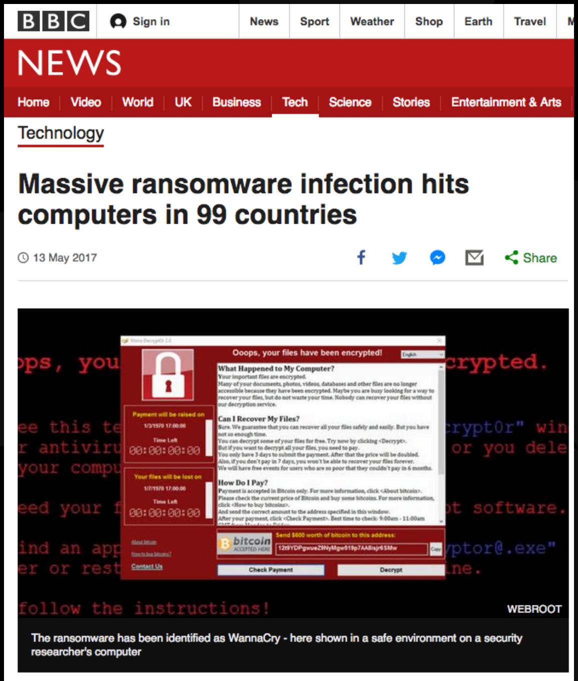
EternalBlue:
Exploit Analysis and Beyond

WHO AM I?

Emma McCall

Cyber Security Analyst @ Riot Games

@RiotNymia on Twitter

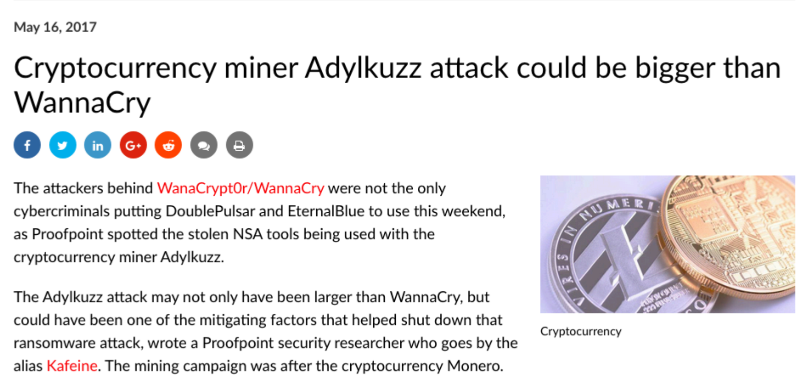


Technology

Massive ransomware infection hits computers in 99 countries

13 May 2017

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



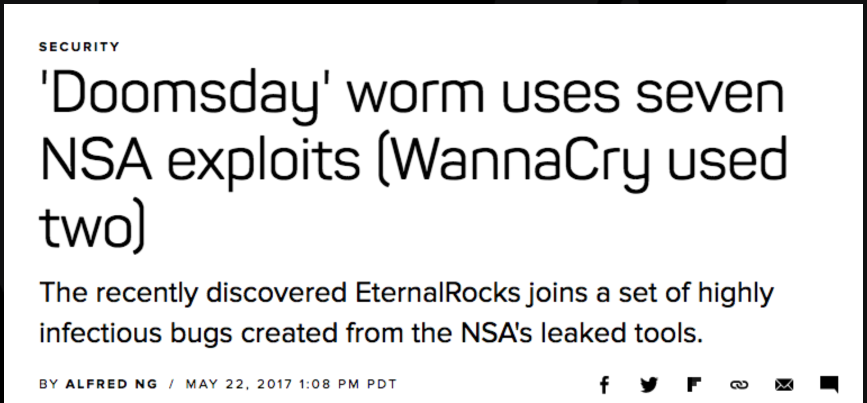
May 16, 2017

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.

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.

Cryptocurrency



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.

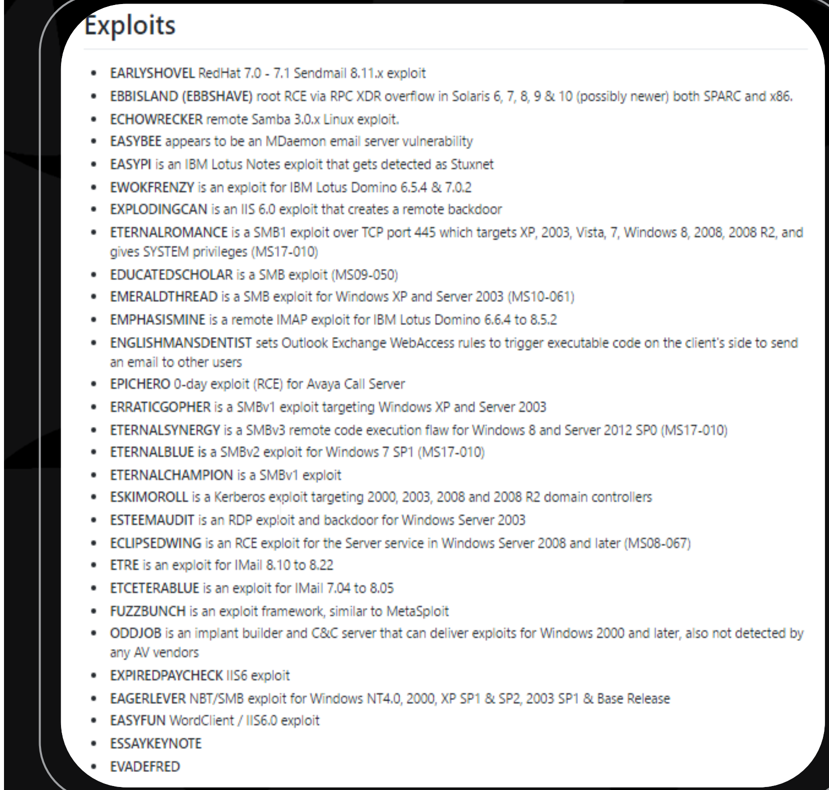
BY ALFRED NG / MAY 22, 2017 1:08 PM PDT

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 8.5.2
- **ENGLISHMANSDENTIST** 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)
- **ETRE** 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:

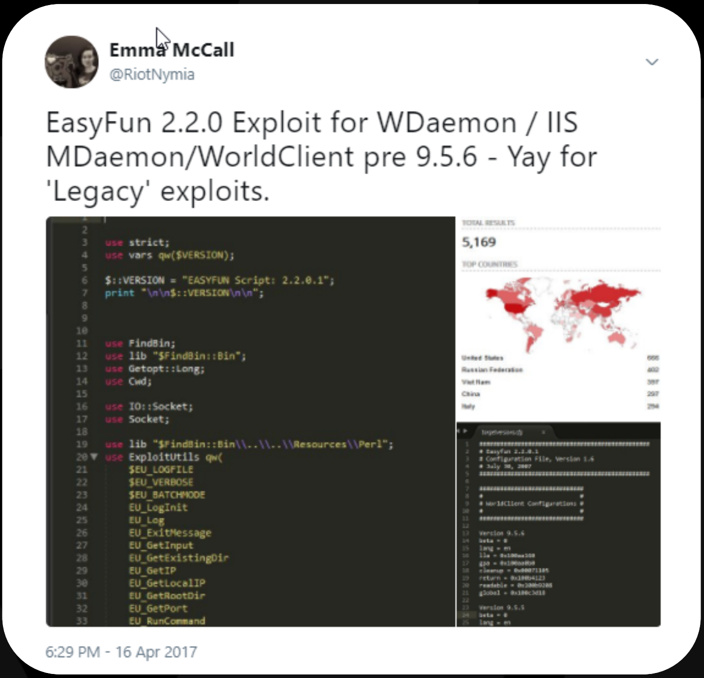
- Fuzzbunch – Exploitation Framework
- DanderSpritz – Command and Control Solution
- DoublePulsar – Backdoor Trojan
- EternalBlue – SMB Exploit

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.

```
use strict;
use vars qw($VERSION);

$::VERSION = "EASYFUN Script: 2.2.0.1";
print "\n\n$::VERSION\n\n";



use FindBin;
use lib "$FindBin::Bin";
use Getopt::Long;
use Cwd;

use IO::Socket;
use Socket;

use lib "$FindBin::Bin\\..\\..\\Resources\\Perl";
use ExploitUtils qw(
    $EU_LOGFILE
    $EU_VERBOSE
    $EU_BATCHMODE
    EU_LogInit
    EU_Log
    EU_ExitMessage
    EU_GetInput
    EU_GetExistingDir
    EU_GetIP
    EU_GetLocalIP
    EU_GetRootDir
    EU_GetPort
    EU_RunCommand
```

TOTAL RESULTS
5,169

TOP COUNTRIES

United States	666
Russian Federation	402
Viet Nam	397
China	297
Italy	294

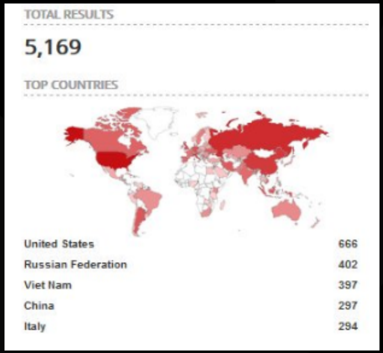
```
###########################################################
# EasyFun 2.2.0.1
# Configuration File, Version 1.6
# July 30, 2007
###########################################################

##############################
#                            #
# WorldClient Configurations #
#                            #
##############################

Version 9.5.6
beta = 0
lang = en
lla = [illegible]
gpo = [illegible]
cleanup = [illegible]
return = [illegible]
readable = [illegible]
global = [illegible]

Version 9.5.5
beta = 0
lang = en
```

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….



