個案分析-

垃圾郵件 APT 攻擊分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/12

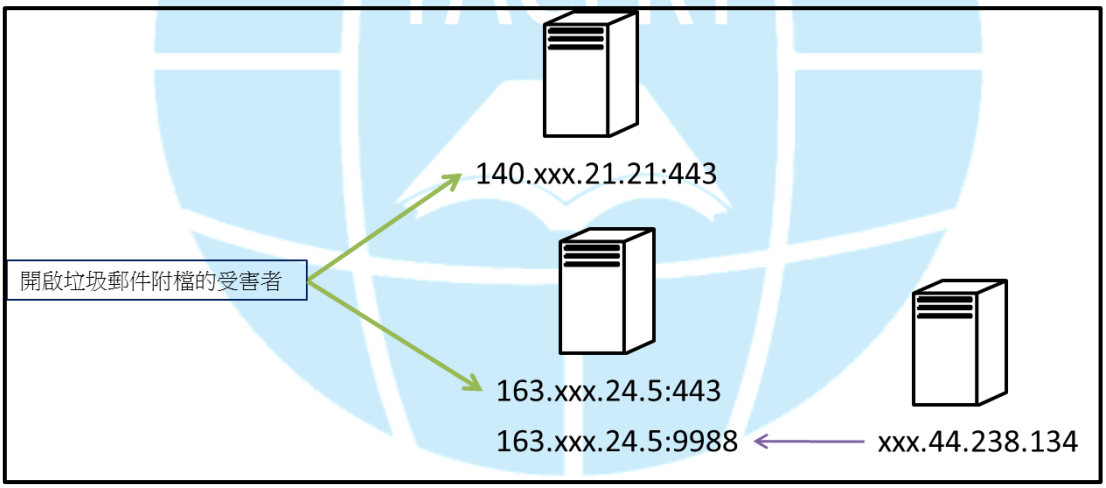
前言

APT 為進階持續性滲透攻擊(Advanced Persistent Threat 的縮寫)，APT 攻擊會根據攻擊目標的喜好和生活型態，客製惡意網頁、文件、垃圾郵件等，持續不斷地發送，引誘攻擊目標點擊或打開，就像釣客為了釣到特定的魚，而去研究魚的習性喜好，製作出魚喜歡的餌，並且在特定地點和時間使用這個餌，引誘目標上勾。

APT 攻擊又以垃圾郵件最常見，一封精密巧妙的郵件，如果收件者是工作的同事，附檔又是跟工作相關的文件，基於工作上的需要，要人不打開都難，這也是 APT 攻擊最難防範的地方。

事件說明

本次的案例分析起因來自於一封附檔名為「102 年政府行政機關辦公日曆表.xls」的郵件，該郵件的附檔並不是子虛烏有，而是政府機關每年度的行事曆，這個惡意的郵件附檔利用社交工程，發送給相關的政府人員，引誘他們打開。附檔打開後，會在背景下載惡意程式，連線到其他主機的 443 port，而這些被連線的主機，其中有兩個位於 TANet（140.xxx.21.21 與 163.xxx.24.5）。示意圖如圖一。

