

EternalBlue:
Exploit Analysis and Beyond

WHO AM I?

Emma McCall

Cyber Security Analyst @ Riot Games

[@RiotNymia](#) on Twitter

BBC Sign in News Sport Weather Shop Earth Travel

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

Massive ransomware infection hits computers in 99 countries

13 May 2017

Facebook Twitter Messenger Email Share

The ransomware has been identified as WannaCry - here shown in a safe environment on a security researcher's computer

May 16, 2017

Cryptocurrency miner Adylkuzz attack could be bigger than WannaCry



The attackers behind **WanaCrypt0r/WannaCry** were not the only cybercriminals putting DoublePulsar and EternalBlue to use this weekend, as Proofpoint spotted the stolen NSA tools being used with the cryptocurrency miner Adylkuzz.



Cryptocurrency

The Adylkuzz attack may not only have been larger than WannaCry, but could have been one of the mitigating factors that helped shut down that ransomware attack, wrote a Proofpoint security researcher who goes by the alias **Kafeine**. The mining campaign was after the cryptocurrency Monero.

SECURITY

'Doomsday' worm uses seven NSA exploits (WannaCry used two)

The recently discovered EternalRocks joins a set of highly infectious bugs created from the NSA's leaked tools.

BY ALFRED NG / MAY 22, 2017 1:08 PM PDT



JUST A LITTLE HISTORY

- ▶ Black Market Intelligence Auction Approx. August 2016
 - ▼ No bites
- ▶ April 14th 2017
 - ▼ Group calling themselves 'Shadowbrokers'
 - ▼ Equation Group (NSA) Tools and Exploits dumped onto GitHub

THE DUMP

Exploits

- EARLYSHOVEL RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- EBBISLAND (EBBSHAVE) root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.
- ECHOWRECKER remote Samba 3.0.x Linux exploit.
- EASYBEE appears to be an MDAemon email server vulnerability
- EASYPI is an IBM Lotus Notes exploit that gets detected as Stuxnet
- EWOKFRENZY is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- EXPLODINGCAN is an IIS 6.0 exploit that creates a remote backdoor
- ETERNALROMANCE is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)
- EDUCATEDSCHOLAR is a SMB exploit (MS09-050)
- EMERALDTHREAD is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- EMPHASISMINE is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 6.5.2
- ENGLISHMANSIDENTIST sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users
- EPICHERO 0-day exploit (RCE) for Avaya Call Server
- ERRATICGOPHER is a SMBv1 exploit targeting Windows XP and Server 2003
- ETERNALSYNERGY is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)
- ETERNALBLUE is a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- ETERNALCHAMPION is a SMBv1 exploit
- ESKIMOROLL is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers
- ESTEEMAUDIT is an RDP exploit and backdoor for Windows Server 2003
- ECLIPSEDWING is an RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)
- ETRÉ is an exploit for IMail 8.10 to 8.22
- ETCETERABLUE is an exploit for IMail 7.04 to 8.05
- FUZZBUNCH is an exploit framework, similar to MetaSploit
- ODDJOB is an implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors
- EXPIREDPAYCHECK IIS6 exploit
- EAGERLEVER NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release
- EASYFUN WordClient / IIS6.0 exploit
- ESSAYKEYNOTE
- EVADEFRED

Overall ~35 Exploits and tools

- ▶ SMB
- ▶ SendMail
- ▶ Kerberos
- ▶ IIS
- ▶ Windows XP -> 10

THE DUMP

Of particular note were:

- Fuzzbunch – Exploitation Framework
- DanderSpritz – Command and Control Solution
- DoublePulsar – Backdoor Trojan
- EternalBlue – SMB Exploit

ETERNALBLUE

- ▶ Where has EternalBlue been seen?
 - ▼ WannaCry Ransomware
 - ▼ Adylkuzz Viral Crypto Miner
 - ▼ Zealot - Apache Struts
- ▶ Lateral movement in ALL cases

JUST SOMETHING THAT POPPED UP



Emma McCall
@RiotNymia

EasyFun 2.2.0 Exploit for WDaemon / IIS
MDaemon/WorldClient pre 9.5.6 - Yay for
'Legacy' exploits.

```
1 use strict;
2 use vars qw($VERSION);
3
4 $::VERSION = "EASYFUN Script: 2.2.0.1";
5 print "\n\n$::VERSION\n\n";
6
7
8
9
10
11 use FindBin;
12 use lib "$FindBin::Bin";
13 use Getopt::Long;
14 use Cwd;
15
16 use IO::Socket;
17 use Socket;
18
19 use lib "$FindBin::Bin\\..\\..\\Resources\\Perl";
20 use ExploitUtils qw(
21     $EU_VERBOSE
22     $EU_BATCHMODE
23     EU_LogInit
24     EU_Log
25     EU_ExitMessage
26     EU_GetInput
27     EU_GetExistingDir
28     EU_GetIP
29     EU_GetLocalIP
30     EU_GetRootDir
31     EU_GetPort
32     EU_RunCommand
33 );
```

6:29 PM - 16 Apr 2017

Slight segue to look at this one:

- ▶ Exploit for MDAemon pre v9.5.6
 - ▼ v9.5.6 was Released in October 2006
- ▶ Shodan check on 16th April 2017... Lets have a closer look at that number....



