TACERT 資安電子季報-第三季

目錄：

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(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。

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 7 月至 9 月，共成立 3,740 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。

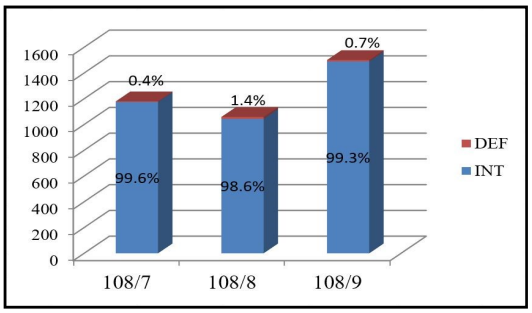


圖 1. 108 年第三季資安事件類型比例圖

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。

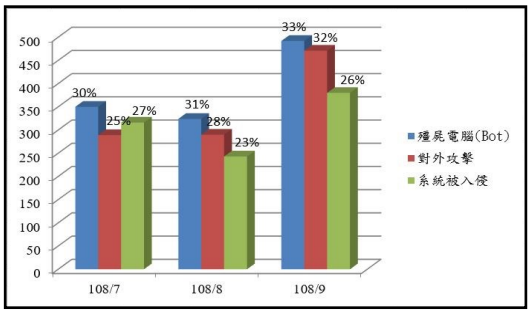


圖 2. 108 年第三季 INT 子類型前三名比例圖

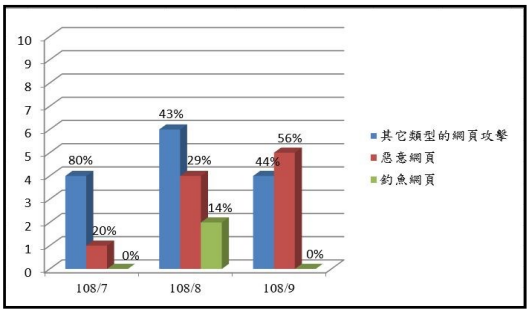


圖 3. 108 年第三季 DEF 子類型前三名比例圖

安全性公告

※ 108/08/29 Pulse Connect Secure 產品存在安全漏洞(CVE-2019-11510、CVE-2019-11539)，允許未經授權使用者取得帳號與密碼，請儘速確認並進行更新！

※ 108/09/11 Exim 存在安全漏洞(CVE-2019-15846)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

※ 108/09/11 北韓駭客組織 HIDDEN COBRA 利用惡意程式 BADCALL 運用知名網站憑證進行 fake TLS 連線，以及利用惡意程式 ELECTRICFISH 建立隱密通道進行通訊，請各單位注意防範！

※ 108/09/24 微軟 Internet Explorer 與 Windows Defender 存在安全漏洞(CVE-2019-1367 與 CVE-2019-1255)，允許攻擊者遠端執行任意程式碼與阻斷服務，請儘速確認並進行更新

資安事件個案分析-網路釣魚攻擊事件分析報告-1

※ 事件簡介：

2019/6/25 本中心收到一封來自某知名大學的信件，主旨為「要求報價(XX 大學)UNI894/BU463」，為了解該信件之攻擊行為與對收件者之危害程度，本中心進行信件檢測。

