TWCERT/CC 資安情資電子報

2018 年 6 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、參與 2018 國際迷彩嘉年華

6 月 9 日至 10 日國防部、台北市政府產發局及中華民國玩具槍協會於台北市花博公園爭艷館舉辦「2018 國際迷彩嘉年華」，相信迷彩的熱愛者一定也對於國家抱有一顆愛國的赤子之心，又因政府大力宣導資安及國安，資安不再是資安專家的責任，資安意識提昇屬人人有責，TWCERT/CC 亦於會場上設立攤位，主動出擊，希望民眾除了熱愛迷彩之外，亦可藉機了解 TWCERT/CC 業務及提升資安意識。

2.2、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 台灣分會將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，接軌國際資安社群有助於掌握全球發展趨勢。

TWCERT/CC 亦將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 分析師羅文翎受邀分享講題「個資外洩一瞬間」，將介紹 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。

2.3、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連網裝置，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 亦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、英國國民保健署防勒索病毒，升級作業系統至 WINDOWS 10

英國國民保健署(NHS)在 2017 年 WannaCry 勒索病毒攻擊後，全面將作業系統汰舊換新為 Windows 10，藉此避免往後類案再度發生。英國政府投入約 15 億英鎊，供 NHS 在未來三年能夠改善整體醫療資安環境。

資料來源：

https://www.bleepingcomputer.com/news/government/uk-health-agency-switches-to-windows-10-citing-wannacry-ransomware-outbreak/

https://www.itnews.com.au/news/uk-health-service-shifts-to-win10-after-ransomware-attacks-489984

3.1.2、為確保資安，國軍營區禁用中國大陸品牌手機

美國眾議院軍事委員會公布 2019 年 NDAA 法案，明禁任何美國政府機關使用華為或中興公司等中國大陸公司所生產的科技產品。我國國軍已禁止使用中國大陸品牌的手機，並且會透過教育擴大宣導以確保資訊安全。

資料來源：

https://www.ydn.com.tw/News/288443

https://www.nownews.com/news/20180508/2749815

3.1.3、TRELLO 漏洞可能導致使用者機敏資料外洩

Trello 為線上免費專案管理工具，許多系統開發團隊或個人都仰賴此工具來管制及記錄專案中的各項大小進度及細節，但近期有資安專家發現 Trello 存在一漏洞，可能導致使用者機敏資料外洩並遭有心人士竊取，且只需要用 Google 搜尋功能就可以達成。

Trello 的版面(Board)可以由使用者自行設定隱私(Visibility)，但不論設定為公開(Public)或是私人(Private)，皆可能利用 Google Hacking 技巧被搜尋到。例如在 Google 搜尋欄位中輸入「intext:password and inurl:trello.com」，就可以搜尋出數頁結果，從搜尋結果可看出皆為在 Trello 的版面中提到與密碼相關的資訊。實際點入連結觀看，會發現有些版面設定為公開，而有些版面則是私人的所以無法閱覽，但不論是何者，都可以直接透過 Google 搜尋結果

得到部分訊息，包含系統開發細節、系統漏洞處理進度及帳號密碼等，因此只要曾記錄在該平台上之資料都有可能已經外洩。

TWCERT/CC 建議使用者切勿將機敏資訊存於 Trello 中，且應儘速更改曾於 Trello 中記錄帳號之密碼，以免遭有心人士利用。

資料來源：

https://securityaffairs.co/wordpress/72380/data-breach/trello-data-leak.html

https://medium.freecodecamp.org/discovering-the-hidden-mine-of-credentials-and-sensitive-information-8e5ccfef2724

3.1.4、新病毒 VPNFILTER 來襲，可能影響全球 50 萬網路設備

近期有大量網路設備已經遭 VPNFilter 病毒感染，受害者遍布至少 54 個國家，目前已知可能被感染的設備品牌包含 Linksys、MikroTik、NETGEAR、TP-Link 的 SOHO 路由器(小型家用/辦公用路由器)及 QNAP NAS 設備。VPNFilter 病毒包含三階段攻擊，若遭感染，會導致網站憑證遭竊取，及流經 SCADA 的 Modbus 通訊協定之流量遭竊聽。

若使用這些產品的使用者，建議採取以下措施：

1. 重置 SOHO 路由器及 NAS 設備至原廠狀態後重開機，若已感染病毒者可以此方法暫時移除病毒
2. 立即將設備之軟/韌體更新至最新版本

資料來源：

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware

3.1.5、立院三讀「資通安全管理法」，公務機關及關鍵基礎設施提供者未通報資安事件最重罰 500 萬

立法院會 5 月 11 日三讀通過制定「資通安全管理法」，未來各公務機關應設置資安長，推動及監督資安事務；經行政院核定的關鍵基礎設施提供者應訂定資安計畫，且若未通報資安事件，可罰 30 萬至 500 萬元。

新法規範 3 類對象，除了公務機關、公營事業與政府捐補助之財團法人以外，還包括能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等 8 大領域的關鍵基礎設施提供者。

資料來源：

http://m.ltn.com.tw/news/politics/breakingnews/2422795

3.1.6、歐洲刑警組織將建立暗網調查小組

歐洲刑警組織(Europol)轄下歐洲網路犯罪中心(European Cybercrime Centre，EC3)長久以來透過工具、策略及技術分享，協助在暗網中進行非法交易調查，例如他們在 2017 年就協助相關執法單位查獲 Alphabay 及 Hansa 兩個暗網交易平台。Europol 預計建立一暗網調查小組(Dark Web Team)，並將與歐盟各國成員及全球執法單位合作，以有效減少非法交易量。該小組將會針對暗網調查提供全面性的策略，包含分享情資、提供技術支援、發展工具、提供教育訓練及提升防範意識等。

暗網提供一個匿名空間，讓來自全球的犯罪者得以在上面買賣槍械、藥物、網路攻擊工具及電腦病毒，而交易通常透過比特幣來完成。

資料來源：

https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure

https://www.securityweek.com/europol-creates-dark-web-investigations-team

3.2、駭客攻擊事件及手法

3.2.1、日本數十台同品牌網路攝影機遭針對式入侵

據日本產經新聞報導，日本超過 60 台佳能(Canon)網路攝影機遭有心人士入侵，並在受影響的設備的視訊畫面上印有短語「I'm Hacked. bye2」。

據日本社交網站文章表示，5 月 6 日星期日即發生多起攝影機畫面遭印字的事件，但據報導，類似的事件自 4 月中旬以來就一直持續數週。受影響的網路攝影機多在日本政府網路上，並用於監控公共場所，如政府大樓、河川、廣島的魚市場，神戶殘疾人護理設施和那霸公司私人總部等。

