個案分析-

惡意程式m.exe
分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/07

前言

通報時間:	2013-06-04 11:04:20
事件單編號:	AISAC-241XX
通報機關名稱:	XXXXX 國民小學
影響等級:	1 級
事件分類:	INT
事件說明:	此 IP(210.xx.xx.90)電腦主機向外發送廣告信件。

事件說明

一、透過收容惡意程式資料庫網站 Malc0de Database 尋找 IP 210.xx.xx.90 所感染的惡意程式為：
2013-05-21，http://audpuu5b.zeqromoj.ru/m.exe，檔圖為黃色螞蟻

。

二、將此惡意程式下載於 VMware 系統執行，並側錄感染的測試 VM 主機網路流量並分析其行為，側錄時間為 2013/05/31-2013/06/06，側錄檔 pcap 共約 1.39GB。

三、測試 VM 主機環境：
1. 作業系統：Win7 Enterprise (x64)
2. IP 位址：140.xx.xx.60
3. 未安裝系統修補套件

四、惡意程式 m.exe 行為：
1. 執行 m.exe 後，該程式會自行轉變為隱藏檔執行。
2. 在登錄機碼中寫入開機自動執行，名稱為 SonyAgent 試圖讓人誤以為是 SONY 的相關程式，且無供應商名稱。

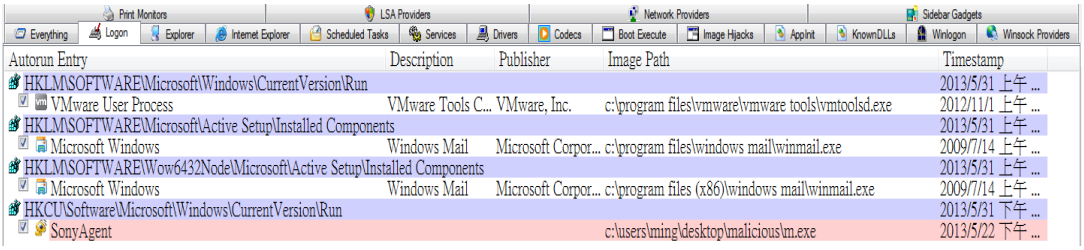


圖 1、使用 autoruns 於登錄機碼中發現 m.exe 會於開機時自動執行

3. 惡意程式 m.exe 會去連結啟用許多系統的 dll 檔，以開啟網路相關服務。位於 C:\Windows\SysWOW64\和 C:\Windows\System32\ 共有 36 個 dll 系統檔。

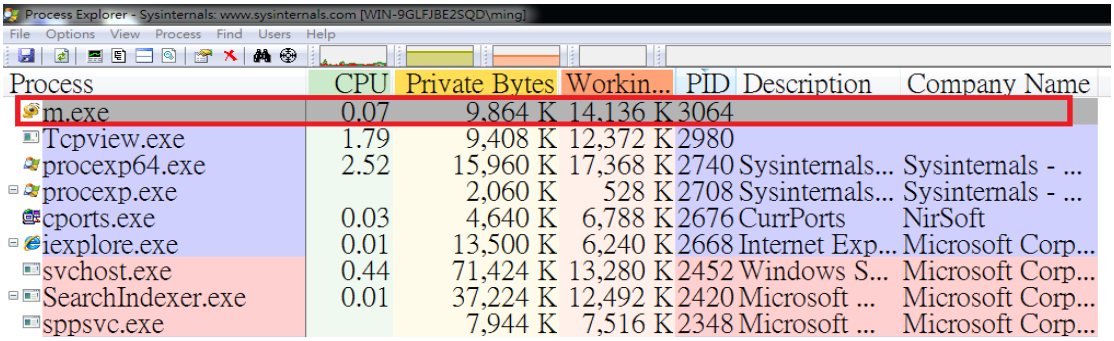


圖 2、使用 procexp 顯示惡意程式 m.exe 執行中

4. 測試 VM 主機被開啟的 Port 及 Serivce：

(1). TCP Port 80：作為郵件中繼站(Mail Relay)、HTTP 中繼站(HTTP Relay)

