



TWCERT/CC 資安情資電子報

2018 年 7 月份

目錄

第 1 章、 摘要	1
第 2 章、 TWCERT/CC 近期動態.....	2
2.1、 參與 FIRST Annual Conference 2018.....	2
2.2、 參與 TiEA 資安講座-資安防禦最前線	3
2.3、 參與 The Honeynet Project Annual Workshop 2018	3
2.4、 協辦 2018 國際資訊安全組織台灣高峰會	4
2.5、 預計參展 HITCON Community 2018 研討會	5
第 3 章、 國內外重要資安新聞	6
3.1、 國內外資安政策、威脅與趨勢	6
3.1.1、 國家通訊傳播委員會與經濟部舉辦「物聯網資安標準認證制度 公開說明會」	6
3.1.2、 歐盟聲稱卡巴斯基實驗室軟體「確認為惡意」	6
3.2、 駭客攻擊事件及手法	7
3.2.1、 售票服務 Ticketfly 遭網頁置換，駭客竊取客戶與員工資料庫....	7
3.2.2、 美國 DHS 與 FBI 公布北韓駭客組織 HIDDEN COBRA 所利用的 惡意程式 Joanap 及 Brambul，請大家注意防範(轉行政院技服中心資訊)	9
3.2.3、 智利銀行 SWIFT 系統遭駭，近千萬美元失竊.....	11
3.2.4、 歐洲電子零售商 Dixons Carphone 遭駭客攻擊，10 萬筆用戶信 用卡資料外洩.....	13
3.2.5、 Trik 垃圾郵件殭屍網路洩漏 4300 萬有效電郵地址.....	14
3.2.6、 航班追蹤服務 Flightradar24 遭受資料洩露，用戶儘速更改密碼	16
3.2.7、 Necurs 殭屍網路的 CSE 惡意軟體 ZLab-Ursnif 銀行木馬新變	

種襲擊義大利公司	18
3.2.8、 訂房系統 FastBooking 資料遭竊，上百家已知飯店受到影響 ..	19
3.2.9、 上億造訪人次之票務服務 Ticketmaster 系統之套件遭駭	21
3.2.10、 Gentoo Linux 的 Github 帳號遭駭，內容可能遭惡意竄改 ..	23
3.3、 軟硬體漏洞資訊	24
3.3.1、 區塊鏈平台 EOS 新漏洞，有遭探勘接管之虞	24
3.3.2、 硬碟感震設計成破綻，聲波攻擊能促發 DoS	25
3.3.3、 鎖定 Blue Coat 安全閘道 ASG & ProxySG 瑕疵，駭客硬闖 SAML 認證	26
3.3.4、 威聯通升級 Proxy Server，消彌 CSRF 等 4 項弱點	27
3.3.5、 今年第二波 Flash Player 0-Day 攻擊，瞄準中東 Office 用戶 ..	28
3.3.6、 三項漏洞曝光，令 Foscam IP Camera 無法承受連鎖攻擊	29
3.3.7、 高階腳本語言 Perl 測出 directory traversal 破綻，面臨檔案覆蓋 風險	30
3.3.8、 Intel CPU 再爆預測執行式旁道分析威脅 — Lazy FP state restore	31
3.3.9、 佳能 6 款印表機測出管理者認證 bypass 缺失	32
3.3.10、 更新加密工具 GnuPG，阻止偽造簽章事件	33
3.3.11、 零號字 ZeroFont 釣魚術等待全球 Office 365 用戶上鉤	34
3.3.12、 Splunk 企業版權限控管失誤，將暴露系統資訊	35
3.3.13、 iOS 瑕疵忽略密碼錯誤上限，令暴力破解攻陷 iPhone	36
3.3.14、 硬體漏洞 RAMpage 衝擊 6 年內生產 Android 設備	37
3.4、 資安研討會及活動	38
第 4 章、 2018 年 06 月份事件通報統計	48

第 1 章、摘要

為提升我國民眾資安意識，TWCERT/CC 於每月發布資安情資電子報，統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、威脅與趨勢、駭客攻擊事件、軟硬體漏洞、資安研討會活動及資安事件通報統計分析等資訊。

第 2 章、TWCERT/CC 近期動態

2.1、參與 FIRST Annual Conference 2018

TWCERT/CC 於 6 月 24 日至 29 日前往馬來西亞吉隆坡，參與資安事件應變小組論壇 (Forum of Incident Response and Security Teams, FIRST) 2018 年會，於會中參與各項議程及會員大會，與各國 CERT、CSIRT、PSIRT 資安專家進行交流，探討國際資安政策、威脅及趨勢，增進與各國組織之熟稔程度，並參與惡意鑑識、逆向工程、情資分享平台實作等教育訓練，並參與網路奪旗競賽 (Capture the flag, CTF)，另因 TWCERT/CC 為亞太區電腦緊急事件回應小組 (Asia Pacific Computer Emergency Response Team, APCERT) 會員，因此於會中參加 APCERT 成員午餐會談，了解亞太地區各國 CERT/CSIRT 最新動態。

TWCERT/CC 於今年擔任 FIRST 會員推薦人，協助我國群暉科技之 PSIRT 成為 FIRST 會員，並輔導其熟悉 FIRST 中各項活動及事務，以利群暉科技能於國際資安組織中取得更多資訊，有效增進我國廠商之資安能量，後續亦將持續協助國內有意加入 FIRST 之組織，除使我國於 FIRST 會議中有更多代表席次及發言權，提升我國於國際資安組織之能見度，並可達到國際資安聯防之效益。



2.2、參與 TiEA 資安講座-資安防禦最前線

6 月 27 日台灣網路暨電子商務產業發展協會 (TiEA) 於 AppWorks Open Space 舉辦一場 TiEA 資安講座-資安防禦最前線，此次 TWCERT/CC 分析師沈紀威出席會議擔任講師，講題為「資安聯防新思維-民間企業資安通報面面觀」，針對企業內部如何自主建立 CSIRT 團隊，並逐步建立起資安聯合防禦體系進行相關分享。



2.3、參與 The Honeynet Project Annual Workshop 2018

7 月 9 日至 10 日 The Honeynet Project Taiwan Chapter 於集思台大會議中心舉辦 THE Honeynet Project Annual Workshop 2018。Honeynet Project 是一個致力於提升網路安全性的國際非營利研究機構，過去 17 年來，已經開發了許多開源工具，並發布與網路攻擊相關的網路安全研究。

今年的會議重點將會放在網路詐欺、Honeypot、機器學習、工業控制系統與物聯網等相關安全議題，此次 TWCERT/CC 分析師羅文翎亦於會中分享「Development of Honeynet Projects in APCER」講題，針對 APCERT 內部實行的 Honeynet 相關專案進行介紹。



2.4、協辦 2018 國際資訊安全組織台灣高峰會

7 月 11 日至 12 日雲端安全聯盟(Cloud Security Alliance) 、The HoneyNet Project 台灣分會及 OWASP 台灣分會於集思台大會議中心舉辦 2018 國際資訊安全組織台灣高峰會，會議上將呈現國際資訊安全組織最新研究成果，有來自國內外的專業講師帶來的精彩分享，提供與會人員掌握全球資訊安全發展脈動與趨勢，會議內容涵蓋雲端服務安全、誘捕資安技術、網站應用程式安全、事件掌握與應變等議題，可接軌國際資安社群並有助於掌握全球發展趨勢。

TWCERT/CC 亦於此次會議設立攤位進行 TWCERT/CC 業務及資安意識推廣，此外，於 7 月 12 日 TWCERT/CC 分析師羅文翎於會中分享講題「個資外洩一瞬間」，介紹 TWCERT/CC 如何協助個資外洩的電商業者解決問題，透過鑑識實例，以及防護做法進一步說明，以免資安事件重蹈覆轍。



2.5、預計參展 HITCON Community 2018 研討會

7 月 27 日至 28 日 HITCON 將於台北南港展覽館一館 5 樓舉辦 HITCON Community 2018 研討會，此次會議是第一場台灣導入數位貨幣的會議，會眾將可輕鬆使用數位錢包及 HITCON Token 來交易及兌換週邊商品，亦規劃區塊鏈遊戲，讓與會者可從中更了解區塊鏈及數位貨幣。另一個有趣的活動為 HITCON Hackdoor，以一種新型態的密室逃脫形式，結合解謎、教學和競賽，由淺入深地帶領大家學習和挑戰生活中各種物聯網裝置，如 IP CAM、WIFI、印表機、門禁系統或任何資安系統可能存在的資安問題。

TWCERT/CC 將於此次會議設立攤位進行 TWCERT/CC 業務及資安意識推廣，和以往不同的是，TWCERT/CC 攤位特別規劃「挖掘受駭 IP CAM，通報 TWCERT/CC」活動，會眾通報內容經 TWCERT/CC 審核通過後，即有機會獲得 HITCON Token。

第 3 章、國內外重要資安新聞

3.1、國內外資安政策、威脅與趨勢

3.1.1、國家通訊傳播委員會與經濟部舉辦「物聯網資安標準認證制度公開說明會」

國家通訊傳播委員會與經濟部於 6 月 11 日假台大醫院國際會議中心舉辦「物聯網資安標準認證制度公開說明會」，公布物聯網設備資安認證標章制度及未來政策推動方向。



資料來源：

https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=78782

3.1.2、歐盟聲稱卡巴斯基實驗室軟體「確認為惡意」

反卡巴斯基實驗室的言論在歐洲繼續升溫，歐洲議會通過動議將莫斯科防毒公司的軟體標示為「被確認為惡意軟體」。目前沒有證據表明公開支持這些主張，歐盟委員會 4 月份也曾聲明沒有跡象表明該防病毒引擎存在任何危險。

作為回應，卡巴斯基實驗室表示，在收到歐洲議會的澄清之前，

它已停止與包括歐洲刑警組織在內的歐洲機構在內的所有工作，也暫停了與 No More Ransom 計畫的合作。另他們亦否認它與任何政府合作，且與任何政府都沒有關係，並且該公司從未幫助過，也不會幫助世界上任何政府的網路間諜活動。



資料來源：

<https://www.bankinfosecurity.com/eu-claims-kaspersky-lab-software-confirmed-as-malicious-a-11080>

