Dissecting WannaCry: Technical Analysis, Consequences, and Countermeasures against Ransomware Attacks

Abdur Rafay Saleem
Department Of Computer Science
University of Central Florida
ab464825@ucf.edu

Abstract— **This research paper aims to discuss the famous WannaCry ransomware that affected a record number of computer systems around the globe. It will explore this malware in-depth, covering all angles. Firstly, we will introduce its history and explain the category of malware in which it falls. Following this, we will unfold the attack details and explore the technical aspects that allowed it to succeed. Moreover, we will discuss the impact and the different real-world damages it caused. Furthermore, we will discuss the recovery process and preventative measures that could be taken. We will also cover the challenges in attributing cyber attacks to specific perpetrators. Finally, we will discuss how it impacted the cybersecurity industry and what lessons could be drawn from its study.**

***Index Terms*—WannaCry, ransomware, worm, propagation, analysis, vulnerability, prevention.**

I. INTRODUCTION

The digital age has brought with it a vast number of advancements as well as a host of new challenges. One such challenge that has emerged prominently in recent years is the threat of cyber attacks. Ransomware attacks have proven to be particularly destructive. This paper focuses on one of the most infamous ransomware attacks in history—the WannaCry attack.

A. Background on Ransomware

Ransomware dates back to the late 1980s. The first ransomware was called the AIDS Trojan. However, the concept of ransomware for attacks was not very common in the 2000s and became more widespread in the 2010s. That is the period during which these malwares started to get more sophisticated.

Ransomware is a type of virus or malware that encrypts all personal data-related files of an owner on an infected system. The computer's operations are left untouched and continue to operate as usual. However, the victim's data, such as documents, videos, pictures, etc., are encrypted. The encrypted files display a warning from the attackers that threatens to erase the data and demand a ransom to release the decryption key to unlock the files. Cryptocurrencies like Bitcoin are used for payments since their wallet addresses' are untraceable and payments are instant. If any attempt is made to bypass or break the encryption, the ransomware erases the data forever. The attackers can also threaten to leak the data if the ransom is unpaid.

Initially, the ransomware used simple techniques such as screen locks, etc. However, they have now advanced to more dangerous file encryption methods that target various file types and systems [2]. These attacks can cause long-lasting and severe consequences for individuals and businesses. Attacks in the past have affected healthcare organizations, government agencies, manufacturers, critical sectors, etc.

B. Overview of the WannaCry Attack

In May 2017, malware spread rapidly across the globe by targeting Windows O.S. computer systems. It was a ransomware attack known as WannaCry. The WannaCry ransomware exploited a vulnerability in Microsoft Windows's network file-sharing protocol. This protocol was called the Server Message Block (SMB) protocol. This protocol contained a vulnerability called EternalBlue. It was discovered and kept secret by the U.S. National Security Agency (NSA). However, it was later leaked and made public by a hacker group called the Shadow Brokers.

The WannaCry ransomware was crafted as a worm to spread autonomously through networks. It infected any unpatched systems and encrypted their files. This worm functionality enabled WannaCry to scan for and infect other vulnerable systems on the same network to amplify its impact [12]. Once the system's data was encrypted, it would display a ransom note demanding a payment to unlock it. This payment varied between $300 to $600 and was threatened to increase as time passed. The attack infected hundreds of thousands of computers in one day. It had its victims across more than 150 countries around the globe. It caused widespread disruption and significant economic losses across several sectors worldwide.

C. Significance of Studying the WannaCry Attack

The WannaCry incident is recognized to be among the most destructive cyber incidents in history. Its global impact is useful for understanding the importance of robust cybersecurity measures and the scary consequences of unpatched vulnerabilities. The resulting economic damage was huge, underscoring the real-world danger of cyber threats to critical infrastructure and services. Moreover, the attack was also important in the context of international relations. North Korea was assumed to be the perpetrator by various cybersecurity firms and government agencies. Attributing the attack to North Korea raised questions about the involvement of nations in cyber warfare. Despite this attribution, it is challenging to confirm the involvement of any specific actor.

