個案分析-

C 大學的中繼站主機分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/2

I. 事件簡介

1. 近期接獲行政院 ICST 通報 C 大學疑似一台主機 120.X.X.2 感染成為 C&C 中繼站。
2. 該主機是一台 windows server 2008 的系所網頁伺服器，主要提供系所介紹及相關資訊。
3. 此外該主機有啟用 FTP 服務供系上老師及學生能夠上傳或下載資料。
4. 該主機同時會占用大量網路頻寬，造成系所對外網路速度不穩。
5. 本單位偕同 ICST 前往該大學進行數位鑑識並且側錄主機封包。

II. 事件檢測

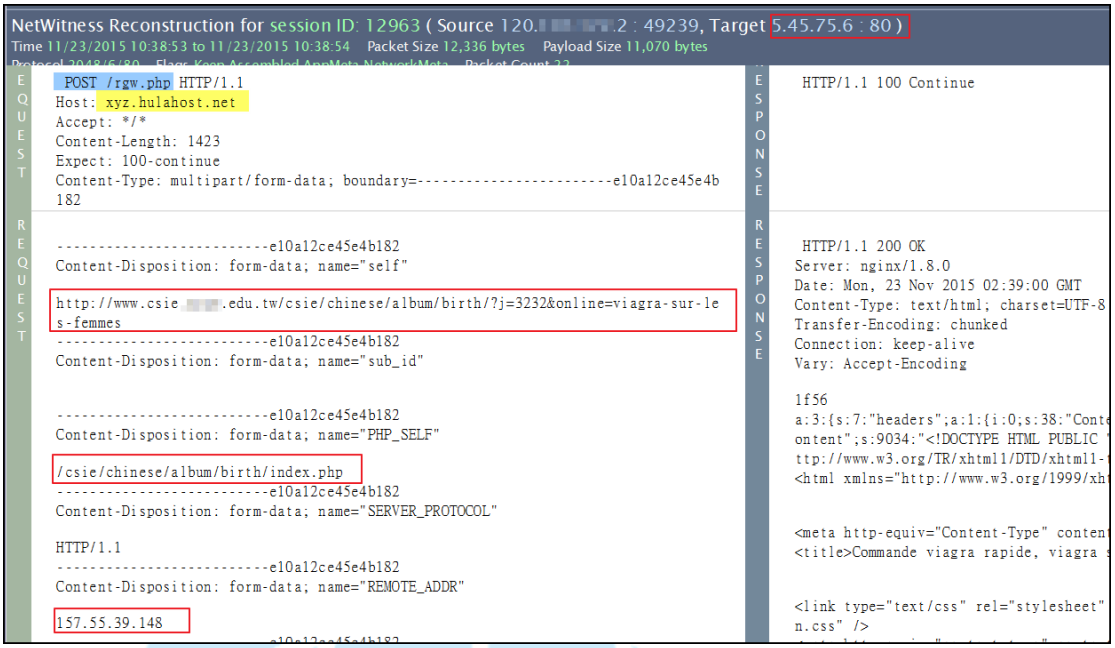
1. 從 netstat 指令得知，該主機有開啟 port 80 及 21，分別為 Web service、FTP service 供使用者能夠存取。

```
 5    TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
 6   [inetinfo.exe]
 7    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
 8   [httpd.exe]
 9    TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
10    RpcSs
11   [svchost.exe]
12    TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
```

2. 從背景程序列表中檢查，PID 2308 的程式 anydesk.exe 疑似是被植入的軟體，並非使用者安裝。

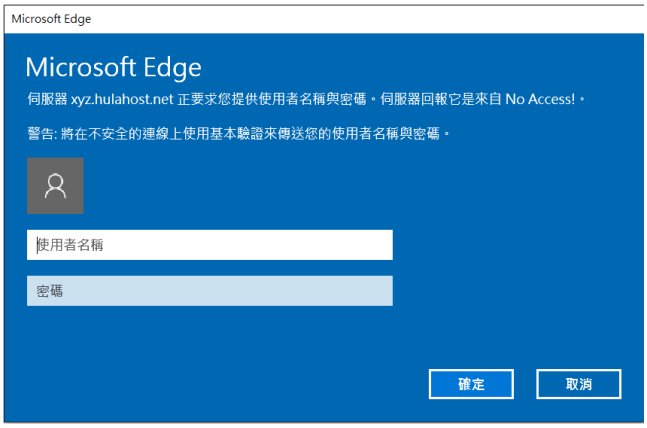
```
47  cmd.exe          3372 Services    0    2,124 K Unknown         NT AUTHORITY\SYSTEM
48  anydesk.exe      3800 Services    0   12,760 K Unknown         NT AUTHORITY\SYSTEM
49  cmd.exe          4128 Services    0    2,096 K Unknown         NT AUTHORITY\SYSTEM
50  anydesk.exe      2308 Services    0   12,768 K Unknown         NT AUTHORITY\SYSTEM
51  UI0Detect.exe     656 Services    0    6,040 K Unknown         NT AUTHORITY\SYSTEM
52  httpd.exe        5016 Services    0   67,928 K Unknown         NT AUTHORITY\SYSTEM
```

