International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Case Study of the WannaCry Ransomware Attack and its Global Impact

Khushboo Roy, Om Shende

G H Raisoni University, Amravati, Maharashtra, India

Abstract

The rapid growth of digital technologies and networked systems has significantly increased the risk of cyber threats worldwide. Among these threats, ransomware has emerged as one of the most dangerous forms of malware due to its ability to encrypt user data and demand payment for its recovery. One of the most notable ransomware incidents in recent history is the global outbreak of WannaCry, which occurred in May 2017. The WannaCry attack spread rapidly across computer networks by exploiting a vulnerability in the Server Message Block (SMB) protocol of Microsoft Windows operating systems. This vulnerability was exploited using the EteralBlue exploit, which allowed the malware to propagate automatically between vulnerable systems without requiring user interaction. As a result, the attack infected more than 200,000 computers across over 150 countries within a short period of time, making it one of the largest and most disruptive cyberattacks in history.

The objective of this research paper is to analyse the WannaCry ransomware attack from a technical, operational, and cybersecurity perspective. The study focuses on understanding the architecture and behaviour of the malware, the vulnerability exploited during the attack, the propagation mechanism used to spread across networks, and the overall impact on global digital infrastructure. The attack particularly affected critical sectors such as healthcare, banking, transportation, and telecommunications. One of the most widely reported incidents occurred in the United Kingdom where several hospitals operated by the National Health Service were forced to cancel appointments and medical procedures due to system failures caused by the ransomware infection. This incident highlighted the vulnerability of essential services to cyber threats and emphasized the importance of strong cybersecurity measures.

The research methodology adopted in this study is based on a qualitative case study approach using secondary data collected from reliable sources such as security advisories issued by Microsoft, reports published by the National Cyber Security Centre, government cybersecurity alerts, academic journals, and technical research publications. These sources were analysed to understand the technical working of the ransomware, the timeline of the attack, and the strategies used by cybersecurity experts to contain the outbreak. The analysis also examines the discovery of the so-called "kill-switch" domain by a security researcher, which helped slow down the spread of the malware.

In conclusion, the WannaCry ransomware attack serves as a critical case study for understanding modern cyber warfare and digital vulnerabilities. The lessons learned from this incident emphasize the importance of proactive cybersecurity measures, continuous monitoring of network systems, and rapid response mechanisms to mitigate potential cyber threats. By examining the technical structure and global impact of the WannaCry attack, this research aims to contribute to a better understanding of ransomware behaviour and to support the development of stronger cybersecurity frameworks for the protection of digital infrastructure.

KEYWORDS*: WannaCry Ransomware, Cybersecurity, Malware Attack, EternalBlue Exploit, Data Encryption, Network Security, Microsoft Windows, Cyber Threats, Information Security, SMB Vulnerability.*

1. Introduction

The rapid growth of information technology and internet connectivity has significantly improved communication, business operations, and digital services worldwide. However, this rapid digital transformation has also increased the risk of cyber threats and malicious attacks. Among the various types of cyber threats, ransomware has become one of the most dangerous and disruptive forms of malware. Ransomware is a type of malicious software designed to block access to a computer system or encrypt files until a ransom is paid to the attacker. These attacks often target individuals, organizations, and government institutions, causing severe financial and operational damage [3].

One of the most significant ransomware incidents in cybersecurity history is the outbreak of WannaCry that occurred in May 2017. This cyberattack spread rapidly across computer networks worldwide by exploiting a vulnerability in the Windows operating system developed by Microsoft. The vulnerability existed in the Server Message Block (SMB) protocol and was exploited using a tool known as EternalBlue. Microsoft had previously released a security patch (MS17-010) to fix this vulnerability; however, many organizations failed to update their systems, leaving them exposed to the attack [1].

Once a computer system became infected, the malware automatically scanned other vulnerable systems within the same network and infected them without requiring user interaction. This worm-like behaviour enabled the ransomware to spread rapidly across connected systems and networks. According to cybersecurity reports, the attack infected more than 200,000 computers across over 150 countries within a very short period of time [2].

The WannaCry incident demonstrated how vulnerable modern digital infrastructures can be when security updates and patch management are not properly implemented. It also highlighted the importance of strong cybersecurity practices such as regular software updates, network monitoring, data backup strategies, and employee awareness

programs [4], [5]. Understanding the causes, technical mechanisms, and consequences of the WannaCry attack is essential for developing stronger cybersecurity defences and preventing similar ransomware attacks in the future.