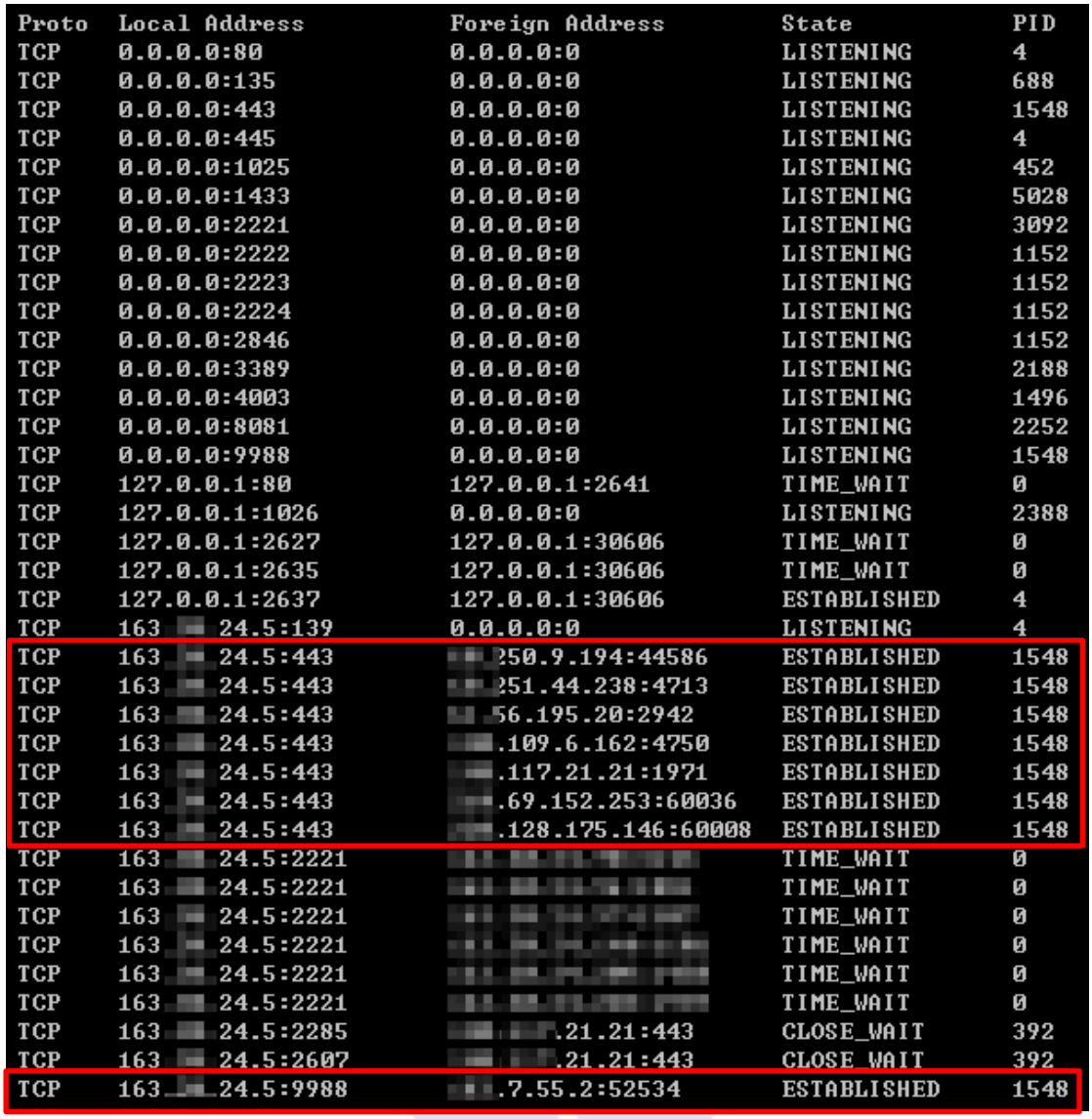


圖一 網路連線示意圖

- 163.xxx.24.5 主機資訊
  - 圖書館系統
  - Windows 2003
  - 防火牆狀態關閉
  - 遠端桌面開啟

– IIS、MSSQL 服務開啟

由圖一可以看到，163.xxx.24.5 上的 443 port 提供給開啟垃圾郵件附檔的受害主機連線，另外一個 9988 port，則是由駭客使用，由 PID 相同得知這兩個埠號由相同的程式使用。



Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	688
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1548
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	452
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	5028
TCP	0.0.0.0:2221	0.0.0.0:0	LISTENING	3092
TCP	0.0.0.0:2222	0.0.0.0:0	LISTENING	1152
TCP	0.0.0.0:2223	0.0.0.0:0	LISTENING	1152
TCP	0.0.0.0:2224	0.0.0.0:0	LISTENING	1152
TCP	0.0.0.0:2846	0.0.0.0:0	LISTENING	1152
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	2188
TCP	0.0.0.0:4003	0.0.0.0:0	LISTENING	1496
TCP	0.0.0.0:8081	0.0.0.0:0	LISTENING	2252
TCP	0.0.0.0:9988	0.0.0.0:0	LISTENING	1548
TCP	127.0.0.1:80	127.0.0.1:2641	TIME_WAIT	0
TCP	127.0.0.1:1026	0.0.0.0:0	LISTENING	2388
TCP	127.0.0.1:2627	127.0.0.1:30606	TIME_WAIT	0
TCP	127.0.0.1:2635	127.0.0.1:30606	TIME_WAIT	0
TCP	127.0.0.1:2637	127.0.0.1:30606	ESTABLISHED	4
TCP	163.[redacted]24.5:139	0.0.0.0:0	LISTENING	4
TCP	163.[redacted]24.5:443	[redacted]250.9.194:44586	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted]251.44.238:4713	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted]56.195.20:2942	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted].109.6.162:4750	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted].117.21.21:1971	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted].69.152.253:60036	ESTABLISHED	1548
TCP	163.[redacted]24.5:443	[redacted].128.175.146:60008	ESTABLISHED	1548
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2221	[redacted]	TIME_WAIT	0
TCP	163.[redacted]24.5:2285	[redacted].21.21:443	CLOSE_WAIT	392
TCP	163.[redacted]24.5:2607	[redacted].21.21:443	CLOSE_WAIT	392
TCP	163.[redacted]24.5:9988	[redacted].7.55.2:52534	ESTABLISHED	1548

