個案分析-

K大學 SYN Flood 的殭屍主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/2

I. 事件簡介

1. 近期接獲該校資訊安全管理的老師反映，校內有一台主機疑似遭受入侵成為駭客所用的殭屍電腦。
2. 該主機主要因為占用大量的網路頻寬流量，造成網路壅塞而被發現疑似正在進行中繼站或者其他攻擊行為。
3. 本單位協助該校進行封包側錄並鑑識，找出其發生的原因及解決方式。
4. 經過詢問主機基本狀態，為一台 Ubuntu Linux 主機並有啟用 SSH service 讓管理者方便登入維護。

II. 事件檢測

1. 透過 SSH 遠端登入該主機檢查網路狀態，並透過 netstat 指令發現有可疑連線正與外部 IP 的 port 2822 進行連線，而該連線的程式名稱卻是 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.[redacted]:36143    118.193.206.44:2822     ESTABLISHED 883/gnome-terminal
tcp   140.[redacted]:22       140.[redacted]:49816    ESTABLISHED 2415/sshd: [redacted] [pr
tcp6  :::22                   :::*                    LISTEN      920/sshd
tcp6  ::1:631                 :::*                    LISTEN      553/cupsd
```

2. 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/woqcayiyan
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)
```

3. 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:~#
```

4. 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。

   1. 「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/loc
al/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
~
~
```

5. 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/S90woqcayiyan」。

```
root@ubuntu:~# locate S90woqcayiyan
/etc/rc1.d/S90woqcayiyan
/etc/rc2.d/S90woqcayiyan
/etc/rc3.d/S90woqcayiyan
/etc/rc4.d/S90woqcayiyan
/etc/rc5.d/S90woqcayiyan
root@ubuntu:~#
```

6. 捷徑檔 S90woqcayiyan 為連結至路徑檔案「/etc/init.d/woqcayiyan」，並檢視其內容可知真正作用的執行檔確實位於「/boot/woqcayiyan」，且不論以何運行級別[1-5]開機皆會啟用。

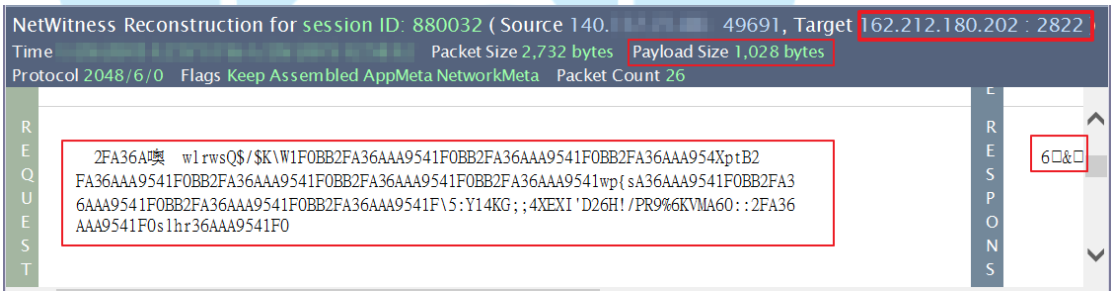
```
# Default-Start:        1 2 3 4 5
# Default-Stop:
# Short-Description:    woqcayiyan
### END INIT INFO
case $1 in
start)
        /boot/woqcayiyan
        ;;
stop)
        ;;
*)
        /boot/woqcayiyan
        ;;
esac
```

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

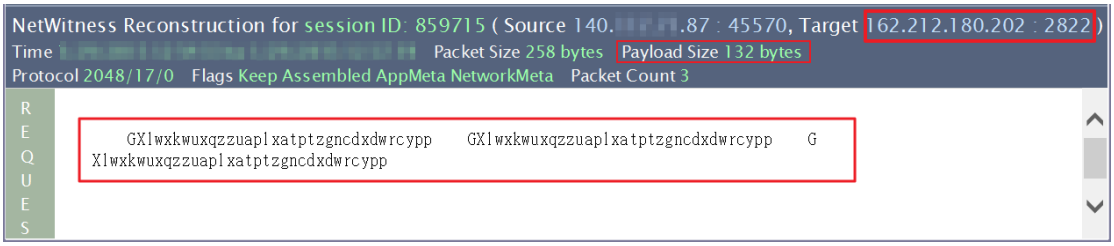
7. 檢查其側錄的封包內容得知，惡意程式主要會連到外部的 port 80 和 port 2822，其中 port 2822 的連線數很少，大多都是 port 80 連線數最多。

