TACERT 資安電子季報-第三季

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(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

- 教育部於 104 年 10 月執行「教育部 104 年度學術機構分組資通安全通報演練計畫」，並委由臺灣學術網路危機處理中心(TACERT)辦理。透過本次演練檢視所有機關(構)學校的資料更新程度，並了解各區域、縣市網路中心及機關(構)學校通報反應能力。

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

- 2015/7~2015/8 開源碼網站安全暨防護實作之資安巡迴研討會
- 2015/8/18 資安事件鑑識分析與應用教育訓練
- 2015/8/28-8/29 台灣駭客年會 HITCON 2015

本季資安事件類型趨勢

教育機構資安通報平台自 104 年 7 月至 9 月，共成立 4,415 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 98% ，其 INT 類型(圖 2)又以「系統被入侵」、「對外攻擊」及「殭屍網路 BOT」的子類型比率最高，觀察本季學術網路資安事件有較下降的趨勢。

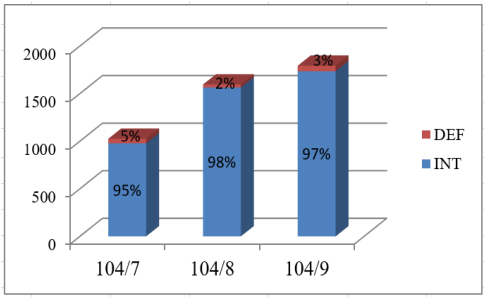


圖 1. 104 年第三季資安事件類型比例圖

DEF 類型(圖 3)以「網頁置換」、「惡意網頁」及「釣魚網站」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。

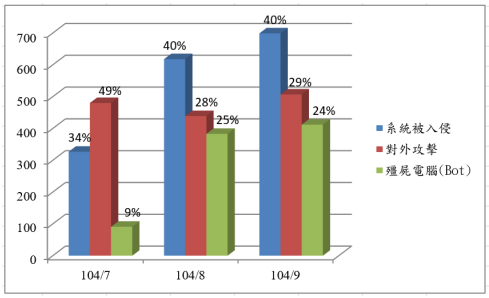


圖 2. 104 年第三季 INT 子類型前三名比例圖

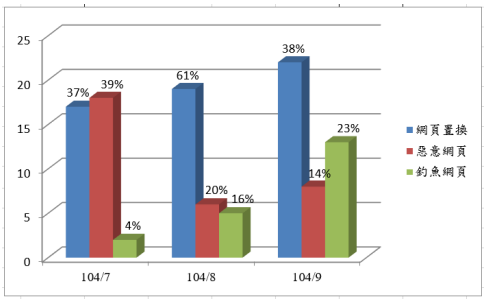


圖 3. 104 年第三季 DEF 子類型前三名比例圖

安全性公告

※ 104/07/13 駭客透過 Hacking Team Flash Zero-Day (CVE-2015-5119)漏洞進行攻擊

※ 104/07/14 微軟 7 月份發佈 15 項安全公告，請儘速更新。

※ 104/07/24 Google Chrome 存在多個弱點，建議請使用者儘速更新！

※ 104/08/11 微軟 8 月份發佈 15 項安全公告，請儘速更新。

※ 104/08/26 Apple Safari 存在系統存取等多個弱點，建議請使用者儘速更新！

※ 104/09/08 微軟 9 月份發佈 12 項安全公告，請儘速更新。

※ 104/09/25 VMware vCenter Server 存在 LDAP 憑證驗證弱點，建請儘速評估更新！

※ 104/09/30 Adobe Shockwave Player 存在系統存取等弱點，建議請使用者儘速更新！

資安事件個案分析-Android智慧型裝置的APP惡意程式分析報告-1

※ **事件簡介：**

一. 六月初收到來自合作的資安團隊轉發 ICST 的智慧型裝置病毒樣本，供本單位進行測試分析。

二. 該惡意程式主要是由國內警政署 165 反詐騙單位所提供，表示該詐騙網址及惡意程式可能已經在國內流竄一段時間。

三. 該惡意程式為副檔名 APK 的安裝檔案，故為作業系統 Android 的手機或平板裝置所設計。

四. 檢測方式透過 Android 模擬器及實體手機進行測試。

※ **事件檢測**

一. 該惡意程式完整檔案名稱為「cht.tw_h_61n11_PhoneContent.apk」，開頭名稱帶有「cht.tw」會誤導使用者認為是某 ISP 業者所開發之 APP。