ETERNALBLUE

- ▶ Exploit for Windows Server Message Block (SMB)
 - ▼ Affected both versions v1 and v2
 - ▼ Remote Code Execution on victim machine

WHAT

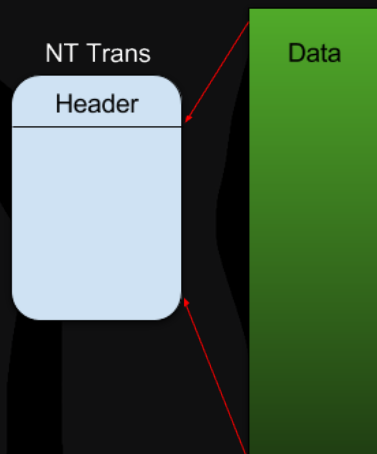
- ▶ Exploitation targeted the following services
 - ▼ TCP 445 (Microsoft Domain Service)
 - ▼ TCP 139 (NetBIOS Session Service)

HOW

THEN WHAT

ETERNALBLUE

- ▶ First things first: How does SMB data transfer work?



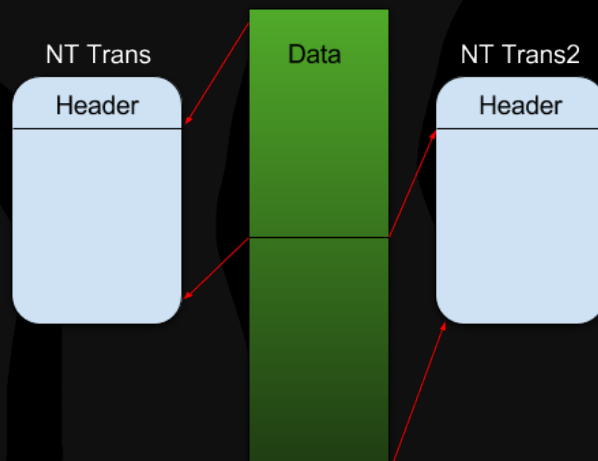
WHAT

HOW

THEN WHAT

ETERNALBLUE

- ▶ First things first: How does SMB data transfer work?
 - ▼ Data larger than SMB MaxBufferSize in Trans2



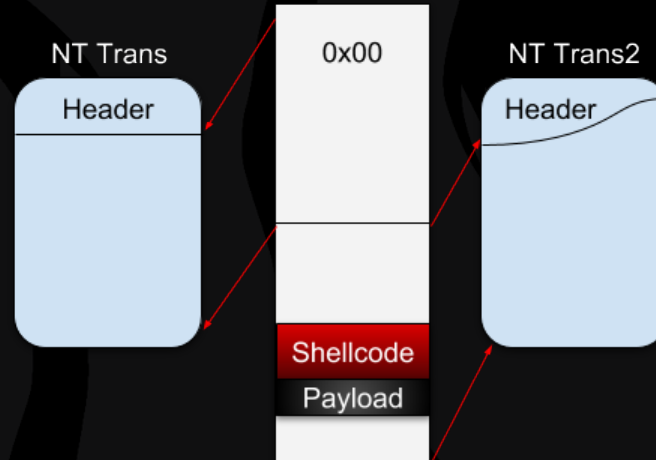
WHAT

HOW

THEN WHAT

ETERNALBLUE

- ▶ Exploits Non-Paged Pool Overflow in srv2.sys
 - ▼ Fills NT Trans with Zeros
 - ▼ Malformed Trans2 packet containing shellcode and Encrypted Payload