3. 從封包紀錄中得知，主機會大量向紐西蘭目的端 5.45.75.6 發送大量封包，主要是透過網域名稱 xyz.hulahost.net 進行 HTTP POST 連線。傳送內容包含一些其他遠端主機 IP 及 PHP 等資訊。



4. 透過 Virustotal 掃描該網址 xyz.hulahost.net，偵測比例為 1/66 的惡意網站。

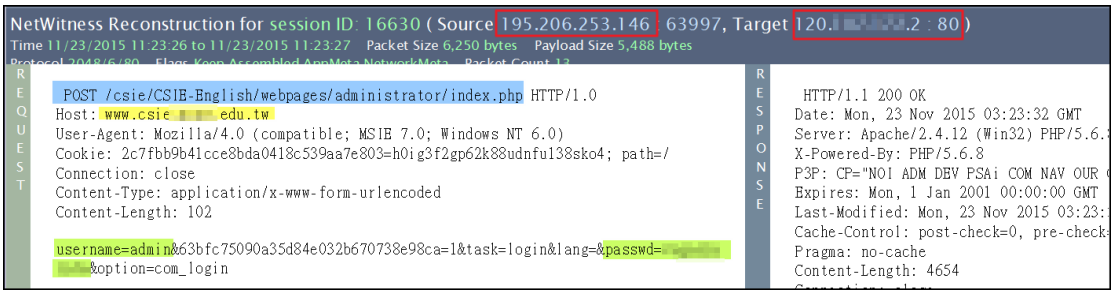
5. 透過瀏覽器開啟該網址 xyz.hulahost.net 會出現要求輸入帳號密碼的登入頁面，可能為駭客所使用的一台 C&C 主機。

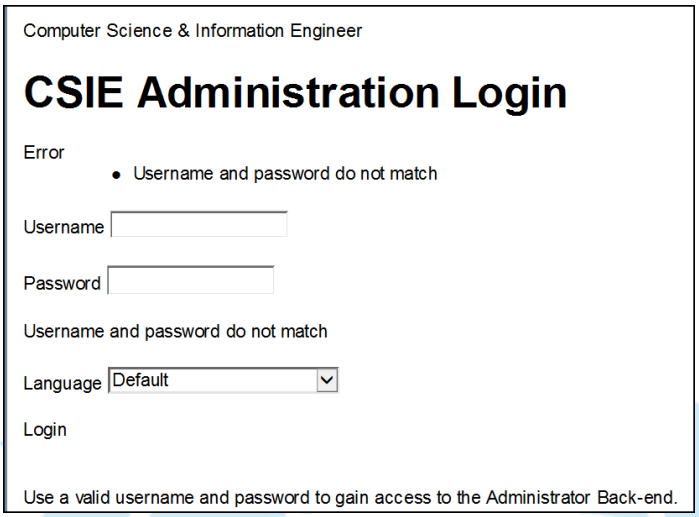


6. 此外從主機的網址路徑 http://120.X.X.2/img/log.log 檔案中，發現到很多紀錄包括了 IP、OS 版本、瀏覽器版本及網址等資訊。推論這些可能是存取過網站 www.molihua.org 的 IP 紀錄，並被駭客將資料存放在 120.X.X.2 的 web server 中。