Studying the WannaCry attack can provide some valuable lessons. These include incident response and attack prevention strategies and how they can be applied to the broader cybersecurity landscape. It is essential to study it to get insights, keep systems updated and patched, understand the potential economic impact of such cyber attacks, and stress the need for international cooperation and collaboration in combating them. Additionally, the attack led to increased investments in cybersecurity infrastructure and became a case study in many cybersecurity courses and training programs. In the following sections, we will dive deeper into these aspects and explore the specifics of the WannaCry attack. The goal is not just to recount the events of the attack but to use it as a learning tool to better understand and prepare for future cybersecurity threats.

II. TECHNICAL DETAILS OF THE ATTACK

A. The Vulnerability Exploited (EternalBlue SMB Exploit)

The attack was performed using a vulnerability called EternalBlue in the Microsoft Windows operating system. This vulnerability lied in the OS's protocol called Server Message Block (SMB) and exploiting it could allow attackers to execute their own code on infected systems remotely.

Microsoft Windows uses the SMB protocol for network file sharing and remote services. This protocol allows clients and servers to share resources over an authenticated network session. The session setup begins with an exchange of a series of negotiations between the client and the server to agree on the SMB version to use. The vulnerability specifically resided in how the protocol handled specially crafted packets during the negotiation of this session. It was a buffer overflow vulnerability, allowing overwriting of the program's memory with a payload code. The EternalBlue vulnerability was exploited by sending malformed crafted packets during the negotiation session [11]. These packets contained a malformed payload that allowed an attacker to trigger the buffer overflow and overwrite the contents of the memory with its code. This allowed the attacker a backdoor channel into the targeted system with elevated privileges. If the exploit is successful, it will allow the attacker to control the compromised system completely. Then, they can execute malicious code, such as deploying ransomware or other malware payloads.

Various versions of Windows, such as Win 7, Server 2008 R2, and others, were affected by this vulnerability. These were still widely used at the time. The EternalBlue vulnerability could be exploited remotely and without user interaction. This combined with a wormable propagation, made it highly severe. Microsoft released a security update (MS17-010) to address the issue a few months before the WannaCry attack. However, the vulnerability's impact was worsened because many systems had not been patched with this update.

B. How the Attack Unfolded and Spread

The attack began on May 12, 2017, when many systems were affected by a virus known as WannaCry. Reports started arriving from all over the world, revealing that people's files were being encrypted and ransom demanded by an unknown attacker group. This malware contained two modules that allowed it to perform its intended attack vector.

1) Worm Module: The WannaCry ransomware was deployed as a worm virus. It rapidly spread through networks by leveraging the EternalBlue exploit. Once a single system was infected, the ransomware would scan the local network for other vulnerable machines running unpatched versions of Windows. This was done using a technique known as port scanning. In port scanning, the malware would send requests to different ports on a computer to see if they were open. It would then use the same exploit to gain unauthorized access and infect these systems with the ransomware payload. Any computer on the same network was susceptible to infection without a direct internet connection. Once a computer was infected, it would start acting as a scanner, looking for more connected victims. This allowed it to propagate autonomously within networks. It reached a global scale within no time as more and more systems got infected.

2) Cryptographic Module: The WannaCry would initiate its file encryption process after compromising a system. The ransomware utilized robust encryption algorithms such as RSA-2048 and AES-128. It encrypts many file types, such as documents, images, videos, databases, etc. The encryption process worked as follows:

1) a unique 128-bit AES key was generated on each infected system.
2) This AES key was then used to encrypt the victim's files using the AES-128 algorithm in CBC (Cipher Block Chaining) mode.
3) The unique AES key was encrypted using an embedded RSA-2048 public key hard-coded into the ransomware.
4) The encrypted AES key was then stored on the victim's system. It ensured that only the attackers with the corresponding RSA private key could decrypt it and subsequently recover the files.