WHAT

HOW

THEN WHAT

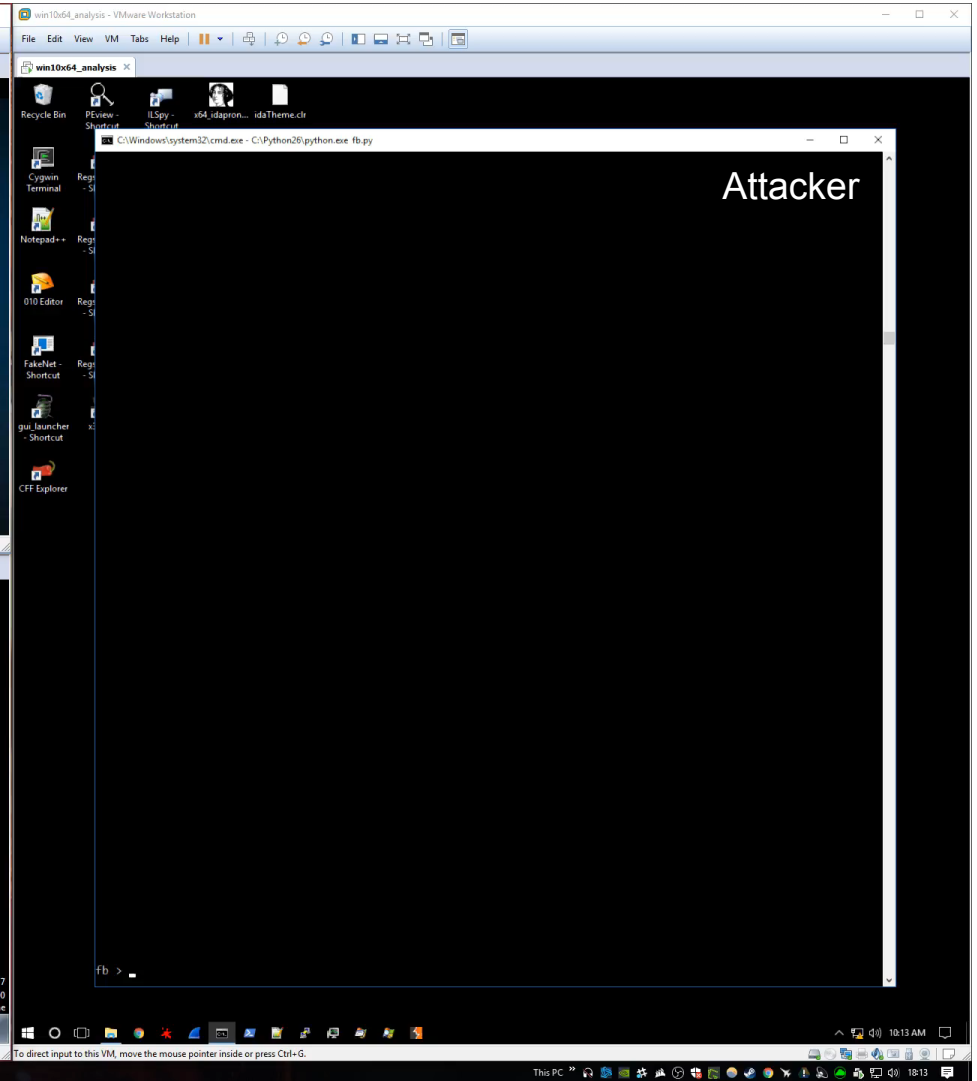
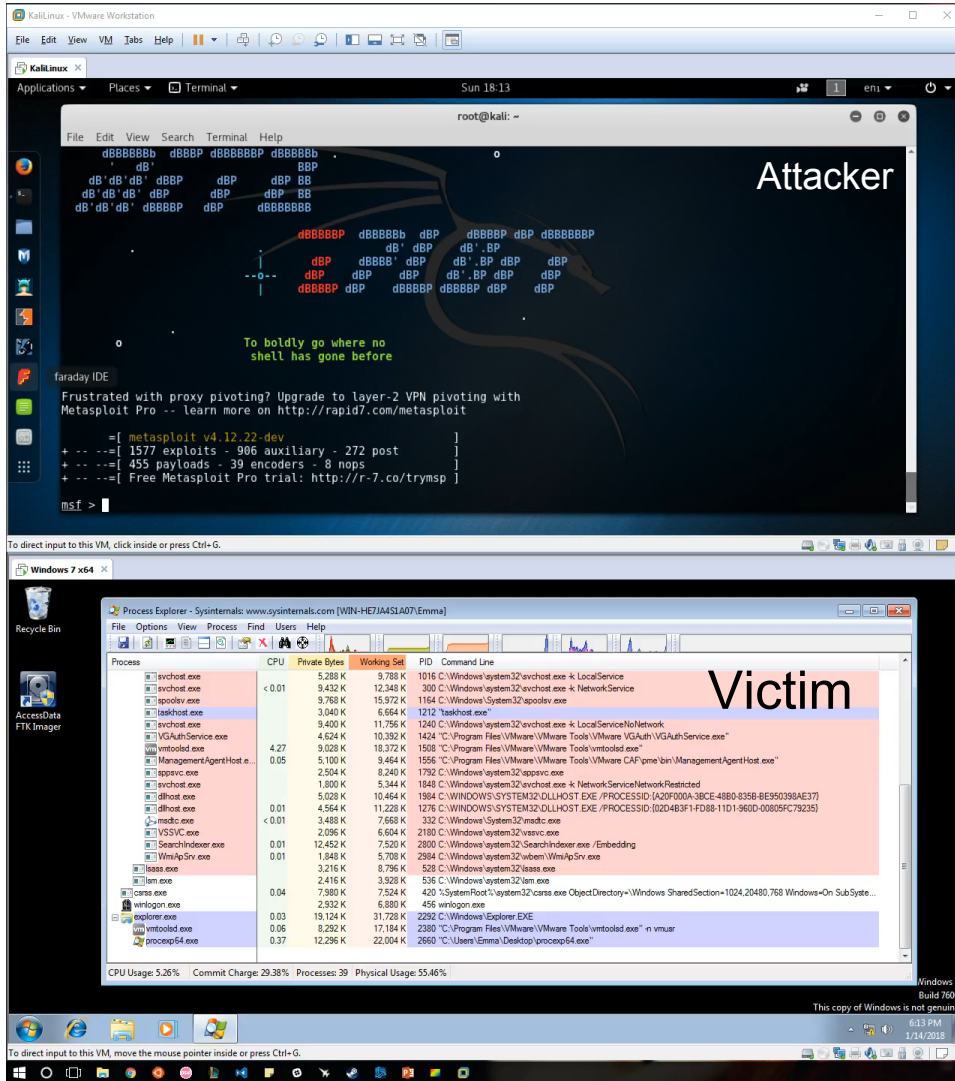
ETERNALBLUE