3.2、駭客攻擊事件及手法

3.2.1、售票服務 Ticketfly 遭網頁置換，駭客竊取客戶與員工資料庫

美國售票技術公司的網站 Ticketfly 負責出售美國許多主要夜總會的門票，包括「Brooklyn Bowl」和華盛頓特區的「9:30 Club」。

近日 Ticketfly 網站遭駭客掌控並聲稱竊取該公司的客戶資料庫，駭客更傳了一份檔案給 Motherboard，聲稱是從 Ticketfly 網站所竊取的員工和客戶資料作為佐證。

根據 Twitter 上張貼的截圖，該公司遭駭客以一張 V 怪客的圖

片對其網頁進行置換攻擊，並在網頁上留下「Ticketfly HackeD By IsHaKdZ」以及「Your Security Down im Not Sorry」的字樣。

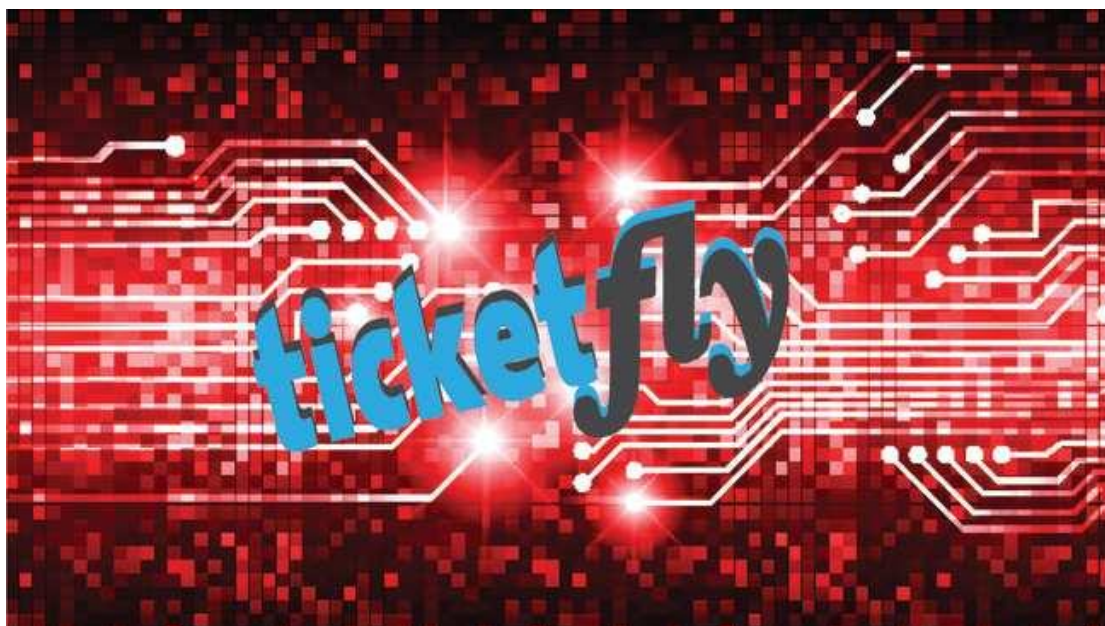
由 Eventbrite 公司所擁有的 Ticketfly 將該網站暫時下架並發布消息稱該公司確曾遭受網路攻擊，並表示在下架網站後正持續研究這個問題。將努力儘快使系統重新上線，但並沒有說明是否有任何活動門票被盜竊或其他損害，也拒絕回應駭客是否與該公司聯繫。

在與 Motherboard 的電子郵件對話中，駭客聲稱已經向 Ticketfly 發出了一個漏洞警告，該漏洞允許他掌控 Ticketfly 及其網站的「所有資料庫」。駭客分享他和一些 Ticketfly 員工提到這個漏洞的兩封電子郵件表示，他們向該公司要求 1 比特幣以分享漏洞的細節，但沒有得到回應。

駭客更指明已上傳了一系列疑似被駭客入侵的檔案至一台伺服器，其中包含幾個 CSV 檔，似乎含有 Ticketfly 客戶和員工的個人詳細資訊，包括姓名、住宅和電子郵件地址以及電話號碼。每個電子表格都包含數千個姓名。

Motherboard 嘗試確認這些檔案的真實性，發現其中一些名稱與使用 Ticketfly 員工的真實姓名和電子郵件地址相對應，目前已確認 6 個使用者的個人資訊，表示被駭客攻擊的資料是有效的。

●TWCERT/CC 建議，Ticketfly 客戶近期若接獲來自 Ticketfly 的電郵或任何媒介之訊息，務必確認來源，不要隨意開啟附件或連結等，以免遭有心人士利用。



資料來源：

https://motherboard.vice.com/en_us/article/mbk3nx/ticketfly-website-database-hacked-data-breach

3.2.2、美國 DHS 與 FBI 公布北韓駭客組織 HIDDEN COBRA 所利用的惡意程式 Joanap 及 Brambul，請大家注意防範(轉行政院技服中心資訊)

美國國土安全部(DHS)與聯邦調查局(FBI)公布最新北韓駭客組織 HIDDEN COBRA 所利用的惡意程式：Joanap 遠端存取後門程式與 Brambul 網路檔案分享系統蠕蟲。

若資訊設備遭受感染會有以下風險：

- 1.個人或單位資料遭竊取。
- 2.個人工作或單位運作被影響而中斷停擺。
- 3.資訊設備資源被利用於對外攻擊。

建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過下列方式檢查感染與否：

1. 路徑「%WINDIR%\system32\」下存在檔案

「mssscardprv.ax」。

2.嘗試寄信至 redhat@gmail.com 。

3.嘗試寄信至 misswang8107@gmail.com 。

4.嘗試連線至 HIDDEN COBRA-IP 黑名單，如參考連結。

影響平台：微軟作業系統。

建議措施：部署黑名單於防護設備進行偵測，監控是否有資訊設備已遭入侵。

若確認資訊設備已遭入侵，建議處理措施：

1.重新安裝作業系統，並更新作業系統及相關安裝軟體。

2.更換系統使用者密碼。

3.安裝及啟用防毒軟體防護。

4.安裝及啟用防火牆防護。

日常資訊設備資安防護建議：

1.持續更新作業系統及辦公室文書處理軟體等安全性修補程式。

若所使用的作業系統已不再提供更新程式，建議升級至較新版本作業系統。

2.系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除或停用。系統上非必要的服務程式亦建議移除或關閉。

3.安裝及啟用防毒軟體防護，並持續更新病毒碼及掃毒引擎。

4.安裝及啟用防火牆防護，並設定防火牆規則僅開放所需之通訊埠。



資料來源：

<https://www.us-cert.gov/ncas/alerts/TA18-149A>

<https://www.us-cert.gov/ncas/analysis-reports/AR18-149A>

https://twcert-official-file.s3.hicloud.net.tw/HIDDEN_COBRA-IP.csv

3.2.3、智利銀行 SWIFT 系統遭駭，近千萬美元失竊

智利知名銀行 Banco de Chile 於 5 月底遭受駭客透過 SWIFT 系統進行攻擊，導致鉅額損失。

智利銀行先後於 5 月 24 日及 5 月 28 日發出聲明表示分行機構故障以及確認遭受病毒感染攻擊，兩則公告都聲明只影響到銀行本身及其服務品質，而客戶資金、客戶紀錄的安全性以及資料的完整性皆受到保障，並未在此次攻擊中遭受影響。

據 Bleeping Computer 報導指出，認為駭客是利用磁碟抹除惡意軟體 KillDisk 的變種破壞智利銀行的數百台電腦，以分散員工的注意力，同時試圖透過銀行的 SWIFT 轉帳系統竊取資金，且根據銀行員發布在網路上的圖片，惡意軟體使受感染的 PC 系統崩潰，導致處於無法啟動狀態，表示它硬碟的主開機紀錄(MBR)受到影響。

而據當地新聞指出，智利銀行高層表示，此次攻擊屬針對 SWIFT

系統之零時攻擊，使用的惡意軟體名稱為 swaqp.exe，目前相關線索仍不多。另經研判，進行攻擊的搶匪可能來自東歐或亞洲，攻擊者透過 Luksic Group(Grupo Luksic)和 Citibank 竊取美金 1000 萬，最後證實得手的金額為美金 867 萬 2000 元，且這些交易大多是將金額匯款至香港。

此次攻擊事件發生後，銀行高層迅速反應，並與 Microsoft 和 Dreamlab 合作以確認事件狀況，而銀行方面也強調純粹此次事件造成的損失只影響了銀行本身，客戶權益則無損。



資料來源：

<http://www.latercera.com/pulso/noticia/gerente-general-banco-chile-eduardo-ebensperger-ciberataque-evento-fue-destinado-danar-al-banco-no-los-clientes/198912/>

<https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/>

<https://www3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica>

<https://www3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica>

[de-prensa/noticias-y-comunicados/declaracion-publica2](https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/)
<https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/>

3.2.4、歐洲電子零售商 Dixons Carphone 遭駭客攻擊，10 萬筆用戶信用卡資料外洩

英國老牌電器與消費電子零售商 Dixons Carphone 發現有「未經授權的存取」該公司持有的某些資料，並迅速展開調查且聘請一家外部公司來釐清案件。

該零售商解釋，有人試圖在 Currys PC World 和 Dixons Travel 商店的其中一個處理系統中侵入 590 萬張卡。但是，這些卡中有 580 萬張具有芯片和 PIN 的保護功能。

在這種情況下，針對這些卡片存取的資料既不包含 PIN 碼、卡片驗證值(CVV)，也不包含任何能夠進行持卡人識別或購買的驗證資料。迄今為止沒有證據表明由於駭客行為而導致資料遭到濫用。

然而對客戶來說壞消息是遭侵入的資訊包括信用卡資料，大約有 10.5 萬張非歐盟發行的信用卡，由於缺少晶片和 PIN，已經處於被盜用狀態，立即通過信用卡供應商通知相關發卡公司，以便可以採取適當措施保護客戶。

另外，除信用卡之外，入侵者還存取包含非財務 120 萬筆的個人資料紀錄，例如姓名、地址或電子郵件地址。

這不是公司第一次遭遇資安洩漏，Dixons Carphone 旗下的移動部門 Carphone Warehouse，在 2015 年也遭遇了一次重大駭客攻擊。此次資料外洩影響了大約 300 萬人。

針對此次事件該公司沒有透露其系統是何時遭受入侵的；沒有提供確切發現入侵的時間；也沒有透露過了多久才展開調查。

●TWCERT/CC 建議，受影響的客戶可能暴露在網路釣魚攻擊的

風險中，如近期接獲相關信用卡有關之電郵或交易，請務必保持警惕，以免遭有心人士利用。



資料來源：

<https://securityaffairs.co/wordpress/73479/data-breach/dixons-carphone-hacked.html>

