TACERT 資安電子季報-第二季

目錄：

最新消息	1
本季資安事件類型趨勢	2
安全性公告	2
個案分析-帶有惡意程式的垃圾郵件 SPAM 攻擊分析	3
個案分析-校園主機感染 WannaCry 病毒事件分析報告	5
攻擊預警-預防 Petya 勒索病毒攻擊的方法	7
TACERT 組織介紹	7

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

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(TANet Computer Emergency Response Team, 簡稱 TACERT)中心負責編撰，自 2012 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

◆ 為確保資安事件能夠即時通知與處理，煩請各連線單位於資安連絡人發生異動時，務必確保資安事件的處理業務能妥善完成交接。

(1). 教育機構資安通報平台的帳號密碼進行交接。

(2). 登入教育機構資安通報平台於「修改個人資料」進行連絡人資訊更新

(3). 新接任的資安連絡人可至本中心網站的資安文件下載資安通報應變手冊，了解通報平台基本操作

近期資安活動

◆ 2017/8 106 年度臺灣學術網路危機處理中心資安巡迴研討會-網路威脅手法暨 DDoS 分析(TACERT)

本季資安事件類型趨勢

教育機構資安通報平台自 106 年 4 月至 6 月，共成立 7,528 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 97% ，其 INT 類型(圖 2)又以「殭屍網路 BOT」、「對外攻擊」及「系統被入侵」的子類型比率最高。

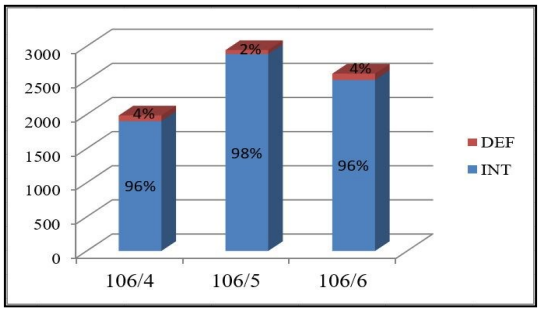


圖 1. 106 年第二季資安事件類型比例圖

DEF 類型(圖 3)以「網頁置換」、「惡意網頁」及「其他類型網頁攻擊」的子類型佔前三名。目前只要於 TANet 中偵測到有釣魚網站、嚴重的 mail spam 或其他嚴重影響網路資源的資安事件發生，教育部資訊及科技教育司會先進行封鎖作業，以避免造成更大之危害，待受害單位完成資安事件通報應變處理後，並通過教育部資訊及科技教育司的複審確認已無安全性風險，才可解除限制。有關 TANet ANTI-SPAM 網址： http://rs.edu.tw/tanet/spam.html。

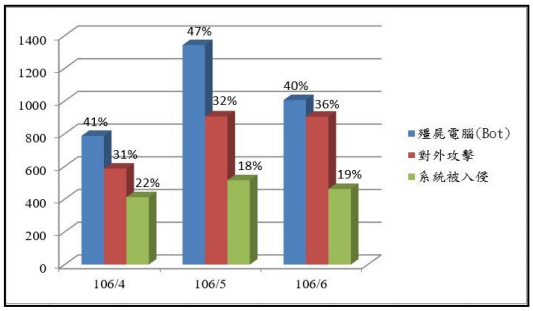


圖 2. 106 年第二季 INT 子類型前三名比例圖

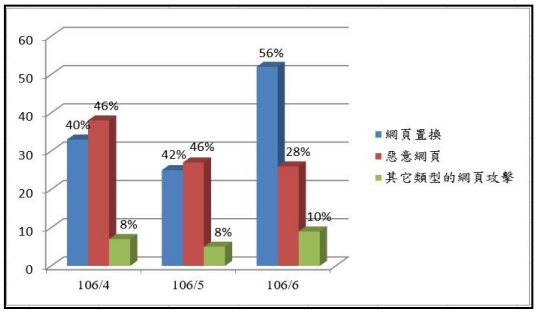


圖 3. 106 年第二季 DEF 子類型前三名比例圖

安全性公告

※ 106/04/06 特定版本 Microsoft IIS 的 WebDAV 服務存在緩衝區溢位弱點(CVE-2017-7269)，允許攻擊者遠端執行任意程式碼或造成阻斷服務

※ 106/04/28 微軟伺服器訊息區塊(SMB)協定存在數個安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速進行更新