(2). UDP Port 53：作為 DNS proxy server

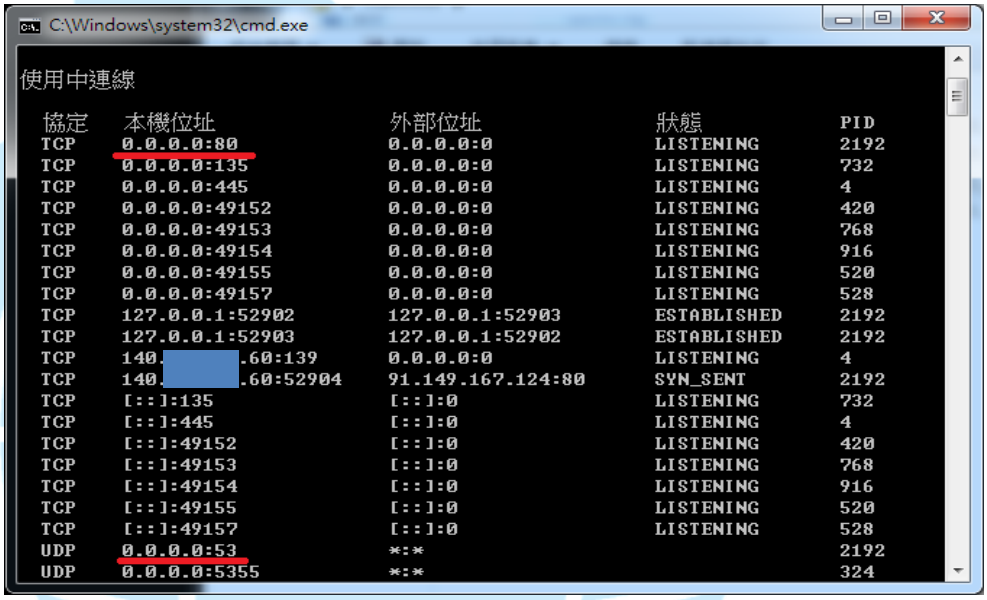


圖 3、指令 netstat 顯示出本機 TCP port 80 和 UDP port 53 被啟用

(3). 惡意程式 m.exe 執行後，觀察 port 和 IP 的連線狀況如下，一開始的程序會顯示 m.exe，但部分會轉為 Unknown 的 PID=0 程序執行，較不易被發現。異常程序都會連至外部 IP 的 port 80。