<https://www.bloomberg.com/news/articles/2018-06-13/dixons-says-almost-6-million-cards-breached-in-cyberattack>

<http://www.dixonscarphone.com/~media/Files/D/Dixons-Carphone/documents/pr-investigation-into-unauthorised-data-access.pdf>

3.2.5、Trik 垃圾郵件殭屍網路洩漏 4300 萬有效電郵地址

Vertek 公司的一位威脅情報分析師在研究最近發布的 Trok 木馬版本時，發現 Trik 垃圾郵件殭屍網路的伺服器存在洩露情況。

而來自 Proofpoint 公司的惡意軟體專家最近也開始在追蹤 Phorpiex / Trik 殭屍網路，這殭屍網路近十年來相當活躍，被許多高

端的駭客用來散發一系列惡意軟體。

這兩種惡意軟體都會從位於俄羅斯 IP 地址的伺服器上下載惡意檔案，然而由於該伺服器配置錯誤，導致任何人都可以直接訪問該 IP，進而獲取儲存資訊。

這台伺服器上一共有 2201 個文字文件，依照 1.txt 到 2201.txt 的順序標記，每個文件包含大約 20,000 份電子郵件地址資訊，總量超過 4300 萬。

研究人員認為，該伺服器的運營商一直在使用這些電郵地址列表來為其他攻擊者提供服務，透過惡意垃圾郵件散播各種惡意軟體。

研究人員證實這些電郵地址都是有效電郵地址，且在 44,020,000 筆地址中，有 43,555,741 筆是唯一的，這些龐大的電子郵件地址來自世界各地，專家統計了 460 萬個獨特的電子郵件域名，絕大多數電子郵件地址都很舊(Yahoo:1060 萬筆、AOL:830 萬筆)。

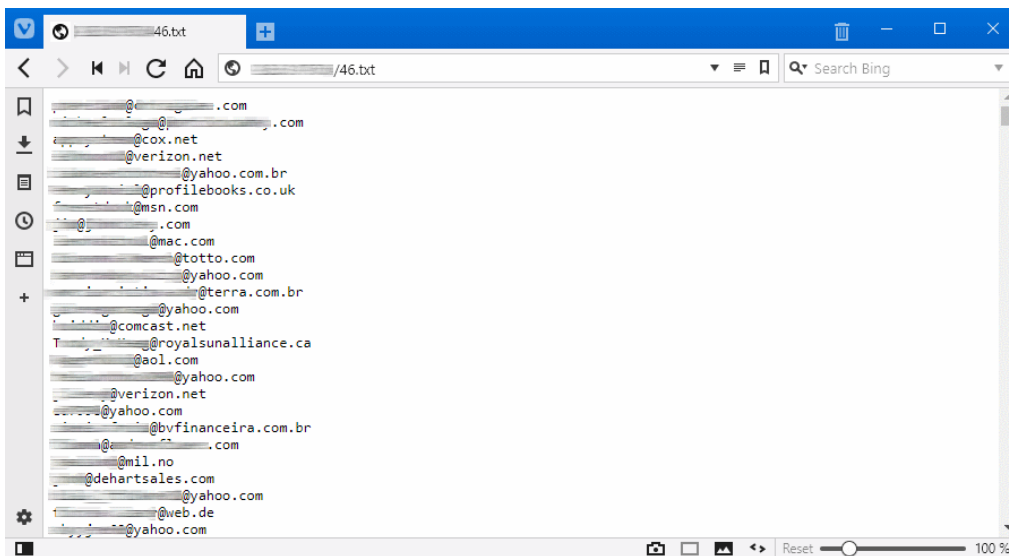
特別的是，儘管洩漏的列表中包含了很多自定義電子郵件域名，但包含的 Gmail 地址非常少，這表示電子郵件地址資料庫不完整，或者此惡意軟體活動有意針對使用舊電子郵件服務的用戶。

以下為外洩資料中統計前 10 名電子郵件網域

- 1.yahoo[.]com : 8907436 筆
- 2.aol[.]com : 8397080 筆
- 3.comcast[.]net : 788641 筆
- 4.yahoo[.]co[.]in : 433419 筆
- 5.sbcglobal[.]net : 432129 筆
- 6.msn[.]com : 414912 筆
- 7.rediffmail[.]com : 316128 筆
- 8.yahoo[.]co[.]uk : 294427 筆
- 9.yahoo[.]fr : 286835 筆
- 10.verizon[.]net : 282279 筆

●TWCERT/CC 建議，惡意釣魚郵件在網路上甚為氾濫，平時務必建立良好接收電郵習慣：

- 1.不要輕易相信標題聳動的電郵。
- 2.點選郵件內任何連結前要確認。
- 3.確認來源前，不要任意開啟任何附件。
- 4.不明來源信件未確認前不要輕易開啟。
- 5.即使是已知信任來源，也要有再確認的動作。



資料來源：<https://securityaffairs.co/wordpress/73488/cyber-crime/spam-botnet-leak-data.html>
<https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/>
<https://www.proofpoint.com/us/threat-insight/post/phorpiex-decade-spamming-shadows>

3.2.6、航班追蹤服務 Flightradar24 遭受資料洩露，用戶儘速更改密碼

Flightradar24 是一家提供實時航班飛行狀況的網際網路服務商。網站提供航班的飛行軌跡、出發地、目的地、航班號、註冊編號、飛

行器型號、當前位置、高度和空速等。

近期 Flightradar24 會員可能會收到來自 Flightradar24 要求會員更改密碼的電子郵件，因為 Flightradar24 發現一台伺服器遭到入侵以及非法存取。

據 Flightradar24 稱，駭客可能存取過在 2016 年 3 月 16 日之前註冊的帳戶相關的電子郵件地址和密碼 hash 值。

該公司透過電子郵件向用戶通報此事件並要求他們更改密碼，受影響的用戶密碼已重置。最初，收到該郵件的許多用戶以為資料洩露的通知可能是網路釣魚攻擊，因為沒有來自 Flightradar24 的官方消息，但後來該公司承認該事件並確認該電子郵件是合法的。

Flightradar24 表示確認伺服器漏洞可能導致此事件，安全漏洞只限於一台伺服器，在確定遭受入侵當下，即立刻關閉該伺服器，並對此事件受到影響客戶造成之不便感到抱歉。

該公司同時強調確認沒有跡象表明任何個人和財務資訊暴露，也沒有付款資訊被洩露。Flightradar24 既不處理也不儲存付款資訊。

壞消息是，該公司承認當初是以舊的 hash 演算法保護密碼，因此攻擊者可能輕易破解，Flightradar24 自 2016 年起才推出更安全的 hash 演算法。

目前尚不清楚有多少用戶受到影響，該公司報告說，事件只涉及「小部分」用戶。然而 FlightRadar24 聲稱每月用戶數超過 4000 萬，這意味著受影響的用戶數量可能不容小覷。

FlightRadar24 迅速向瑞典數據保護局報告此事件，以符合歐盟的「通用資料保護條例」(GDPR)。

●TWCERT/CC 建議，FlightRadar24 用戶除儘速更改密碼，且如接獲疑來自 FlightRadar24 的要求更改密碼信件之電郵信件，請確認來源，並儘可能僅透過官網服務變更密碼，不論來源合法與否，不要輕易點選信件連結，以免遭有心人士利用。



資料來源：<https://securityaffairs.co/wordpress/73740/data-breach/flightradar24-data-breach.html>

<https://forum.flightradar24.com/threads/11945-Security-breach-email?p=106525>

3.2.7、Necurs 殭屍網路的 CSE 惡意軟體 ZLab-Ursnif 銀行木馬新變種襲擊義大利公司

從 6 月 6 日開始，惡名昭彰的銀行木馬 Ursnif 其新變種攻擊義大利幾間公司。這種惡意軟體在資安界眾所周知，Ursnif 銀行木馬病毒是 2016 年金融領域最活躍的惡意代碼，這樣的趨勢一直持續到 2017 年。

在之前的攻擊活動中，Ursnif 銀行木馬專門針對日本、北美、歐洲和澳大利亞的用戶，後來作者改進了他們的規避技術，以針對世界各地的用戶，特別是在日本。

該惡意軟體能夠竊取用戶的憑證，如本地 webmail、雲儲存、加密貨幣兌換平台和電子商務網站的憑證。

CSE Cybsec ZLab 研究人員對最新版本的惡意軟體進行分析，在發現可疑檔案後開始調查，該檔案用於針對其客戶的目標式攻擊。

該攻擊活動中使用的是針對義大利公司的一個武器化的微軟

Word 檔案附件，並使用社交工程技術誘騙用戶啟用巨集來查看內容。

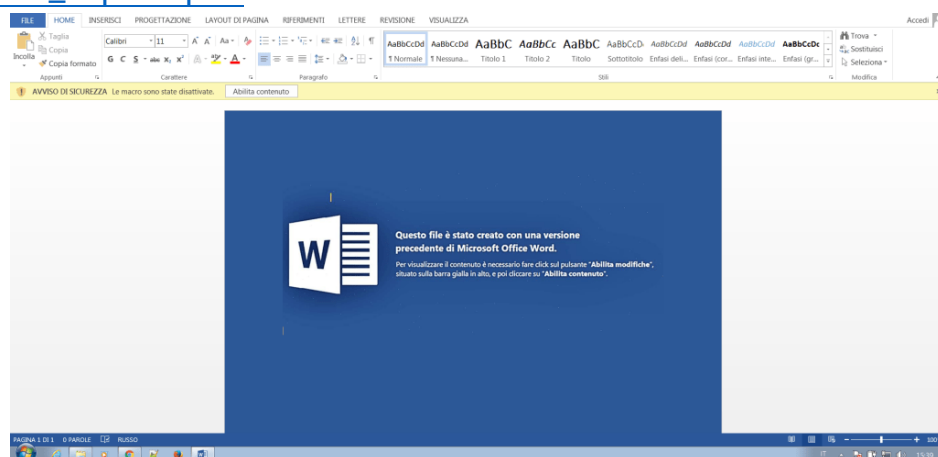
此外，一旦 Ursnif 感染過一台新機器，將試圖傳播給受害電子郵件帳戶的地址簿中的任何其他用戶，且為了誘騙其他受害者打開惡意郵件，電郵訊息會以回覆受害者過去來往信件的方式呈現。

在調查涉及義大利公司最近一次釣魚活動的域名時，研究人員發現，其中許多域名是透過相同的電子郵件地址註冊的：「whois-protect [.] hotmail [.] com」。

