TWCERT/CC 資安情資電子報

2018 年 10 月份

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team/Coordination Center

目錄

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、於 10 月 3 日舉辦「2018 台灣資安通報應變年會-企業無可避免的資安管理責任」

這次會議是 TWCERT/CC 成立以來所舉辦最盛大的資安研討會，今年參與人數多達 450 人左右，比起去年增加了 100 多名與會者，令人相當驚艷！代表越來越多人開始對資安重視，以及對 TWCERT/CC 的認識。

今年的會議是以企業無可避免的資安管理責任為主軸，本次研討會共有 11 場精彩議程，上午分別進行兩場 Keynote 及座談會，下午則分別以「電子商務資訊安全」及「資安事件應處策略」進行分場研討，另外，在會議議程中間休息時間，亦特別邀請到 9 家資安廠商/社群前來分享資安防護策略及資安治理理念，研討會場邊設有 15 家資安廠商/社群/單位，提供一個讓聽眾與廠商近距離接洽的機會，另外也有攤位集點換贈品及抽獎的活動。參與此場會議主要目的是，讓聽眾了解「資安防禦與管理之因應之道」、「如何自主建置資安事件應變團隊」、「資安通報的重要性及好處」，以及「面臨資安管理法之應對方式」。

在當今的網路世代，資安問題將愈來愈受重視，企業經營時，更應考量必要的資安防護，並制定完善的資安政策及通報應變標準作業流程，才能面對席捲而來的資安威脅與挑戰。通訊傳播委員會主委詹婷怡擔任貴賓致詞表示：「隨著重大資安事件愈來愈頻繁，國人應如何強化與改善資安防禦措施及資安緊急應變機制，國家也應建立資安聯防體系，並提升整體資安防禦能量，以因應瞬息萬變的資安威脅。」

第一位 Keynote 演講者行政院資安處副處長徐嘉臨亦特別針對「資通安全管理法」及其 6 個子法實施內容進行解說，包含各公務機

關、關鍵基礎設施提供者、公營事業、政府捐助之財團法人被賦予的責任，以完備資安防護與通報義務之法源基礎，作為後續推動國家資通安全工作之基石，確保國家安全與公共利益。

另外，此次特別邀請到國際上非常知名的資深資安專家 Adli Wahid 擔任第二位 Keynote 演講者，Wahid 先生以多年國際資安合作的經驗，分享自身在亞太網路資訊中心 (Asia Pacific Network Information Centre, APNIC)及資安事件應變小組論壇 (Forum of Incident Response and Security Teams, FIRST)協助各國家建置資安事件應變中心的心得，以及特別強調組織間在進行情資交流時應建立在彼此的信任之上，且應以共同建立穩健安全的網路環境為目標，互助合作，建立資安聯防體系。

上午時透過座談會的方式，邀請行政院資安處徐副處長擔任主持人，APNIC Adli Wahid、經濟部中小企業處主任秘書陳國樑、TWCERT/CC 主任陳永佳，以及奧義智慧創辦人吳明蔚擔任與談人，以「在面臨網路新時代資安威脅之因應對策」議題進行深入探討。

TWCERT/CC 期盼聽眾能藉由此場會議，提升自己的資安意識，並將所學的知識帶回企業，讓企業內部的資安防護體系及資安政策的建構上能更完善。

會後 TWCERT/CC 也收到各位對於此次研討會提供的建議，我們會精進與改善，未來讓我們一起期待 TWCERT/CC 帶給大家更好的服務以及更精彩的研討會！

簡報資料下載：
https://twcert-official-file.s3.hicloud.net.tw/10.3 可公開簡報.rar

2.2、協辦 TDOH Conf 2018

TWCERT/CC 於 2018 年 9 月 29 日協辦 TDOH Conf 2018，並於會中進行擺攤，推廣業務內容並宣導資安意識。會中 TWCERT/CC 羅文翎分析師發表議題「一頁式詐騙之資安風險面面觀」，探討一頁式詐騙之特色，以及 TWCERT/CC 在協處此類事件中所擔任的腳色。

TDOHacker 成立於 2013 年中，是當時一群對資安極具熱情的學生們所創立，期望利用社群的方式來推廣資訊安全、增加技術交流、改善台灣資安學習環境等。目前依舊耕耘著台灣資安人才培育的土壤，並且在全台各地與多所大專院校都有相關合作經驗和人手，是一個初具規模全國性校園資安社群。

TDOHacker 近年來已有數十場講座舉辦經歷，也協助過多個社群單位與教育單位舉辦講座、課程，並發展多個資安教育平台的專案。平常則舉辦許多小型活動熱絡資安社群間的交流，而從 2016 年開始舉辦如 TDOH - PIPE、Conf 等大型活動，致力於打造更完善的資訊安全學習環境。

2.3、申請並成為 CVE 編號管理者 (CNA)

本中心自 2018 年起參與美國 MITRE 之通用漏洞揭露(Common Vulnerabilities and Exposures, CVE®)計畫，已完成申請並成為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，刻正建置台灣漏洞紀錄 (Taiwan Vulnerability Note, TVN)平台，透過協助國內外廠商處理產品漏洞，以儘快完成漏洞緩解及修補，避免有心人士利用產品漏洞造成使用者遭駭之情況發生。

CVE 編號管理者 (CVE Numbering Authority, CNA) 為一志工組織，可為來自世界各國之國家 CERT、產業 CERT、研究機構、漏洞提報組織或廠商等。每個 CNA 都有不同的權責範圍，並有權限可以對權責範圍內之產品漏洞發布 CVE ID，以及後續對 CVE ID 的內容進行維護。

以上的努力，從安全、便利、效能三面向來推動資通安全，以逐步實現建構台灣網路安全環境之願景。

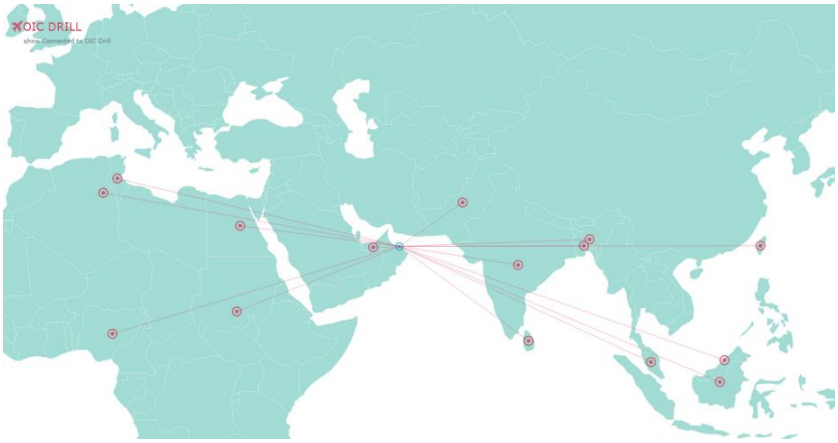
TWCERT/CC 漏洞揭露政策文件下載：
https://twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?id=65

2.4、參與 OIC-CERT 2018 年網路通報應變演練 (OIC Drill 2018)

本中心於 9 月 18 日獲邀，參與一年一度之伊斯蘭合作組織電腦

緊急事件回應小組 (the Organisation of The Islamic Cooperation – Computer Emergency Response Teams, OIC-CERT)2018 年網路通報應變演練 (OIC Drill 2018)，本年度之演練主題為「加密貨幣風險及緊急威脅 (Crypto-currencies Risks and Emerging Threats)」。

此次主辦單位為阿曼國家電腦緊急應變小組 (Oman National CERT, OCERT)，演練內容包含資安通報處置、惡意鑑識及資料情蒐等情境題，讓參與的 CERT 熟悉高風險資安威脅，以及應處方式。



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、新的 Hakai IoT 殭屍病毒針對 D-Link、華為及 Realtek 路由器及 IoT 裝置進行感染

資安專家近期發現一稱作 Hakai（源於日文中破壞之意），針對 IoT 裝置的殭屍網路病毒，有悄悄成長的趨勢。Hakai 的第一版是以已出現多年的 IoT 殭屍病毒 Qbot（也稱作 Gafgyt、Bashlite、Lizkebab、Torlus 或 LizardStresser）作為參考所開發，除複雜度較低，亦無活躍行為，第一次出現是在今年六月，由 NewSky Security 的資安專家所提出討論。

NewSky Security 的資安專家 Ankit Anubhav 指出，該病毒一開始似乎是想追求能見度及吸引大眾注意力，因此甚至把 Ankit 的照片作為殭屍網路 C&C 伺服器 (hakaiboatnet[.]pw)的首頁圖。

但從 7 月底起，資安專家觀察到 Hakai 開始積極入侵使用者裝置，到目前為止發現 Hakai 有能力入侵之裝置如下：

●含有 CVE-2017-17215 漏洞之華為 HG352 路由器

●支援 HNAP 協定之 D-Link 路由器

●使用含有 CVE-2014-8361 漏洞 Realtek SDK 之 IoT 產品及路由器

● 含有特定漏洞之 D-Link DIR-645 路由器 (https://www.exploit-db.com/exploits/38722/)

● 含有特定漏洞之 D-Link DSL-2750B 路由器 (https://www.exploit-db.com/exploits/44760/)

除利用上述漏洞，Hakai 本身亦具備高效率之 Telnet 掃描工具，因此只要目標裝置使用預設密碼或弱密碼，如 root、admin 及 1234 等，甚至可以不用透過漏洞入侵裝置就可取得裝置掌控權。

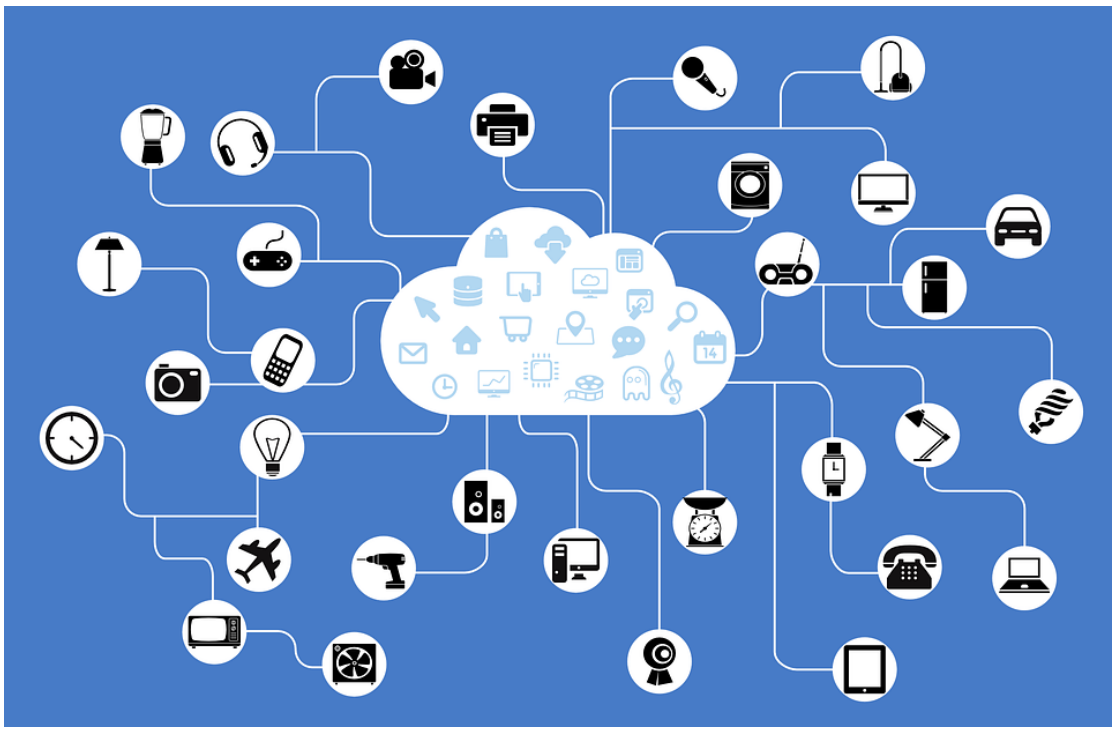
另資安專家發現，Hakai 的作者作風比以往來得低調許多，也把資安專家的照片從 C&C 伺服器中移除，這有可能跟近期另一病毒製造者 Nexus Zeta 因暴露過多個人資訊，而導致被逮捕的事件有關。

