TACERT 資安電子季報-第四季

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

- 教育部於 108 年 9 月 16 日至 108 年 10 月 4 日執行「教育部 108 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

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

108/10/8 2019 台灣資安通報應變年會

本季資安事件類型趨勢

教育機構資安通報平台自 108 年 10 月至 12 月，共成立 4,186 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」、「對外攻擊」及「系統被入侵」的子類型比率最高。

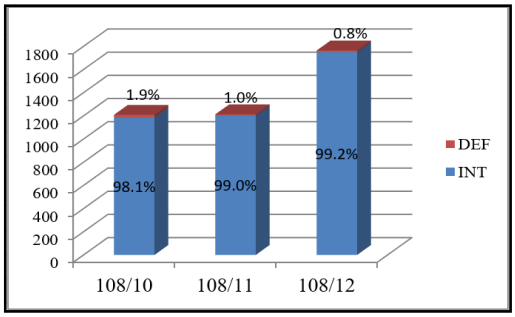


圖 1. 108 年第四季資安事件類型比例圖

DEF 類型(圖 3)以「其他類型網頁攻擊」、「惡意網頁」及「個資外洩」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。

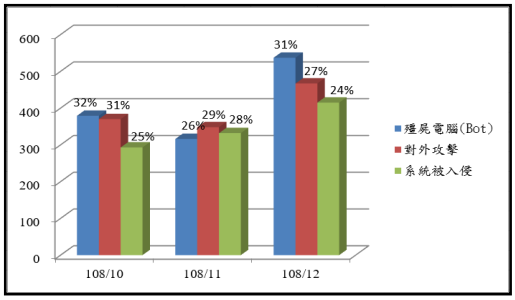


圖 2. 108 年第四季 INT 子類型前三名比例圖

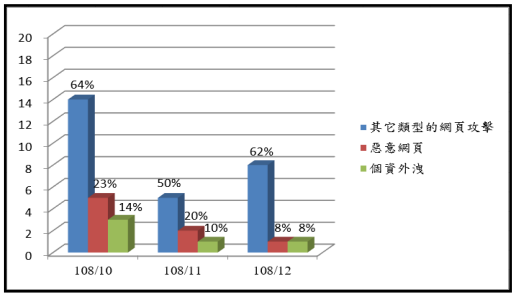


圖 3. 108 年第四季 DEF 子類型前三名比例圖

安全性公告

※ 108/10/03 Exim 存在安全漏洞(CVE-2019-16928)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

※ 108/10/23 惡意 IP 對企業 Office 365 帳號進行暴力破解攻擊，請各單位注意防範！

※ 108/10/30 惡意音源檔案攻擊，請各單位注意防範！

※ 108/11/01 北韓駭客組織 HIDDEN COBRA 所利用的惡意程式 HOPLIGHT，請各單位注意防範！

※ 108/11/06 Lemon Duck PowerShell 加密勒索企業網路！

※ 108/12/26 駭客利用惡意檔案竊取臉書帳號資訊！

資安事件個案分析-假冒寄件者回信之網路釣魚攻擊事件分析報告-1

※ 事件簡介：

本中心於 108/9/27 收到來自 hsxx99@edu.tw 寄件者的回信，信件主旨為「RE:(事件單編號:AISAC-1XXX97)(1 級)事件單結案通知信」，內容以一段英文撰寫，並且包含一個下載連結與 108/7/17 某事件單結案通知信內容。經搜尋，發現此 mail 與某國小的公務信箱類似，且該信的結案通知信也是該國小的資安事件單。為檢測該國小的公務信箱是否有 Auto Reply 功能，本中心在 9/27 以信件主旨:for you 寄測試信，測試後確定該信箱並無自動回信功能，而信箱所有者告知有收到測試信，並且未發現信箱有異常。

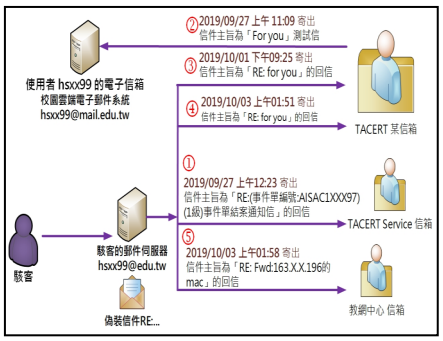


圖 4. 假冒寄件者回信之網路釣魚攻擊事件的發生時間順序

10/1 本中心寄測試信的信箱收到來自 hsxx99@edu.tw 寄件者的回信，而信件主旨為 RE: for you，信件內容為一段英文(含下載連結)與測試信內容。依照收到回信的時間，整理整個事件發生的時間順序如圖 4。為了解這些可疑郵件的攻擊行為與對收信者的危害程度，本中心針對四封來信進行檢測。