※ 106/05/13 勒索軟體 WanaCryptor 2.0 攻擊 Windows 系統漏洞，造成檔案加密無法使用，請儘速進行更新！

※ 106/05/26 特定版本 Samba 軟體存在允許攻擊者遠端執行任意程式碼之漏洞(CVE-2017-7494)，可取得管理者權限，請儘速確認 Samba 軟體版本並進行更新

※ 106/06/09 VMware vSphere Data Protection 存在遠端攻擊弱點，建議請儘速評估更新！

資安事件個案分析-帶有惡意程式的垃圾郵件 SPAM 攻擊分析-1

※ **事件簡介：**

1. 近期發現有針對本單位進行垃圾郵件 SPAM 攻擊，其郵件以“fq”作為主旨，且內容為述說我們大量發送 SPAM 郵件，並要求依照信件內容開啟附加檔案進行修補感染，實質上為惡意程式的壓縮檔案“transcript.zip”。
2. 這次事件收件者位址為單位的公開服務地址，故有心人士會容易取得並且嘗試進行滲透。從郵件 Header 檢查發信者的 IP，為來自越南的 113.161.8.117，而非位於寄件者的網域(.ma)國家摩洛哥，表示寄件者名稱是偽造的。
3. 郵件附加檔案解壓縮後，為一支偽裝成文件檔 TXT 的 SCR 執行檔“transcript.txt….scr”，透過在檔案名稱尾端插入大量空白字元來遮蔽其附檔名 SCR，誘使使用者不注意執行。

※ **事件檢測**

1. 在測試惡意程式時候，預先使用 Win7(x86)來開啟執行該惡意程式 “transcript.txt.scr”，因為預設檔名插入大量空白過於冗長，導致 32 位元系統無法正常辨識執行。因此該惡意程式只對於 64 位元系統有效。

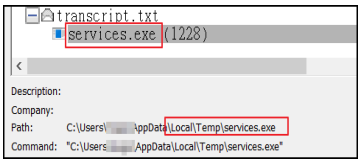


圖 4.

2. 實際執行惡意程式 scr 檔案後，在視窗上並無出現任何訊息，但透過 procexp 檢視背景程式狀態，可以看到 scr 惡意程式產生出新的子程式 services.exe，如圖 4 所示。

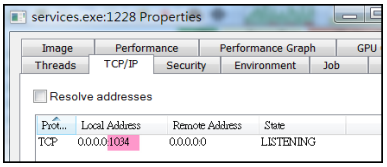


圖 5.

3. 該 services.exe 是由 transcript.txt.scr 所產生，並且位於暫存資料夾內，檢查 services.exe 的連線狀態能看出有開啟 Port Listening，表示能夠讓駭客或 C&C 連入做控制，如圖 5 所示。

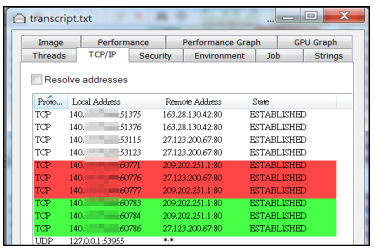


圖 6.

4. 在檢查父程式 transcript.txt.scr 的連線狀態，可以看到有大量的對外連線和流量，檢查以下連線 IP 幾乎都是搜尋引擎網站，如圖 6 所示。
5. 除此之外還觀察到惡意程式 transcript.txt.scr 除了會連到搜尋引擎網站，還會產生大量對外 port 25 的連線，可能是正在對外發送 SPAM 郵件，如圖 7 所示。

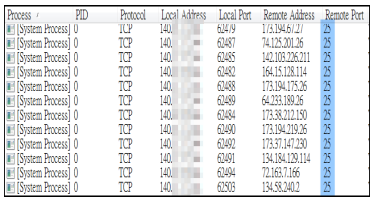


圖 7.

6. 從封包內容來檢視，transcript.txt 連到的 port 80 幾乎都是各大家的搜尋引擎，並且大量搜尋可用的電子郵件網域，並且開始準備發送 SPAM。
7. 檢查其中一比較完整的 SPAM 封包紀錄，得知惡意程式會偽造發信人地址，並且發送給搜尋到的 domain 為 163.com 收件者，通常會夾帶惡意檔案，如圖 8 所示。