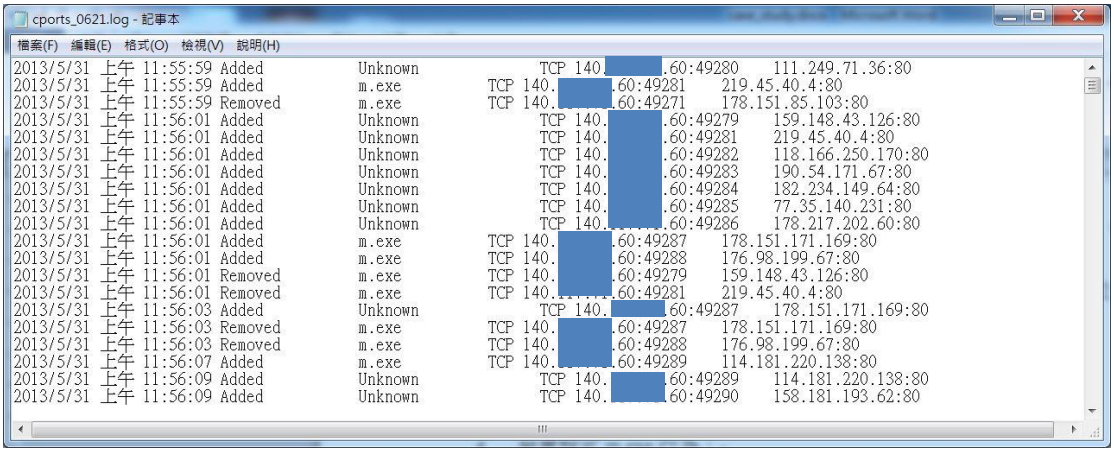


圖 4、currport 的 port 紀錄

5. 測試 VM 主機網路架構圖：

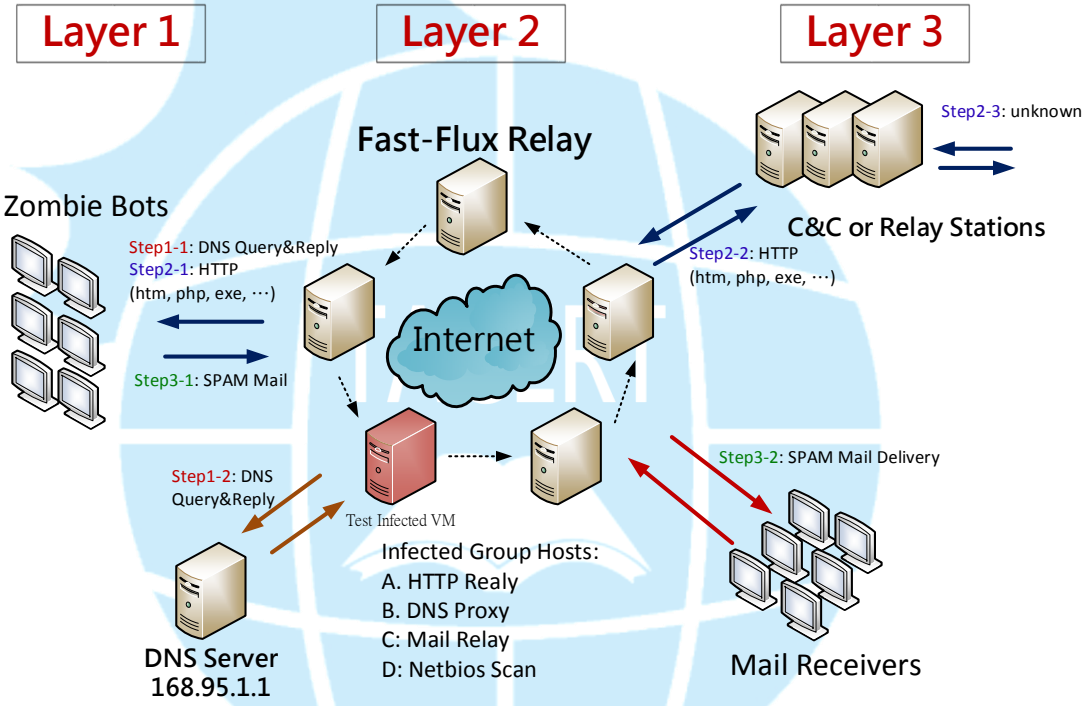


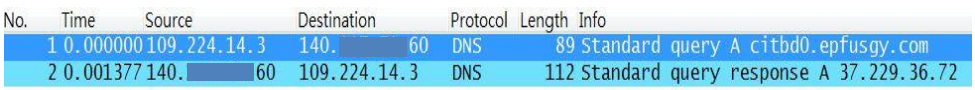
圖 5、紅色主機為此測試 VM 主機

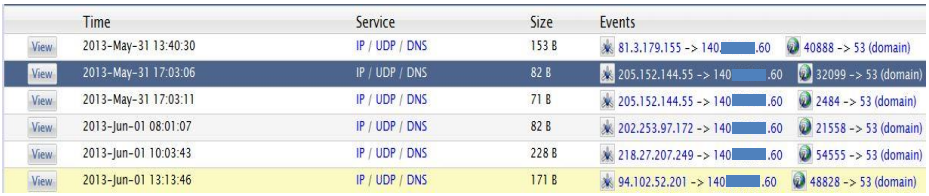
6. 作為 **DNS 代理伺服器** (DNS Poxy Server)：

(1). 紀錄中發現很多 zbots 透過此測試 VM 主機去做 DNS service，主要替其他中繼站做 fast-flux 網域名稱解析。

(2). 測試 VM 主機收到 zbots 的網域名稱 query 後，會轉向測試 VM 主機預設的 DNS 伺服器(此例為 140.117.11.1 和 168.95.1.1)進行網域名稱詢問，解析後再回覆給 zbots，因此測試 VM 主機也作為的 DNS proxy server。

