個案分析-

N 大學受感染的中繼站主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/8

I. 事件簡介

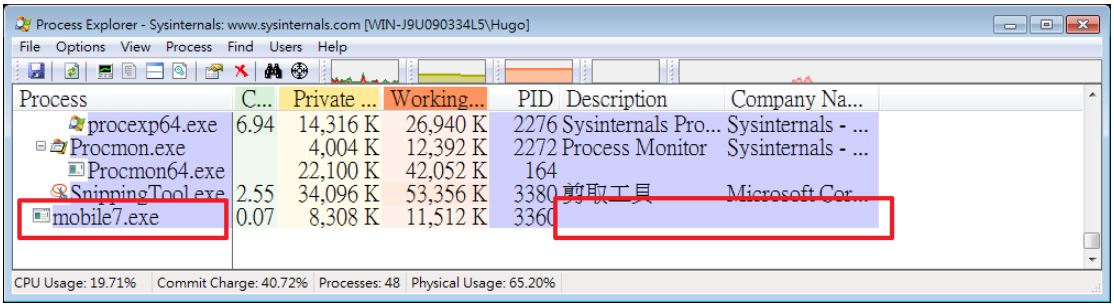
1. 該大學某主機被行政院技服中心偵測到有中繼站惡意連線行為，並偕同本單位協助進行處裡。
2. 該主機為一台作業系統 Win7 的實驗用虛擬機器。
3. 該主機會占用大量的網路頻寬，並且被偵測到有惡意網域名稱對應到該主機 IP。
4. 本單位偕同技服中心針對該主機進行封包側錄並數位鑑識。

II. 事件檢測

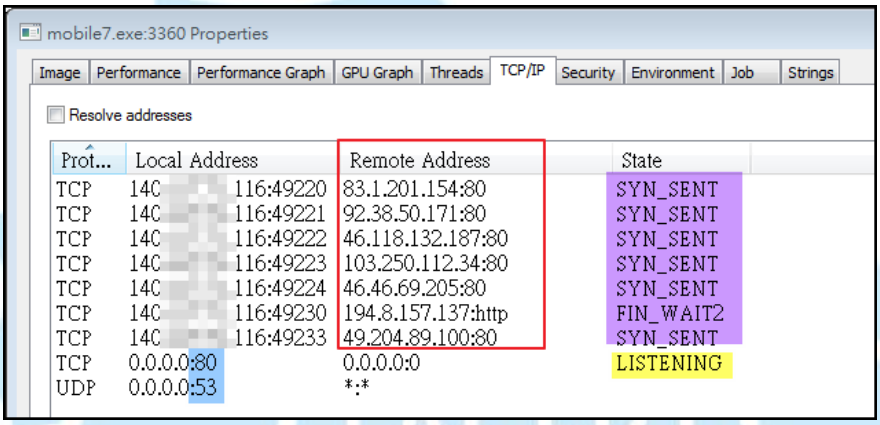
1. 首先檢測該主機的網路連線行為是否異常，透過 tcpview 工具可以看到，有一支 PID 為 0 的未知程式和 mobile7.exe 產生大量的對外網路連線，並且都是連到外部 IP 的網站通訊埠 port 80。
2. 此外 mobile7.exe 的程式開啟了本地通訊埠，分別是 TCP port 80 和 UDP port 53 進行監聽接收。

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
mobile7.exe	2544	TCP	0.0.0.0	80	0.0.0.0	0	LISTENING
mobile7.exe	2544	UDP	0.0.0.0	53	*	*	
[System Process]	0	TCP	140. 116	55195	176.103.55.73	80	TIME_WAIT
mobile7.exe	2544	TCP	140. 116	49213	89.144.2.115	80	ESTABLISHED
[System Process]	0	TCP	140. 116	55207	176.103.54.73	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55208	89.144.2.119	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55209	89.144.2.119	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55210	89.144.2.115	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55211	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55212	176.103.54.73	80	TIME_WAIT
mobile7.exe	2544	TCP	140. 116	55213	176.103.54.73	80	ESTABLISHED
[System Process]	0	TCP	140. 116	55214	89.144.2.119	80	TIME_WAIT
mobile7.exe	2544	TCP	140. 116	55215	89.144.2.119	80	ESTABLISHED
[System Process]	0	TCP	140. 116	55216	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55217	89.144.2.115	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55218	176.103.55.73	80	TIME_WAIT
[System Process]	0	TCP	140. 116	55219	89.144.2.115	80	TIME_WAIT
mobile7.exe	2544	TCP	140. 116	55220	89.144.2.119	80	ESTABLISHED
[System Process]	0	TCP	140. 116	55221	89.144.2.119	80	TIME_WAIT
mobile7.exe	2544	TCP	140. 116	80	123.20.196.234	1096	ESTABLISHED
mobile7.exe	2544	TCP	140. 116	80	177.91.249.28	2283	SYN_RCVD