圖二 由 PID 相同可以得知 port 443 和 port 9988 由同一個程式使用

PID1548 的執行程式為 svchost.exe，放置在 E:\WINDOWS\system32\com\下，合法的 svchost.exe 路徑應該是 E:\WINDOWS\system32\，由放置路徑可以知道此 svchost.exe 不是合法的程式。

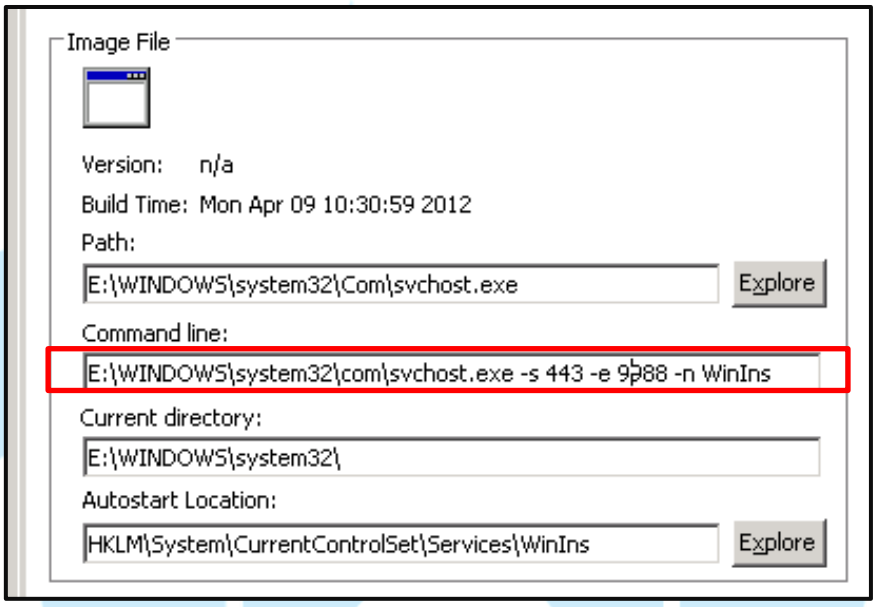
圖三秀出這個假的 svchost.exe 所使用的參數：

– **E:\WINDOWS\system32\com\svchost.exe -s 443 -e 9988 -n WinIns**

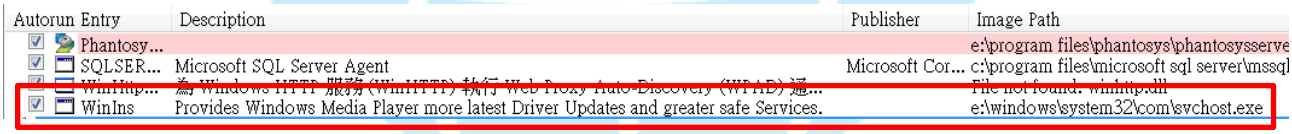
可以看到參數剛好有 443 與 9988 兩個數字，符合圖二的埠號資訊。

Program	IP:Port	
E:\WINDOWS\system32\com\svchost.exe	163.xxx.24.5:443	For Victim
E:\WINDOWS\system32\com\svchost.exe	163.xxx.24.5:9988	For Master

