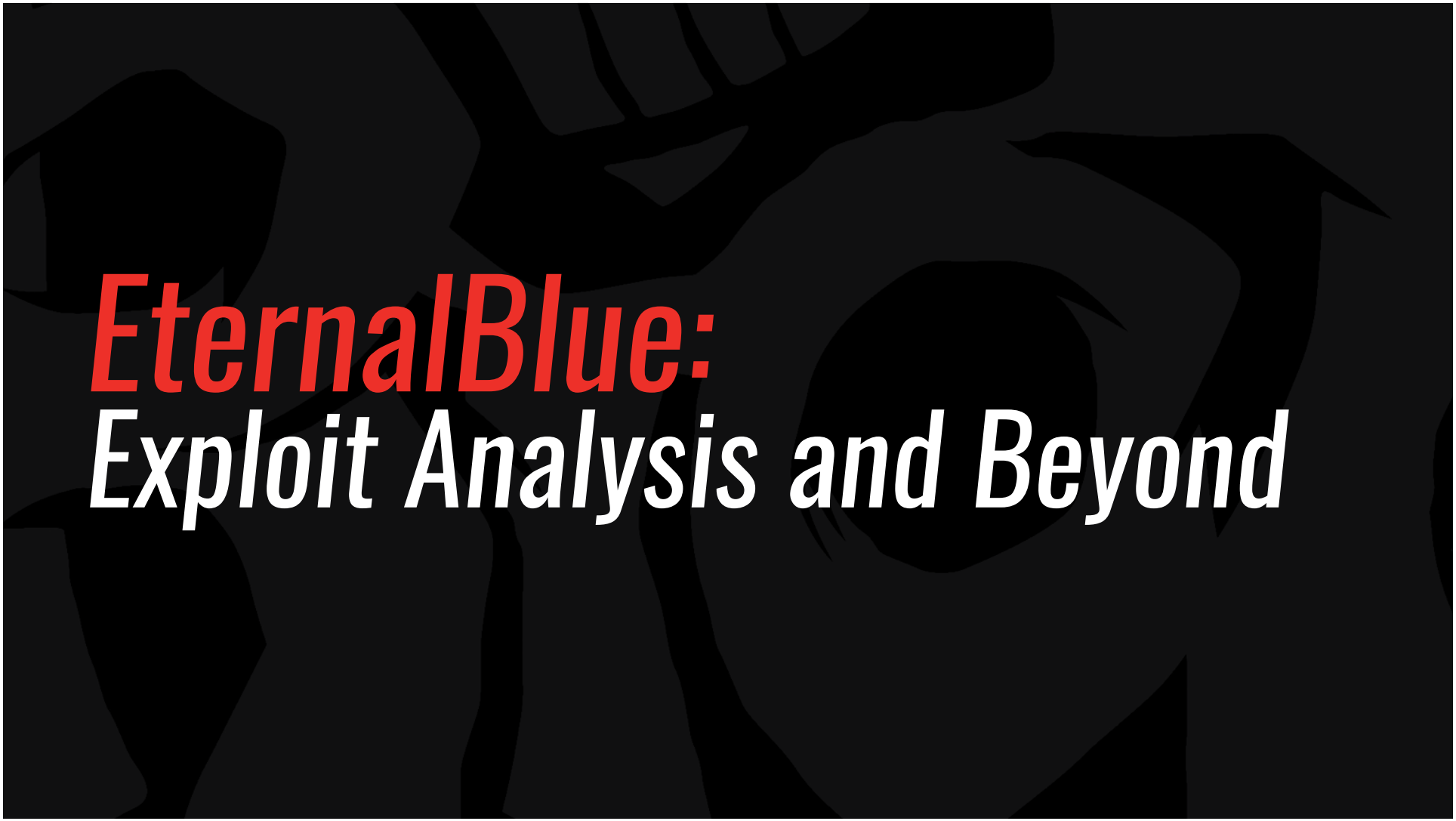

EternalBlue:
Exploit Analysis and Beyond

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 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 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