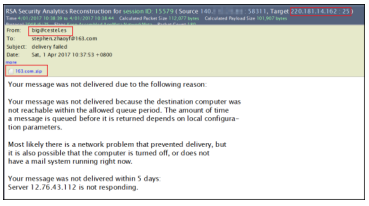
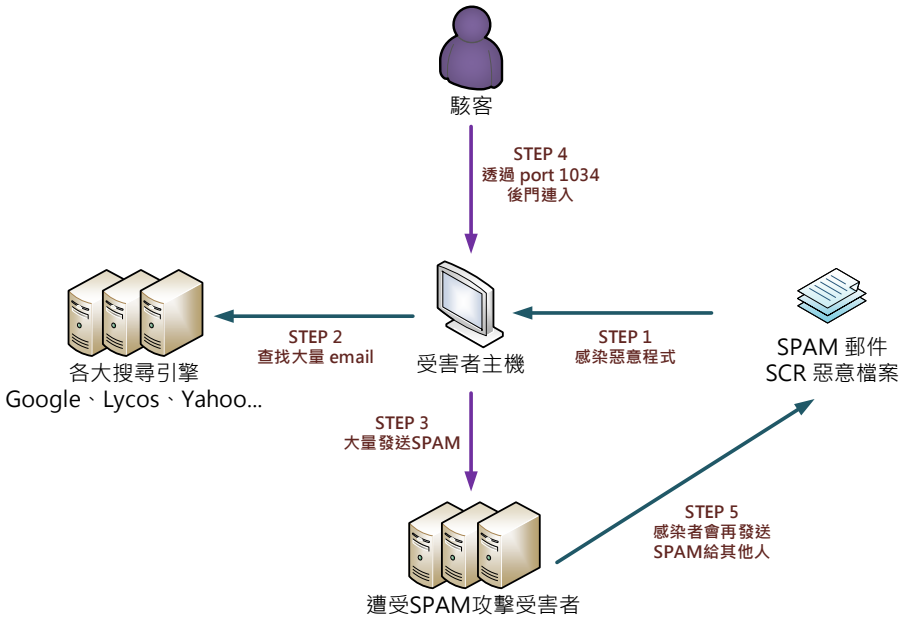


圖 8.

• • •

資安事件個案分析-帶有惡意程式的垃圾郵件 SPAM 攻擊分析-2

※ **網路架構圖：**



※ **運作流程**

1. 受害者開啟 SPAM 郵件中的附加檔案，為偽造成 TXT 的 SCR 惡意程式。
2. 受害主機會開始向外部的各大搜尋網站查找可用的郵件網域名稱。
3. 受害主機開始向搜尋到的 mail 位址發送大量的惡意 SPAM。
4. 駭客 C&C 可能透過 port 1034 連入感染主機，並下達其他攻擊指令。
5. 當新的受害者也感染惡意檔案後，也會開始對外發送 SPAM 郵件並成為新的 Botnet。

※ **建議與總結：**

一. 使用者有開啟遠端桌面 RDP 服務，並且都是使用簡易的三個字元的帳號密碼。
二. 此案例為惡意 SPAM 郵件攻擊，並附加偽造成 TXT 文件檔的 SCR 執行檔惡意程式。
三. 該惡意程式在副檔名 SCR 前塞入.TXT 和冗長的空白字元進行偽裝，一旦執行後會開啟 port 1034 為 Listen 狀態。惡意程式 SPAM 攻擊之前會大量向搜尋網站查找可攻擊的電子郵件網域，並且再對外進行 port 25 的 SPAM 郵件攻擊。
四. SPAM 郵件有可能會偽造寄件者的郵件地址為相同網域的地址，增加後害者上當的機率。
五. 該事件受害者同時也會成為攻擊其他人的加害者，並且成為殭屍網路的主機讓駭客使用。所幸該惡意程式並不會寫入開機自動啟動區，當使用者重開主機後網路攻擊行為就不會再出現。
六. 此類型的社交工程郵件近年來一直很多，有的惡意程式多為加密勒索軟體，更應提高警覺避免誤觸。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安事件個案分析-校園主機感染 WannaCry 病毒事件分析報告-1

※ **前言：**

1. 在今年 5 月中旬爆發 WannaCry 病毒利用 Windows 系統的 SMB 漏洞 透過 TCP445 連接埠來傳播，進行大規模攻擊未更新 Windows 系統的電腦。
2. 本事件為 S 大學之校內一台測試主機發生疑似惡意程式連線行為，對外進行大量 445 連接埠的連線。該主機為測試用的虛擬主機，所安裝的系統為 Windows Server 2008 R2 系統，而且自今年 3 月初過後關機至今年 5 月 17 日才再次開機。
3. 本單位取得該虛擬主機的樣本後，以還原系統的方式進行研究分析。

※ **事件檢測**

1. 首先我們將已感染中毒的虛擬主機在 VM 環境內還原，並執行檢測工具來觀察其程式行為與其對外網路行為。此外，也準備一台 Windows 7 系統的待感染主機，來觀察其病毒感染途徑與網路行為，檢測環境如圖 9 所示。

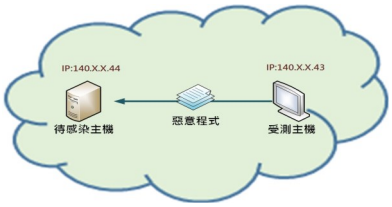


圖 9.