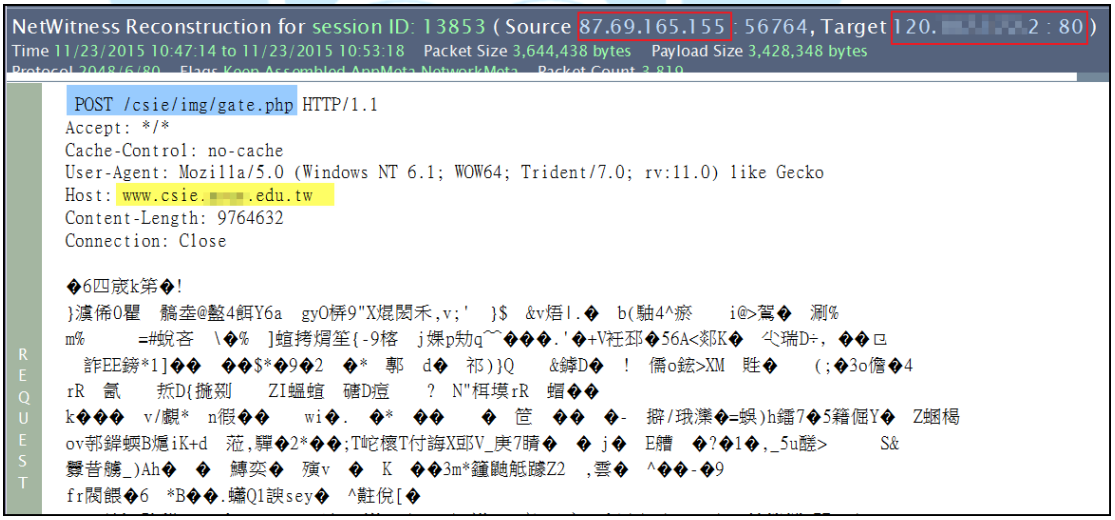
```
109 IP:157.55.112.222 美国微软公司
110 OS:Windows XP
111 Browser:Internet Explorer 7.0
112 Flash:WIN 9,0,115,0
113 JRE:1.7.0
114 Referer:http://www.molihua.org/2011/10/blog-post_369.html
115 Language:en-us
116 Time:2012-12-06 10:08:48 AM
117
118 IP:74.125.184.19 美国加利福尼亚州山景市谷歌公司
119 OS:Windows 95
120 Browser:Chrome 23.0.1271.95
121 Flash:Shockwave Flash 11.5 r31
122 JRE:1.7.0_05
123 Referer:http://www.molihua.org/2012/07/blog-post_919.html
124 Language:zh-CN
125 Time:2012-12-06 11:12:19 AM
```

7. 封包紀錄中有大量的外部 IP 嘗試並且成功存取主機 120.X.X.2 的 Web service，其中以俄羅斯聯邦的 IP 數量最多。路徑為 /csie/CSIE-English/webpages/administrator/index.php，並且使用 HTTP POST 方式成功登入該主機，內容包含了登入帳號及密碼。