此外，資安專家發現有兩個新的 Hakai 變種病毒，分別是 Kenjiro 及 Izuku，也開始在網路中散播，其使用來散播病毒的漏洞如下：

- D-Link DSL-2750B – OS Command Injection
  (https://www.exploit-db.com/exploits/44760/)
- CVE-2015-2051
  (https://www.exploit-db.com/exploits/37171/)
- CVE-2017-17215
  (https://www.exploit-db.com/exploits/43414/)
- CVE-2014-8361
  (https://www.exploit-db.com/exploits/37169/)

TWCERT/CC 建議：

- 使用者若購買 IoT 或路由器等設備，需立即修改預設密碼，並設置中高強度之密碼，且定時進行軟韌體更新。
- 將相關 IoC 加入防火牆中。



資料來源：

https://www.zdnet.com/article/new-hakai-iot-botnet-takes-aim-at-d-link-huawei-and-realtek-routers/

https://www.intezer.com/elf-support-released-hakai-malware/

https://www.thedailybeast.com/newbie-hacker-fingered-for-monster-botnet

https://sidechannel.tempestsi.com/hakai-botnet-shows-signs-of-intense-activity-in-latin-america-724ffb84d5cb

3.1.2、金管會規範，金融業資產規模兆元以上需設立「資安長」

金管會副主委黃天牧於 9 月 6 日表示，金管會規定銀行業、保險業等都要設資安專責主管，若資產規模 1 兆元以上，則必須設「獨立」的資安長的專責主管，與資訊處分開，職位較高在協理以上。

他強調，金融被駭或系統發生故障，民眾對無法跨行提款的容忍度較低，一二分鐘都不應發生，金融屬國家重要基礎設施，應更強化資安風險控管。

金管會去年 12 月也已委託財金公司成立金融資安資訊分享與分析中心 (F-ISAC)，將銀行、證券、保險業納入聯防體系，其六大功能包括資安事件改善依據、協助資安事件應變、資安諮詢與教育訓練、情資研判分析、資安資訊分享、通報服務。截至今年 8 月底，已共有 281 家會員，提供警訊及報告逾 200 則。黃天牧亦表示，會根據業者提供的警訊及報告進行分析，以達成資安早期預警、應變及聯防機制，提升應變力與防護力。

資料來源：

https://www.chinatimes.com/realtimenews/20180906002449-260410

https://udn.com/news/story/7239/3352282

3.1.3、我國已建立資安學院，初批將招募 200 人

行政院資通安全處已於九月底正式成立「資安學院」，初期將招募、訓練約兩百位資安專業人才。

該學院並非另行成立實體的資安機構，而是統合目前坊間已有的資安訓練機構，將來希望擴大成立世界級的「資安研訓機構」。

資料來源：

http://news.ltn.com.tw/news/politics/paper/1229811

3.1.4、總統核定我國首部資通安全戰略報告

國家安全會議考量我國資安環境、戰略可行性及可執行性，提出了我國首部資安戰略報告，為數位國家、創新經濟奠定堅實基礎。

國家資通安全戰略報告-資安即國安電子檔下載網址：

https://www.president.gov.tw/File/Doc/588f1a08-5ea7-41df-b0d0-482a00b45322

資料來源：

https://www.president.gov.tw/issue/439

https://www.president.gov.tw/File/Doc/588f1a08-5ea7-41df-b0d0-482a00b45322

3.1.5、弱密碼導致 Google 帳號遭竊，造成個資及財務損失數百萬元

刑事局今年 7 月初接獲報案，民眾帳戶內存款遭盜轉一空，損失合計 200 多萬元，經偵辦後逮捕 8 名嫌犯，並持續清查被害人數。

嫌犯利用民眾把電話號碼作為 Google 帳號及密碼的習性，以暴力猜解方式破解不特定民眾 Google 帳號，登入 Google 雲端取得被

害人存放於雲端的個人及金融資料，再利用社交工程，向銀行客服變更聯絡電話為人頭電話，並接收網路銀行的動態密碼以登入被害人帳戶，將帳戶內金額盜轉至其他人頭帳戶，再由車手進行提領。

資料來源：

https://www.cib.gov.tw/news/Detail/35282

http://news.ltn.com.tw/news/society/breakingnews/2542802

https://www.chinatimes.com/realtimenews/20180906001701-260402

3.2、駭客攻擊事件及手法

3.2.1、英國航空公司遭駭，38 萬筆客戶詳細資訊外洩

日前加拿大航空才爆發 App 資料遭未經授權的存取，迫使該公司鎖定其所有的 170 萬帳戶，且影響了 20,000 名客戶。

如今英國航空公司亦遭駭客入侵，38 萬筆客戶個人和信用卡資訊被攻擊者竊取，被盜資料不包括旅行或護照細節。

該公司在其網站上發布資料洩露通知，該安全漏洞影響範圍從 2018 年 8 月 21 日 22:58 到 2018 年 9 月 5 日 21:45，包括在網站和

App 上預訂的客戶個人和財務細節。

英國航空公司已啟動內部調查並通知警方和有關當局，並正在調查從網站和 App 竊取的客戶資料。該航空公司確認該駭侵行為已得到解決，其服務現在正常運作。

英國航空公司正在與受影響的客戶進行溝通，並建議可能受到駭侵事件影響的客戶更改密碼並選擇一個獨特且高強度的密碼以及與其銀行或信用卡供應商進行聯繫。

隱私權倡導者和安全專家認為，由於新的歐洲 GDPR 資料保護法，公司可能面臨巨額罰款。

資料來源：
https://www.bleepingcomputer.com/news/security/british-airways-loses-customer-payment-card-data-in-breach/
https://securityaffairs.co/wordpress/75980/data-breach/british-airways-hacked.html
https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

3.2.2、Apple 知名 App「Adware Doctor」竊取用戶瀏覽紀錄，用戶請儘速刪除

Apple 的 Mac App Store 中一個非常受歡迎的知名 App，旨在保護其用戶免受廣告軟體和惡意軟體威脅，卻在未經使用者同意的情

況下秘密竊取使用者瀏覽紀錄，並將其發送到中國大陸的伺服器。

該 App 名為「Adware Doctor」，Mac App Store 排名第一的付費 App，也是該商店第四大最受歡迎的付費 App，售價 4.99 美元，並定位為防止惡意軟體和惡意檔案感染使用者的 Mac 的最佳 App。

然而，Twitter 帳號為@privacyis1st 的資安研究人員在近一個月前檢測到 Adware Doctor 的可疑間諜軟體行為，並且上傳關於如何洩露用戶瀏覽器歷史紀錄的概念驗證影片展示。

研究人員向蘋果公司展示 Adware Doctor 在此期間的可疑活動，然而即使 Apple 在一個月前接獲警告，卻沒有立即對該 App 採取任何行動。該 App 來自名為「Yongming Zhang」的開發人員，仍在 Mac App Store 中活躍。

研究員隨後與前 NSA 員工 Patrick Wardle 調查了 Adware Doctor，深入了解該 App 後在部落格文章表示 App 迴避 Apple 的沙箱並隱蔽地收集用戶的瀏覽器歷史紀錄，然後將其轉移到中國大陸的伺服器，公然違反 Apple 的開發者指南。

根據 Wardle 的說法，Adware Doctor 透過流行的網路瀏覽器，包括 Chrome、Firefox 和 Safari 收集用戶的敏感資料，主要是用戶存取或搜索過的所有網站，然後將這些資料發送到由 App 製造商運營的中國大陸伺服器 http:// yelabApp[.]com/。

Wardle 表示，一般而言，反惡意軟體或反廣告軟體工具需要合法存取用戶的檔案和目錄。例如，掃描它們以查找惡意程式碼，但是一旦用戶點擊允許 Adware Doctor 對於用戶主目錄權限的請求，就可以對所有用戶的檔案進行全權存取。所以除了檢測和清理廣告軟體，也同時收集和洩露任何用戶檔案。

根據 Wardle 的貼文，Adware Doctor 逃脫 Apple 的 App 沙箱並調用與流行的 Web 瀏覽器相關的行程，包括 Safari、Chrome 和 Firefox，然後將紀錄資料壓縮為 ZIP 存檔，透過調用

sendPostRequestWithSuffix 方法進行滲透將其上傳到伺服器。

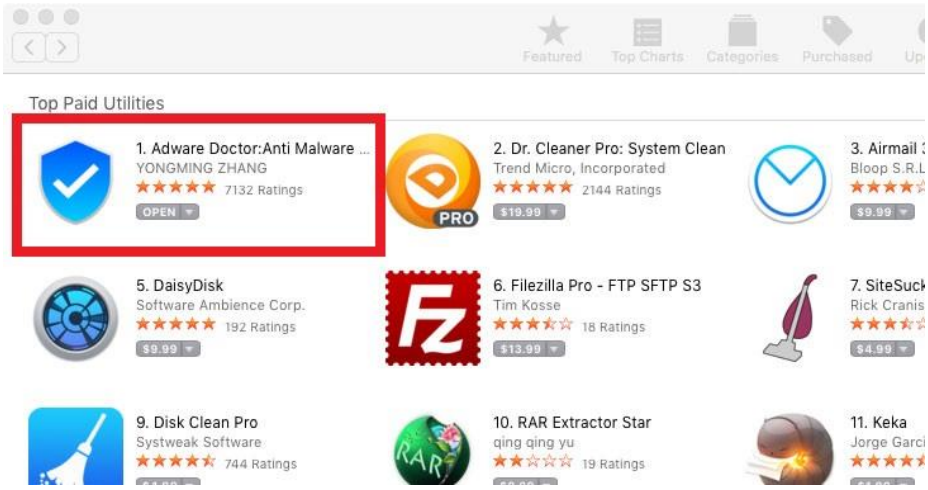
而 Malwarebytes 的 Mac 和行動安全總監 Thomas Reed，他的公司正在監控自 2015 年以來該開發商的活動。Thomas Reed 指出，Adware Doctor 最初被命名為「Adware Medic」，其設計明顯是為了模仿 MalwareBytes 在 2015 年的「AdwareMedic」App。