這個電子郵件地址直接連接到臭名遠播的 Necurs 殭屍網路，這是過去幾個月用來推送許多其他惡意軟體的惡意體系結構，包括 Locky、Jaff、GlobeImposter、Dridex、Scarab 和 Trickbot。

ZLab 研究人員發布的報告中提供了針對義大利公司的 Ursnif 惡意軟體變體的更多細節，包括 IoC 和 Yara 規則。

完整的 ZLaB 惡意軟體分析報告可透過以下 URL 下載：
http://csecybsec.com/download/zlab/20180621_CSE_Ursnif-Necurs_report.pdf



資料來源：<https://securityaffairs.co/wordpress/73865/malware/ursnif-banking-hits-italy.html>

3.2.8、訂房系統 FastBooking 資料遭竊，上百家已知飯店受到影響

據 Bleeping Computer 報導，數百家飯店的客戶的個資和信用

卡資料 6 月遭不明身分的攻擊者竊取。

這些資料來自於一家總部設在巴黎的法國訂房系統供應商 FastBooking，該公司在其網站上聲稱高達 100 個國家的 4,000 多家飯店使用其飯店預訂軟體。

事件發生在 6 月 14 日，攻擊者利用伺服器上託管的應用程式中的漏洞安裝惡意工具（惡意軟體），這個工具允許入侵者遠端存取伺服器，並用來竊取伺服器的資料。直到 FastBooking 的員工在其伺服器上發現這個惡意工具，事件才曝光。

事件時間表：

2018 年 6 月 14 日，下午 8:43 UTC – 攻擊者入侵 FastBooking 的系統。

2018 年 6 月 19 日，下午 3:40 UTC - FastBooking 發現入侵。

2018 年 6 月 19 日，下午 9:02 UTC - FastBooking 遏止洩漏事件。

根據 FastBooking 表示，入侵者竊取了飯店客人姓名、國籍、郵政地址、電子郵件地址和飯店預訂相關資訊（飯店名稱、入住和退房細節）等資訊。

在某些情況下，入侵者甚至也獲得了信用卡的詳細資訊，例如信用卡上印的名稱、卡號和截止日期。

在針對日本市場的新聞稿中，FastBooking 表示，事件影響了 380 家日本飯店。Bleeping Computer 認為，全球受影響的飯店數量要比日本的數量多，可能超過 1000 家。

該公司目前尚未公開受影響飯店的總數，被盜私人細節的客人數量以及從 FastBooking 伺服器獲取信用卡細節的客人人數，第一家向客戶通報 FastBooking 外洩事件的飯店是日本的 Prince Hotels & Resorts。該連鎖飯店表示，此次事件影響了 124,963 名入住其 82 家飯店的客人。

● TWCERT/CC 建議，FastBooking 客戶近期如收到來自 FastBooking 信件，務必確認真偽，並切勿輕易點選附件或連結，並注意近期信用卡交易狀況，以免遭駭客利用。



資料來源：<https://www.bleepingcomputer.com/news/security/hundreds-of-hotels-affected-by-data-breach-at-hotel-booking-software-provider/>
<http://www.princehotels.com/news/notice-of-unauthorized-access-to-or-acquisition-of-prince-hotels-resorts-reservations-system/>

3.2.9、上億造訪人次之票務服務 Ticketmaster 系統之套件遭駭

知名的票務服務 Ticketmaster 是美國經營線上售票的網站，是很多美國大型運動賽事和多個美國一級場館的獨家合作售票業者，擁有上億的造訪人次。

Ticketmaster 公告一項資料洩露事件，該事件影響整體客戶群約 5%，並導致姓名、地址、電子郵件地址、電話號碼付款詳細資訊以及 Ticketmaster 登錄詳細資訊等客戶資料被盜。

洩漏事件並非出自 Ticketmaster 本身，而是 Ticketmaster 在全球各地網站上部署提供人工智慧即時聊天套件的供應商 Inbenta。

Ticketmaster 稱，6 月 23 日星期六，它發現這個即時聊天套件被用來向 Ticketmaster 用戶傳送惡意軟體。惡意軟體正在收集紀錄和洩露客戶詳細資訊。

該公司表示，並非所有網站訪問者都受到影響，因為並非所有用

戶都登錄到網站或進行購買，主要以 2017 年 9 月至 2018 年 6 月 23 日期間購買或試圖購買機票的國際用戶將受到影響，北美用戶除外。

英國用戶也受到影響，但程度較輕，Ticketmaster 表示，該惡意資料收集僅在 2018 年 2 月至 6 月 23 日期間影響其英國網站。

Ticketmaster 仍在調查事件。且向其認為受到影響並收集其個人資料的用戶發送了電子郵件，並在發現外洩事件後，週六在其所有網站上禁用了 Inbenta 小套件。該公司已經為其英國用戶發布了一個網站，提供關於客戶如何請求免費的 12 個月身分監控服務的資訊。

Inbenta 沒有提出意見。Bleeping Computer 詢問此事件是否會影響 Inbenta 的其他客戶。該公司在其網站上列出了 Groupon、Change.org、Schlage 和 Ticketbis 等客戶。

英國國家網路安全中心(NCSC)的一名發言人稱，該組織在知曉此次攻擊事件後，正在與各方夥伴合作展開調查。

● TWCERT/CC 建議，Ticketmaster 客戶近期如收到來自 Ticketmaster 信件，務必確認真偽，並切勿輕易點選附件或連結，如欲更改密碼務必使用官網提供之變更密碼服務，避免使用信件密碼變更連結，並注意近期信用卡交易狀況，以免遭駭客利用。



資料來源：

<https://www.bleepingcomputer.com/news/security/ticketmaster-announces-data-breach-affecting-5-percent-of-all-users/>

3.2.10、Gentoo Linux 的 Github 帳號遭駭，內容可能遭惡意竄改

如果使用者近期從 Gentoo 的 GitHub 託管的儲存庫中提取了任何內容，請務必注意，因為駭客已經干預該開源專案的資料。

Linux 官方發行機構在星期四發出警告，揭露 6 月 28 日，UTC 時間 20:20 左右，未知的個人已經獲得了 Gentoo 組織的 Github 控制權，並修改了儲存庫的內容以及頁面的內容，並表示在努力確定該組織及其儲存庫的確切範圍並重新獲得控制權前，所有託管在 GitHub 上的 Gentoo 代碼現在都應視為被駭侵。

基本上，如果您透過 GitHub 從 Gentoo 下載並安裝了素材，那麼可能會因此引入惡意代碼而受到威脅。直到威脅清除前，建議避免從專案的中心組織帳戶中獲取任何內容。

另外，Gentoo 不認為程式碼的主副本被篡改，因 Gentoo 將主版本與 GitHub 託管的版本分開存放在未被駭客入侵的伺服器上，GitHub 上只是 mirror。因此，使用者應能夠透過 Gentoo.org 網站獲得沒有太多問題的軟體乾淨副本。

所發布之警告沒有揭露篡改代碼的來源、如何做到以及事件長達多久。



資料來源：

https://www.theregister.co.uk/2018/06/28/gentoo_linux_github_hacked/
[https://archives.gentoo.org/gentoo-
announce/message/dc23d48d2258e1ed91599a8091167002](https://archives.gentoo.org/gentoo-announce/message/dc23d48d2258e1ed91599a8091167002)

3.3、軟硬體漏洞資訊

3.3.1、區塊鏈平台 EOS 新漏洞，有遭探勘接管之虞

EOS.IO 本身是加密貨幣的代幣與區塊鏈平台，而開放原始碼的 EOS，視作 Blockchain 3.0，使軟體工程師能在區塊鏈基礎上發展去中心化應用程式，由 block.one 公司以 c++ 開發的 EOS tokens 乃全球第 5 大加密貨幣，排名在 Bitcoin、Ethereum、Ripple、Bitcoin Cash 之後，近期 EOS 被披露數項新弱點，其 binaryen.cpp 函數出現 buffer out-of-bounds write 弱點，若 node 解析惡意 WASM 格式的智慧合約檔案時，將覆寫緩衝區，並避開 DEP、ASLR 等防禦技術，啟動反向 shell 回連攻擊方，駭客能逐步控制整個 EOS 網內全部 node 設備，甚至操縱 supernode，製造 botnet 軍團或挖礦大隊；block.one 於 5 月 29 日修復，然中國大陸資安研究單位 Qihoo 360 表示該修復措施僅針對 64 位元，32 位元 node 作業系統仍具風險，block.one 後於 5 月 30 日更新檔案。另外 EOS 區塊鏈 node 被瑞士 IP 為 185.169.231.209 發動掃描，試圖搜尋線上 EOS 的 RPC API 終端設備，試圖從 port 8888 挖掘 list_keys 密鑰資訊，官方表示該 API 非標準規格，僅供測試，停用即可。



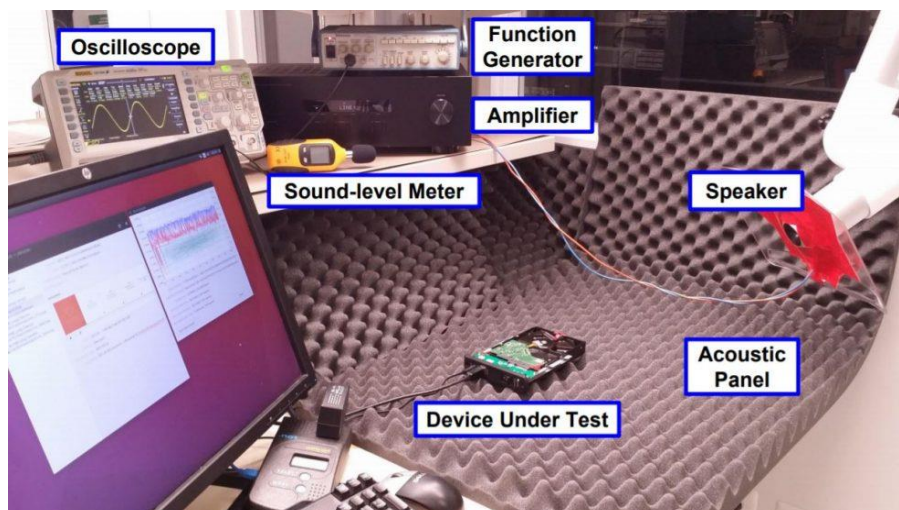
資料來源：

<http://blogs.360.cn/blog/eos-node-remote-code-execution-vulnerability/>

<https://thehackernews.com/2018/05/eos-blockchain-smart-contract.html>

3.3.2、硬碟感震設計成破綻，聲波攻擊能促發 DoS

人類聽覺領域之外的超音波，或是有聲訊號，都可能成為現代硬碟的剋星，原音共鳴(acoustic resonance)本是普通的物理現象，然聲音本身即是震動能量，在特定頻率與距離，可持續刺激硬碟防震感震結構，觸發 shock sensor-driven feedforward 機制，進而強制讀寫頭(head)停宕，斷絕本機 OS 資料來源。據實際探勘證明，現行主流廠牌硬碟，受到音頻 21~31 kHz 之超音波，竟於 8 秒內失能，一般聲波亦能於 2 分鐘內瓦解硬碟運作，音波攻擊技術，對目前 DVR 監控設備極為致命，且聲波攻擊採證不易，無論源頭從外部喇叭或內部喇叭，皆難以分析攻擊過程，鑒於此弱點在於結合物理特性與硬碟韌體，故發展防禦技術，應從回饋控制、ultrasonic wave 辨識、抗噪材料等方面入手，降低硬碟結構對聲波敏感度，始得專注偵測實體震動。