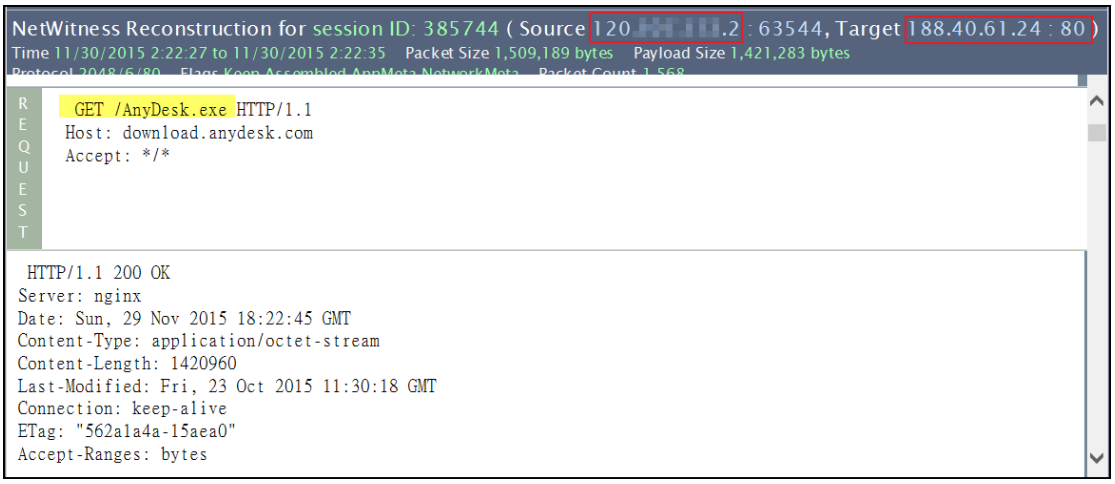




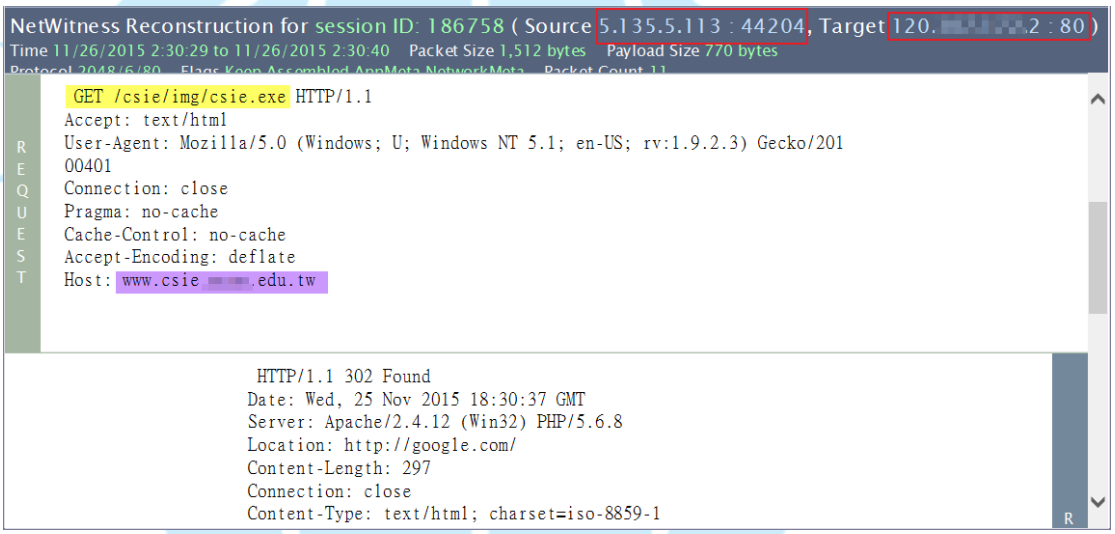
8. 其次排名第二多的外部 IP 為以色列的 87.69.165.155，此 IP 透過 HTTP POST 到 /csie/img/gate.php 所接收，其內容是經過加密過的密文無法解讀，且 payload size 都有 3MB 以上，推論可能包含重要的機敏資訊。在此可以斷定該路徑 /csie/img/ 內容應該就是駭客所植入。



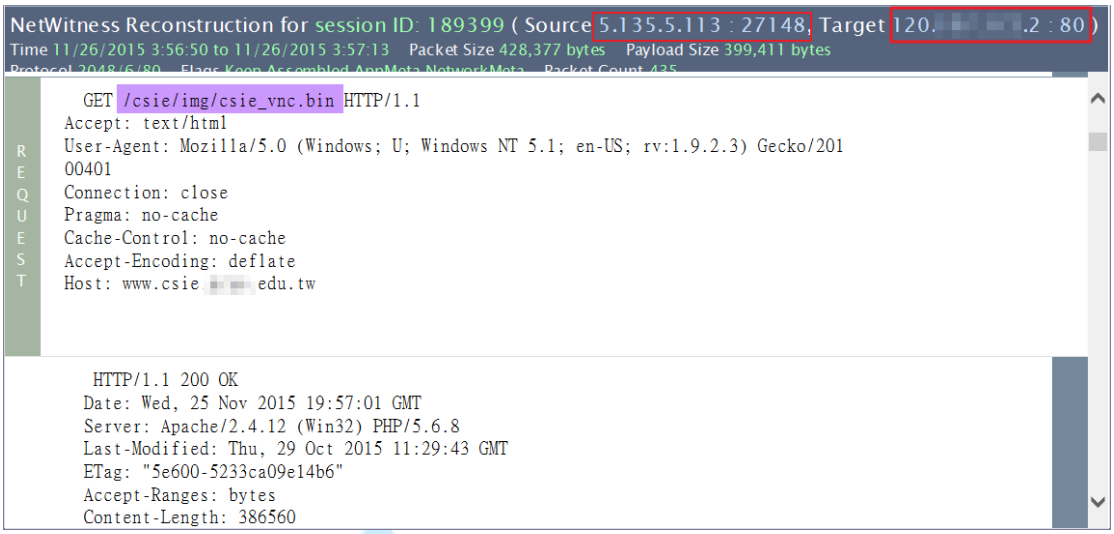
9. 封包紀錄中有觀察到該主機向德國 188.40.61.24 下載安裝一個 AnyDesk.exe，該程式雖非惡意程式，但是為遠端桌面控制軟體，且可能為駭客所用。