兩年前在 App Store 上發現了一款一樣名為 Adware Medic 的 App，而真正的同名 App 則被刪除，MalwareBytes 檢測到這一點，並聯繫 Apple，該 App 被從商店中刪除，但很快被一個名為 Adware Doctor 的相同應用程序取代，並成為 Mac Store 最高收入的實用 App。

由於該 App 未經用戶同意收集用戶資料而違反了眾多 App 商店規則和指南，並且繞過 Apple 的沙箱保護措施，因此幾週前 Wardle 就此問題與 Apple 聯繫，一開始沒有見到有採取任何措施。

後續在 Wardle 的部落格文章被幾家媒體採訪後，Apple 終於從 Mac App Store 中刪除了 Adware Doctor，以及開發者的其他 App「AdBlock Master」。

此外，從 Adware Doctor 用戶收集資料的中文伺服器目前處於離線狀態得知，可能是因為該 App 已受到媒體關注，已經下載了 Adware Doctor 的用戶強烈建議儘快從系統中刪除該 App。



資料來源：

https://thehackernews.com/2018/09/mac-adware-removal-tool.html
https://securityaffairs.co/wordpress/76011/hacking/Apple-removes-adware-doctor.html
https://twitter.com/privacyis1st/status/1031428304543395840
https://objective-see.com/blog/blog_0x37.html
https://blog.malwarebytes.com/threat-analysis/2018/09/mac-App-store-Apps-are-stealing-user-data/

3.2.3、駭客針對 Jaxx 錢包用戶進行網路釣魚，詐取 backup phrase

Jaxx 是知名的加密貨幣錢包，支援多種類型的硬幣，包括比特幣和乙太幣等，在桌面和行動平台上的下載量超過 120 萬。由加拿大區塊鏈新創公司 Decentral 所有。

至少一個星期前，Jaxx 加密貨幣錢包網站被發現一個偽造版本，提供惡意連結誘騙用戶洩露保護虛擬資金專屬的「backup phrase」(用於回復並取得錢包掌握權之字串密碼)。

Flashpoint 的安全研究人員在接獲網路犯罪活動引起的一連串感染警告後，於 8 月 30 日發現了這問題。然而從攻擊者網域名稱的建立日期來看，該活動可能已於 8 月 19 日開始。

除了註冊可能容易與合法的 Jaxx 網站、jaxx[.]io 及使用 Cloudflare 混淆的網域名稱外，攻擊者還會逐行複製原始版本。

Flashpoint 在一份報告中解釋，對於偽造變種的 Jaxx 網站，用戶幾乎沒有產生懷疑，因為攻擊者在將受害電腦安裝合法錢包軟體時遇到了點麻煩。

同時，在 macOS 或 Windows 平台下，惡意軟體會以 Java 檔(JAR)和.NET 應用程式的格式在後台默認安裝。如果有人要求提供錢包的行動版本，他們就會收到合法檔案。

Flashpoint 資深惡意軟體研究員 Paul Burbage 說，Windows 惡意軟體可以將檔案洩露到命令控制伺服器 (C&C)，以及下載 KPOT

Stealer 和 Clipper，這兩個惡意軟體也在俄羅斯地下論壇上銷售。Clipper 的目的是監控數位錢包地址的剪貼板，並用攻擊者控制的其他數位錢包地址替換它們。

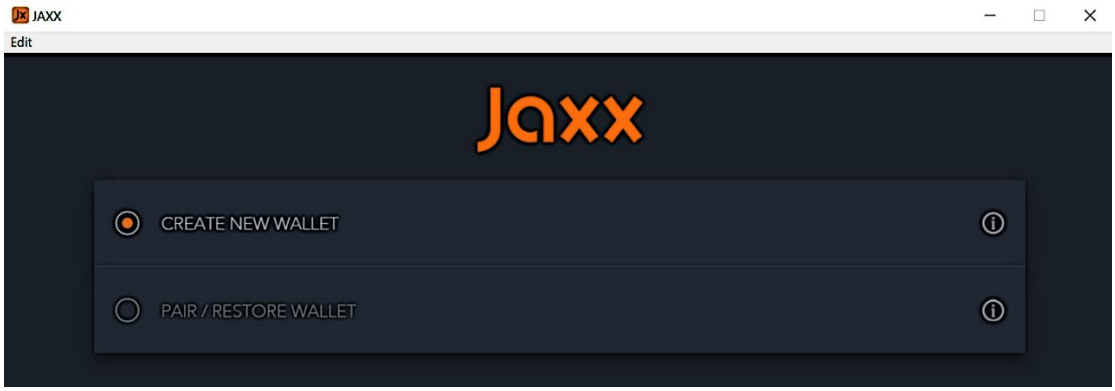
KPOT 竊取器從本地驅動竊取訊息。macOS JAR 檔也指向俄羅斯的犯罪者，因為它是使用俄語 IDE（整合開發環境）DevelNext 編譯的。Burbage 表示能夠確定該偽造網站是由俄羅斯 VPS 提供商 hostland[.]ru 託管的。

當用戶運行 JAR 檔案時，他們會看到一條訊息，通知出現無法建立新錢包的技術問題。接下來即被引導到一個請求 Jaxx 錢包「backup phrase」的應用程式畫面。這實際上是解密錢包以訪問數位資金的密碼。

Flashpoint 表示，當「backup phrase」被洩露給攻擊者的網路伺服器，受害者會收到另一個混合的俄語和英語錯誤訊息「Server is not available. Try again in 4 hours」。

啟動.NET 應用程式的 Windows 用戶會獲得一個聲稱是 Jaxx 錢包測試版的 Google Docs 位址檔案連結。安裝後，惡意軟體會將本機端所有 txt、doc 及 xls 檔案傳送到 C&C 伺服器，相當有可能是攻擊者搜索加密貨幣錢包地址。接下來就是下載合法的 Jaxx 軟體、KPOT 竊取程序和 Clipper 惡意軟體。

Flashpoint 表示，Cloudflare 已暫停該偽造網站服務，Jaxx 也迅速採取應對偽造網站的支援行動，以保護其客戶群。Burbage 指出這是針對 Jaxx 錢包用戶的社交工程活動，沒有任何跡象表明 Jaxx 軟體或其系統中存在漏洞或安全漏洞。



資料來源：

https://www.bleepingcomputer.com/news/security/cybercriminals-go-phishing-for-jaxx-wallet-users/

https://www.flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/

3.2.4、推送通知服務 Feedify 遭駭，成為 Ticketmaster 和英國航空公司駭侵事件間接加害者

Feedify 為線上網站提供推送通知服務。企業可以在其網站上嵌入 Feedify JavaScript 函式庫，在獲得用戶同意接收桌面通知的權限後，網站發布新內容時，即可以透過 Feedify 後端將通知推送給各自的用戶。

雖不若 Feedify 網站之聲稱該公司擁有超過 4,000 名客戶，然而使用 PublicWWW 服務進行的搜索顯示，此特定函式庫仍已嵌入在 250 到 300 個站點中。

推送通知服務 Feedify 近期成為 Magecart 的網路犯罪行為的最新受害者，最近被認定為 Ticketmaster 和英國航空公司駭侵行為背後的罪魁禍首。

根據化名「Placebo」的線上資安研究人員稱，該公司的一個 JavaScript 文件被惡意程式碼感染，用以竊取信用卡的詳細資訊。Placebo 的調查結果得到了 RisqIQ 資安研究員 Yonathan Klijnsma 和資安專家 Kevin Beaumont 的證實。

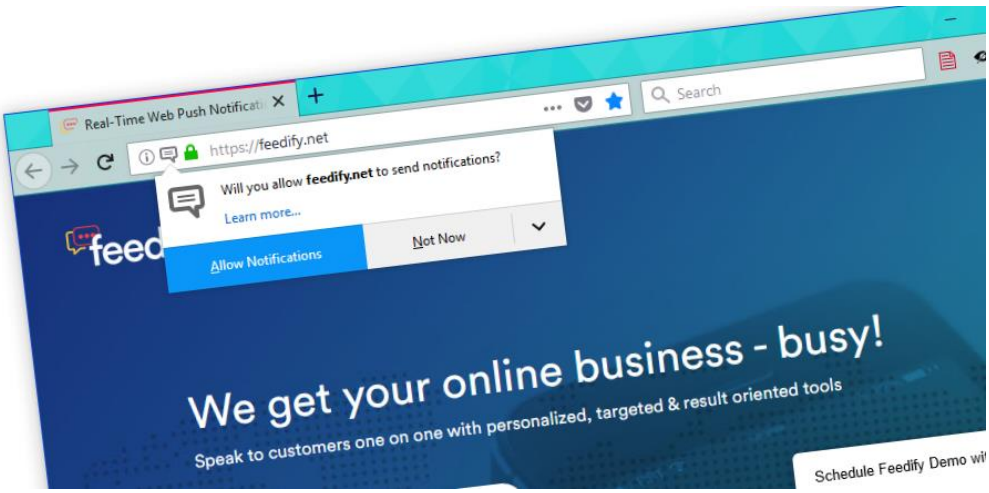
Magecart 組織將惡意程式碼添加到 Feedify 客戶嵌入其網站名為 feedbackembad-min-1.0.js 的檔案中。Klijnsma 表示，透過 RisqIQ 的 PassiveTotal 平台獲得的資料使他的公司能夠記錄駭客何時更改該特定文件的內容。

Klijnsma 表示從紀錄發現，約 2018 年 8 月 17 日星期五於格林威治標準時間 16:51:01 開始受到 Magecart 的影響。資安研究員 Placebo 表示，他於 9 月 11 日通知 Feedify，惡意程式碼在同一天即被刪除。

但是在過了 24 小時內，同一個檔案遭到入侵和編輯，再次被夾帶 Magecart 程式碼。在 Feedify 進行干預以刪除程式碼後，Magecart 內部人員第三次將其程式碼重新添加到檔案中。

Feedify 背後的駭客團隊 Magecart 自 2015 年以來保持活躍。前兩年，該集團主要針對 Magento 線上商店。他們會使用舊的漏洞入侵電子商務網站並放置收集信用卡詳細資訊的惡意程式碼，這些程式碼會將資訊傳送到他們自己的伺服器上。

該組織在 2017 年末和 2018 年初逐漸改變策略，將目標瞄向主要服務，尤其託管 Web 基礎設施。最著名的是當他們駭侵了 Inbenta 聊天服務並在無數網站上部署了竊取密碼的程式碼以及 Inbenta 聊天小套件，其中最大的是 Ticketmaster。