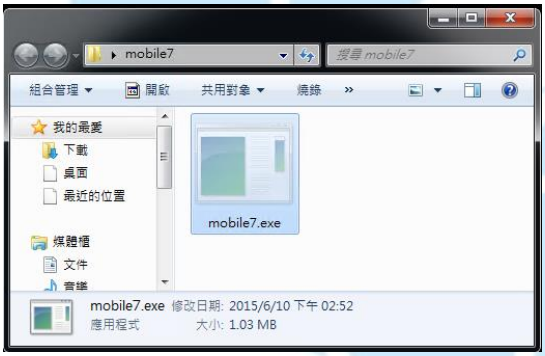
3. 使用 procexp 工具來檢視所有背景程式的執行狀態，發現該程式 mobile7.exe 確實正在執行中，並且沒有顯示明確的 Description 和 Company Name，研判應為惡意程式。



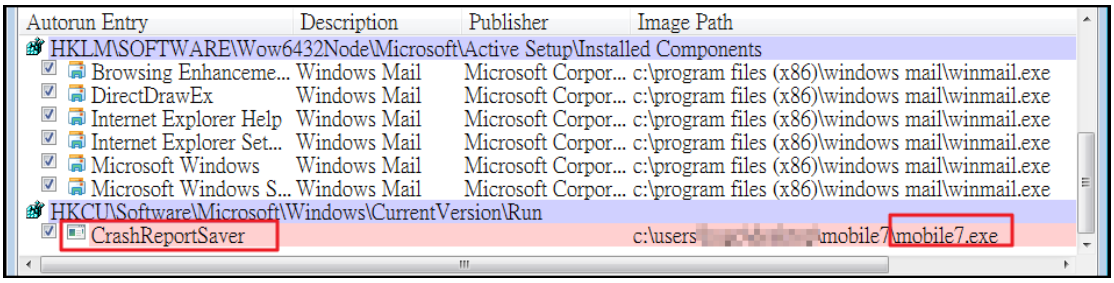
4. 檢視 mobile7.exe 程式的網路狀態，可以看到該程式正在發送封包至外部 IP 主機，並且開啟 port 80 和 53 為 Listening 狀態。



5. 實地檢查該檔案的位置資料夾，發現到該檔案為隱藏的執行檔，因此若無開啟顯示隱藏檔選項則不易發現其存在。



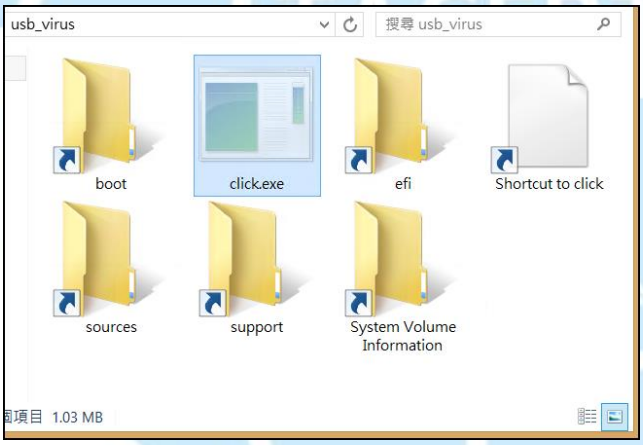
6. 通常惡意程式會伴隨該機自動啟動，因此透過 autoruns 工具檢查是否異常，的確出現一個名為 CrashReportSaver 的開機啟動註冊碼，路徑名稱就為 mobile7.exe 所有。



7. 透過隨身碟插入測試是否會感染外接 USB 裝置，發現惡意程式的確會植入到隨身碟根目錄中，產生 1.03MB 的隱藏檔 click.exe。

8. 值得注意的是隨身碟內所有的資料夾都會被惡意程式改成隱藏資料夾，而會另外產生相同資料夾名稱的捷徑，這些捷徑通通指向 click.exe 執行。

   1. 捷徑內容為「C:\WINDOWS\system32\cmd.exe F/c "start %cd%\click.exe && %windir%\explorer %cd%\sources"」。
   2. 一旦不注意開啟偽裝資料夾，就會執行到惡意程式。



9. 透過 Virustotal 線上掃描 mobile7.exe 和 click.exe 發現，其實就是完全相同的惡意程式，且相當高的偵測率為 29/57 的木馬程式。

SHA256: 311a000ec4401817b82b855774c29d0104b5551faf46bd8c7265cc25620d28b3

檔案名稱: a2f887ceb792ed128efe050a4d493b20389ce185

偵測率: 29 / 57

分析日期: 2015-06-11 07:46:30 UTC (1 月, 1 週 前)