官員承認，千葉縣八千代市和琦玉縣上尾市的河川監視攝影機，皆可能因未更改攝影機的預設密碼所致。日本佳能公司在第一次獲報有關入侵事件後，於 4 月 26 日發布了一份安全說明，建議客戶更改預設密碼。

專家表示，連接到網際網路的網路攝影機通常可以透過電腦、智能手機和其他設備進行遠程監控，是典型的物聯網帶來的便利。但專家提醒，駭客亦可以藉此利用這種網路攝影機作為攻擊政府或公司電腦系統的手段。

●TWCERT/CC 建議，安裝使用網路攝影機，務必更改其預設密碼，如非必要，儘可能與對外網路實體隔離，以內部區域網路進行監控作業。

資料來源：

https://www.bleepingcomputer.com/news/security/hackers-deface-canon-security-cameras-in-japan/

http://www.nationmultimedia.com/detail/breakingnews/30344769

https://tw.appledaily.com/new/realtime/20180507/1349244/

http://cweb.canon.jp/caution/180426.html

http://cweb.canon.jp/pdf-catalog/webview/pdf/nwc-security.pdf

3.2.2、英國雪菲爾德信用合作社遭駭，上萬筆用戶資料外洩

英國雪菲爾德信用合作社(SCU)日前遭受網路攻擊，約 15,000 名信用社會員的個人資料被盜。SCU 表示被存取的資料包括姓名、地址、國家保險號碼和銀行資料在內等資訊。

SCU 在會員信中表示，攻擊事件發生在 2018 年 2 月 14 日，但直到近期遭受駭客要求支付贖金否則發布資料等威脅，才發現此事。SUC 會員可能處於遭受有心人士詐騙的風險。

南約克郡警方表示，它正在與 SCU 和 Action Fraud 合作。SCU 則表示，自事件發生以來，已進行審查和增加其安全機制，並將駭侵細節轉交給有關當局，包括警察和新聞局辦公室(ICO)。

受託人董事長 Fiona Greaves 表示，據信駭客利用 brute-force(暴力破解)方式攻擊並獲取資料，他們用不同的密碼組合攻陷電腦系統，透過反覆試驗來有效猜測正確的資料。

SCU 已建議其會員審視他們的銀行和信用報告，以察覺任何不尋常的活動。

資料來源：

http://www.bbc.com/news/uk-england-south-yorkshire-44039296

3.2.3、俄羅斯政府網站遭匿名者駭客組織攻陷

5 月 10 日，知名駭客組織 Anonymous 針對俄羅斯現行的審查制度，特別是最近禁止加密即時通訊軟體 Telegram 事件，在俄羅斯聯邦國際合作署(Rossotrudnichestvo)的官方網站上發動網路攻擊，其子網域遭駭客惡意網頁置換。

4 月，Telegram APP 因拒絕將用戶的加密密鑰交給俄羅斯聯邦安全局(FSB)以進行調查的要求，而遭俄羅斯強制禁止使用(連同數百萬個 IP 位址)。

接著在 5 月 3 日，俄羅斯媒體和通信管理機構 Roskomnadzor 開始打壓 Telegram 的訊息服務，包括封鎖超過 50 個虛擬專用網絡(VPN)、網路代理和匿名。

世界著名的匿名組織以 NSFW(Not Safe/Suitable For Work)的圖片和訊息對 Rossotrudnichestvo 的一個子網域發動網頁置換攻擊，並留下挑釁訊息，宣示對俄羅斯現行的審查制度的反擊。

Rossotrudnichestvo 的主網站目前保持運作，而其攻擊目標子網域(prev[.]rs[.]gov[.]ru)仍處於離線狀態。

資料來源：

https://www.hackread.com/anonymous-hacks-russian-govt-website-against-censorship/

3.2.4、美國 Chili's 連鎖餐廳遭駭，信用卡資料外洩

如果你在過去兩個月裡在 Chili's 餐館裡吃過飯，那麼你可能要檢查一下你的信用報告和信用卡帳單。

布林克國際公司(Brinker)於 5 月 11 日宣布，該公司在全球 31 個國家擁有 1,600 多家 Chili's 和 Maggiano's 餐廳，遭受客戶付款資料外洩事件。

根據初步調查發現，連鎖餐廳的付款系統感染了惡意軟體，可能導致未經授權存取或信用卡資料遭竊，該公司發布通知警告大眾近期在 Chili's 餐廳使用信用卡可能發生資料外洩。

惡意軟體收集的資訊，包括信用卡或轉帳卡號碼和持卡人姓名，Brinker 表示，Chili's 餐廳不收集社會保險號碼、完整的出生日期或

國家身分證號碼，因此相關資料沒有洩露疑慮。

雖然尚不清楚 1600 多家餐廳中有多少家餐廳受到影響，但該公司仍然敦促客戶「出於謹慎」採取措施，以保護他們的資訊。這些建議包括透過個人信用檔案向 Equifax、Experian 和 TransUnion 三個國家信用報告機構提供欺詐警報，並審查個人銀行帳戶資訊相關可疑活動。

Brinker 建議除客戶監控其銀行和信用卡報表中的任何可疑活動，也建議客戶可以訪問公司設置的網頁，以接收有關此事件的資料洩露和更新的更多資訊，並提供信用監控和欺詐解決服務。

資料來源：

http://www.post-gazette.com/life/dining/2018/05/14/Chilis-restaurant-customer-data-credit-card-numbers-cyber-attack-malware/stories/201805140137

https://securityaffairs.co/wordpress/72481/data-breach/chilis-payment-card-breach.html