資料來源：

<https://www.youtube.com/watch?v=v0yh9fG00zo&feature=youtu.be>

<https://thehackernews.com/2018/05/hard-drive-failure-hack.html>

3.3.3、鎖定 Blue Coat 安全閘道 ASG & ProxySG 瑕疵，駭客硬闖 SAML 認證

Symantec 併購 Blue Coat 後，發展整合式安全產品，Blue Coat 推出企業級 Web 安全閘道器，賣點在安全與加速，旗下 Advanced Secure Gateway、ProxySG 兩款商品，經研究具安全認證迴避漏洞，因為錯誤解析 SAML response，無法正確處理帶有註解資料的 XML 節點，導致遺失註解之後的本文資訊，若遠端駭客攔截變造 SAML response，不會造成加密簽章失效，藉此規避 SAML 安全控管，冒充合法用戶存取設備，然此漏洞不影響管理者連線控制台時身分認證，僅評為中度危險，或許因威脅不大，官方網站目前仍無解決方式。



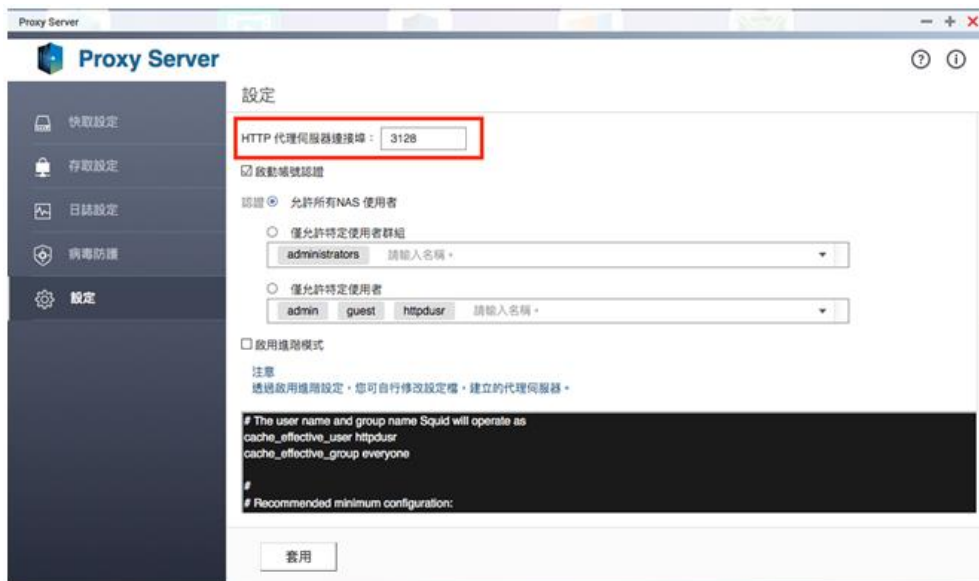
資料來源：

https://support.symantec.com/en_US/article.SYMSA1450.html

<https://securitytracker.com/id/1040993>

3.3.4、威聯通升級 Proxy Server，消彌 CSRF 等 4 項弱點

國內 NAS 第二大廠威聯通，技術能力包含硬體製造和軟體開發，以 QNAP 品牌行銷世界，專屬作業系統 QTS 平台，支援 Proxy Server 軟體建置，利用 NAS 扮演代理伺服器，達成效率與節約，近日公布 Proxy Server 弱點 4 項但保留技術細節，駭客實行 CSRF 及 XSS 攻擊手段，可送出特製 URL 及 Javascript 程式碼，憑藉受害者帳號身分，控制瀏覽器介面；或者恣意執行 QTS 作業系統指令，甚至透過惡意 request 竄改 Proxy Server 設定值，影響系統安全，QNAP Systems 已針對相關瑕疵升級 Proxy Server，可直接下載。



資料來源：

<https://www.qnap.com/en/security-advisory/nas-201806-01>
<https://securitytracker.com/id/1041025>

3.3.5、今年第二波 Flash Player 0-Day 攻擊，瞄準中東 Office 用戶

今年 2 月初，北韓藉 Flash Player 弱點發動首波 0-Day 攻擊，入侵南韓人士，6 月初證實波斯灣國家卡達，爆發第二波 Flash Player 0-Day 在野攻擊，去年因卡達與四鄰國雪崩式斷交，政經局勢不穩，疑似因此遭駭客鎖定，自 2 月起籌備 C&C server，部分網域為 people.doha(杜哈，卡達首都)，並設計阿拉伯語系試算表(salary.xlsx)，嵌入惡意 Flash Player 內容，此一武器化 xlsx 檔案經 email 散布，採取魚叉式釣魚手法，一旦惡意試算表開啟則連線 C&C server，依序下載惡意 swf(Shock Wave File)及 shellcode，先觸發堆疊緩衝區溢位，再以受害者身分權限，執行駭客準備之程式碼，全程攻擊階段可謂典型 APT，此項 Flash Player 弱點極為嚴重，Adobe 已火速發布更新版本，順便修補另外 3 個重要漏洞(Type Confusion、Integer Overflow、越界讀取記憶體)，改善資訊洩漏、執行任意碼等負面影響。



資料來源：

<http://blogs.360.cn/blog/cve-2018-5002-en/>
<https://securityaffairs.co/wordpress/73291/hacking/cve-2018-5002-zero-day.html>

3.3.6、三項漏洞曝光，令 Foscam IP Camera 無法承受連鎖攻擊

安全研究團隊 VDOO 專攻 IoT 資安領域，據其分析，Foscam 監控設備使用 Linux 平台，存在 3 種嚴峻瑕疵能形成連鎖攻擊，駭客只要以掃描或越權存取等手段，獲得 IP Camera 位址，可藉 `strncat()` 函數合併 URI 路徑元件字串與根路徑 `/tmp/www`，取得完整路徑，濫用 `lighttpd` web server 客製化程式碼刪除暫存快照之功能，毀掉關鍵檔案，繞過身分驗證；再塞入大量字元當成 `callbackJson` 字串參數，讓 `prepare_reply_func()` 串接 `callbackJson` 與其他資料時觸發 `Buffer Overflow`，導致程式功能 crash，迫使 `watchdog` 自動重啟程序，從而盜取管理者憑證；擁有管理者身分後，惡意改變 NTP 伺服器 URL 內容，換成 `;mal_command;` 之類分號包夾惡意指令之格式，經 `setSystemTime` 指令處理變造之 NTP 伺服器 URL，完成惡意指令注入，且以 `root` 身分執行有害的 Shell Command；究其原因在於軟體設計缺陷，過多程序採用 `root` 身分，嚴重違反權力分割概念；外部程序替代既有 API 執行 shell commands 引進風險；輸入值過

濾能力欠佳；及韌體檔案僅採 AES 128 加密區塊鍵保護，加密演算過弱，令駭客得以快速窺探軟體架構全貌，目前仍未察覺在野攻擊事例，已確認相關漏洞影響 18 種韌體與 55 款機型，Foscam 已修補所屬弱點韌體。



資料來源：

<https://blog.vdoo.com/2018/06/06/vdoo-has-found-major-vulnerabilities-in-foscam-cameras/>
<https://www.bleepingcomputer.com/news/security/patches-available-for-dangerous-bugs-in-popular-brand-of-ip-cameras/>

3.3.7、高階腳本語言 Perl 測出 directory traversal 破綻，面臨檔案覆蓋風險

Perl 是高階、通用、直譯、動態的腳本程式語言，師法眾多語言特性(C、sed、awk、shell)，廣泛應用於各領域，囿於其 Archive::Tar 模組具目錄遍歷瑕疵，遠方駭客製作惡意 tar 格式壓縮檔，內藏同名之一般檔案與 symlink(符號鏈結)，受害者解壓縮後，將突破 Archive::Tar 模組保護機制，能產生任意路徑與檔案，或者覆蓋既有路徑與檔案，破壞原始資料，新版 Perl 已釋出並修補缺陷。



資料來源：

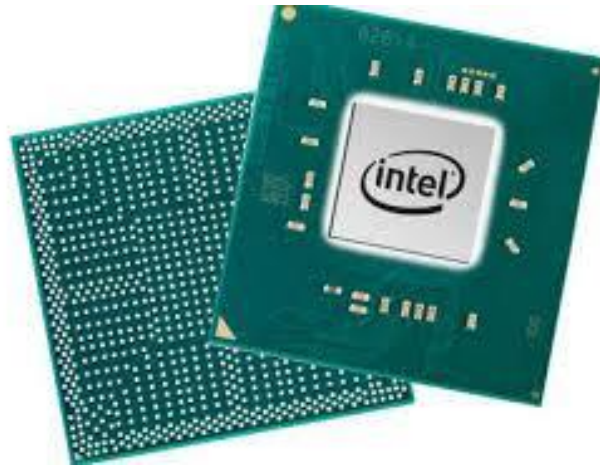
<https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=900834>