※ 事件檢測

1. 首先，查看信件內容(如圖 4 所示)，信件內容提到這是來自某大學的問候，在某教授的指導下，請收件者在 2019 年 6 月 27 日當天或之前提供 2019 年預算的報價。在信件中有一個名為「要求報價 25-06-2019-pdf」的 zip 壓縮檔，該信件是以國內某知名大學的名義發出，若收件者為其常聯絡的廠商或其他業界公司，則收信者會點開此信件並開啟附件的可能性將大大增加。
2. 使用微軟的 Message Header Analyzer 分析信件的網際網路標題(如圖 5)，從 Received headers 發現該信件由 cvps10523477067.hostwindsdns.com(美國 IP:104.168.171.157)所寄出，非來自寄件者所在地台灣(.tw)，表示寄件者名稱是偽造的。
3. 在其他 Header 資訊方面，發現若收信者回信則會回覆至 41e7e96794e44c007edebc97801881aa@batono.ge 的信箱，而該信箱為 References 的五個參考信箱之一，而從 References 發現這些信箱都是來自俄羅斯(ru)與喬治亞(ge)。本信件的 Message-ID 為 7f8b935baa66618911d956af5439fe95@某知名大學英文縮寫.edu.tw，偽裝為某知名大學所發出的信件，而且該信件的重要性設定為最優先，吸引收信者開啟信件。
4. 將信件的附件「要求報價 25-06-2019.pdf.zip」解壓縮(圖 6)，發現解壓縮後原以為是 pdf 檔的檔案變成執行檔，若檢視時未設定視窗秀出副檔名，則使用者會以為是 pdf 檔而開啟它，這是一個常見的引誘使用者上當的小技巧。
5. 在執行「要求報價 25-06-2019.pdf.exe」後，發現該檔案在原所屬位置的資料夾內消失。檢視背景程式運作情形，發現該程式在執行後產生一個與自己相同名稱的程式來持續執行著，而且兩者的程式路徑相同，存在原所屬位置的資料夾內，但是查看資料夾卻無任何檔案存在。
6. 當「要求報價 25-06-2019.pdf.exe」執行時，整個受害主機的記憶體使用率逐漸升高，佔用大多數的記憶體用量(圖 7)，最後系統會出現記憶體即將用盡的警訊。

圖 4.釣魚信件內容

圖 5.信件的網際網路標題

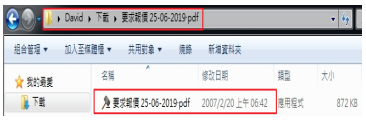


圖 6.檢視該執行檔的檔案內容，發現該檔案是在 2007/2/20 6:42 建立的，但是存取日期卻是 1601/1/1 8:57，推測這些時間可能不是準確的，而在詳細資料內則寫明產品名稱為 GravisDextrosazone8，原始檔名為 GravisSCURRIED.exe

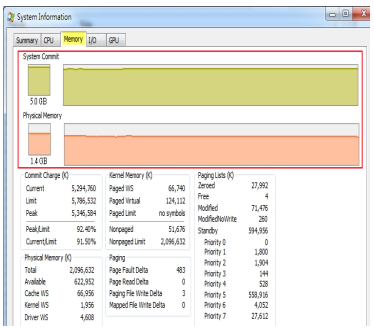
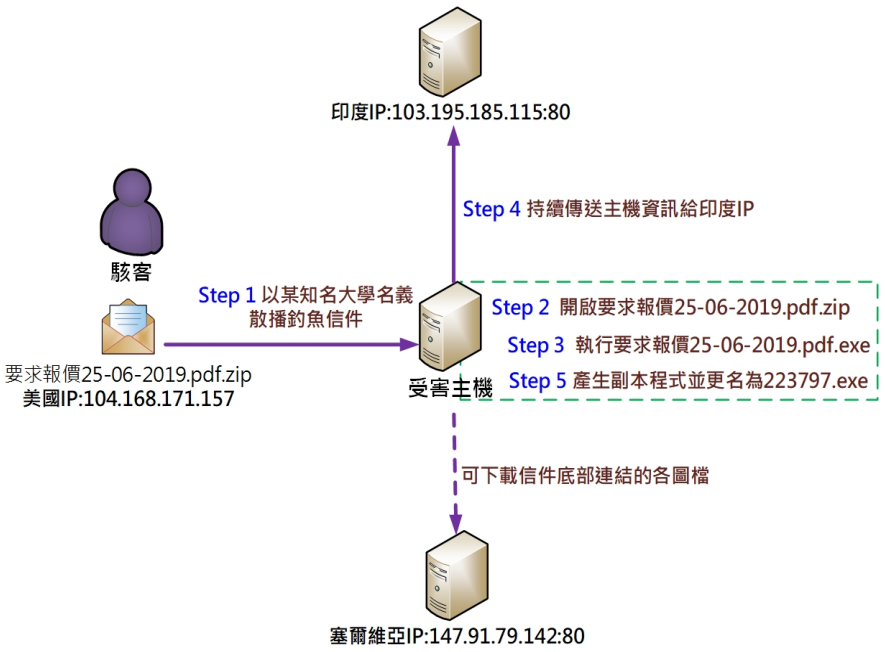