- ▶ Initial Payload: DoublePulsar
 - ▼ Non-Persistent
 - ▼ Customisable Process Name / Command Line
 - ▼ Code Execution via .DLL or raw shellcode upload
- ▶ Initially Uploaded DLLs came from 2 sources
 - ▼ Created via 'Danderspritz'
 - ▼ Via Metasploit (Meterpreter)

WHAT

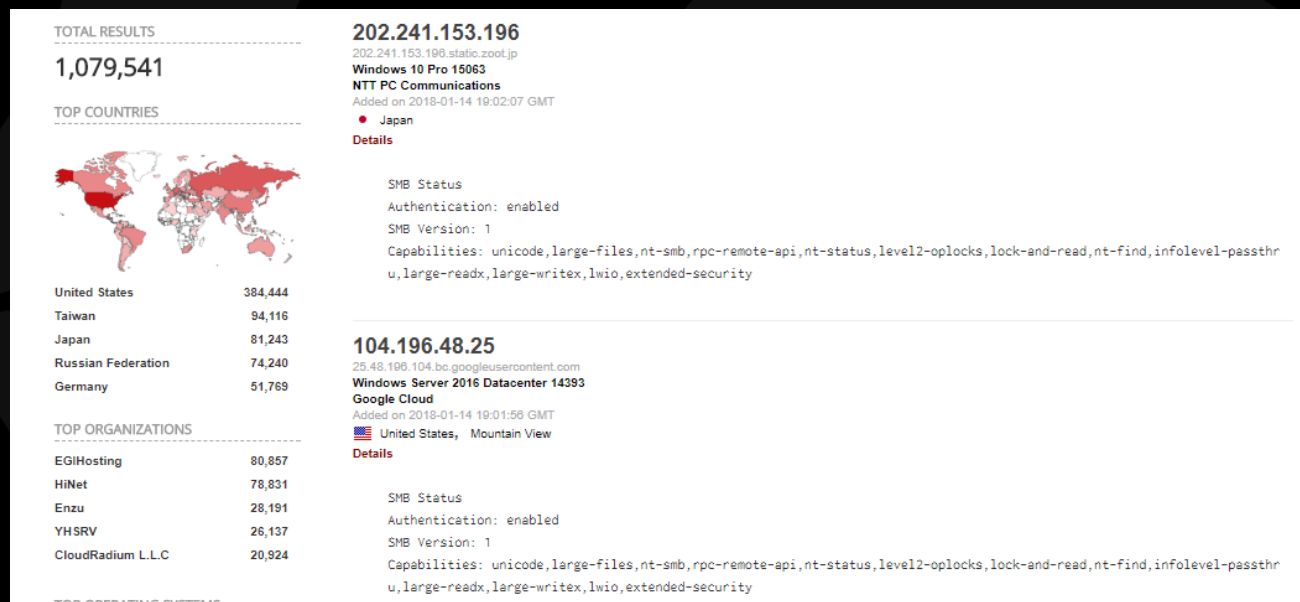
HOW

THEN WHAT



ETERNALBLUE

► TCP 445 On the internet?



