# TACERT 資安電子季報-第二季

目錄：



## TACERT 資安電子季報簡介

TACERT 資安電子季報由臺灣學術網路危機處理中心(Taiwan Academic Network Computer Emergency Response Team，簡稱 TACERT)中心負責編撰，自 101 年度起，每季將匯整當季學術網路資安事件類型趨勢、安全性公告、資安事件個案分析、資安新知等資訊，期能提供學術網路使用者學習資安知識與能力，共同加強學術網路的防護。

## 最新消息

- 教育部資安團隊每年度辦理的教育訓練規劃已放置於 TACERT 網站的「教育訓練」項目，請有興趣的人員可自行參閱！

資安網站連結

- TACERT 網站
- 教育機構資安通報平台
- 教育部全民資安素養網

## 近期資安活動

108/8 108 年度臺灣學術網路危機處理中心資安巡迴研討會-資安趨勢暨網路安全概要

108/9/25~108/9/27 TANET 2019 - 臺灣網際網路研討會暨資訊安全 x 資訊學門成果發表會

## 本季資安事件類型趨勢

教育機構資安通報平台自 108 年 4 月至 6 月，共成立 5,521 張資安事件單資安事件類型大致可分為 INT (Intrusion ，入侵攻擊)與 DEF (Deface ，網頁攻擊)兩種類型。本季 INT 類型佔所有資安事件類型中的 99% ，其 INT 類型(圖 2)又以「殭屍網路 BOT」、「系統被入侵」及「對外攻擊」的子類型比率最高。

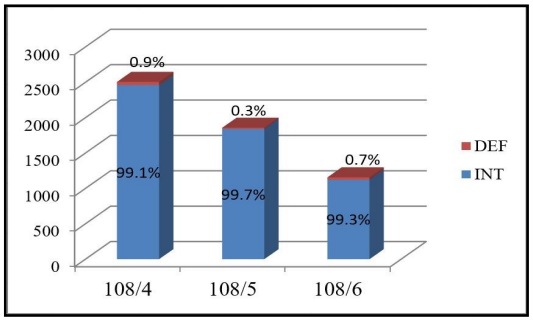



圖 1. 108 年第二季資安事件類型比例圖

DEF 類型(圖 3)以「其他類型網頁攻擊」、「個資外洩」及「惡意網頁」的子類型佔前三名。近期觀察到學術網路惡意挖礦類型事件有日益增加的趨勢，提醒各單位加強防範，建議措施：①避免連線可疑網站；②定期修補系統；③定期更新軟體；④安裝防毒軟體；⑤安裝外掛擴充套件；⑥使用高強度的密碼，並且避免重複使用相同密碼登入其他系統。

