I Would Cry As well

Nicholas Gray

Old Dominion University

CS462

Nasreen Arif

04/10/2025

I Would Cry As Well

Introduction

WannaCry? There is no better name for this attack that left the United Kingdom's National Health Service and other organizations in shambles. On May 12th 2017, a global ransomware attack known as "WannacCry" was executed. WannaCry targeted old unpatched versions of Microsoft Windows which included Windows 7, Windows Server 2008, Windows XP, and Windows server 2003. This attack was massive before they knew it over 300,000 computers across 150 countries had been affected. Since WannaCry was a ransomware attack it encrypted files and demanded a ransom in bitcoin to be paid to get those files back. It has never been confirmed, but WannaCry is said to have been attributed to the Lazarus group which is a hacking organization in North Korea. The reason why the WannaCry ransomware attack is accredited to the Lazarus group is due to multiple pieces of evidence that would indicate it was them. There are code similarities between WannaCry's code and malware previously used by the Lazarus Group, the domains and servers used in WannaCry is also the sane as the infrastructure used by the Lazarus group and The ransom payments made in Bitcoin during the attack were traced to wallets connected to the Lazarus Group. A British cybersecurity researcher by the name of Marcus Hutchins had no intention of foiling the wannacry attack, but during his analysis of the malware, he discovered a kill switch within the code. The kill switch was a feature that checked whether a specific domain was registered. If the domain was active, the malware would stop spreading; if not, it would continue infecting systems. Marcus Hutchins noticed the unregistered domain

during his analysis and decided to register it to study the malware further, in doing so he accidentally stopped the spread of the ransomware attack. What a guy!

Vulnerability

How was the WannaCry ransomware attack possible? It's pretty simple, according to Waleed Alraddadi and Harshini Sarvotham "WannaCry malware exploits the vulnerability that is in the Server Message Block (SMB) protocol of the Windows implementation. SMB is a Transport protocol used for file sharing, printer sharing and access to remote services in Windows. SMB protocol operates over TCP ports 139 and 445." SMB is a protocol that allowed users to access many things remotely without directly using the physical system so the attackers were able to exploit to protocol to gain unauthorized access. The reason why the SMB protocol was able to be exploited is because of the creation of an exploit that was developed known as EternalBlue.

Exploit how it works

The EternaBlue exploit targets the vulnerability that lies within the SMB protocol of older versions of Windows. The EternalBlue Exploit was developed by the U.S. National Securty Agency (NSA) after they discovered the vulnerability. According to Manish Shivanadhan "it was part of their secret toolkit," and "became public when a hacker group called the Shadow Brokers leaked the NSA's tools." This is odd for a few reasons because had the NSA informed Microsoft of the vulnerability when they first discovered it, then WannaCry wouldn't be a thing or who knows maybe it would, but under a different attack vector. The EternalBlue exploits a flaw in the SMB protocol, allowing attackers to send specially crafted packets to a target system. Which in turn allowed them to gain unauthorized access and execute malicious code. EternalBlue was so effective because once an attacker gains access to a machine, EternalBlue can rapidly propagate through networks, infecting other vulnerable systems. As stated by Zian Liu

once EternalBlue is executed “it will send multiple SMB (Server Message Block) requests to the victim machine through the SMB protocol. As a result, the victim machine must respond to these requests.” The goal here clearly was to overwhelm the server using buffer overflow. EternalBlue is an exploit with so much appeal that it was also the star in other famous attacks like NotPetya and Bad Rabbit.

Impact

WannaCry affected more than 50 trusts within the United Kingdom’s National Health Service (NHS). At some point “more than 60 NHS trusts were hit” which meant “many facilities could not access patient records, which led to delays of non-urgent surgeries and cancelled patient appointments” (Collier, 2017). The staff had no access to patient records, appointment systems, communication tools (email), and diagnostic equipment. Many staff members had to revert to manual processes, using pen and paper for record-keeping and relying on personal mobile phones for communication due to the disruption of key systems. Any patients that had an emergency or in need of ambulance were being rerouted to facilities that were not affected by WannaCry. Something that is often overlook is the fact that many medical devices are connected to the network, if the network is down then NHS staff literally could not complete their job even if they wanted to. Not only was the United Kingdom’s National Health Service effected, WannaCry had also impacted FedEx, Deutsche Bahn, Nissan, and way much more. Fedex was hit and made a statement to remediate the problem. Deutsche Bahn is a German train station that was showing the railway operator's departure boards, but it wasn’t displaying the train schedules, instead it had the ransom demands. The impact that WannaCry had on Nissan was that all the production going on at their Sunderland plant in the United Kingdom had stopped. WannaCry infected over 300,000 computers and put a ransom to release the infected computer of $300 USD to be paid in bitcoin,

but they probably only amassed somewhere between $150,000 USD to $400,000. The full extent of the WannaCry ransomware attack isn't completely understood, but it's very easy to see why it's considered one of the largest cyber attacks in history.