<https://securitytracker.com/id/1041048>

3.3.8、Intel CPU 再爆預測執行式旁道分析威脅 — Lazy FP state restore

自今年 1 月以來，全球裝配 CPU 的資訊產品，無論行動裝置或個人電腦，幾乎都難免有鬼魅(Spectre)和熔毀(Meltdown)兩類漏洞，且陸續衍生 Variant 4、Variant 3a 等弱點變體，此皆源於 CPU 結構設計為追求運算效率所衍生之副作用，如今 Intel 再度公開微處理器產品設計瑕疵，牽涉到 Lazy FP state restore 硬體機制，因浮點運算單元(Floating Point Unit)狀態資料量大，進行 task 切換時速度慢，FPU 使用率低，僅必要時調用，鑑此，延遲 FPU state save&restore 作業，直至呼叫次個 FP 指令之前，然延遲期間資料仍置舊 task 儲存區原位，駭客利用晶片上處理單元設計失策，得窺探 FPU 註冊值，形成 side-channel 分析式攻擊，挖掘 AES 密鑰及其他輸入資料與計算結果。若主機裝配弱點處理器，影響軟體包含 kernel 4.9 之前版本之 Linux、Red Hat Enterprise Linux 5、6、7、MRG 2，以及 Windows Server 2008、Google chrome OS、Xen 全數系統版本，根本解決

方式為啟用 Eager FPU restore。



資料來源：

http://www.theregister.co.uk/2018/06/13/intel_lazy_fpu_state_security_flaw/
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00145.html>

3.3.9、佳能 6 款印表機測出管理者認證 bypass 缺失

日商佳能株式會社(Canon)所生產印表機，部分機型遭測試出認證機制可被繞開，就 LBP6650、LBP3370、LBP3460、LBP7750C 四款機型，對 web 介面送出內藏 frame.cgi?page=DevStatus 字串之惡意請求，可迴避 Administrator Mode 密碼驗證階段；而 MF210、MF220 二機型之 System Manager Mode 亦有類情，以 /portal_top.html 字串加工 request 後送出，能直接進入 System Manager Mode 介面，經由上述手法，駭客得以獲得設備狀態且全權更改系統設定，Canon 無相關安全更新訊息，僅回應，用戶未按手冊最佳作法且保留出場預設值，始具備弱點條件。



資料來源：

<https://nvd.nist.gov/vuln/detail/CVE-2018-11692>

<https://imgur.com/a/QE3GfLw>

3.3.10、更新加密工具 GnuPG，阻止偽造簽章事件

GNU Privacy Guard 簡稱 GnuPG，係完整且免費的 OpenPGP 標準建置，以萬能鑰管理系統保護簽章資料，眾多前端應用程式均借重其現成加密技術，可謂是全球最普及的 email 用戶端數位簽章軟體，經分析因其程式 mainproc.c 瑕疵，未對妥善檢查檔名參數，遠端攻擊者得以伺機注入多種控制符號，並偽造 status message 交由其他程式解析，若負責解析的程式採用--status-fd 2 選項，則偽冒攻擊生效，詐騙者訊息被用戶程式解析且信任，與一個月前禍及 Thunderbird、Apple Mail、Outlook 的加密工具漏洞「eFail」相較，本次 SigSpooof 更為嚴重，影響電郵安全、備份安全、更新檔部署等工作領域，亦衝擊如 Git 般的 source code 版本控制系統，GnuPG Project 已更新版本，可公開下載。



資料來源：

<https://lists.gnupg.org/pipermail/gnupg-announce/2018q2/000425.html>

<https://neopg.io/blog/gpg-signature-spoof/#proof-of-concept-ii-signature-and-encryption-spoof-enigmail>

3.3.11、零號字 ZeroFont 釣魚術等待全球 Office 365 用戶上鉤

以色列雲端安全公司 Avanan 指出，Office 365 所搭配之 natural language processing 引擎，雖為反釣魚 AI 技術，但面對 ZeroFont 釣魚攻擊則束手無策，因 ZeroFont 會在正常文章內插入隨機字串，形成無文章結構的垃圾篇幅，讓人工智慧找不出邏輯，無從警告用戶，然而該等隨機字串以 HTML 語法 `<span style="FONT-SIZE: 0px">` 控制，不在 GUI 顯示，收信者所見均為正式內容，誤導受害者深信詭計，接受駭客來信指示，恐衍生後續勒索軟體、木馬程式、洩露機密等實質損失，已證實出現 ZeroFont 案例且正持續圖謀全球弱點用戶，然確切受害數量不明，據悉微軟已著手解決該演算法缺失，但官方暫無公開訊息。



資料來源：

<https://www.avanan.com/resources/zerofont-phishing-attack>
<https://sensorstechforum.com/zerofont-phishing-attack-bypasses-office-365-security/>

3.3.12、Splunk 企業版權限控管失誤，將暴露系統資訊

營運決策支援系統 Splunk® Enterprise，能蒐集 IT 建設、安全系統、商務程式各類 log 格式，產生分析報表，經測試 REST 終端存在權限控管破綻，遠端駭客於 URL 直接對設備 IP 之 port 8000，附加_raw/services/server/info/server-info?output_mode=json 之請求，竟可獲得設備 OS、硬體、Splunk license key 等資訊，所幸核心商務資料無外洩之虞，Splunk 已升級版本修補瑕疵，並建議 REST endpoint 需要搭配適合的叢集裝置始得避免風險。



資料來源：

<https://www.splunk.com/view/SP-CAAAP5E#announce1>
<https://securitytracker.com/id/1041148>

3.3.13、iOS 瑕疵忽略密碼錯誤上限，令暴力破解攻陷 iPhone

甫於 6 月初，Apple 發布最新版本 iOS 12 新聞，本月尚未結束，Hacker House 成員 Matthew Hickey 就挖掘出各版 iOS 共通破綻，當然 iOS 12 也名列其中。蘋果所開發 Secure Enclave Processor(SEP)，安全飛地處理器，具備獨立硬體、韌體、啟動程序，與隔離資料交換管道，以貫徹全面資料保護機制，包括 Erase Data 功能，可偵測密碼登入失敗次數，達上限時悉數自毀隱私資料，避免外洩，然 iOS 介面缺點在於，忽略重複及過快 pin 碼不檢查，若 iPhone 外接鍵盤之類實體裝置，可 bypass 密碼錯誤次數上限，連續輸入 6 碼 pin 進行 brute force 破密，取得 iPhone 控制權，蘋果暫無修補方案。



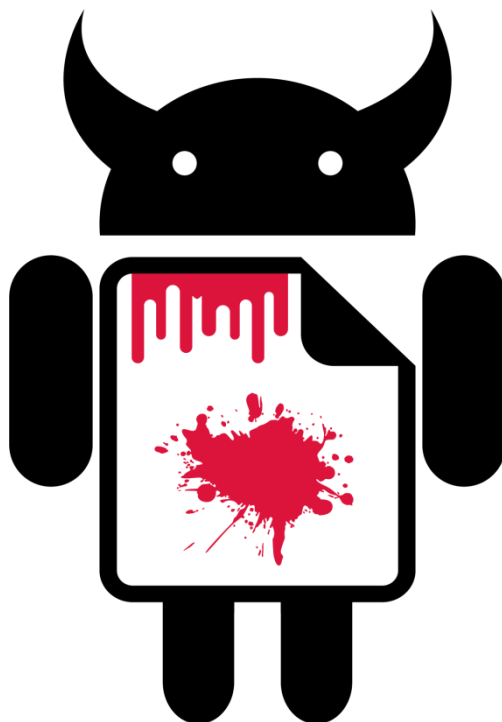
資料來源：

<https://vimeo.com/276506763>

<https://securitytracker.com/id/1041177>

3.3.14、硬體漏洞 RAMpage 衝擊 6 年內生產 Android 設備

來自學術界與科技公司的 8 人小組，研究出最新 Rowhammer 變體，稱作 RAMpage，該嚴重瑕疵專門針對 6 年內出廠 Android 行動裝置，駭客操縱惡意程式，可突破 ION 次系統之記憶體管控，闖入 memory page 界限，越權觸及其他程式專用隱密內容，如同管理者般存取密碼、照片、電郵、商務文件等，研究團隊提供測試工具俾供檢查設備是否具有 RAMpage 徵兆，亦開發今年獲獎之修補工具 GuardION，藉著隔離政策防止資料結構遭變更，儘管 Google 認同 RAMpage 能干擾 Android 裝置，然對 GuardION 一事感到過度反應，迄今仍無官方安全更新。



資料來源：

<https://rampageattack.com/>
<https://vvdveen.com/publications/dimva2018.pdf>

3.4、資安研討會及活動

時間	研討會/課程 名稱	研討會相關資料
2018/07/ 09	「2018 資訊 安全發展趨 勢研討會」場 次(三) 、(四)	【資安研討會】「2018 資訊安全發展趨勢研討會」場次(三) 、(四) 日期：2018 年 07 月 09 日(一) 09：00 - 12：00 (場次三)/2018 年 07 月 09 日(一) 14：00 - 17：00 (場次四) 地點：台北世貿一館 2 樓 第 2 會議室(臺北市信義路五段 5 號) 主辦單位：中華民國資訊軟體協會 線上報名連結 場次三： http://www.cisanet.org.tw/News/activity_more?id=MzU0

時間	研討會/課程名稱	研討會相關資料
		場次四： http://www.cisanet.org.tw/News/activity_more?id=MzU1 活動概要： 搭配「資訊安全主題館」展出內容，於世貿一館 2 樓舉辦「2018 資訊安全發展趨勢研討會」，邀集國內外優秀資訊安全專家，分享 GDPR 歐盟通用資料保護規則、人工智慧安全、資訊安全檢測、資料保全防護、資料虛擬隔離、特權帳號管理、雲端桌面安全、資安防禦應變、網路進階防護等資訊安全解決方案與成功應用範例，提供與會者洞悉未來資訊安全防護發展脈絡，期能促進供需雙方相互交流！ **報名參加可獲 2018 智慧生活軟體應用展門票 1 張
2018/07/11-12 2018/07/25-26	107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安攻防與監控實務課程	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安攻防與監控實務課程 課程時間：2018 年 07 月 11 日(三) - 07 月 12 日(四)/2018 年 07 月 25 日(三) - 07 月 26 日(四) 受訓地點：協志聯合科技資安實戰攻防演練中心 (台北市中山北路三段 22 號 13 樓) 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzQx 課程簡介： 本課程設計除透過瞭解資訊安全所面臨之風險與處理方法，藉以學習如何採取相對應之控制措施之外，並由滲透測試與資安偵測與監控之實務操作，讓結業學員學

