KARNATAK LAW SOCIETY'S

GOGTE INSTITUTE OF TECHNOLOGY

UDYAMBAG, BELAGAVI-590008

(An Autonomous Institution under Visvesvaraya Technological University, Belagavi)

(APPROVED BY AICTE, NEW DELHI)

Department of Computer Science and Engineering

Academic Year 2024-25

Seminar Report on "**WannaCry Ransomware Attack (2017)"**for the subject"**Cyber Security** "(21CS71)

Submitted By:

Name	USN
Harshad Joshi	2GI21CS069
Jay Kale	2GI21CS073
Raghavendra B	2GI21CS119
Omkar Patil	2GI21CS106

Under the guidance of

Prof. Sagar Pujar

Karnataka law society's

GOGTE INSTITUTE OF TECHNOLOGY

Udyambag Belagavi-590008

Karnataka India

Department of Computer Science and Engineering

Certificate

This is to certify that the Course Project work "**Wanna Cry Ransomware Attack (2017)"** for the subject" carried out by Harshad J, Jay K, Reghavendra B, Omkar P. USNs: 2GI21CS069, 2GI21CS073, 2GI21CS0119, 2GI21CS106 for Cyber Security(21CS721) is submitted in partial fulfilment of the requirements for 7 semester B.E. in COMPUTER SCIENCE AND ENGINEERING, Visvesvaraya Technological University, Belagavi. It is certified that all corrections/ suggestions indicated have been incorporated in the report. The course project report has been approved as it satisfies the academic requirements prescribed for the said degree.

Date:05/12/2024 **Guide:**

Place: Belagavi **Prof. Sagar Pujar**

INTRODUCTION

The WannaCry ransomware attack, launched on May 12, 2017, stands as one of the most far-reaching and disruptive cyberattacks in history, affecting over 230,000 computers across more than 150 countries. It represented a new era of global ransomware threats, demonstrating the devastating potential of malware that exploits unpatched vulnerabilities in widely used systems. The attack primarily targeted computers running Microsoft Windows, using a leaked exploit known as **EternalBlue**, which took advantage of a vulnerability in the Windows Server Message Block (SMB) protocol. Once infected, systems were locked down as WannaCry encrypted files and demanded a ransom payment in Bitcoin for their recovery, typically between $300 and $600 per device.

WannaCry's rapid spread and global impact were exacerbated by its worm-like ability to self-propagate across vulnerable networks, infecting systems without requiring user interaction. This led to significant disruptions in industries ranging from healthcare and telecommunications to transportation and manufacturing. One of the most prominent victims was the **UK's National Health Service (NHS)**, where operations were canceled, critical medical equipment was rendered unusable, and patient care was severely impacted. Other major organizations, such as FedEx, Renault, and Telefónica, also suffered significant operational downtime.

The attack was made possible by EternalBlue, an exploit allegedly developed by the U.S. National Security Agency (NSA) and leaked by a hacker group known as **Shadow Brokers** in April 2017. Although Microsoft had released a patch for the vulnerability (MS17-010) two months earlier, many organizations failed to apply it, leaving their systems exposed. WannaCry exploited this oversight, highlighting the global lack of awareness and preparedness to address rapidly evolving cyber threats.

While a cybersecurity researcher known as **MalwareTech** inadvertently mitigated the attack by discovering a "kill switch" domain that slowed its spread, the incident revealed critical weaknesses in global cybersecurity frameworks. It emphasized the importance of timely patch management, proactive cybersecurity strategies, and international collaboration to combat cyber threats.

The WannaCry ransomware attack is now studied as a defining moment in cybersecurity history, offering key lessons about the risks posed by outdated systems, inadequate patching, and the misuse of cyberweapons. It serves as a sobering reminder of the catastrophic impact cyberattacks can have on critical infrastructure, businesses, and individuals in an increasingly interconnected world.

