# Eternal Blue


By Justin Loke – 3rd February 2019.

## Introduction

**EternalBlue** refers to software vulnerability in Microsoft's Windows operating system (**EternalBlue MS17-010**). The Eternal Blue enables hackers to remotely execute arbitrary codes and gain access to a specific network by sending crafted packets. It exploits through Microsoft's Windows Operating System (OS) **Server Message Block (SMB)** version 1 protocol which a network file is sharing protocol that allows access to files on a remote server. Exploiting through the SMB enables malwares utilizing Eternal Blue exploit to spread to all devices connecting to the compromised network. (Primer, 2019)

The original code dropped by "Shadow Brokers" contained 3 additional "Eternal" exploits that are known as **Eternalromance**, **Eternalsynergy** and **Eternalchampion**. Another variant is known as **EternalRocks** which utilized up to 7 exploits. (SentinelOne, 2019)

The famous ransomware, WannaCry which is a crypto-ransomware utilizes this Eternal Blue exploit to spread. The ransomware spreads itself across the network and infecting every electronic devices connected to the compromised network. Other form of malwares such as Trickbot (Modular banking Trojan), CoinMiner and WannaMine that are in short cryptominers that utilizes EternalBlue exploit to gain access to devices to mine cryptocurrencies. (Primer, 2019)

## History

The history of EternalBlue exploit was initially leaked by "The Shadow Brokers" group on April 14, 2017. The leak involved various exploitation tools including EternalBlue that were based on the SMB protocol.

Next, EternalBlue exploit works on all Windows operating system versions prior to Windows 8. These versions are able to contain an interprocess communication share [IPC$] that allows a null session. This results in enabling an established connection through anonymous login and null session to be allowed by default. Null sessions allow the client to send different commands to the server.

Microsoft released patches for the vulnerabilities involved in the leak under the name "**MS17-010**". The CVE related to the EternalBlue in MS17-010 is **CVE-2017-0144**. (Grossman, 2017)

## How Does EternalBlue works?

Based on the article by SentinelOne, EternalBlue requires using a Windows function named "**srv!SrvOS2FeaListSizeToNt**". (SentinelOne, 2019)

EternalBlue mainly takes advantage through 3 different bugs:

1) Mathematical error when the protocol tries to cast an OS/2 FileExtended Attribute (FEA) list structure to an NT FEA structure in order to determine how much memory to allocate. A miscalculation error results in creating an integer overflow that will cause less memory to be allocated than expected which leads to what is known as a **buffer overflow**. Having more data written than expected, the extra data can overflow into an adjacent memory space. (SentinelOne, 2019)

2) The second bug enables the **buffer overflow** to be triggered. This is due to the difference in the SMB protocol's definition of 2 related sub commands (**SMB_COM_TRANSACTION2** and **SMB_COM_NT_TRANSACT** ). Both commands have _SECONDARY command that is utilized when there is too much data to include in a single packet. The main difference between **TRANSACTION2** and **NT_TRANSACT** is that the latter calls for a data packet having twice the size of

the former. This proves to be significant because a validation error occurs if the client intends to send a crafted message using the **NT_TRANSACT** sub-command before the **TRANSACTION2** command. While the SMB protocol recognizes that 2 separate sub-commands have been received, it will assign the type and size of both packets (allocates memory accordingly) based on the type of the previous packet received. Since the last packet received is smaller, the first packet will occupy more space than it is allocated. (SentinelOne, 2019)

**3)** When the attacker has managed to achieved the initial overflow from the previous 2 bugs, they will proceed to exploit through the 3rd bug within the **SMBv1** which allows heap spraying. Using heap spraying, the attacker is able to write and execute shellcode to gain control of the system. (SentinelOne, 2019)

## Eamples of EternalBlue variants

The table below show the types of malwares using EternalBlue exploit.

**Table 1: Types of malware using EternalBlue exploit.**

| Name | Description |
|---|---|
| **WannaCry/WannaCryptor** | Ransomware that uses EternalBlue exploit. |
| **EternalRocks** | Utilizes up to 7 exploits. (SentinelOne, 2019) |
| **Yatron** | Ransomware that uses EternalBlue and DoublePulsar exploits to spread to other devices on a network. (Abrams, 2019) |
| **Trickbot** | A modular banking Trojan. (Primer, 2019) |
| **CoinMiner** | Utilizes EternalBlue exploit to gain access to devices to mine cryptocurrencies. (Primer, 2019) |
| **WannaMine** | Utilizes EternalBlue exploit to gain access to devices to mine cryptocurrencies. (Primer, 2019) |

## Recommendations

The steps below are some of the advices given from cyber security researchers on preventing from being affected by EternalBlue.

- Update devices with Microsoft Windows OS with the latest security update for Microsoft Windows SMBv1.
- Depending on situations, disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
- Utilize Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communication to client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At minimum, create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Apply the Principle of Least Privilege to all systems and services and run all software as a non-privileged user (one without administrative privileges).

(Primer, 2019)

**Keywords**

| Name | Description |
|---|---|
| **Heap spraying** | Refers to a technique causes allocating a chunk of memory at a given address. (SentinelOne, 2019) |
| **SMB** | SMB is Server Message Block Protocol. It refers to a client-server communication protocol used for sharing access to files and devices on a network. The protocol can carry transaction protocols for interprocess communication. (Rouse, 2020) |
| **Ransomware** | A form of malware that encrypts a victim's files. The attacker/hacker will demand a ransom from the victim in order to restore access to the encrypted data upon payment. (Fruhlinger, 2018) |
| **Buffer Overflow** | A buffer overflow occurs when more data is loaded into a fixed-length buffer which is more than the buffer can process. The extra |

| | |
|---|---|
| | information causes to overflow into adjacent memory space, corrupting or overwriting the data stored in that space. This overflow results typically in a system crash but creates an opportunity for hackers to run arbitrary code or manipulate coding errors to perform malicious actions. (VERACODE, 2020) |

## Works Cited

Abrams, L. (12 March, 2019). *Yatron Ransomware Plans to Spread Using EternalBlue NSA Exploits*. Retrieved 3 February, 2020, from BLEEPINGCOMPUTER: https://www.bleepingcomputer.com/news/security/yatron-ransomware-plans-to-spread-using-eternalblue-nsa-exploits/

Fruhlinger, J. (19 December, 2018). *Ransomware explained: How it works and how to remove it*. Retrieved 3 February, 2020, from CSO: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Grossman, N. (29 September, 2017). *EternalBlue – Everything There Is To Know.* Retrieved 3 February , 2020, from research.checkpoint.com: https://research.checkpoint.com/2017/eternalblue-everything-know/

Primer, S. (January, 2019). *EternalBlue.* Retrieved 3 February, 2019, from www.cisecurity.org: https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf

Rouse, M. (2020). *Server Message Block Protocol (SMB protocol)*. Retrieved 3 February, 2020, from TechTarget: https://searchnetworking.techtarget.com/definition/Server-Message-Block-Protocol

SentinelOne. (27 May, 2019). *Eternalblue | The NSA-developed Exploit That Just Won't Die*. Retrieved 3 February, 2020, from SentinelOne: https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

VERACODE. (2020). *WHAT IS A BUFFER OVERFLOW? LEARN ABOUT BUFFER OVERRUN VULNERABILITIES, EXPLOITS & ATTACKS*. Retrieved 3 February, 2020, from VERACODE: https://www.veracode.com/security/buffer-overflow