... what about on your LAN?

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

NETWORK ANALYSIS

- ▶ Run it.
 - ▼ In a lab!
 - ▼ <https://medium.com/@xNymia> For all your lab creation needs
- ▶ Sysinternals and Wireshark are your best friends
- ▶ Comparison against known good SMB traffic
- ▶ Look for irregularities and patterns in multiple samples
- ▶ Check protocol docs

NETWORK ANALYSIS

eb_sample.pcap

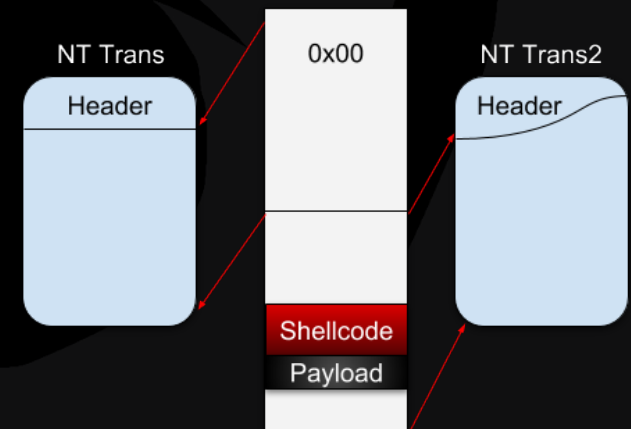
Apply a display filter ... <%%/>

No.	Time	Source	Destination	Protocol	Multiplex ID	Port	Info
13	0.001375	192.168.159.128	192.168.159.130	SMB		65 vsanredirector	Trans2 Response, SESSION_SETUP,
14	0.005256	192.168.159.130	192.168.159.128	SMB		65 microsoft-ds	NT Trans Request, <unknown>
15	0.005377	192.168.159.128	192.168.159.130	SMB		65 vsanredirector	NT Trans Response, <unknown (0)>
16	0.005460	192.168.159.130	192.168.159.128	TCP		microsoft-ds	[TCP segment of a reassembled PD

Max Setup Count: 1
Reserved: 0000
Total Parameter Count: 30
Total Data Count: 66512
Max Parameter Count: 30
Max Data Count: 0
Parameter Count: 30
Parameter Offset: 75

0000 00 0c 29 be 12 40 00 0c 29 e0 2f 9f 08 00 45 00 ..).@..)/...E.
0010 04 64 1d 85 40 00 00 06 18 bb c0 a8 9f 82 c0 a8 .d... ..
0020 9f 00 09 53 01 bd fe 06 7d ba 34 56 aa 06 50 18 ...S...).4W. P.
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 18 07 c0 00 00 00 00 00 00 00 00
0050 00 00 00 08 ff fe 00 08 41 00 14 01 00 00 1e 00 A.....
0060 00 00 d0 03 01 00 1e 00 00 00 00 00 00 00 1e 00K.....h.....
0070 00 00 4b 00 00 00 d0 03 00 00 68 00 00 00 01 00
0080 00 00 00 cc 03 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Total number of data bytes (smb.tdc), 4 bytes

Packets: 334 - Displayed: 334 (1



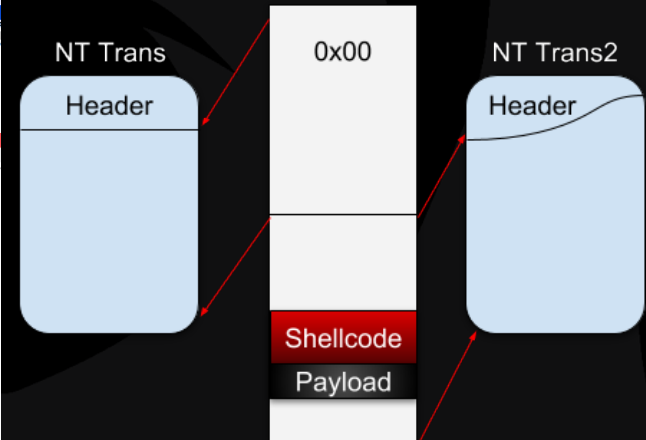
NETWORK ANALYSIS

The image shows a Wireshark packet capture analysis of a file named 'eb_sample.pcap'. The packet list on the left shows three packets. Packet 21, at time 0.005663, is an SMB packet from 192.168.159.130 to 192.168.159.128, port 65, identified as a 'Trans2 Secondary Request (Malformed Packet)'. The packet details pane shows the SMB structure, with the 'Byte Count (BCC): 30305' field highlighted in red. Below this, the 'Expert Info (Error/Malformed): Malformed Packet (Exception occurred)' is also highlighted in red. The packet bytes pane shows the raw data in hexadecimal and ASCII, with a red box highlighting the payload area starting at offset 0x29. The status bar at the bottom indicates 'Packets: 334 - Displayed: 334 (100.0%) - Load time: ...'.