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

WHAT

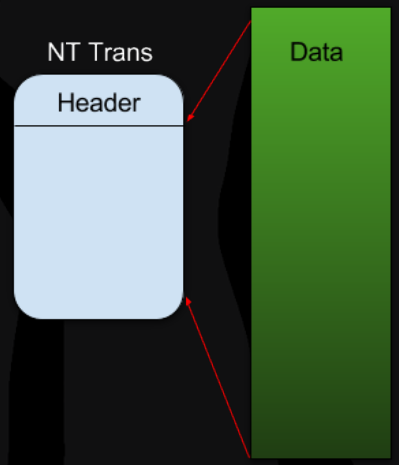
HOW

THEN WHAT

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



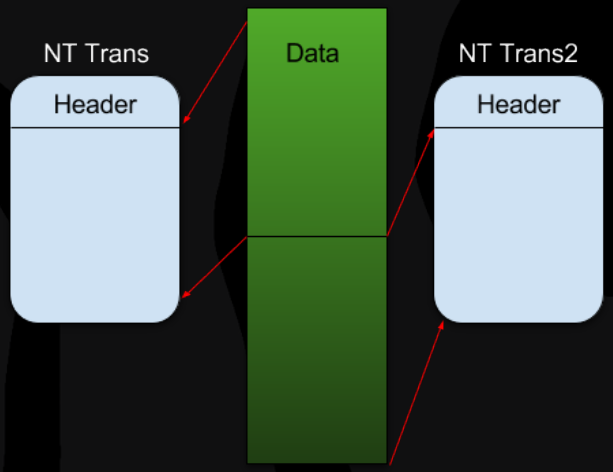
WHAT

HOW

THEN WHAT

ETERNALBLUE

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



WHAT

HOW

THEN WHAT

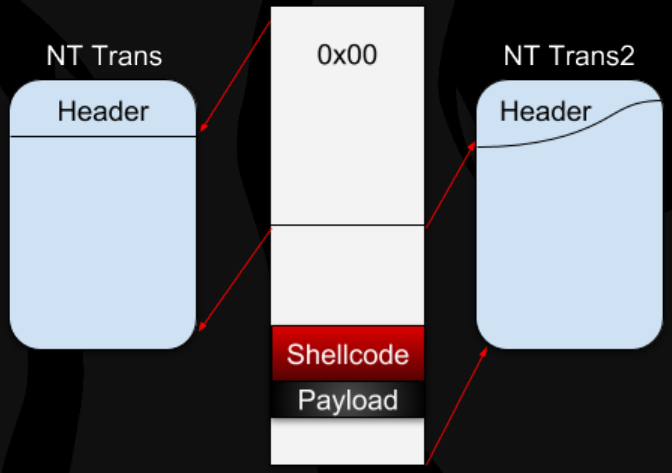
ETERNALBLUE

- 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