二. 首先使用 Android 模擬器 Genymotion 開啟 Android 版本為 4.4.4 的裝置，並且設定中選項安全性裡的「不明的來源」啟用，確保程式能被允許安裝。

三. 將惡意程式「cht.tw_h_61n11_PhoneContent.apk」進行安裝並同時進行網路封包側錄，安裝過程中會出現應用程式權限聲明，幾乎完全掌控手機資訊。

四. 安裝完成後在程式集選單中會出現一個小綠人的 APP LOGO，且名稱為「PhoneContent」的應用程式，開啟此 APP 後出現一串文字「已过试用期」及 Button 的功能按鍵(圖 4)。

五. 嘗試點擊 Button 按鍵並無任何反應，此時惡意程式已經成功存取裝置資訊，而使用者藉此才可能發現到已經上當中毒。

六. 然而檢查側錄的網路封包，卻並無發現任何可疑外部流量，故研判此惡意程式可能在模擬器環境中不會作用。

七. 第二次檢測使用實體裝置 Nexus S，且作業系統為 Android 4.1.2，安裝過程中畫面如同先前第一次檢測，實際開啟 APP「PhoneContent」後並檢查側錄的網路封包，得到相同的結果查無異狀。

八. 第三次使用相同實體裝置 Nexus S 檢測，但是有裝入可通話用的 SIM 卡，並檢查側錄的網路封包後發現開始出現可疑的網路流量。惡意程式會將手機資訊加密後，透過 HTTP POST 方式傳送到上層的中國北京中繼站 http://202.108.23.85/app.gif ，如圖 5 所示。

圖 4.

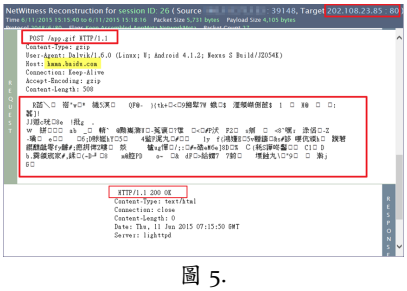


圖 5.

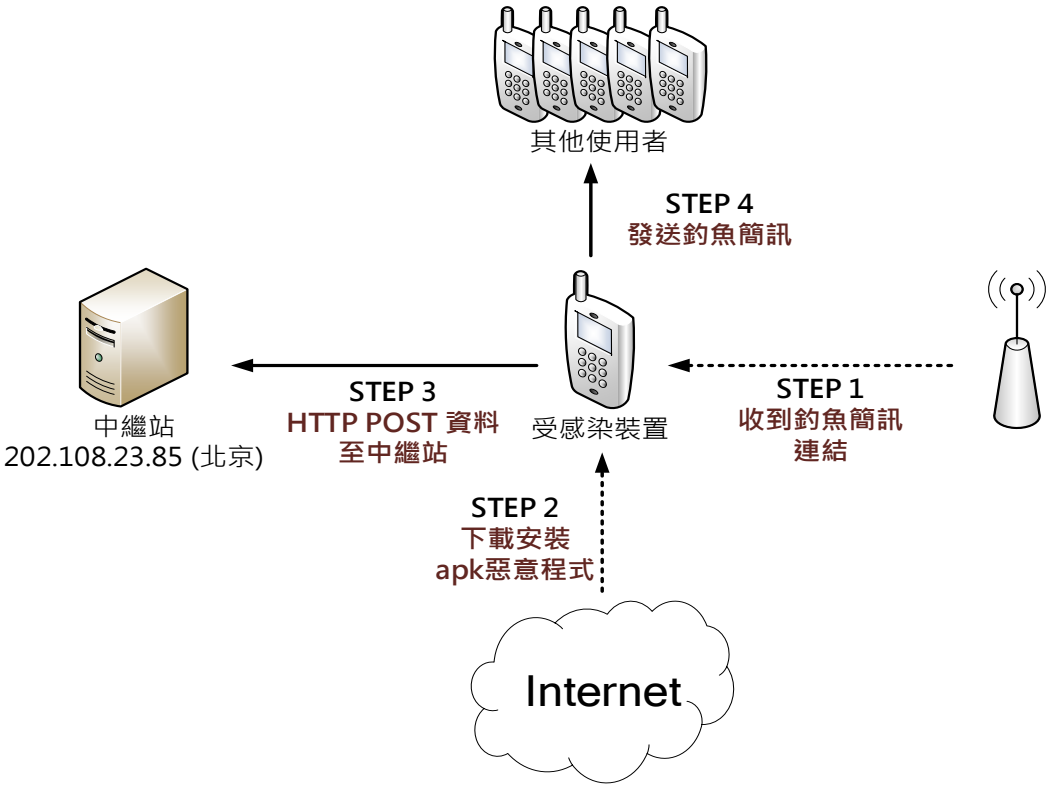
九. 透過圖檔軟體無法正常開啟擷取的 app.gif，故判定此檔案是被加密過後偽裝成 gif 圖形檔。