表一 惡意程式放置路徑以及其所使用的埠號

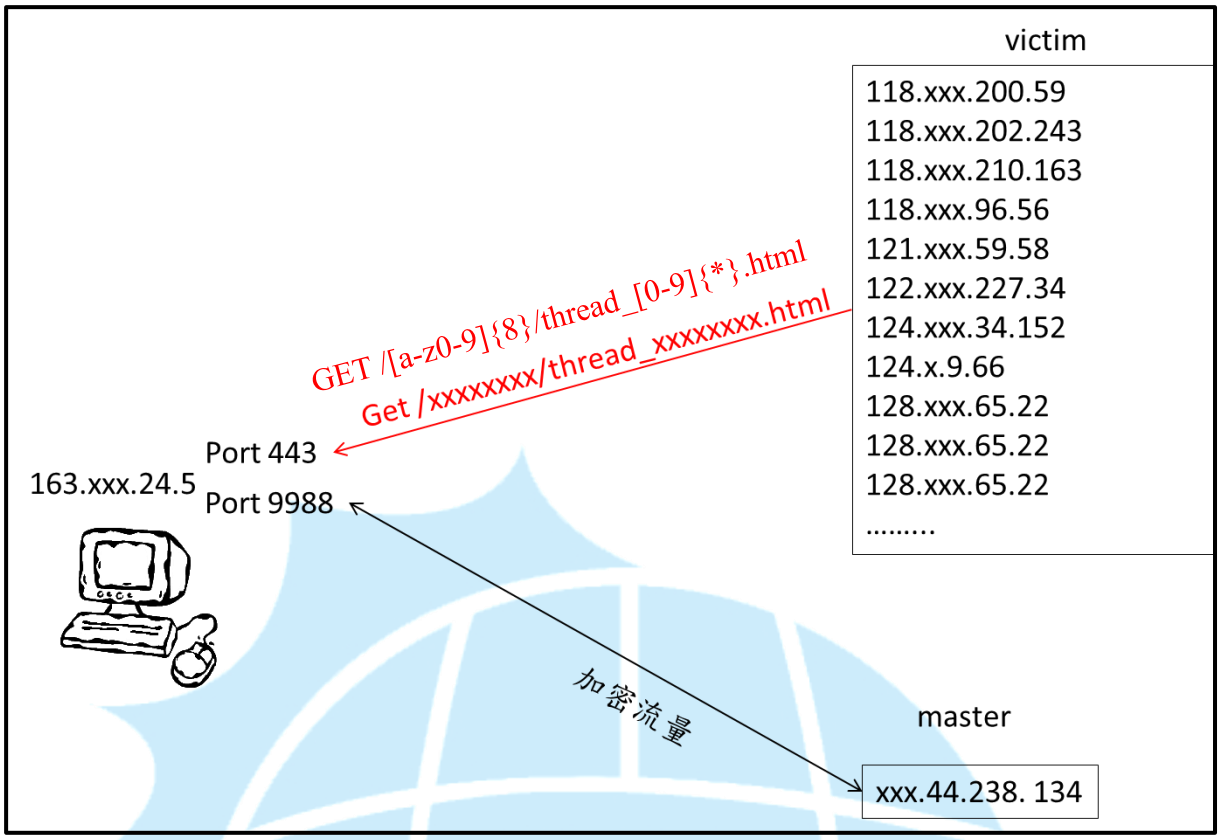


圖三 PID1548 程式的放置路徑以及使用參數



圖四 E:\WINDOWS\system32\com\svchost.exe 在登錄檔中的註冊資訊

在 163.xxx.24.5 主機上側錄流量（時間約一天），發現約有 102 個不同的 IP 自動與 163.xxx.24.5:443 有連線的動作，往來的封包表頭有相似之處，如圖四。



圖五 與 163.xxx.24.5 連線的 IP 狀況

建議措施

電子郵件附檔

- 在開啟前先進行掃描，線上資源如 VirusTotal
- 將附檔上傳到 Google Doc 開啟

主機或個人電腦

- 使用防火牆
- 備份網路開啟的埠號，定時比對是否有異常埠號打開
- 對系統檔案進行 Hash，定時比對

由於目前的惡意活動，都會牽涉到網路活動，對著重於提供服務的伺服器而言，

只要定期檢視有沒有異常的服務在網路狀態上,很輕易就可以發現異常。相對而言，個人主機上的惡意活動就比較難發現，只能依賴使用者對主機的狀況判斷。其中，對系統檔案 Hash，定期比對是一個比較麻煩但也相當準確的方法，麻煩的是每次有更動系統檔就要重新 Hash（更新、安裝新軟體等都會更動到）。這邊提供的建議雖然無法百分之百防範，但至少能對主機的資訊安全起一層的保護。