3.2.5、Rail Europe 火車購票系統遭入侵，多筆信用卡資料外洩

如果您在過去幾個月預訂了歐洲度假的火車票，您可能需要查看銀行對帳單。

Rail Europe 公司是用來購買歐洲火車票的網站，近期揭露發生為期三個月的信用卡和簽帳卡資料洩露事件，由提交加利福尼亞司法部長的一封信所公布。

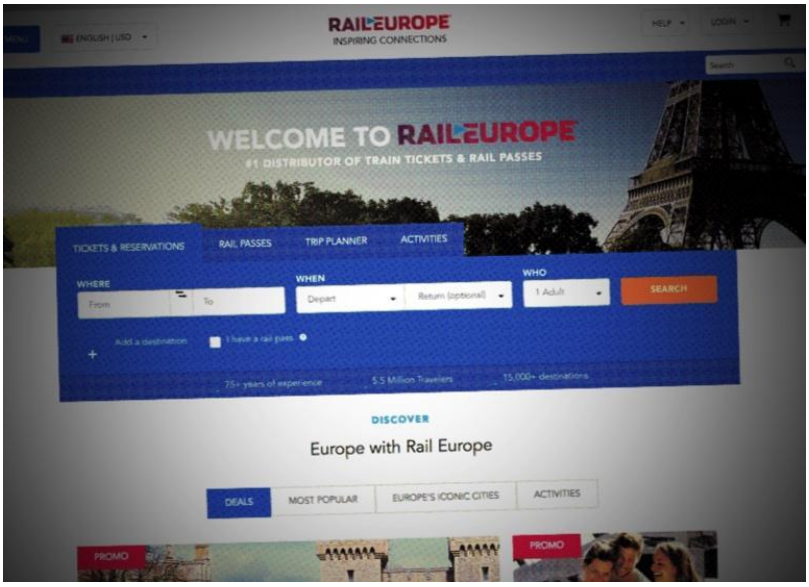
該公司稱駭客在 2017 年 11 月下旬和 2018 年 2 月中旬之間將信用卡側錄惡意軟體放在其網站上進行資料竊取。

遭竊信用卡資料包括信用卡號碼、到期日期和驗證碼，其他資料包含網站上的姓名、性別、交付和發票地址、電話號碼、電子郵件地址，在某些情況下甚至含有用戶帳號和密碼等。

Rail Europe 公司表示，已從已知的安全代碼中「替換並重建」了受駭的系統。儘管該公司沒有說明駭客如何入侵其系統來安裝信用卡側錄惡意軟體，但該信也稱在駭客入侵後已更改密碼以及更新認證。

目前還不知道有多少客戶受到影響。加利福尼亞數據違規法規定，任何影響超過 500 名州居民的洩漏事件都必須向州檢察長辦公室公開列出洩漏通知。

據該公司網站稱，該網站去年擁有超過 500 萬的客戶。



資料來源：

https://www.zdnet.com/article/rail-europe-had-a-three-month-long-credit-card-breach/

https://oag.ca.gov/system/files/RENA%20Customer%20Notification_0.pdf

3.2.6、Securus 電話定位服務資料外洩，上千筆個資遭駭客掌握

據報導，Securus 遭受網路攻擊導致資料外洩，未知駭客成功竊取 2,800 名用戶的登錄憑證，其中包括用戶名、電子郵件、脆弱的雜湊密碼(使用安全係數很低的 MD5 演算法)、電話號碼等。

Securus 電話定位服務主要從 AT&T、Sprint、T-Mobile 和 Verizon 等電信公司獲得手機位置數據，然後將其提供給客戶，也幫助執法機構監控美國的大部分手機，主要透過使用能存取其位置 API 的 Web 界面，Securus 能夠即時成功訪問行動通信基地台，即可透過這些紀錄獲取手機資料以用來跟蹤。

Motherboard 的 Joseph Cox 與駭客聯繫，並在網站互享了一些樣本資料。據稱一個從「警察」資料庫獲取的電子表格，這些資料經 Cox 測試(以忘記密碼功能來驗證資料)證實是合法的，目前還不清

楚向 Motherboard 提供資料的駭客是否破解了所有密碼，也不清楚 Securus 本身是如何儲存這些密碼的。

此外，對失竊資料的快速分析顯示，它包含 2011 年前的資訊，而受影響的客戶包括印第安納波里斯、費尼克斯和明尼阿波利斯的城市員警和治安部門。

Electronic Frontier Foundation 的律師 Andrew Crocker 在電話採訪中告訴 Motherboard :「Securus 無需許可證即可進行定位追蹤，並允許其用戶在未經審查的情況下獲取此服務。這是一個問題。如果一個系統不對使用監控權的用戶進行設限，那麼它將成為一個雙重問題。」

資料來源：

https://www.hackread.com/securus-cops-track-cellphone-users-has-been-hacked/

https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/

https://www.xcnnews.com/kj/3754568.html

3.2.7、青少年監控 APP「TeenSafe」上萬使用者資料暴露於網路

已知至少有一台用於家長監控青少年手機活動的伺服器已經暴

露了成千上萬的父母和孩子的帳戶和資料。

「TeenSafe」手機 APP 自稱是跨 iOS 和 Android 的「安全」監控應用程式，可讓父母查看孩子的訊息和位置，監控和他們打電話的人和時間以及存取他們的網路瀏覽紀錄，查出他們安裝哪些 APP，並聲稱有超過 100 萬的父母使用這項服務。

雖然青少年監控應用程式是有隱私和侵入爭議，該公司稱，該 APP 可以讓父母不需透過他們的孩子的同意，但這家總部位於加利福尼亞州的公司將其伺服器託管在亞馬遜的雲端，卻不受任何的保護並且無需密碼即可存取。

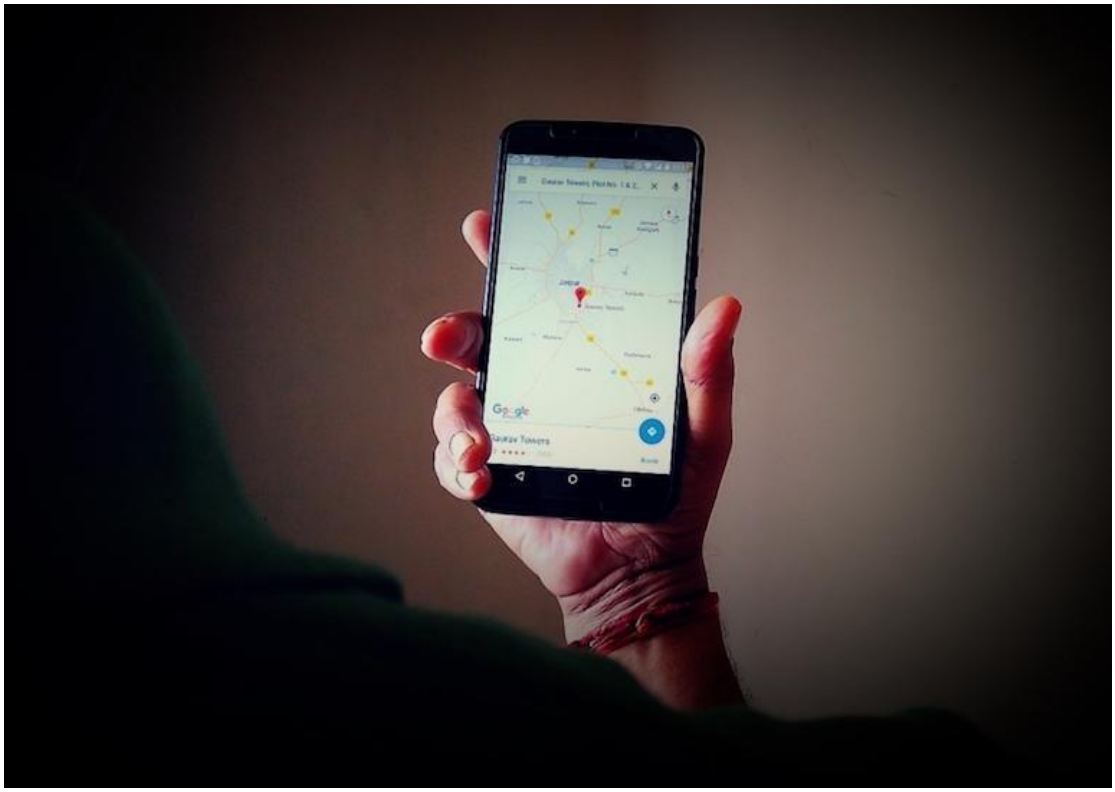
英國安全研究人員 Robert Wiggins 在搜尋公開資料和暴露在外資料時，發現兩台資料洩漏的伺服器，並在 ZDNet 提醒該公司後，兩台伺服器都被下線，TeenSafe 發言人週日並通知 ZDNet 已採取行動將一台公開的伺服器關閉，並開始提醒可能會受到影響的客戶。