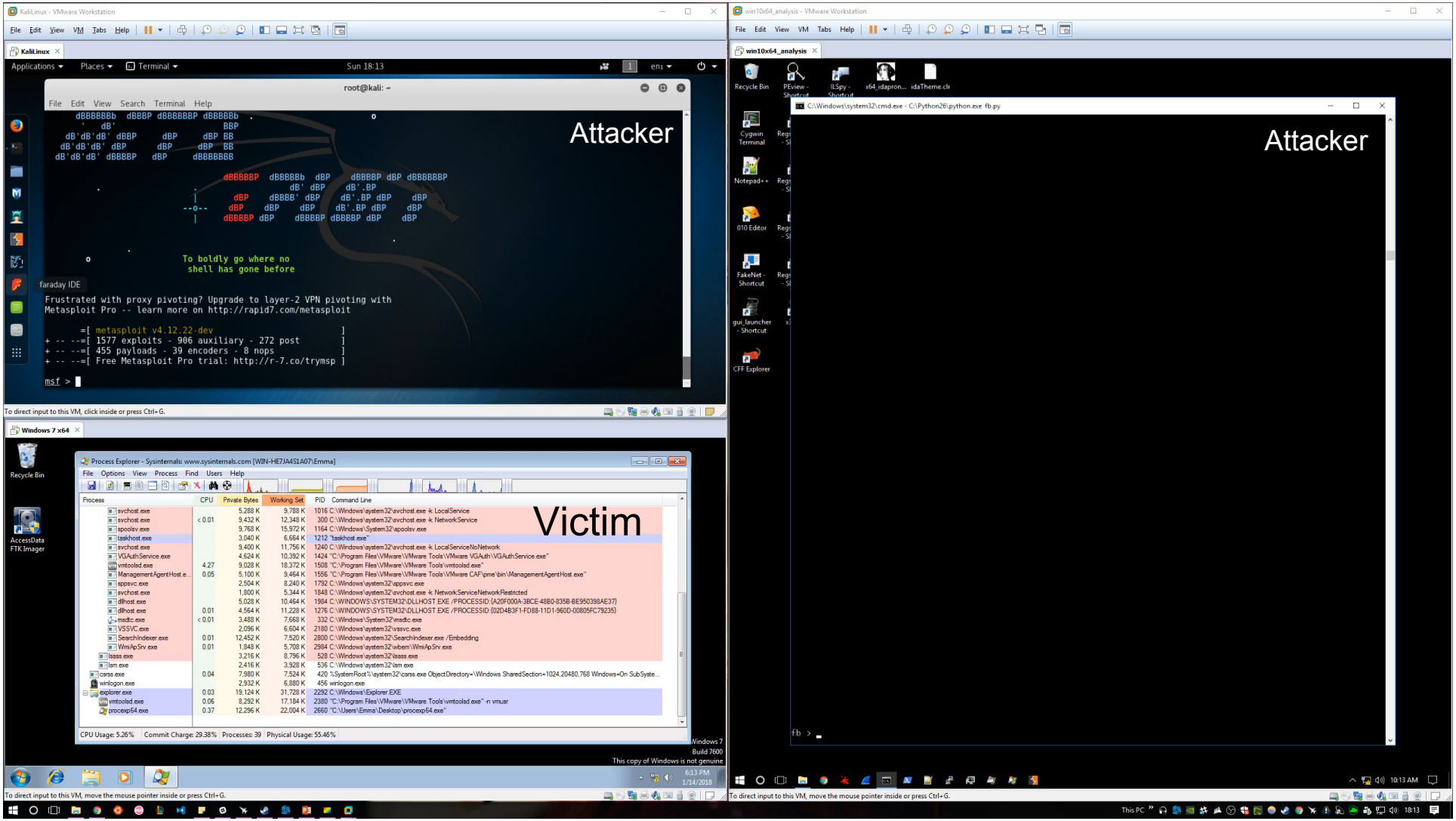
ETERNALBLUE

- 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

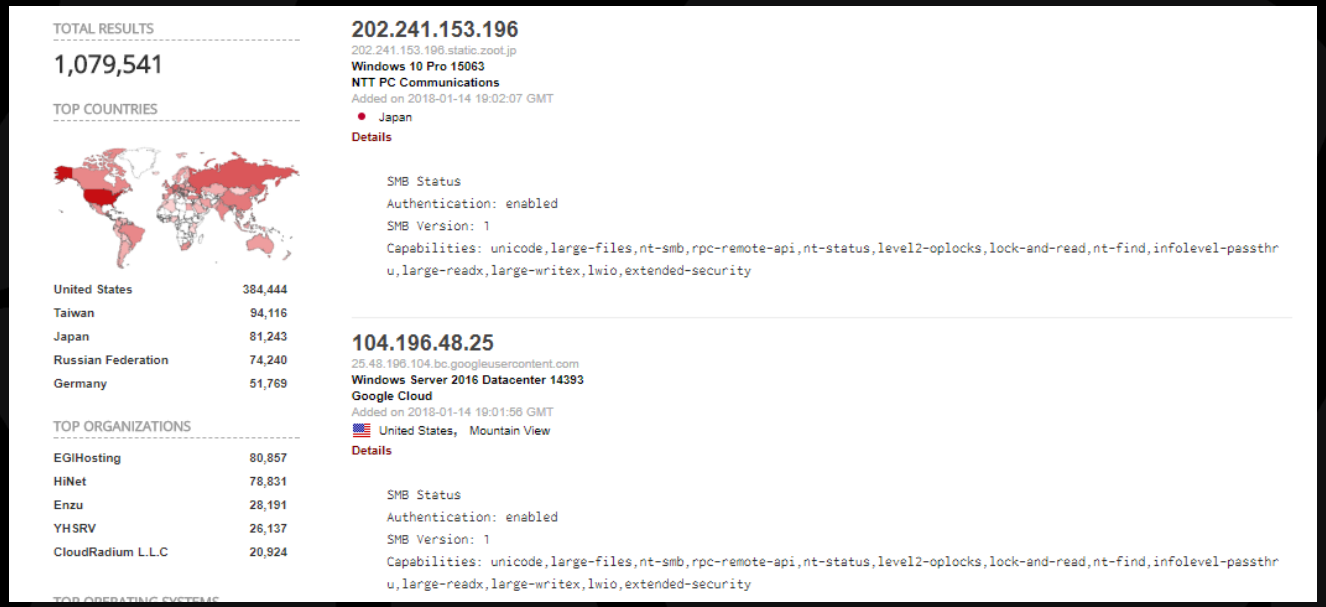
HOW

THEN WHAT


KaliLinux - VMware Workstation
root@kali: ~
Attacker
To boldly go where no
shell has gone before
faraday IDE
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 >
To direct input to this VM, click inside or press Ctrl+G.
Windows 7 x64
Process Explorer - Sysinternals: www.sysinternals.com [WIN-HE7JA4S1A07\Emma]
