EternalBlue Exploits

A case study of a malware family

ANURAG MALYALA

2K15/CO/035

Cyber Forensics IT-312(A)

EternalBlue Exploits

A family of malwares that keeps on giving

ETERNALBLUE, is an exploit developed by the U.S. National Security Agency (NSA) according to testimony by former NSA employees. [1]. It was leaked by the Shadow Brokers hacker group on April 14, 2017 and was used as part of the worldwide WannaCry ransomware attack on May 12, 2017. The exploits were also used to help carry out the 2017 NotPetya cyberattack on June 27, 2017 and reported to be used as part of the Retefe banking trojan since at least September 5, 2017.

Introduction

EternalBlue is the name given to a software vulnerability in Microsoft's Windows operating system. The tech giant has called it EternalBlue MS17-010 and issued a security update for the flaw on March 14. The vulnerability works by exploiting the Microsoft Server Message Block 1.0. The SMB is a network file sharing protocol and "allows applications on a computer to read and write to files and to request services" that are on the same network.

SMB provides support for what are known as SMB Transactions. Using SMB Transactions enables atomic read and write to be performed between an SMB client and server. If the message request is greater than the SMB MaxBufferSize, the remaining messages are sent as Secondary Trans2 requests. This vulnerability affects the srv2.sys kernel driver and is triggered by malformed Secondary Trans2 requests.

Working [2]

After the initial SMB handshake, which consists of a protocol negotiate request/response and a session setup request/response, the ransomware connects to the IPC$ share on the remote machine. Another related aspect of this attack is that the malware is configured to connect to a hardcoded local IP

Next it sends out an initial NT Trans request, which is a huge payload size and consists of a sequence of NOPs. What it essentially does is move the SMB server state machine to a point where the vulnerability exists so that the attacker can then exploit it using a special crafted packet.

Speaking the SMB language, the large NT Trans request leads to multiple Secondary Trans2 Requests to accommodate for the large request size. These Secondary Trans2 requests are malformed. They act as a trigger point for the vulnerability, and the request data portion contains the shellcode and encrypted payload, which is the launcher for the malware on the remote machine.

On successfully triggering the vulnerability, an encrypted payload containing the stager for the malware is loaded on the remote machine. The payload delivered to the remote machine launches a service “mssecsvc” from within the lsass process. This service scans the local network and the internet for machines that are accessible and have exposed SMB ports. The service then uses the vulnerability to gain access to a remote machine and deliver the malware payload, thus completing the full cycle. All these activities happen very quickly, and the attack penetrates all machines in a typical LAN within minutes.

According to Microsoft, it was the US's NSA that was responsible, by dint of its controversial strategy of "stockpiling of vulnerabilities", for, at the least, preventing Microsoft from timely public patching of this, and presumably other, hidden bugs [3]

Case 1:

WannaCry Ransomware

When:
12-15 May 2017

Location:
Worldwide (Initial NHS England)

Aliases:
WanaCrypt0r, WanaDecrypt0r

Mode of propagation:
Worm

Ransom:
300-600 USD as bitcoins

Damage:
2-300,000 infected computers.

Introduction

WannaCry is a zero-day exploit built on the EternalBlue leak. It is a self-propagating malware that uses encryption to hold the victims' data ransom. It knocked down the U.K. National Health Service hospitals offline to shutting down a Honda Motor Company in Japan.

The ransomware is a worm type and remotely executes code by SMB vulnerability by the network. If a Windows machine doesn't have MS17-010 patch, infection diffuses through the network even when user doesn't take any action. WannaCry ransomware targets 176 extensions, of which most of the file formats include major Microsoft Office files (.ppt, .pptx, .doc, .docx, .xls, .xlsx) and many image file formats (.tiff, .jpg, .bmp, .png).

Unlike other ransomwares till date, the WannaCry ransomware has a worm backend which allows it to self-propagate over the network, i.e. it is distributed autonomously through the network without any user action. it includes a "transport" mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself [4]. Every Windows computer without patch is vulnerable to the infection.

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

The perpetrators are still unknown. whomever they are -- have made headlines. Not only has their attack compromised hundreds of thousands of individuals and even wreaked havoc for hospitals and their patients, it has ultimately spurred a global response from law enforcement and the security industry.

DoublePulsar

DOUBLEPULSAR IS A BACKDOOR IMPLANT TOOL DEVELOPED BY THE U.S. NATIONAL SECURITY AGENCY'S (NSA) EQUATION GROUP THAT WAS LEAKED BY THE SHADOW BROKERS IN EARLY 2017. THE TOOL INFECTED MORE THAN 200,000 MICROSOFT WINDOWS COMPUTERS IN ONLY A FEW WEEKS,

Why did it work so well?

When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data. then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network.

The main victims of such cybercrime were Windows 8, 2003 and XP users, because the last released security update for XP was in April 2014, and many didn't install the newer update as of March this year. Microsoft had stopped supporting these versions of windows, but an emergency update was released for them to fight this cyber-attack.

Response

The day after the initial attack in May, Microsoft released emergency security patches for Windows 7 and Windows 8.1, as well an out-of-band security updates for end of life products Windows XP, Windows Server 2003 and Windows 8; these patches had been created in February of that year following a tip off about the vulnerability in January of that year.