資料來源：

https://www.zdnet.com/article/feedify-becomes-latest-victim-of-the-magecart-malware-campaign/

https://securityaffairs.co/wordpress/76239/cyber-crime/magecart-compromised-feedify.html

https://unwire.pro/2018/09/12/british-airways-breach-hackers-tactics-ticketmaster-uk/news/

https://twitter.com/ydklijnsma/status/1039605816737722368

https://twitter.com/Placebo52510486/status/1039585013057118209

https://github.com/gwillem/magento-malware-scanner/blob/master/corpus/frontend/magentocore.js

https://publicwww.com/websites/https%3A%2F%2Fmagentocore.net%2Fmage%2Fmage.js/

3.2.5、Magecart 肆虐，電子零售商 Newegg 加入受害者行列

繼英國航空公司和 Feedify 漏洞事件後，其背後 MageCart 的專用以竊取信用卡的惡意腳本再次發動侵襲，這次是針對最大的線上電子零售商之一 Newegg。

Newegg 是一個相當知名的電子零售商，2016 年的業務規模為 26.5 億美元，由於 Newegg 是電子組件、電腦和硬體領域最大的線上零售商之一，受此漏洞影響的受害者數量可能非常龐大。

資安研究員 Yonathan Klijnsma 在 RiskIQ 博客文章中在這一波攻擊指出，Alexa 網站排名顯示，Newegg 在美國名列第 161 名最受歡迎的網站，Newegg 估計每月接待超過 5000 萬訪客，在整整一個月的瀏覽過程中，可以假設這次駭侵事件影響受害者人數規模相當大。

根據 Volexity 和 RiskIQ 的聯合分析，Magecart 駭客組織設法滲透到 Newegg 網站並竊取了在 2018 年 8 月 14 日至 9 月 18 日期間輸入信用卡資料的所有客戶的信用卡詳細資訊。

Veloxity 在他們的報告中表示，透過其全球感測器 (Sensor)網路，在 2018 年 8 月 16 日三天後在 Newegg 網站確認攻擊。基於從其感測器網路獲得的資料，攻擊者有可能提前開始攻擊。

RisqIQ 和 Volexity 發布兩份報告詳細說明 MageCart 腳本如何在一個多月的時間內注入 Newegg 網站，同時悄悄竊取客戶的付款資訊。

根據報導，攻擊者於 8 月 13 日註冊了一個名為 neweggstats[.]com 的網域名稱。類似於 Newegg 的合法網域名稱 newegg[.]com，並獲得了 Comodo 為其網站發布的網域名稱 SSL 憑證。

一天後，該組織將竊取資料的腳本程式碼注入 Newegg 網站的付款處理頁面，攻擊者建立之 neweggstats[.]com 被用作收集從 Newegg 網站竊取的信用卡詳細資訊的儲存網站。

Veloxity 進一步表示，這些攻擊於 8 月 16 日左右在 Newegg 的網站上發起。 當用戶在 Newegg 購買商品時，他們會被要求輸入他們的送貨資訊，然後繼續到他們輸入付款資訊的第二頁。在結帳流程的第二頁，Newegg 從客戶收集付款資訊，注入了 15 行的 MageCart 腳本。

當頁面加載時，腳本會將自己綁定到用戶輸入信用卡詳細資訊後按下的按鈕。按下此按鈕時，腳本將獲取表單的內容，將其轉換為 JSON，然後將其上載到 https://neweggstats[.]com/GlobalData/ 的網頁。

當然這個 neweggstats.com 網站並不歸 Newegg 所有，而是由攻擊者操作。這使得他們可以竊取在網站遭到駭客攻擊的月份內從 Newegg 購買商品的客戶的信用卡詳細資訊。然而對於用戶而言，完全不得而知其駭侵行為，就像沒有發生任何事情一樣。

Klijnsma 在推特上發布了一些可以使像 MageCart 這樣的腳本

較難竊取付款細節的付款表單和提交流程的配置方法。

Newegg 已經開始向他們的客戶發送電子郵件，為駭侵事件道歉並解釋發生的事情。根據 Newegg Danny Lee 發送的電子郵件，該公司將建立一個關於此駭侵事件的常見問題解答，並在 9 月 21 日之前將其發布在他們的網站上。

資料來源：
https://www.bleepingcomputer.com/news/security/newegg-credit-card-info-stolen-for-a-month-by-injected-magecart-script/
https://thehackernews.com/2018/09/newegg-credit-card-hack.html
https://www.volexity.com/blog/2018/09/19/magecart-strikes-again-newegg/
https://www.riskiq.com/blog/labs/magecart-newegg/
https://twitter.com/ydklijnsma/status/1042463653121814528

3.2.6、資安專家於 Google Play 發現數個假冒金融 App 從 Android 用戶獲取信用卡資料

據 ESET 的 Lukas Stefanko 報導，在官方 Android Google Play 商店中發現並刪除了 6 個偽造的金融類型 App，假扮銀行和加密貨幣交換 App 用以信用卡資料和登錄憑據的網路釣魚。

假冒的 Android App 將自己偽裝成奧地利加密貨幣交易所

Bitpanda 的官方 App，並假扮來自瑞士、英國、紐西蘭、澳大利亞和波蘭的銀行。

這些惡意 App 於 2018 年 6 月被放在 Google Play，已經被下載並安裝在超過一千種不同的 Android 設備上，直到 Google 發現了它們的真正目的並將其刪除。

雖然所有的 App 在上傳到官方 Android 商店時都使用了不同的設計和開發者名稱，但 Stefanko 在他們的程式碼中發現了相當相似之處，以得出皆來自於相同的詐騙攻擊者。

為了對受害者的登錄憑據和信用卡支付資料進行網路攻擊，偽造 App 使用的表單旨在要求目標受害者填寫敏感資料並將其發送給攻擊者的服務器。

用以網路釣魚的表單在設備啟動 App 後即會顯示，並且在成功將目標的敏感資料發送給攻擊者後，他們向受害者顯示「thank you」或「congratulations」的訊息，然後自行退出。

Stefanko 建議所有已安裝有該 Android App 的用戶，應立即卸載，並更改密碼和信用卡密碼，且檢查銀行帳戶是否有可疑交易。

●TWCERT/CC 建議，若想避免成為利用冒充官方金融服務的偽造 Android App 網路釣魚攻擊受害者，可以採取的最關鍵步驟就是安裝從專屬金融機構網站連結的正版 App，切勿任意下載安裝來路不明之第三方 App，以免遭駭客利用。

資料來源：
https://news.softpedia.com/news/fake-finance-Apps-phish-credit-card-data-from-android-users-522793.shtml
https://www.welivesecurity.com/2018/09/19/fake-finance-Apps-google-play-target-around-world/
https://www.helpnetsecurity.com/2018/09/19/bogus-finance-Apps/

3.2.7、AdGuard 遭受暴力嘗試攻擊，已重設所有使用者密碼

AdGuard 是跨 Android、iOS、Windows 及 Mac 平台的知名廣告攔截器，在全球擁有超過 500 萬用戶，是最著名的廣告攔截器之一。

該公司的首席技術官 Andrey Meshkov 於 9 月 21 日宣布已重置所有用戶密碼，起因為近期一名未知攻擊者試圖透過猜測密碼登錄用戶帳戶，該公司在遭受暴力攻擊後做出此一決定。

Meshkov 表示，攻擊者利用其他公司遭到入侵後遭暴露在外的電子郵件和密碼，這種將偷到的帳號密碼來入侵受害者的其他網路帳

號的攻擊類型被稱為撞庫攻擊或帳密填充攻擊 (credential stuffing attacks)。

AdGuard 首席技術官表示，攻擊者在攻擊中成功獲得了一些用於儲存廣告攔截器設定的 AdGuard 帳戶，但不知道攻擊者究竟存取了哪些帳戶，也不清楚攻擊者試圖對這些帳戶做些什麼，但該系統並沒有被攻破。

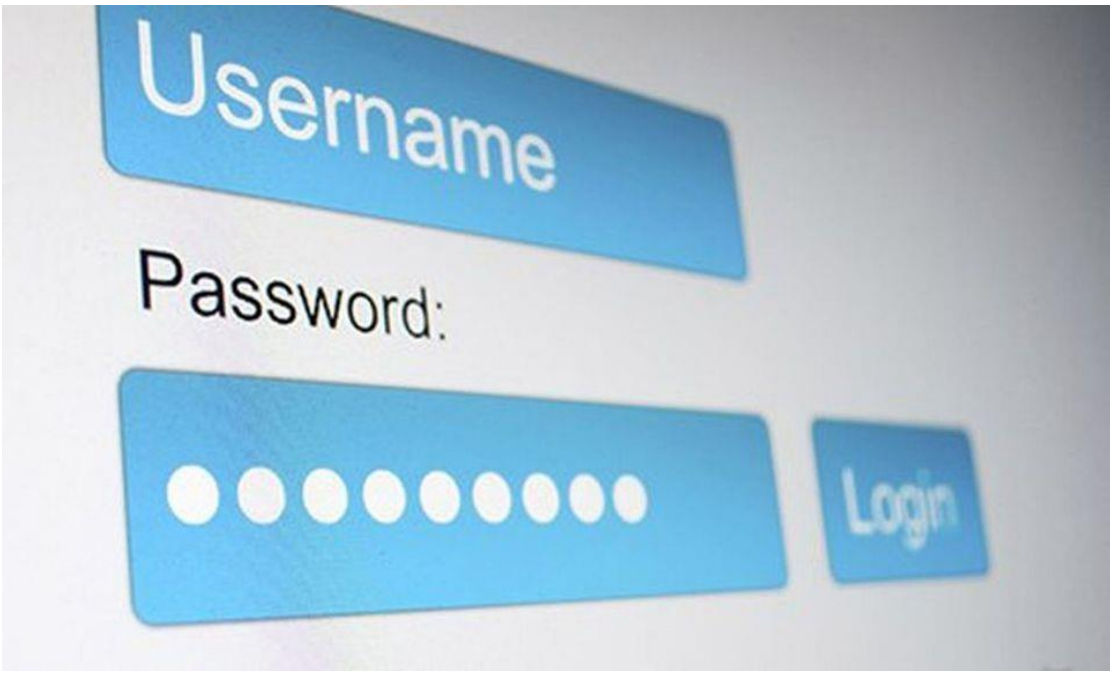
Meshkov 表示，儲存在 AdGuard 資料庫中的所有密碼都是加密的，因此無法檢查已知洩漏的資料庫中是否存在任何密碼。這就是為什麼該公司決定重置所有用戶的密碼的原因。

該公司表示，AdGuard 已連接到資安專家 Troy Hunt 設置的外洩通知資料庫「Have I Been Pwned」API，以便當用戶配置的新密碼已在其他網路服務中被外洩時，AdGuard 系統會向他們發出警告。

AdGuard 執行官還透露，該公司在其速率限制系統在密碼猜測階段發現了大量失敗的登錄嘗試後發現了該攻擊，大多數攻擊都已停止，但有些攻擊是成功的，這通常發生在攻擊者幸運在首次登錄嘗試期間猜測到正確組合時。