No.	Time	Source	Destination	Protocol	Multiplex ID	Port	Info
19	0.005618	192.168.159.130	192.168.159.128	TCP		microsoft-ds	[TCP segment of a reassembled PDU]
20	0.005662	192.168.159.130	192.168.159.128	TCP		microsoft-ds	[TCP segment of a reassembled PDU]
21	0.005663	192.168.159.130	192.168.159.128	SMB		65	Trans2 Secondary Request (Malformed Packet)

Parameter Offset: 25668
Data Count: 26224
Data Offset: 14658
Setup Count: 85
Reserved: 64
Byte Count (BCC): 30305
[Malformed Packet: SMB]
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

0000 00 0c 29 be 12 40 00 0c 29 e0 2f 9f 08 00 45 00 ...).e..)./...E.
0020 9f 80 09 53 01 bd fe 86 9d 97 34 56 aa ad 50 18 ...S....4V.P.
0040 08 03 c6 64 00 00 65 36 6d 70 57 4b 78 39 62 58 ...d..e6 mpKx9bX
0060 72 45 41 50 65 62 30 37 54 4c 73 4a 4e 7a 32 65 rEAPe07 TL5JN2ze
0080 42 53 4c 45 55 71 41 78 58 55 33 6a 32 47 37 55 BSLUQAx XU3j2GTU
00a0 46 36 35 61 33 50 4d 7a 77 33 67 46 69 79 4a 7a F65a3PMz w3gFiyJz
00c0 35 46 70 66 59 75 5a 73 57 6a 72 76 79 63 4b 6b 5PpfYuzs WjrvyCKk
00e0 51 72 62 67 49 31 4d 4d 42 63 4d 49 36 45 49 4b OrbgIjMM B0M16EIK
0100 38 4a 7a 31 69 4a 49 38 35 67 76 4e 54 31 38 78 8Jz1lJlT8 SgvNT18x
0120 63 70 49 6c 4f 38 72 75 42 35 41 36 61 58 6e 42 cpl08ru B5A6aXnB
0140 43 56 52 4e 67 49 66 64 68 74 48 64 30 64 45 54 CVRNqIfd htHd0dET
0160 43 58 42 5a 69 78 76 2f 4a 6a 5a 39 48 6d 5a 4f CxBZ1xv/ JjZ9HmZ0
0180 6e 70 67 47 78 48 6f 47 4c 55 39 55 6c 43 7a 46 npg6xHoG LU9U1Czf
01a0 62 77 31 38 6d 2f 6d 51 69 76 76 65 5a 67 64 76 bw18m/mQ lvevZgdv
01c0 65 32 42 47 45 56 57 64 2b 31 52 68 58 66 5a 58 e28GEVmd +lRhXfZX
01e0 78 51 51 74 30 70 4e 6e 61 52 54 37 4b 44 55 31 xQ0t0pNn aRT7KDU1
0200 4b 5a 4b 54 4c 74 52 77 63 71 57 45 55 35 36 4b KZKTLlRw cQNEU56K
0220 5a 52 44 65 74 33 63 54 59 44 4d 2f 57 4c 61 79 ZR0et3cT YDMWlay
0240 58 2f 48 73 42 56 42 55 46 49 5a 4f 6b 48 4a 5a X/HsBVBu FIZ0KHJZ
0260 4e 62 73 7a 77 69 32 52 61 4a 61 65 66 74 51 6f Nbszw12R aJaft0o
0280 69 56 69 32 42 41 51 33 4f 67 54 37 37 2f 51 31 iV12BAQ3 0gT77/Q1
02a0 71 67 38 5a 56 6a 47 61 79 6a 46 33 75 52 4a 39 qg8ZVjGa yJf3uRj9



NETWORK ANALYSIS

► Interesting Multiplex ID

No.	Time	Source	Destination	Protocol	Length	Details
12	0.001275	192.168.159.130	192.168.159.128	SMB	136	65 Trans2 Request, SESSION_SETUP
13	0.001375	192.168.159.128	192.168.159.130	SMB	93	65 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
14	0.005256	192.168.159.130	192.168.159.128	SMB	1138	65 NT Trans Request, <unknown>
15	0.005377	192.168.159.128	192.168.159.130	SMB	93	65 NT Trans Response, <unknown (0)>
16	0.005460	192.168.159.130	192.168.159.128	TCP	1514	[TCP segment of a reassembled PDU]
17	0.005461	192.168.159.130	192.168.159.128	TCP	1514	[TCP segment of a reassembled PDU]