0 0

分析 | 檔案詳細資料 | 其他資訊 | 評論 0 | 投票 | 行為資訊

防毒	結果	更新
ALYac	Trojan.Injector.BLS	20150611
AVG	Inject2.CHTQ	20150611
AVware	Trojan.Win32.GenericIBT	20150611
Ad-Aware	Trojan.Injector.BLS	20150611
Arcabit	Trojan.Injector.BLS	20150611
Avira	TR/Crypt.Xpack.23250	20150611
Baidu-International	Trojan.Win32.Injector.CCNF	20150610
BitDefender	Trojan.Injector.BLS	20150611

10. 檢測網路封包觀察其網路行為，觀察到此主機有開啟 port 53 去接收外部主機的封包，確實為 DNS 伺服器功能，專門用來解析其他惡意網域名稱。從紀錄來看至少有 600 個惡意網址的解析紀錄，依查詢排名前幾名為「bayermun.biz、gorodkoff.com、demyator.biz、mydear.name、www.mydear.name 」等。

11. 這些惡意網址透過 Virustotal 掃描，偵測出的比率其實很低或者是零。

URL: http://mydear.name/

偵測率: 3 / 63

分析日期: 2015-06-09 18:13:31 UTC (1 月, 1 週 前)

URL: http://demyator.biz/

偵測率: 1 / 63

分析日期: 2015-05-05 13:22:07 UTC (2 月, 2 週 前)

URL: http://bayermun.biz/

偵測率: 1 / 63

分析日期: 2015-05-05 14:01:02 UTC (2 月, 2 週 前)

URL: http://gorodkoff.com/

偵測率: 0 / 63

分析日期: 2015-07-21 15:24:43 UTC (11 小時, 12 分鐘 前)

bayermun.biz (49,560) - gorodkoff.com (24,807) - demyator.biz (2,530) - mydear.name (2,066) - www.mydear.name (1,022) - ns1.gorodkoff.com (851) - ns3.gorodkoff.com (843) - ns6.gorodkoff.com (841) - ns2.gorodkoff.com (841) - ns4.gorodkoff.com (832) - ns5.gorodkoff.com (768) - ns6.mydear.name (314) - ns5.mydear.name (289) - ns3.mydear.name (287) - ns2.mydear.name (287) - ns1.mydear.name (276) - ns4.mydear.name (256) - goloduha.info (256) - greystoneexpress.com (123) - ns4.bayermun.biz (106) - ns3.demyator.biz (99) - ns2.demyator.biz (99) - ns5.demyator.biz (95) - ns1.greystoneexpress.com (92) - ns5.greystoneexpress.com (91) - ns2.greystoneexpress.com (88) - ns3.greystoneexpress.com (86) - ns6.greystoneexpress.com (84) - ns4.greystoneexpress.com (84) - ns4.demyator.biz (84) - ns1.bayermun.biz (83) - ns2.bayermun.biz (81) - ns1.goloduha.info (81) - ns6.bayermun.biz (80) - ns6.goloduha.info (79) - ns6.demyator.biz (72) - ns1.demyator.biz (71) - ns5.bayermun.biz (66) - ns3.bayermun.biz (62) - ns2.goloduha.info (62) - ns5.goloduha.info (46) - ns3.goloduha.info (36) - ns4.goloduha.info (25) - www.bayermun.biz (14) -

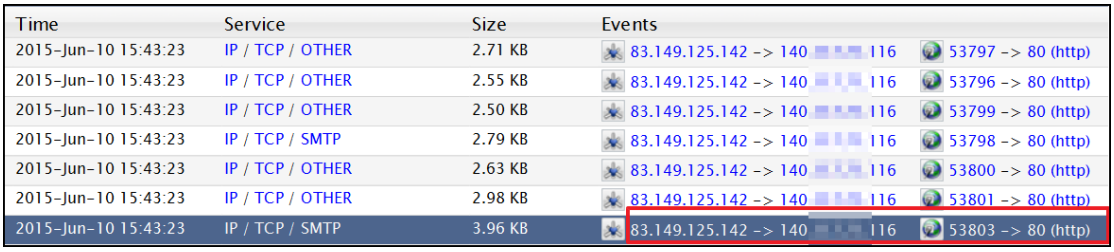
12. 以上這些網址透過 DNS 解析出來的 IP 每個時間點都不同，所以產生一個網址對應至多個 IP 現象，表示駭客透過 Fast Flux 技術快速切換中繼站