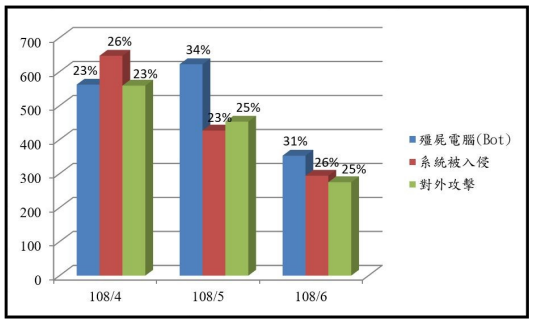



圖 2. 108 年第二季 INT 子類型前三名比例圖

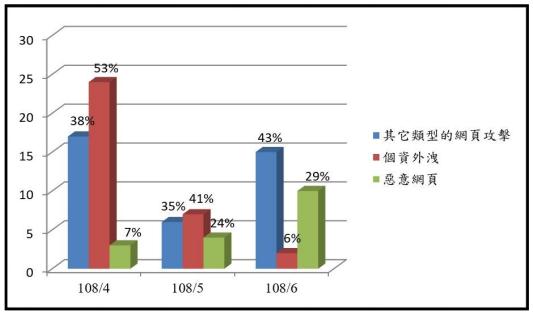



圖 3. 108 年第二季 DEF 子類型前三名比例圖

## 安全性公告

※ 108/04/10 華碩電腦 ASUS Live Update 工具程式可能遭受 APT 攻擊，建議使用者儘速更新！

※ 108/05/15 Toshiba 和 Brother 印表機 Web Services 列印存在安全漏洞，攻擊者可利用進行反射放大 DDos 攻擊。

※ 108/06/03 校園數位學習平台 WMP 智慧大師含有 Command Injection 漏洞！

※ 108/06/10 校園英聽教材互動廣播系統 存在 資料庫注入攻擊 漏洞 ，請盡速確認並進行修補作業！

※ 108/06/10 eClass 平台 存在 任意檔案下載 漏洞，請盡速確認並進行修補作業！

# 資安事件個案分析-InfoSteal 竊聽程式攻擊事件分析報告-1

※ **事件簡介：**

1. 在 2019/2 中旬趨勢科技研究員在掃描中國、台灣、義大利與香港的漏洞主機時，發現一個新型態攻擊工具包結合了木馬與工具來散播挖礦程式與竊取資料，並且會透過 Internet 與區域網路散播自己。在成功地侵入受害主機後，多階段的感染過程會使用趨勢科技稱為 Trojan.Win32.INFOSTEAL.ADS 的惡意程式來開始，它將會連線 C2 伺服器來傳送主機資訊，並且下載惡意程式的負載(payload)。
2. 在學術網路內，INFOSTEAL 惡意程式的偵測規則為「MALWARE-CNC Win.Trojan.Fakewmi variant outbound connection attempt」，而且在 2019/3 首次偵測到有 18 件資安事件，至 2019/4 上升為 38 件，整個呈現上升趨勢。
3. 為了瞭解此類型攻擊行為可能造成的影響，本中心取得起始的惡意程式樣本來進行檢測。

※ **事件檢測**

1. 首先，使用一台安裝 Windows 7 64 位元作業系統的虛擬主機進行隔離環境測試，將樣本 InfoSteal.exe 放於主機上執行。在執行前，其經 Virustotal 檢測之惡意程度為 61/70。
2. 程式 InfoSteal.exe 在執行後，即於所在的資料夾中消失。觀察主機對外的網路連線狀況，發現 svchost.exe 會對外連線美國 IP:23.41.139.27:80，如圖 4 所示。
3. 檢查主機上防火牆的輸入規則設定，發現三個非系統本身預設的規則，分別為 ShareService、UDP 與 UDP2，這三個規則開啟了本機端的 65533、65532 與 65531port，允許主機上的任何程式執行時，讓任何人從遠端任何位址來進行連線，推測這些 port 的開啟為駭客的攻擊行為之一。
4. 檢視背景程式運作情形，發現有三個程式的 Description 與 Company Name 為空白，正常的程式應該有資訊，推測可能為惡意程式，如圖 5 所示。
5. 查看程式 svchost.exe wmiex.exe 與 taskmgr.exe 在主機內的檔案存放位置，發現在那些位置無法看到這些程式，要透過將資料夾選項的檢視設定修改為「不隱藏保護的作業系統檔」之後才看得到這些檔案，讓使用者不容易發現它們的存在，如圖 6。
6. 從程式 svchost.exe、wmiex.exe 與 taskmgr.exe 的屬性「Strings」內容，發現這三個程式的字串都提到賽門鐵克的憑證與憑證下載網址(如圖 7 所示)，推測這三個惡意程式可能被嵌入賽門鐵克的憑證，這樣竊取憑證的設計容易造成防毒軟體判定它為合法的程式。

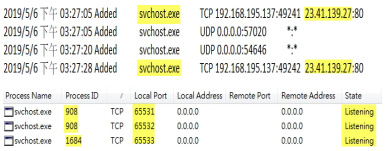



圖 4.發現 Process ID 908 與 1684 的程式 svchost.exe 執行時有開啟三個 port:65531~65533，連線狀態一直為 Listening

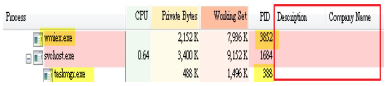



圖 5.

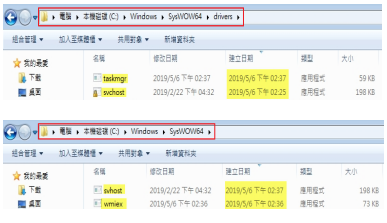


圖 6.由建立日期判斷此為 InfoSteal.exe 執行後所產生的檔案，其中 svchost.exe 與 svhost.exe 兩者建立時間相同，而且檔案大小相同，推測可能為相同檔案

