurers have to take into account various factors like the intent behind the attack, the motivations of the perpetrators, and the potential implications for national security.

Conclusion

The NotPetya ransomware attack of June 2017 was a pivotal moment in cybersecurity history, revealing the severe implications of modern cyber threats on global security, infrastructure, and international relations. This attack, which was designed primarily to cause damage rather than to extract ransom, highlighted the destructive potential of cyber warfare and underscored critical lessons for both the public and private sectors.

NotPetya’s impact was far reaching, affecting thousands of organizations across various industries and countries. By exploiting the MS EternalBlue vulnerability, NotPetya spread rapidly, encrypting and rendering data inaccessible across networks. This incident emphasized the urgent need for a unified global approach to cybersecurity. The attack illustrated how vulnerabilities can have cascading effects, highlighting the necessity for international cooperation to develop robust cybersecurity policies, standardized best practices, and frameworks for coordinated incident response. The interconnected nature of today’s digital landscape means that threats are not confined by national borders, underscoring the importance of a collective, global effort in cybersecurity.

The ethical implications of NotPetya are profound. The malware's apparent ties to state-sponsored actors and its indiscriminate nature challenge traditional rules of warfare. The attack, which caused significant economic damage and disruption without a clear financial motive, raises serious questions about the ethics of using cyber tools for geopolitical objectives. It challenged the conventional understanding of accountability and proportionality in conflict, highlighting the need for new international norms and agreements. These should address how nations conduct cyber operations, how they respond to attacks, and how to protect civilian targets from collateral damage.

NotPetya also underscored the vulnerabilities in cyber-physical systems and critical infrastructure. The attack's ability to disrupt essential services such as power grids, transportation systems, and financial institutions highlighted the necessity of securing IT systems. The integration of cybersecurity measures with physical security protocols is crucial for protecting critical infrastructure from sophisticated cyber threats. This means that organizations must adopt a holistic approach to security that considers both digital and physical aspects of their operations.

In response to NotPetya, many organizations have significantly enhanced their security practices. Improvements have included more rigorous patch management, better network segmentation, and advanced intrusion detection and prevention systems. These measures are designed to limit the spread of malware and reduce the likelihood of similar attacks succeeding in the future. The attack's long-term impact is evident in the increased focus on preparedness and resilience, with organizations now more aware of the need for comprehensive incident response plans and regular security training.

The NotPetya attack has had a lasting impact on the field of cybersecurity. It has highlighted the urgent need for global cooperation, raised ethical concerns about cyber warfare, and demonstrated the vulnerabilities in critical infrastructure. The lessons learned from NotPetya continue to shape the way organizations and governments approach cybersecurity, driving advancements in technology and practices designed to protect against future threats. As the digital landscape evolves, the insights gained from NotPetya will remain critical in developing effective strategies to address and mitigate the risks of large-scale cyber attacks.

Bibliography

https://en.wikipedia.org/wiki/Petya_(malware_family)

https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

https://logrhythm.com/blog/notpetya-technical-analysis/

https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks

https://www.kaspersky.com/blog/notpetya-ransomware/15873/

https://msrc.microsoft.com/blog/2017/07/01/eternalblue-the-exploit-behind-the-wannacry-ransomware-attack/

https://www.symantec.com/security-center/writeup/2017-061213-1154-99

https://www.europol.europa.eu/activities-services/main-reports/notpetya-ransomware-attack-impact-and-response

https://www.cisa.gov/publications-library/lessons-learned-notpetya-attack

https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/