The WannaCry ransomware attack was not just a technical failure but a wake-up call for industries worldwide. Its effects went beyond financial losses, disrupting essential services and exposing systemic vulnerabilities in the way organizations handle cybersecurity. WannaCry demanded immediate attention to fundamental security practices, including the importance of timely software updates, proper network segmentation, and employee training.

The ransomware targeted a critical flaw in the Microsoft Windows operating system, which had already been addressed by a patch released by Microsoft in March 2017. However, the failure of organizations to apply this patch left millions of systems exposed. This lack of basic cybersecurity hygiene turned what could have been a

BACKGROUND

The WannaCry ransomware attack occurred against the backdrop of a rapidly evolving cybersecurity landscape. By 2017, ransomware had already become a lucrative tool for cybercriminals, with high-profile incidents targeting hospitals, financial institutions, and government agencies. These attacks exploited vulnerabilities in outdated systems, using sophisticated methods to encrypt critical data and demand payment in cryptocurrency. WannaCry, however, marked a significant escalation in the scale and sophistication of ransomware campaigns.

The origins of WannaCry trace back to the leaked **EternalBlue** exploit, which was allegedly developed by the NSA to exploit a vulnerability in Microsoft's SMB protocol. EternalBlue was leaked to the public in April 2017 by a hacking group called Shadow Brokers. Despite widespread warnings from security researchers and the release of a patch (MS17-010) by Microsoft, many organizations failed to act swiftly, leaving millions of systems vulnerable to attack.

When WannaCry was unleashed on May 12, 2017, it spread at an unprecedented speed, infecting systems in over 150 countries within hours. The ransomware exploited unpatched Windows systems, encrypting files and displaying a ransom note demanding payment in Bitcoin. Victims were given a three-day window to pay $300, with the ransom doubling after this period. If no payment was received within seven days, the encrypted files were permanently deleted.

One of the attack's most devastating consequences was its impact on critical infrastructure. The UK's NHS was among the hardest hit, with nearly 20,000 medical appointments canceled, including surgeries. Ambulances were diverted, and patient records became inaccessible, putting lives at risk. The attack also disrupted operations at major corporations such as Renault, Nissan, and Deutsche Bahn, causing significant financial and operational losses.

Although the attack was somewhat contained by the discovery of a "kill switch" domain—accidentally identified by MalwareTech—the damage had already been done. WannaCry revealed glaring weaknesses in global cybersecurity preparedness and highlighted the urgent need for better patch management, awareness, and coordinated incident response.

This incident also shed light on the global nature of cyber threats and the challenges of attribution. While many experts attributed the attack to a North Korean hacking group known as **Lazarus**, the evidence was circumstantial, and the exact perpetrators remain a subject of debate. What is clear, however, is that WannaCry's impact transcended geographical and sectoral boundaries, affecting organizations and individuals alike.

PROBLEM STATEMENT

The WannaCry ransomware attack of May 2017 highlighted severe gaps in global cybersecurity defenses, exposing weaknesses in both technical infrastructure and organizational preparedness. The attack leveraged the **EternalBlue** exploit to target a vulnerability in Microsoft's Server Message Block (SMB) protocol, which had already been patched months earlier. However, despite the availability of the patch, thousands of systems remained vulnerable due to poor patch management and outdated operating systems.

Once infected, systems were locked with ransomware that encrypted critical files, displaying a ransom demand in Bitcoin. Victims were forced to either pay the ransom or face permanent data loss. WannaCry's unprecedented spread affected over 230,000 computers across 150 countries, disrupting critical services such as healthcare, manufacturing, and transportation.

The problem was multifaceted. On the technical front, organizations failed to implement basic cybersecurity measures such as regular patch updates, proper network segmentation, and backup systems. From an organizational perspective, many institutions lacked adequate incident response plans, threat detection systems, and staff training to handle such attacks. Furthermore, the attack underscored the ethical debate over government agencies hoarding vulnerabilities, as the NSA's development of EternalBlue indirectly facilitated the attack.