網域名稱的 IP 位址，以提高中繼站存活的機會。

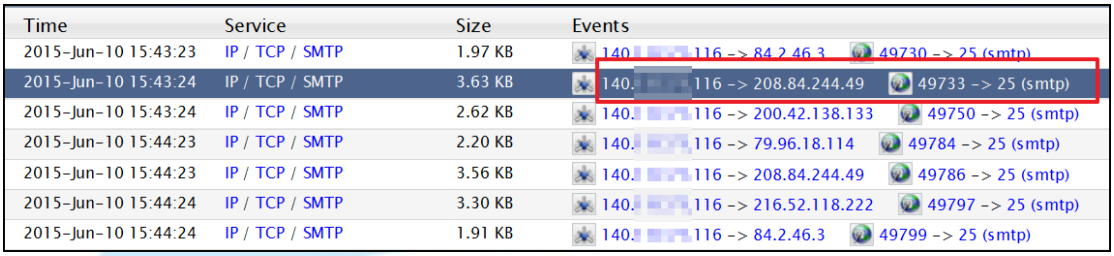
13. 從另一角度觀察網域名稱與 IP 關係，由於也有許多惡意網域名稱對應到單一感染主機 140.X.X.116，表示此中繼站群是透過 Double-Flux 技術雙向切換，更不易被相關單位追查發現，屬於大型的殭屍網路活動。

14. 觀察該中繼站網路行為，底層的殭屍電腦會向該中繼站的 port 80 發送封包，而中繼站則將收到封包中繼至遠端的 SMTP 伺服器，封包內容為登入 SMTP 伺服器郵件帳號後，透過該帳號向外發送惡意釣魚郵件，故中繼站成為殭屍電腦的 proxy 伺服器去登入遠端郵件伺服器。藉由此方式單從郵件伺服器紀錄來看就無法追查到底層殭屍電腦位址。

    1. 從下圖舉例可知，底層殭屍電腦 83.149.125.142 發送封包給中繼站的 port 80，中繼站則再向上層 SMTP 伺服器 84.2.46.3 進行帳號登入並發送惡意電子郵件。

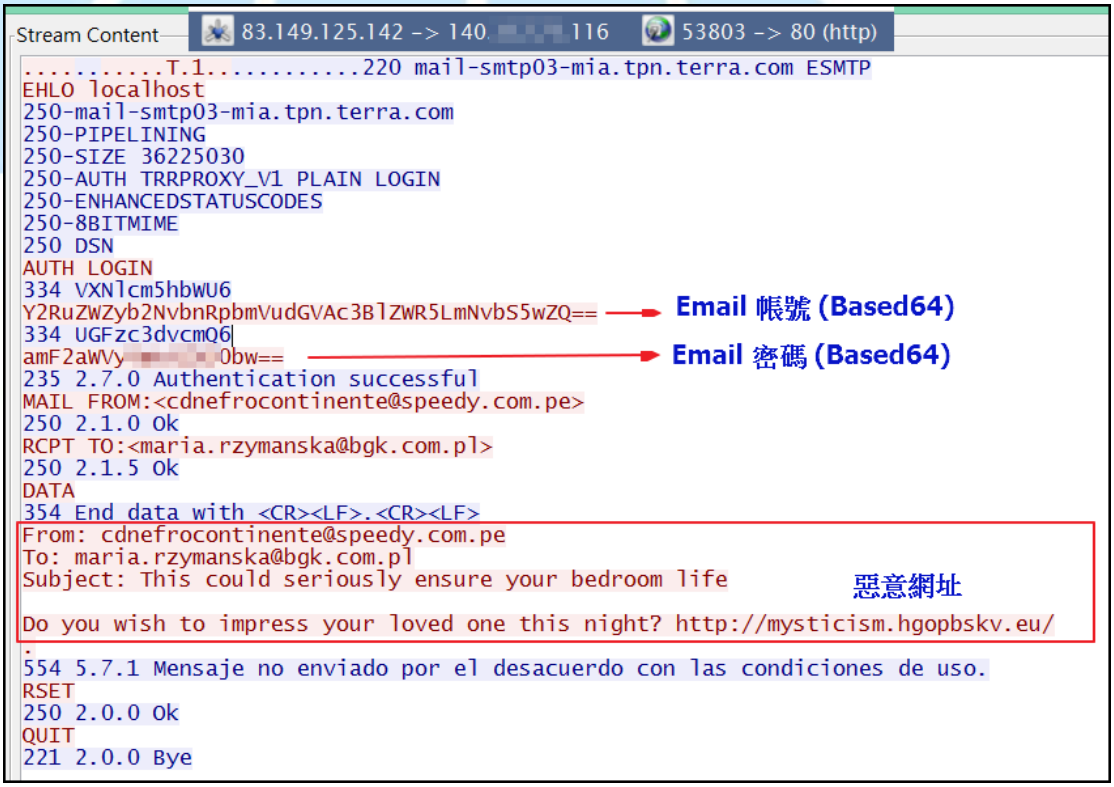


Time	Service	Size	Events
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.71 KB	83.149.125.142 -> 140 116 53797 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.55 KB	83.149.125.142 -> 140 116 53796 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.50 KB	83.149.125.142 -> 140 116 53799 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / SMTP	2.79 KB	83.149.125.142 -> 140 116 53798 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.63 KB	83.149.125.142 -> 140 116 53800 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / OTHER	2.98 KB	83.149.125.142 -> 140 116 53801 -> 80 (http)
2015-Jun-10 15:43:23	IP / TCP / SMTP	3.96 KB	83.149.125.142 -> 140 116 53803 -> 80 (http)