2. 以 Nmap 工具檢視受測主機對外的連接埠資訊，發現 135、445、3389、49154 等連接埠為開啟狀態(如圖 10)。

```
Discovered open port 3389/tcp on 140.[redacted].43
Discovered open port 135/tcp on 140.[redacted].43
Discovered open port 445/tcp on 140.[redacted].43
Discovered open port 49154/tcp on 140.[redacted].43
```

圖 10.受檢測主機對外開啟的連接埠

3. 透過 Currports 工具發現有一個執行中的程式 mssecsvc.exe，正在產生大量對外連線 445 連接埠行為，嘗試對外進行連線攻擊(如圖 11)。

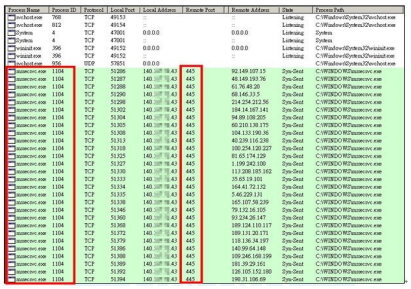


圖 11. mssecsvc.exe 對外連線 445 連接埠行為側錄

4. 透過 procexp 與 procmon 工具檢視背景程式狀態，發現程式 mssecsvc.exe 執行時會啟動另一個程式 tasksche.exe。
5. 查看程式 mssecsvc.exe 與 tasksche.exe 的內容，發現此兩個執行檔的建立日期皆為 106 年 5 月 17 日 11:07，推測可能為受測主機感染病毒的時間點。
6. 由事件檢視紀錄，發現到兩程式 mssecsvc.exe 與 tasksche.exe 在建立時只有 mmsecsvc.exe 成功執行(如圖 12)，而程式 tasksche.exe 啟用失敗，並且發生不正確的 XML 語法錯誤(如圖 13)。

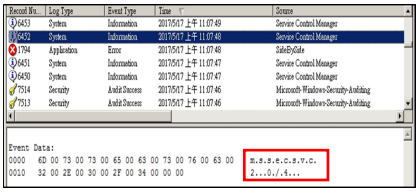


圖 12. 在 11 時 7 分系統執行 mssecsvc.exe 成功的紀錄

7. 因為受測主機存在 mssecsvc.exe 與 tasksche.exe 兩程式，又有大量以 445 連接埠對外連線攻擊的行為，因此推斷受測主機可能感染到 WannaCry 病毒。接著搜尋主機內是否存在該病毒特徵:tasksche.exe 執行後會產生的三個檔案(@WanaDecryptor@.exe、Taskdk.exe 與 Taskdl.exe)，結果無法搜尋到，可能與 tasksche.exe 無法被成功開啟有關。

