

個案分析-

M大學之電子郵件社交工 程事件分析報告



TACERT 臺灣學術網路危機處理中心團隊製

2014/07

一. 事件簡介

1. 103 年 3 月中旬一位署名「On Behalf Of 系統管理者」寄了一封主旨為『【資訊安全通知】有關資訊安全，請全校教職員生配合事項。』給全校主管及師生，並夾帶惡意程式檔案引誘用戶打開去安裝。

From: cornmail@163.com [<mailto:cornmail@163.com>] On Behalf Of 系統管理者
Sent: Tuesday, March 18, 2014 11:06 AM
To: all@...edu.tw
Subject: 【資訊安全通知】有關資訊安全，請全校教職員生配合事項。

一、依 18/3 資訊安全暨個人資料保護推行委員會第四次會議決議：郵件統一安裝登入安全控件，以免郵件帳號密碼被騙取，未安裝安全控件可能導致某些郵件收取問題，安裝后可以恢復。

二、請自行登入 Mail2000 或 █████ 做郵件帳號密碼的變更，帳號包括個人帳號及公務帳號及校友帳號。

三、密碼變更原則為：

- (一) 密碼不得空白
- (二) 密碼不得跟帳號名稱相同
- (三) 新密碼可與舊密碼相同
- (四) 密碼為 6 至 14 個字元
- (五) 密碼須同時包含英文字母及數字

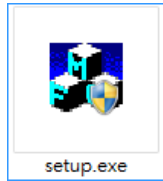
四、各單位資訊管控員個人帳號在去年已套用更為嚴格的密碼變更要求，因此不在此次要求範圍。

五、若有相關問題，請與分機 █████ 或 Call Center █████ 聯絡，或 help@...edu.tw。

2. 其信件內文提到『資訊安全暨個人資料保護推行委員會第四次會議決議』讓人誤以為真實會議，然而仔細查看該校確實有該會議，但並非第四次會議也無提及郵件安全性議題，故內容可知為偽造。
3. 從寄件者的位址為「cornmail@163.com」可以直接判定為非管理人員帳號，網域名稱為「Guangzhou, P. R. China」所註冊擁