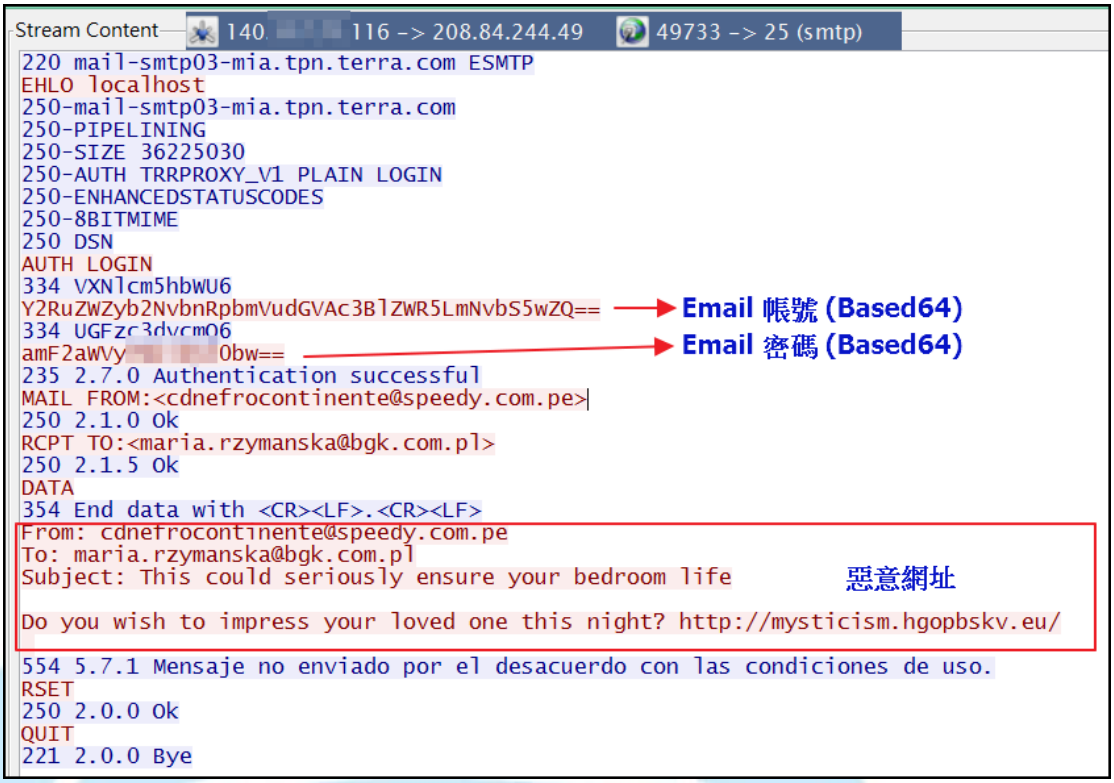


Time	Service	Size	Events
2015-Jun-10 15:43:23	IP / TCP / SMTP	1.97 KB	140 116 -> 84.2.46.3 49730 -> 25 (smtp)
2015-Jun-10 15:43:24	IP / TCP / SMTP	3.63 KB	140. 116 -> 208.84.244.49 49733 -> 25 (smtp)
2015-Jun-10 15:43:24	IP / TCP / SMTP	2.62 KB	140. 116 -> 200.42.138.133 49750 -> 25 (smtp)
2015-Jun-10 15:44:23	IP / TCP / SMTP	2.20 KB	140. 116 -> 79.96.18.114 49784 -> 25 (smtp)
2015-Jun-10 15:44:23	IP / TCP / SMTP	3.56 KB	140. 116 -> 208.84.244.49 49786 -> 25 (smtp)
2015-Jun-10 15:44:24	IP / TCP / SMTP	3.30 KB	140. 116 -> 216.52.118.222 49797 -> 25 (smtp)
2015-Jun-10 15:44:24	IP / TCP / SMTP	1.91 KB	140. 116 -> 84.2.46.3 49799 -> 25 (smtp)