TOTAL RESULTS
5,169

TOP COUNTRIES

United States	666
Russian Federation	402
Viet Nam	397
China	297
Italy	294

ETERNALBLUE

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

WHAT

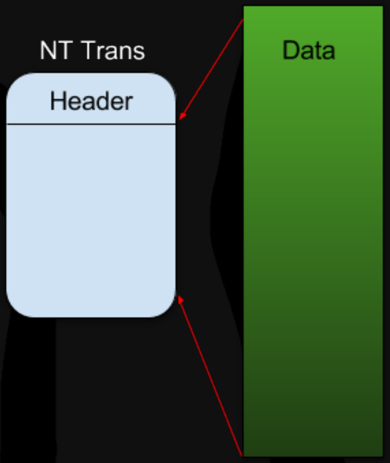
HOW

THEN WHAT

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

ETERNALBLUE

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



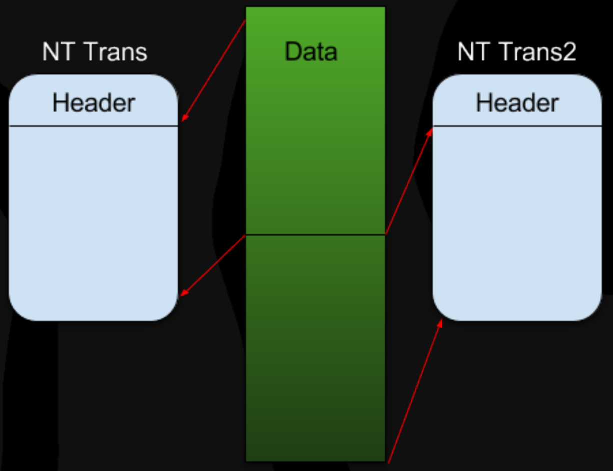
WHAT

HOW

THEN WHAT

ETERNALBLUE

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



WHAT

HOW

THEN WHAT

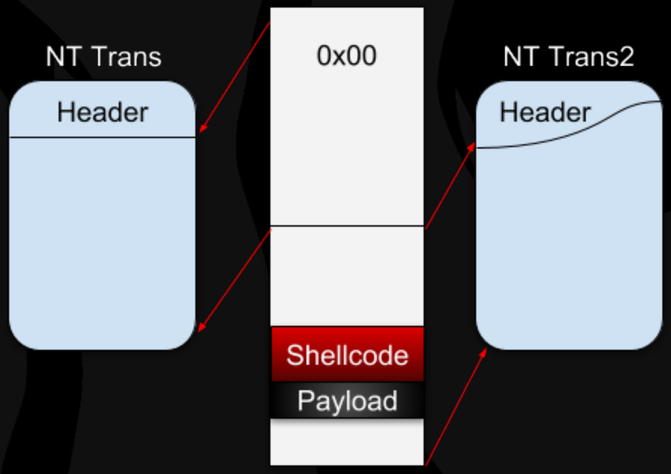
ETERNALBLUE

- 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

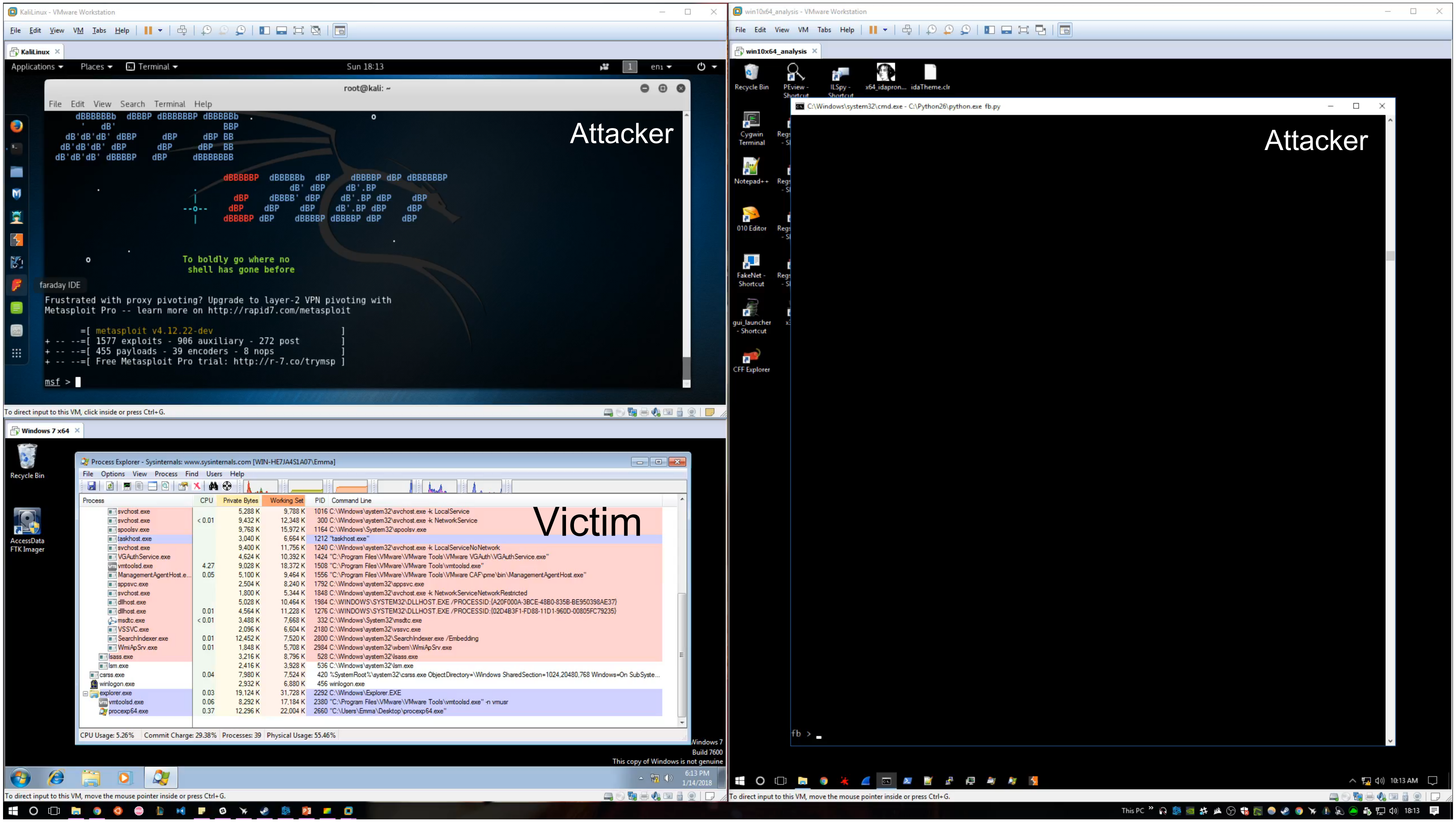
- Initial Payload: DoublePulsar
  - Non-Persistent
  - Customisable Process Name / Command Line
  - Code Execution via .DLL or raw shellcode upload

- Initially Uploaded DLLs came from 2 sources
  - Created via ‘Danderspritz’
  - Via Metasploit (Meterpreter)