▼ SMB Header

Server Component: SMB
[Response to: 12]
[Time from request: 0.000100000 seconds]
SMB Command: Trans2 (0x32)
NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)

> Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
> Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Names Allowed
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
> Tree ID: 2048 (\\192.168.159.128\IPC\$)
Process ID: 65279
User ID: 2048
Multiplex ID: 65

▼ Trans2 Response (0x32)

```
0000 00 0c 29 e0 2f 9f 00 0c 29 be 12 40 08 00 45 00 ..)/... )..E.
0010 00 4f 00 5b 40 00 00 06 39 fa c0 a8 9f 00 c0 a8 .O.[@... 9.....
0020 9f 82 01 bd 09 53 34 56 aa 5f fe 86 7d ba 50 18 ....S4V _..}.P.
0030 00 ff 00 28 00 00 00 00 00 23 ff 53 4d 42 32 02 ...((... .#.SMB2.
0040 00 00 c0 98 07 c0 00 00 00 00 00 00 00 00 00 00 .....
0050 00 00 00 08 ff fe 00 08 41 00 00 00 00 00 00 00 ..... A....
```

NT Status code (smb.nt_status), 4 bytes

Packets: 334 · Displayed: 334 (100.0%) · Load time: 0:0.3

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

DETECTION CREATION

- ▶ We have 4 indicators now
 - ▼ Multiplex ID 64/65
 - ▼ Multiplex ID 81/82
- ▶ Lets flex our learnings
 - ▼ Suricata IDS Rules
 - ▼ Snort IDS Rules

```
alert tcp $HOME_NET any -> any any (msg:"EXPLOIT Possible ETERNALBLUE SMB Exploit Attempt Stage 1/2  
- Tree Connect AndX MultiplexID = 64 - MS17-010";  
flow:to_server,established; content:"|FF|SMB|75 00 00 00 00|"; offset:4; depth:9; content:"|40 00|";  
distance:21; within:23; flowbits: set, SMB.v1.AndX.MID.64; classtype:trojan-activity; sid:5000074; rev:1;)
```



DETECTION CREATION

SMB Packet

```
0010 < ..... Frame / TCP / IP Headers .....>
0020 00 00 00 60 FF 53 4D 42 75 00 00 00 00 18 07 C0
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE
0040 00 08 40 00 04 FF 00 60 00 08 00 01 00 35 00 00
0050 5C 00 5C 00 31 00 39 00 32 00 2E 00 31 00 36 ...
```

NetBios Header

SMB Structure - "|FF|SMB|75 00 00 00 00|"

Multiplex ID - "|40 00|"

SMB Content

DETECTION CREATION

```
alert tcp $HOME_NET any -> any any (msg:"EXPLOIT Possible ETERNALBLUE SMB Exploit Attempt Stage 1/2  
- Tree Connect AndX MultiplexID = 64 - MS17-010";  
  flow:to_server,established; content:"|FF|SMB|75 00 00 00 00|"; offset:4; depth:9; content:"|40 00|";  
  distance:21; within:23; flowbits: set, SMB.v1.AndX.MID.64; classtype:trojan-activity; sid:5000074; rev:1;)
```

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

IMPACT IDENTIFICATION

- ▶ What is actually vulnerable?
- ▶ Run it.
 - ▼ In lots of labs!



IMPACT IDENTIFICATION

- ▶ What has already been compromised?
 - ▼ Scan the internet?

