個案分析-

Multi-Functional Malware 分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/7

目錄

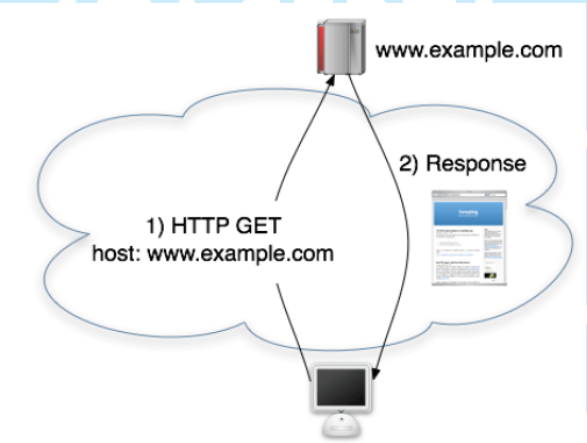
前言

Fast Flux 本來是一種 DNS 技術，一些流量大的網站，例如 Google 或 Yahoo，會將網站迅速對應至不同的實體機器，以達到網路流量負載平衡(Network Load Balance)的目的，以減少單個網頁伺服器故障而無法提供服務造成損失。

後來，該技術被駭客利用，用來隱藏釣魚網站或惡意程式的載點，Fast Flux 被駭客拿來利用時，也一樣不斷地變化網域對應的實體位址，比較不一樣的是，這些被對應的機器通常都是受害端，駭客則利用這些機器來保護其惡意網站，試圖讓惡意網站躲避偵測，延長其存活壽命。

一般沒有經過 Fast Flux 掩護的網站，網頁存取過程如圖一所示。

- 步驟一：客戶端在瀏覽器上輸入網站（www.example.com）URL，向網站 GET 一個頁面
- 步驟二：當網站收到這樣的請求後，網站會根據 URL Response 一個對應的頁面



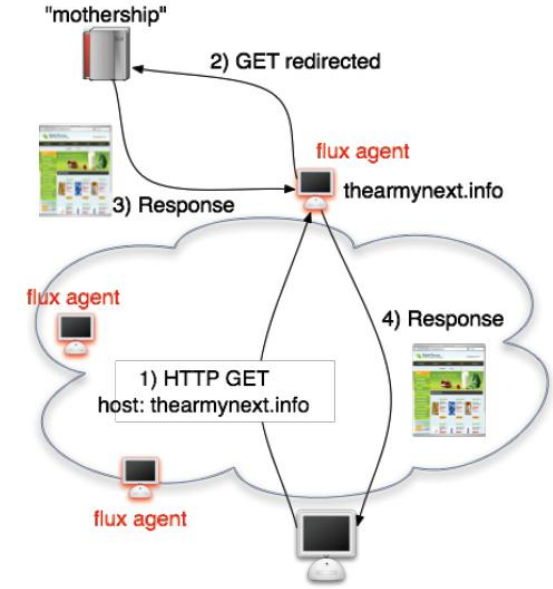
圖一 正常的網頁存取過程

相對於一般的網頁存取方式，圖二則是透過 Fast Flux 技術的網頁存取，增加了 Flux Agent（快速變動網域代理人）。

- 步驟一：客戶端向惡意網站送出請求，要 GET thearmynext.info 頁面，但在這個部份因為加入 Flux Agent 的關係，使得客戶端的請求並不會直接送達惡意網站，而是與多個 Flux Agent 之一連線，傳送 GET 請求給 Flux Agent。
- 步驟二：Flux Agent 沒有實質的網站內容，純粹只是一個中繼站，但是具有流

量導向的功能，因此可以將請求導向惡意網站，由惡意網站作實質的處理。

- 步驟三：收到 Flux Agent 送來的請求後，惡意網站 Response 對應的頁面。最後，快速變動網域代理人將 Response 的頁面透過 80 port 導到原本送出請求的客戶端，完成透過 Fast Flux 的互動