WHAT

HOW

THEN WHAT


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux
Applications Places Terminal Sun 18:13
root@kali: ~
File Edit View Search Terminal Help
faraday IDE
Attacker
To direct input to this VM, click inside or press Ctrl+G.
Windows 7 x64
Recycle Bin
AccessData FTK Imager
Victim
Windows 7
Build 7600
This copy of Windows is not genuine
6:13 PM
1/14/2018
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
win10x64_analysis - VMware Workstation
File Edit View VM Tabs Help
win10x64_analysis
Recycle Bin
PEview - Shortcut
ILSpy - Shortcut
x64_idapron...
idaTheme.clr
Cygwin Terminal
Notepad++
010 Editor
FakeNet - Shortcut
gui_launcher - Shortcut
CFF Explorer
C:\Windows\system32\cmd.exe - C:\Python26\python.exe fb.py
Attacker
10:13 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
This PC
18:13

```
       dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
        '   dB'                     BBP
     dB'dB'dB' dBBP     dBP     dBP BB
    dB'dB'dB' dBP      dBP     dBP  BB
   dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.22-dev                         ]
+ -- --=[ 1577 exploits - 906 auxiliary - 272 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Process Explorer - Sysinternals: www.sysinternals.com [WIN-HE7JA4S1A07\Emma]

File Options View Process Find Users Help

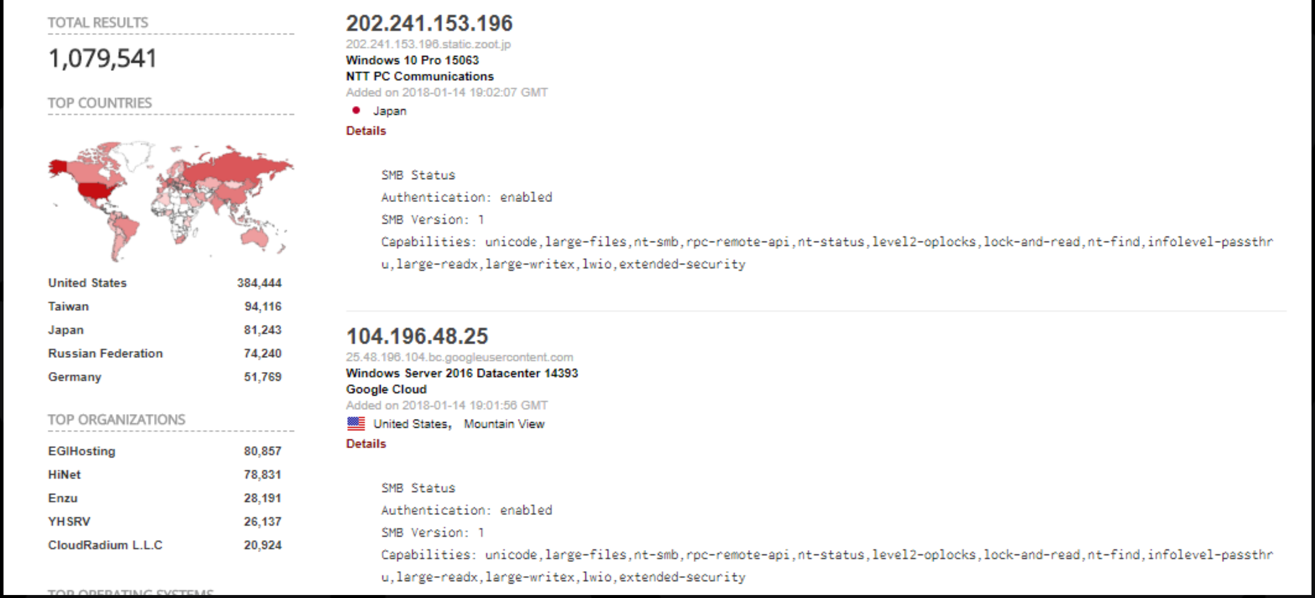
Process	CPU	Private Bytes	Working Set	PID	Command Line
svchost.exe		5,288 K	9,788 K	1016	C:\Windows\system32\svchost.exe -k LocalService
svchost.exe	< 0.01	9,432 K	12,348 K	300	C:\Windows\system32\svchost.exe -k NetworkService
spoolsv.exe		9,768 K	15,972 K	1164	C:\Windows\System32\spoolsv.exe
taskhost.exe		3,040 K	6,664 K	1212	"taskhost.exe"
svchost.exe		9,400 K	11,756 K	1240	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
VGAuthService.exe		4,624 K	10,392 K	1424	"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
vmtoolsd.exe	4.27	9,028 K	18,372 K	1508	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
ManagementAgentHost.e...	0.05	5,100 K	9,464 K	1556	"C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe"
sppsvc.exe		2,504 K	8,240 K	1792	C:\Windows\system32\sppsvc.exe
svchost.exe		1,800 K	5,344 K	1848	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
dllhost.exe		5,028 K	10,464 K	1984	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{A20F000A-3BCE-48B0-835B-BE950398AE37}
dllhost.exe	0.01	4,564 K	11,228 K	1276	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{02D4B3F1-FD88-11D1-960D-00805FC79235}
msdtc.exe	< 0.01	3,488 K	7,668 K	332	C:\Windows\System32\msdtc.exe
VSSVC.exe		2,096 K	6,604 K	2180	C:\Windows\system32\vssvc.exe
SearchIndexer.exe	0.01	12,452 K	7,520 K	2800	C:\Windows\system32\SearchIndexer.exe /Embedding
WmiApSrv.exe	0.01	1,848 K	5,708 K	2984	C:\Windows\system32\wbem\WmiApSrv.exe
lsass.exe		3,216 K	8,796 K	528	C:\Windows\system32\lsass.exe
lsm.exe		2,416 K	3,928 K	536	C:\Windows\system32\lsm.exe
csrss.exe	0.04	7,980 K	7,524 K	420	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyste...
winlogon.exe		2,932 K	6,880 K	456	winlogon.exe
explorer.exe	0.03	19,124 K	31,728 K	2292	C:\Windows\Explorer.EXE
vmtoolsd.exe	0.06	8,292 K	17,184 K	2380	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
procexp64.exe	0.37	12,296 K	22,004 K	2660	"C:\Users\Emma\Desktop\procexp64.exe"

CPU Usage: 5.26% Commit Charge: 29.38% Processes: 39 Physical Usage: 55.46%

```
fb >
```

ETERNALBLUE

- TCP 445 On the internet?



TOTAL RESULTS

1,079,541

TOP COUNTRIES

United States	384,444
Taiwan	94,116
Japan	81,243
Russian Federation	74,240
Germany	51,769

TOP ORGANIZATIONS

EGIHosting	80,857
HiNet	78,831
Enzu	28,191
YHSRV	26,137
CloudRadium L.L.C	20,924

TOP OPERATING SYSTEMS

202.241.153.196
202.241.153.196.static.zoot.jp
Windows 10 Pro 15063
NTT PC Communications
Added on 2018-01-14 19:02:07 GMT
● Japan
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthr
u,large-readx,large-writex,lwio,extended-security
```

