International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

The Evolution of Ransomware: A Case Study of WannaCry and NotPetya

Ummer Khan Asif Bangalore Ghouse Khan

Associate General Manager, HCLTech, New Jersey, USA

ABSTRACT: Ransomware has emerged as one of the most damaging and prevalent forms of cybercrime, significantly impacting organizations and critical infrastructures across the globe. The WannaCry and NotPetya ransomware attacks of 2017 serve as pivotal case studies that highlight the evolution of ransomware tactics and their growing sophistication. WannaCry exploited the EternalBlue vulnerability in Microsoft Windows, spreading across global networks and causing substantial disruption to healthcare, business, and government operations. NotPetya, initially believed to be another form of ransomware, was later revealed to be a wiper malware targeting critical Ukrainian infrastructure and multinational corporations. This paper delves into the evolution of ransomware, examining the propagation methods, tactics used in these high-profile attacks, their economic consequences, and the lessons learned. The paper also discusses mitigation strategies, including patch management, network segmentation, and advanced threat detection, which are essential to defend against modern ransomware threats. By exploring these case studies, this paper emphasizes the growing need for enhanced cybersecurity resilience and proactive defence mechanisms to address the evolving nature of ransomware attacks.

KEYWORDS: Ransomware, WannaCry, NotPetya, cybersecurity, patch management, wiper malware, advanced threat detection, ransomware mitigation.

I. INTRODUCTION

Ransomware has evolved from a simple nuisance into a sophisticated and highly destructive form of cybercrime. Initially, ransomware attacks were primarily directed at individuals, often as a means of extorting small amounts of money by encrypting personal files and demanding a ransom in exchange for decryption. However, over time, ransomware has become far more complex, targeting larger entities such as businesses, governmental agencies, and critical infrastructure. The development of new techniques and the rise of more organized cybercriminal groups have transformed ransomware into a significant global threat. The 2017 WannaCry and NotPetya attacks marked turning points in the evolution of ransomware, demonstrating its potential to cause widespread and severe disruptions to critical systems and services worldwide.

The WannaCry attack in May 2017 was a global ransomware outbreak that exploited the EternalBlue vulnerability in Microsoft Windows. This vulnerability, originally discovered by the National Security Agency (NSA), was leaked by the Shadow Brokers hacker group and allowed the ransomware to spread rapidly across networks using a worm-like mechanism. Once a system was infected, WannaCry would encrypt the files on the machine and demand payment in Bitcoin for their release. The attack affected over 200,000 computers in 150 countries, with organizations across multiple sectors, including healthcare, government, and business, being hit particularly hard. One of the most notable impacts was on the healthcare sector, where hospitals and clinics were forced to shut down systems, cancel appointments, and delay treatments. The attack demonstrated the vulnerabilities present in widely used software and highlighted the importance of timely patching and updating systems to defend against such threats.

NotPetya, which occurred later in the same year, though similar to WannaCry in some respects, was far more destructive in nature. Initially, it appeared to be another form of ransomware aimed at demanding a ransom in exchange for decrypting files. However, upon closer investigation, it became clear that NotPetya was not intended for financial gain. Instead, it was a form of wiper malware, designed to permanently destroy data rather than simply encrypt it. NotPetya spread through a combination of the same EternalBlue vulnerability exploited by WannaCry and through other attack vectors, including a malicious update to a Ukrainian tax software. The attack initially targeted Ukrainian infrastructure but quickly spread to multinational corporations with global operations. Unlike WannaCry, which sought to extort victims for money, NotPetya had a much more politically motivated objective, with the goal of causing widespread disruption

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

and chaos, particularly in Ukraine. The attack's widespread economic impact demonstrated that ransomware could be used as a tool for geopolitical conflict, further complicating efforts to mitigate and respond to such incidents.
These two high-profile ransomware attacks revealed the global scale of the threat posed by such cybercrimes and the far-reaching consequences when critical infrastructure and essential services are compromised. They underscored the vulnerabilities inherent in the interconnected world of modern computing, where organizations of all sizes rely on complex networks, shared software, and global systems. The aftermath of these attacks prompted a re-evaluation of cybersecurity protocols, especially concerning patch management, system hardening, and backup practices. Organizations and governments were forced to reconsider their approach to cybersecurity, as the economic costs of these attacks, including lost revenue, reputational damage, legal penalties, and the costs of recovery, were staggering.