圖 7.受害主機的記憶體使用率逐漸升高

資安事件個案分析-網路釣魚攻擊事件分析報告-2

※ **網路架構圖：**



1) 駭客以國內某知名大學名義散播釣魚信件。
2) 收件者收信後解壓縮附件「要求報價 25-06-2019.pdf.zip」,並開啟它。
3) 收件者的主機開始執行「要求報價 25-06-2019.pdf.exe」。
4) 「要求報價 25-06-2019.pdf.exe」執行後，主機會持續傳送主機資訊給印度 IP:103.195.185.115:80。
5) 「要求報價 25-06-2019.pdf.exe」產生一個副本程式並更名為 223797.exe，來代替自己執行。

※ **建議與總結：**

1. 本個案的攻擊手法為駭客以知名大學名義寄發網路釣魚的信件，企圖騙取收信者的信任，而附件的壓縮檔「要求報價 25-06-2019.pdf.zip」解開後使用者看到的是含.PDF 的中文檔名，更容易降低收件者的警戒心。
2. 「要求報價 25-06-2019.pdf.exe」執行後產生副本並更名為 223797.exe，但使用 Process 偵測工具查看「要求報價 25-06-2019.pdf.exe」的存放路徑，無法看到它對應到 223797.exe。因 223797.exe 本身為隱藏檔，又存放位置為 C:\系統使用者的隱藏資料夾，因此，使用者發現它的機率便大大降低。
3. 從信件的內容發現該信件有塞爾維亞的連結在信件底部，卻以中文撰寫信件內容與以中文命名附件檔案，推測駭客可能以某信件範本來進行修改，而本身對於中文與台灣的大學環境有一定程度的了解。
4. 對於本個案的攻擊手法有下列幾點建議措施，提供參考。
   (1) 不要隨意開啟不明來源的信件或信件附檔。
   (2) 定期更新防毒軟體的病毒碼，以利即時阻擋惡意程式的攻擊。
   (3) 可疑的信件如需開啟，建議於虛擬機或其它備用主機上開啟較佳。
   (4) 定期備份主機資料。

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 GoGaLocker 攻擊事件分析報告-1

※ **前言：**

1. 知名資安公司賽門鐵克在 2019 年 7 月所發佈的「TARGETED RANSOMWARE: An ISTR Special Report」報告指出，GoGalocker 是 2019 年 1 月出現的一種新的目標式勒索軟體威脅，而從 2017 年 1 月至 2019 年 5 月受目標式勒索軟體家族攻擊影響的組織數量圖可以看到，GoGalocker 在 2019 年 2 月開始有攻擊行為。

2. 為了解 GoGaLocker 之攻擊行為與危害程度，本中心取得樣本後進行檢測。

※ **事件檢測**

1. 首先，使用一台有 Windows 7 32 位元作業系統的虛擬主機，並且將 GoGaLocker 樣本 65d5dd067.exe 放於該主機內。

2. 在執行前檢視 65d5dd067.exe 的內容，發現該程式的數位簽章是由 ALISA LTD 所簽署(圖 8)，推測此為駭客用合法的憑證對其勒索軟體進行數位簽章的隱藏手法，藉此避免惡意程式被發現。