Researcher Marcus Hutchins accidentally discovered the kill switch domain hardcoded in the malware. Registering a domain name for a DNS sinkhole stopped the attack spreading as a worm, because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do. [5]

Adrian Guinet created a "WannaKey", a solution to the WannaCry ransomware based on its flaws. He cautioned that it wouldn't work if the infected computer was rebooted or if the malware overwrote the decryption key. [6]

Impact

around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan. [7]

One of the largest agencies struck by the attack was the National Health Service hospitals in England and Scotland, and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected.

1 Affected Countries (In red)

Case 2:

Petya and NotPetya

When:
March 2017

Location:
Ukraine

Aliases:
GoldenEye

NotPetya

Mode of propagation:
EternalBlue

Ransom:
300-600 USD as bitcoins

Damage:
2.5 Million USD loss in revenues.

Introduction

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting.

It subsequently demands that the user make a payment in Bitcoin to regain access to the system. In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagates via the EternalBlue exploit. The key differentiator here is, unlike WannaCry, it has no method to decrypt the data.

Attack on Ukraine

A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms [8]. Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia.

The cyberattack was based on a modified version of the Petya ransomware. Like the WannaCry ransomware attack in May 2017, Petya uses the EternalBlue exploit previously discovered in older versions of the Microsoft Windows operating system. When Petya is executed, it encrypts the Master File Table of the hard drive and forces the computer to restart. It then displays a message to the user, telling them their files are now encrypted and to send US$300 in bitcoin to one of three wallets to receive instructions to decrypt their computer. At the same time, the software exploits the Server Message Block protocol in Windows to infect local computers on the same network, and any remote computers it can find.

Security experts found that the version of Petya used in the Ukraine cyberattacks had been modified, and subsequently has been named NotPetya or Nyetna to distinguish it from the original malware. NotPetya encrypted all the files on the infected computers, not just the Master File Table, and in some cases the computer's files were completely wiped or rewritten in a manner that could not be undone through decryption

Working

When the infected fie Petya will reboot your computer. You'll see what looks like the standard Windows CHKDSK screen you expect to see after a system crash. The malware is already working behind the scenes to make your files unreachable.

What earned Petya the description "the next step in ransomware evolution" despite its initially unimpressive infection rate is the way it encrypts your files. Rather than searching out specific files and encrypting them, like most ransomware does, it installs its own boot loader, overwriting the affected system's master boot record, then encrypts the master file table, which is the part of the filesystem that serves as sort of a roadmap for the hard drive.

Your files are still there and still unencrypted, but the computer can't access the part of the filesystem that tells it where they are, so they might as well be lost. At this point, the ransomware demands a Bitcoin payment to decrypt the hard drive.

! # NotPetya isn't ransomware. This is in fact the most shocking — and important — thing about NotPetya. It looks like ransomware, complete with a screen informing the victim that they can decrypt their files if they send Bitcoin to a specified wallet. For Petya, this screen includes an identifying that they're supposed to send along with the ransom; the attackers use this code to figure out which victim just paid up. But on computers infected with NotPetya, this number is just randomly generated and would be of no help in identifying anything. And it turns out that in the process of encrypting the data, NotPetya damages it beyond repair.

Impact

During the attack initiated on 27 June 2017, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. It is said to be the most destructive cyberattack ever.

The business interruption to the Maersk, the world's largest container ship and supply vessel operator, was estimated between $200 and $300m in lost revenues.

Case 3:

EternalRocks

This can be called the final form (till date) of the EternalBlue exploits. EternalRocks or MicroBotMassiveNet is a computer worm that infects Microsoft Windows. It uses seven exploits developed by the NSA.

EternalRocks uses EternalBlue, DoublePulsar, EternalChampion, EternalRomance, EternalSynergy, ArchiTouch and SMBTouch -- all tools leaked by the Shadow Brokers.

Unlike WannaCry, which alerts victims they've been infected through ransomware, EternalRocks remains hidden and quiet on computers.

EternalRocks first installs Tor, a private network that conceals Internet activity, to access its hidden servers. After a brief 24 hour "incubation period", the server then responds to the malware request by downloading and self-replicating on the "host" machine.

The malware even names itself WannaCry to avoid detection from security researchers. Unlike WannaCry, EternalRocks does not possess a kill switch and is not ransomware.

Works Cited

[1] W. Post, ""NSA officials worried about the day its potent hacking tool would get loose. Then it did".," [Online]. Available: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

[2] N. O. W. T. Ali Islam, "SMB Exploited: WannaCry Use of "EternalBlue"," [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html.

[3] J. Titcomb, ""Microsoft slams US government over global cyber attack". The Telegraph". *The Telegraph.*

[4] ""Player 3 Has Entered the Game: Say Hello to 'WannaCry'"," [Online]. Available: "Player 3 Has Entered the Game: Say Hello to 'WannaCry'".

[5] A. News, "'Just doing my bit': The 22yo who blocked the WannaCry cyberattack"," [Online]. Available: http://www.abc.net.au/news/2017-05-16/ransomware-cyberattack-marcus-hutchins-gives-interview/8530574.

[6] A. Technica, "Adrian Guinet created a “WannaKey”, a solution to the WannaCry ransomware based on its flaws. He cautioned that it wouldn’t work if the infected computer was rebooted or if the malware overwrote the decryption key.," [Online]. Available: https://arstechnica.co.uk/security/2017/05/windows-xp-wannacry-decryption/.

[7] ""Global alert to prepare for fresh cyber attacks"". *Financial Times..*

[8] "A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms". *Reuters.*