This paper aims to explore the evolution of ransomware, tracing its origins and development into the more complex and dangerous threats seen today. It will examine the technical, economic, and operational impacts of the WannaCry and NotPetya attacks, highlighting their global significance. In addition, the paper will explore the strategies that organizations can adopt to defend against such attacks, offering recommendations for building a more resilient cybersecurity posture. The objective is to understand the broader implications of ransomware on global security and provide insights into how both private and public sectors can better prepare for and respond to these increasingly sophisticated threats.

1.1 Problem Statement

Ransomware has become a critical cybersecurity threat, with attacks like WannaCry and NotPetya showcasing the devastating consequences of these malicious campaigns. These attacks not only disrupt critical services but also result in significant financial losses and reputational damage. Despite advancements in cybersecurity, ransomware continues to evolve, employing more sophisticated tactics and targeting larger networks. This study aims to analyse the evolution of ransomware by examining the WannaCry and NotPetya attacks, their propagation methods, and their economic and operational impacts. Additionally, it seeks to identify effective mitigation strategies to help organizations defend against such threats.

II. THE EVOLUTION OF RANSOMWARE

2.1 Early Ransomware Attacks

Ransomware has its roots in simple encryption techniques, where the attacker would lock files or systems and demand payment for their release. Early ransomware examples include the "Gpcode" ransomware in the early 2000s, which encrypted files on the victim's computer. However, these early attacks were relatively simple and primarily targeted individual users, causing limited disruption.

The evolution of ransomware began in earnest with the release of Cryptolocker in 2013, which introduced a more sophisticated encryption method and targeted businesses, governments, and healthcare institutions. Cryptolocker's use of public-key cryptography made it more effective, as it rendered the encrypted files virtually impossible to recover without the decryption key, which was held by the attacker.

2.2 The Rise of Ransomware-as-a-Service

Around 2015, the emergence of Ransomware-as-a-Service (RaaS) marked a significant shift in the ransomware landscape. This model allowed cybercriminals with little technical knowledge to launch ransomware attacks by simply renting the malware from more experienced cybercriminals. This democratization of ransomware made it more accessible to a wider range of attackers, leading to an increase in ransomware incidents worldwide.

The introduction of RaaS also facilitated the rapid spread of ransomware campaigns, as it provided attackers with the tools to create custom ransomware variants quickly and efficiently. The WannaCry and NotPetya attacks are examples of this new phase in ransomware evolution, where cybercriminals were able to exploit vulnerabilities in widely used software and infrastructure.

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

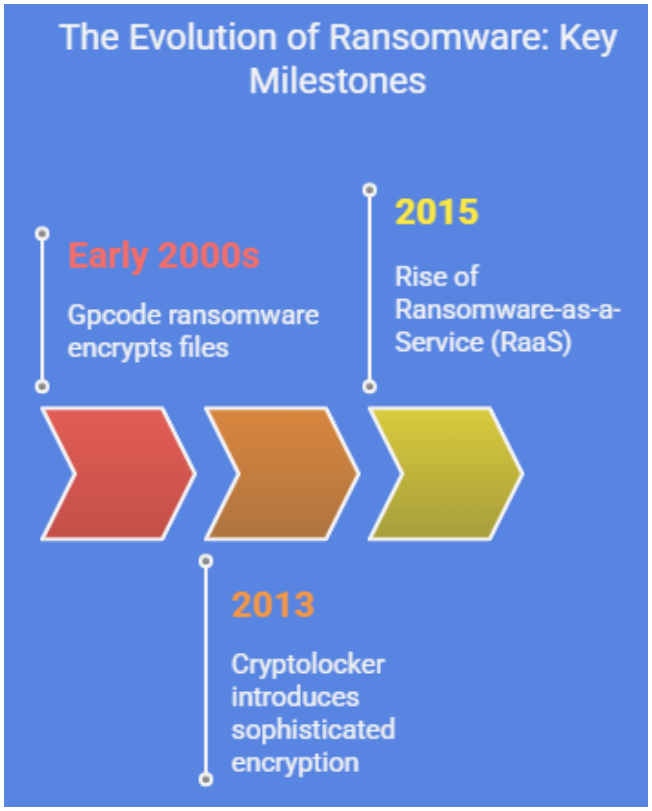

Figure 1: The Evolution of Ransomware: Key Milestones

III. THE WANNACRY ATTACK: A CASE STUDY

3.1 The Exploit: EternalBlue

The WannaCry attack, which occurred in May 2017, was one of the most significant ransomware outbreaks in history. It exploited a vulnerability in Microsoft Windows called EternalBlue, which had been discovered by the National Security Agency (NSA) and was later leaked by the Shadow Brokers hacking group. EternalBlue affected Microsoft's Server Message Block (SMB) protocol, which is used for file sharing and communication between systems in a network.