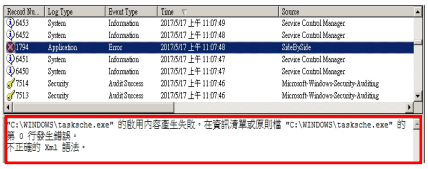
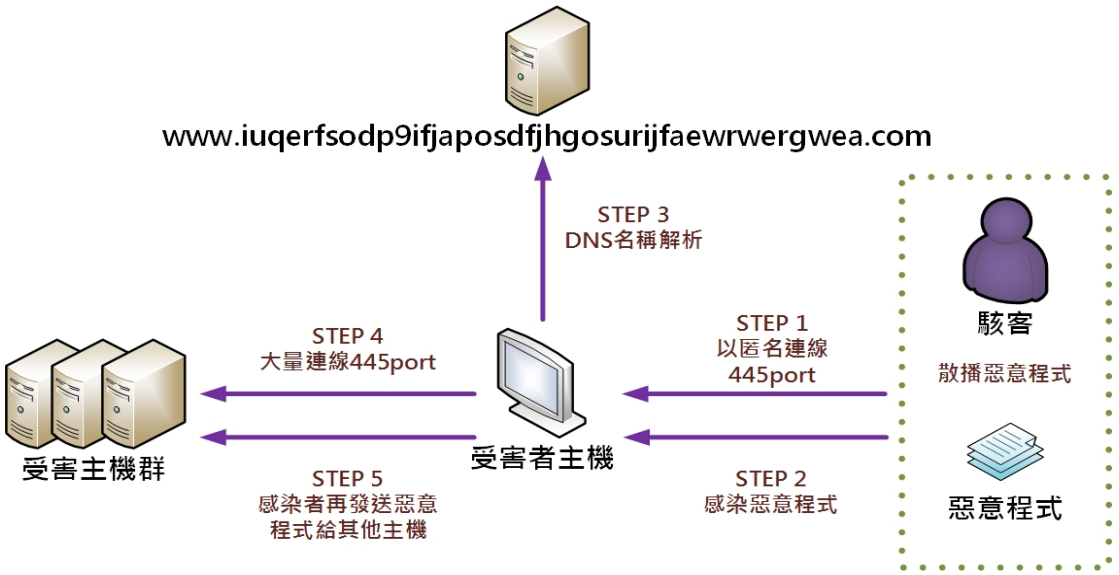


圖 13. 在 11 時 7 分系統執行 tasksche.exe 啟動失敗的紀錄

• • •

資安事件個案分析-校園主機感染 WannaCry 病毒事件分析報告-2

※ **網路行為架構圖**



1. 駭客散播惡意程式，以匿名方式 445port 連線受害者主機。
2. 植入惡意程式 mssecsvc.exe 於受害主機，該程式會呼叫與執行另一個惡意程式 tasksche.exe。
3. mssecsvc.exe 進行 DNS 名稱解析。
4. 受害者主機對外進行大量 445 port 攻擊。
5. 受害者主機植入惡意程式到受感染主機。

※ **建議與總結：**

此個案為電腦未執行系統更新來修補 SMB 漏洞，而被駭客透過開啟的 445 port 植入惡意程式。為有效預防感染 WannaCry 病毒，建議使用者進行下列的防禦措施:

1. 關閉 Windows 系統的 445 通訊埠。
2. 立即使用隨身碟、外接硬碟或者雲端空間，備份重要資料。
3. 使用 Windows Update 自動更新或手動更新微軟 KB4012215 的漏洞修補程式(漏洞編號 MS17-010)。
4. 確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。

詳細完整個案分析報告，請參閱 TACERT 網站！

攻擊預警-預防 Petya 勒索病毒攻擊的方法

繼 106 年 5 月中旬 WannaCry 勒索病毒事件後，近日在全球各地陸續爆發新型勒索病毒 Petya，尤其以歐洲最為嚴重，該病毒非之前舊型 Petya 病毒，而其攻擊行為比 WannaCry 病毒更勝一籌，駭客除了使用 SMBv1 漏動外，也會利用 Windows 的遠端指令功能 PsExec 或是 WMIC（Windows Management Instrumentation）來執行命令，包括傳染至其他電腦。為避免感染此病毒，建議使用者盡快做好防範措施。

＊ 建議措施

1. 設定 Windows 密碼與加強密碼強度
2. 建立預防 Petya 的 Kill - Switch 檔案
3. 關閉 Windows 系統的 445 連接埠。
4. 定期使用隨身碟、外接硬碟或者雲端空間備份重要資料。
5. 使用 Windows Update 自動更新或手動更新微軟的 Windows 的 SMBv1 漏洞修補程式(漏洞編號 MS17-010)與 Office 應用程式弱點修補程式(漏洞編號 CVE-2017-0199)
6. 確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。
7. 因病毒執行加密時會建立排程，讓系統自動重新開機，建議使用者發現系統無預警自動重新開機時，應即刻關閉電腦電源，以避免進一步的加密行為。

完整報告請參閱「預防 Petya 勒索病毒攻擊的方法」技術文件。

TACERT 組織介紹

臺灣學術網路危機處理中心(TANet Computer Emergency Response Team, 簡稱 TACERT)於 2010 年 6 月正式成立，由教育部委由國立中山大學進行營運。主要的任務為協助處理 TANet 各連線單位的電腦網路資通安全危安事件。除了扮演教育體系的資訊安全應變窗口，並盡力維護台灣學術網路的使用安全。

圖 17.TACERT 網站

臺灣學術網路危機處理中心(TACERT)

電話：(07)525-0211　傳真：(07)525-1535

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)