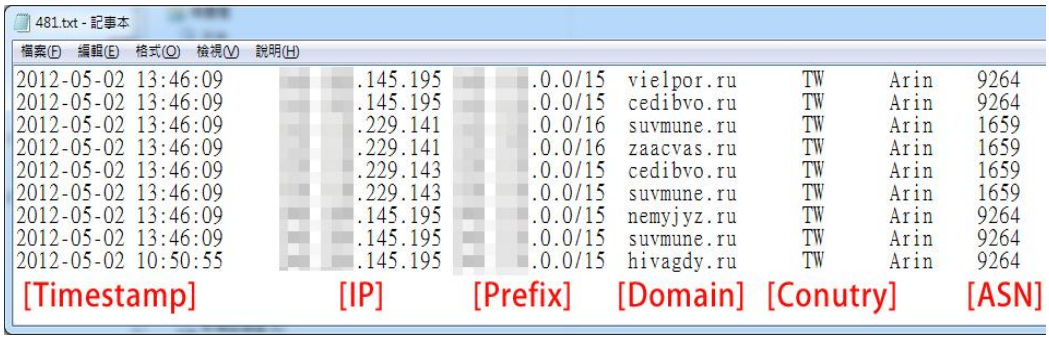


圖二 利用 Flux Agent 存取網路資源

透過上述方法，客戶端就無法與真正的惡意網站連線，存取服務都需經由 Flux Agent 負責，當資安人員要追蹤時，也只會發現 Flux Agent 的存在，實質的惡意網站則因為客戶端沒有與它作實際連線，而被隱藏起來，透過這種方式即可躲避偵查，延長惡意網站的壽命。

Fast Flux Domain 檢舉

國外某危機處理中心定期會發佈 Fast Flux Domain 檢舉信件給對應的網路位址所在單位，檢舉的信件如圖三（僅列出小部份），裡面列出該單位偵測到 Fast Flux Domain 的時間，以及在偵測當下對應的網路位址。被檢舉的網路位址所對應的 Fast Flux Doaim 非常多樣化，每天檢舉的 Fast Flux Domain 都不同，這表示這些被偵測到的 Fast Flux Domain 存活時間低，生成快。



圖三 檢舉內容

Fast Flux Domain 與對應的 IP

這些檢舉文件裡的 Fast Flux Domain 與 IP，有一些隸屬於學術網路，列出如表一。有一些 IP 所對應的 Fast Flux Domain 有多個（例如 140.xxx.145.195 與 163.xxx.104.29 與 163.xx.253.86），有一些則僅有一個對應的 Domain。

Date	IP	Fast Flux Domain
5/2	140.xxx.145.195	[vielpor.ru][cedibvo.ru]….
5/22	163.xxx.104.29	[xequjxx.ru][ykrijxx.ru][hyjamxx.ru]…..
5/22	163.xxx.139.245	[borutxx.ru]….
5/24	210.xxx.121.159	[oxcimxx.ru]
5/24	163.xx.253.86	[ebmeqbe.ru][oxcimxx.ru]