Meshkov 表示，AdGuard 未來將使用更嚴格的規則來選擇密碼，並打算在將來支援雙因素身分驗證。

●TWCERT/CC 建議，AdGuard 使用者如接獲重設密碼信件通知，務必確認信件來源，並應使用官方重設密碼服務，切勿輕易點選信件連結，且不同網路服務應使用不同之密碼，以免遭駭客利用。



資料來源：

https://www.zdnet.com/article/adguard-resets-all-user-passwords-after-credential-stuffing-attack/

https://techcrunch.com/2018/09/20/adguard-resets-all-user-passwords-after-account-hacks/

3.2.8、日本再傳交易所虛擬貨幣遭竊，約損失 6000 萬美元

日本虛擬貨幣交易所 Tech Bureau 旗下平台 Zaif 的伺服器在 9 月 14 日 17:00 到 19:00 之間的兩個小時內遭駭客攻擊。

該交易所在 9 月 20 日表示，在 9 月 17 日檢測到伺服器問題，第二天 9 月 18 日確認駭客攻擊後在第一時間已暫停 Zaif 存款及提領交易，並通知主管機關及警方。

Zaif 表示，駭客從其熱錢包中偷走了比特幣、比特幣現金和 MonaCoin，三者價值總計 67 億日元（約合 5967 萬美元）。

熱錢包是將貨幣資料存放在網際網路。駭客可以透過網路獲取存取權限，一般認為相較而言，與利用離線的方式將虛擬貨幣儲存在類似 USB 的硬體裝置的「冷錢包」更容易遭受駭客攻擊。

在被盜的 5967 萬美元（67 億日元）中，3780 萬美元是比特幣（5,966 比特幣），近 2000 萬美元（22 億日元）屬於母公司 Tech Bureau，而 4000 萬美元（45 億日元）屬於交易所的客戶。

Tech Bureau 在聲明中表示，拒絕談論該起事件發生的細節，除已請當局進行調查，未來也將制定相關的措施，讓用戶不再受駭客所影響。Tech bureau 也正向其他交易所協調融資五十億日圓，做為用戶賠償準備。

日本主要的虛擬貨幣交易平台 Coincheck 在今年年初就曾遭到駭客入侵，有 5.23 億個新經幣 (XEM)被盜轉，使得日本金融廳(Financial Services Agency, FSA)介入調查。

分析師 Joseph Young 於 9 月 21 日在推特發文指出，目前所有被攻擊的主流交易所，均為日韓交易所（Bithumb、Zaif、Coincheck 及 Cointrail），更說各國政府與安全機構均表示，這四所交易所的安全系統都很糟糕，而目前在歐美的交易所，如 Coinbase、幣安及 Kraken 等，仍未被攻擊過。

資料來源：

https://www.reuters.com/article/us-crypto-currencies-japan-cybercrime/japan-hit-by-another-cryptocurrency-heist-60-million-stolen-idUSKCN1M001K
https://news.bitcoin.com/japanese-regulated-exchange-zaif-hacked-btc/
https://www.zdnet.com/article/zaif-cryptocurrency-exchange-loses-60-million-in-july-hack/
https://www.darkreading.com/threat-intelligence/japanese-cryptocurrency-exchange-hit-with-$60m-theft/d/d-id/1332855
https://www.securityweek.com/japan-digital-currency-exchange-hacked-losing-60-million

3.2.9、SHEIN-時尚購物網站遭駭，650 萬用戶資料外洩

美國線上時尚零售商 SHEIN，總部位於 Brunswick 北部，成立於 2008 年，目前全球 80 多個國家最大的線上時裝零售商之一，該網站最初旨在為女性生產「實惠」和時尚的服裝。

該公司近期承認，在不知名的駭客竊取了近 650 萬客戶的個人身分資訊（personally identifiable information, PII）之後，該公司遭遇了嚴重的資料洩露。

SHEIN 上週末透露，其伺服器已成為今年 6 月開始的「協同犯罪網路攻擊」的目標，直到 8 月 22 日該公司意識到該潛在的盜竊行為為止。

此後不久，該公司掃描駭客可能再次滲入並利用的伺服器以刪除所有可能的後門入口點， SHEIN 向客戶保證，該網站現在可以安全使用。

雖然有關此事件的詳細資訊很少，但線上零售商透露，惡意駭客設法竊取了在其網站上註冊的 642 萬客戶的電子郵件地址和加密密碼憑證。

該公司表示，駭侵行為始於 2018 年 6 月，並持續到 2018 年 8 月初，約 642 萬客戶受到影響，該公司強調通常不會在其系統上儲

存任何信用卡資訊，並且目前沒有證據表明其客戶的任何信用卡資訊都來自其系統。

若該公司沒有信用卡詳細資訊被盜，那麼線上零售商應該不是受到最近影響了包括 Ticketmaster、British Airways 和 Newegg 在內的一系列 Magecart 網路攻擊。

●TWCERT/CC 建議：

1. SHEIN 用戶近期如接獲更改密碼之電子郵件，務必確認信件來源，切勿任意點選或下載郵件中之連結或附件，並應透過官方線上服務變更密碼，且不同網路服務應保持使用不同密碼之習慣，以免遭駭客利用。

2. 如有信用卡資料遭盜疑慮，務必確認近期交易情況，並主動聯繫所屬銀行或信用卡公司。

資料來源：

https://thehackernews.com/2018/09/shein-data-breach.html

https://securityaffairs.co/wordpress/76541/data-breach/shein-security-breach.html

www.shein.com/datasecurity

3.3、軟硬體漏洞資訊

3.3.1、CA 公布 Project & Portfolio Management、Release Automation、Unified Infrastructure Management 產品瑕疵，企業客戶請關注修補進度

CA Technologies 前身為組合國際電腦股份有限公司(Computer Associates Inc)，就大型主機 (Mainframe)、分散式、虛擬化、雲端運算等異質 IT 環境，研發管理和保護技術方案，供應自動化及負載平衡相關服務，經分析三款特定軟體，計有 9 項中、高風險缺陷，系統恐受遠端攻擊，例如：PPM 因輸入值過濾欠佳，易遭 XSS 與 SQL 隱碼攻擊，且 XOG 功能模組處理特製 XML 外部 entity 時，恐讓駭客伺機發動請求偽冒並觸及機敏資訊，另 SSL 密碼以明文無保護方式儲存；至於版本部署工具 Release Automation 則因物件反序列化錯誤而導致任意程式碼執行事件；負責基礎架構一致性的 UIM，竟內建 Hard Coded 長密碼詞組與密鑰，且對於檔案存取行為疏於身分認證，危及帳號安全和資料完整性；CA 公司已釋出對應修補方式，使用上述產品之企業宜檢視安裝版本及修補進度。

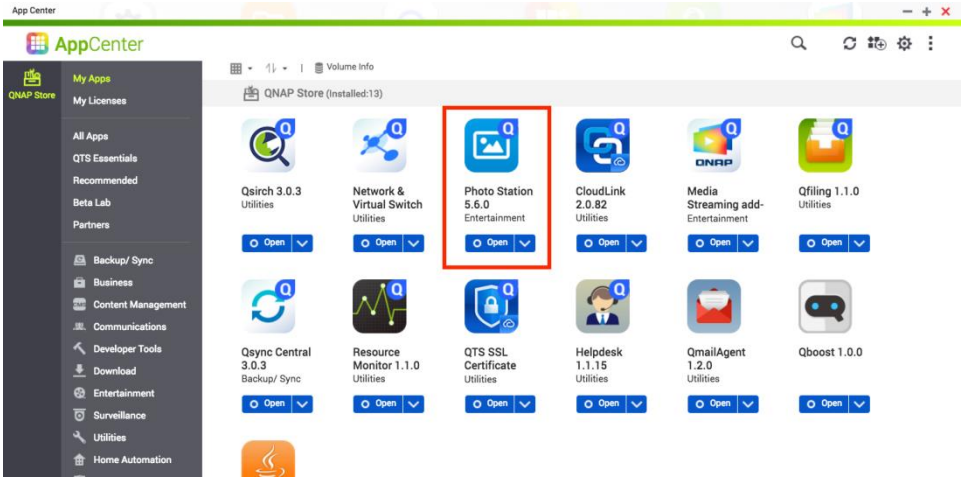
資料來源：

https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180829-02--security-notice-for-ca-unified-infrastructure-mgt.html

https://securitytracker.com/id/1041591

3.3.2、QNAP 改善照片時光屋 Cross-site Scripting 弱點

國內 NAS 大廠威聯通旗下商品 Photo Station，功能為增刪管理 NAS 內影像檔，並支援進階搜尋與臉部偵測，經分析，具中度危險漏洞，因輸入值未妥善檢驗，容許駭客循網頁介面注入程式碼，發動跨站台腳本攻擊，上述事件皆影響 NAS 共同用戶系統安全，QNAP Systems 已針對相關瑕疵升級 Photo Station，可直接下載。



資料來源：

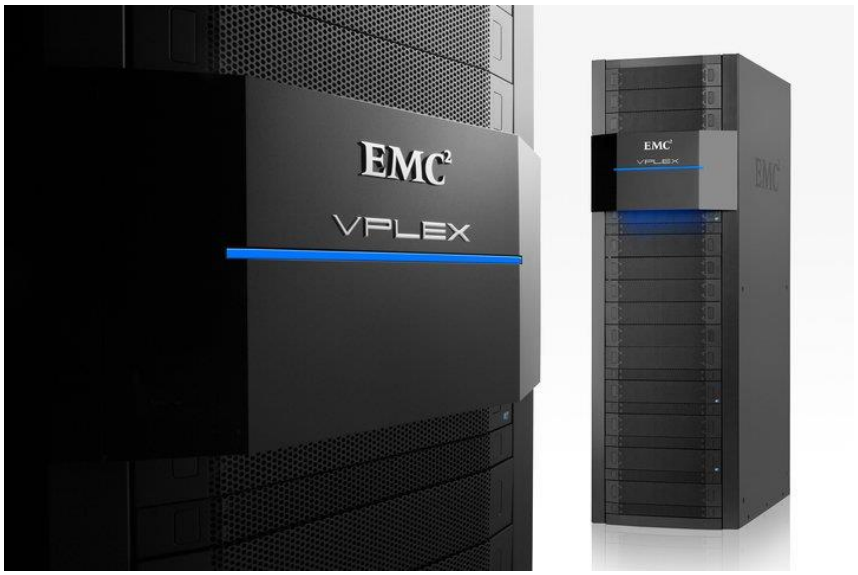
https://www.qnap.com/zh-tw/security-advisory/nas-201808-23

https://exchange.xforce.ibmcloud.com/vulnerabilities/148881

3.3.3、Dell EMC 修補 VPlex GeoSynchrony 檔案存取安全缺陷

Dell EMC 旗下 VPlex 係儲存虛擬化平臺，能整合相異儲存架構，而 VPlex 硬體控制器是多核心刀鋒裝置，每組 VPlex 控制器運行作業系統 GeoSynchrony，搭配 Witness 自動執行負載平衡、故障處理，經研究指出，Witness 因檔案存取許可權設定不符安全規範，造成重