(3). 至少有 2145 個 zbots (112 個國家)向此測試 VM 主機做網域名稱詢問，解析出的網域名稱有 198 個。





	Time	Service	Size	Events
View	2013-May-31 13:40:30	IP / UDP / DNS	153 B	81.3.179.155 -> 140.[redacted].60 40888 -> 53 (domain)
View	2013-May-31 17:03:06	IP / UDP / DNS	82 B	205.152.144.55 -> 140.[redacted].60 32099 -> 53 (domain)
View	2013-May-31 17:03:11	IP / UDP / DNS	71 B	205.152.144.55 -> 140.[redacted].60 2484 -> 53 (domain)
View	2013-Jun-01 08:01:07	IP / UDP / DNS	82 B	202.253.97.172 -> 140.[redacted].60 21558 -> 53 (domain)
View	2013-Jun-01 10:03:43	IP / UDP / DNS	228 B	218.27.207.249 -> 140.[redacted].60 54555 -> 53 (domain)
View	2013-Jun-01 13:13:46	IP / UDP / DNS	171 B	94.102.52.201 -> 140.[redacted].60 48828 -> 53 (domain)

圖 6、 Zbots 向此測試 VM 主機 140.xx.xx.60 詢問網域名稱的 IP

7. 作為 **HTTP 中繼站**（HTTP Relay）：

(1). 測試 VM 主機開啟 port 80 來接收 zbot 傳送的檔案，並中繼給下一層中繼站的 port 80，紀錄中發現下一層至少有 734 個中繼站，研判至少為三階層的網路架構，本主機為於第二層的中繼站。

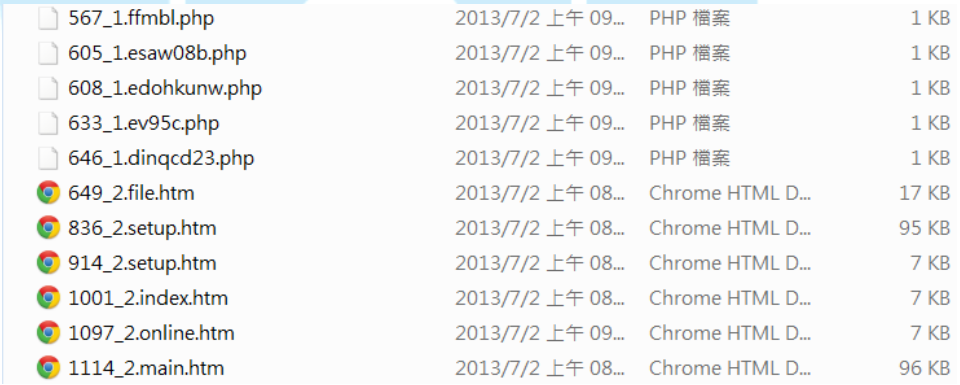
(2). 測試 VM 主機會使用 Fast-Flux 技術變換許多網域名稱讓其他 zbot 主機連入，紀錄中約有 200 個網域名稱會對應至此測試 VM 主機 140.xx.xx.60。

(3). 主要連結下一層的中繼站有 6 個，依傳輸排名為 193.105.134.89、78.83.177.242、78.83.177.250、193.105.134.189、89.45.14.47、89.45.14.49。

(4). 這些 IP 皆為國外的中繼站，並已被 McAfee SiteAdvisor 及 Virustotal 確定列為惡意網站。

(5). 此惡意程式會向這些中繼站的 Port 80 做 HTTP 中繼 htm、php、exe 檔，並透過分析發現 htm 和 php 不是合法的檔案標頭，其內容都是編碼過的資料且無法解碼。

(6). 其中 pcap 截錄出的 htm 和 php 檔共 10,141 個，解析其內容皆為加密過的亂碼，故無法得知 zbot 所傳送檔案資訊。



567_1.ffmbl.php	2013/7/2 上午 09...	PHP 檔案	1 KB
605_1.esaw08b.php	2013/7/2 上午 09...	PHP 檔案	1 KB
608_1.edohkunw.php	2013/7/2 上午 09...	PHP 檔案	1 KB
633_1.ev95c.php	2013/7/2 上午 09...	PHP 檔案	1 KB
646_1.dinqcd23.php	2013/7/2 上午 09...	PHP 檔案	1 KB
649_2.file.htm	2013/7/2 上午 08...	Chrome HTML D...	17 KB
836_2.setup.htm	2013/7/2 上午 08...	Chrome HTML D...	95 KB
914_2.setup.htm	2013/7/2 上午 08...	Chrome HTML D...	7 KB
1001_2.index.htm	2013/7/2 上午 08...	Chrome HTML D...	7 KB
1097_2.online.htm	2013/7/2 上午 09...	Chrome HTML D...	7 KB
1114_2.main.htm	2013/7/2 上午 08...	Chrome HTML D...	96 KB