表一 與學術網路有關的 IP

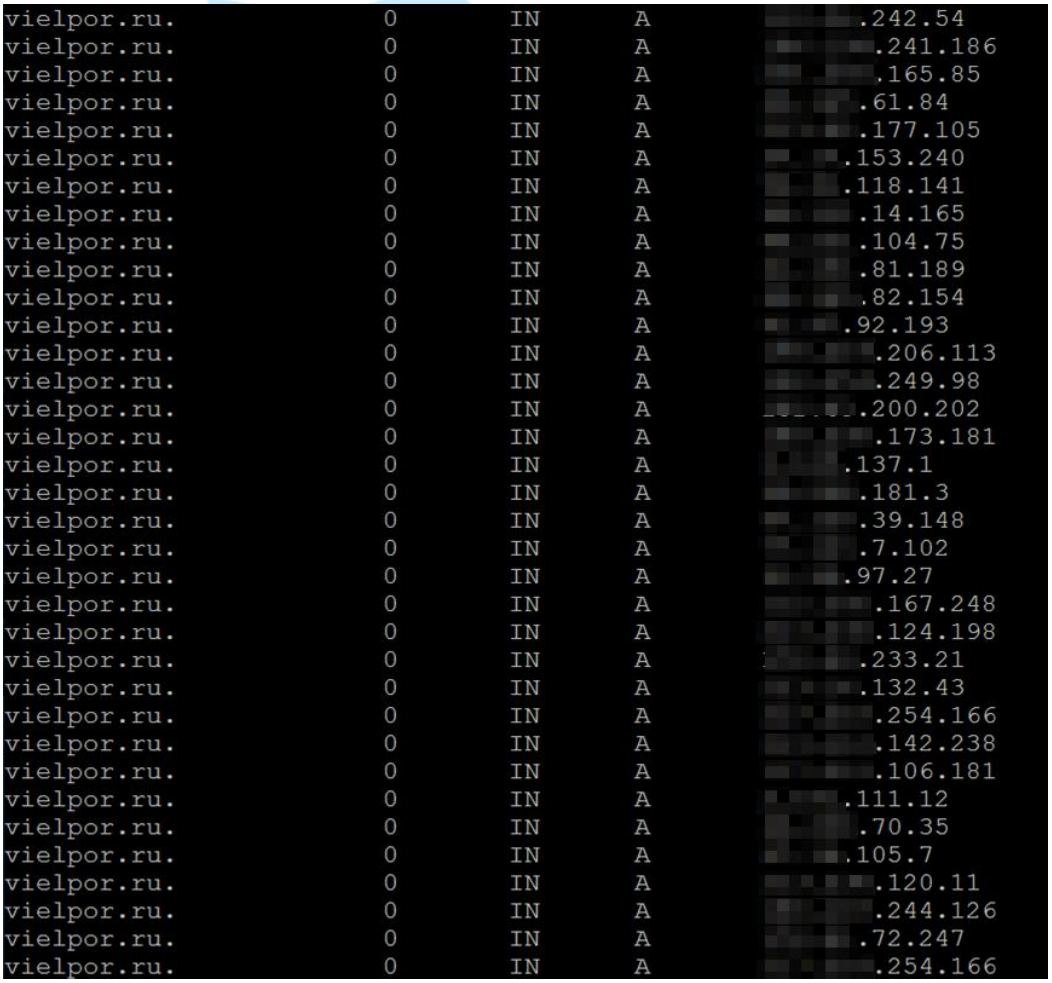
從上述列表裡面找出兩個 IP 調查，其資料如下：

- 140.xxx.145.195
  - C 單位
  - Win XP, General PC, no Web server
  - %SystemRoot%\System32\Temp 底下有一個名為 **temp68.exe** 的異常程式
- 163.xxx.139.245
  - Z 高中

- Win XP, General PC, no Web server
- %SystemRoot%\System32\Temp 底下有一個名為 **temp94.exe** 的異常程式

[140.xxx.145.195] 與 [163.xxx.139.245] 在 [%SystemRoot%\System32\Temp] 這個路徑底下都有一個以[temp]開頭的惡意程式，分別為 temp68.exe 與 temp94.exe，他們都佔用了主機的 80port 與 53port，且這兩個埠號上有非常大量的網路連線。

若以 140.xxx.145.195 對應的 vielpor.ru 為例子，在 Linux 命令列下使用 dig 指令，一分鐘執行一次 #dig vielpor.ru ，在十六小時內，得出 vielpor.ru 所對應，不重複的網路位址共有 1500 多個，如圖四。



圖四 vielpor.ru 對應的網路位址（僅列出一小部份）

所有在圖四中列出的 IP，都可以下載到一個檔名固定（avaxxx.exe），網路行為與[temp68.exe][temp94.exe]兩個惡意程式行為相似的惡意程式，表二列出一些下載的時間與大小，由時間可以看出惡意程式更新速度極快，推測是為了躲避偵測而做的些微修改。

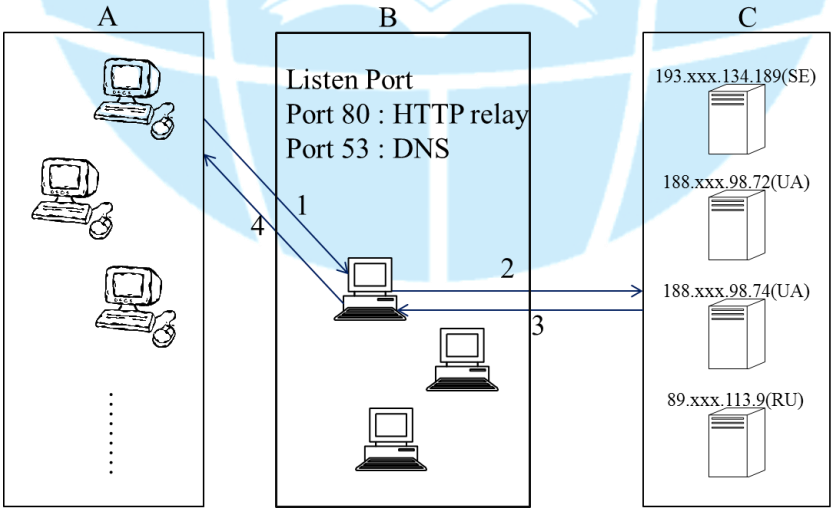
Downloaded Date	size	檔名
2012-05-22	793600 bytes	avaxxx.exe
2012-05-23	814080 bytes	avaxxx.exe
2012-05-24	821760 bytes	avaxxx.exe
2012-05-25	822272 bytes	avaxxx.exe
2012-06-07	858112 bytes	avaxxx.exe
2012-06-12	792576 bytes	avaxxx.exe