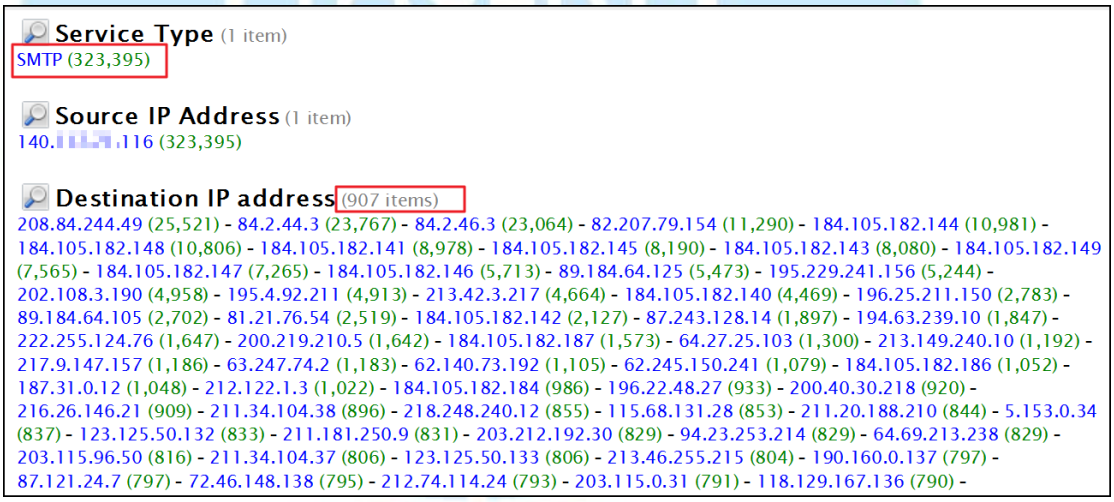
2. 檢視底層殭屍電腦 83.149.125.142 發送至中繼站的封包內容，包含了加密過的帳號密碼，以及誘使他人開啟的惡意網址連結。



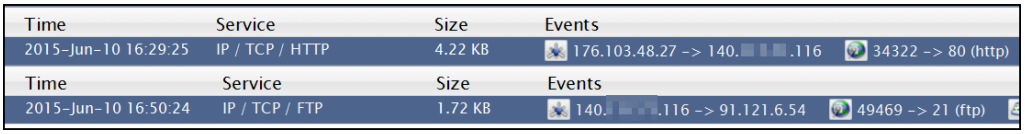
3. 檢視中繼站發送至 SMTP 伺服器 208.84.244.49 的封包內容，其內容與殭屍電腦發送至中繼站內容一樣，都包含帳號密碼以及惡意網址。

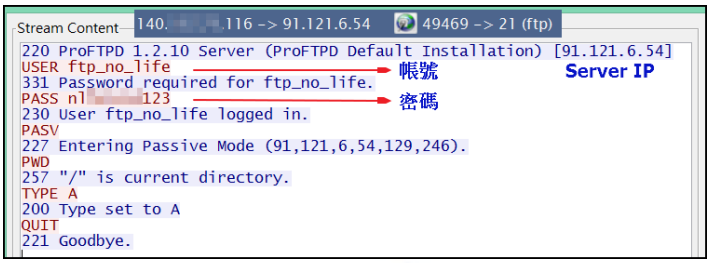


4. 從封包記錄上來看，約有 900 個相異的 SMTP 伺服器被中繼站嘗試登入帳號密碼發送惡意釣魚郵件。

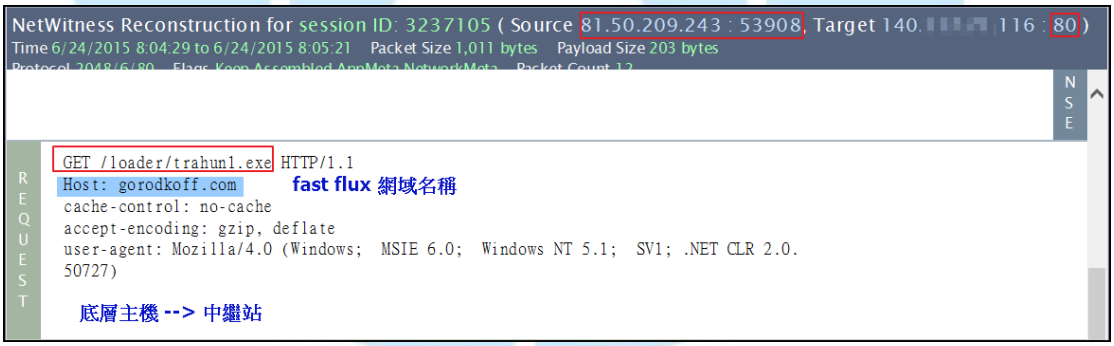


15. 除此之外中繼站也被殭屍電腦用來登入遠端的 FTP 伺服器，例如殭屍電腦 176.103.48.27 透過中繼站的 port 80 發送登入封包至 FTP 伺服器 91.121.6.54:21，封包內容中包含了明文的 FTP 帳號和密碼，以及 FTP server 的 IP 資訊，並透過此帳號密碼測試確實能登入該 FTP 伺服器。



