EternalBlue

EternalBlue is a very well known vulnerability throughout the cybersecurity world due to the actual impact it had. This vulnerability was discovered, and thought to have been developed by the National Security Agency (NSA), but was kept a secret for over five years. It then infamously manifested itself in the WannaCry and NotPetya cyberattacks in 2017 thrusting it into public view. But what is it and why is it so dangerous?

Technical Description

EternalBlue (CVE-2017-0144) utilizes a weakness in the Server Message Block (SMB) protocol version 1 to inject foreign code onto the targeted system. The SMB protocol enables file sharing by providing access to shared files, servers, printers and other ports on a network which makes it a prime target for possible attacks. This protocol is used mostly by Windows 7 or Windows Server 2008 operating systems but this vulnerability can also affect any computers running Windows 8 and 10 as well as servers running Windows Server 2012 or 2016. Therefore any machines running these operating systems are susceptible to this vulnerability.

The SMBv1 protocol is infiltrated when attackers manipulate how the protocol handles packets that are being transferred from one host to another. Packets are manipulated to shuffle around the data they are carrying in order to accommodate the malicious code that the attacker wants to be executed on the target device. The packet is then delivered to the device and the malicious code slips onto the device unnoticed. Once on the target device, the code can be executed to do anything the attacker desires including obtaining administrator access to all of the device's files. Once established on a device any sensitive data can be scraped, malicious software can be installed and the attacker can do virtually whatever they want with the infiltrated device.

Once the attacker has infiltrated a single device on a network the vulnerability can then be triggered to automatically expose all of the other devices that are on that network. The fact that this vulnerability can move across a network relatively easily makes it much more dangerous to any exposed organizations. In the many attacks that used this vulnerability, one of the key components was the ability for attackers to move across the network to either find the valuable sensitive information or capture as many devices as possible to increase the effectiveness of their attack.

EternalBlue Attack Examples

- **WannaCry:** This attack was a ransomware cryptoworm that would encrypt a user's information and then demand a Bitcoin ransom. WannaCry combines the EternalBlue vulnerability with a DoublePulsar backdoor tool. The EternalBlue vulnerability is used to gain access to a system using the SMB protocol described above. The code that is executed on the victim device is the DoublePulsar tool which creates a backdoor, enabling the ransomware to be executed on the device. Once the ransomware was installed the user's files would then be encrypted and a demand for the ransom of $300 to $600 in bitcoin would be made. Perhaps the most devastating part of the WannaCry attack was its ability to exploit the EternalBlue SMB vulnerability automatically. Once the ransomware was installed on a device it would use the SMB protocol to find other devices that the infected device was communicating with and

automatically exploit those devices as well. Due to its ability to spread over networks and even the internet automatically, hundreds of thousands of devices were affected.

- **NotPetya:** The NotPetya attack is very similar to WannaCry in that it uses the EternalBlue vulnerability to spread a type of ransomware, in this case, a modified version of Petya. NotPetya is thought to have originated in an update to Ukrainian tax accounting software called MeDoc. It was placed here because of the widespread use of the software around the country. NotPetya uses EternalBlue to inject code that encrypts the Master File Table of a device and forces the device to restart. Once the device restarts it is locked with a message demanding a ransom. This attack, however, did more than just encrypt the files, it damaged most of them and made a large portion of them unrecoverable. The EternalBlue vulnerability was again used to spread the ransomware across networks. Any devices that shared files with the infected computer were also infected via the SMB protocol being exploited.

Resolution

In response to the vulnerability being made public Microsoft issued security bulletin MS17-010 which outlined the issue and the patches that were being released to address the problem. However, many users did not install the patches in a timely manner and this led to many of the before mentioned well-known attacks that exposed the vulnerability. In response to these large scale attacks, Microsoft released emergency security patches to cover all unsupported Operating Systems to help mitigate the potential fall out of these large scale attacks.

Risk Assessment

The EternalBlue exploit affects a broad range of Windows operating systems which many organizations depend upon for their day to day business. These include Windows 7 all the way up through some versions of Windows 10.

The EternalBlue vulnerability is labeled “severe” by NIST CVSS Standards. The Common Vulnerability Scoring System (CVSS) exists to help organizations understand and evaluate the seriousness of specific vulnerabilities. The final score of each vulnerability is determined based on eight different variables. Higher scores represent more serious dangers. The max score is 10.