104.196.48.25
25.48.196.104.bc.googleusercontent.com
Windows Server 2016 Datacenter 14393
Google Cloud
Added on 2018-01-14 19:01:56 GMT
United States, Mountain View
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthr
u,large-readx,large-writex,lwio,extended-security
```

… 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

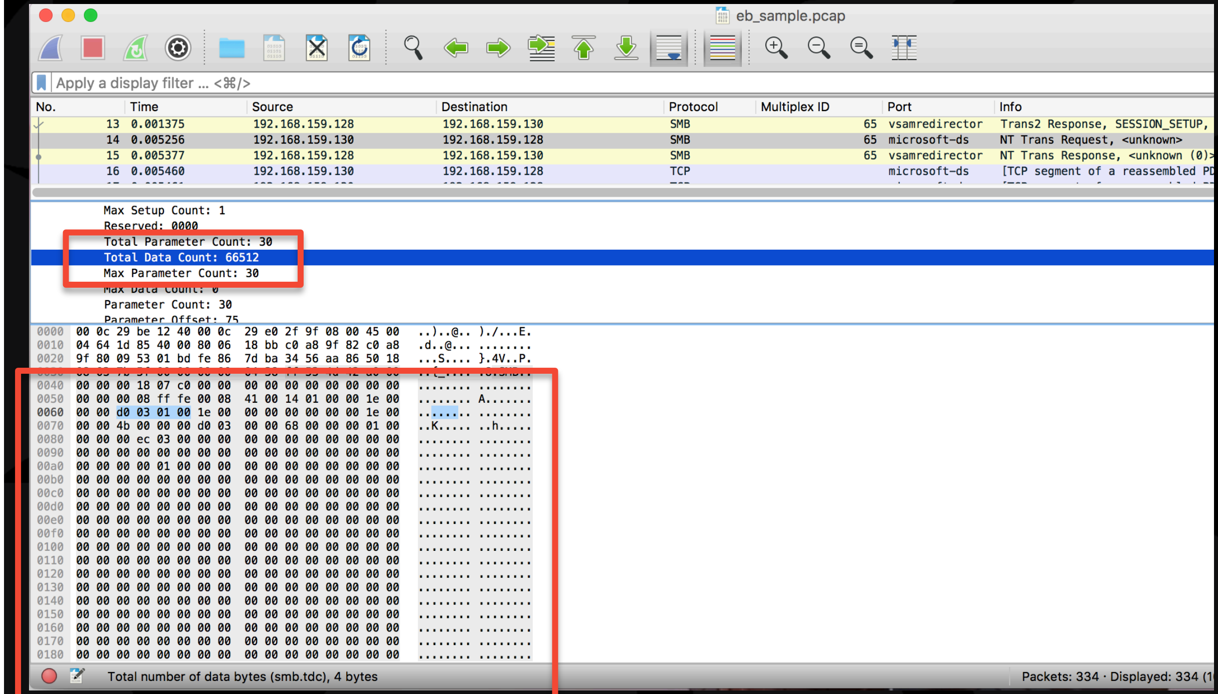
NETWORK ANALYSIS

- 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 ... <⌘/>

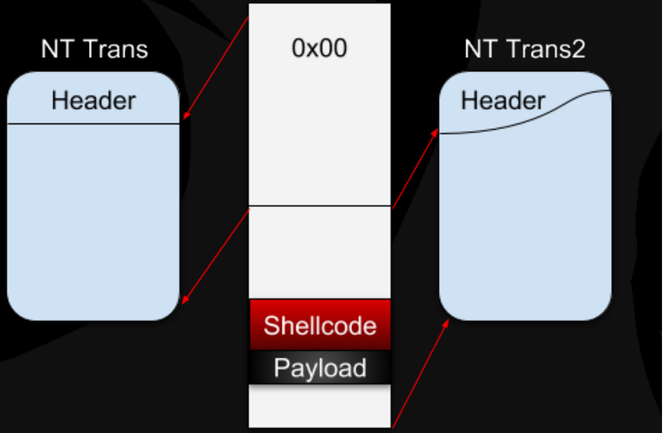
```
No.  Time       Source            Destination       Protocol  Multiplex ID  Port            Info
  13 0.001375   192.168.159.128   192.168.159.130   SMB                 65  vsamredirector  Trans2 Response, SESSION_SETUP,
  14 0.005256   192.168.159.130   192.168.159.128   SMB                 65  microsoft-ds    NT Trans Request, <unknown>
  15 0.005377   192.168.159.128   192.168.159.130   SMB                 65  vsamredirector  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
```

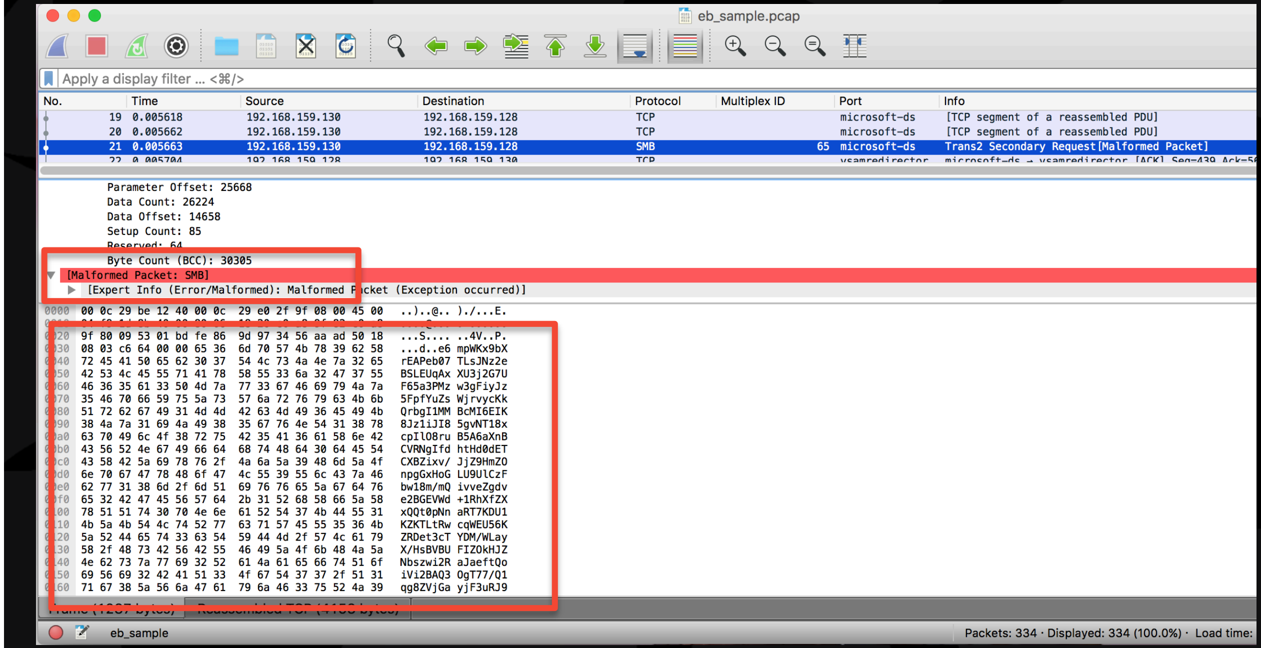
```
0000  00 0c 29 be 12 40 00 0c  29 e0 2f 9f 08 00 45 00   ..)..@.. )./...E.
0010  04 64 1d 85 40 00 80 06  18 bb c0 a8 9f 82 c0 a8   .d..@... ........
0020  9f 80 09 53 01 bd fe 86  7d ba 34 56 aa 86 50 18   ...S.... }.4V..P.
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00   ........ ........
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 00   ........ ........
0070  00 00 4b 00 00 00 d0 03  00 00 68 00 00 00 01 00   ..K..... ..h.....
0080  00 00 00 ec 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 00 00   ........ ........
00a0  00 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 00 00   ........ ........
00c0  00 00 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 00 00   ........ ........
00e0  00 00 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 00 00   ........ ........
0100  00 00 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 00 00   ........ ........
0120  00 00 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 00 00   ........ ........
0140  00 00 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 00 00   ........ ........
0160  00 00 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 00 00   ........ ........
0180  00 00 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