十. 檢查上層中國北京的中繼站 202.108.23.85 的 port 80，在瀏覽器輸入該位址會出現“HTTP/1.0 500 Internal Server Error”，表示該主機的 port 80 確實是有開啟服務，研判專門接收感染手機的資料所用。

• • •

資安事件個案分析-Android智慧型裝置的APP惡意程式分析報告-2

※ **網路架構圖：**



※ **運作流程**

一. 一般使用者可能收到來自釣魚連結的簡訊。
二. 使用者不小心從連結網站下載到惡意程式。
三. 使用者安裝惡意程式後機敏性資料就被竊取回傳到上層中繼站。
四. 受感染裝置會向其他通訊錄聯絡人發送釣魚簡訊。

※ **建議與總結：**

一. 此事件的惡意程式通常透過手機簡訊方式感染
二. 該病毒會識別感染設備是否有 SIM 卡語音通訊功能，因此模擬器和未插入 SIM 卡的設備不會回傳資料給中繼站。
三. 使用者一旦下載安裝惡意程式後，機敏性資料就會回傳給上層中繼站。
四. 使用者開啟安裝的 APP 後無法正常操作該軟體「PhoneContent」。
五. 感染裝置可能會向通訊錄聯絡人發送釣魚簡訊。
六. 此時就算將 APP 移除，但手機的個資已經被回傳竊取。
七. 因為移除惡意程式 APP 不一定能清除乾淨，建議將系統重置為原始狀態。
八. 建議安裝手機用的防毒軟體，大多病毒都能被偵測阻擋。
九. 手機病毒近年來非常氾濫，故來路不明的檔案不要輕易安裝。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安事件個案分析-綁架勒索電腦檔案的惡意程式事件分析報告-1

※ 前言：

一. 近年來惡意程式越來越多樣化，以往都只是感染主機成為中繼站或殭屍電腦，但另一種的惡意程式卻會破壞使用者的檔案資料，並且勒索使用者相當的金額，造成嚴重損害。

二. 學術網路中的確有部分主機遭受過惡意勒索軟體(ransomware)的侵害，然而往往找不出明確的感染途徑及惡意程式樣本。

三. 受害者往往必須向駭客支付比特幣作為檔案的解密贖金。

四. 本單位取得的惡意程式樣本進行研究分析，主要以 CryptoWall 的惡意勒索軟體測試。

※ 事件檢測

一. 使用 VM 虛擬主機並且為 Windows 7 系統進行隔離環境測試。

二. 惡意程式樣本名稱為 CTBLOCKER.exe，實際執行後原本的惡意程式會開始針對內部文件、影音、圖像檔案進行加密，然後惡意程式主體就會自我刪除。

三. 測試時候將其中一個資料夾內放入一些文件檔，包含了 docx、xlsx、jpg、pdf 四種格式檔案做測試，而惡意程式感染後的確就無法正常再開啟這些檔案。

四. 當所有磁碟內部的關聯檔案都被加密後，在被加密的檔案資料夾中產生四個檔案(圖 7)，主要內容是引導後害者如何進行繳付勒索贖金。

五. 惡意程式執行後會自動開啟 HELP_DECRYPT.HTML 網頁檔案以及 HELP_DERCRYPT.TXT 文字檔案，如圖 8 所示，並其內容都是告知使用者檔案已經被加密，並且要求贖金才能夠取回檔案。

六. 從跳出的訊息得知該惡意程式應為知名的 CryptoWall 3.0，是 Cryptolocker 的改良版本，駭客宣稱文檔的加密技術是使用 RSA-2048 的方式加密，並且必須透過提供的網址去付贖金以取得解密的私鑰，否則無法復原檔案。