圖 7、測試 VM 主機 pcap 截錄出的部分檔案

(7). 其中 pcap 截錄出 exe 檔共 1,255 個，都是惡意程式，大多命名為 m.exe、calc.exe 或其他隨機命名的 exe 檔案。而 m.exe 即為此案

的惡意程式，且檔案 Logo 不是唯一樣式。

75579_1.cnp3lxoenik.exe	2013/7/2 上午 09:40	應用程式	1 KB
75692_1.fopkq.exe	2013/7/2 上午 08:59	應用程式	1 KB
76038_1.houz53vu.exe	2013/7/2 上午 09:40	應用程式	1 KB
76526_1.ajjs2g4h.exe	2013/7/2 上午 08:59	應用程式	1 KB
77445_1.biisgyfjjc.exe	2013/7/2 上午 09:40	應用程式	1 KB
77452_1.biisgyfjjc.exe	2013/7/2 上午 09:40	應用程式	1 KB
78060_1.hz8fxz06eq.exe	2013/7/2 上午 09:40	應用程式	1 KB
78263_1.cccm8eg7h.exe	2013/7/2 上午 09:40	應用程式	1 KB
78908_1.rasta01.exe	2013/7/2 上午 08:59	應用程式	807 KB

圖 8、測試 VM 主機 pcap 截錄出的惡意執行檔

8. 作為**垃圾郵件中繼站**(Mail Relay)，利用 TCP port 80 負責接收上一層 zbot 主機發送的垃圾郵件或惡意郵件，並轉送給許多受害者，誘使收件者開啟惡意郵件或連結。

(1). 此中繼站接收到的 Email 位址約有 435 個，來源端有 3 個國家、9 個 IP 位址，依排名為 Germany、Netherlands、France。

(2). 此中繼站發送出的 Email 位址約有 435 個，目的地有 38 個國家、121 個 IP 位址。

(3). 來源端與目的地的 Email 位址個數一樣是因為只做 Mail Relay 的緣故，而非主機自己產生郵件。

(4). 以下為部分重建的取樣郵件，內文都有惡意網站連結。

NetWitness Reconstruction for session ID: 426477 (Source 140.[redacted].60 : 62708, Target 200.45.191.16 : 25)
Time 6/03/2013 10:02:25 to 6/03/2013 10:02:46 Packet Size 3,344 bytes Payload Size 752 bytes

From: vivianababor@arnet.com.ar
To: gilroy@rakli.fi
Subject: Discount price of male supplements
more

http://balolaptopcaocap.webdoanhnghiep.org/object.html Are you dreaming about extra fire in your loving life?

NetWitness Reconstruction for session ID: 501941 (Source 140.[redacted].60 : 56984, Target 200.45.191.16 : 25)
Time 6/03/2013 22:28:07 to 6/03/2013 22:28:21 Packet Size 3,349 bytes Payload Size 757 bytes

From: alfredoolivieri@arnet.com.ar
To: sheehans_2000@yahoo.com
Subject: Very good way to develop your loving life
more

Burn your impulse to the limit http://nude-celeb-pics.pix43.com/Louis.html

NetWitness Reconstruction for session ID: 560062 (Source 140.[redacted].60 : 65131, Target 208.84.244.49 : 25)
Time 6/04/2013 8:03:39 to 6/04/2013 8:03:47 Packet Size 2,901 bytes Payload Size 723 bytes

From: ventas@proyecto-siete.com
To: roberthpatch@netscape.net
Subject: Improve your possibilities in bed
more

http://www.spajderr.tkdami.net/toe.html Incredible ensuring effect on male health

