IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Case Study on WannaCry Ransomware: Technical Analysis, Global Impact, and Lessons for Future Cyber Defence

Poornima Rai
Assistant Professor, Department of Information Technology,
Sikkim Skill University, Sikkim.
raipoornima641@gmail.com

Abstract: *WannaCry, a ransomware attack that occurred in May 2017, became one of the most notorious cyber incidents in recent history. This review paper analyses the technical aspects of the WannaCry ransomware, its impact on global systems, and the lessons learned in its wake. By exploiting vulnerability in Microsoft Windows' Server Message Block (SMB) protocol, WannaCry was able to propagate rapidly across networks, encrypting data and demanding ransom in Bitcoin. This paper delves into the mechanisms of the attack, it's devastating global consequences, particularly on sectors like healthcare and telecommunications, and evaluates the existing defence measures. The paper concludes with recommendations for enhancing cyber security measures and preventing future ransomware attacks.*

Keywords: WannaCry, ransomware, cyber security, patch management, cyber defence, global impact, vulnerabilities..

I. INTRODUCTION

Ransomware has emerged as one of the most critical cybersecurity threats in recent years, with WannaCry being one of the most infamous examples of its devastating capabilities. WannaCry refers to a broader family of ransomware variants, including all named forms such as WannaCrypt, WCry, WanaCrypt, and WanaCrypt0r [1].The WannaCry ransomware attack, which occurred in May 2017, spread rapidly across the globe, affecting more than 230,000 computers in over 150 countries [2]. Targeting vulnerabilities in Microsoft Windows, the attack encrypted vital data, rendering systems unusable and demanding a ransom in Bitcoin for decryption keys. This attack crippled critical sectors, especially healthcare, causing significant disruptions in services and leading to widespread financial losses.The WannaCry attack exploited a known vulnerability, highlighting significant flaws in cyber security protocols and patch management. While the global response to the attack led to swift recovery in some areas, the incident exposed the vulnerabilities in both individual systems and organizational defence strategies. This paper aims to provide a comprehensive analysis of the WannaCry ransomware, exploring its technical mechanisms, global impact, and the lessons learned for strengthening future cyber defences systems.

II. LITERATURE REVIEW

The WannaCry ransomware attack in May 2017 has been widely studied because of how quickly it spread, how it worked, and the damage it caused around the world. Many researchers have looked into the technical side of the attack, how it spread across systems, its impact on different industries, and the lessons it taught the cyber security world.

1. How WannaCry Worked and Spread

WannaCry used a weakness in Microsoft Windows called **EternalBlue** to spread. This weakness was in a part of Windows known as **SMBv1 (Server Message Block)**. The exploit, named EternalBlue, was originally found by the **U.S. National Security Agency (NSA)** but was later leaked by a hacker group called **Shadow Brokers** [3]. This

DOI: 10.48175/IJARSCT-26806

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

allowed WannaCry to install itself on computers without users needing to click anything, which made it very dangerous [1][2].

Researchers like **Chen and Bridges** [11] studied how WannaCry behaves once inside a computer. They found that the ransomware looks for specific patterns, changes system settings, and locks up important files. Another study by **Kao** [12] showed how WannaCry keeps itself active in the system and how it encrypts files using advanced methods.

2. How It Spread and How It Was Stopped

One of the things that made WannaCry so dangerous was that it could move from one computer to another without human help. It scanned networks and found other machines that had not been updated or patched, and then it infected them [2][4].The spread was finally slowed down when a cyber security expert, **Marcus Hutchins**, found a hidden "**kill switch**" in the WannaCry code. This was a web address that the malware tried to contact. Once Hutchins registered that domain, it stopped the malware from continuing to spread [5]. This unexpected discovery helped reduce the damage, even though many systems had already been affected.

3. Impact on Healthcare and Other Sectors

WannaCry caused problems in many industries, but the **healthcare sector** was hit the hardest. In the **UK**, the **National Health Service (NHS)** had to cancel surgeries and appointments because their systems were locked. Some hospitals even had to turn away emergency patients [6]. This showed how old and outdated systems in hospitals were easy targets for cyber attacks.Other industries like **transportation**, **telecommunications**, and **shipping** were also affected. Companies like **FedEx** and **Telefonica** reported big issues in their operations [3][10]. These problems happened mainly because they had not updated their systems in time.