C. The Kill Switch and Its Role in Slowing the Attack

The WannaCry ransomware spread aggressively, but a "kill switch" helped slow it down. A kill switch is a way for the program to terminate its activity based on some condition or logic. These are usually written into the system during testing and removed before the attack. However, its authors accidentally left such a kill switch feature hard-coded into the ransomware.

On the day of the attack, a 22-year-old cybersecurity researcher named Marcus Hutchins (also known as MalwareTech) was analyzing the code samples of this malware when he discovered this kill switch. He noticed a suspicious domain name embedded in the code. The kill switch attempted to connect to a specific domain name before initiating the encryption process on an infected system. This domain was stored in the code as a random character URL. If the connection to this domain were successful, the ransomware would terminate its execution without encrypting any files or spreading further. However, if the connection fails, it will proceed with its malicious activities, encrypting files and scanning for other vulnerable systems on the network.

Hutchins registered the domain out of curiosity and, as a result, activated the kill switch. Any new WannaCry infections would be automatically terminated when they tried connecting to this newly registered domain. This prevented the ransomware from encrypting files and spreading further. This unintentional failsafe bought valuable time for security researchers worldwide to analyze the ransomware. Soon, they developed mitigation strategies and deployed patches to protect vulnerable systems.

While the kill switch did not entirely stop the WannaCry attack, it slowed its propagation and limited further significant damage and disruption. This accidental kill switch highlights the importance of thorough code analysis in cybersecurity and the potential for unintended vulnerabilities or weaknesses in malware design.

D. Challenges in Attack Attribution

One of the significant challenges surrounding the WannaCry attack was attributing it to a specific threat actor or group. Initially, the infamous Lazarus Group was believed to be the original actor. However, since this organization has long been believed to be backed by North Korea, any blame could lead to the deterioration of international relations. Hence, the authenticity of the attribution process remains complex and subject to debate.

Furthermore, multiple techniques such as false flags, code randomization, and encryption hide the digital footprint. The involvement of multiple actors can make the attribution process more complex in cyber attacks [3]. Additionally, state-sponsored cyber operations often involve plausible deniability and the exploitation of vulnerabilities obtained from third parties.

The WannaCry attack highlights the attribution challenges in attacks involving advanced persistent threats (APTs) and shows the importance of measures such as Counter Threat Intelligence (CTI).

III. Impact and Consequences

A. Global Reach and Scale of the Attack

The WannaCry ransomware attack affected systems in over 150 countries across the globe, making it an unprecedented global threat. The spread of a ransomware attack was made possible due to the highly interconnected nature of modern computer networks. Starting in Europe and Asia, the malicious software quickly gained a foothold, and within hours, it had already spread to other regions across the globe, including the Americas, Africa, and Oceania. Although the exact number of infected systems remains uncertain, over 300,000 computers were estimated to be compromised within the first few days of the attack. It's important to note that this figure might not be accurate as many infections may have gone unreported, especially in areas with limited cybersecurity resources. This incident highlights the potential for a single cyber threat to have far-reaching consequences.

B. Disruption to Critical Infrastructure and Services

The WannaCry attack caused significant disruptions across various sectors, including healthcare, transportation, telecommunication, and government agencies. The attack affected at least 80 healthcare facilities in the UK, causing hospitals to cancel appointments, reject non-critical patients, and redirect ambulances. It also disrupted telecommunication services in Spain and Portugal, leading to the temporary closure of factories by major automotive manufacturers. Furthermore, it caused chaos in government services in Russia and India.

C. Economic Costs and Damages

The WannaCry attack significantly impacted the global economy, resulting in substantial financial losses. These losses were caused by a variety of factors, including:

1) Operational disruptions and downtime
2) Cost of incident response and recovery efforts
3) Lost productivity and revenue
4) Expenses related to system restoration and data recovery
5) Potential legal liabilities and regulatory fines

Multiple high-profile organizations have reported significant financial impacts, but accurate numbers are difficult to determine [4]. Some examples are:

- FedEx: The global logistics company estimated losses of around $300 million due to the attack.
- NHS: The U.K.'s National Health Service suffered more than £92 million in losses.
- Renault: The French automaker temporarily halted production at several sites. The estimated losses were around $400 million.
- Maersk: The Danish shipping and logistics giant faced disruptions to their operations and I.T. systems. The I.T. offered between $200 to $300 million in losses.
- Deutsche Bahn: The German national railway operator's services were disrupted and losses of approximately $10 million.
- Nissan: The Japanese automaker had to shut down its Sunderland plant in the U.K. for several months. This led to an estimated loss of thousands of vehicles in downtime costs.

