WannaCry Ransomeware Attack and Eternal Blue

Emil Jonsson(emijonss), Max Oesterle, Ronghua Li

May 27, 2020

1 Introduction

In May 2017 Windows machines were targeted by a ransomware cryptoworm nicknamed WannaCry. It encrypted all files on the targeted machine and demanded 300$ in bitcoin be paid to a specified bitcoin wallet within a couple of days. The problem with this attack was that it could self propagate through a known vulnerability called EternalBlue (precisely CVE-2017-0145) using the publicly know dropper DOUBLEPULSAR, which caused it to spread quickly both on the local network and to random vulnerabe computers on the internet. It disrupted organizations worldwide with over 200,000 infected computers and caused up to 4 billion dollars of damage [1]. Once a computer was affected a note was left on the machine explaining what had happened and giving instructions on how to pay with bitcoins to get the decryption key.

2 Spreading Mechanism

WannaCry scans the local network and random IP addresses for victims being vulnerable to EternalBlue. Once it has found a vulnerable IP address, it tries to infect the new victim and, if successful, runs modified code from the DOUBLEPULSAR backdoor on kernel level to drop its payload [7].

3 EternalBlue

EternalBlue is an exploit developed by the United States National Security Agency. It takes advantage of Microsoft's implementation of the Server Message Block (SMB) and can lead to arbitrary code execution on machines running the unpatched version of SMBv1 on Windows 7 or Windows Server 2008 and earlier [3].

EternalBlue exploits 3 different bugs in Microsoft's SMB implementation by sending specially crafted messages to the SMBv1 server [3]. The vulnerability was found several years before the WannaCry attack and kept secret by the NSA to make use of it in their own offensive operations. The hacker group Shadow Brokers, which is believed to operate from Russia [8] stole the NSA's exploit amongst others from the NSA in early 2017, causing them to notify Microsoft. Shadow Brokers leaked the exploit to the public about a month after Microsoft issued a patch in April 2017.

3.1 Bug 1 - Casting

The first bug occurs while converting a list of file extended attributes (FEA) into a different format. When updating the list's size (a 32-bit ulong), the size value is updated as if it was a 16-bit ushort. That means that the most significant 16 bits are not updated and the remaining size value is way larger than the actual allocated buffer size, which leads to a buffer overflow on the heap. The bug occurs for size values greater than or equal 2^{16} [6].

This bug could be found by a static code analysis tool which is checking unsafe parsing between types or a fuzzer tool which fuzzes the list size, combined with a dynamic checking of buffer accesses like valgrind does.

3.2 Bug 2 - Parsing

The second bug allows to trigger bug 1. It uses the SMB transaction sub-commands which basically split a sub-command (respectively its data) into multiple requests if the data to be sent exceeds a certain value. First, a primary transaction request is sent, followed by multiple secondary transaction requests. The exploit uses two different types of the transaction function, Trans2 and NT Trans. The field specifying the amount of data which can be sent is located in the request header. For the NT Trans version this field has the size DWORD, for the Trans2 version it has the size WORD. The amount of data which can be sent therefore differs. Also, no validation exists if the secondary request matches the previous request. It is possible to send a NT Trans primary request followed by a Trans2 secondary request. The Trans2 request will be parsed as a NT Trans request which means that its WORD-sized header field will be treated as a DWORD field. Bug 1 is triggered [3].

This parsing bug might have been found by verifying the processing of different possible request orders. The request order leading to wrong parsing would have triggered bug 1 which than could have been backtracked to wrong parsing.

3.3 Bug 3 - Allocation

The overflow mentioned above occurs in a large non-paged pool structure in memory. Large non-paged pools do not have pool headers. Therefore, a tightly connected pool can be allocated after a previous pool which contains driver data. In the heap grooming phase, a hole is left to be filled by a specified size of data later. However, when FEA list transforms into NTFEA list, the data size is actually way more larger than the allocated hole, which would cause out of bound writes to the next chunk. This will then lead to the data overflow to the vulnerable buffer where attacker can execute malicious code [5].

4 Solution

WannaCry had a built in kill switch where it attempted to poll a specific ip-address before running. If this domain was found the program would stop, otherwise it would attempt to spread. The kill switch was found by a malware analysis expert named MalwareTech who decided to register the domain and hereby stopped the spread [4]. The stop was only temporary since simply removing the code which queried the domain removed the kill switch. Nonetheless, it probably saved billions of dollars of damage by giving potential victims time to remove the vulnerability.

Microsoft released patches for Windows XP, 7, 8, and Windows Server 2003 which fixed the EternalBlue bugs. Reports from two years after the incident claim that around a million computers are still vulnerable to EternalBlue and the vulnerability is still actively use for exploits and WannaCry-like ransomware.[2]

References

[1] Jonathan Berr. “”WannaCry” ransomware attack losses could reach $4 billion”. In: (May 16, 2017). URL: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses.

[2] Catalin Cimpanu. “One Year After WannaCry, EternalBlue Exploit Is Bigger Than Ever”. In: (May 11, 2018). URL: https://www.bleepingcomputer.com/news/security/one-year-after-wannacry-eternalblue-exploit-is-bigger-than-ever/.

[3] Nadav Grossman. “EternalBlue – Everything There Is To Know”. In: (Sept. 29, 2017). URL: https://research.checkpoint.com/2017/eternalblue-everything-know/.

[4] MalwareTech. “How to Accidentally Stop a Global Cyber Attacks”. In: (May 13, 2017). URL: https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

[5] William Gamazo Sanchez. “MS17-010: EternalBlue’s Large Non-Paged Pool Overflow in SRV Driver”. In: (June 2, 2017). URL: https://blog.trendmicro.com/trendlabs-security-intelligence/ms17-010-eternalblue/.

[6] Microsoft Defender ATP Research Team. "Analysis of the Shadow Brokers release and mitigation with Windows 10 virtualization-based security". In: (May 13, 2017). URL: https://www.microsoft.com/security/blog/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security.

[7] Microsoft Defender ATP Research Team. "WannaCrypt ransomware worm targets out-of-date systems". In: (May 13, 2017). URL: https://www.microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems.

[8] zerosum0x0. *DEF CON 26 - Demystifying MS17-010 Reverse Engineering the ETERNAL Exploits*. 2018.