4. Lessons from WannaCry

Many researchers agree that the attack could have been prevented if organizations had updated their systems earlier. Microsoft had released a patch (update) to fix the problem two months before the attack (March 2017), but many companies didn't apply it [8][9].Traditional security tools like antivirus programs and firewalls didn't work well against WannaCry because it didn't behave like normal viruses. It spread too fast and didn't need users to click on anything [7]. As a result, researchers such as **Jones** [1] and **Akbanov** [2][3] suggest using smarter tools like **behavior-based detection systems** that watch for unusual activity, not just known threats.

5. Importance of Backup, Training, and Cooperation

Studies also highlight the importance of **data backups**. Organizations that had regular backups were able to recover quickly. Those without backups had to choose between paying the ransom or losing their data.Training employees about **cyber security**, especially about not clicking on suspicious links or opening unknown attachments, is also important. Even though WannaCry didn't rely on people clicking anything, many other types of ransomware do [10].

Finally, sharing information between companies, governments, and cyber security experts helped control the damage. Groups like **Europol** and **INTERPOL** worked together to investigate the attack and reduce further harm [5].

III. TECHNICAL ANALYSIS OF WANNACRY

WannaCry is a type of ransomware that targets computers running Microsoft Windows, specifically exploiting vulnerability in the Server Message Block (SM B) protocol. The attack was made possible by the exploitation of a flaw in Windows systems, identified as EternalBlue [1], which was initially discovered by the United States National Security Agency (NSA) but was leaked by the hacker group Shadow Brokers in April 2017 [3]. The vulnerability allowed WannaCry to propagate across networks without requiring user interaction, making it particularly dangerous.

IV. EXPLOITATION OF THE SMB VULNERABILITY

The EternalBlue vulnerability (CVE-2017-0144) allows attackers to send specially crafted packets to the vulnerable SMBv1 protocol, triggering a buffer overflow and granting the attacker remote code execution capabilities. This remote

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 7, May 2025 Impact Factor: 7.67

code execution (RCE) vulnerability enables WannaCry to spread rapidly within an unpatched network by infecting all connected machines.

Once a system is infected, the ransomware encrypts files using a symmetric encryption algorithm and then demands a ranom, typically in Bitcoin, for the decryption key. The encrypted files are marked with the extension .WNCRY, making it clear that the files have been affected. To prevent further infections, WannaCry uses a double-spread mechanism, leveraging both Ransomware-as-a-Service (RaaS) infrastructure and SMB exploitation, thus accelerating the spread of the infection.

V. WANNACRY PROPAGATION AND SPREAD

WannaCry uses a worm-like propagation mechanism, meaning it can self-replicate and spread across vulnerable systems without requiring user interaction. Once the malware infects a machine, it attempts to identify other vulnerable systems within the same network using the EternalBlue exploit. If the targeted systems are not patched, they become infected, thus propagating the attack to other machines in the same network or even to external networks, increasing the scale of the attack.

A highly virulent strain of ransomware, known as WannaCry, infected hundreds of thousands of computers globally following its emergence on Friday, May 12. What distinguishes WannaCry from typical ransomware is its ability to propagate autonomously across an organization's network by exploiting critical vulnerabilities in Windows systems. These vulnerabilities had been addressed by Microsoft in March 2017 through Security Bulletin MS17-010 [4].

VI. THE ROLE OF THE KILL SWITCH

The ransomware's spread was briefly halted when a security researcher, Marcus Hutchins, discovered a "kill switch" within the WannaCry code [5]. This kill switch was a domain name that, if activated, would stop the malware from further infecting systems. Hutchins discovered that the ransomware was attempting to contact an unregistered domain before continuing its spread. Once the domain was registered, the attack's propagation ceased. Although this action mitigated further damage, the initial impact had already caused significant harm to global networks.