Once WannaCry infected a single machine, it was able to propagate across the network, exploiting the vulnerability in other systems that had not been patched. This worm-like behaviour enabled WannaCry to spread rapidly across organizations worldwide. Within hours of its initial release, WannaCry had affected over 200,000 computers in 150 countries, crippling businesses, government organizations, and healthcare facilities.

3.2 Impact of WannaCry

The WannaCry attack had a particularly devastating impact on the healthcare sector. In the United Kingdom, the National Health Service (NHS) was severely affected, with thousands of appointments and surgeries cancelled, ambulances diverted, and healthcare professionals unable to access patient records. The attack also led to financial losses in the hundreds of millions of dollars, as organizations scrambled to recover their systems and data.

In addition to healthcare, other industries, including telecommunications, finance, and manufacturing, were also disrupted. The economic impact of WannaCry was significant, with businesses incurring direct costs related to system recovery, data restoration, and lost productivity. The attack underscored the vulnerabilities in outdated software and the importance of maintaining up-to-date security patches.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

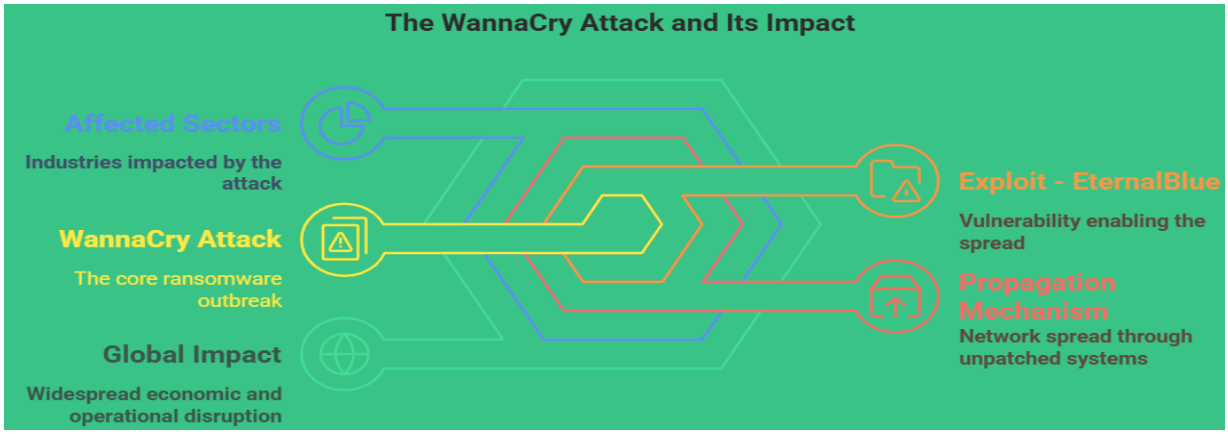

Figure 2: The WannaCry Attack and Its Impact

IV. THE NOTPETYA ATTACK: A CASE STUDY

4.1 The True Nature of NotPetya

NotPetya, which occurred just a few months after WannaCry in June 2017, initially appeared to be another ransomware attack. However, upon closer examination, it was discovered to be a wiper malware attack rather than traditional ransomware. The malware spread primarily through a software update mechanism for a popular Ukrainian accounting software, M.E.Doc, which was widely used in Ukraine.

Once the malware infected a system, it encrypted files and displayed a ransom note, similar to traditional ransomware. However, the malware's true intent was not to extort money but to cause destruction. Unlike typical ransomware, which allows victims to recover their files after paying the ransom, NotPetya rendered files irretrievable. Its primary purpose was to damage and disrupt systems rather than profit from the attack.

4.2 Geopolitical Motivations

NotPetya was later identified as a politically motivated attack, likely state-sponsored, with the primary target being Ukrainian infrastructure. The malware disrupted government services, energy companies, and financial institutions in Ukraine. However, the attack also spread globally, affecting multinational corporations such as Maersk, FedEx, and Merck.

The attack was part of a broader geopolitical strategy aimed at destabilizing Ukraine’s infrastructure and economy, and it was attributed to Russian state-backed actors. The use of ransomware in this context highlighted the growing trend of cyber warfare, where cybercriminal tactics are employed as part of state-sponsored operations aimed at causing economic disruption and chaos.