該資料庫儲存的資料包括與 TeenSafe 關聯的父母的電子郵件地址以及其相應孩子的 Apple ID 電子郵件地址，還包括孩子的設備名稱(通常只是名字)以及設備的唯一標識符，更包含孩子 Apple ID 的明文密碼。由於該 APP 需要關閉雙因素身分驗證，所以查看此資料的有心人士只需使用憑證即可侵入孩子的帳戶以存取其個人資料內容。

其中資料還包含帳戶操作失敗的相關錯誤訊息，例如，父母查找孩子的即時位置未完成之紀錄。而這些紀錄尚包含如照片、手機訊息或父母、子女的位置。在伺服器離線前，過去三月中已至少有 10200 條紀錄包含客戶資料(部分重複)，其中一個伺服器似乎僅儲存測試資料，但不知道是否其他暴露的伺服器有額外的資料。

ZDNet 更透過 iMessage 在外洩資料中嘗試與其父母聯繫，並得到部分回應表示曝光的電郵地址確實是用來設定孩子的 Apple ID。

目前還不清楚為什麼這些資料，包括青少年的 Apple ID 設置密碼是以明文形式儲存。該公司在其網站上聲稱，它是「安全的」，並使用加密來混淆資料，以避免發生資料洩露，並表示將繼續評估此情況，並在可用時「提供更多資訊」。



資料來源：

https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/

3.3、軟硬體漏洞資訊

3.3.1、時隔一月，Drupalgeddon 第 3 代來襲

以 PHP 開發之 Drupal，係自由開源的內容管理系統(CMS)，中文化後在國內有固定支持者推廣其應用技術，Drupal 平台將內容視同 node，藉由後端 module 調整顯示、排列、分類等方式，搭配權限控管可架構論壇網站，近期高危漏洞 Drupalgeddon 3，繼一個月前 Drupalgeddon 2，再度威脅 Drupal 網站，囿於其 core 級表單

API 無法嚴謹過濾輸入值，致使惡意請求能伺機偷渡 payload，以「%2523」形式經解碼轉換成「%23」，成為 Unicode 之「#」編碼，假冒陣列資料 key 值而執行運算，將衍生 RCE 攻擊，因 core 牽涉多種子系統共同應用方式，駭客可循不同網頁途徑入侵，恣意進行挖礦、後門、勒索軟體、置換網頁等攻擊手段，Drupal team 已針對主流版本升級並公告，部分舊版已逾維護範圍，因全球 Drupal 開發網站超過百萬，建議網管者即刻因應，若站台修補遲緩，難以降低後續遭駭風險。

資料來源：

https://thehackernews.com/2018/04/drupalgeddon3-exploit-code.html

https://pastebin.com/pRM8nmwj

3.3.2、Twitter 承認記錄密碼明文，用戶宜火速換密

自 2006 年 3 月創辦迄今，Twitter 成長為 3.3 億用戶的社群網路，微網誌為其特色，日前遭披露其弱點，Twitter 系統雖使用工業標準之 bcrypt( )函數，將密碼明文轉換成亂數，然因程序瑕疵，竟誤存明文資料於特定 log 檔，儘管 Twitter 公司指稱，目前尚無徵兆顯示會員個資遭濫用，然拒絕透露實際受影響人數，據知 Twitter 使用者達 3.3 億，且其用戶未接獲告警此事發生，故多數人尚未察覺密碼可能面臨外洩風險，倘若 Twitter 內部員工圖謀不軌，將會是繼

FaceBook 洩漏個資之後的嚴重跨國資安事件，Twitter 公司正組織專案防止類案復犯，並建議迅速換密並啟用雙元認證，強化身分驗證力度。

資料來源：

https://www.bleepingcomputer.com/news/security/twitter-admits-recording-plaintext-passwords-in-internal-logs-just-like-github/

https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

3.3.3、數位學習平台 Blackboard Learn 與 Shibboleth 身分驗證整合，易受 URL 轉址攻擊

由 Blackboard Inc 開發之 Blackboard Learn(舊稱 Blackboard 學習管理系統)，將傳統面授式課程單元，改採線上提供，以 Web server 型態模擬教學環境，並放客製化架構，可結合學生資訊與身分驗證協定，分析指出，Blackboard Learn 與 Shibboleth 單一登入整合運用時，其認證請求出現輸入值查核錯誤，故攻擊者有機可趁，於網址內填入惡意 URL，誘使受害者開啟，操作者誤以為正透過 Shibboleth 進行登入，實則 URL 被重新導向至惡意網頁，目前仍無官方更新公告。

資料來源：

http://seclists.org/fulldisclosure/2018/Apr/57

https://securitytracker.com/id/1040767

3.3.4、威聯通升級 NAS 作業系統 QTS，消彌 XSS 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，其專屬 Turbo NAS 作業系統 QTS，以 Linux 為基礎，具備儲存管理、快照備份、安全監控等功能，近日公布 QTS 因疏於核驗輸入值，恐招致 cross-site scripting 攻擊，繼而洩露用戶隱私資訊，QNAP Systems 已針對該瑕疵升級韌體，可直接下載。