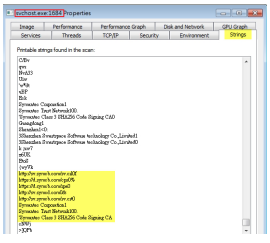
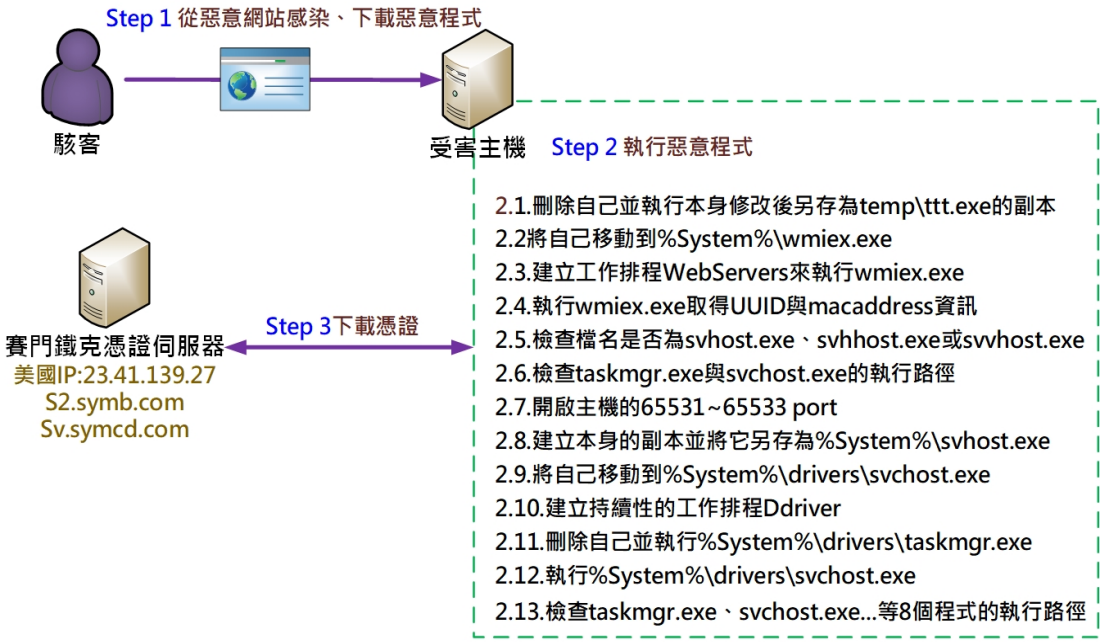


圖 7.

## 資安事件個案分析-InfoSteal 竊聽程式攻擊事件分析報告-2

※ **網路架構圖：**




※ **建議與總結：**

1. 本個案的攻擊手法主要在感染主機後，將惡意程式安裝於 Windows 系統檔存放的資料夾內，會檢查是否有相關的舊版本軟體存在，透過刪除與初始化將這些舊版本軟體、檔案和程序重新安裝與設定，來讓受害主機感染最新版的惡意軟體。
2. 該惡意程式在執行後，會利用自己本身的資源建立一個 c:\windows\temp\ttt.exe 來啟動更新作業。
3. 它會檢查檔案名稱是否為 svhost.exe、svhhost.exe 或 svvhost.exe，如果不是，則會終止所有舊版的惡意軟體、啟用防火牆，並且開放 port。
4. 它會在驅動程式中植入修改後的自身副本，並建立一個工作排程來執行 wmiex.exe，作為線上連線來傳送系統資訊。
5. 由於它開啟 65531~65533port，能讓任何程式從任何來源來使用這些 port，容易讓駭客為遠端管理植入駭客工具於主機內。
6. 放於主機系統檔資料夾內的惡意程式，一般是隱藏狀態，如果不解除隱藏保護，則使用者看不到它們的存在，將使它們持續潛伏在受害主機內來竊取資訊。
7. 關於本個案之資安防護措施，有下列幾點建議提供參考：① 不隨意瀏覽不明來源的網站；② 不隨意點選不明來源的連結；③ 定期更新系統、修補漏洞與更新病毒碼；④ 定期檢視主機 port 開啟的狀況；⑤ 定期使用防毒軟體進行全系統的完整掃描。

*詳細完整個案分析報告，請參閱 TACERT 網站！*

## 資安事件個案分析-NSA 攻擊工具事件分析報告-1

### ※ 前言：

在 2019/3 月底本中心發現在學術網路內從 2019/3 起陸續有來自 http:// 47[.]106[.]217[.]147/svchosa.exe 與 http://m9f[.]oss-cn-beijing[.]aliyuncs[.]com /svchosa.exe（IP: 59.110.185.187)的惡意程式攻擊事件，該惡意程式名稱為 svchosa.exe，與系統檔 svchost.exe 之名稱僅一個字母之差，為了解該惡意程式的攻擊行為，本中心進行該程式的鑑識分析作業。