要系統檔案不設防，攻擊者可遠端接觸 VPN 組態值，若佔據中間人位置，甚可偽造、控制兩端點之 VPN 連線流量，干擾通訊隱私，戴爾公司業已升級 GeoSynchrony 軟體，相關資源無公開下載點，企業客戶需洽原廠授權代理商始可獲得。



資料來源：

https://Appuals.com/dell-emc-vplex-geosynchrony-users-requested-to-upgrade-to-v6-1-to-avoid-insecure-file-permissions-vulnerability/

https://seclists.org/fulldisclosure/2018/Sep/10

3.3.4、友訊無線路由器 DIR-846 韌體破綻招致 RCE

D-Link 開發 WIFI 網路產品(型號：DIR-846)，近日被 galaxylab 的研究者 bigbear 測試出韌體漏洞，只要駭客獲得管理者權限帳號連線 Cookies，可製作惡意 HTTP Request，針對網路狀態斷層掃描(SetNetworkTomographySettings)進行參數設定，且探勘命令以 root 權限，成功實施 Remote Command Execution，由於官方修補尚無音訊，設備用戶請從密碼強度與白名單方式強化資安管控。

資料來源：

https://github.com/PAGalaxyLab/VulInfo/blob/master/D-Link/DIR-846/RCE_0/D-Link%20DIR-846%20RCE.md

https://raw.githubusercontent.com/PAGalaxyLab/VulInfo/master/D-Link/DIR-846/RCE_0/dlink2.pn

https://raw.githubusercontent.com/PAGalaxyLab/VulInfo/master/D-Link/DIR-846/RCE_0/dlink1.png

3.3.5、Tor 火速升級瀏覽器，敉平 0-Day 漏洞：Bypass NoScript 套件

Tor 源於洋蔥路由器 (The Onion Router)縮寫，1990 年代中期由美國海軍研究機構開發，以保護情報通訊，核心技術「洋蔥路由」如同洋蔥一般，層層加密保護，隱藏用戶真實 IP，避免網路監控及流量分析的追蹤手段，實踐匿名通訊自由，而 Tor Browser 係由 Mozilla Firefox ESR 修改而成，此開源瀏覽器支援 Windows、Mac OS X、Linux、Unix、BSD、Android 等平台，特色是中斷連網後，自動刪除 Cookie、歷史紀錄等敏感資料，近日甫經 Zerodium 披露其 0-Day

探勘技術，可針對 Tor 瀏覽器運用之 NoScript 擴充插件發動攻擊，蓄意變更 Content-type 表頭成為 JSON 格式，斲喪 XSS 反制能力，令惡意 JavaScript 突破 NoScript 白名單限制，此嚴重缺失未及註冊 CVE 編號，然 The Tor Project Inc.已修補並推出新版 Tor Browser，而 NoScript Classic 亦改良完畢。

資料來源：

https://twitter.com/Zerodium/status/1039127214602641409

https://noscript.net/getit#classic

3.3.6、防火牆 ModSecurity 核心規則集 Paranoia Level 1 疏於防禦 SQL injection

標題所列 Paranoia Level 非指偏執狂、妄想症等精神醫學用語，而是追求安全防護的執著，未免部分讀者誤解，故不直譯，ModSecurity 係普遍應用之公開網頁程式防火牆 (WAF)，可搭配 OWASP (Open Web Application Security Project)維護的免費核心規則集 (Core Rule Set, CRS)，初始設計為 Apache HTTP Server

之模組，後續發展成 HTTP 封包過濾軟體，亦支援 Microsoft IIS、NGINX 等伺服器平台，其商用 CRS 維護者 Trustwave SpiderLabs 研究室，測試出在 PL1 等級狀態，輸入特定語法表述結構{`函數名稱`sql 指令敘述}，能成功發動 SQL injection，破壞資料庫機密性與完整性，證實 Core Rule Set PL1 具有嚴重瑕疵，而前述 SQL injection 手法在 Core Rule Set PL2 則被阻擋，因 Paranoia Level 2 包含 1 條規則 (ID: 942150, SQL Injection Attack)，可攔截同類隱碼攻擊。

資料來源：

https://github.com/SpiderLabs/owasp-modsecurity-crs/issues/1167

https://nvd.nist.gov/vuln/detail/CVE-2018-16384

3.3.7、微軟證實 FragmentSmack 衝擊多版 Windows 作業系統

今年初，芬蘭 Aalto 大學網路通訊系研究員 Juha-Matti Tilli，分析出 SegmentSmack（惡意 TCP 封包）、FragmentSmack（惡意 IP 封包）二項漏洞影響 Linux，並表示 macOS 與 Windows 亦具類情。8 月中 Linux 釋出修補同時，微軟未作回應，至上週始證實，現行 Windows 及 Server 確有 FragmentSmack 弱點，攻擊者利用 IP 片斷封包重組演算法特性，大量送出偽造片段資料，且無法重組為正常 IP 封包型態，累積 TCP/IP Stack，導致 CPU 無法應付如此複雜之資料運算，故使用率飆高至頂，形成 DoS，然而真正的危機是分散式

FragmentSmack 所建構之大規模殭屍網路侵襲，即眾所皆知的 DDoS。桌機用戶罕見受此威脅，然伺服器管理員就該關注此事，儘快檢查設備更新進度，若無法即時獲得更新，可暫時以 netsh 命令防禦 FragmentSmack 攻擊。

資料來源：

https://www.internetnewsblog.com/windows-systems-vulnerable-to-fragmentsmack-90s-like-dos-bug/

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180022

3.3.8、論壇軟體 MyBB 開發團隊，升級新版以消彌 SQL Injection & XSS 風險

國外免費開源的論壇軟體 MyBB，使用 PHP 及 MySQL 開發，據 StefanT 與 Numan OZDEMIR 研究結果，測試不同危險程度漏洞，MyBB Group 亦釋出最新版 MyBB 1.8.19，解決相關軟體缺失，因 MyBB 程式界面對輸入字串疏於檢驗，故填入惡意 Email 欄位資料，無法辨識錯誤電郵地址格式，甚至能發動 SQL Injection 危害資料庫；而 Visual Editor 亦有類似缺點，駭客能注入<script>alert ('XSS 入侵')</script>或相似手法，遂行常駐跨站台腳本攻擊；且使用者控制介面，對附件管理權責限制控管有誤，附件檔案易遭受非法存取。

資料來源：
https://blog.mybb.com/2018/09/11/mybb-1-8-19-released-security-maintenance-release/

3.3.9、華碩電競路由器 GT-AC5300 韌體遭披露 5 項弱點

Republic of Gamers (ROG)品牌，係華碩開發之無線電競路由器系列，其 ROG Rapture GT-AC5300，號稱採用 Aiprotection 及趨勢 IPS 等安全技術，然其 8 月釋出之韌體版本 3.0.0.4.384_32738，近日被披露數項漏洞，發送單行請求「GET / HTTP/1.1\r\n」即可製造 DoS；而參數錯漏字 timestap，恐因 NULL pointer 反參照而中斷服務；惡意設定變數 sh_path0 為過長字串，可探勘函數 ej_select_list()內指令 strcpy()，觸發緩衝區溢位；而利用 CSRF 手法，可透過 start_Apply.htm 重設密碼；最後藉惡意請求控制 AppGet.cgi 介面 hook 參數，可達成 XSS 效果，目前暫無安全更新。

資料來源：

https://github.com/PAGalaxyLab/VulInfo/blob/master/ASUS/buffer_overflow/ASUS%20GT-AC5300%20stack%20overflow.MD

https://nvd.nist.gov/vuln/detail/CVE-2018-17023

3.3.10、留神 4GEE WiFi Mini 數據機 driver 資料夾，恐用以接管 Windows

據 ZeroDayLab 研究員 Osanda Malith Jayathissa 分析，英國行動網路電信業者 EE (Everything Everywhere)，販售之 4GEE WiFi Mini 數據機，因 Alcatel 開發過程之軟體瑕疵，導致 ServiceManager.exe 所在資料夾，兼有 Unquoted Service Path 及權限控管疏漏，數據機驅動程式所在資料夾 (C:\Program Files (x86)\Web Connecton\EE40\BackgroundService\)，其增刪讀寫完整權力竟設定給一般帳號，故駭客無需管理者身分，可直接以同檔名惡意程式，覆蓋既有 ServiceManager.exe，主機重開機後旋即生效，由於探勘技術門檻甚低，攻擊者不費吹灰之力，便可於本機取得系統權限並恣意操作，安裝後門或間諜軟體，該事件列為高度威脅，使用

者一旦循USB連接PC與Modem，則瞬間弱化Windows環境安全，業者已公布升級韌體，用戶宜儘速更新。

資料來源：

https://www.youtube.com/watch?v=hOjMMOiYMzs&feature=youtu.be

https://osandamalith.com/2018/09/17/ee-4gee-mini-local-privilege-escalation-vulnerability-cve-2018-14327/

3.3.11、整數溢位漏洞 Mutagen Astronomy 正潛藏多種 Linux 版本

天文異變 (Mutagen Astronomy)這個充滿科幻味的詞，並非討論外太空議題，而是針對最新發現之 Linux kernel 嚴重瑕疵所命名，據 Qualys 研究室指出，Red Hat、CentOS、Debian 等 Linux Kernel，其函數 create_elf_tables()計算過程恐觸發整數溢位，導致變數 items 成為負值，干擾後續堆疊指標精確性，從而指向錯誤記憶體位置，上述事態危及 2007 年 7 月 19 日至 2017 年 7 月 7 日 Kernel 版本，且僅限 64 位元系統環境，因攻擊技術需搭配足夠位址空間，駭客於本機入侵得手，將獲致 root 權限，目前僅有臨時解決方法 (回溯 1 年以前修補)，而探勘驗證程式碼已釋出，治本性修補仍在研發中，使用者宜關注最新進度。

資料來源：

https://meterpreter.org/cve-2018-14634/?cn-reloaded=1

https://www.zdnet.com/article/new-linux-mutagen-astronomy-security-flaw-impacts-red-hat-and-centos-distros/

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
2018/10/20	ISDA 白帽入門讀書會 WarGame 輕鬆學資安 Part 2	【資安訓練課程】ISDA 白帽入門讀書會 WarGame 輕鬆學資安 Part 2 日期：2018 年 10 月 20 日 (六) 13:30-17:30 地點：台北市中正區重慶南路一段 77 號 3 樓-4 線上報名連結： https://reg.shield.org.tw/info.php?no=39 報名時間：2018 年 10 月 5 日至 18 日 活動議程： 13:30-14:00 入場 14:00-17:00 初階關卡 Part 2 17:00-17:30 FAQ 活動概要： 本次活動適合入門學員參加，從資安遊戲 WarGame 中學習網頁攻擊技巧，繼續學習不同面向的攻擊技巧，從中了解防禦知識。想學資安卻不知道從何開始？讓