8. 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 主機或中繼站。

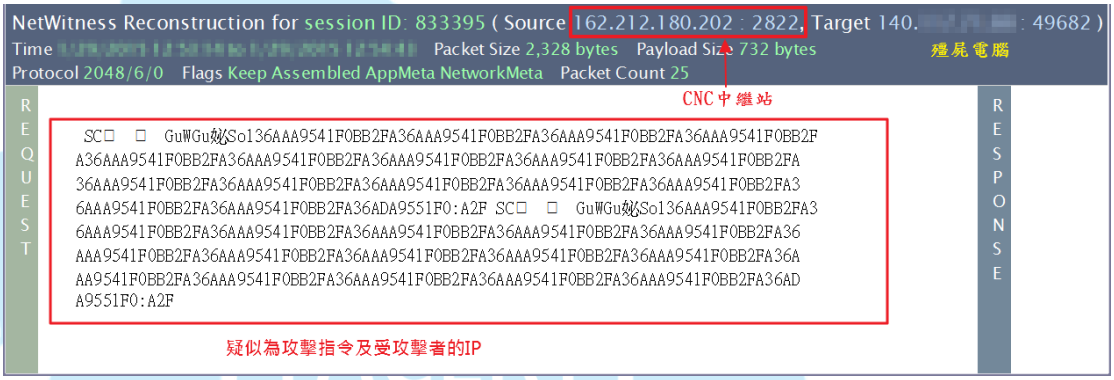
   1. 隨機檢視一個 session，由主機 IP 向美國的位址 162.212.180.202 的 TCP port 2822 進行資料傳送，而傳送資料都是經過加密，此可能為回報用途。



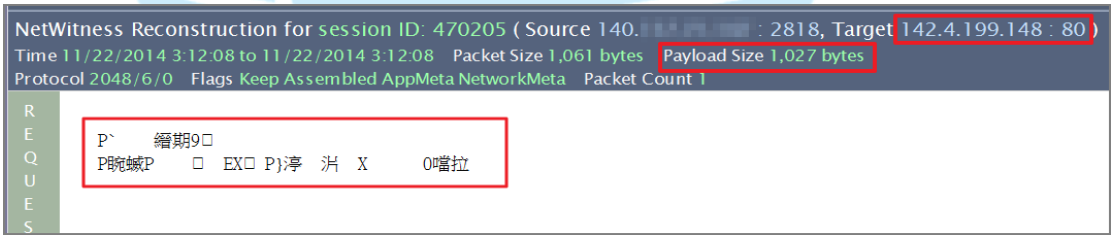
   2. 另一種是主機端會偽造成其他 IP 向 C&C 162.212.180.202 的 UDP port 2822 進行資料回報，其為 132bytes 經過加密的內容大小，而其偽造的規則通常只是隨機改變原本 IP 的幾個數字。



3. 待 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。



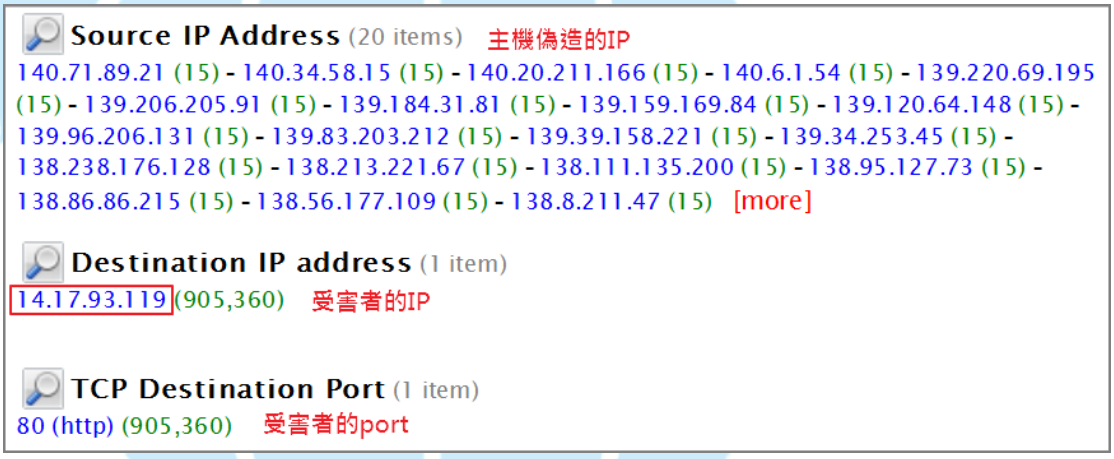
9. 查看 port 80 的連線狀態，主要殭屍主機收到上層 C&C 指令後，在短時間內耗盡可用頻寬，開始大量向外部 IP 進行 SYN Flood 的攻擊，並且送出的都是 payload 為 1Kbyte 的 SYN 加密封包。