VII. GLOBAL IMPACT OF WANNACRY

The WannaCry ransomware attack had a devastating global impact, affecting more than 230,000 computers across 150 countries within just a few days. The attack primarily targeted organizations and industries that had not applied critical security patches, leaving them vulnerable to exploitation. The attack impacted various critical sectors, including healthcare, government services, telecommunications, and the oil and gas industry. While the ransomware's reach was extensive, its consequences were especially severe in specific areas such as healthcare, transportation, and telecommunications [2].

Impact on Healthcare

The healthcare industry was one of the most severely affected by WannaCry. The attack disrupted hospital networks and healthcare services, leading to widespread operational chaos. In the United Kingdom, the National Health Service (NHS) was one of the most high-profile victims, with more than 60 NHS organizations affected. The ransomware caused the cancellation of medical appointments, delayed surgeries, and diverted emergency patients. For example, critical systems used for patient care were rendered inoperable, forcing medical staff to rely on outdated manual systems.

The WannaCry attack highlighted the vulnerabilities in the healthcare sector, which relies heavily on legacy systems that are often not updated or patched due to the cost and complexity involved in doing so. The lack of regular updates and proper patch management allowed WannaCry to spread rapidly within healthcare networks, resulting in substantial disruption to critical services.

In today's rapidly evolving, global, and data-driven socioeconomic landscape, the most significant threat to civilian healthcare may no longer be physical terrorist attacks on medical facilities. Instead, it may come from unforeseen cyber attacks aimed at compromising the security of healthcare information systems [6].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Impact on Transportation and Other Industries

Apart from healthcare, WannaCry had significant repercussions in other industries, including telecommunications, manufacturing, and transportation. For instance, FedEx, one of the largest courier services, was impacted by the ransomware, leading to delays in shipments and operational inefficiencies. The attack caused disruptions in the company's internal systems, forcing them to implement workarounds for the affected services.

Other companies, especially those with outdated IT infrastructure, experienced service interruptions, financial losses, and reputational damage. In the case of Telefonica, one of Spain's largest telecommunications companies, internal systems were compromised, affecting communication networks and services.

Financial Losses and Response

While the total financial losses from the WannaCry attack are difficult to quantify, estimates suggest that the total damage could have exceeded $4 billion globally. This includes costs related to system downtime, loss of productivity, ransom payments, and recovery efforts. The attack prompted global organizations, governments, and cyber security agencies to respond with emergency patching efforts and increased awareness of the need for robust cyber security protocols.

The attack also led to greater collaboration among international cyber security bodies, such as Europol and INTERPOL, which coordinated efforts to track down the responsible actors. The response was mixed, with some companies managing to contain the damage quickly through patches and backups, while others struggled to recover due to inadequate cyber security measures.

VIII. ANALYSIS OF WANNACRY DEFENCE MECHANISMS

Despite the widespread damage caused by WannaCry, the attack revealed several critical weaknesses in existing defence mechanisms. The primary reason for the rapid spread of the ransomware was the failure to patch systems that were vulnerable to the EternalBlue exploit. This section examines the existing defence mechanisms, their shortcomings, and lessons learned for improving future cyber defences.

Ineffectiveness of Traditional Security Measures

Traditional security measures such as antivirus software, firewalls, and intrusion detection systems (IDS) were largely ineffective in defending against WannaCry. While these tools can prevent a wide range of threats, they were not equipped to handle a fast-moving, worm-like ransomware attack that exploited an unpatched vulnerability in a widely used protocol.

- *Antivirus software*: Many antivirus solutions were unable to detect WannaCry until after it had spread, leaving systems vulnerable during the early stages of the attack. The ability of WannaCry to propagate without user interaction also made traditional endpoint defences ineffective.
- *Firewalls:* While firewalls can block inbound and outbound traffic, they were unable to prevent the ransomware from exploiting the SMB vulnerability on local networks. Firewalls typically do not block internal traffic based on known exploits unless they are specifically configured to do so.
- *Intrusion Detection Systems (IDS):* IDS tools were ineffective at detecting the rapid and automated spread of the ransomware because an Intrusion Detection System (IDS) can identify and notify about potential attacks, but it does not take action to block or prevent them [7]. Traditional IDS tools focus on known signatures or anomalous network traffic but failed to identify WannaCry's self-propagating nature in real-time.