時間	研討會/課程名稱	研討會相關資料
		ISDA 帶您從 WarGame 穿越資安世界的大門。
2018/11/2、11/3、11/10、11/17、11/30	行政院資安學院 物聯網資安培訓課程（中華電信）	【資安訓練課程】行政院資安學院 物聯網資安培訓課程（中華電信） 日期：2018/11/2、11/3、11/10、11/17、11/30 (9:10-16:20，每天 6 小時) 地點：中華電信學院 (新北市板橋區民族路 168 號，近板橋捷運站) 主辦單位：經濟部工業局 參與對象：物聯網資安研發人員、檢測人員、負責物聯網管理的資安人員 課程報名連結： https://www.accupass.com/event/1810080517061259295030 課程費用：原價 3 萬元，工業局補助學費 50% 課程簡介： 隨著物聯網科技與應用蓬勃發展的同時，資安也面臨了前所未有的挑戰。行政院資安處於今年九月起成立資安學院，推動金融與物聯網資安人才培訓。中華電信基於多年物聯網資安服務、平台與研發實務經驗，特別淬鍊精華，整理資安防護要點，規劃專業培訓課程，從法規、技術、到資安攻防，全方位協助您提升資安專業能力。
2018/11/3、11/10、11/17、11/23、11/30	行政院資安學院 金融資安培訓課程（中華電信）	【資安訓練課程】行政院資安學院 金融資安培訓課程（中華電信） 日期：2018/11/3、11/10、11/17、11/23、11/30 (9:10-16:20，每天 6 小時) 地點：中華電信學院 (新北市板橋區民族路 168 號，近板橋捷運站) 主辦單位：經濟部工業局 參與對象：金融相關機關中高階主管、資安管理人員 課程報名連結： https://www.accupass.com/event/1810080421341299737238

時間	研討會/課程名稱	研討會相關資料
		課程費用：原價 3 萬元，工業局補助學費 50% 課程簡介： 隨著金融科技蓬勃發展的同時，資安也面臨了前所未有的挑戰。 行政院資安處於今年九月起成立資安學院，推動金融與物聯網資安人才培訓。 中華電信基於多年金融領域資安服務實務經驗，特別淬鍊精華，整理資安防護要點，規劃專業培訓課程，從法規、管理到技術全方位協助您提升資安專業能力。
2018/11/3	白帽菁英萌芽計畫〈入門一〉ISDA 白帽駭客巡迴(國立東華大學)	【資安訓練課程】白帽菁英萌芽計畫〈入門一〉ISDA 白帽駭客巡迴 巡迴第 8 站：國立東華大學 日期：2018 年 11 月 3 日（六）13:00-18:00 地點：國立東華大學 線上報名連結： https://reg.isda.org.tw/info.php?no=28 報名時間：2018 年 9 月 29 日至 10 月 29 日 報名注意事項： 活動對象為各大專院校與高中職等在學之學生，學生名額優先，學生家長與教育人士請出示證件。 活動議程： 13:00~13:30 活動簡介 13:30~14:20 WarGame#1 LV1 14:30~15:20 WarGame#1 LV2 15:30~16:20 WarGame#1 LV3 16:30~17:00 FAQ 活動概要： 只要有心，人人都可以成為白帽駭客，ISDA 團隊將帶領各位學員來挑戰極限！ 在這個萬物皆可駭的年代，該學習什麼樣的技能，與培

時間	研討會/課程名稱	研討會相關資料
		養正確的觀念，來成為「白帽菁英」的一員。本次活動中，ISDA 的專業資安教育訓練團隊，將透過 WarGame 實作教學，傳授您擁有基本的白帽駭客技能，取得進入資安界與駭客圈的入場券。 白帽菁英萌芽計畫，將舉辦於全台灣八個縣市，落實推廣全台灣的資安教育活動。
2018/11/10-2018/11/18	認證系統安全從業人員 SSCP 輔導班	【資安訓練課程】認證系統安全從業人員 SSCP 輔導班 日期：2018 年 11 月 10 日至 11 月 18 日（假日班） 活動地點：台北市復興南路一段 390 號 2 樓 主辦單位：財團法人資訊工業策進會 數位教育研究所數位人才培育中心 課程資訊及報名： http://taipei.iiiedu.org.tw/course/security/187-asq902.html 承辦人：羅小姐 電話： (02)66316586 E-Mail：showyann@iii.org.tw 課程簡介： 培養學員具通過 SSCP 認證考試之實力 培養學員具實務從事資安工作之知識與能力 培養學員具備網路通訊安全、封包分析、監控與惡意程式碼防治、風險處理、災害復原等實用知識與應用
2018/11/13	資安趨勢與企業因應管理 (可抵內稽)	【資安訓練課程】資安趨勢與企業因應管理 (可抵內稽) 日期：2018 年 11 月 13 日 9:30~16:30 上課地點：新竹市光復中學-國中部東側教學大樓推廣中心 203 教室 (位於 2 樓沙發區旁) 新竹市光復路二段 153 號 2 樓 主辦單位：電腦稽核協會 (CAA) 課程資訊及報名： http://www.caa.org.tw/education.asp?type=65+IT+Audit%E8%88%87%E8%B3%87%E8%A8%8A%E

時間	研討會/課程名稱	研討會相關資料
		6%B2%BB%E7%90%86#ITG1642018 課程費用：NT$3,300 元，含稅、上課教材、茶點 (全天課程含午餐)，電腦稽核協會及內稽協會會員可享會員價 3,000 元 課程大綱： 1.新科技與資安新議題 2.資安新聞與案例 3.駭客攻擊趨勢與防範作為 4.安全管理與日誌保存 5.關鍵資訊基礎設施防護概論 筆試測驗 16:30~ 課程簡介： 因應新科技帶來的資安威脅，企業如何管理作為，使用最近的資安案例說明企業如何防範與因應，導入日誌保存讓資安事件調查。
2018/11/15	網站安全與稽核簡介(Ⅰ) (可抵內稽)	【資安訓練課程】網站安全與稽核簡介 (Ⅰ) (可抵內稽) 日期：2018 年 11 月 15 日 9:30~16:30 上課地點：電腦稽核協會訓練教室 (位置圖：http://www.caa.org.tw/map.asp) 110 台北市信義區基隆路 1 段 143 號 2 樓之 2 (捷運市政府站 1 號出口) 主辦單位：電腦稽核協會 (CAA) 課程資訊及報名： http://www.caa.org.tw/education.asp?type=55+ISACA%E5%B0%88%E6%A5%AD%E7%B3%BB%E5%88%97#ISP102-a2018 課程費用：原價 3,300 元，含稅、上課教材、茶點 (全天課程含午餐)，電腦稽核協會及內稽協會會員可享會員價 3,000 元 課程大綱：

時間	研討會/課程名稱	研討會相關資料
		1.ISO 27001:2013 改版增加加密之控制領域、PCI/DSS 對加密之要求與網站安全因應之道 2.程式碼簽章 (Code Signing)簡介 3.TLS 安全機制與各類 SSL 憑證 4.電子簽章法解析 5.由 DigiNotar CA、Comdo CA 遭受攻擊事件、CNNIC/WoSignCA 被部分瀏覽器移出 CA 信賴清單/Symantec 濫發憑證事件、GlobalSign 出包與各瀏覽器大廠之要求，談如何慎選 CA 與 SSL 憑證、Code Signing 憑證 6.上述主題之網站安全檢測與稽核 筆試測驗 16:30 ~ 課程簡介： 新版個資法施行後加重罰則與駭客攻擊手法翻新，對於組織之網站安全維護帶來衝擊，ISO 27001:2013 版新增加有關加密之領域，本課程從個資法、電子簽章法解析、ISO 27001:2013 改版等之標準與法規遵循、DigiNotar CA 與 Comodo CA 遭受攻擊等資安事件、技術與管理等多面向，討論如何稽核網站安全，並能針對企業如何慎選 CA 與善用 SSL 憑證、程式碼簽章、網頁圖像保護技術、網站弱點掃瞄及滲透測試，來因應網站安全議題。
2018/11/19	網路與系統安全實務查核 (可抵內稽)	【資安訓練課程】網路與系統安全實務查核 (可抵內稽) 日期：2018 年 11 月 19 日 9:30~16:30 上課地點：電腦稽核協會訓練教室 (位置圖：http://www.caa.org.tw/map.asp) 110 台北市信義區基隆路 1 段 143 號 2 樓之 2 (捷運市政府站 1 號出口) 主辦單位：電腦稽核協會 (CAA) 課程資訊及報名： http://www.caa.org.tw/education.asp?type=65+IT

時間	研討會/課程名稱	研討會相關資料
		+Audit%E8%88%87%E8%B3%87%E8%A8%8A%E6%B2%BB%E7%90%86#ITG1252018 課程費用：原價 3,300 元，含稅、上課教材、茶點 (全天課程含午餐)，電腦稽核協會及內稽協會會員可享會員價 3,000 元 課程大綱： 1.網路安全的威脅與攻擊模式簡介 2.網路及網路安全基礎架構簡介 3.防火牆及入侵防禦安全管理 4.作業系統安全查核重點 5.資訊安全管理與技術框架實務分享 筆試測驗 16:30 ~ 課程簡介： 針對目前網路安全威脅與攻擊模式進行說明，透過實務網路與系統安全查核經驗，帶領學員學習面對防火牆、入侵防禦及相關作業系統安全控管及查核技巧，並於課程中展示相關查核工具，以提昇學員相關資安與稽核專業知識。
2018/11/23	網站安全與稽核簡介(II) (可抵內稽)	【資安訓練課程】網站安全與稽核簡介 (II) (可抵內稽) 日期：2018 年 11 月 23 日 9:30~16:30 上課地點：電腦稽核協會訓練教室 (位置圖：http://www.caa.org.tw/map.asp) 110 台北市信義區基隆路 1 段 143 號 2 樓之 2 (捷運市政府站 1 號出口) 主辦單位：電腦稽核協會 (CAA) 課程資訊及報名： http://www.caa.org.tw/education.asp?type=55+ISACA%E5%B0%88%E6%A5%AD%E7%B3%BB%E5%88%97#ISP102-b2018 課程大綱：

時間	研討會/課程名稱	研討會相關資料
		1.個資法施行衝擊與網站安全因應之道 2.網頁圖像保護 3.原碼檢測、網站弱點掃瞄與滲透測試簡介 4.網站 DDoS 攻擊防護 5.網站及後端主機所需防火牆及 IDS/IPS 簡介 6.以上主題之檢測與稽核 筆試測驗 16:30 ~ 課程簡介： 新版個資法施行後加重罰則與駭客攻擊手法翻新，對於組織之網站安全維護帶來衝擊，ISO 27001:2013 版新增加有關加密之領域，本課程從個資法、電子簽章法解析、ISO 27001:2013 改版等之標準與法規遵循、DigiNotar CA 與 Comodo CA 遭受攻擊等資安事件、技術與管理等多面向，討論如何稽核網站安全，並能針對企業如何慎選 CA 與善用 SSL 憑證、程式碼簽章、網頁圖像保護技術、網站弱點掃瞄及滲透測試，來因應網站安全議題。
2018/11/24-12/8	認證資訊系統安全專家 CISSP 輔導班	【資安訓練課程】認證資訊系統安全專家 CISSP 輔導班 日期：2018 年 11 月 24 日至 12 月 8 日 活動地點：台北市復興南路一段 390 號 2 樓 主辦單位：財團法人資訊工業策進會 數位教育研究所數位人才培育中心 課程資訊及報名： http://taipei.iiiedu.org.tw/course/security/247-asq901.html 課程費用：35 小時 / 56000 元，優惠價 32000 元 承辦人：羅小姐 電話： (02)66316586 E-Mail：showyann@iii.org.tw 課程簡介： 1.培養學員具通過 CISSP 考試之實力。 2.培養學員具評估及建置企業整體資訊安全管理之知