七. 嘗試連到顯示的贖金頁面，無法直接透過瀏覽器開啟，因為網址並非正式的網域名稱，無法用一般的 DNS 去解析出來。(圖 9)

八. 必須透過所謂的 Tor 洋蔥瀏覽器去開啟惡意網址「6i3cb6owitcouepv.onion/1figm5j」才能成功，因為該瀏覽器會透過代理伺服器的中繼站 IP 對外連線，所以也無法反向追查到駭客真正的位置。(如圖 10 所示)

九. 透過 Tor Browser 開啟「6i3cb6owitcouepv.onion/1figm5j」後，會先出現輸入圖形驗證碼的程序，才能進入解碼的服務頁面，如圖 11 所示)

圖 6. 透過 Virustotal 線上掃毒，該病毒的檢測比例 41/57 相當高，為 CryptoWall 3.0 的勒索軟體

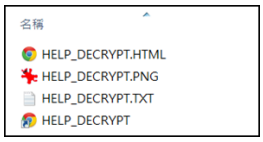


圖 7.

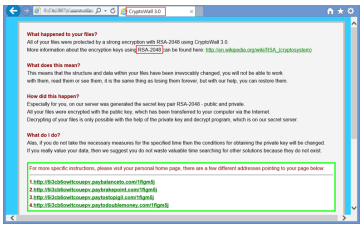


圖 8.

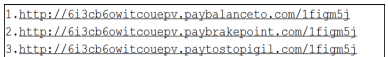


圖 9.

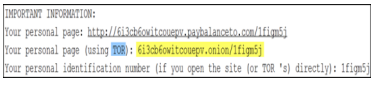


圖 10.

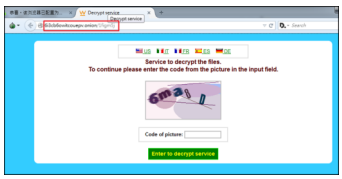
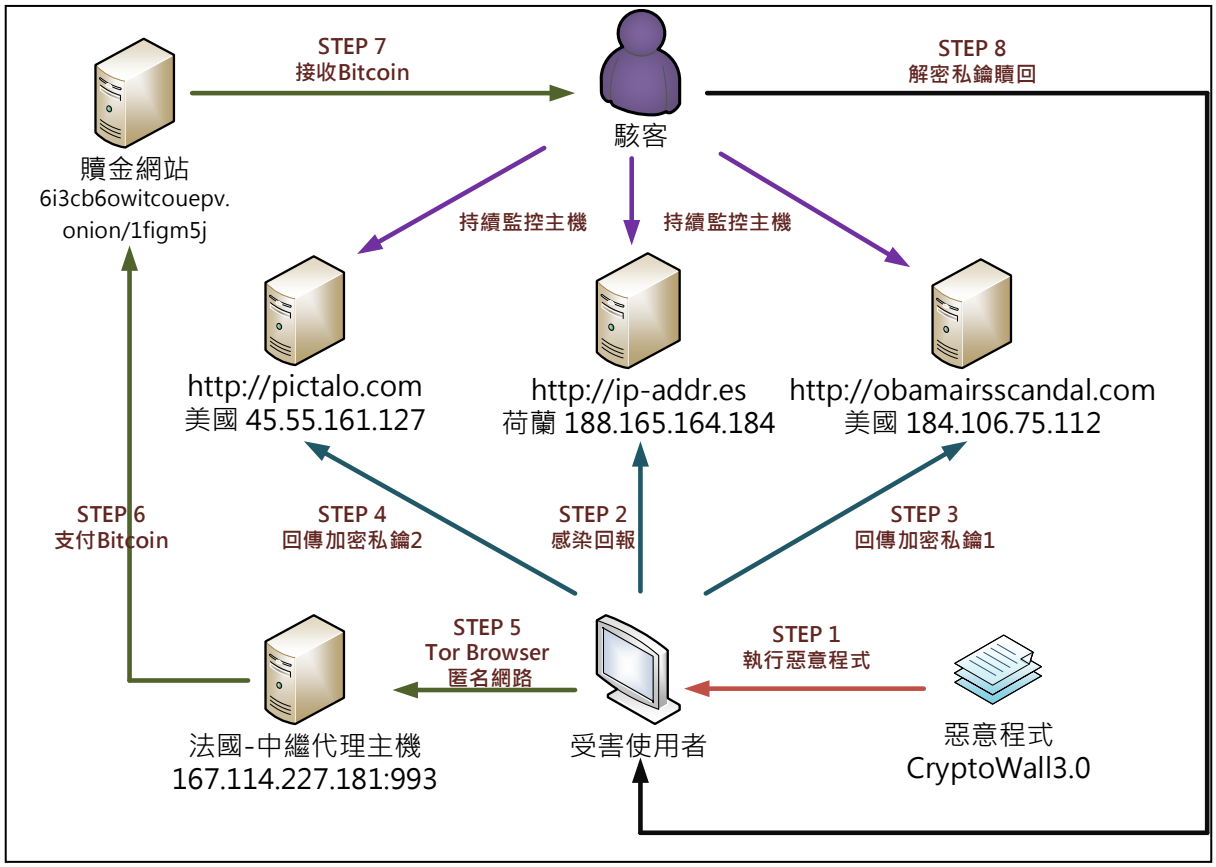