Patch Management and the Importance of Regular Updates

One of the key lessons from the WannaCry attack is the critical importance of patch management. Microsoft had released a security update (MS17-010) to address the SMB vulnerability in March 2017, two months before the attack [8]. However, many organizations had not yet applied the patch, leaving their systems exposed. This highlights the need

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

for organizations to establish robust patch management policies and ensure that updates are deployed across all devices in a timely manner.

While some companies and individuals were able to mitigate the damage by applying the patch before the ransomware reached them, others were caught off guard due to inconsistent or delayed patching practices. This emphasizes the need for automated patch management systems that can ensure timely and consistent application of critical updates.

Backup and Recovery Systems

Another critical defence mechanism highlighted by WannaCry is the importance of backup and recovery systems. Organizations that had robust and regular backups were able to restore their systems and data with minimal downtime, reducing the overall impact of the attack. In contrast, organizations without proper backup systems were forced to either pay the ransom or spend extensive time and resources on recovery efforts.

Having isolated backups that are not connected to the network can prevent ransomware from encrypting backup data, ensuring that organizations have a reliable recovery point in the event of an attack.

Advanced Detection and Behavioural Analysis

While traditional security measures were ineffective, the advanced detection and behavioral analysis technologies have shown promise in identifying and stopping similar threats. These technologies look for abnormal patterns of behavior on systems and networks, such as unusual file modifications or unusual network traffic, which are indicative of a ransomware attack.

Emerging solutions such as Endpoint Detection and Response (EDR) and Network Traffic Analysis (NTA) focus on behavioral anomalies rather than relying on signature-based detection, making them more effective in detecting new and evolving threats like WannaCry.

IX. LESSONS LEARNED AND RECOMMENDATIONS FOR FUTURE CYBER DEFENCE

The WannaCry ransomware attack provided invaluable lessons on the vulnerabilities within both individual organizations and global cyber security infrastructures. While some organizations were able to recover swiftly, many others faced severe consequences due to poor preparedness. This section outlines the key lessons learned from the WannaCry attack and provides recommendations to bolster defences against similar future threats.

Regular Patch Management is Crucial

One of the most critical takeaways from WannaCry is the importance of timely and consistent patch management. WannaCry ransomware could have been prevented by applying the appropriate security patch provided by Microsoft. The most effective method was to update the operating system to its latest version. Notably, the critical patch—Microsoft Security Bulletin MS17-010—were released on March 14, 2017, prior to the outbreak. This update addressed vulnerability in the SMB protocol exploited by the EternalBlue exploit. However, despite Microsoft's designation of the patch as critical, a significant number of systems remained unpatched by May 2017, allowing the ransomware to spread rapidly across networks many organizations failed to apply the patch on time, leaving them open to attack [9].

Recommendation: Organizations must implement an effective patch management system to ensure that all critical patches are applied as soon as they are released. Automating the patching process and conducting regular vulnerability scans can help organizations identify and address unpatched systems before they become targets for attacks.

Importance of Backup Systems

The attack demonstrated the importance of robust backup and recovery strategies. Organizations that maintained offline backups were able to restore systems quickly, while those without such measures faced prolonged downtime or were forced to pay the ransom.

Recommendation: Regularly back up critical data and ensure that backups are isolated from the main network. Use a 3-2-1 backup strategy (three total copies of data, two on different media, and one off-site) to provide a reliable and secure recovery option. Ensure that backups are regularly tested to verify their integrity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Network Segmentation and Isolation

WannaCry's ability to propagate quickly within networks highlighted the need for network segmentation and isolation. Without segmentation, the attack spread rapidly, impacting not only individual systems but entire networks, including organizational assets in critical sectors like healthcare and transportation.

Recommendation: Organizations should implement network segmentation to limit the spread of malware. Critical systems should be isolated from the rest of the network, and strict access controls should be enforced to prevent lateral movement of threats. Additionally, applying least-privilege access policies can help mitigate the impact of successful attacks.