表二 惡意程式列表

網路活動

觀察該惡意程式執行之後所產生的網路流量，歸納出下面的活動圖，將網路流量上出現的節點分為 ABC 三群（實驗主機具有 Public IP，位於 B 群）：

1. A 群為第一層，在 NAT 後面或是在網路上面不具有實體網路位址的主機
2. B 群為第二層，**被檢舉的 Fast Flux Domain 所對應的主機即為此群的主機之一**
3. C 群主機網路位址變化不大，回應 B 群 Proxy 的請求



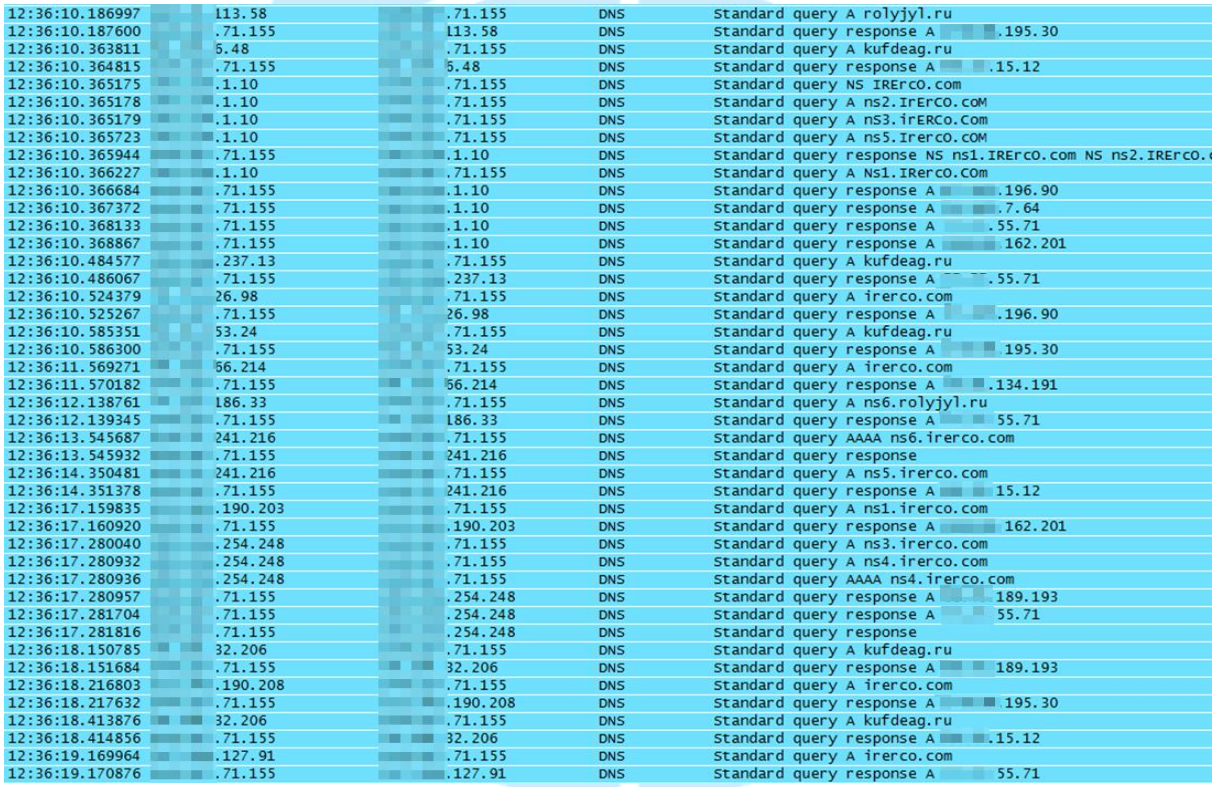
圖五 網路活動示意圖

B 群主機的惡意行為多樣化，以下逐一列出：