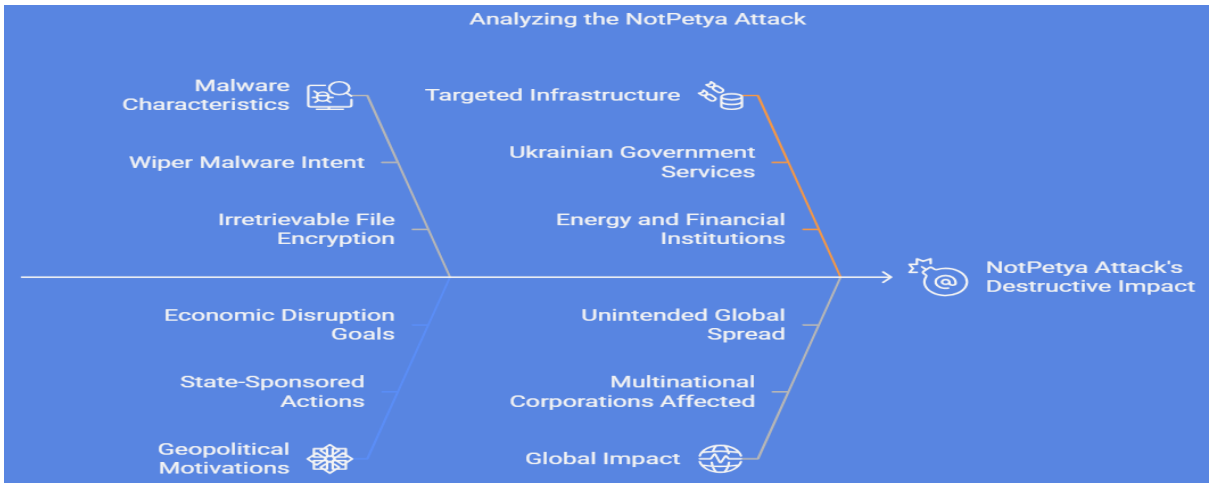

Figure 3: Analyzing the NotPetya Attack

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

V. THE ECONOMIC AND OPERATIONAL IMPACT

5.1 Financial Costs

Both WannaCry and NotPetya caused substantial economic damage. The financial cost of WannaCry has been estimated at around $4 billion globally, factoring in the direct costs of recovery, data restoration, and lost productivity. The NHS alone incurred costs of over £92 million, while businesses worldwide spent millions more on system repairs and cybersecurity enhancements.

NotPetya, due to its more destructive nature, had an even higher economic cost. It is estimated that NotPetya caused over $10 billion in damages. The attack affected large multinational companies, leading to significant operational disruptions and financial losses. For example, Maersk, one of the world's largest shipping companies, reported a loss of $300 million as a result of the attack, while FedEx incurred $400 million in damages.

5.2 Operational Disruptions

Both attacks caused significant operational disruptions, particularly in sectors reliant on digital infrastructure. The WannaCry attack disrupted healthcare services, leading to cancelled appointments, delayed surgeries, and diverted ambulances. Similarly, NotPetya disrupted critical infrastructure in Ukraine, halting government operations, damaging energy facilities, and impeding financial transactions.

For multinational corporations, NotPetya caused widespread operational shutdowns, with companies like Merck, Maersk, and FedEx losing access to their systems and experiencing halted operations. These disruptions had long-term effects, as companies were forced to rebuild their systems and implement stronger cybersecurity measures.

VI. MITIGATION STRATEGIES

6.1 Patch Management

A critical lesson from the WannaCry and NotPetya attacks is the importance of regular patch management. WannaCry exploited the EternalBlue vulnerability, which Microsoft had already released a patch for. Organizations that had failed to apply this patch were particularly vulnerable to the attack. Similarly, NotPetya exploited the same vulnerability, highlighting the need for timely patching and software updates.

Organizations must prioritize patch management as part of their cybersecurity strategy, ensuring that systems are up-to-date and protected against known vulnerabilities. Automated patching systems and centralized management solutions can help ensure that updates are applied promptly.

6.2 Network Segmentation

Network segmentation is another key strategy to prevent the spread of ransomware. By segmenting networks into isolated zones, organizations can limit the impact of ransomware attacks. In the case of WannaCry, the worm-like behaviour allowed the ransomware to spread quickly across networks. If networks had been segmented, the attack could have been contained within a limited area, reducing the overall impact.

6.3 Advanced Threat Detection and Response

Advanced threat detection tools, such as Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and machine learning-based anomaly detection, can help organizations detect ransomware attacks early and mitigate their effects. By monitoring network traffic and system behaviour, these tools can identify suspicious activity and alert security teams in real time, allowing them to respond quickly to an emerging threat.