User Awareness and Training

The role of user awareness in preventing cyber threats cannot be overstated. Many ransomware attacks are successful due to human error, such as clicking on phishing links or downloading malicious attachments. While WannaCry didn't rely directly on user interaction, educating employees about general cyber security practices can prevent other types of ransomware and malware attacks.

Recommendation: Regularly train employees on identifying phishing attempts and other social engineering tactics. Promote a security-first culture where employees are aware of the potential threats and the steps they can take to protect the organization.

Enhanced Threat Intelligence Sharing and Collaboration

The WannaCry attack demonstrated the value of threat intelligence sharing and collaboration across organizations, governments, and cybersecurity bodies. The discovery of the kill switch that halted the attack was a result of collaboration among researchers and security experts. Furthermore, global responses from entities such as Europol and INTERPOL helped mitigate the damage.

Recommendation: Organizations should actively engage in information-sharing platforms and collaborate with other entities to exchange threat intelligence. Governments and cyber security firms must continue to work together to track emerging threats, share real-time intelligence, and develop coordinated responses to large-scale cyberattacks.

Adoption of Advanced Security Technologies

As cyber threats evolve, so must security technologies. Traditional security measures such as antivirus software and firewalls are no longer sufficient to defend against sophisticated ransomware like WannaCry. More advanced approaches, such as Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA), and behavioral analytics, offer better protection by focusing on detecting abnormal activity rather than relying on signature-based detection.

Recommendation: Organizations should adopt next-generation security technologies that use AI and machine learning to detect and respond to threats in real time. Deploying these advanced systems can help identify and neutralize emerging threats before they cause significant harm.

X. CONCLUSION

The WannaCry ransomware attack of 2017 remains one of the most significant cyber security incidents in recent history [10]. It exploited the EternalBlue vulnerability in Windows systems to spread rapidly, affecting hundreds of thousands of computers across the globe. The attack had a far-reaching impact, particularly on critical sectors such as healthcare, transportation, and telecommunications. However, the attack also provided valuable insights into the importance of proactive cyber security measures.

The primary lesson from WannaCry is the critical importance of patch management, as the vulnerability exploited by the ransomware had been known and patched months before the attack. Additionally, the importance of backup systems, network segmentation, user awareness, and advanced security technologies became evident. The global response to the attack demonstrated the value of collaboration and information-sharing among cyber security experts, organizations, and governments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Going forward, organizations must adopt a multi-layered approach to cyber security, incorporating both technological defences and human factors. By implementing robust patch management systems, maintaining secure backups, segmenting networks, and investing in advanced detection technologies, organizations can significantly reduce the risk of similar attacks in the future. The lessons learned from WannaCry should serve as a wake-up call for organizations to strengthen their cyber security practices and adopt a proactive stance against emerging threats

REFERENCES

[1] N. S. Justin Jones, "Ransomware Analysis and Defense WannaCry and the Win32 environment," INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, pp. 57-69.
[2] V. G. V. I. D. M. M. D. L. Maxat Akbanov∗, "Static and Dynamic Analysis of WannaCry," pp. 1-5.
[3] V. G. V. a. M. D. L. Maxat Akbanov1, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," Journal of Telecommunications and Information Technology, pp. 113-124, 2019.
[4] "What you need to know about the WannaCry Ransomware," 2017.
[5] E. Woollacott, "Marcus Hutchins on halting the WannaCry ransomware attack – 'Still to this day it feels like it was all a weird dream'," 2022.
[6] T. A. Mattei, "Privacy, Confidentiality, andSecurityofHealthCareInformation: Lessonsfromthe," 2017.
[7] "Intrusion Detection System (IDS)".
[8] "MS17-010: Security update for Windows SMB Server: March 14, 2017".
[9] J. Fruhlinger, "WannaCry explained: A perfect ransomware storm," 2022.
[10] M. P. Savita Mohurle, "A brief study of Wannacry Threat: Ransomware Attack 201," International Journal of Advanced Research in Computer Science, vol. 8, pp. 1-3, 2017.
[11] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware," pp. 1-9, 2017.
[12] D.-Y. KAOa, "The Dynamic Analysis of WannaCry Ransomware," International Conference on Advanced Communications Technology (ICACT), pp. 1-8, 2018.