有，故幾乎能判定為大陸駭客所使用。

4. 該信件的附加檔案為 setup.zip，解壓縮後為『setup.exe』，但大小只有 132 KB 並執行需要管理者權限，相當可疑。

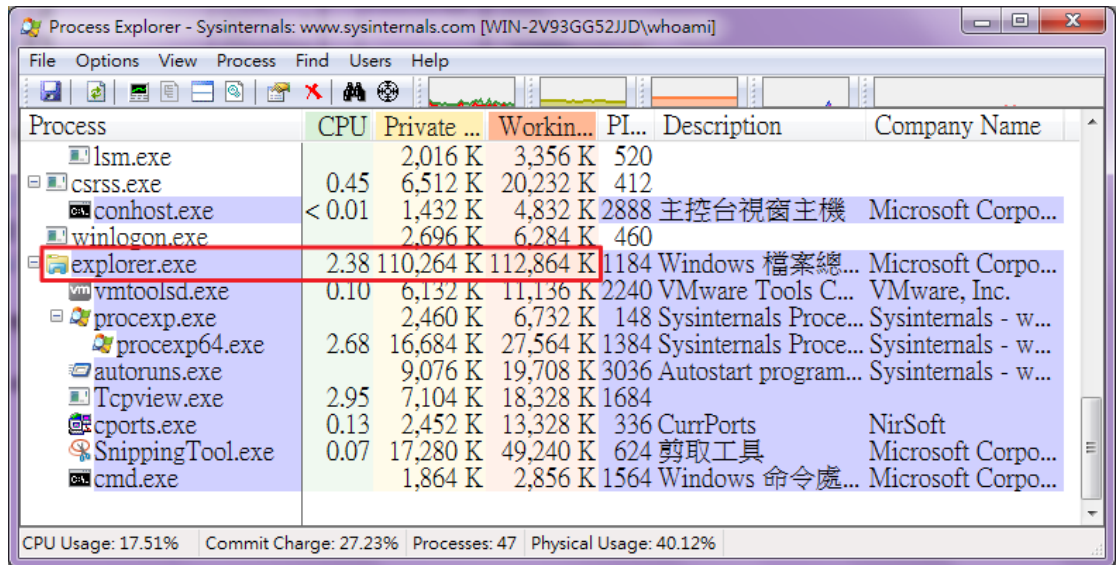


二. 事件檢測

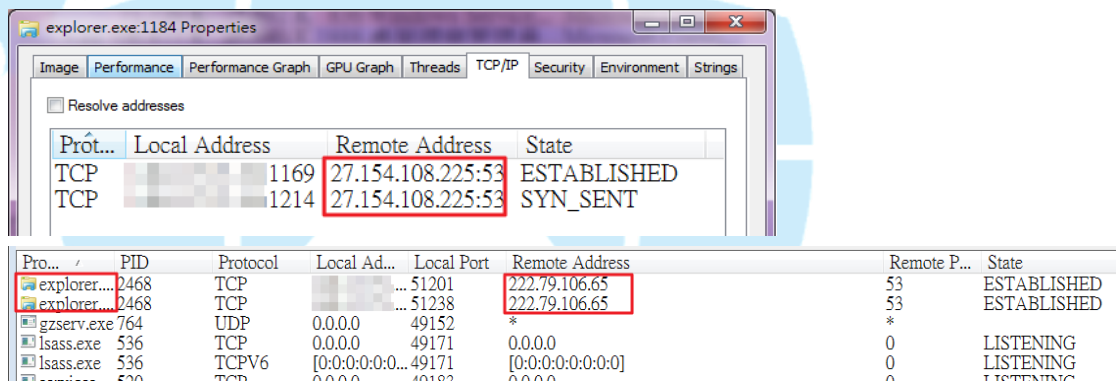
1. 首先將該惡意程式『setup.exe』上傳至 Virustotal 檢測，發現檢測出的比例居然是 0/50，也就是說沒有任何一家的防毒軟體能偵測出是惡意程式。

SHA256:	aab6310e50abdf56c4cfdd5e9c3f04471dbfd7e6f17cec383e84a9c819d108b0	
File name:	setup.exe	
Detection ratio:	0 / 50	
Analysis date:	2014-03-18 08:18:43 UTC (3 months, 1 week ago)	

2. 實地用系統 Win7 (x64) 進行檔案測試，並且側錄其網路封包行為。
 - A. 將 setup.zip 解壓後得出 setup.exe 執行檔，執行該檔案待執行完畢後惡意程式及自我移除，隨後立即檢查背景程式執行情形卻看不出明顯異常。



- B. 過了一段時間檔案總管系統程式「explorer.exe」的 CPU 及 RAM 的使用率偏高一些，檢測其網路行為赫然發現居然開始向外部連線傳送資料。



- C. 此紀錄的主要有兩個連外 IP，分別為「27.154.108.225」和「222.79.106.65」，這些 IP 皆來自中國的福建省廈門。
- 從網域名稱「dynamic.163data.com.cn」判斷為動態非固定 IP。
 - 「163data.com.cn」網域名稱為「中国电信集团公司」所擁有。