圖 11.

資安事件個案分析-綁架勒索電腦檔案的惡意程式事件分析報告-2

※ **網路行為架構圖**



※ **建議與總結：**

一. 使用者可能透過被 APT 攻擊或網路下載執行到惡意程式而遭受感染。

二. 主機一旦被感染後，惡意程式會開始加密所有磁碟中的文件檔、圖片檔和影音檔案。

三. 惡意程式一旦加密完各類檔案後會自我刪除，不讓使用者取得惡意程式。

四. 惡意程式隨後會跳出網頁和文件資訊，引導受害者如何去支付贖金來取得解密私鑰。

五. CrytoWall 3.0 號稱使用 RSA-2048 加密，因為沒有私鑰基本上是無法救回檔案，建議使用者要**定期備份重要資料避免無法挽回。**

六. 理論上付了贖金給駭客，取得解密私鑰及工具就能解開。然而誰也無法保證能成功救回檔案，可能導致檔案遺失又折損金錢。

七. 建議使用者將系統重新安裝，避免病毒遺留的影響往後可能再次發生。

八. 建議使用者將作業系統更新，並且更新常用套件如 Adobe Flash Player、Adobe Reader、Java 等，這些漏洞都有可能導致感染 Cryptowall 勒索程式。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安新知-DNS 放大攻擊

DNS 放大攻擊(DNS Amplification Attacks) 造成原因為攻擊端偽裝 IP 進行 DNS 查詢，透過回應流量之放大效果造成受害 IP 遭放大流量攻擊，此攻擊多為 DNS 未設定限制造成。

解決方法：

- 設定 ACL 限制遞迴查詢網段
- 關閉遞迴查詢(recursive query)

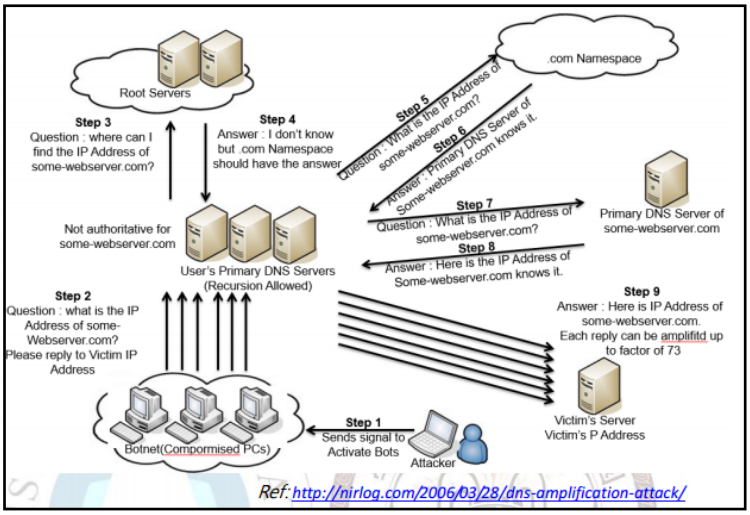


圖 12.DNS 放大攻擊流程圖

參考資料：北區 SOC-DNS amplification attack

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。

TACERT 主要營運項目包含：(1)資安事件的通報應變(2)資安事件的技術支援與諮詢服務(3)資安預警情資(4)資安防護教育訓練

圖 14.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)