※ 事件檢測

1. 首先，使用微軟的 Message Header Analyzer 分析第一封 108/9/27 來信的網際網路標題(如圖 5 所示)，從 Received headers 內容發現該信由 atl4mhob11.registeredsite.com(美國 IP:209.17.115.49)所寄出，非來自寄件者所在地台灣(.tw)，表示寄件者名稱 hsxx99@edu.tw 是偽造的。

圖 5. 使用微軟的 Message Header Analyzer 分析第一封釣魚信

2. 查看信件內容發現一個連結 ATTACHMENT DOCUMENT，點擊後會開啟網址 https://barawey.com/wp-content/uploads/2019/09/link/inv_4790.zip，但是檔案找不到。
3. 檢視第二封 108/10/1 來信的網際網路標題(如圖 6 所示)，從 Received headers 內容發現該信由 qproxy2.mail.unifiedlayer.com (美國 IP:69.89.16.161) 所寄出，非來自寄件者所在地台灣(tw)，表示寄件者名稱 hsxx99@edu.tw 是偽造的。

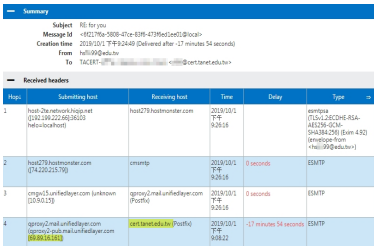


圖 6. 檢視 10/1 的第二封釣魚信

4. 由第二封 108/10/1 來信的內容，發現與第一封來信相同，存在一個連結 ATTACHMENT DOCUMENT，點擊該連結會開啟網址 https://www.petrousorth.com/wp-content/uploads/2019/09/cabl/inv_46394655.zip。接著會下載一個檔名為 RESN4998003289934_396600 的 zip 壓縮檔，解壓縮後會看到一個檔名為 RESN4998003289934_396600.js 的 Jscript 指令檔(如圖 7 所示)。

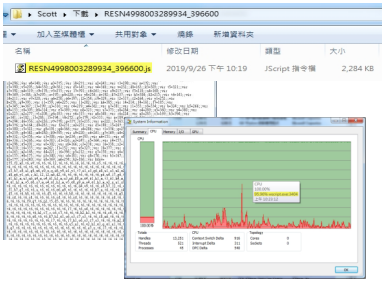
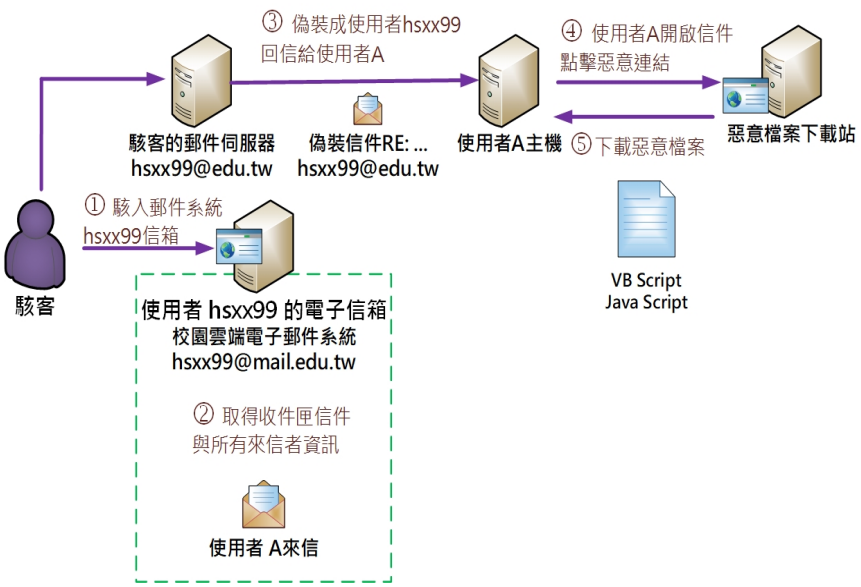