時間	研討會/課程名稱	研討會相關資料
		習到有效的資安防禦實務，俾利資訊安全產業與相關企業對於資安防禦人才之運用。再從滲透測試概論去檢視駭客如何進行資安攻擊，且帶入駭客思維與自身遇到的案例作為延伸以增加學員的深度及廣度。透過逐步練習一些經典的案例和解說近幾年的新的網頁開發工具或技術可能所帶來的新型態的攻擊，認識這幾年資安上的變化。最後提供 Lab 進行攻擊演練，親身體驗以駭客角度去看整體企業資安。有別於過往與坊間一般資安理論課程，此次課程設計著重於瞭解稽核規定與事故應變措施→理解駭客攻擊思維→熟悉企業級防禦手段等流程，最後透過實機操作(hands on lab)方式，與台灣第一座企業級「資安實戰攻防演練中心」- Cisco Cyber Range 的合作，讓學員能從超過 20 種的攻擊案例與九種技術解決方案中模擬實際資安危害情事，並瞭解如何應對處置，使其回到工作崗位上時便能具備一定程度的攻防實務技巧。 課程大綱： 1.資訊安全風險處理與控制 2.滲透測試方法與實務 3.資訊安全偵測與監控實務
2018/07/16-17 2018/07/23-24	107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - ICS/SCADA 資訊安全實務課程(高雄)	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - ICS/SCADA 資訊安全實務課程(高雄) 課程時間：2018 年 07 月 16 日(一) - 07 月 17 日(二)/2018 年 07 月 23 日(一) - 07 月 24 日(二) 受訓地點：高雄 - 巨匠電腦資訊 - 電腦教室 (高雄市新興區中山一路 242 號) 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id

時間	研討會/課程名稱	研討會相關資料
		=MzQy 課程簡介： 本課程設計藉由 ICS/SCADA 資安威脅、弱點與風險之探討與研析，加以理解 ICS/SCADA 所面臨之風險外，透過 ICS/SCADA 資安事故處理研析與演練，讓學員學習 ICS/SCADA 資安事故處理實務，俾利關鍵基礎設施營運商對於關鍵資訊基礎設施保護人才之運用。ICS/SCADA 為因應近年來人機介面友善化與遠端操控等需求，系統內早已具備各種運算及通信功能，更因而成為駭客攻擊的對象；其中以關鍵基礎設施(CI)、關鍵資訊基礎設施(CII)內部之 ICS/SCADA 的資安事故更讓人重視，本會特聘各界處理 ICS/SCADA 資安事故之資深講師親臨現場，現身說法，透過案例解析與實務演練的方式，讓與會學員能有效的學習到理論與實務面上的知識。 課程大綱： 1.ICS/SCADA 資安威脅探討 2.ICS/SCADA 弱點與風險研析 3.ICS/SCADA 資安事故處理實務
2018/07/19	D Forum 2018 雲端資安論壇：個資與企業營業秘密防護	【資安研討會】D Forum 2018 雲端資安論壇：個資與企業營業秘密防護 日期：2018 年 07 月 19 日(四) 地點：台北六福皇宮 B3 永康殿(台北市南京東路三段 133 號) 主辦單位：DIGITIMES 線上報名連結： https://ssl.digitimes.com.tw/OnLine4/DataInput.asp?ProdGroup=051A71023-0

時間	研討會/課程 名稱	研討會相關資料
		活動概要： 企業各維運單位，既要追求業務成長，同時兼顧營業秘密安全、個人資料防護...2018 年，市場籠罩在一片資訊外洩的恐懼之中。 如何獲得「免於資料外洩恐懼」的自由？這是 2018 年，企業各營運、IT 管理單位最渴望獲得的答案！
2018/07/26	ANTICIPATE	【資安研討會】ANTICIPATE 日期：2018 年 07 月 26 日(四) 地點：台北寒舍艾麗酒店 5F 宴會廳(台北市信義區松高路 18 號) 主辦單位：F5 線上報名連結： https://interact.f5.com/twanticipate2018.html?utm_source=f5drop&utm_medium=email&utm_campaign=f5drop&mkt_tok=eyJpIjoiT1RZNU16Sm1PVGsxT1RGbSIsInQiOiJCSExsdFpzSmlmaUU3bUVOZm1DK3ZOeWwrTU4wVjhyUUgzXC9NVnI2cjN1ckRuK2JsWkpcL0Rsc1ozWXhYcUJKcGx4ek1ISXRQREx5V2lEV1wvd0k3NVJTNzcyN1g2c2Nxd21QNVdZbzhCWnRrQjA2dkhJYnJSQmZRTiViVWJzZTZhcXNsV2JYXC9vTzNSVnRONHVNNXVwbFNBPT0ifQ%3D%3D 活動概要： 加入我們的行列，獲得所需的知識與靈感來發展您的應用程式及企業，並在以應用程式為中心的多雲世界裡脫穎而出。身處在當前的數位轉型浪潮裡，您的應用程式就是您的企業。企業所需的技能、規範、統籌管理正面臨典範轉移。尤其在現時今日，您的事業範疇更是取決於您的能力—交付產品的速度有多快、靈活度有多高、如何善用經驗、如何在動態的市場裡確

時間	研討會/課程名稱	研討會相關資料
		保可靠運作。這些能力可透過應用程式來實現。因此，當前許多企業的成敗往往取決於其使用的應用程式。這些程式不僅是您的員工的必備工具，還協助連結您與您的客戶、交付您的產品。它們同時也能在受到防火牆保護的大後方擔負資料開道的角色。絕大多數的網路攻擊都發生在應用程式層級，保護這些企業運作相關的功能，就意味著保護這些應用程式並讓它們正常運作。
2018/07/29	TDOH Conf 2018 Call for paper	【資安研討會】TDOH Conf 2018 Call for paper 收稿截止日期：2018 年 07 月 29 日(日) 主辦單位：TDOH 投稿報名連結： https://blog.tdohacker.org/2018/05/tdoh-conf-2018-call-for-paper.html?m=1 活動概要： 年度主題—駭客地下城 (Underground Hacking) 徵稿嘍！舉凡機器學習、資訊安全相關技術或研究、CTF 競賽經驗、社群參與或資訊安全相關經驗等各式題材皆歡迎您與我們一同分享；除上述所提及之類型外，其他資訊安全相關題材亦均可自由投稿。內容須基於資訊安全技術，可以是 Coding 技巧、工具使用對資安推廣與資安人才培育等等。 **正式活動日期為 9 月 29 日在左營蓮潭國際會館喔！
2018/08/01-08	107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - ICS/SCADA 資訊安全實務課程(台北) 課程時間：2018 年 08 月 01 日(三) - 08 月 08 日(三) 受訓地點：臺北 - 巨匠電腦 - 電腦教室 (臺北市公園路 30 號 3 樓)

時間	研討會/課程名稱	研討會相關資料
	訓 - ICS/SCADA 資訊安全實務課程(台北)	主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzM2 課程簡介： 本課程設計藉由 ICS/SCADA 資安威脅、弱點與風險之探討與研析，加以理解 ICS/SCADA 所面臨之風險外，透過 ICS/SCADA 資安事故處理研析與演練，讓學員學習 ICS/SCADA 資安事故處理實務，俾利關鍵基礎設施營運商對於關鍵資訊基礎設施保護人才之運用。ICS/SCADA 為因應近年來人機介面友善化與遠端操控等需求，系統內早已具備各種運算及通信功能，更因而成為駭客攻擊的對象；其中以關鍵基礎設施(CI)、關鍵資訊基礎設施(CII)內部之 ICS/SCADA 的資安事故更讓人重視，本會特聘各界處理 ICS/SCADA 資安事故之資深講師親臨現場，現身說法，透過案例解析與實務演練的方式，讓與會學員能有效的學習到理論與實務面上的知識。 課程大綱： 1. ICS/SCADA 資安威脅探討 2. ICS/SCADA 弱點與風險研析 3. ICS/SCADA 資安事故處理實務
2018/08/23	CLOUDSEC 2018	【資安研討會】CLOUDSEC 2018 日期：2018 年 08 月 23 日(四) 地點：台北國際會議中心(台北市信義區信義路五段 1 號) 主辦單位：趨勢科技 線上報名連結： https://www.cloudsec.com/tw/registration.html 活動概要： 數位轉型在即，全面連網的需求讓 IT 與企業成長的關

時間	研討會/課程名稱	研討會相關資料
		係更加緊密。運用 CLOUD 與 AI 提升生產力、Design-in-Security 降低風險、FINTECH 推動新型態金融服務，IT 為企業帶來更多新機會。而面對新平台、新技術、獲利導向的駭客心態，加上有限的資源與支援，都讓資安挑戰更加艱鉅。CLOUDSEC 八年來持續提供一個讓企業組織獲取國際新知與經驗交流的平台。今年的 CLOUDSEC 請到 ZDI (Zero-Day Initiative) 來台分享資安漏洞最新趨勢，邀請您共同體驗新技術、討論新應用、並解決資安問題。
2018/08/29-30 2018/09/05-06	107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程(第一梯)	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程(第一梯) 課程時間：2018 年 08 月 29 日(三) - 08 月 30 日(四)/2018 年 09 月 05 日(三) - 09 月 06 日(四) 受訓地點：臺北巨匠電腦 - 電腦教室 (臺北市公園路 30 號 3 樓) 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzQz 課程簡介： 課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務，俾利資訊安全產業與相關企業對於資安事故處理人才之運用。本課程邀請業界致力於資安事故處理與數位鑑識等專家共同指導，讓學員透過講師自身處理過的案例經驗中，了解各項資安事故發生後的處置手段，並接由數位鑑識相關專業講師教導如何保全事故後的數位跡證，透過理論與實務相輔佐的方式，讓學員能夠制定一套適用於各公司的資安事故緊急應變 SOP，往後遭遇資安事故時，便能即時應

時間	研討會/課程名稱	研討會相關資料
		對處變，更甚而從源頭進行預防。 課程大綱： 1.資安事故處理實務 2.數位鑑識處理實務
2018/09/13-14	107 年度新興資安產業生態系推動計畫 - 資安專業人才培育 - 資安法規與制度研析課程	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育 - 資安法規與制度研析課程 課程時間：2018 年 09 月 13 日(一) - 09 月 14 日(二) 受訓地點：中華民國資訊軟體協會 教育訓練室 (台北市大同區承德路二段 239 號 6 樓) 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzMy 課程簡介： 本課程設計除透過資訊安全法律規範與資訊安全案例之探討與研析，藉以學習資安法規之要求外，並由國際資安管理制度之探討與國際資安管理制度建置實務之演練，讓結業學員理解資安法規之要求事項與學習資安管理制度之規劃與建置實務俾利資訊安全產業與相關企業對於資安管理制度建置人才之運用。特邀請熟悉財金法、資訊法及工程法之現職律師與專擅科技法律的資深顧問現身說法，透過實際案例回顧，告知學員過往案例中因忽視法遵基礎與資安規範所造成的損害，並結合國內現有法規與國外資安相關管理制度和法規之比較讓學員的資安法規知識不僅限於適用國內法，更能拓展自身公司之產品與服務符合不同國家之資安法規制度。 課程大綱： 1.資訊安全法律暨案例研析 2.國際資安管理制度建置實務
2018/09/	107 年度新興	【資安訓練課程】107 年度新興資安產業生態系推動計