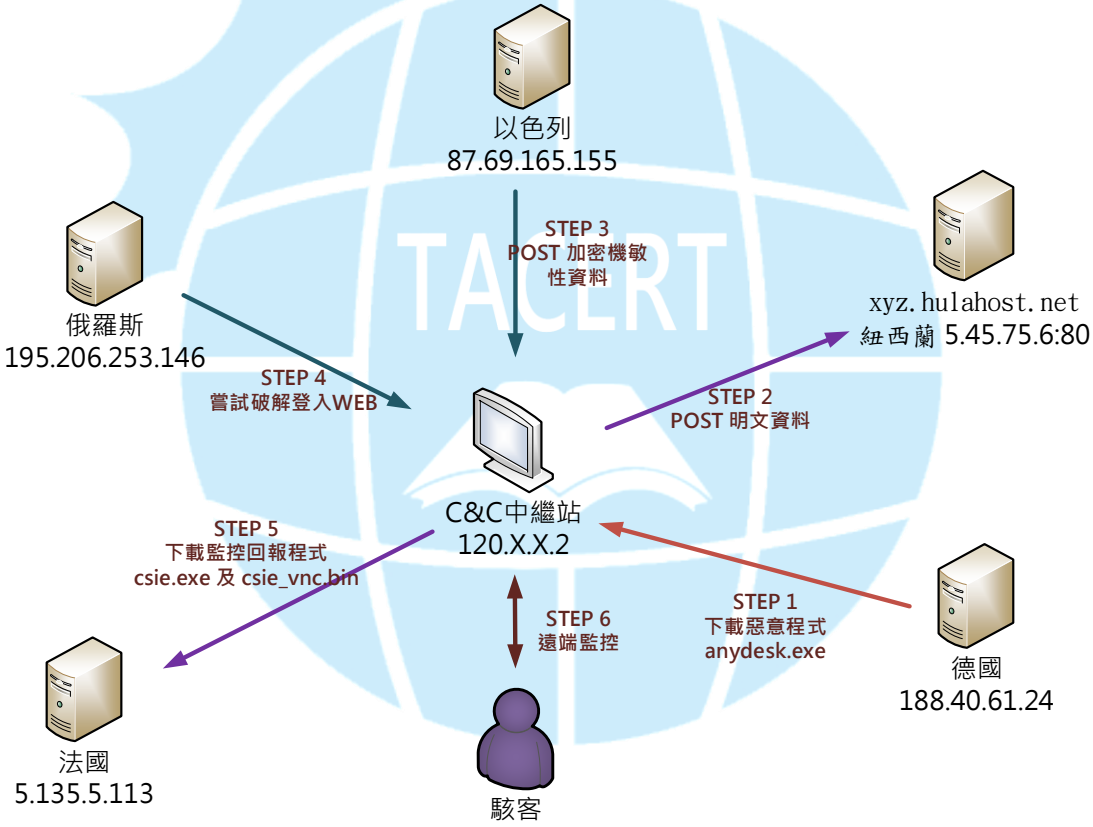
10. 共 345 個相異外部 IP 會嘗試向該感染主機下載 /csie/img/csie.exe 執行檔，以法國的 5.135.5.113 為最多，不過該 csie.exe 執行檔在側錄封包期間已經被移除，可能為底層殭屍電腦固定報到用途。



11. 封包紀錄中有來自許多國外 IP 的連線，以透過 HTTP GET 存取一個 bin 的執行檔案，位置是網站的 /csie/img/csie_vnc.bin。其中以法國 5.135.5.113 存取次數最多，平均間隔 20 分鐘下載一次，應為監控主機存活使用。



III. 網路架構圖



1. 使用者可能下載到惡意程式 anydesk.exe 成為駭客的中繼站。
2. 主機感染惡意程式後會向 xyz.hulahost.net 傳送底層 BOT 的資料。
3. 底層許多 BOT 如以色列 IP 向中繼站傳送加密過的機敏性資料。
4. 許多外部主機嘗試暴力破解登入中繼站 Web 主機的後台。
5. 部分主機如法國 5.135.5.113 持續向中繼站下載惡意檔案 csie.exe 和

csie_vnc.bin，推斷用來監控中繼站的存活。

IV.建議與總結

1. 此個案取得資訊大多以側錄封包為主，故只能以網路封包去推論中繼站的網路行為。
2. 該主機疑似因為 HTTP 的漏洞而遭受感染成為 C&C 中繼站，並在 Web 路徑資料夾中植入 /img/ 的惡意程式，如 gate.php 和 cise_vnc.bin。
3. 該主機同時也會下載安裝 anydesk.exe 的遠端控制軟體讓駭客操控。
4. 該中繼站會接收來自底層殭屍電腦的資料，並且向上層發送加密或明文的資料，加密資料可能包含重要的機敏性資訊。
5. 因為該主機有啟用登入 Web 後台頁面，故被大量主機嘗試暴力登入 Web 後台。
6. 該主機也被駭客用來暫存其他網站 www.molihua.org 的登入紀錄，該網站主要是反對中國政權的內容議題。
7. 網站管理者要時常檢測 Log 紀錄及通訊埠使用情形，以避免遭受駭客入侵成為 C&C 中繼站。