個案分析-

事件單附檔中的來源 IP 與目的 IP

TACERT 臺灣學術網路危機處理中心團隊製

2013/03

前言

學術網路資安偵測團隊於開立資安事件單時會夾帶事件的原始佐證資料至教育機構資安通報平台中(事件附檔下載方法請按這裡)，事件附檔提供資安聯絡人更進一步的資訊，找出資安事件發生原因並處理之。事件單本身並沒有提供太多的事件相關訊息，多數時候僅能仰賴事件附檔中的事件發生時間、目標主機網路位址兩個資訊辨認事件發生原因。日前接獲一線單位資安聯絡人來電，表示資安事件誤判，究其原因，其實是事件佐證資料裡面的**來源**與**目的** IP 讓人誤會，因而以為是誤判。

事件描述

主機資訊：

- Ubuntu
- Web Server（Apache2）提供學生上繳電子檔作業
- 主機前端防火牆對外網僅開放 http/https/dns/SMTP/DHCP6/FTP/NTP 服務

#s		開始時間	名稱	來源 IP	來源 Port	來源地國名	目的 IP	目的 Port	目的地國名	集合事件數
1		2013/01/ 19:	Malware: Potential Malicious File Transfer Detected by GTI File Reputation (Artemis)	163. .148	80	Taiwan	118.165. .168	1756	Taiwan	1
2		2013/01/ 19:	Malware: Potential Malicious File Transfer Detected by GTI File Reputation (Artemis)	163. .148	80	Taiwan	118.165. .168	1652	Taiwan	1
3		2013/01/ 19	Malware: Potential Malicious File Transfer Detected by GTI File Reputation (Artemis)	163. .148	80	Taiwan	118.165. .168	1708	Taiwan	1

圖 1 事件附檔

圖 1 為此案例的事件附檔，其攻擊來源為 163.xx.xx.148:80，目標為 118.165.xxx.168 以字面上的「來源 IP」與「目的 IP」來看，會以為是 163.xx.xx.148 發動對 118.165.xxx.168 的攻擊，因此事件處理人認為這起事件是誤報，因為其主機前端的防火牆，僅提供 http/https/dns/SMTP/DHCP6/FTP/NTP 這幾個服務通過，而 port 1756、1652、1708 並不在這些服務之列。

實際上，事件附檔中的「來源 IP」與「目的 IP」，僅是帶有符合偵測特徵封包的「來源」與「目的」IP，而**非這個 TCP 連線的起始「來源 IP」與「目的 IP」**。以這個例子來說，佐證資料顯示帶有攻擊特徵的封包來源是 163.xx.xx.148:80，port 80 HTTP。初步判斷這

起資安事件和 163.xx.xx.148 主機上的 Web Server 有關係，調出 163.xx.xx.148 主機的 Web Log，尋找符合時間與 118.165.xxx.168 網路位址的紀錄：

```
118.165.xxx.168 [22/Jan/2013:19:37:21 +0800]
"GET /moodle/file.php/23/moddata/assignment/31/997/%E4%BC%81%E9%B5%9D-
%E8%B6%85%E8%A1%80%E8%85%A5%E7%89%88.exe?forcedownload=1 HTTP/1.1"
200 694679
```

圖 2 163.xx.xx.148 主機的 Web Log 中符合事件附檔的紀錄

從 Web Log 中可以看到 118.165.xxx.168 這個 IP 在與事件附檔符合的時間點，從 163.xx.xx.148 下載了一個檔案，在 Log 中由於 URL 編碼的關係，看起來很不能理解，將編碼還原之後，可以得到檔案的完整路徑名稱：

/moodle/file.php/23/moddata/assignment/31/997/企鵝-超血腥版.exe

163.xx.xx.148 提供學生上傳作業，校內學生把這個平台當成網路硬碟，上傳了被防毒軟體偵測出有問題的 Flash 小遊戲，回到家之後，登入學校的平台下載該 Flash 小遊戲，因而觸發資安事件。Http 連線必須先經過三向交握（如圖 3）：

一、 118.165.xxx.168 主動送出 SYN 給 163.xx.xx.148:80 請求服務

二、 163.xx.xx.148 送出 SYN+ACK 答應

三、 118.165.xxx.168 回應 ACK

四、 之後 163.xx.xx.148 把 118.165.xxx.168 請求的「**企鵝-超血腥版.exe**」傳送給它

由於惡意檔案的傳送出現在第四步驟，所以事件單的附檔來源是 163.xx.xx.148 目的是 118.165.xxx.168 因而造成事件負責人的誤解，以為該事件單是誤報。

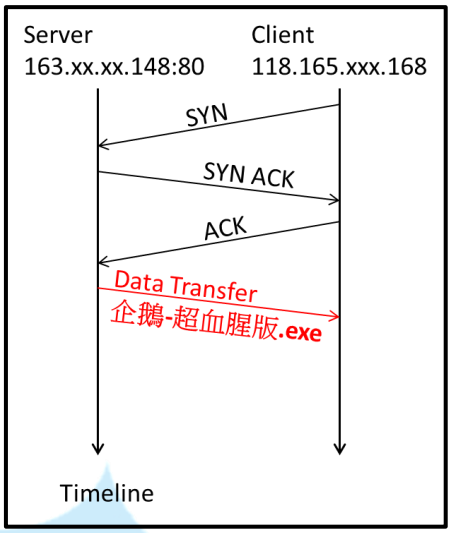

圖 3 事件的連線流程，惡意流量從 Server 端到 Client 端時被偵測到

埠號與服務

在網路通訊協定的規範文件中（RFC1700），port 0 到 port 1023 是保留給系統服務，或是擁有特權的服務使用，其中比較常見的如下列：

Port Number	Service
20/tcp	FTP Data
21/tcp	FTP
23/tcp	telnet
25/tcp	SMTP
53/udp	DNS
80/tcp	HTTP

表 1 常見的 Port 以及其服務

如果遇到事件附檔中，攻擊主機的來源 Port 是某個服務使用的特殊 Port，多半和該服務有關係，可以直接將事件單附檔中的時間與目的網路位址當關鍵字，到該服務的 Log 中比對，找出可能原因。

建議措施

- **建議上傳檔案應先經過防毒軟體掃描再儲存**

電子化是不可避免的趨勢，學校提供平台上傳作業立意良善，也讓作業可以電子檔的樣式呈現，但是難以要求使用者對上傳的檔案先進行掃毒再上傳，所以建議由伺服器端將上傳的檔案放置位置獨立出來，可以避免與重要的系統放置在同一個硬碟或同一台主機，加上不斷上傳的檔案會佔用硬碟空間，可以避免重要的系統碟空間被用光，並且在使用者上傳到伺服器時進行防毒掃描，對檔案進行基本的過濾。