Fig. 1. WannaCry ransomware message displayed on infected computer systems demanding Bitcoin payment.

2. Literature Review

The increasing dependence on digital infrastructure has led to a rapid rise in cyber threats, among which ransomware attacks have become a major concern for organizations and governments worldwide. Several researchers and cybersecurity institutions have studied ransomware attacks to understand their evolution, technical mechanisms, and impact on global infrastructure. The ransomware attack caused by WannaCry has been widely analysed in cybersecurity literature because of its rapid propagation and global disruption.

2.1. Ransomware and Its Evolution

Ransomware is a form of malicious software designed to restrict access to a computer system or encrypt important files until a ransom payment is made by the victim. Early ransomware attacks primarily relied on user interaction, such as opening malicious email attachments or clicking infected links. These attacks typically spread through phishing campaigns or compromised websites [3]. Over time, ransomware techniques evolved and became more sophisticated, incorporating advanced encryption algorithms and automated propagation mechanisms. The WannaCry ransomware represented a major shift in ransomware evolution by introducing worm-like capabilities that allowed it to automatically spread across networks without requiring user interaction. This automated propagation significantly increased the speed and scale of infection compared to traditional ransomware attacks.

2.2. Vulnerability Exploitation

Several studies indicate that the success of the WannaCry attack was largely due to the exploitation of a vulnerability in the Server Message Block (SMB) protocol used in Microsoft Windows operating systems. The attack utilized the EternalBlue exploit, which targeted unpatched systems and allowed attackers to execute malicious code remotely [1]. The vulnerability had been previously identified and a security update was released by Microsoft; however, many organizations had not installed the update at the time of the attack. Research findings suggest that delayed patch management and outdated systems significantly increased the vulnerability of computer networks to ransomware infections.

2.3. Impact on Global Infrastructure

The WannaCry attack caused significant disruption to global digital infrastructure, affecting multiple sectors such as healthcare, banking, telecommunications, and transportation. One of the most severely affected organizations was the National Health Service (NHS) in the United Kingdom, where hospital computer systems became inaccessible due to encrypted files. This resulted in cancelled surgeries, delayed medical treatments, and disruptions to emergency healthcare services [2]. Cybersecurity studies emphasize that inadequate cybersecurity practices, including weak network security policies and lack of regular software updates, played a major role in the widespread impact of the attack. [4] [5]

3. Research Methodology

This research adopts a qualitative case study approach to analyse the global ransomware attack caused by WannaCry. The case study method is particularly useful for examining real-world cybersecurity incidents because it allows researchers to analyse technical behaviour, causes, and consequences of cyberattacks in detail. The WannaCry attack represents one of the most significant ransomware outbreaks in modern cybersecurity history, affecting thousands of organizations and critical infrastructures across the world. Therefore, studying this attack helps in understanding how vulnerabilities in computer systems can be exploited and how cybersecurity defences can be improved to prevent similar incidents in the future.

The research methodology focuses on collecting and analysing information from reliable and credible secondary data sources. Since the WannaCry attack has been widely documented by cybersecurity researchers, government organizations, and technology companies, the study relies primarily on previously published data and technical reports. These sources provide

detailed insights into the attack timeline, malware behaviour, vulnerabilities exploited, and the response measures taken by organizations after the incident.

3.1. Data Collection

The data for this research was collected from several credible sources to ensure the accuracy and reliability of the information used in the study. Multiple sources were examined to obtain comprehensive technical and analytical insights into the ransomware attack.

Cybersecurity Reports: Technical reports published by cybersecurity organizations provided detailed information about the structure, behaviour, and propagation of the WannaCry malware. These reports helped explain how the ransomware spreads across networks and how it encrypts files on infected systems.

Government Security Advisories: Security alerts and threat intelligence reports issued by national cybersecurity agencies were reviewed to understand the timeline of the attack, the affected sectors, and the mitigation strategies recommended by cybersecurity authorities.

Academic Journals and Research Publications: Peer-reviewed academic research papers were studied to analyse ransomware evolution, malware propagation techniques, and the broader cybersecurity implications of the WannaCry attack.