Victim
Windows 7
Build 7600
This copy of Windows is not genuine
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
win10x64_analysis - VMware Workstation
C:\Windows\system32\cmd.exe - C:\Python26\python.exe fb.py
Attacker
fb >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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

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

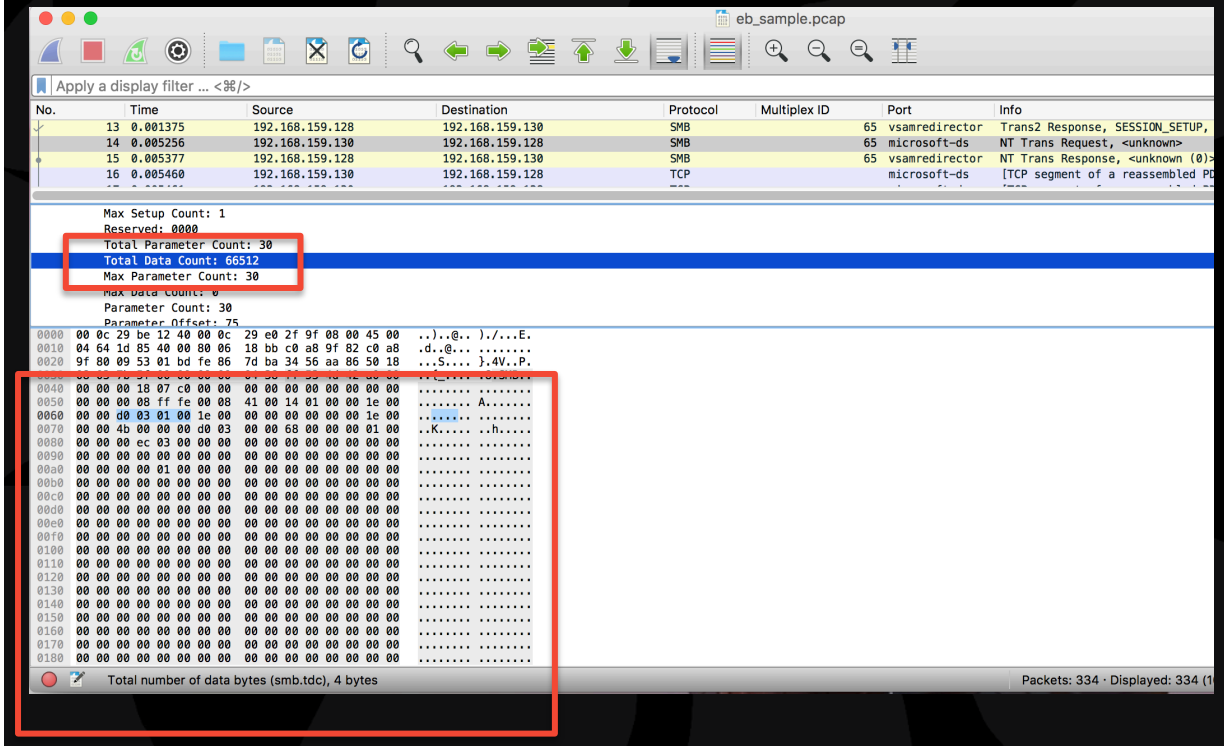
WHAT CAN I DO?