IP address: 222.79.106.65

Host name: 65.106.79.222.broad.xm.fj.dynamic.163data.com.cn

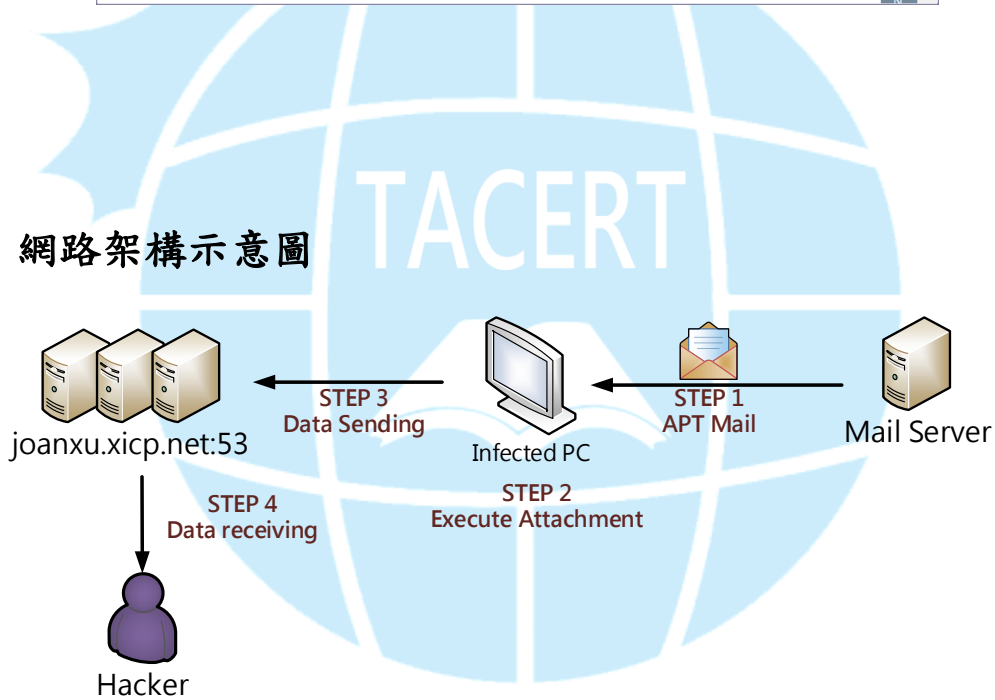
IP address: 27.154.108.225

Host name: 225.108.154.27.broad.xm.fj.dynamic.163data.com.cn

- D. 惡意程式可能透過某種系統漏洞，合法控制 explorer.exe，將感染主機的所有文件存取權限取得，利用網路行為 SYN_SENT 傳送至上層主機的 DNS PORT 53，以規避可能的資安設備偵測。
- E. 從網路封包來分析發現，感染主機會不斷向網域名稱發送加密資料，該網域名稱為「joanxu.xicp.net」，經過 DNS 解析 IP 就是「222.79.106.65」和「27.154.108.225」。
- a. 由於 DNS 正解析都是對應到此兩 IP，且此兩 IP 都網域反解析皆不是「joanxu.xicp.net」，研判此兩 IP 可能也是中繼站跳板。
- b. 該網域名稱「xicp.net」的註冊商為上海的一間公司，「SHANGHAI BEST ORAY INFORMATION S&T CO. LTD.」，可能為中國的駭客所為。
- F. 從側錄的封包中無法得知傳送的資料內容，都是經過特殊加密方式的密文。



三. 網路架構示意圖



- STEP 1:** 個人電腦主機收到偽造的APT惡意郵件。
- STEP 2:** 個人電腦主機執行郵件的附加惡意檔案並遭受感染。
- STEP 3:** 受感染主機會透過合法「explorer」程序，將主機資料傳至網址「joanxu.xicp.net:53」，IP為「222.79.106.65」或「27.154.108.225」。
- STEP 4:** 駭客可接收來至「joanxu.xicp.net」的中繼資料達到資料竊取目的。

四. 結論

1. 該資安事件主要是透過偽造的 APT 郵件社交工程攻擊方式。
2. 當使用者誤執行郵件附加檔案 setup.exe 後，原本的檔案會自行移除且取得系統程式權限，並不會產生明顯的惡意程式在背景執行。
3. 檔案總管程式 explorer.exe 會不定期對外部網址進行連線，並且將資料透過加密方式傳送出去。
4. 針對 explorer.exe 進行 Virustotal 檢測也無任何異常，故無法明確針對有問題檔案進行排除。因為 explorer.exe 是系統檔案，若將之移除會造成系統無法正常使用。
5. 任何電子郵件只要有附加檔案(特別是執行檔)，一定要多加留意可能的危險。

五. 建議措施

1. 因為 setup.exe 並無產生新的惡意程式，故舊有防毒軟體無法偵測出異常行為。
2. 最佳的解決方式就是重新安裝作業系統，並安裝防毒軟體做基本防護。
3. 開啟郵件前務必檢查來源端位址是否正常，若非公司內部網域可能都是惡意郵件。
4. 就算是公司網域來源端位址的郵件也要特別注意附加檔案是否

異常，若為 exe、com 或 scr 等執行檔就不要開啟。

5. 現今網路攻擊方式太多樣化，使用者養成良好資安觀念才是最安全的保護方式。