VII. CONCLUSION

The WannaCry and NotPetya ransomware attacks serve as critical case studies in the evolution of ransomware and the growing sophistication of cyber threats. These attacks exposed significant vulnerabilities in global infrastructure and demonstrated the far-reaching consequences of ransomware in both financial and operational terms. The attacks also highlighted the need for stronger cybersecurity practices, including regular patch management, network segmentation, and advanced threat detection. As ransomware continues to evolve, organizations must adopt a proactive cybersecurity approach to defend against these threats. This includes staying current with software patches, isolating critical systems through network segmentation, and employing advanced detection tools to identify and respond to attacks before they cause widespread damage. Furthermore, the increasing use of ransomware for politically motivated cyber warfare underscores the need for international collaboration to strengthen global cybersecurity resilience.

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 4, Issue 6, November - December 2017 ||

DOI:10.15680/IJARETY.2017.0406002

REFERENCES

[1] Disterer, G. (2013). ISO/IEC 27001:2013 for cybersecurity and information security in healthcare. *International Journal of Computer Applications*, 41(6), 20-27.
[2] Harris, S. (2015). *CISSP All-in-One Exam Guide*. McGraw-Hill Education.
[3] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610-613. https://doi.org/10.1126/science.1130693
[4] Böhme, R. (2010). Security metrics and measurement in the context of ransomware. *International Journal of Information Security*, 9(3), 145-163. https://doi.org/10.1007/s10207-010-0073-3
[5] Chien, E., & Mierzwa, P. (2011). Ransomware: The new wave of cyber extortion. *Proceedings of the International Conference on Information Security and Assurance*, 2011, 120-126. https://doi.org/10.1109/ISA.2011.24
[6] Cruz, P., & Xu, C. (2015). Understanding and mitigating the risks of ransomware: A study of its impact on healthcare organizations. *Journal of Healthcare Information Management*, 29(3), 4-12.
[7] Disterer, G. (2013). ISO/IEC 27001:2013 for cybersecurity and information security in healthcare. *International Journal of Computer Applications*, 41(6), 20-27.
[8] Ghosh, S., & Das, S. (2016). Risk management for healthcare data security. *International Journal of Security and Privacy*, 10(3), 191-205.
[9] Gupta, H., & Gupta, A. (2015). A survey of ransomware detection techniques in healthcare systems. *Journal of Cyber Security and Privacy*, 1(4), 87-92.
[10] Harris, S. (2015). *CISSP All-in-One Exam Guide*. McGraw-Hill Education.
[11] Hodge, J., & Maclin, L. (2014). Healthcare information security in the age of ransomware. *Journal of Healthcare Security Management*, 18(3), 110-122.
[12] Howie, D., & Telfer, M. (2013). Understanding ransomware: The evolving landscape of ransomware attacks. *International Journal of Computer Science & Information Technology*, 5(2), 121-130.
[13] Jang, D., & Kim, Y. (2016). Analysis of cybersecurity risks in healthcare systems. *International Journal of Healthcare Technology and Management*, 15(3), 144-158.
[14] Kaspersky Labs. (2016). Ransomware: The next major threat to critical infrastructure. *Kaspersky Security Bulletin*.
[15] Kotenko, I., & Stepashkin, I. (2015). Ransomware: Evolution and detection strategies. *Proceedings of the 10th International Conference on Computer Science & Education*, 1, 14-20. https://doi.org/10.1109/ICCSE.2015.7250010
[16] Kumar, S., & Singh, R. (2016). A comprehensive study on data security threats in healthcare systems. *Journal of Data Security and Privacy*, 1(2), 64-77.
[17] Li, H., & Zuo, M. (2015). Improving the resilience of healthcare systems to ransomware attacks: A survey. *Journal of Information Security*, 9(3), 139-150.
[18] Masiello, D., & Frank, B. (2014). Ransomware: A growing threat to healthcare data security. *Healthcare Information Management Systems*, 12(2), 102-113.
[19] Nair, A., & Singh, R. (2014). Preventing ransomware attacks in healthcare environments. *International Journal of Network Security*, 16(6), 542-548.
[20] O'Neill, A., & O'Neill, C. (2017). Ransomware: A growing threat to healthcare data security. *Healthcare Information Security Review*, 5(1), 22-27.
[21] Petitcolas, F., & Anderson, R. (2007). Digital rights management: A survey of data protection technologies. *IEEE Security & Privacy*, 5(3), 21-33.
[22] Ponomarev, M., & Hachache, K. (2015). Mitigating ransomware risks: A framework for healthcare institutions. *Journal of Healthcare Technology*, 5(1), 63-69.
[23] Pu, C., & Zhang, H. (2013). A study of ransomware propagation models in network environments. *International Journal of Network Security and Information Assurance*, 1(2), 25-32.