時間	研討會/課程 名稱	研討會相關資料
19-20 2018/09/ 26-27	資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程(第二梯)	畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程(第二梯) 課程時間：2018 年 09 月 19 日(三) - 09 月 20 日(四)/2018 年 09 月 26 日(三) - 09 月 27 日(四) 受訓地點：臺北巨匠電腦 - 電腦教室 (臺北市公園路 30 號 3 樓) 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzQ0 課程簡介： 課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務，俾利資訊安全產業與相關企業對於資安事故處理人才之運用。本課程邀請業界致力於資安事故處理與數位鑑識等專家共同指導，讓學員透過講師自身處理過的案例經驗中，了解各項資安事故發生後的處置手段，並接由數位鑑識相關專業講師教導如何保全事故後的數位跡證，透過理論與實務相輔佐的方式，讓學員能夠制定一套適用於各公司的資安事故緊急應變 SOP，往後遭遇資安事故時，便能即時應對處變，更甚而從源頭進行預防。 課程大綱： 1.資安事故處理實務 2.數位鑑識處理實務

第 4 章、2018 年 06 月份事件通報統計

本中心每日透過官方網站、電子郵件、電話等方式接收資安事件通報，2018 年 6 月收到通報計 4415 筆，以下為各項統計數據，分別為通報來源統計圖、通報對象統計圖及通報類型統計圖。

通報來源統計圖為各國遭受網路攻擊事件，屬於我國疑似遭利用發起攻擊或被攻擊之 IP，向本中心進行通報之次數，如圖 1 所示；通報對象統計圖為本中心所接獲之通報中，針對通報事件責任所屬國家之通報次數，如圖 2 所示；通報類型統計圖則為本中心所接獲的通報中，各項攻擊類型之筆數，如圖 3 所示。

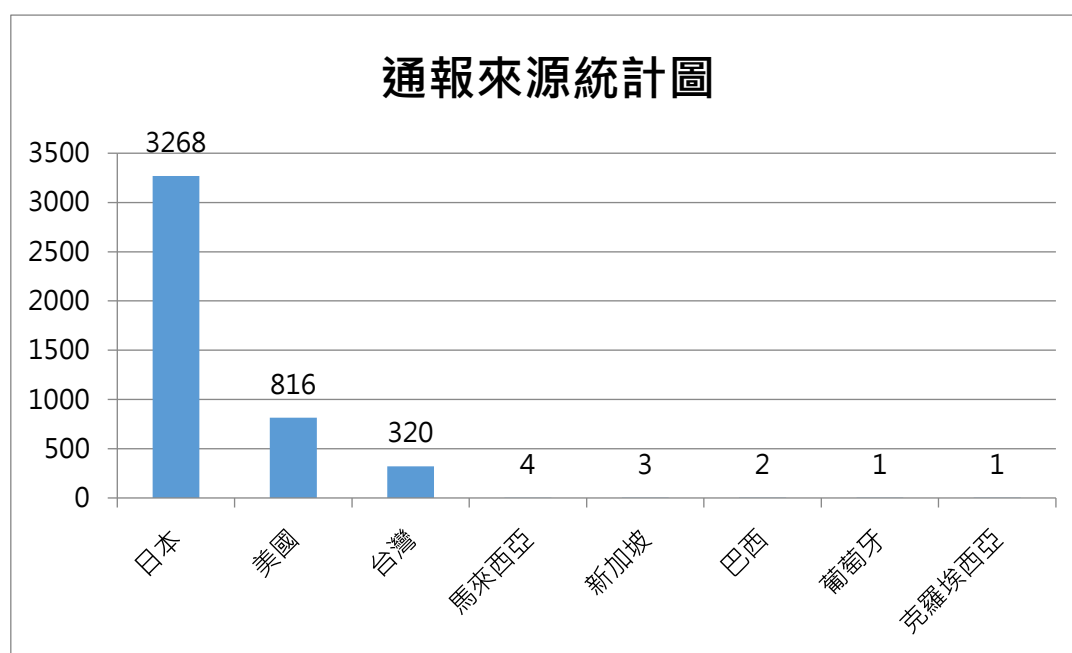


圖 1、通報來源統計圖

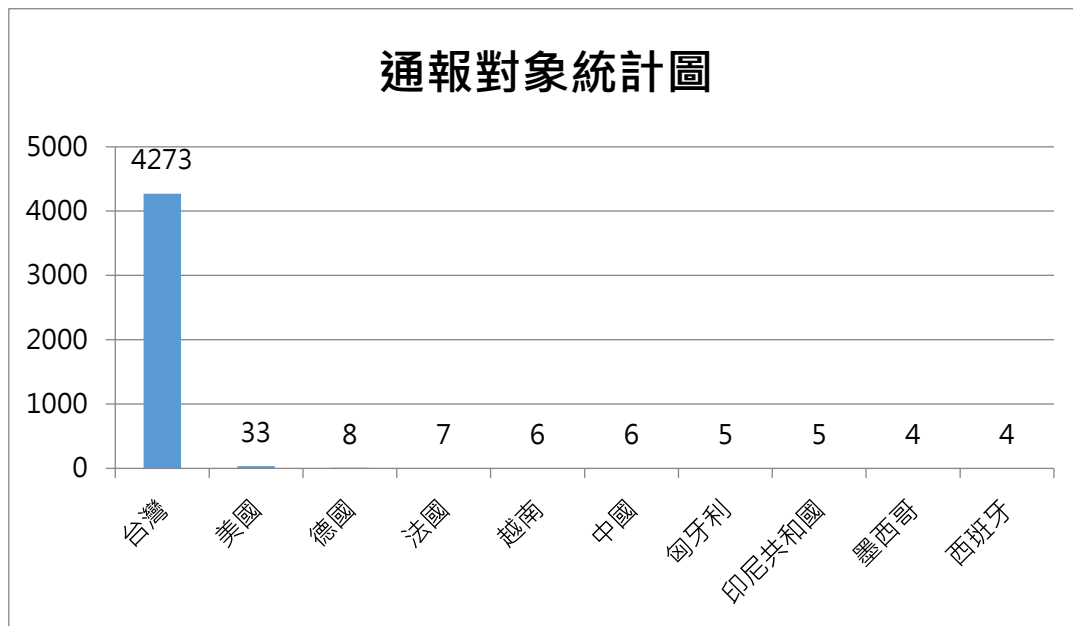


圖 2、通報對象統計圖

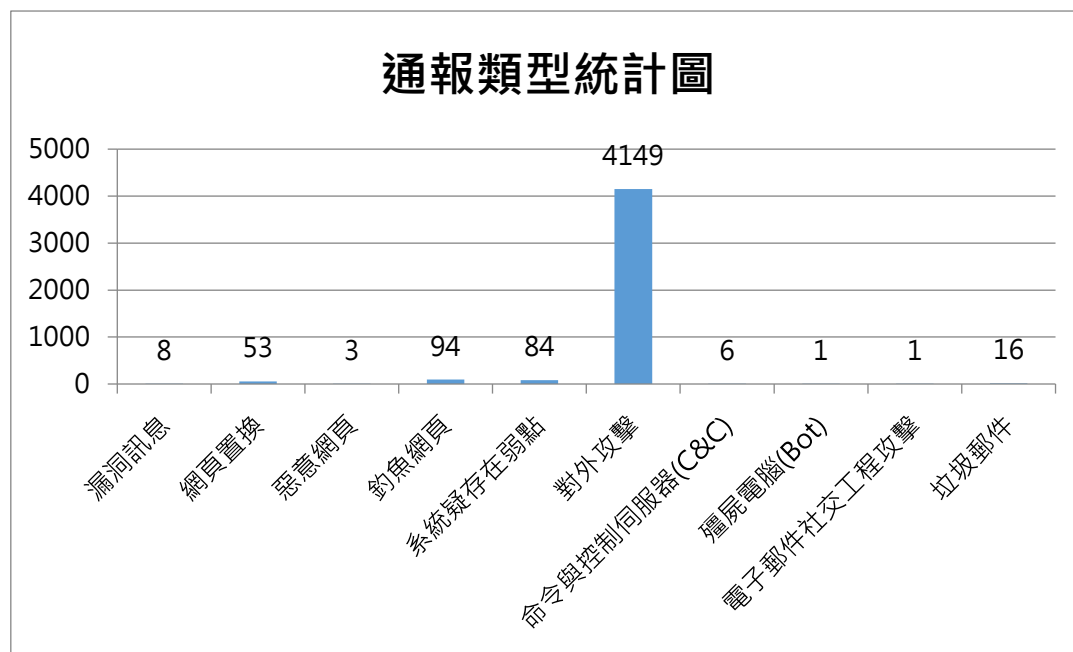


圖 3、通報類型統計圖

本月通報案件中，有網頁的任意檔案下載(Arbitrary File Download)漏洞，可經由該漏洞取得後端系統中的任意資料。

建議網頁程式中，檢查允許下載的路徑、檔名及副檔名。並於系統管控檔案可存取的系統權限，以免遭任意下載、存取資料，其中包含主機之敏感檔案。於事前修補相關弱點及漏洞，事發時立即處理，後續本中心仍持續提醒相關用戶，對於所收到之事件通報進行相關處理，以減少駭侵事件發生時所造成的損害。

發行單位：台灣電腦網路危機處理暨協調中心

(Taiwan Computer Emergency Response Team/Coordination Center)

出刊日期：2018 年 7 月 9 日

編輯：羅文翎、陳韋伶

服務電話：03-4115387

市話免付費服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官 網：<https://www.twcert.org.tw/>

粉絲專頁：<https://www.facebook.com/twcertcc>

資安電子報訂閱：<http://i-to.cc/S5HzJ>

線上電子報閱覽：<https://twcertcc.blogspot.tw/>

如有任何疑問或建議，歡迎您不吝指教。