The WannaCry attack posed significant challenges for both public and private sectors, emphasizing the interconnectedness of modern systems and the risks posed by a single unpatched vulnerability. It highlighted the urgent need for proactive threat management, international cooperation, and improved cybersecurity practices to prevent similar incidents in the future.

CHALLENGES FACED

1. **Failure to Patch Systems:**
   Despite Microsoft releasing the MS17-010 patch two months prior to the attack, many organizations did not update their systems. This failure was partly due to reliance on legacy systems, especially in industries like healthcare, where upgrading software is often slow and costly.
2. **Use of Outdated Operating Systems:**
   A significant number of affected systems were running outdated versions of Windows, such as Windows XP, which no longer received regular security updates. This lack of support left these systems highly vulnerable to exploitation.
3. **Global Scale of Impact:**
   The attack's rapid spread across 150 countries overwhelmed cybersecurity teams and revealed the difficulty of coordinating a global response to a cyber crisis. Organizations struggled to contain the attack, particularly in sectors with limited technical expertise.
4. **Impact on Critical Infrastructure:**
   WannaCry caused severe disruptions to essential services, particularly in the healthcare sector. The UK's NHS had to cancel surgeries, reschedule appointments, and divert ambulances, putting patient safety at risk. Similar disruptions occurred in manufacturing, logistics, and transportation.
5. **Inadequate Backup Systems:**
   Many organizations lacked robust backup systems, leaving them with no way to recover encrypted files without paying the ransom. This lack of redundancy amplified the attack's impact and financial cost.
6. **Poor Incident Response:**
   Many affected organizations lacked incident response plans, resulting in delayed containment and recovery. This absence of preparedness increased downtime and prolonged the attack's effects.
7. **Ethical and Geopolitical Questions:**
   The use of the NSA-developed EternalBlue exploit fueled debates about the role of government agencies in cybersecurity. Critics argued that vulnerabilities should be disclosed to vendors immediately rather than weaponized for offensive purposes.
8. **Unclear Attribution:**
   While the attack was widely attributed to the North Korean Lazarus Group, definitive proof was lacking, complicating efforts to assign responsibility and take appropriate action.
9. **Lack of Cybersecurity Awareness Among Employees:**
   Many organizations had insufficient training programs for employees, leaving them vulnerable to phishing scams or mishandling suspicious files. While WannaCry spread through a vulnerability, social engineering could have amplified its impact in unprepared environments.
10. **Absence of Network Segmentation:**
    Many organizations operated on flat networks without proper segmentation, allowing WannaCry to move laterally and infect multiple systems rapidly. This design flaw enabled attackers to maximize the scope of their attack.

LESSONS LEARNED

1. Importance of Timely Patch Management:
   The WannaCry attack exploited a known vulnerability in Windows systems (EternalBlue) that Microsoft had patched months before the attack. This underscores the critical need for organizations to implement timely patch management processes to close known security gaps.
2. Need for Regular Data Backups:
   Organizations that maintained up-to-date, offline backups of critical data were able to recover faster and avoid paying the ransom. Regularly testing recovery procedures ensures backups are reliable and effective during emergencies.
3. Adopting Strong Network Segmentation:
   Proper network segmentation can significantly limit the lateral movement of ransomware within an organization, isolating infected systems and minimizing the attack's impact. Critical systems should always be separated from less secure parts of the network.
4. Increased Investment in Cybersecurity Infrastructure:
   The attack highlighted the importance of robust cybersecurity infrastructure, including intrusion detection systems (IDS), firewalls, and endpoint protection. Organizations must prioritize cybersecurity in their budgets to prevent similar breaches.
5. Awareness of Legacy Systems Risks:
   Many organizations were using outdated or unsupported operating systems like Windows XP, which were especially vulnerable to WannaCry. It emphasized the need to upgrade legacy systems or use compensating controls to mitigate risks.
6. Improved Incident Response Preparedness:
   Organizations need detailed and rehearsed incident response plans to handle cyberattacks effectively. The lack of coordination and slow responses exacerbated WannaCry's impact, demonstrating the value of quick containment and communication.
7. Global Cooperation Against Cybercrime:
   The attack revealed the need for stronger international collaboration in identifying and neutralizing cyber threats. Governments, private sectors, and global organizations must work together to share threat intelligence and improve collective defenses.
8. Value of Disabling Unused Features:
   The SMBv1 protocol exploited in the WannaCry attack was outdated and unnecessary in many systems. Organizations learned the importance of disabling unused or vulnerable features to reduce their attack surface.
9. Adoption of Zero Trust Security Models:
   WannaCry demonstrated the need to move away from perimeter-focused security to Zero Trust models, where no user or system is trusted by default, and continuous verification is required for access.