資料來源：

https://www.qnap.com/en/security-advisory/nas-201804-27

https://www.cybersecurity-help.cz/vdb/SB2018043005?affChecked=1

3.3.5、處理器軟體開發者手冊 debug exception 解釋混淆，恐造成多種 OS 非預期狀態

本次瑕疵非屬單一軟硬體設計不良所致，而是牽涉到 Intel 64 和 IA-32 處理器架構之軟體開發者手冊(Software Developer's Manual, SDM)，這份手冊內有專門討論硬體除錯例外(Hardware debug exception)的篇幅，其中某幾段系統程式指南相關敘述，被不當使用在部分作業系統 kernel 開發階段，將對平台環境造成無法預料之結果，特別是 MOV SS 與 POP SS 等組合語言指令，將干擾延遲某些 interrupt，使 OS kernel 無法預判事件發生順序，亦影響 debug exception 指向較低等級 ring(環式緩衝區)，駭客甚可藉此運用 kernel 專用的 ring 0，可能在 Windows、macOS、Xen、FreeBSD 平台擴權操作，或是導致 Linux 內核發生 crash。

資料來源：

https://www.kb.cert.org/vuls/id/631579

https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=631579&SearchOrder=4

3.3.6、駭客新招 baseStriker 打破 Office 365 保護機制

經 Avanan 研究員分析，指出 Office 365 出現問世以來最嚴重的瑕疵，駭客已運用特定手法 baseStriker，全面繞過微軟 Advanced Threat Protection 與 Safe Links 的防護，攻擊原理係運用<base>標籤，配賦惡意 URL 之前段局部字串，再以正常<href>tag 填入其餘字串，Safe Links 檢查<base>tag 內容時，因非完整惡意網址故誤判為無害，又忽略後段<href>tag 零星字串，可是閱讀郵件時，連結效果卻是完整的惡意 URL，一時不察則受害，此項弱點評為高危險性，雖不至嚴重等級，然已證實駭客組織利用該技術在野攻擊，為免受釣魚網站、勒索軟體波及，目前尚未推出修補更新，Office 365 使用者接近 1 億，鑑此，終端用戶應謹慎處理電郵來信，或者選擇安全性高之電郵服務。

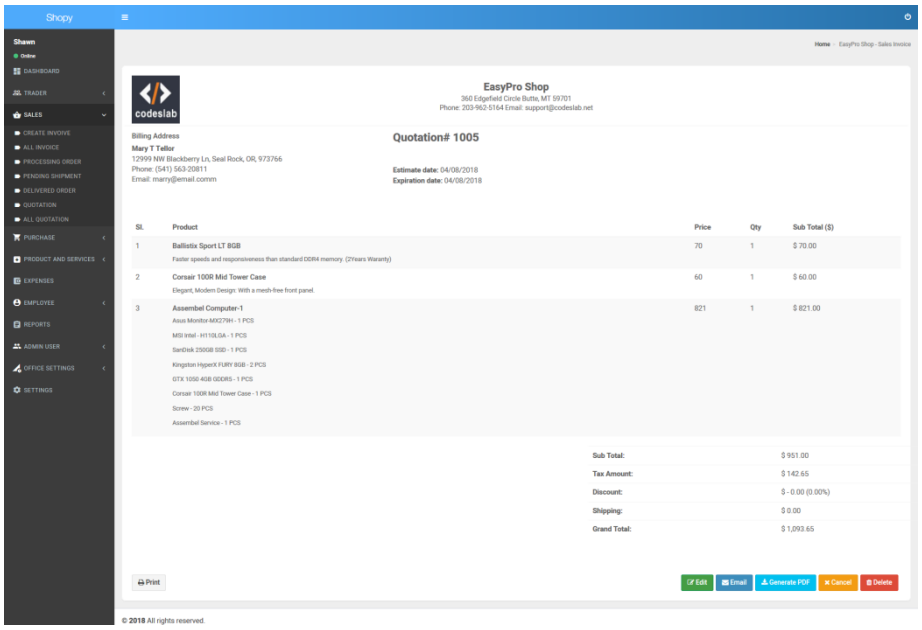
資料來源：

https://www.youtube.com/watch?v=rOmFuC4rLJY&feature=youtu.be

https://www.avanan.com/resources/basestriker-vulnerability-office-365

3.3.7、留神 Shopy POS 系統匯出 CSV 檔案可埋藏指令

熟悉 Excel 的操作者，必然熟悉 Comma Separated Values(CSV)檔案，表格資料儲存為純文字形式，常以逗號分隔其欄位，經分析 Shopy Point of Sale，察覺該系統匯出之 CSV 格式，可能被低權限使用者注入指令，指令字串埋藏於 Customer Name 欄位，故輸出資料只要包含消費者姓名資訊，例如發票紀錄，均可能遭利用 Shopy 弱點實行 RCE，由於探勘實驗環境為 Kali Linux 2.0 及 Mac OS 10.13，在其他作業系統之安防機制下，相同探勘手法能否奏效仍屬未知。補充說明，Shopy 為 Envato Pty Ltd 所開發商用 POS 系統，並非發音近似之蝦皮(shopee)購物，讀者切莫混淆。



資料來源：

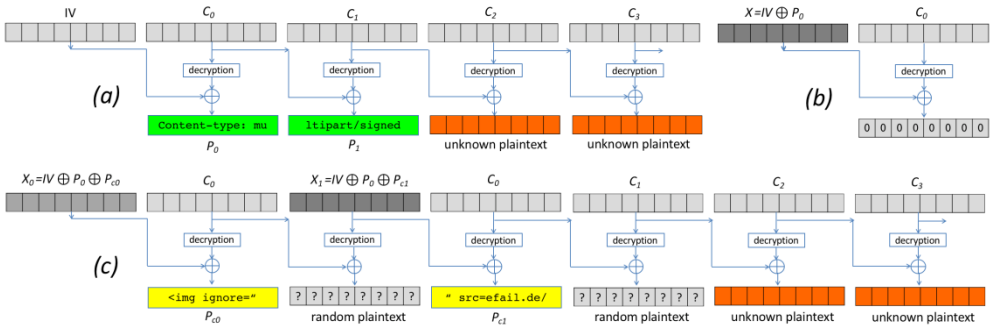
https://www.exploit-db.com/exploits/44534/

https://www.secnews24.com/2018/05/01/cve-2018-10258-a-csv-injection-vulnerability-was-discovered-in-shopy-point-of-sale-v1-0-that-allows-a-use/