1. HTTP Relay Proxy
2. DNS
3. Spammer
4. Fake Anti-virus

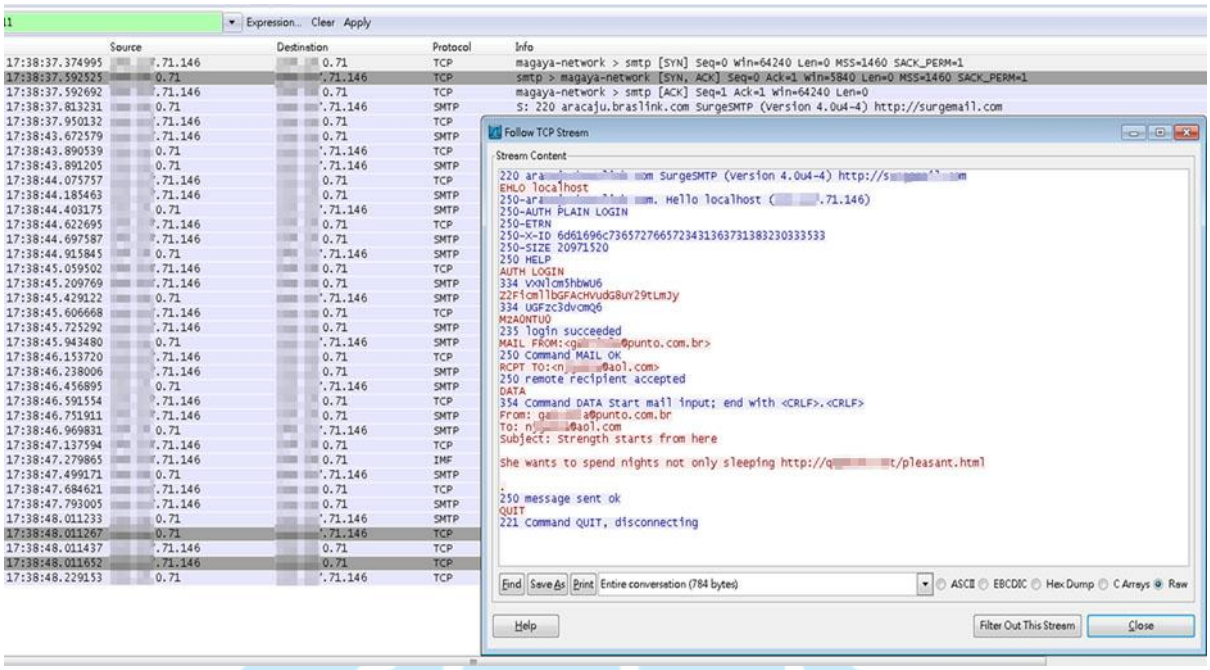
網路流量佔最多的是 Proxy 傳遞資料的活動，也有一些 DNS 流量，其行為是讓其他受害主機查詢 Fast Flux Domain 對應的網路位址，如圖六。

圖六中，zypzieb.ru 這個 Domain 短時間內被查詢了多次，每次對應的網路位址都不相同，由此可推斷，此惡意程式在利用 Fast Flux 掩蓋自身的同時，自己擔當 DNS 伺服器，私下形成自己的網絡。圖七則是 Spam 的流量。