FINDINGS

1. Exploitation of Known Vulnerabilities:
   The WannaCry attack capitalized on a vulnerability in Microsoft's Server Message Block (SMBv1) protocol, which had been publicly disclosed and patched two months prior to the attack. This demonstrated a widespread failure among organizations to apply critical security updates promptly.
2. Wide Impact Across Industries:
   The ransomware affected over 200,000 systems across 150 countries, targeting organizations in healthcare, transportation, finance, manufacturing, and telecommunications. This highlighted the global and cross-industry vulnerability to cyber threats.
3. High Dependency on Outdated Systems:
   Many organizations affected by WannaCry, including the UK's National Health Service (NHS), were using unsupported operating systems such as Windows XP. This reliance on legacy systems created significant security risks.
4. Rapid Spread Through Network Worm Capabilities:
   WannaCry's self-propagating nature, enabled by the EternalBlue exploit, allowed it to spread quickly across networks without requiring user interaction, amplifying the attack's reach and impact.
5. Lack of Effective Incident Response Plans:
   Many affected organizations lacked a well-defined or rehearsed incident response plan, resulting in delayed containment, increased downtime, and greater financial losses.
6. Role of Kill Switch in Mitigating the Attack:
   A security researcher accidentally discovered a "kill switch" in the WannaCry code that halted the ransomware's spread. This finding showed that attackers sometimes leave unintentional vulnerabilities in their malware.
7. Inadequate Backup Strategies:
   Organizations without reliable offline data backups suffered the most, as they were forced to choose between paying the ransom or losing critical data. This highlighted the importance of regular and secure backup systems.
8. Failure of Traditional Security Measures:
   Traditional antivirus solutions and firewalls were largely ineffective against WannaCry due to its novel propagation techniques, emphasizing the need for advanced threat detection systems.
9. Financial Losses and Operational Disruptions:
   The attack caused billions of dollars in damages globally, including lost revenue, remediation costs, and reputational harm. In healthcare, patient care was delayed or disrupted due to the attack's impact on critical systems.
10. Rise of Ransomware as a Service (RaaS):
    WannaCry demonstrated how ransomware could be distributed as a service, enabling less-skilled attackers to execute sophisticated campaigns using tools developed by others.
11. Failure of Patching Policies Across Organizations:
    The attack exposed the widespread inadequacy of patch management policies, with