1. Attack Vector – Medium through which exploitation is possible
2. Attack Complexity – Complexity involved in exploitation
3. Privileges Required – Privileges required for exploitation
4. User Interaction – Can be exploited without user
5. Scope – Whether it affects other vulnerable components
6. Confidentiality – Impact to confidentiality
7. Integrity – Impact on trustworthiness of information
8. Availability – Impact to availability of impacted component

EternalBlue’s CVSS score is an 8.1/10. This high score helps us to understand the severity and danger related to the exploit. This score comes from the fact that it can be exploited through network access, requires no elevated permissions or user interaction, and presents a high risk to confidentiality,

integrity, and availability. The only vectors which keep EternalBlue from reaching a score of 10 are Attack, Complexity, and Scope.

Threats

In the days following The Shadow Broker's release of EternalBlue in April 2017, security experts began to see it used to "extract passwords from browsers, and to install malicious cryptocurrency miners." While these uses may seem alarming enough on their own, what came next was on a whole other level.

In May 2017, the world was attacked by a piece of ransomware called WannaCry. This ransomware utilized EternalBlue to spread quickly and infiltrate many different flavors of the Windows Operating System. Once it had successfully entered into a system, it would encrypt all files and show a ransom demand on the screen. After encryption completed, the only way to remedy them was to pay the ransom and hope that the hackers would send the unlock key.

The incredible speed at which WannaCry was spreading called much attention to it and a fix, unrelated to EternalBlue, was quickly found by a British security researcher. In November 2017, after being attacked by WannaCry, the NHS said "the [attack] had potentially serious implications for the NHS and its ability to provide care to patients"[1].

NotPetya

Within a month of WannaCry's initial release, another piece of ransomware called NotPetya was released in the Ukraine. NotPetya utilized the same EternalBlue exploit with a bit of a twist. Unlike WannaCry, NotPetya could "spread within corporate networks, but without [jumping] from one network to another."[2] This strategy kept it from gaining the unwanted attention that WannaCry gained. According to CBS News[3], "FedEx, Merck, and Maersk, the world's largest shipping firm. Ultimately it caused more than $10 billion in damage."

Healthcare Industry Effect

As outlined above in greater detail, the EternalBlue vulnerability is very versatile. Because it merely allows malicious individuals to run their code on vulnerable computers it provides a very broad threat to businesses. Not only can it be used to open a computer up for a large ransomware attack, but it can be used to install software, turn a computer into a zombie cryptocurrency miner, or any other number of things. Due to the breadth of potential attacks, there isn't a single business process that wouldn't be affected by a significant EternalBlue attack.

Ransomware

Both WannaCry and NotPetya (explained above) are excellent examples of what a vulnerability like EternalBlue can do to a business. In both cases, the vulnerability was used to initiate severe ransomware attacks and essentially shut down the digital infrastructure of targeted businesses. Such an attack can cripple a business. Without access to records saved on a computer or server a business can no longer track sales or purchases, access important administrative documents, look up customer/client data or

[1] https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/
[2] https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware
[3] https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/

anything else. Because healthcare organizations are very reliant on digital record-keeping, severe ransomware attacks can temporarily freeze virtually all business processes for those companies. Until the attack is resolved and the data is restored the revenue cycle would come to a virtual standstill as data relating to orders would be inaccessible; the expenditure cycle would also suffer because financial records, budgets, and purchase records would be either permanently or temporarily lost.

Data Breaches

In addition to being used for ransomware attacks, EternalBlue is a vulnerability that could potentially be used for a data breach like the 2013 Target data breach. In the case of a significant data breach, an organization's customer base would be greatly affected. Millions of healthcare records and sensitive financial information could be leaked. The targeted company would likely suffer from damage to their reputation, a decrease in business, and the cost of securing the system to deter future attacks.

Risk Management

The EternalBlue vulnerability can be mitigated by thorough implementation of security frameworks and internal controls. Healthcare organizations that carefully apply the NIST Cyber Security Framework (CSF), are HIPAA compliant, and establish secure internal controls will greatly reduce the severity of the EternalBlue vulnerability.

NIST Cyber Security Framework

Since 2017, more than 40%[4] of healthcare organizations have been affected by the EternalBlue vulnerability. This vulnerability resulted in various attacks, such as WannaCry, NotPetya, and BadRabbit ransomwares, and the EternalRocks computer worm. The average healthcare organization spends $1.4 million to recover from a cyber attack[5].