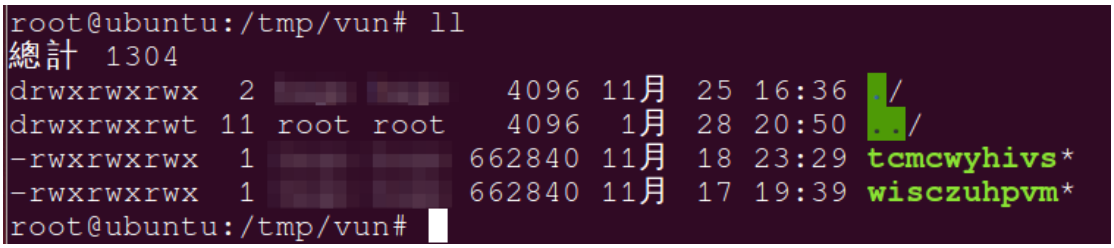
10. 該惡意程式進行 SYN Flood 的攻擊態樣有兩種：

1. 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。

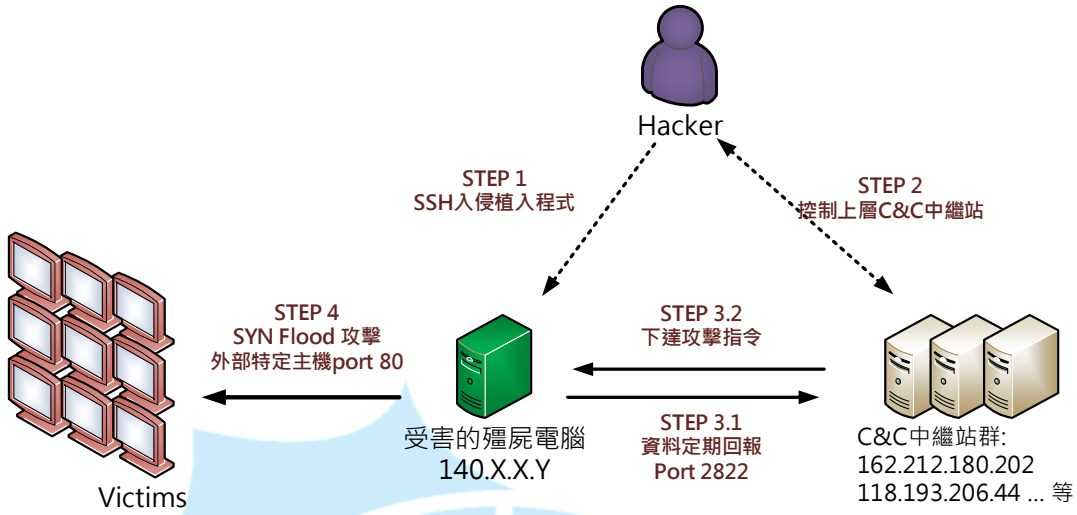
2. 一種是偽造本機端的大量 IP 對單一特定主機進行攻擊，此種方式完全捨棄原本機端的 IP，全而偽造成其他 IP 來進行攻擊，來躲避追查來源端，受害者也多為網站伺服器。從記錄上來看偽造的 IP 數量約 50000 筆，國家數為 171 國。



11. 最後在「/tmp/vun/」 資料夾中發現兩支可疑的程式，分別為「tcmcwyhivs」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後續結果。



III. 網路架構圖



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。

IV. 運作流程與結論

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「tcmcwyhivs」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/woqcayiyan」。
4. 該 woqcayiyan 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。

V. 問題排除與防範建議

1. 先移除被植入的後門檔案 /tmp/vun/「tcmcwyhivs」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/S90woqcayiyan 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。