Security Updates from Microsoft: Official security bulletins and vulnerability patches released by Microsoft were examined to understand the Server Message Block (SMB) protocol vulnerability that was exploited by the attackers. These updates also provided information regarding the security patch MS17-010 which was designed to fix the vulnerability.

Online Cybersecurity Databases: Various cybersecurity platforms and digital research repositories were used to gather information related to the number of infected systems, global distribution of the attack, and incident response actions taken by organizations worldwide.

Collecting data from these diverse sources helped provide a comprehensive and reliable foundation for analysing the WannaCry ransomware attack.

3.2. Data Analysis

After the required data was collected, the information was carefully analysed to understand the behaviour and impact of the ransomware attack. The analysis focused on examining the technical functioning of the malware, the vulnerabilities exploited, the scale of damage caused by the attack, and the response measures taken by affected organizations and cybersecurity agencies.

Technical Working of WannaCry

The study analysed how the ransomware infects systems, installs malicious code, and spreads automatically across vulnerable networks. Unlike earlier ransomware attacks that required user interaction, WannaCry incorporated worm-like capabilities that allowed it to propagate without human involvement.

Identification of Vulnerabilities

Special attention was given to examining the vulnerability in the Server Message Block (SMB) protocol of Windows operating systems. Attackers used the EternalBlue exploit to gain unauthorized access to vulnerable systems and execute malicious code remotely.

Assessment of Global Damage

The research analysed the overall scale of the attack, including the number of infected computers, the countries affected, and the sectors that experienced disruptions. Healthcare, banking, transportation, and telecommunications sectors were among the most severely impacted.

Evaluation of Organizational Response

The study also examined how governments, cybersecurity organizations, and technology companies responded to the attack by releasing security patches, issuing threat advisories, and implementing emergency response strategies.

3.3. Working Mechanism of WannaCry

1) Understanding the working mechanism

Ransomware is essential for analysing how the attack spread so rapidly across global networks. The WannaCry malware followed a structured process that allowed it to infect systems, propagate across networks, encrypt files, and demand ransom payments from victims.

2) Exploitation of SMB Vulnerability:

The attack began by exploiting a vulnerability in the Server Message Block (SMB) protocol used in Windows operating systems. Attackers used the EternalBlue exploit to gain access to vulnerable systems and execute malicious code remotely.

3) Self-Propagation Across Networks:

Once a system was infected, the ransomware scanned the local network to identify other vulnerable systems. Using the same SMB exploit, it automatically spread to those systems without requiring user interaction.

4) File Encryption Process:

After successfully gaining control of the infected computer, the malware began encrypting various types of files stored on the system. These included documents, images, databases, and other important data. Strong encryption algorithms were used to prevent victims from accessing their files.

5) Ransom Demand:

Once the encryption process was completed, the ransomware displayed a message informing victims that their files had been locked. The message demanded a ransom payment ranging from approximately 300 to 600 US dollars in Bitcoin cryptocurrency in exchange for a decryption key.

6) Kill Switch Discovery:

An interesting feature of the WannaCry malware was the presence of a hidden "kill switch" domain embedded within its code. A cybersecurity researcher discovered this domain while analysing the malware behaviour. After registering the domain, the spread of the ransomware slowed significantly, helping limit further infections.

7) Communication with Command and Control Server:

After infecting the system, the WannaCry malware attempts to communicate with external servers known as Command and Control (C2) servers. These servers are controlled by the attackers and are used to manage the ransomware operation. Through this communication, the malware can verify infection status, manage ransom payment information, and sometimes download additional malicious components. This connection also helps attackers monitor the number of infected systems and coordinate their ransomware campaign. However, in the case of WannaCry, the presence of the kill switch domain limited the communication process and helped slow down the global spread of the attack.