### ※ 事件檢測

1. 首先，使用兩台在同一區域網路的 Win 7 虛擬機(155 主機與 137 主機）進行 svchosa.exe 檢測，並在 155 主機(IP:192.168.195.155)上執行 svchosa.exe。


圖 8. 程式 svchosa.exe 經 Virustotal 檢測，其惡意比例為 55/70，多家防毒軟體公司以 Downloader 或 CoinMiner 命名它。

2. 檢視主機對外連線狀況，發現 svchosa.exe 會連線 2 個中國 IP，它也會針對區域網路內各 IP 進行兩個 port 的掃瞄(port scan:139port 與 445port)，而因執行 svchosa.exe 產生的 oysks.exe 會連線至新加坡與日本。在 svchosa.exe 執行一段時間後，會發現 svchostlong.exe 與 serverlong.exe 會連線區域網路內 137 主機的 445port，而 svchosa.exe 會在區域網路的 portscan 作業結束後連線中國 IP。

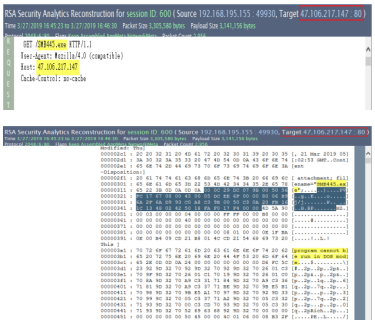


圖 9. 連線中國 IP 下載兩個程式

3. 查看連線中國 IP:47.106.217.147:80 之封包內容，發現它會下載 SMB445.exe 與 services.exe 兩程式至主機內，如圖 10 所示。

4. 查看連線日本 IP:103.101.30.10:80(如圖 11 所示)與新加坡 IP:139.99.72.56:80 之封包內容，發現這兩個連線皆為向礦池報到來進行挖礦作業之連線行為。

圖 10 連線日本 IP 為向礦池報到來

5. 檢視背景程式運作情形，如圖 12 所示，發現在 svchosa.exe 執行後會循環式地執行 ipconfig.exe（清除 DNS 快取）、taskkill.exe（強制結束 ipconfig.exe)、oysks.exe(執行挖礦）與 taskkill.exe(強制結束 oysks.exe)等程序，其中會在 C:\$aywke 產生 oysks.exe 來執行挖礦。

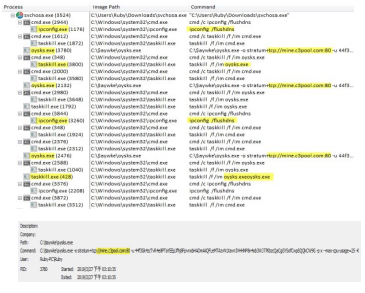
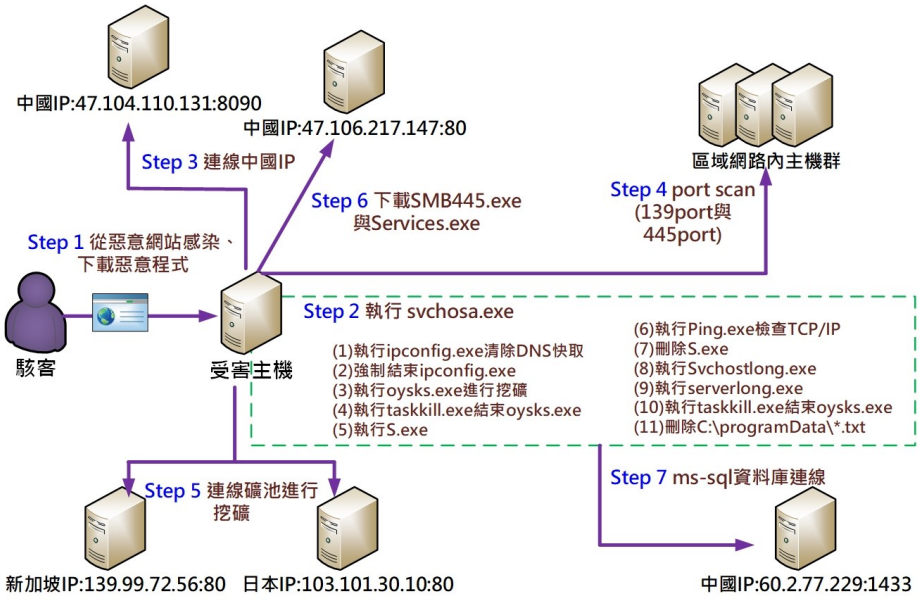


圖 11.