The WannaCry attack caused direct monetary losses and significant indirect costs for many organizations. These included expenses related to incident response teams and cybersecurity consultants. Also, efforts that went into restoring systems and the cost of increasing security for future attacks. Small and medium-sized businesses (SMBs) were hit the hardest, as they required robust cybersecurity measures and disaster recovery plans. Many SMBs experienced significant financial difficulties or even the possibility of bankruptcy due to the disruptions caused by the WannaCry attack.

Additionally, the attack underlined the potential long-term consequences of such incidents. These may include reputational harm, loss of customer confidence, and legal liabilities arising from data breaches or service disruption.

D. Potential Harm to Individuals' Privacy and Data

The WannaCry attack raised concerns about the harm it could cause to individuals' privacy and data. Although the privacy objective of ransomware is financial gain through extortion, the encryption of personal files could lead to data and privacy breaches. Furthermore, there was no guarantee that the attacker would unlock the files after payment.

The nature of the attack meant that individuals' personal computers and devices were also vulnerable to infection. The attackers could access files containing personal data, financial records, or other confidential information. This produced the threat of sensitive information being exposed online or held for ransom. This could further lead to instances of identity theft, financial fraud, or extortion.

The incident highlighted the risks of ransomware attacks and the importance of robust data protection measures, regular backups, and safe storage practices.

IV. Recovery and Preventative Measures

A. Incident Response and Recovery Efforts

After the attack, the affected entities had to undertake significant efforts to recover from the ransomware's impact and restore their systems and data. These efforts often involved the following steps:

1) Containment and isolation: Identifying infected systems and isolating the network layers can help prevent the spread of viruses to others.
2) Data recovery: Attempting to recover encrypted files from available backups or using decryption tools developed by security researchers.
3) System restoration: Rebuilding and reinstalling operating systems, applications, and data on affected machines after removing the ransomware.
4) Patching and updates: The necessary security patches and updates address the EternalBlue vulnerability and other potential exploits.

Many organizations also had to employ cybersecurity firms to establish incident response teams. Government agencies had to intervene to create policies to aid in their recovery efforts and conduct forensic investigations.

B. Importance of Software Updates and Patching

This attack highlights the critical importance of regularly applying the latest security patches and updates. Microsoft released a security update (MS17-010) in March 2017 to address the EternalBlue vulnerability exploited by WannaCry. However, a significant number of systems remained unpatched, which allowed the ransomware to spread rapidly. This incident underscored the need for organizations and individuals to implement robust patch management practices. They should prioritize the timely installation of security updates. Otherwise, the systems are prone to exploitation by cyber threats, leading to devastating consequences.

C. Backup Strategies and Data Recovery

Good backups of important data are crucial to recover from attacks like ransomware, including WannaCry. Those who regularly backed up their data could restore their systems and minimize losses, even if they couldn't decrypt the locked files.

However, WannaCry also showed problems in how some backups were done. In some cases, the backup systems were also hit by the ransomware, making the backups useless. This highlighted the need for secure, separate backup solutions and regularly checking that the backups are working and can be used to restore data.[5].

D. User Education and Awareness of Phishing Attacks

Ransomware and other malware often get in through social engineering tricks. These can be complex, multi-pronged attacks or as simple as fake emails and websites. WannaCry initially infected systems using unusual phishing methods.

Companies should raise cybersecurity awareness and train employees to spot and avoid potential threats. This means recognizing suspicious emails, links, or attachments and quickly reporting possible security incidents. By doing this, employees can become an active defense against cyberattacks since humans are often the weakest link. If some WannaCry victims had been better informed about these techniques, they could have prevented the attacks [6].