eb_sample.pcap

Apply a display filter ... <⌘/>

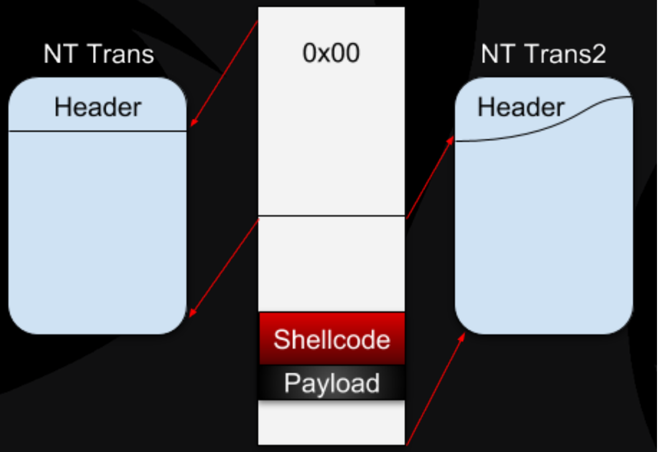
```
No.   Time      Source           Destination      Protocol  Multiplex ID  Port            Info
   19 0.005618  192.168.159.130  192.168.159.128  TCP                     microsoft-ds    [TCP segment of a reassembled PDU]
   20 0.005662  192.168.159.130  192.168.159.128  TCP                     microsoft-ds    [TCP segment of a reassembled PDU]
   21 0.005663  192.168.159.130  192.168.159.128  SMB                 65  microsoft-ds    Trans2 Secondary Request[Malformed Packet]
   22 0.005704  192.168.159.128  192.168.159.130  TCP                     vsamredirector  microsoft-ds → vsamredirector [ACK] Seq=439 Ack=5
```

```
        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.
0020  9f 80 09 53 01 bd fe 86  9d 97 34 56 aa ad 50 18   ...S.... ..4V..P.
0030  08 03 c6 64 00 00 65 36  6d 70 57 4b 78 39 62 58   ...d..e6 mpWKx9bX
0040  72 45 41 50 65 62 30 37  54 4c 73 4a 4e 7a 32 65   rEAPeb07 TLsJNz2e
0050  42 53 4c 45 55 71 41 78  58 55 33 6a 32 47 37 55   BSLEUqAx XU3j2G7U
0060  46 36 35 61 33 50 4d 7a  77 33 67 46 69 79 4a 7a   F65a3PMz w3gFiyJz
0070  35 46 70 66 59 75 5a 73  57 6a 72 76 79 63 4b 6b   5FpfYuZs WjrvycKk
0080  51 72 62 67 49 31 4d 4d  42 63 4d 49 36 45 49 4b   QrbgI1MM BcMI6EIK
0090  38 4a 7a 31 69 4a 49 38  35 67 76 4e 54 31 38 78   8Jz1iJI8 5gvNT18x
00a0  63 70 49 6c 4f 38 72 75  42 35 41 36 61 58 6e 42   cpIlO8ru B5A6aXnB
00b0  43 56 52 4e 67 49 66 64  68 74 48 64 30 64 45 54   CVRNgIfd htHd0dET
00c0  43 58 42 5a 69 78 76 2f  4a 6a 5a 39 48 6d 5a 4f   CXBZixv/ JjZ9HmZO
00d0  6e 70 67 47 78 48 6f 47  4c 55 39 55 6c 43 7a 46   npgGxHoG LU9UlCzF
00e0  62 77 31 38 6d 2f 6d 51  69 76 76 65 5a 67 64 76   bw18m/mQ ivveZgdv
00f0  65 32 42 47 45 56 57 64  2b 31 52 68 58 66 5a 58   e2BGEVWd +1RhXfZX
0100  78 51 51 74 30 70 4e 6e  61 52 54 37 4b 44 55 31   xQQt0pNn aRT7KDU1
0110  4b 5a 4b 54 4c 74 52 77  63 71 57 45 55 35 36 4b   KZKTLtRw cqWEU56K
0120  5a 52 44 65 74 33 63 54  59 44 4d 2f 57 4c 61 79   ZRDet3cT YDM/WLay
0130  58 2f 48 73 42 56 42 55  46 49 5a 4f 6b 48 4a 5a   X/HsBVBU FIZOkHJZ
0140  4e 62 73 7a 77 69 32 52  61 4a 61 65 66 74 51 6f   Nbszwi2R aJaeftQo
0150  69 56 69 32 42 41 51 33  4f 67 54 37 37 2f 51 31   iVi2BAQ3 OgT77/Q1
0160  71 67 38 5a 56 6a 47 61  79 6a 46 33 75 52 4a 39   qg8ZVjGa yjF3uRJ9
```