圖 9、測試 VM 主機 pcap 截錄出的惡意郵件

9. NETBIOS:測試 VM 主機對許多 IP 做 UDP Port 137 的 Name query NBSTAT，目標總數約有 11,311 次且國別數有 132 個，截錄的檔案為無法辨識的 raw 檔。

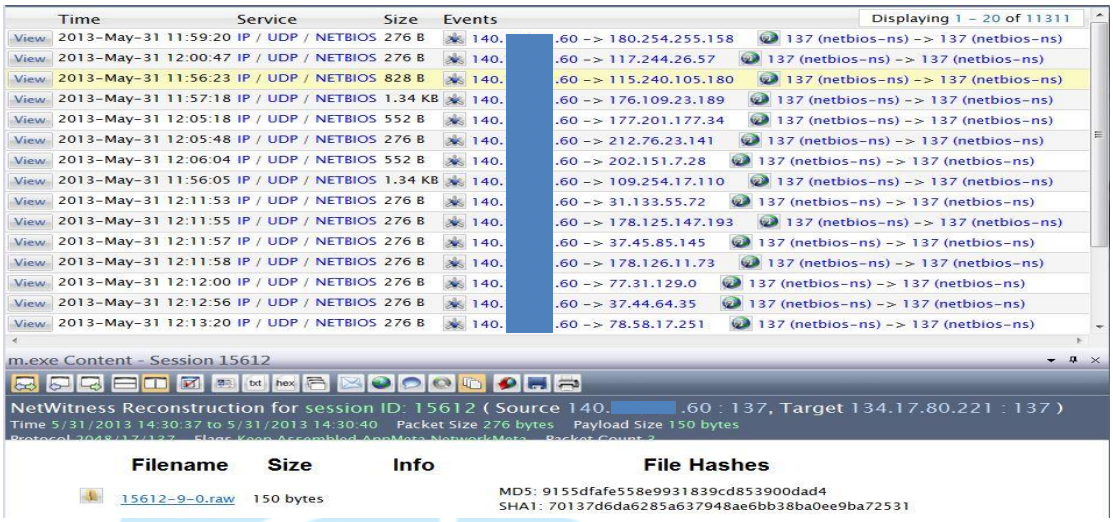


圖１０、測試 VM 主機 pcap 截錄看到 netbios 疑似 scan 非特定網段 IP

五、Google Earth 整合：

1. 觀察測試 VM 主機所連入的 Zbots 主要分布於全世界各地，以歐洲和日本較為密集。

(1). 中國的點很少，推測可能是中國駭客利用他國 IP 所為。

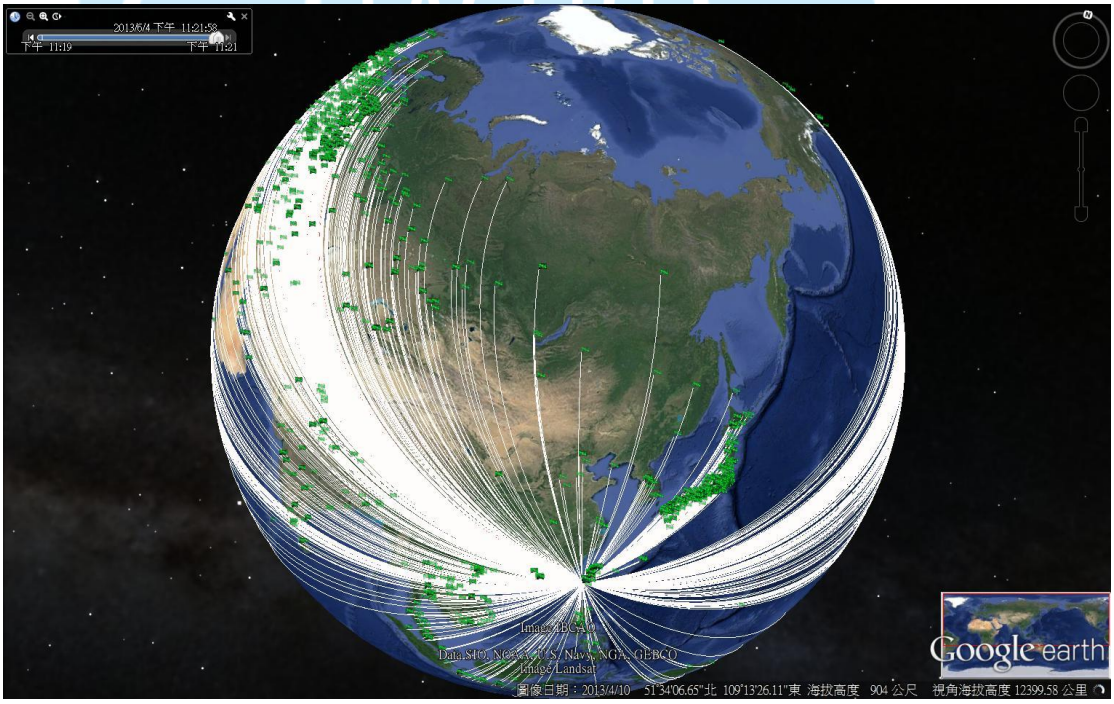


圖１１、測試 VM 主機所連入的 Zbots 分布，綠點為 zbots。

2. 觀察測試 VM 主機所連出的中繼站主要分布在歐洲、北美洲和日本，特別是瑞典和保加利亞為大宗。紅色線表示此 IP 的 Session 數量極多。