This highlights how important it is to educate and raise awareness among users to fight cyber threats.

V. Aftermath and Lessons Learned

A. Changes in Cybersecurity Policies and Regulations

The WannaCry attack was a security breach and a global wake-up call. It exposed the vulnerability of numerous systems to cyber threats and demonstrated the catastrophic potential of a single piece of malware.

In response, many countries and regulatory bodies looked at their cybersecurity policies and made significant changes. The UK, for instance, brought in new rules called the Network and Information Systems (NIS) Regulations in 2018 [7]. These set clear standards for cybersecurity and made it mandatory for employees to report incidents.

The European Union also took a significant step in implementing the General Data Protection Regulation (GDPR) in the same year. This regulation imposed rigorous data protection requirements on organizations handling personal information. It made it obligatory to inform authorities and affected individuals during a data breach, bolstering regional data security.

B. Investment in Cybersecurity Infrastructure

WannaCry prompted a significant shift in thinking about cybersecurity at the highest levels. Governments and regulators recognized the need to take a more proactive approach to safeguard against future malware attacks and implemented appropriate measures accordingly. This led to an increased allocation of resources towards cybersecurity initiatives. These include:

1) Upgrading and modernizing I.T. infrastructure
2) Implementing advanced security solutions and threat detection systems
3) Enhancing incident response and disaster recovery capabilities
4) Providing cybersecurity training and awareness programs for employees

The demand for cybersecurity professionals surged massively after the attack as more and more companies started investing in making a more skilled and stronger cybersecurity workforce. [8].

C. New Technologies to Combat Ransomware

The WannaCry attack also spurred research and development efforts to create new technologies and strategies to combat ransomware and other malware threats. Some notable developments include:

1) Ransomware protection solutions: Software and tools designed to detect infections or suspicious activity and stop malware infections prematurely. Also, tools to minimize data loss through backup and recovery mechanisms.
2) Decryption platforms based on blockchain technology have been developed to distribute decryption keys through crowd-sourcing. This has the potential to weaken the ransomware business model.
3) Artificial Intelligence (AI) and Machine Learning (ML) techniques: Use of AI and ML algorithms to improve threat detection, vulnerability analysis, and response capabilities to detect evolving ransomware variants [9].

These new tools and techniques were designed to give organizations and people better protection against ransomware attacks and boost their overall cybersecurity strength.

D. Best Practices for Proactive Cybersecurity

The lessons learned from WannaCry reinforced the importance of changing our approach to cybersecurity. More emphasis should be placed on hackathons and competitions to make it a more interesting area for individuals to focus on and improve. This includes implementing best practices such as:

1) Regular software updates and patch management
2) Robust backup and disaster recovery strategies
3) Continuous security monitoring and threat intelligence
4) User awareness and training programs
5) Incident response and business continuity planning
6) Collaboration and information sharing among organizations and security communities

Embracing these practices can help organizations better prepare for and mitigate the risks posed by cyber threats. It will also increase their protection against ransomware attacks and enhance their cybersecurity infrastructure.

E. Preparing for Future Cybersecurity Threats

This attack highlighted the need for increased vigilance and preparation against cyber attacks. Cyber attackers continue to develop more sophisticated techniques daily, requiring staying on top of technology and a reiterative research cycle. Every entity must stay ahead of potential threats by:

1) Continuously monitoring and assessing emerging cyber risks
2) Investing in cybersecurity research and innovation
3) Fostering international cooperation and information sharing
4) Strengthening cybersecurity policies and rules
5) Promoting cybersecurity education and awareness

Learning from these past incidents can help the global community better anticipate and reduce future threats. This will help anticipate future threats even before they emerge and minimize their impact before they can cause any significant damage. [10].