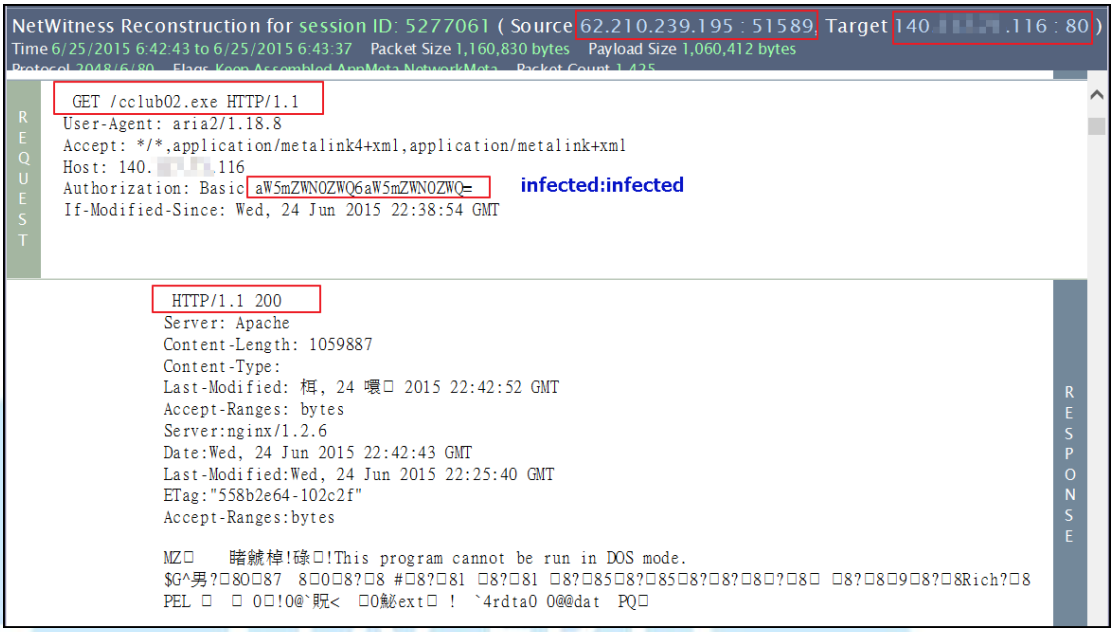


16. 除此之外中繼站也會用來傳送 EXE 執行檔，大多殭屍主機會透過 fast-flux 網域名稱 gorodkoff.com 連到中繼站，再透過中繼站向上層主機下載惡意程式執行檔，這些上層主機有 176.103.55.73、176.103.54.73、89.144.2.115、89.144.2.119 共四個。



1. 然而底層主機 62.210.239.195 直接連到中繼站 IP 而非網域名稱，向上層主機 176.103.54.73 登入帳號密碼「infected:infected」來下載 惡意程式 cclub02.exe，研判 62.210.239.195 可能是上層駭客所用的 IP。
2. 經外部檢測該惡意程式的主機 176.103.54.73 位於烏克蘭，使用 linux 系統並有開啟 port 80 作為中繼站使用。