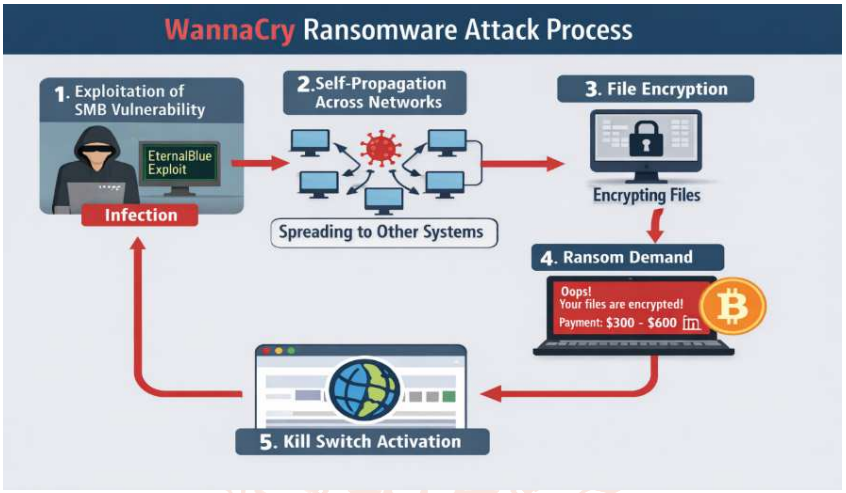

Fig. 2. WannaCry ransomware propagation and attack flow across vulnerable computer networks

4. Result

The analysis of the WannaCry incident shows that the attack spread rapidly due to unpatched vulnerabilities in the Windows operating system. The ransomware exploited a weakness in the Server Message Block (SMB) protocol, allowing attackers to gain remote access to vulnerable computers. Although a security patch had been released earlier by Microsoft, many organizations had not updated their systems, which made them highly vulnerable to the attack.

The study also found that the worm-like propagation capability of WannaCry allowed it to spread automatically across networks without user interaction. Within a short period of time, the ransomware infected more than 200,000 computers in over 150 countries. Several sectors such as healthcare, banking, telecommunications, and government organizations were severely affected by the attack.

One of the most significant impacts was observed in healthcare institutions where important systems became inaccessible due to file encryption. Hospitals experienced service disruptions, and several appointments and medical procedures had to be cancelled. This demonstrated the serious consequences that cyberattacks can have on essential public services.

The research also highlights the importance of timely software updates and proper cybersecurity practices. Organizations that had installed the necessary security patches were largely protected from the attack. The discovery of a "kill switch" domain by a cybersecurity researcher helped slow down the spread of the ransomware and reduced further infections.

Overall, the results indicate that the WannaCry attack exposed major weaknesses in global cybersecurity infrastructure and emphasized the need for better vulnerability management, regular system updates, and improved network security measures.

The impact of the WannaCry attack was severe:

1) Over 200,000 computers infected

2) Spread across 150+ countries

3) Estimated billions of dollars in losses

4) Healthcare, banking, and telecom sectors affected

The attack exposed major weaknesses in global cybersecurity infrastructure. Organizations relying on outdated systems were the most vulnerable.

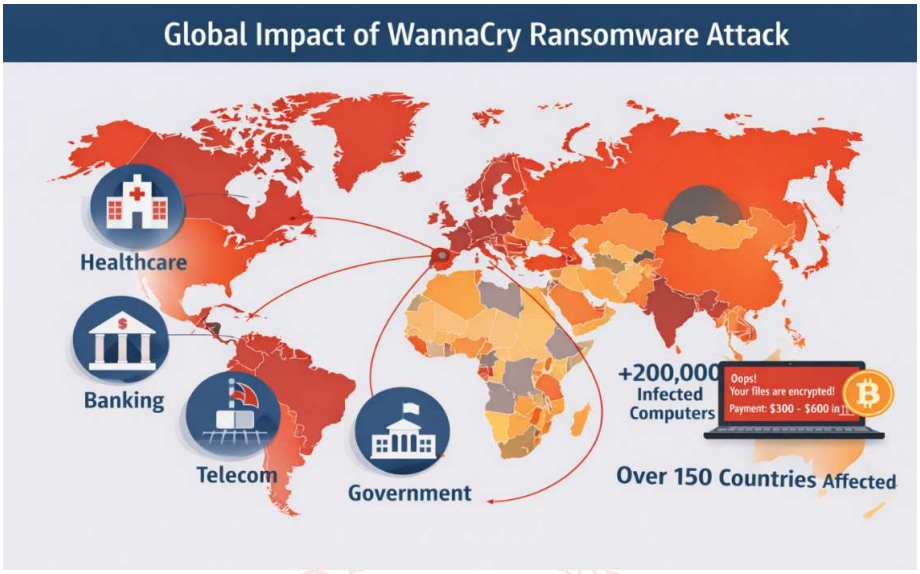

Fig. 3. Global spread and impact of WannaCry ransomware attack across different sectors and countries.