VI. CONCLUSIONS

The WannaCry ransomware attack is a significant cybersecurity event that has left a lasting impact on the global community [1]. This incident highlighted the devastating consequences of neglecting software updates and vulnerabilities. Moreover, it displayed the potential for a piece of software to affect both the virtual and physical lives of people worldwide.

Several key lessons have emerged through an in-depth analysis of the WannaCry attack:

1) The importance of robust cybersecurity measures such as regular software updates, patch management, and user awareness programs.
2) Reliable backup strategies and data recovery solutions are needed to reduce the impact of ransomware and other malware threats.
3) The challenges of finding perpetrators of attacks in cases involving APTs and nation-state actors.
4) The potential economic and operational consequences of cyber attacks. Also, the importance of cybersecurity investments and incident response planning.
5) International cooperation is needed to combat global cyber threats and establish a resilient cybersecurity landscape.
6) Continued commitment to cybersecurity research is needed to stay ahead of evolving threats.

A. Final Thoughts and Recommendations

The recent WannaCry ransomware attack is a strong reminder of how interconnected our digital world is and how cyber threats can spread beyond geographical boundaries. This attack has highlighted the need for a comprehensive cybersecurity approach that involves all stakeholders, including governments, private sector organizations, cybersecurity professionals, and individual users.

Recommendations for individuals, organizations, and policymakers include:

1) Prioritizing regular software updates and patch management to address known vulnerabilities.
2) Implementing robust backup and disaster data recovery strategies to ensure business continuity.
3) Promoting cybersecurity awareness and training programs to empower users as the first line of defense against cyber threats.
4) Investing in cybersecurity infrastructure, incident response capabilities, and developing skilled cybersecurity professionals.
5) Fostering international cooperation in information sharing and cybersecurity policies and regulations that address global cyber threats.

We can minimize the potential for incidents like WannaCry by taking steps in advance and embracing a culture of cybersecurity surveillance to build a more secure and resilient digital ecosystem for the future.

References

[1] F. Fransen, A. Smahi, ..., ”Lessons learned from the WannaCry ransomware attack,” IEEE Security & privacy, 2018.

[2] K.PrivacyZ. Zhao, ..., ”Behind closed doors: measurement and analysis of CryptoWall ransomware in the U.S.,” in ProceedU.S. of USENIX Conference on Offensive Technologies (WOOT’16).

[3] J. Gardiner and D. Jamieson, ”The rise of cybersecurity counterintelligence: Attribution and the new normal in cyberspace,” Journal of Cyber Policy, 2020.

[4] P. Karanja, ”WannaCry ransomware statistics: Facts, figures, and cost,” Comparitech, Dec. 2019. Available: `https://www.comparitech.com/blog/information-security/wannacry-ransomware-statistics/`

[5] R. A. Grimes, ”Ransomware-resistant backup strategies,” CSO Online, Jun. 2017. Available: `https://www.csoonline.com/article/3199820/ransomware-resistant-backup-strategies.html`

[6] K. Parsons, A. McCormac, ..., ”The importance of staff awareness and teaching practice for countering phishing attacks,” in Proceedings of the 3rd International Conference on Cyber Security and Protection of Digital Services, (Cyber Security 2017).

[7] S. Khaleghian and S. Sallo, ”The UK’s NIS RegulatiU.K.’s A year in review,” Computer Fraud & Security 2019.

[8] M. Oltsik, ”The life and times of cybersecurity professionals 2018,” Enterprise Strategy Group, Inc., 2018.

[9] A. Azmoodeh, A. Dehghantanha, ..., ”Detecting crypto-ransomware in IoT networks based on energy consumption footprint,” Journal of Ambient Intelligence and Humanized Computing, 2020.

[10] M. Bromiley, ”Lessons from the WannaCry Incident,” 2017 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2017 4th IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, 2017

[11] Microsoft Security Response Center, ”Revoked MSFT Vulnerability,” Microsoft, Mar. 2017. Available: `https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144`

[12] N. Scheid, ”The WannaCry ransomware: analysis of the malware and vectors of infection,” ACM SIGSAC Conference on Computer and Communications Security (CCS 2017), 2017.