圖 7. 以記事本開啟後會看到一堆變數設定，而當此檔案被讀取時，程式 wscript.exe 的執行會使 CPU 使用率高達 100%

• • •

資安事件個案分析-假冒寄件者回信之網路釣魚攻擊事件分析報告-2

※ 網路架構圖：



(1) 駭客駭入校園雲端電子郵件系統的 hsxx99 信箱。

(2) 駭客取得使用者 hsxx99 信箱內收件匣信件與所有來信者資訊。

(3) 依照收件匣信件內容偽裝成使用者 hsxx99 回信給使用者 A。

(4) 使用者 A 開啟回信後點擊惡意連結 ATTACHMENT DOCUMENT。

(5) 透過惡意連結引導使用者 A 下載惡意檔案至使用者 A 主機內。

※ 建議與總結：

1. 經信箱所有者與信箱管理單位確認公務信箱 hsxx99@mail.edu.tw 的狀態，得知該信箱曾有來自國外 IP 的異常存取紀錄，確認該信箱有被駭現象。
2. 從駭客的攻擊行為得知，本案非一般的隨機釣魚攻擊事件，駭客在取得受駭信箱內所有信件後，以回信方式對所有來信者進行釣魚攻擊，想透過這些人曾經寫過的信件內文來誘騙收到釣魚信的收件者。
3. 從第 2~4 封信件所附連結 ATTACHMENT DOCUMENT 下載至主機的 Java Script 檔與 VB Script 檔執行情形，推測駭客可能在測試如何將惡意程式透過郵件散播到主機內。
4. 針對本類型的釣魚攻擊事件，有下列預防措施提供使用者參考。
   (1) 不隨意開啟不明來源的信件(/附件檔)或點擊不明來源的夾帶連結。
   (2) 定期更換電子郵件信箱的登入密碼，並加強密碼強度。
   (3) 若收到可疑的信件內容，建議親自與寄件者確認信件內容的正確性。
   (4) 定期進行防毒軟體的病毒碼更新，確保主機能第一時間阻擋病毒攻擊。
   (5) 定期進行電子郵件信箱的重要信件備份。
   (6) 定期進行電腦主機資料備份。

*詳細完整個案分析報告，請參閱 TACERT 網站！

資安事件個案分析-勒索病毒 GlobeImposter 攻擊事件分析報告-1

※ **前言：**

1. 2019/8/29 全台醫療機構陸續傳出電腦主機遭受勒索病毒攻擊，至 2019/9/1 共有 22 家醫院受害。駭客將中毒電腦作為跳板，利用密碼管理與 RDP 漏洞竄入衛福部電子病歷交換系統(EEC)專屬 EEC Gateway VPN 網路，並開始擴散病毒。由於 EEC 所用 VPN 網路為各大醫院自主管理與共用之內部網路，並未分割 VLAN，造成該勒索病毒得以急速擴散。

2. 本事件爆發之勒索病毒為 GlobeImposter「十二主神」2.0 版本，主要的攻擊程式為 Apollon865.exe，它會通過社交工程或 BlueKeep RDP 漏洞進行擴散，為了解 Apollon865.exe 的攻擊行為與對受害者的危害程度，本中心對病毒樣本進行檢測。

※ **事件檢測**

1. 使用一台具有網路磁碟與 32 位元 Windows 7 作業系統的虛擬主機，將惡意程式 Apollon865.exe 於該主機上執行，執行後桌面會出現被勒索通知信覆蓋的黑色畫面(如圖 8)，無法看到任何可以點選開啟程式或資料夾的路徑。

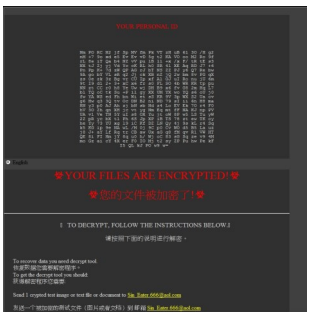


圖 8. 被勒索通知信覆蓋的黑色畫面

2. 在 Apollon865.exe 執行一段時間後會在原資料夾中消失，只剩下 HOW TO BACK YOUR FILES.exe 與 ids.txt 兩個檔案。

3. 執行 HOW TO BACK YOUR FILES.exe 後，發現其開啟勒索通知信，而以執行檔作為勒索通知信的方式與一般以文字檔當勒索通知信有很大的差別，因為文字檔很容易被關閉，而執行檔的方式若遇無資訊能力的使用者，可能無法將它關閉，容易造成使用者的恐慌。檢視勒索通知信的內容，可分為三個部分:YOUR PERSONAL ID、YOUR FILES ARE ENCRYPTED! 與 MOST IMPORTANT!!!。