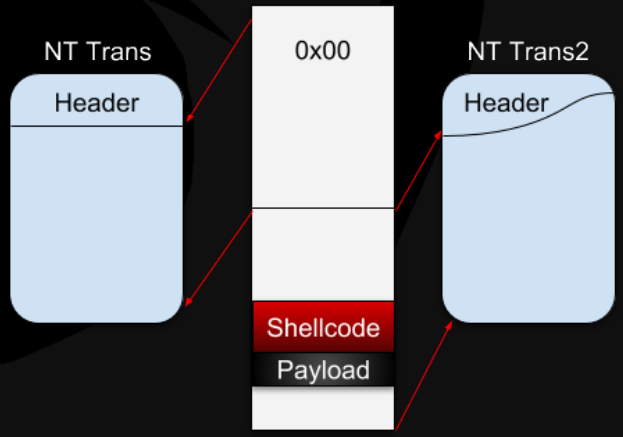
- NETWORK ANALYSIS
- DETECTION CREATION
- IMPACT IDENTIFICATION
- MITIGATION ADVICE
- BINARY ANALYSIS

NETWORK ANALYSIS

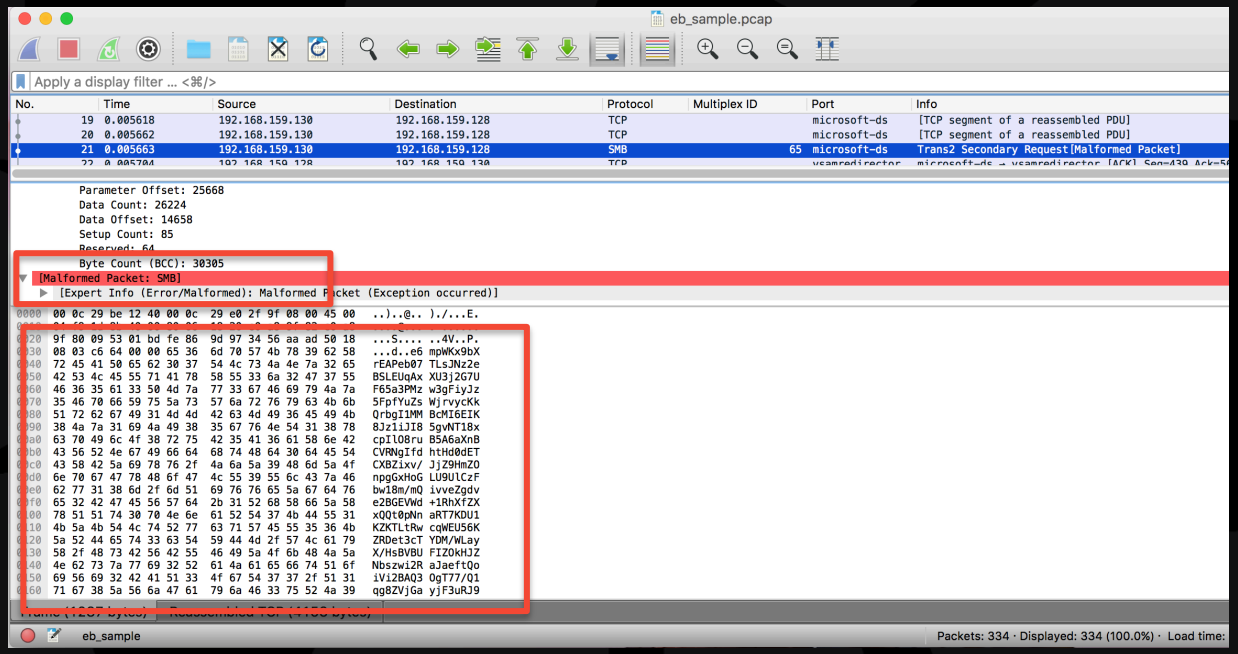
- Run it.
  - ….. In a lab!
  - https://medium.com/@xNymia For all your lab creation needs
- Sysinternals and Wireshark are your best friends
- Comparison against known good SMB traffic
- Look for irregularities and patterns in multiple samples
- Check protocol docs