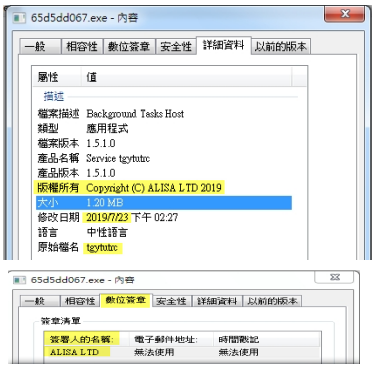


圖 8. 該程式的數位簽章是由 ALISA LTD 所簽署

3. 65d5dd067.exe 經 Virustotal 檢測，其惡意比例為 59/68，而且有多家防毒軟體公司以 Lockergoga 命名它。

4. 執行 65d5dd067.exe 後，發現該程式在其所在之位置原地消失，但在 C:\使用者\Ruby\AppData\Local\Temp 資料夾內會發現另一個與它相同的程式 tgytutrc[4 位亂數].exe(如 tgytutrc1471.exe)(圖 9)，而且在 Temp 資料夾內也會產生一個 tgytutrc[4 位亂數].exe.cmd(如 tgytutrc1471.exe.cmd)的 Windows 命令指令碼。

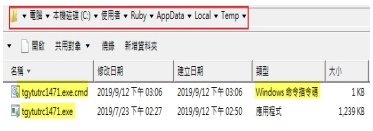


圖 9. Temp 資料夾

5. 在執行 65d5dd067.exe 後，主機陸續出現檔案被加密的狀態(如圖 10 所示)，而且被加密的檔案皆會延伸出一個.locked 的副檔名。除了將檔案加密外，該程式也會將視窗設定的背景顏色全部改為淺灰色，而在桌面左下角的工作列圖示也變成白色。在加密後查看主機檔案被加密情形，發現除了 C:\windows 資料夾內的檔案與 txt 文字檔沒被加密外，主機內的檔案都被加密。

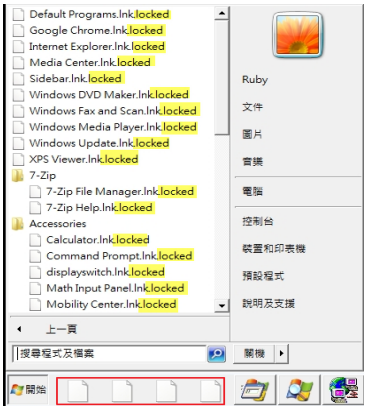
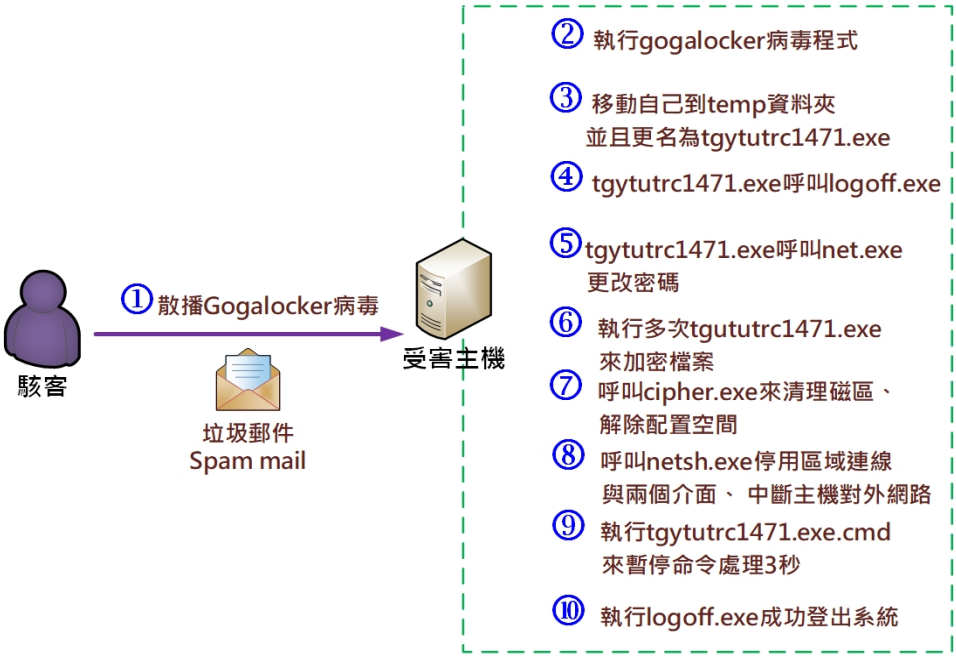