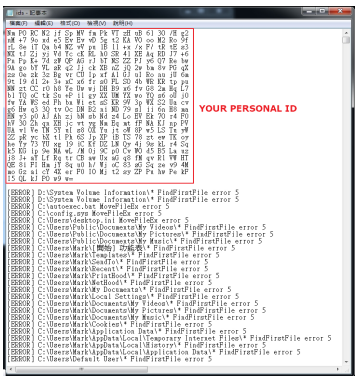


圖 9. ids.txt 內容

4. 檢視 ids.txt 內容，發現內容為 YOUR PERSONAL ID 與執行程式時產生錯誤的紀錄，推測該勒索病毒似乎處於調試階段，故病毒加密後會在同目錄下釋放一個 ids.txt，用於存放 ID 和列印錯誤信息。

5. 檢視主機內檔案被加密情形，除了 C:\windows 與 C:\Program Files 兩個資料夾內檔案沒有被加密外，主機內的檔案都被加密了，被加密的檔案都會延伸出一個副檔名 Apollon865。

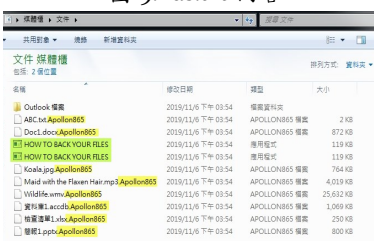
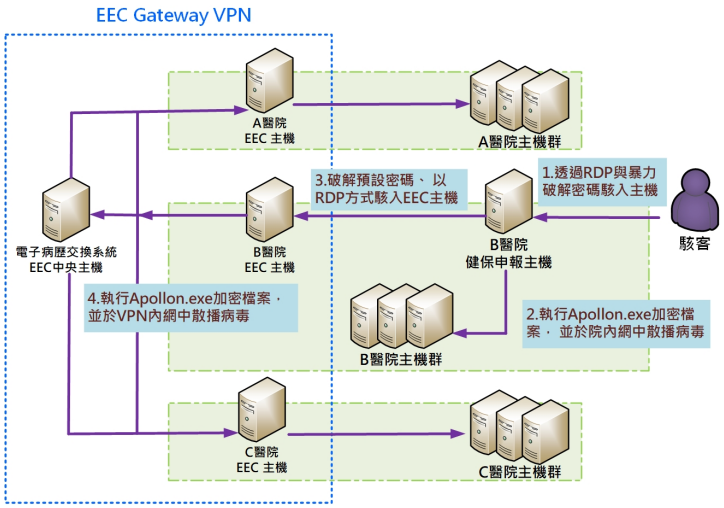


圖 10 而且在每個被勒索病毒拜訪過的資料夾，則會放入勒索通知信 HOW TO BACK YOUR FILES.exe

• • •

資安事件個案分析-勒索病毒 GlobeImposter 攻擊事件分析報告-2

※ 事件攻擊行為示意圖



(1) 駭客透過遠端桌面連線(RDP)與暴力攻擊破解密碼，駭入某醫院健保申報主機。

(2) 駭客執行勒索軟體 Apollon.exe 來加密檔案，並且於醫院內部網路中散播病毒。

(3) 駭客破解該醫院所屬 EEC 主機預設密碼，並以 RDP 方式駭入 EEC 主機。

(4) 駭客執行 Apollon.exe 來加密檔案，並且於 VPN 內網中散播病毒。

※ 建議與總結：

1. 本事件發生主要因為 RDP 漏洞與密碼被破解造成，駭客以受害主機為跳板，進而攻擊醫院內部網路與 EEC Gateway VPN 網路。

2. 勒索軟體 GlobeImposter 最早被發現是在 2017 年 3 月，在 2018 年該病毒於中國大陸各醫療機構中流竄，造成不少損失。本事件受害主機所感染的 GlobeImposter 是 2.0 版本，有別於 1.0 版，新增了對於勒索通知信 HOW TO BACK YOUR FILES.exe 的中文敘述。

3. 勒索軟體 GlobeImposter 在執行後會呼叫 cmd.exe 來執行一些指令，它會刪除影子副本、啟動 Browser、關閉一些資料庫服務、刪除所有事件日誌與變更遠端桌面連線服務的設定，最後會刪除自己本身。

4. 由該事件可以發現許多現有醫院存在的資安問題，詳述如下。

   (1)醫院各主機容易存在弱密碼問題。(2)醫院對於主機的維護依賴委外廠商居多，容易造成主機管理的遠端連線問題。(3)醫院對於內部網路的防護措施比外部網路還薄弱。(4)健保所使用的 EEC gateway VPN 因未切割 VLAN，容易形成所有 EEC 主機都處於同一網路。因此，當一台主機感染病毒，則其他主機也會感染病毒。