## 資安事件個案分析-NSA 攻擊工具事件分析報告-2

※ **網路行為架構圖**




※ **建議與總結：**

1. 本個案的攻擊手法是透過惡意程式 svchosa.exe 感染受害主機後，該主機會使用美國國安局(NSA)外洩的著名攻擊工具 EternalBlue(Svchostlong.exe)與 DoublePulsar (Serverlong.exe)來攻擊區域網路內含有 SMB 漏洞的主機。
2. Svchosa.exe 會在受害主機之 C:\建立一個含有挖擴程式的隱藏資料夾，來進行挖礦，而其資料夾命名與挖礦程式的檔案命名皆是亂數命名，不固定資料夾名稱與檔案名稱。
3. 區域網路內受感染的主機會執行惡意的 VBScripts 來下載惡意程式，並且執行隱藏的挖擴程式。
4. 針對本個案的資安防護與處理作業，提供幾點建議如下。
   (1) 修補 Windows 系統 SMB 服務漏洞。
   (2) 將駭客常使用來攻擊的 port 鎖住，如 445 port。
   (3) 不隨意開啟不明來源的網頁、信件或檔案。
   (4) 定期進行系統與病毒碼更新作業。
   (5) 定期進行系統掃毒作業。

*詳細完整個案分析報告，請參閱 TACERT 網站！*

## 資安新知-釣魚攻擊使用瀏覽器擴充工具 SingleFile 混淆惡意登錄頁面

資料來源：TREND MICRO

SingleFile 是 Google Chrome 和 Mozilla Firefox 的 web 擴充工具，允許用戶將網頁保存為一個 HTML 檔。儘管 web 瀏覽器允許使用者將頁面保存為“.htm”檔，這通常意味著在網頁中使用的不同檔案有多個資料夾。透過將一個頁面、所需的檔案和所有檔案保存在一個 HTML 文檔中，而 SingleFile 簡化了這個過程，使它更方便地處理各種用例，比如存檔網站。然而，它對威脅行動者並沒有失去作用，因為趨勢科技發現他們濫用 SingleFile 來混淆釣魚攻擊。

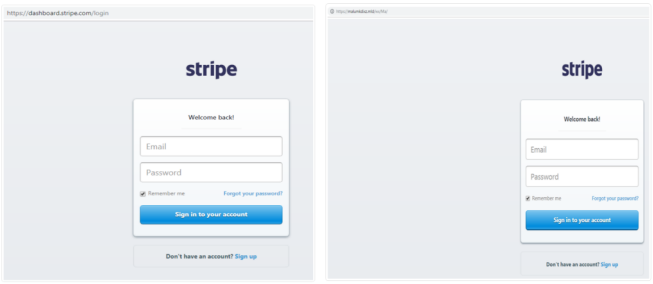



*圖 12. 比較原本 Stripe 登錄頁面(左)與基於生成的 SingleFile 頁面(右)的欺騙登錄頁面。唯一值得注意的區別是 URL*

*圖片來源：TREND MICRO*

研究人員發現的樣本顯示，網路犯罪分子使用 SingleFile 複製合法網站的登錄頁面，作為釣魚活動的一部分。而生成登錄頁面的方法非常簡單:

- 攻擊者訪問要欺騙的網站的登錄頁面（支付處理網站 Stripe 用於找到的樣本中）。
- 然後，他們使用 SingleFile 保存並生成包含整個頁面的文件，包括任何圖片（將保存為 svg 文件）

儘管它很簡單，但欺騙方法看起來非常有效，因為它實際上生成了合法登錄頁面的相同副本。

個人和組織都可以透過最佳解決方案嚴格打擊網路釣魚，將這種攻擊和網路釣魚的威脅降到最低。這些包括 ：

- 任何具有異常 URL 的網站都可能是惡意的，因為大多數公司網站都帶有他們的名字或其品牌名稱。
- 一些威脅行為者創建的 URL 看起來類似於官方網站的 URL。因此，用戶應該仔細檢查他們訪問的網站是否使用了正確的 URL。這可以透過查詢搜尋引擎這樣簡單的事情來實現。
- 除非絕對確定寄件者合法，否則使用者應避免按一下任何連結或透過電子郵件下載接收任何檔案。

臺灣學術網路危機處理中心(TACERT)

電話：(07)525-0211

網路電話代表號： 98400000

電子郵件: service@cert.tanet.edu.tw

地址：高雄市鼓山區蓮海路 70 號(國立中山大學)