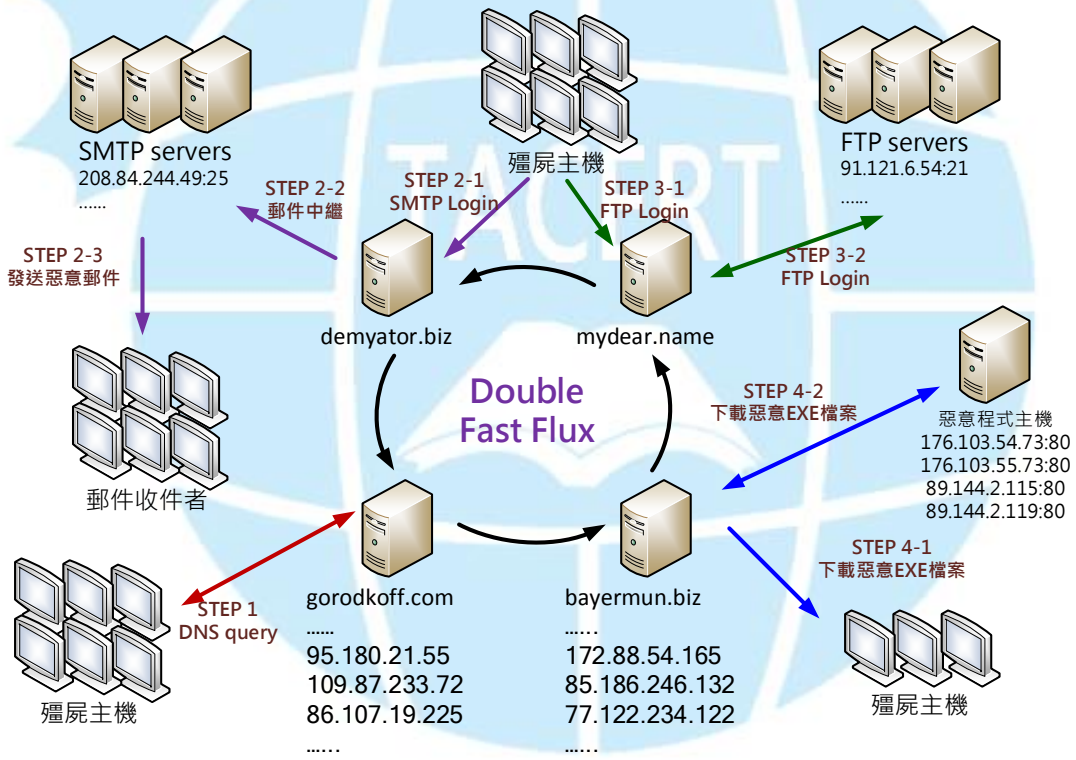
3. 從中繼站到上層主機 176.103.54.73 的封包中，會帶有底層主機的 IP 資訊（X-My-Real-IP: 62.210.239.195），用來讓中繼站能夠正確將檔案 cclub02.exe 回覆給來源端。該檔案大小約為 1.06MB 的惡意程式，透過 Virustotal 的檢測比例為 13/56。



4. 封包紀錄中側錄到的惡意程式有以下 10 個檔案，雖然檔案名稱不同但應該皆為相同作用的惡意程式。

名稱	修改日期	類型	大小
arisx06.exe	2015/7/23 上午 0...	應用程式	1,052 KB
b0be001.exe	2015/7/23 上午 0...	應用程式	1,060 KB
cclub02.exe	2015/7/23 上午 0...	應用程式	1,059 KB
chipdd1.exe	2015/7/23 上午 0...	應用程式	1,060 KB
invi001.exe	2015/7/23 上午 0...	應用程式	1,060 KB
mobile7.exe	2015/7/23 上午 0...	應用程式	1,060 KB
rain003.exe	2015/7/23 上午 0...	應用程式	1,060 KB
suba002.exe	2015/7/23 上午 0...	應用程式	1,059 KB
trahun1.exe	2015/7/23 上午 0...	應用程式	1,059 KB
x640001.exe	2015/7/23 上午 0...	應用程式	1,060 KB

III. 網路架構圖



1. 殭屍主機會向中繼站群發送 DNS query 封包，因此中繼站為 DNS Proxy Servers。
2. 殭屍主機透過中繼站群登入遠端 SMTP 郵件伺服器，並且發送惡意郵件給其他使用者。
3. 殭屍主機也會透過中繼站群登入遠端 FTP 伺服器，上傳或竊取 FTP 伺服器

的資料。

4. 殭屍主機也會透過中繼站群向惡意檔案伺服器下載惡意 EXE 檔案，讓惡意程式在擴散出去。
5. 殭屍主機與中繼站間的連接方式大多是透過惡意網域名稱連接，因此每次建立連線都可能是不同的中繼站。

IV.建議與總結

1. 此事件是一個跨國際的大型中繼站殭屍網路，駭客使用 double Fast Flux 技術變換中繼站的網域名稱及 IP 位址，且至少有 600 個以上惡意網域名稱再做切換。
2. 主機感染後惡意程式 mobile7.exe 會開啟 TCP port 80 進行中繼站資料傳送，開啟 UDP port 53 作為 DNS proxy server，並寫入開機註冊碼中自動執行，主機的相關帳號密碼可能會外洩。
3. 透過 TCP port 80 進行的網路行為有 SMTP relay、 FTP relay 以及 HTTP 的惡意 EXE 程式下載。
4. 殭屍主機能夠登入外部的 SMTP 或 FTP 伺服器，可能是因為感染病毒後帳號密碼被竊取，被駭客利用來發送郵件或竊取 FTP 檔案。
5. 此病毒感染方式通常會透過惡意電子郵件或者隨身碟交叉感染，隨身碟一旦插入感染主機，內部自動會產生隱藏病毒檔，並置換資料夾為惡意捷徑，易使人上當執行。
6. 電子郵件和隨身碟開啟前務必檢查有無可疑之處，避免誤觸惡意程式。
7. 感染此病毒後網路頻寬會被大量使用，只要透過 tcpview 和 procexp 工具就能找出惡意程式位置並且將之移除，並立刻更換常用的帳號密碼。