時間	研討會/課程名稱	研討會相關資料
		識與能力。 3.培養學員具備基本通訊、網路安全技術（Firewall, VPN, NAT...等）及系統存取控制等相關概念 4.培養學員具資訊安全之整體架構、原理、標準與應用，並具相關之資訊法律、電腦犯罪調查等之知識
2018/12/13-14	HITCON Pacific 2018	【資安研討會】HITCON Pacific 2018 時間：2018 年 12 月 13 日至 14 日 地點：台北文創大樓 6F (台北市信義區菸廠路 88 號) 主辦單位：HITCON、iThome 報名網址： https://hitcon.kktix.cc/events/hitcon-pacific-2018 活動簡介： 本次 HITCON Pacific 主題為「Transforming: Cybersecurity and Resilience」，會議將聚焦在各式強韌性資安技術、安防措施等可加強企業關鍵系統的議題上，以因應日新月異的攻擊手法，以期能協助企業與政府單位，有效地縮短資安事件致使的服務停擺時間，進而降低資安事件對其所造成之影響。

第 4 章、2018 年 09 份事件通報統計

本中心每日透過官方網站、電郵、電話等方式接收資安事件通報，2018 年 9 月收到通報計 1631 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。

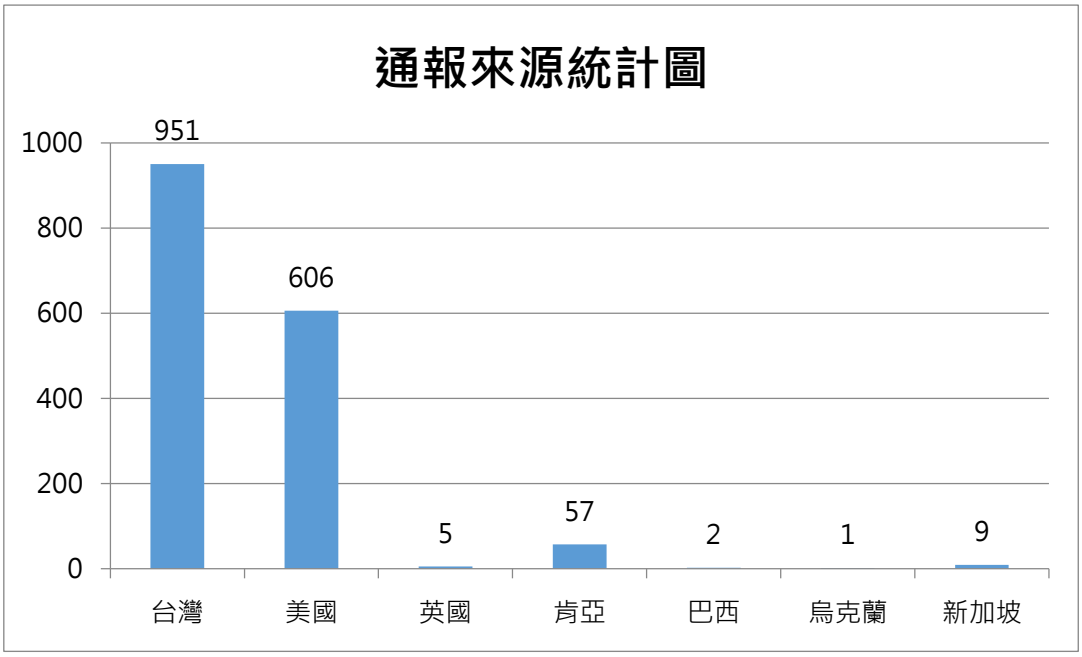


圖 1、通報來源統計圖

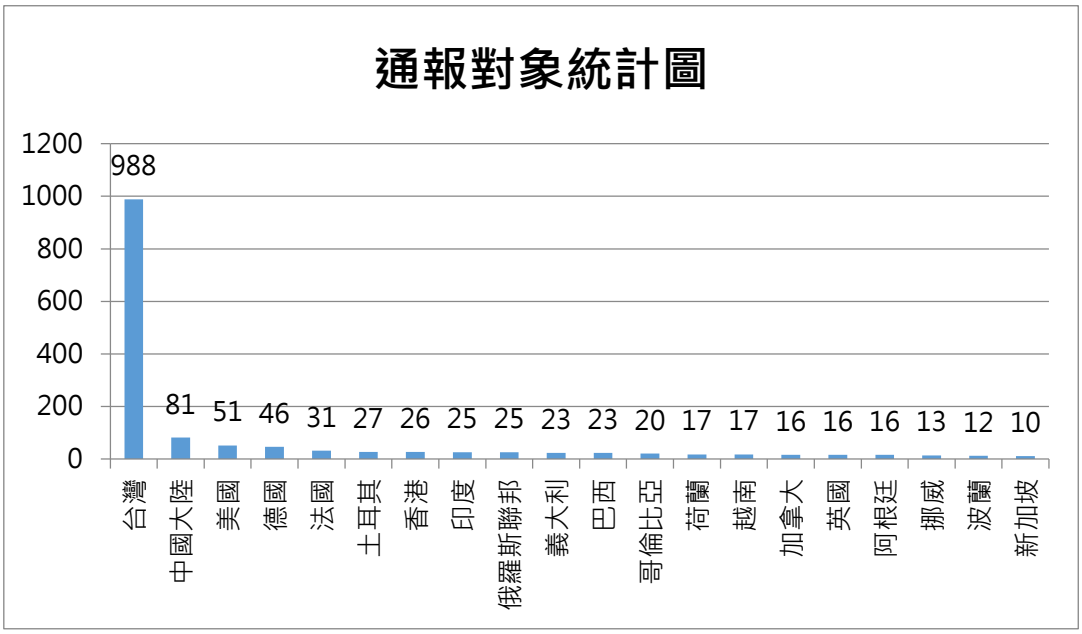


圖 2、通報對象統計圖

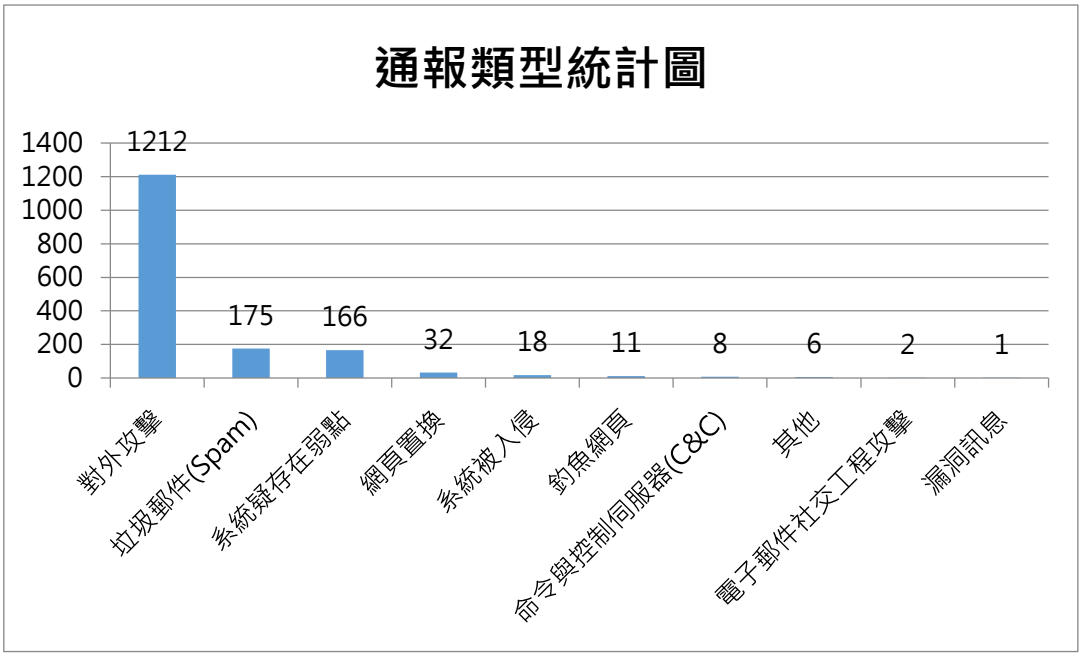


圖 3、通報類型統計圖

本月接獲通報案件中，有某公司的郵件伺服器，遭利用轉發社交工程郵件。該郵件表示：「郵件信箱內容已經超過電子郵件管理員設置的儲存限制，並且在重新進行身分驗證之前將無法收到新電子郵

件」。該信件附上釣魚網站的網路連結，誘騙使用者重新驗證帳戶方式，以騙取用戶輸入其帳號密碼。駭客常透過社交工程手法寄發信件，本中心提醒民眾切勿隨意開啟信件附件及相關連結，若發現疑似釣魚信件可通報 TWCERT/CC。

TWCERT/CC 提醒企業用戶可參考 FBI 發布之注意事項[1]，降低釣魚郵件造成的風險：

(1)勿使用免費申請的電子郵件，企業應該建立自有的郵件伺服器及其網域。

(2)確保防火牆、防毒軟體及垃圾郵件過濾機制有正確啟用並且能夠更新至最新版本。

(3)當發現可疑郵件，應該立即回報並刪除可疑郵件，尤其特別注意不請自來的信件。

(4)若您收到一封看起來是合理聯絡人寄來的信件時，仍應保有警覺性。建議用轉寄 (Forward)而非回復 (Reply)的方式回復此封信件，此舉可以讓您手動填入已知的收件人，以確認此寄件者是否在您已建立的聯繫清單中。

(5)請勿在收到信件時就立刻點選該信件瀏覽其內容。駭客經常使用人們收到信件時就迫不及待開啟來看的人性弱點，企業用戶應提高警覺才讀取信件。

(6)企業可考慮與員工之信件往來時，建置雙因子認證方式使用電子郵件。

(7)建立企業信件的使用習慣，例如您習慣以 ABC_company.com，當收到 ABC-company.com 之信件或內容時，應提高警覺此郵件是否合理。

(8)確保您的電子郵件在傳輸中有加密機制，尤其在傳輸敏感資訊時。

●參考連結：

[1] https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-with-an-email-fortress

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 10 月 15 日

編　　輯：羅文翎

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。