Graham Dungan
February 9, 2025
UIN: 332001764

CSCE 413: Software Security
Self-Study: WannaCry

What is the Vulnerability?
WannaCry is a ransomware worm that exploited Windows operating systems in May 2017. The WannaCry worm would enter a machine, establish a foothold, encrypt all files, and hold the system at ransom, only offering decryption if a payment was made to a Bitcoin wallet.

What was the Root Cause?
The root cause of WannaCry's dissemination was the leak of multiple NSA exploits by a group called the Shadow Brokers. The exploitative software used as part of the attack was EternalBlue and DoublePulsar.

EternalBlue exploited a SMBv1 protocol buffer overflow exploitation that allowed for remote code execution on remote machines. EternalBlue was used for lateral movement through networks, disseminating the WannaCry ransomware across machines.

DoublePulsar is a post-exploitation backdoor that stealthily implements itself within a compromised system allowing payloads to be deployed. DoublePulsar could inject malware directly into memory, which helped it evade antivirus software.

Effectively, EternalBlue was used to spread to other machines, DoublePulsar was used to stealthily establish footholds among these machines and to deploy the WannaCry ransom software.

What is the Extent of its Impact?
Overall, the WannaCry attack was estimated to have infected more than 300,000 computers across 150 countries. While the response to mitigating WannaCry was swift, much of its spread was due to the lack of security updates being applied to Windows systems.

The National Health Service in England and Scotland found most of their technologies were compromised, leading to a mass disruption of their services across both countries. After some investigation, it was found that thousands of computers within this organization were still running Windows XP and were, thus, very much vulnerable to these exploits.

Automotive manufacturing plants, cellular providers, mailing services, power plants, and critical city infrastructure were also greatly affected by these attacks. It is important to note the correlation of organizations that have historically used out-of-date technologies and the prevalence of WannaCry instances.

How to Patch it?
Within a few hours of WannaCry's outbreak, researcher and cybersecurity blogger Marcus Hutchins found a hard-coded kill switch within the malware. Hutchins found that before WannaCry ran, it would attempt to ping a domain. If the WannaCry ransomware could not connect to the domain (by default the domain was not registered and did not receive any connections), it would run on the machine. Hutchins then purchased this domain and created a DNS sinkhole, preventing the further dissemination.

Researchers at the University College London and Boston University created a software called "PayBreak" which could reportedly reverse the damage done by WannaCry (and other ransomware services) by obtaining the keys used for the encryption.

Following, a French developer created "WannaKey", a software solution that attempted to find the two prime numbers used in the generation of the RSA key for encryption via searching through cached memory.

Ultimately Windows released MS17-010, a patch fixing the SMBv1 vulnerability that EternalBlue exploited as well as other SMB-related vulnerabilities.

How Could it Have Been Prevented?
The most direct reasoning as to how this vulnerability occurred was due to the overflow vulnerabilities found in SMBv1 as well as the SMBv1 protocol being accessed over the internet (by which its protocol was not designed to do, nor was it secure).

However, beyond the immediate cause of WannaCry's dissemination by using EternalBlue, many have come to scrutinize the security and storage of vulnerabilities and exploits under the NSA. If the NSA had privately divulged these vulnerabilities to Microsoft, rather than attempt to hold onto them for defense, this entire attack could have been mitigated.

References

1. WannaCry ransomware attack - Wikipedia
2. DNS Sinkhole - Wikipedia
3. EternalBlue - Wikipedia
4. EternalBlue Exploit: What It Is And How It Works - SentinelOne
5. DoublePulsar Backdoor - NHS England