圖 10 主機陸續出現檔案被加密的狀態

6. 65d5dd067.exe 對主機內檔案進行加密後，在主機公用桌面會出現一個 README_LOCKED.txt 的勒索通知信。

資安事件個案分析-勒索病毒 GoGaLocker 攻擊事件分析報告-2

※ **網路行為架構圖**



※ **建議與總結：**

1. 勒索病毒 Gogalocker 在執行後會在原地消失，並且在使用者的隱藏資料夾 AppData\local\Temp 內出現，一般使用者無法輕易地發現它的存在，此手法類似無檔案式的勒索病毒。
2. Gogalocker 病毒使用 ALISA LTD 所簽署的數位簽章來偽裝自己是一個合法的程式，藉此規避防毒軟體的偵測。
3. 除了 C:\windows 內的檔案與 txt 文字檔外，該病毒會將主機內的檔案都加密，並且將主機的視窗背景顏色變更為淺灰色。
4. 它與以往的勒索病毒不同，它會更改具有系統管理者權限的使用者之密碼，而且該病毒執行一段時間後會登出系統，導致受害者無法登入系統。
5. Gogalocker 病毒在加密作業完成、登出系統之前，會停用主機的網卡，關閉主機的區域網路連線功能，讓主機完全無法連網。
6. 受害者因為密碼被更改而無法登入系統，將導致無法查看勒索通知信的內容，推測使用者與駭客取得聯繫的機會很低，也可得知此病毒對受害主機的破壞程度很大，推測駭客的主要目的可能不是勒索金錢。

詳細完整個案分析報告，請參閱 TACERT 網站！

資安新知-挖礦型殭屍網路利用 ADB 漏洞入侵並透過 SSH 傳播

資料來源： TREND MICRO

趨勢科技觀察到一種新的挖礦殭屍網路，它通過開放的 ADB (Android Debug Bridge)埠入侵，並且透過 SSH 進行傳播。這種攻擊利用了開放的 ADB 埠的方式 在預設情況下不具有身份驗證，類似於之前報導的 Satori 殭屍網路變種。這個 bot 的設計允許它從受感染的主機傳播到任何之前與主機有過 SSH 連接的系統。

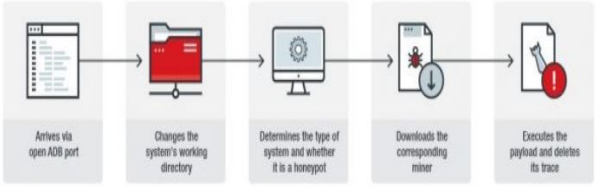


圖 11. 攻擊的感染鏈（圖片來源：TREND MICRO)

儘管 ADB 對於管理員和開發人員來說是一個有用的特性，但重要的是使用 ADB 可能會將設備和與之連接的設備帶來威脅。使用者也可以採用其他最佳實踐來防範非法的挖礦行動和殭屍網路，例如：

- 在必要時檢查和更改預設，以提高安全性
- 更新設韌體並應用可用的補丁
- 瞭解攻擊者用來傳播這些類型惡意軟體的方法，並對其進行針對性防禦

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(5)資安通報演練(6)資安電子季報。

圖 12 .TACERT 網站

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)