ANALYSIS

1. Exploitation of Unpatched Systems: WannaCry used the EternalBlue exploit, targeting organizations that failed to apply critical patches despite warnings.
2. Reliance on Legacy Systems: Outdated systems like Windows XP in sectors like healthcare magnified the attack's impact.
3. Weak Backup Strategies: Organizations lacked reliable offline backups, making them vulnerable to data loss and ransom payments.
4. Rapid Propagation: The malware's worm-like behavior exploited unsecured networks, spreading quickly across unsegmented systems.
5. Outdated Security Measures: Traditional antivirus and firewalls were ineffective against WannaCry's advanced tactics.
6. Global Impact: The attack affected over 150 countries, exposing vulnerabilities in interconnected global systems.
7. Incident Response Failures: Delayed responses due to poorly defined or tested plans allowed the malware to spread further.
8. Economic Losses: The attack caused billions in damages, disrupting critical operations like healthcare and transport.
9. Nation-State Cyberweapons: WannaCry used tools leaked from the NSA, raising concerns about government responsibility for safeguarding cyber arsenals.
10. Kill Switch Discovery: A researcher's accidental discovery of a kill switch halted the malware's spread, revealing flaws in its design.
11. Importance of Cyber Hygiene: Neglecting updates, employee training, and secure configurations left systems vulnerable.
12. Call for Collaboration: The attack spurred global discussions on cybersecurity cooperation and increased investments in defense measures.
13. **Human Factor Vulnerabilities:** Many organizations lacked employee awareness programs, increasing susceptibility to phishing and social engineering attacks.
14. **Absence of Threat Intelligence Sharing:** Limited collaboration between organizations and governments delayed the global response to the attack.
15. **Failure in Endpoint Security:** Weak endpoint protection allowed initial infections to escalate within networks.
16. **Critical Infrastructure at Risk:** Sectors like healthcare and public utilities suffered disproportionately due to their reliance on outdated systems.
17. **Inadequate Patch Management Policies:** Organizations failed to implement structured patch deployment protocols, leaving them exposed despite patch availability.
18. **Dependency on External Tools:** Over-reliance on third-party cybersecurity solutions without independent assessments of vulnerabilities exacerbated risks.
19. **Inconsistent Incident Logging:** Poor logging practices meant that affected entities couldn't effectively track the malware's entry and propagation.
20. **Global Disparity in Cyber Preparedness:** Developing nations were hit harder due to weaker cybersecurity frameworks and lack of resources.
21. **Public Sector Unpreparedness:** Government agencies, including hospitals and utilities, were highly vulnerable due to aging IT systems and slow procurement processes.

RECOMMENDATIONS

1. **Implement Robust Patch Management:**
   Establish automated patching systems to ensure all software and operating systems are updated promptly, especially when critical vulnerabilities are disclosed.
2. **Enhance Network Segmentation:**
   Divide networks into smaller, isolated segments to contain malware spread and limit lateral movement within systems.
3. **Adopt Advanced Threat Detection:**
   Deploy AI-powered threat detection systems to identify and respond to suspicious activities in real-time.
4. **Regular Backups with Offline Storage:**
   Maintain frequent backups of critical data and store them offline to prevent ransomware from encrypting or corrupting backup files.
5. **End-of-Life System Replacement:**
   Gradually phase out unsupported legacy systems and migrate to newer, more secure platforms with ongoing vendor support.
6. **Strengthen Endpoint Security:**
   Deploy robust endpoint protection tools like anti-ransomware software, endpoint detection and response (EDR), and host-based firewalls.
7. **Implement Multi-Factor Authentication (MFA):**
   Use MFA for all access points to reduce the risk of unauthorized access to sensitive systems and data.
8. **Conduct Cybersecurity Training:**
   Regularly educate employees on identifying phishing emails, ransomware tactics, and safe computing practices.
9. **Adopt Zero Trust Architecture:**
   Implement a "never trust, always verify" model that enforces strict access controls, even for internal users.
10. **Perform Regular Vulnerability Assessments:**
    Conduct frequent security audits, penetration testing, and risk assessments to identify and address vulnerabilities before attackers exploit them.
11. **Collaborate on Threat Intelligence:**
    Join cybersecurity information-sharing organizations to stay updated on emerging threats and industry best practices.
12. **Develop a Comprehensive Incident Response Plan:**
    Create and regularly test an incident response plan to ensure quick and coordinated actions during an attack.
13. **Encourage International Cooperation:**
    Governments and private entities must collaborate to develop standardized frameworks for combating global cyber threats.

REFERENCES

- Deep Hub I Medium
- Wanna Cry attack - Search Videos
- Wanna Cry Attack- Search Images