Case Study: The WannaCry Ransomware Attack

Prepared by: Rameen Mughal
Date: August 5, 2025

I. Executive Summary

The WannaCry ransomware attack, launched on May 12, 2017, quickly became one of the most significant cybersecurity incidents in history, affecting over 200,000 computers across more than 150 countries. The attack disrupted operations in major organizations including FedEx, Honda, Nissan, and the UK's National Health Service (NHS). WannaCry is a self-propagating malware classified as crypto-ransomware, a type of malicious software specifically designed to perform harmful actions on computer systems. In this case, it encrypted users' files and demanded payment in Bitcoin for decryption keys, with the primary goal of extorting money from victims in exchange for access to their data. Although a security researcher was able to discover a kill switch that limited further spread, the damage had already been done. The primary impact was on the availability of systems and data.

II. Introduction

This report analyzes the WannaCry ransomware attack by examining its Tactics, Techniques, and Procedures (TTPs), the CIA Triad component compromised, the vulnerability exploited, and the broader implications for cybersecurity. The goal is to understand how this attack occurred and how similar incidents can be prevented.

III. Case Overview

WannaCry is a malware that is classified as a crypto-ransomware which is defined as a software that encrypts users' files and demands them to pay some amount of money in exchange to decrypt their files. The purpose of this kind of malwares is money extortion. Crypto-ransomwares use shock and fear tactics to push users to pay the required ransom for instance in WannaCry, such tactic is being implemented by showing a three-day countdown and threatening the user that the decryption key will be deleted if he didn't pay on time. WannaCry first time seen in the wild on May 12, 2017[1]. WannaCry is considered the biggest ransomware outbreak in the history. It had infected more than 200,000 computers in over 150 countries. WannaCry uses Tor hidden services for its C & C (command and control) communications. The main purpose of the C & C in WannaCry is to check if the victim has paid the ransom and delivering the decryption key.

IV. SMB Vulnerability

The 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. The malware makes use of the Vulnerability in SMB Version 1 (SMB v1) and TCP port 445 to propagate. This vulnerability allows malformed packets from the remote attackers to execute

arbitrary code on the victim's computer. This vulnerability allows malformed packets from the remote attackers to execute arbitrary code on the victim's computer.

The vulnerability exploited was identified as CVE-2017-0144, a flaw in SMBv1 that allowed remote code execution. This vulnerability was weaponized through the EternalBlue exploit, which had been developed by the NSA and later leaked by the Shadow Brokers hacking group. Despite Microsoft releasing a security update (MS17-010) to fix this issue two months before the attack, many systems remained unpatched. The CVSS (Common Vulnerability Scoring System) score assigned to CVE-2017-0144 was 8.1, categorizing it as a critical vulnerability due to its ease of exploitation and severe impact on affected systems.

EternalBlue is a critical exploit developed by the NSA and later leaked by the Shadow Brokers, which targets a vulnerability in Windows SMBv1 (CVE-2017-0144) to allow remote code execution over TCP port 445 without authentication.

V. TTP (Tactics, Techniques and Procedure) Analysis

Tactics: The attackers employed several tactics including *Initial Access* to infiltrate systems, *Execution* to run malicious code, *Lateral Movement* to spread the infection across networks, and *Impact* to disrupt normal operations by encrypting files.

Techniques: They exploited a known vulnerability in SMBv1 using the EternalBlue exploit to gain unauthorized remote access. Upon entry, a dropper was used to deploy the ransomware payload. The malware demonstrated worm-like behavior by scanning and infecting other systems on the same network via TCP port 445.

A dropper is a type of malware that is designed to install or "drop" another malicious program (often more dangerous) onto a target system.

Procedures: The attack began by identifying unpatched Windows machines with SMBv1 enabled. EternalBlue was used to exploit CVE-2017-0144, allowing remote code execution. Once inside, WannaCry deployed its ransomware payload, encrypted users' files, and displayed a ransom demand. It then searched for additional vulnerable machines on the network by DoublePulsar backdoor and repeated the infection process, resulting in rapid and widespread disruption.

VI. CIA Triad Impact Analysis

WannaCry ransomware attack was neither stolen nor altered, confidentiality and integrity were not the main targets. Instead, the attack primarily compromised the availability aspect of the CIA Triad. By encrypting files and locking users out of their systems, WannaCry caused major disruptions, especially in healthcare, where hospitals had to cancel appointments and redirect ambulances. This loss of access to critical data and services highlights a clear breach of availability.

VII. Motive

The main motive for the attackers was the money extortion. The attackers extorted only $140,000 worth of Bitcoin after infecting more than 200,000 computers by August 2017. This amount of money had been collected via only three bitcoin addresses. Money gained by this attack is considered a failure in terms of ransomwares, and in comparison, with number of computers that had been infected by the malware.

One political motive is also considered as WannaCry attack have been linked to Lazarus group. Lazarus group is a North Korean cybercrime group which believed to be sponsored by the North Korean Government. This group have been accused of mounting several major cyber-attacks including the famous Sony Pictures hacking in 2014, and the $81 million Bangladesh central bank heist in 2016. Semantic and Kaspersky (major information security firms) have found similar pieces of code that had been used in previous attacks. For instance, the wiping tool of WannaCry is the same tool that had been used in the Sony Attack.

At the end, we have reached to a surprising conclusion that WannaCry is actually a cyberweapon and not just ransomware which means the main goal behind the attack is destruction and not money gain. This is also one of the reasons that makes WannaCry stands out from other malwares.

VIII. Detection & Response

The WannaCry ransomware attack was detected when systems across various organizations began displaying ransom notes and became inaccessible due to file encryption. Many organizations realized they were under attack only after widespread disruption had already occurred. In a fortunate turn of events, a cybersecurity researcher accidentally discovered a kill switch embedded in the malware, a domain that, when registered, stopped the ransomware from further propagating. This significantly slowed the attack, though it did not decrypt the already infected systems. Despite this, thousands of systems remained locked, and some organizations resorted to paying the ransom while others attempted data recovery through backups and forensic investigation.

IX. Conclusion

The WannaCry ransomware attack highlighted how unpatched systems and poor security hygiene can lead to large-scale disruptions. Though not targeting data confidentiality or integrity, the attack paralyzed essential services, showcasing a serious breach of availability. Future incidents can be mitigated by staying updated on vulnerabilities, investing in cybersecurity training, and maintaining robust incident response protocols. A few lessons

learnt from this attack: updating the system regularly and keeping backup files on an external medium are essential to mitigate the effects of such attacks.

X. References

- A Comprehensive Analysis of WannaCry: Technical Analysis, Reverse Engineering, and Motivation - Waleed Alraddadi, and Harshini Sarvotham
- WannaCry Ransomware Attack – Wikipedia
- Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) – Exploit DB