Currently, almost 60%[6] of healthcare organizations have implemented the NIST CSF. This framework focuses on improving risk assessment and responding to cyber attacks. The core functions of the NIST CSF, as well as how they help reduce the EternalBlue vulnerability are listed below:

- **Identify**. This function is invaluable for organizations to identify and assess their system for possible vulnerabilities. Specifically, within the identify function, there are three different steps that help an organization identify a susceptibility to the EternalBlue vulnerability. The first is Asset Management. During the Asset Management phase, CISOs and analysts can look at current systems and hardware and check to make sure that they are up to date and secure from the EternalBlue vulnerability. Second, is Risk Assessment. During this phase, an organization can look at the risk of EternalBlue and decide if it should be addressable or not. Lastly is Risk Management Strategy. Depending on the level of risk assigned to EternalBlue, management can decide on next steps to controlling for the EternalBlue vulnerability.
- **Protect**. During this stage of the NIST CSF, management implements the necessary change to protect against EternalBlue. This could include requiring weekly updates on all systems and hardware. It might also be installing protective software like McAffee or BitLocker. Another

[4] https://www.hipaajournal.com/40-of-healthcare-delivery-organizations-attacked-with-wannacry-ransomware-in-the-past-6-months/
[5] https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery
[6] https://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/

method of protection is creating a training to help employees understand the risks and likelihoods of cyberattacks and helping them become aware and careful in their online activity.

- **Detect**. This phase includes monitoring systems and logging any suspicious activities or behavior. Monitoring will help protect the system and prevent infected machines exploiting other machines via the EternalBlue vulnerability.
- **Respond**. During this stage of the NIST CSF, management creates a response plan or executes a previously-created plan. This could involve isolating a system or using intensive forensics to uncover the source of the attack.
- **Recover**. Now that the organization has been able to respond from the vulnerability, the best course of action is to make improvements and standards to implement going forward. The goal is to become even more secure and prevent additional incidents from occurring in the future.

The NIST CSF is most effective in reducing the severeness of the EternalBlue vulnerability in the first two stages, identify and protect. Management should be very aware and engaged in those periods, because preventing an attack is significantly better than responding to the vulnerability and recovering.

HIPAA

Being HIPAA-compliant in the healthcare industry is a top priority, as customers expect their medical and financial information to be well protected and secure. Rigorously applying technical and physical safeguards greatly enhances an organization's ability to prevent EternalBlue vulnerabilities and avoid subsequent cyber attacks.

These safeguards include: access controls, audit controls, integrity, person or entity authentication, and transmission security. Physical controls include facility access, workstation use, workstation security, and device and media controls. Effective use of these safeguards help protect against lateral movement inside a system if exposed to the EternalBlue vulnerability. The most important of these safeguards will be addressed below:

- **Transmission security**. Establishing thorough transmission security controls prevent lateral movement within a system/network. These include firewalls, authentication, and data security. This helps protect systems when executable packets are sent within the EternalBlue vulnerability.
- **Workstation security**. Appropriate workstation security is essential to preventing EternalBlue. Most applied to the EternalBlue vulnerability is regular updates and system monitoring. Consistent patch updates and monitoring workstations will go a long way in preventing access via EternalBlue.

Internal Controls

The best internal controls[7] currently implemented by healthcare organizations to reduce the possibility of EternalBlue vulnerability are:

- Regular update policies. As soon as software patches are released, management must make system updates a top priority.
- Anti-virus software. Up-to-date anti-virus software is key for monitoring and detecting intrusion and attacks that can result from the EternalBlue vulnerability.

[7] https://www.ncua.gov/newsroom/ncua-report/2017/protect-your-systems-against-eternalblue-vulnerability

- Access privileges. Instituting the practice of least-privilege access helps manage the use of administrative functions and helps keep the entire system more secure. Attackers will be more hard-pressed to get access, in addition to finding admin access by properly implementing least-privilege.
- Educate employees. Educating employees helps organizations to have a smarter and more aware internal force. Practicing with employees to avoid suspicious emails and links will better the company in the long term.

Other internal controls could be implemented by looking at Center for Internet Security (CIS) controls. The CIS controls[8] are a priotized set of actions designed to protect organizations and data from known attack vectors. Secure actions from the CIS controls to ensure in healthcare organzations would be:

1. Malware defenses,
2. Data recovery capabilities,
3. Data protection,
4. Application software security, and
5. Incidence response and management

Summary

In sum, the EternalBlue vulnerability is most severe when dealing with out of date software, ineffective controls, and unaware management. Rigorously applying the NIST CSF, technical and physical safeguards from the HIPAA, and proper internal controls will protect organizations from $1.4 million dollar costs from a cyberattack instituted through the EternalBlue vulnerability.

[8] https://calcomsoftware.com/cis-controls-how-to-approach-them/