5. 針對 GlobeImposter 勒索病毒的攻擊，有下列預防措施提供使用者參考。

   (1)定時更新電腦主機之系統與相關程式，並且修復漏洞。(2)對於主機的管理，定期更改帳戶密碼，並設置強密碼，避免使用統一的密碼。(3)定期備份重要資料於其他備援裝置中。(4)不要隨意開啟或點擊不明來源的郵件(或副檔)。(5)不要從不明來源的網站下載軟體或檔案。(6)關閉非必要的文件共享權限。(7)關閉非必要業務的 RDP 連線。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安新知-2019 年精進的網路釣魚手法簡介

資料來源： ZDNet

微軟於 2019 年 12 月發布了一份關於病毒與網路安全趨勢的報告。報告中指出，在幾個重要的趨勢中，網路釣魚是近兩年中少數幾個逐漸增加的攻擊手法並分析 2019 年度看到比較精明的三種網路釣魚攻擊手法。

1、劫持查詢結果

這是一個多層次的病毒攻擊，犯罪組織透過竄改 Google 搜尋結果來達到目的。網路釣魚攻擊流程如下：

(1) 駭客將正當網站的流量導向他們控制的網站。
(2) 網址成為某個特定關鍵字的 Google 搜尋結果的最佳搜尋結果。
(3) 駭客寄一封含有那個特定關鍵字的 Google 搜尋結果的電子郵件給受害者。
(4) 如果受害者點開連結並點開了最佳搜尋結果，他們將會被導向一個被攻擊者控制的網站。
(5) 這個網站接著會將受害者重新導向網路釣魚頁面。

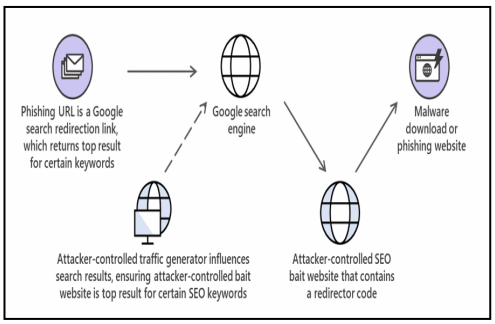


圖 11. 劫持查詢結果的攻擊流程圖(圖片來源：微軟)

2、濫用 404 錯誤頁面

當大部分的釣魚信都有一個駭客想要引誘使用者連上的釣魚網址，但此攻擊手法卻是包含了指向不存在的頁面的連結。當微軟的安全系統掃描這個頁面時，他們會得到一個 404 錯誤(因為這個連結並不存在)，微軟就會將這個連結視為安全的連結。但是當一個真正的使用者造訪這個網址時，釣魚網站會偵測到使用者並且重新導向他們至真正的釣魚頁面而不是伺服器的 404 錯誤頁面。

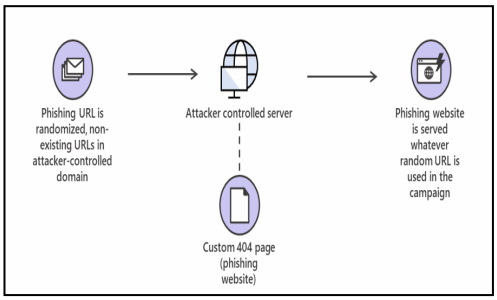


圖 12. 濫用 404 錯誤頁面的攻擊流程圖(圖片來源：微軟)

3、中間人釣魚

第三個釣魚手法是一個使用中間人(Man-in-the-middle，縮寫 MitM)伺服器的技術。駭客不從正當的網站中複製一小部分並製作出一個粗淺的模仿品，而是從微軟的網站獲取公司的資訊，例如：標誌、標題、文字、以及背景圖片，創造一個和正常網站一模一樣的登入頁面，大幅降低了使用者的疑心。但是，中間人攻擊並不是完美的，因為釣魚網站的網址還是會顯示出來，就像其他釣魚網站一樣，不過，這也代表使用者可以透過仔細觀察網址來避免受害。

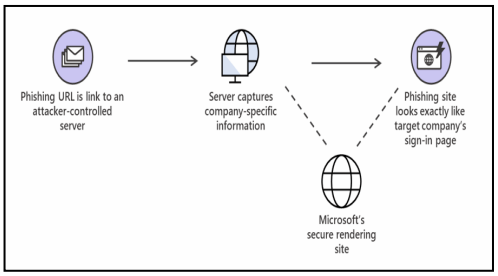


圖 13. 中間人釣魚的攻擊流程圖(圖片來源：微軟)