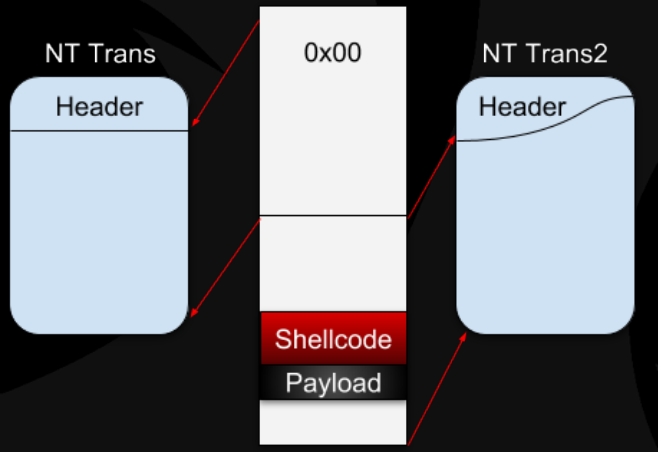
NETWORK ANALYSIS





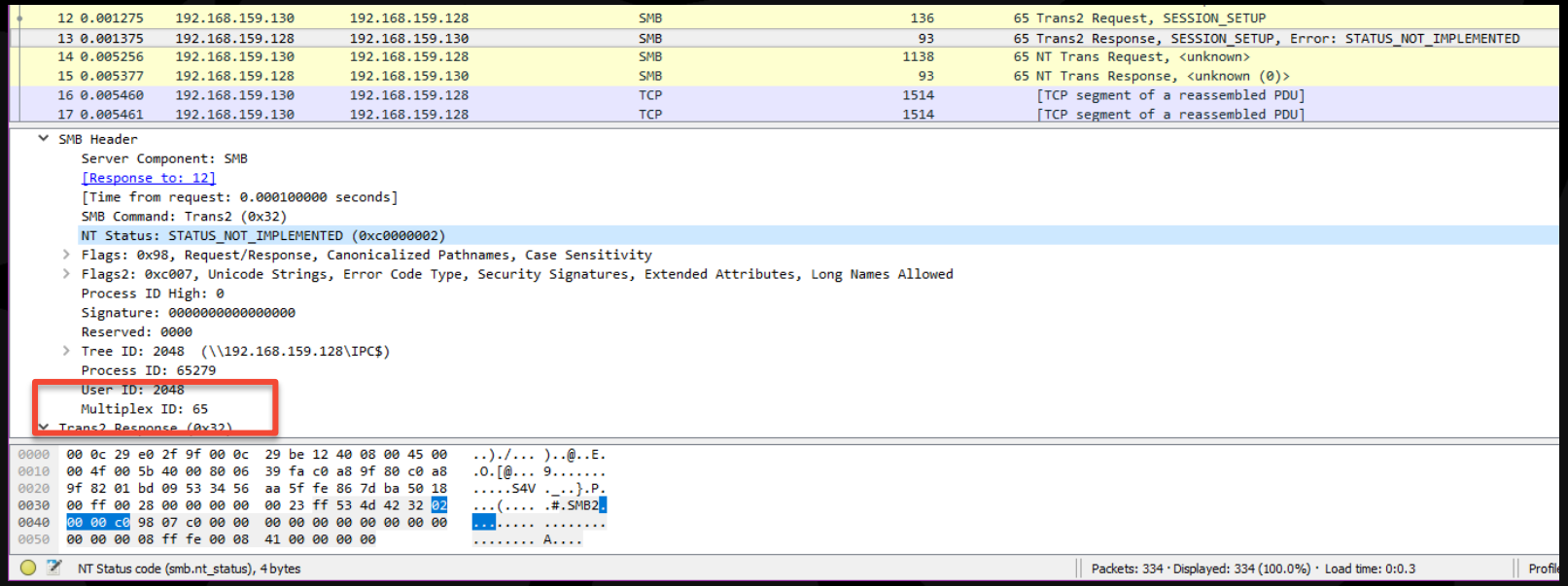
NETWORK ANALYSIS





NETWORK ANALYSIS

- Interesting Multiplex ID



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 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?

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

```
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.

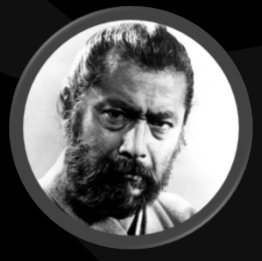
… AND BEYOND

- 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

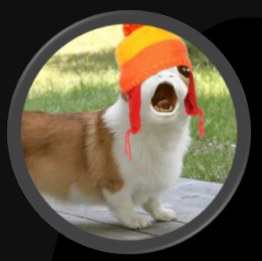
Be Heard

THE GANG

Dan Tentler
@Viss



DEY!
@ronindey



Kevin Beaumont
@GossiTheDog

Emma McCall
@RiotNymia