3.3.8、電郵加密標準 OpenPGP 和 S/MIME 出現嚴重缺陷 eFail，能直接外洩明文訊息

如同去年 WPA2 無線通訊協定發生 KRACKs 弱點，另有廣泛應用的點對點加密標準被歐洲研究機構找到破綻，各家電郵系統均能支援的 OpenPGP、S/MIME，正面臨新穎攻擊手法 eFail，乍看之下形似 email，正說明了與 email 的關聯性，能存取用戶主機、帳號、email server 的駭客，只要蒐集資料夠完備，就能假造信件內容，插入 html 載入外部資源之語法，利用電郵軟體自動解密運算與編碼 URL 相關邏輯機制，將明文訊息夾在 request 內，洩漏給惡意網站，Direct Exfiltration 對網頁郵件之洩密危害最直接，Apple Mail、iOS Mail、Postbox、Thunderbird 等軟體均無法倖免，而較複雜的 Malleability gadget 攻擊，須對 S/MIME 之 Cipher Block Chaining 區塊密文運

算，或 PGP 的 Cipher Feedback 模式，反覆注入惡意 block，將 <img> tag 密集填進原始密文，製造出類似的解密明文外洩效果，由於該嚴重漏洞影響範圍甚鉅，幾乎主流 email 軟體都無法完全防禦 eFail 式攻擊，短期內各軟體商暫無修補檔，電子邊防基金會(Electronic Frontier Foundation, EFF)建議移除 PGP 及 S/MIME 工具，釜底抽薪的做法則是重新研議 OpenPGP、S/MIME 標準文件，避免類似瑕疵，本文提醒使用者注意收信內容是否異常，建議選用其他點對點加密方案，或是以加密附件傳遞機敏訊息，國內電郵服務商亦應重視此議題，儘速補強漏洞肇因。



資料來源：

https://efail.de/efail-attack-paper.pdf

https://thehackernews.com/2018/05/pgp-smime-email-encryption.html

3.3.9、火速更新 Adobe Photoshop 及 Acrobat Reader，化解 0-day 連鎖攻擊

市占率頗高的 Adobe 軟體，適用 Windows 與 macOS 環境，經分析旗下商品共查出 48 項弱點，Photoshop 具越界寫入記憶體漏洞，被評為嚴重等級；至於 Acrobat Reader 主流版本，包含高風險弱點 23 項與嚴重弱點 24 項，越界讀取記憶體、Memory Corruption 及 NTLM 單一登入 hash 遭竊等，皆引發資料外洩；Double Free、緩衝區溢位、使用釋放記憶體、Out-of-bounds write、Type Confusion、反參照非可靠指標均導致任意代碼執行；ESET 研究員

指出，Acrobat Reader 雙重釋放相同記憶體，為極嚴重之 0-day 漏洞，若與微軟 Windows 之 Win32k 元件擴權 0-day 漏洞相結合，可以製造 exploit chain，以武裝化 PDF 檔案，控制 Button 物件觸發 Double Free，再以 heap-spray 獲得大片記憶體存取權，最後利用 Microsoft Win32k 元件擴權為 kernel 模式，執行 Portable Executable 檔案，能影響.exe、.dll、.sys 等格式，所幸頗具威力的連鎖攻擊技術，因為其創造者提前暴露此事，防毒軟體公司 ESET 已通報 Adobe 修補，並於 5 月公告升級。

資料來源：

https://www.bleepingcomputer.com/news/security/shadowy-hackers-accidentally-reveal-two-zero-days-to-security-researchers/

https://thehackernews.com/2018/05/adobe-security-patch-update.html

3.3.10、急報 DrayTek 28 型 Vigor 路由器漏洞，竄改 DNS 指向中國大陸 IP

居易科技(DrayTek)為國內網路設備製造商，其路由器、交換器、防火牆、VPN 裝置主要外銷歐洲，本月多名消費者抱怨被不明人士更動路由器 DNS 設定，IP 定址為 38.184.121.95，屬中國電信管轄，

此事件被定義為 0-day 攻擊，在公開前約已持續二週，也許是大型攻擊前期行動，由於未遺留可疑登入紀錄，判斷特徵應是類似CSRF(跨站台請求偽冒)之探勘手段，而非破密後控制設備參數。基於產品安全顧慮，居易科技公司暫無規劃公開弱點探勘技術細節，僅 5 月 18 日於官網說明此次事件影響，並釋出更新韌體，在回應該漏洞事件的同時，查詢該惡意 IP 已無任何回應，顯然該設備東窗事發後被離線處置。至於 28 款弱點機型在韌體確實修補前，應檢查 DNS IP 是否正常，且關閉遠端存取管理介面功能，養成 https://連線作業習慣，以根除密碼遭竊、插播廣告、妨礙金融等危害。

資料來源：
https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks
https://www.bleepingcomputer.com/news/security/draytek-router-zero-day-under-attack/

3.3.11、弱點稽核軟體 Nessus 雙破綻，招致 Session Fixation & XSS 攻擊

弱點偵測軟體 Nessus®，可遠端掃瞄主機 IP，辨識各種 OS、VM、資料庫，稽核其系統設定安全性、修補狀態、入侵徵兆，產生評估報告並提供建議，國內約 500 家企業採用，且開放非企業環境

之個人免費使用。專門找出弱點的系統，這回被發現自身弱點，一個是 Cross-site scripting，另外還有固定 Session 攻擊法(Session Fixation)，組合兩項漏洞特性，遠端認證駭客，可上傳特製.nessus 檔案，讓管理者瀏覽時執行腳本程式，取得 cookies 等隱私資料，再利用 cookie 內 session ID 相關資訊，假冒受害者身分操作，即使管理者已更換密碼，駭客仍可連線 Nessus 進行系統維管，Tenable Network Security 已公告升級版軟體改善缺失。

資料來源：

https://www.tenable.com/security/tns-2018-05

https://devco.re/blog/2014/06/03/http-session-protection/

3.3.12、受 Bitvise SSH server/client 漏洞衝擊，資料傳送將意外終止

一個 7 人規模的居家工作型公司 Bitvise，針對 Windows 平台遠端操作需求，以 C++開發主流安全通道產品 SSH server 及 SSH client(前身分別是 WinSSHD 與 Tunnelier)，輕巧的兩層式架構與保密性，令其在翻牆軟體排行榜名列前茅，該公司亦提供 FlowSsh 函式庫，令第三方可開發相容性程式，經測試相關軟體，發掘共同瑕疵，其 zlib compression 函式庫元件運作時，會讓多組 SSH session 在同一時間連線至 server，形成 race condition，彼此破壞 session 內解壓縮資料，妨礙 SSH 正常功能；另外 Secure FTP 送出 SSH_FXP_CLOSE 訊息後未追蹤處理進度，隨即關閉 SFTP 通道與 SSH session，攻擊者藉惡意資料，可觸發記憶體存取錯誤，且無法記錄最終傳輸工作是否如預期般完成；而 SSH server 介面 Control