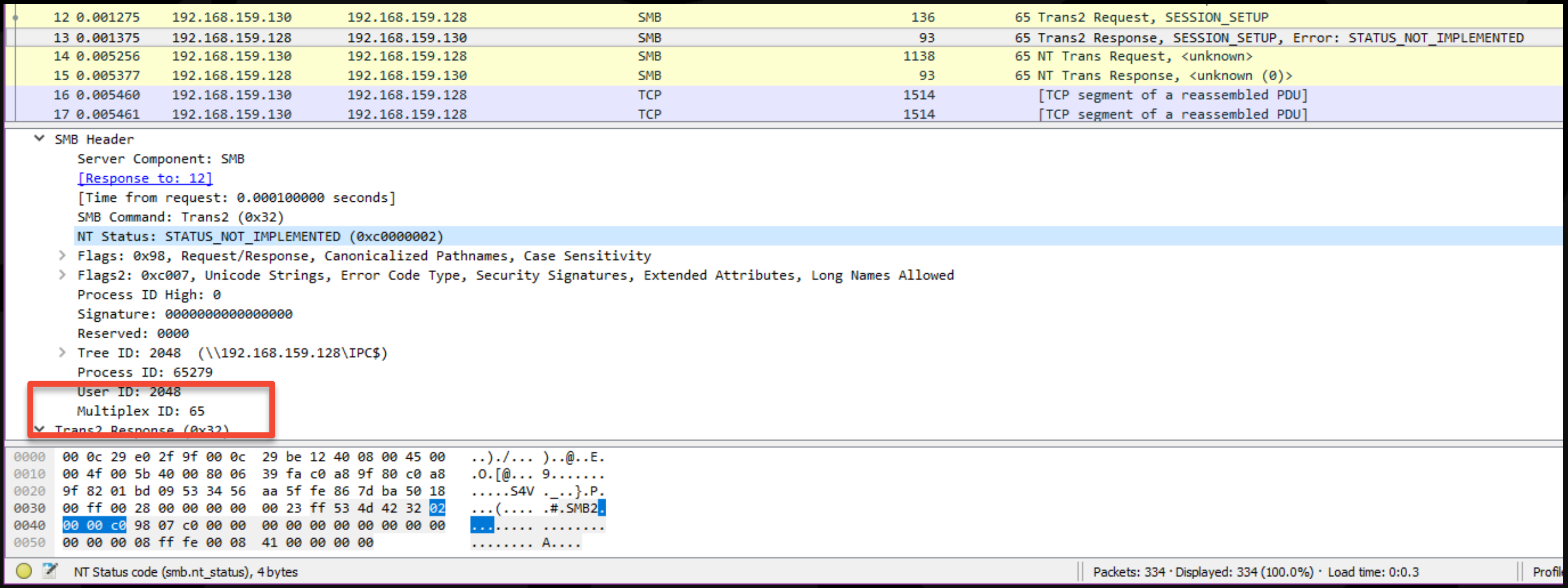
eb_sample

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



NETWORK ANALYSIS

- Interesting Multiplex ID



```
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]
```

```
v 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
v 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 80 06  39 fa c0 a8 9f 80 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            ........ A....
```

NT Status code (smb.nt_status), 4 bytes   Packets: 334 · Displayed: 334 (100.0%) · Load time: 0:0.3   Profil

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?

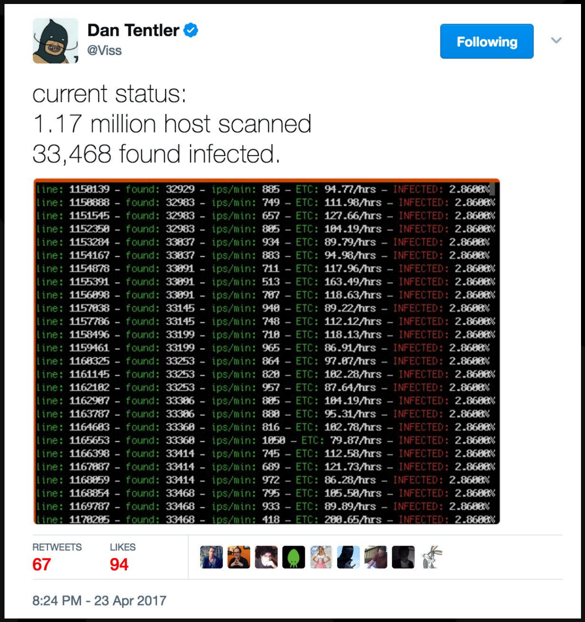
- NETWORK ANALYSIS
- DETECTION CREATION
- IMPACT IDENTIFICATION
- MITIGATION ADVICE
- BINARY ANALYSIS