12:36:10.186997	113.58	.71.155	DNS	Standard query A rolyjyl.ru
12:36:10.187600	.71.155	113.58	DNS	Standard query response A .195.30
12:36:10.363811	5.48	.71.155	DNS	Standard query A kufdeag.ru
12:36:10.364815	.71.155	5.48	DNS	Standard query response A .15.12
12:36:10.365175	.1.10	.71.155	DNS	Standard query NS IRErcO.com
12:36:10.365178	.1.10	.71.155	DNS	Standard query A ns2.IrErCO.coM
12:36:10.365179	.1.10	.71.155	DNS	Standard query A nS3.irERCo.Com
12:36:10.365723	.1.10	.71.155	DNS	Standard query A ns5.IrercO.cOM
12:36:10.365944	.71.155	.1.10	DNS	Standard query response NS ns1.IRErcO.com NS ns2.IRErcO.
12:36:10.366227	.1.10	.71.155	DNS	Standard query A Ns1.IRercO.COm
12:36:10.366684	.71.155	.1.10	DNS	Standard query response A .196.90
12:36:10.367372	.71.155	.1.10	DNS	Standard query response A .7.64
12:36:10.368133	.71.155	.1.10	DNS	Standard query response A .55.71
12:36:10.368867	.71.155	.1.10	DNS	Standard query response A 162.201
12:36:10.484577	.237.13	.71.155	DNS	Standard query A kufdeag.ru
12:36:10.486067	.71.155	.237.13	DNS	Standard query response A .55.71
12:36:10.524379	26.98	.71.155	DNS	Standard query A irerco.com
12:36:10.525267	.71.155	26.98	DNS	Standard query response A .196.90
12:36:10.585351	53.24	.71.155	DNS	Standard query A kufdeag.ru
12:36:10.586300	.71.155	53.24	DNS	Standard query response A 195.30
12:36:11.569271	56.214	.71.155	DNS	Standard query A irerco.com
12:36:11.570182	.71.155	56.214	DNS	Standard query response A .134.191
12:36:12.138761	186.33	.71.155	DNS	Standard query A ns6.rolyjyl.ru
12:36:12.139345	.71.155	186.33	DNS	Standard query response A 55.71
12:36:13.545687	241.216	.71.155	DNS	Standard query AAAA ns6.irerco.com
12:36:13.545932	.71.155	241.216	DNS	Standard query response
12:36:14.350481	241.216	.71.155	DNS	Standard query A ns5.irerco.com
12:36:14.351378	.71.155	241.216	DNS	Standard query response A 15.12
12:36:17.159835	.190.203	.71.155	DNS	Standard query A ns1.irerco.com
12:36:17.160920	.71.155	.190.203	DNS	Standard query response A 162.201
12:36:17.280040	.254.248	.71.155	DNS	Standard query A ns3.irerco.com
12:36:17.280932	.254.248	.71.155	DNS	Standard query A ns4.irerco.com
12:36:17.280936	.254.248	.71.155	DNS	Standard query AAAA ns4.irerco.com
12:36:17.280957	.71.155	.254.248	DNS	Standard query response A 189.193
12:36:17.281704	.71.155	.254.248	DNS	Standard query response A 55.71
12:36:17.281816	.71.155	.254.248	DNS	Standard query response
12:36:18.150785	32.206	.71.155	DNS	Standard query A kufdeag.ru
12:36:18.151684	.71.155	32.206	DNS	Standard query response A 189.193
12:36:18.216803	.190.208	.71.155	DNS	Standard query A irerco.com
12:36:18.217632	.71.155	.190.208	DNS	Standard query response A 195.30
12:36:18.413876	32.206	.71.155	DNS	Standard query A kufdeag.ru
12:36:18.414856	.71.155	32.206	DNS	Standard query response A .15.12
12:36:19.169964	.127.91	.71.155	DNS	Standard query A irerco.com
12:36:19.170876	.71.155	.127.91	DNS	Standard query response A 55.71

圖六 惡意程式的 DNS 伺服器活動



圖七 SPAM 流量內容

此外，它也利用人們害怕自己電腦中毒的心理狀態，跳出假的警告視窗通知使用者主機已經中毒，並且需要使用者付費（輸入信用卡資料）後才能清除主機上的惡意程式，使用者輸入信用卡資料後假警告視窗便會消失，猶如病毒已經被清除。

結論

隨著網路蓬勃發展，網頁應用程式多樣化，惡意程式也漸趨複雜化，單一惡意行為的惡意程式已不能滿足駭客的需求，前陣子出現的 Stuxnet、Duqu 和 Flame 三隻惡意程式，正代表著惡意程式的發展趨勢，它們不再進行簡單的惡意行為，取而代之的是更多功能、更廣泛的惡意活動。

惡意程式不僅功能多樣化，傳播途徑也一樣多樣化，這次的例子並沒有找到確實的證據來證明主機如何被感染，但 avaxxx.exe 這個惡意程式下載之後的 Icon 是一個防毒軟體常看到的盾圖樣，所以推測可能是將自己偽裝成防毒軟體，讓使用者下載之後感染主機。