Panel 匯入檔案功能，處理超過 5000 筆輸入則超載當掉，Bitvise 已升級軟體版本解決異常事件。

資料來源：

https://www.bitvise.com/ssh-server-version-history#security-notification-741

https://www.bitvise.com/index

3.3.13、操作 strongSwan VPN，慎防 Buffer Underflow 中斷系統功能

早期由 FreeS/WAN 專案分支出來的 C 語言開放原始碼 strongSwan，能在 Linux 平台實踐 IPsec 功能，並採用 X.509 公開金鑰認證，其 VPN 特性著重在組態介面單純、強化加密認證、IPsec 規則支援複雜 VPN 網路、模組化設計具高擴展性，經分析 charon server 原始碼 stroke_socket.c，察覺 Buffer Underflow 破綻，若遭受 vpn 或 root 群組成員遠端攻擊，導致指標誤置於緩衝區起始處之前，後續操作恐耗盡系統資源而發生 DoS，原本 strongSwan 僅為 Linux 通信安全而設計，然相關技術已輸出應用至 Android、FreeBSD、Mac OS X、Windows 等平台，故此項漏洞可能影響多種 OS，目前已知 SUSE Linux 確定具弱點風險且於 5 月 24 日修補，其餘 CentOS、Red Hat 等 20 家軟體業者迄今尚無正面回應，而 strongSwan 已公開升級軟體與局部修補 source code。

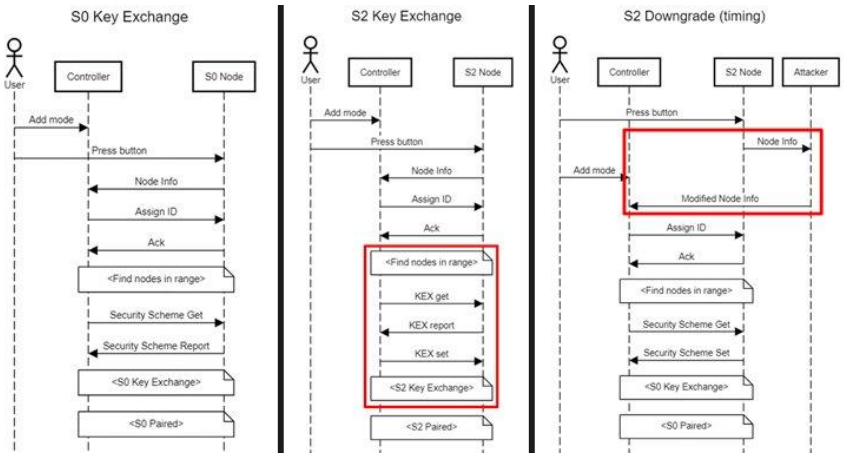
資料來源：

https://www.kb.cert.org/vuls/id/338343

https://zh.wikipedia.org/wiki/StrongSwan

3.3.14、Z-Shave 攻擊恐影響全球上億 IoT 智慧裝置

物聯網領域目前沒有單一優勢無線技術，而是 Wi-Fi、藍牙、ZigBee、Thread 等標準共存，鑑此，Silicon Labs 將 Z-Wave 技術投入快速增長的市場需求，全球現有 2400 類物聯網智慧設備採用 Z-Wave 協定，然 Z-Wave 設備容許 S0 與 S2 兩種安全架構並存，新舊機型配對連線時，配合舊機而降級為 S0，然 S0 有眾所周知的破綻，使用 16 bit 密鑰「0000000000000000」，故駭客有可能讓使用 S2 之設備 DoS 而離線，以惡意裝置加入 Z-Wave 網路，製造配對過程降級事件發生，再解密其流量加以竄改，進而控制其他智慧家電，盜取資產，據英國 Pen Test Partners 研究員實作 Z-Shave 攻擊手法，透過降級安全標準，可破解智慧門鎖並永久性控制，證實現有 Z-Wave 協定確有瑕疵，全球上億 IoT 均受影響，但並非極端嚴重威脅，畢竟 Z-Shave 僅針對技術面漏洞，在現實環境仍有諸多因素可阻礙 Z-Shave 攻擊。



資料來源：

https://youtu.be/kw3Ypoi4kIY

https://www.bleepingcomputer.com/news/security/z-shave-attack-could-impact-over-100-million-iot-devices/

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
2018/06/20	全方位企業防禦解決方案	【資安研討會】全方位企業防禦解決方案 日期：2018 年 06 月 20 日(三) 地點：集思台大會議中心 蘇格拉底廳 (台北市羅斯福路四段 85 號 B1) 主辦單位：吉康科技 線上報名連結： http://www.gcomtw.com/seminar/Synopsys/180620/180620Invitation.html 活動概要： 自 2015 年起，國際上陸續發生多起藉由物聯網(IoT)設備的資安攻擊事件，其隱藏的資安問題直接影響國家、企業、人身安全。因此，各種物聯網裝置(Device)與服務(Service)設計之初，就必須同時考慮資安防護能力。吉康科技從軟體開發階段即提供完整安全性檢測方案，包含靜態編碼分析、通訊協定的異常輸入檢測、開

時間	研討會/課程名稱	研討會相關資料
		源軟體漏洞檢測等多面向的軟體工具，將資安防禦的觀念導入開發流程，可提早預防資安攻擊造成的損失。 近年由於個資外洩事件頻傳，促使各國對於資料保護訂立嚴格的法規，其中企業最關注的莫過於歐盟今年 5 月 25 日起強制執行的 GDPR。為了協助企業遵循法規，吉康科技也提供追踪與管理應用程式的安全漏洞、監控開源軟體與評估安全性風險、應用程式弱點掃描的完整安全性檢測方案，滿足使用者期望的個資保護及隱私安全。 當前的資安防護已經從單一環節的控管，演進成系統工程，除了裝置與應用程式的安全性檢測，再加上網路可視性資安檢測以及 APT 威脅掃描，可幫助企業建立全方位的資安防禦系統，預防資安攻擊以保持業界領先地位。
2018/06/21	2018 資安風險與金融科技大未來	【資安研討會】2018 資安風險與金融科技大未來 日期：2018 年 06 月 21 日(四) 地點：台北晶華酒店 4 樓 貴賓廳 1 (台北市中山區中山北路二段 39 巷 3 號) 主辦單位：台灣數位鑑識發展協會 線上報名連結： http://www.gss.com.tw/eDM/eDM20180621_conference_ithome.html 活動概要： 新科技出現為人們帶來便利，同時也出現蓬勃的駭客經濟，威脅猖獗又無可避免，資安問題為企業、政府帶來巨大影響，雖然我們無法完全避免資訊外洩或攻擊，但卻有可能從各面向做好周全準備，降低損失並保障組織營運。