 **Dan Tentler** 
@Viss Following

current status:
1.17 million host scanned
33,468 found infected.

```
line: 1158139 - found: 32929 - ips/min: 885 - ETC: 94.77/hrs - INFECTED: 2.8600%
line: 1158888 - found: 32983 - ips/min: 749 - ETC: 111.98/hrs - INFECTED: 2.8600%
line: 1159145 - found: 32983 - ips/min: 657 - ETC: 127.66/hrs - INFECTED: 2.8600%
line: 1152358 - found: 32983 - ips/min: 885 - ETC: 104.19/hrs - INFECTED: 2.8600%
line: 1153204 - found: 33837 - ips/min: 994 - ETC: 89.79/hrs - INFECTED: 2.8600%
line: 1154167 - found: 33837 - ips/min: 883 - ETC: 94.98/hrs - INFECTED: 2.8600%
line: 1154878 - found: 33891 - ips/min: 711 - ETC: 117.96/hrs - INFECTED: 2.8600%
line: 1155391 - found: 33891 - ips/min: 513 - ETC: 163.49/hrs - INFECTED: 2.8600%
line: 1156998 - found: 33891 - ips/min: 787 - ETC: 118.63/hrs - INFECTED: 2.8600%
line: 1157838 - found: 33145 - ips/min: 948 - ETC: 89.22/hrs - INFECTED: 2.8600%
line: 1157786 - found: 33145 - ips/min: 748 - ETC: 112.12/hrs - INFECTED: 2.8600%
line: 1158496 - found: 33199 - ips/min: 718 - ETC: 118.13/hrs - INFECTED: 2.8600%
line: 1159451 - found: 33199 - ips/min: 955 - ETC: 86.91/hrs - INFECTED: 2.8600%
line: 1168325 - found: 33253 - ips/min: 864 - ETC: 97.87/hrs - INFECTED: 2.8600%
line: 1161145 - found: 33253 - ips/min: 828 - ETC: 182.28/hrs - INFECTED: 2.8600%
line: 1162182 - found: 33253 - ips/min: 957 - ETC: 87.64/hrs - INFECTED: 2.8600%
line: 1162987 - found: 33386 - ips/min: 885 - ETC: 104.19/hrs - INFECTED: 2.8600%
line: 1163787 - found: 33386 - ips/min: 888 - ETC: 95.31/hrs - INFECTED: 2.8600%
line: 1164683 - found: 33368 - ips/min: 815 - ETC: 182.78/hrs - INFECTED: 2.8600%
line: 1165653 - found: 33368 - ips/min: 1958 - ETC: 79.87/hrs - INFECTED: 2.8600%
line: 1166398 - found: 33414 - ips/min: 745 - ETC: 112.58/hrs - INFECTED: 2.8600%
line: 1167887 - found: 33414 - ips/min: 689 - ETC: 121.73/hrs - INFECTED: 2.8600%
line: 1168859 - found: 33414 - ips/min: 972 - ETC: 86.28/hrs - INFECTED: 2.8600%
line: 1168824 - found: 33468 - ips/min: 795 - ETC: 195.58/hrs - INFECTED: 2.8600%
line: 1169787 - found: 33468 - ips/min: 933 - ETC: 89.89/hrs - INFECTED: 2.8600%
line: 1178285 - found: 33468 - ips/min: 418 - ETC: 288.65/hrs - INFECTED: 2.8600%
```

RETWEETS 67 LIKES 94

8:24 PM - 23 Apr 2017

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

MITIGATION ADVICE

- ▶ How can we help others mitigate?
 - ▼ Patching can be difficult
 - ▼ What other options can we offer?
- ▶ Disable SMBv1?
- ▶ What did **Riot** do?
 - ▼ Suricata detections
 - ▼ No external SMB
 - ▼ Firewallled Inbound SMB on workstations

WHAT *CAN* I DO?

NETWORK ANALYSIS

DETECTION CREATION

IMPACT IDENTIFICATION

MITIGATION ADVICE

BINARY ANALYSIS

BINARY ANALYSIS

- ▶ Sometimes worthwhile disassembling

```
var_17 byte ptr 4
hInstance= dword ptr 4
hPrevInstance= dword ptr 8
lpCmdLine= dword ptr 0Ch
nShowCmd= dword ptr 10h

sub     esp, 50h
push    esi
push    edi
mov     ecx, 0Eh
mov     esi, offset aHttpWwwIuqerfs ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
lea     edi, [esp+58h+szUrl]
xor     eax, eax
rep movsd
movsb
mov     [esp+58h+var_17], eax
mov     [esp+58h+var_13], eax
mov     [esp+58h+var_F], eax
mov     [esp+58h+var_8], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_3], ax
push    eax ; dwFlags
```

```
.data:004313D0 aHttpWwwIuqerfs db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwea.com',0
```

...Simplest things right under your nose.

... AND BEYOND

- ▶ So shits going down, **what can I do?**
 - ▼ Get a lab setup
 - ▼ Grab a sample
 - ▼ Run it. Don't be too afraid
 - ▼ What can I do with this data?
 - ▼ Blogging, Tweeting, IRC / Slack / Discord
- ▶ A few don'ts for good measure:
 - ▼ Don't work in a silo, talk to people
 - ▼ Don't run dodgy files on your main machine

Be Heard

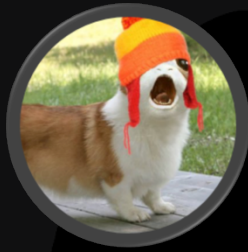
THE GANG



Dan Tentler
@Viss



DEY!
@ronindey



Kevin Beaumont
@GossiTheDog



Emma McCall
@RiotNymia