Mitigations and Prevention

WannaCry could have been prevented if the NSA had made Microsoft aware of the vulnerability on SMB protocol on earlier versions of windows. Some things that would have enhanced the security and alleviated the problems associated with SMB are:

- **Applying security patches:** Ensuring all systems are updated with the latest security patches. Microsoft released a patch for the EternalBlue vulnerability in March 2017, two months before WannaCry struck.
- **Backup Data Regularly:** If an organization maintains secure and offline backups of critical data. This will ensure that even if ransomware encrypts files, data can easily be restored without paying a ransom.
- **Use Antivirus and Endpoint Protection**: Deploying antivirus software and endpoint protection tools to detect and block ransomware before it can execute.
- **Network Segmentation**: If an organization segments their network into smaller segments, it will help limit the spread of malware. This prevents an infection in one part of the network from affecting the entire system.
- **Disable SMBv1 Protocol**: Since WannaCry exploited the SMBv1 protocol using EternalBlue, disabling it can reduce the risk of similar attacks from reoccurring.
- **Implement Firewalls and Intrusion Detection Systems**: Use firewalls to block unauthorized access and intrusion detection systems to monitor and respond to suspicious activity.

- **Restrict Administrative Privileges**: Organizations need to adopt the concept known as least privilege. Limiting user access to only what is necessary for their role can help minimize the potential damage if an account is compromised. This will stop attackers from immediately having access to everything on the network.
- **Regular Penetration Testing**: The easiest way to stay ahead of attackers would be to conduct regular security assessments to identify and address vulnerabilities before attackers can exploit them. These assessments can be done internally, externally, or by bug hunters or maybe a combination of all them. It's better to be safe than sorry, clearly.
- **Incident Response Plan**: Develop and test an incident response plan to ensure a swift and effective reaction to ransomware attacks.

Going Forward, Lessons Learned

Ever since the WannaCry ransomware attack, the impact it has had then continues to affect life today for the better. Since that attack organizations have expressed their desire to increase their cybersecurity standards and procedures by:

1. **Focus on Healthcare Cybersecurity**: The United Kingdom's NHS's being taking down during the attack highlighted just how fragile the healthcare systems are in the face of cyber threats. This has directly led to increased investment in securing medical devices and infrastructure to protect patient care.
2. **Emphasis on Patching and Updates**: WannaCry's success was largely due to unpatched systems. Organizations are now more proactive in applying security updates and maintaining robust patch management processes.
3. **Increased Awareness of Cyber Threats**: WannaCry served as a wake-up call for governments, businesses, and the general public. It highlighted how

vulnerable critical systems are to cyberattacks, emphasizing the importance of staying vigilant and proactive.

4. **Global Collaboration**: The attack demonstrated the global nature of cyber threats, prompting international cooperation on cybersecurity policies, intelligence sharing, and law enforcement efforts.

References

Collier, R. (2017, June 5). NHS ransomware attack spreads worldwide. CMAJ : Canadian Medical Association journal = journal de l'Association medicale canadienne. https://pmc.ncbi.nlm.nih.gov/articles/PMC5461132/

Shivanandhan, M. (2023, September 11). EternalBlue Explained – An In-Depth analysis of the notorious Windows flaw. freeCodeCamp.org. https://www.freecodecamp.org/news/eternalblue-explained-an-analysis-of-the-windows-flaw/

Liu, Z. (n.d.). Working mechanism of EternalBlue and its application in Ransomworm. arXiv.org. https://arxiv.org/abs/2112.14773

Alraddadi, W., & Sarvotham, H. S. (n.d.). A comprehensive analysis of WannaCry: technical analysis, reverse engineering, and motivation. https://people-ece.vse.gmu.edu/coursewebpages/ECE/ECE646/F20/project/F18_presentations/Session_III/Session_III_Report_3.pdf