(1). 中國的點很少，推測可能是中國駭客利用他國 IP 所為。

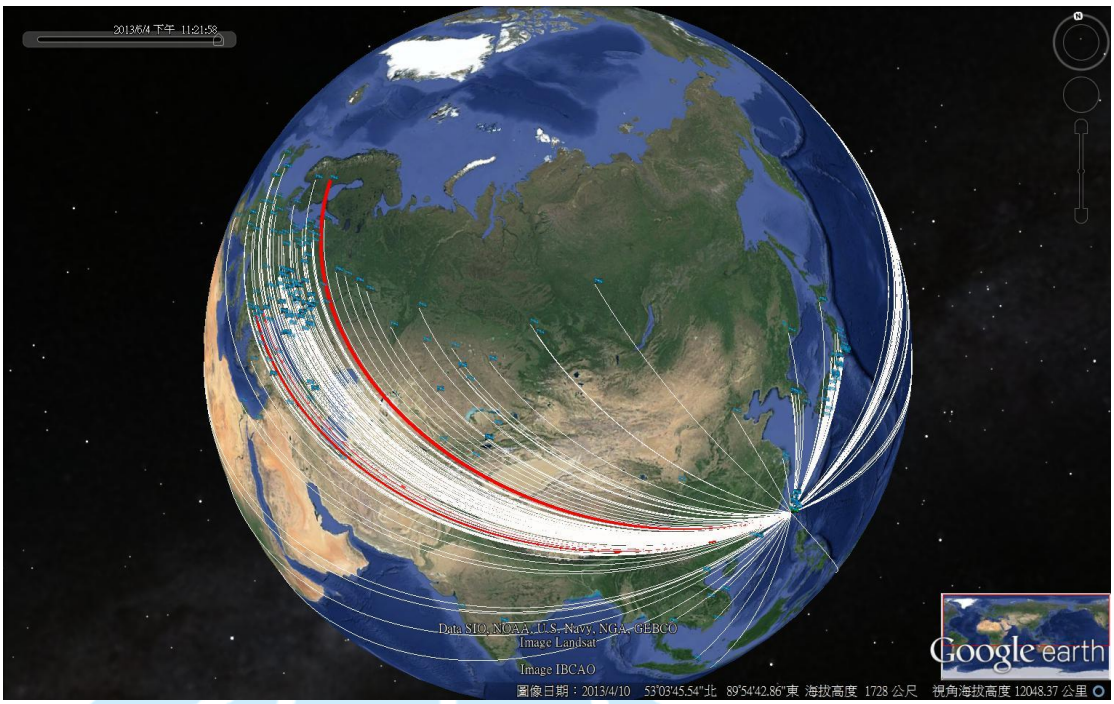


圖１２、測試 VM 主機所連出的中繼站分布。

建議措施

1. 此惡意程式容易夾帶於郵件連結或各式附檔(doc, pdf, xls, …)中，應避免直接開啟。
2. 檢查主機帳密是否安全，遠端桌面連線非必要可關閉。
3. 感染惡意程式主機會被當作中繼站跳板，同時也會將自己的個人資料外洩。
4. 來路不明的檔案不要輕易開啟，可以先透過 Virustotal 進行線上掃描。
5. 時常用網路流量監看工具(netstat, tcpview, …)是否有異常流量及 Port 被啟用，以便找出可疑的執行程式。
6. 可用程序監看工具(procexp)將該異常程式移除，可用登錄機碼工具(autoruns)檢查開機自動執行的登錄碼有無異常。
7. 線上檢測惡意網站：
   (1). https://www.virustotal.com/en/
   (2). http://sitecheck.sucuri.net
   (3). http://www.siteadvisor.com