5. Conclusion

The WannaCry ransomware attack remains one of the most significant cybersecurity incidents in modern history. The attack demonstrated how a single unpatched vulnerability in widely used software systems could lead to large-scale disruptions across global digital infrastructure. Within a very short period of time, thousands of organizations and critical sectors such as healthcare, telecommunications, banking, and government services were affected, highlighting the growing risks associated with cyber threats in an increasingly interconnected world.

The analysis of this case study emphasizes the importance of proactive cybersecurity practices. Organizations must ensure that software vulnerabilities are identified and patched promptly to reduce the risk of exploitation by attackers. Regular system updates, continuous network monitoring, and the implementation of strong security policies play a crucial role in protecting digital systems from ransomware attacks. The incident also highlights the need for employee awareness and training programs, as human negligence and delayed updates often contribute to security breaches.

Furthermore, collaboration between technology companies, cybersecurity researchers, and government agencies is essential for effectively responding to large-scale cyber incidents. Security updates and emergency advisories released by organizations such as Microsoft helped reduce the impact of the attack and prevent further infections.

In conclusion, the WannaCry ransomware attack serves as an important lesson for organizations and cybersecurity professionals worldwide. It clearly demonstrates that maintaining strong cybersecurity frameworks, performing regular vulnerability assessments, and implementing effective risk management strategies steps in preventing similar cyberattacks in the future.

References

[1] Microsoft, *"Microsoft Security Bulletin MS17-010: Security Update for Microsoft Windows SMB Server,"* Mar. 2017.Available: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[2] National Health Service (NHS), *"WannaCry Ransomware Cyber Attack Analysis Report,"* 2017.Available: https://digital.nhs.uk/cyber-alerts/2017/cc-1411

[3] US-CERT, *"Indicators Associated with WannaCry Ransomware,"* Technical Alert TA17-132A, 2017.Available:https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

[4] National Cyber Security Centre, *"Global Ransomware Attack Guidance,"* NCSC Report, 2017.Available: https://www.ncsc.gov.uk/guidance/ransomware

[5] Europol, *"WannaCry Ransomware Attack – Global Cybercrime Report,"* European Cybercrime Centre, 2017.Available: https://www.europol.europa.eu

[6] Kaspersky Lab, *"WannaCry Ransomware Used in Worldwide Attacks,"* Security Analysis Report, 2017.Available: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351

[7] Cisco Talos Intelligence Group, *"WannaCry Malware Profile,"* Cisco Security Intelligence Report, 2017.Available: https://blog.talosintelligence.com/2017/05/wannacry.html

[8] Symantec Corporation, *"Internet Security Threat Report: WannaCry Ransomware,"* Symantec Security Response, 2017.Available: https://www.symantec.com/security-center

[9] Q. Chen and R. A. Bridges, *"Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware,"* arXiv, 2017.Available: https://arxiv.org/abs/1709.08753

[10] F. Quinkert, T. Holz, K. Hossain, and E. Ferrara, *"RAPTOR: Ransomware Attack Prediction,"* arXiv, 2018.Available: https://arxiv.org/abs/1803.01598

[11] SANS Institute, *"WannaCry Ransomware Technical Analysis and Prevention Methods,"* SANS Cyber Threat Report, 2017.Available: https://www.sans.org/white-papers

[12] CERT-EU, *"WannaCry Ransomware Campaign Exploiting SMB Vulnerability,"* Security Advisory 2017-012.Available: https://cert.europa.eu/publications/security-advisories/2017-012

[13] Canadian Centre for Cyber Security, *"Microsoft Security Updates MS17-010,"* Cyber Security Alert AV17-068.Available: https://www.cyber.gc.ca/en/alerts/microsoft-security-updates-ms17-010-smbv1

[14] IBM Security, *"WannaCry Ransomware Attack Analysis,"* IBM X-Force Threat Intelligence Report, 2017.Available: https://www.ibm.com/security

[15] Trend Micro Research, *"WannaCry Ransomware: Technical Overview and Global Impact,"* 2017.Available: https://www.trendmicro.com/en_us/research.html

International Journal of Trend in Scientific Research and Development
IJTSRD
International Journal of Trend in Scientific Research and Development
ISSN: 2456-6470