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

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

```
line: 1150139 - found: 32929 - ips/min: 885 - ETC: 94.77/hrs - INFECTED: 2.8600%
line: 1150888 - found: 32983 - ips/min: 749 - ETC: 111.98/hrs - INFECTED: 2.8600%
line: 1151545 - found: 32983 - ips/min: 657 - ETC: 127.66/hrs - INFECTED: 2.8600%
line: 1152350 - found: 32983 - ips/min: 805 - ETC: 104.19/hrs - INFECTED: 2.8600%
line: 1153284 - found: 33037 - ips/min: 934 - ETC: 89.79/hrs - INFECTED: 2.8600%
line: 1154167 - found: 33037 - ips/min: 883 - ETC: 94.98/hrs - INFECTED: 2.8600%
line: 1154878 - found: 33091 - ips/min: 711 - ETC: 117.96/hrs - INFECTED: 2.8600%
line: 1155391 - found: 33091 - ips/min: 513 - ETC: 163.49/hrs - INFECTED: 2.8600%
line: 1156098 - found: 33091 - ips/min: 707 - ETC: 118.63/hrs - INFECTED: 2.8600%
line: 1157038 - found: 33145 - ips/min: 940 - 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: 710 - ETC: 118.13/hrs - INFECTED: 2.8600%
line: 1159461 - found: 33199 - ips/min: 965 - ETC: 86.91/hrs - INFECTED: 2.8600%
line: 1160325 - found: 33253 - ips/min: 864 - ETC: 97.07/hrs - INFECTED: 2.8600%
line: 1161145 - found: 33253 - ips/min: 820 - ETC: 102.28/hrs - INFECTED: 2.8600%
line: 1162102 - found: 33253 - ips/min: 957 - ETC: 87.64/hrs - INFECTED: 2.8600%
line: 1162907 - found: 33306 - ips/min: 805 - ETC: 104.19/hrs - INFECTED: 2.8600%
line: 1163787 - found: 33306 - ips/min: 880 - ETC: 95.31/hrs - INFECTED: 2.8600%
line: 1164603 - found: 33360 - ips/min: 816 - ETC: 102.78/hrs - INFECTED: 2.8600%
line: 1165653 - found: 33360 - ips/min: 1050 - ETC: 79.87/hrs - INFECTED: 2.8600%
line: 1166398 - found: 33414 - ips/min: 745 - ETC: 112.58/hrs - INFECTED: 2.8600%
line: 1167087 - found: 33414 - ips/min: 689 - ETC: 121.73/hrs - INFECTED: 2.8600%
line: 1168059 - found: 33414 - ips/min: 972 - ETC: 86.28/hrs - INFECTED: 2.8600%
line: 1168854 - found: 33468 - ips/min: 795 - ETC: 105.50/hrs - INFECTED: 2.8600%
line: 1169787 - found: 33468 - ips/min: 933 - ETC: 89.89/hrs - INFECTED: 2.8600%
line: 1170205 - found: 33468 - ips/min: 418 - ETC: 200.65/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?

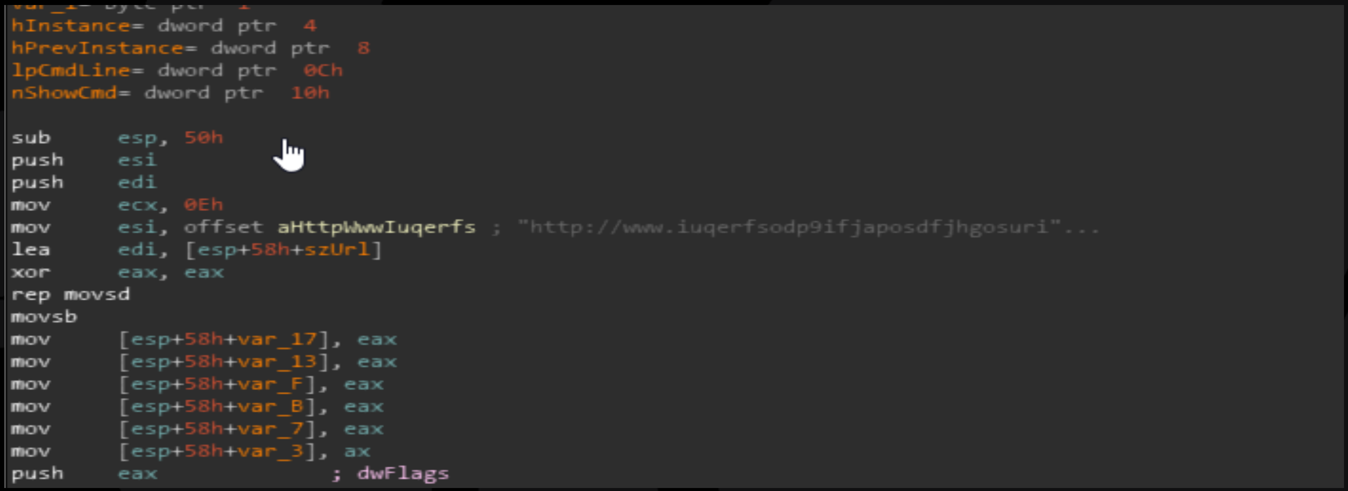
- What did Riot do?
  - Suricata detections
  - No external SMB
  - Firewalled Inbound SMB on workstations

WHAT CAN I DO?

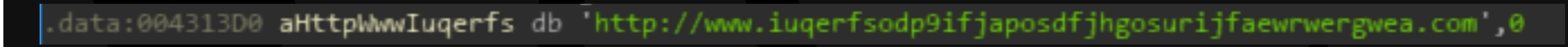
- NETWORK ANALYSIS
- DETECTION CREATION
- IMPACT IDENTIFICATION
- MITIGATION ADVICE
- BINARY ANALYSIS

BINARY ANALYSIS

- Sometimes worthwhile disassembling



```
var_1= byte ptr -1
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_B], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_3], ax
push    eax             ; dwFlags
```



```
.data:004313D0 aHttpWwwIuqerfs db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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