時間	研討會/課程名稱	研討會相關資料
2018/06/22	網際網路零售業資安防護推廣 【商譽優先！網路開店系統的選擇指南】	【資安研討會】網際網路零售業資安防護推廣 【商譽優先！網路開店系統的選擇指南】 日期：2018 年 06 月 22 日(五) 地點：集思台大會議中心 洛克廳 (台北市羅斯福路四段 85 號 B1) 主辦單位：經濟部商業司 線上報名連結：http://cstierp.iii.org.tw/index.php 活動概要： 網路創業資安防護很重要，個資保護怎麼做呢？ 說明會將以資安角度來提供電商業者選擇網路開店系統的評估參考，並透過工具檢測來測試所建置網站的資安風險！面對 5 月底已生效的歐盟 GDPR，將對未來 AI 人工智慧帶來的智慧零售會有什麼影響呢？本說明會要讓電商業者了解未來並輕鬆做好基本資安防護，讓品牌商譽再加分！
2018/06/27-06/29	後量子密碼學微型講座暨研討會	【資安研討會】後量子密碼學微型講座暨研討會 日期：2018 年 06 月 27 日(三)至 2018 年 06 月 29 日(五) 地點：中央研究院資訊科學研究所 106 會議室 (台北市南港區研究院路 2 段 128 號) 主辦單位：中央研究院 線上報名連結： https://www.twisc.org/twisc_event/2018/PQCRYPTO 活動概要： 中央研究院團隊因參與科技部與歐盟地平線 2020 架構計畫合作之「永續可用的後量子密碼學」計畫，將與 TWISC 資安中心合作，假中央研究院於 2018 年 6 月 27 至 28 日舉辦為期 2 天後量子密碼學速成講座。本講座的授課內容將幫助修習過大學以上數學系、資工系或電機系課程人員快速理解後量子密碼學的研究領

時間	研討會/課程名稱	研討會相關資料
		域。並於 2018 年 6 月 29 日舉辦後量子密碼學論壇研討會，邀請多位後量子密碼學領域專家學者專題演講與分享最新研究趨勢。 **微型講座講者陣容** 每部分講習時長約 150 分鐘，且於每天早上 9:40 開始。 1. Daniel J. Bernstein (Lattice-based Cryptography，晶格密碼學) 2. Wouter Castryck (Supersingular Isogeny Cryptography，超奇異同源密碼學) 3. Tanja Lange (Code-based Cryptography，編碼密碼學) 4. Peter Schwabe (Hash-based Cryptography，雜湊函數密碼學) 5. Bo-Yin Yang (Multivariate Quadratic Cryptography，多變量二次密碼學)
2018/07/10-12	2018 國際資安組織台灣高峰會	【資安研討會】2018 國際資訊安全組織台灣高峰會 主辦單位：CSA Taiwan Chapter、The Honeynet Project Taiwan Chapter、OWASP Taiwan Chapter Workshop 日期：2018 年 07 月 10 日(二) 研討會日期：2018 年 07 月 11 日(三)至 2018 年 07 月 12 日(四) 地點：集思台大會議中心(台北市大安區羅斯福路四段 85 號 B1) 線上報名連結：http://2018.twcsa.org/ 活動概要： 今年的國際資訊安全組織台灣高峰會，由 Cloud Security Alliance 台灣分會、The Honeynet Project 台灣分會以及 OWASP 台灣分會共同主辦，同步接軌 Cloud Security Alliance、The Honeynet Project 與 OWASP 等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

時間	研討會/課程名稱	研討會相關資料
		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，接軌國際資安社群有助於掌握全球發展趨勢。
2018/07/27-28	HITCON Community 2018	【資安研討會】HITCON Community 2018 主辦單位：HITCON GIRLS、社團法人台灣駭客協會(Association of Hackers in Taiwan)、CHROOT Security Group 會議日期：2018 年 07 月 27 日(五)至 2018 年 07 月 28 日(六) 會議地點 : 台北南港展覽館一館 5 樓(台北市南港區經貿二路 1 號五樓) 報名日期 ： ■ 第一階段 售票日期：2018/05/05 20:00 - 2018/06/02 12:00 ■ 第二階段 售票日期：2018/06/16 20:00 - 2018/07/07 12:00 會眾票： ■ 一般票票價：新台幣 3,500 元 ■ 學生票票價：新台幣 1,500 元 ■ 此票價包含 HITCON Community 2018 會眾 Badge 乙張、迎賓袋乙份及 HITCON Community 2018 限量 T-Shirt 乙件 升級票： 今年提供一個精美設計且和主題搭配的電路板，歡迎選擇「升級」票種，你將會拿到 HITCON 獨家的特製電路板！(市價約二千元，還有玩不完的多樣功能！) ■ 一般票票價：新台幣 5,000 元 ■ 學生票票價：新台幣 3,000 元 ■ 此票價享會眾票所屬福利，並另包含 HITCON Community 2018 專屬電路板，電路板詳細規格將於日後公布 VIP 票 ■ 票價：新台幣 10,000 元 ■ 此票價享會眾票所屬福利，並另包含 HITCON

時間	研討會/課程名稱	研討會相關資料
		Communtiy 2018 會議廳快速通關、HITCON Community 2018 貴賓室通行權、專屬 VIP 晚宴與高科技電路板，HITCON Community 2018 專屬電路板詳細規格將於日後公布 ■ VIP 晚宴時間：2018 / 07 / 27(五)18 : 00，地點將個別公布 報名網址： https://hitcon.kktix.cc/events/hitcon-cmt-2018 活動概要： 今年的 HITCON Community 以區塊鏈(Blockchain) 作為主題，不只是因為區塊鏈技術中數據的儲存、驗證、傳遞與資安息息相關，更因為分散式節點的去中心化，正是反對權威、支持資訊自由交流的駭客精神。

第 4 章、2018 年 05 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 5 月收到通報計 4813 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。

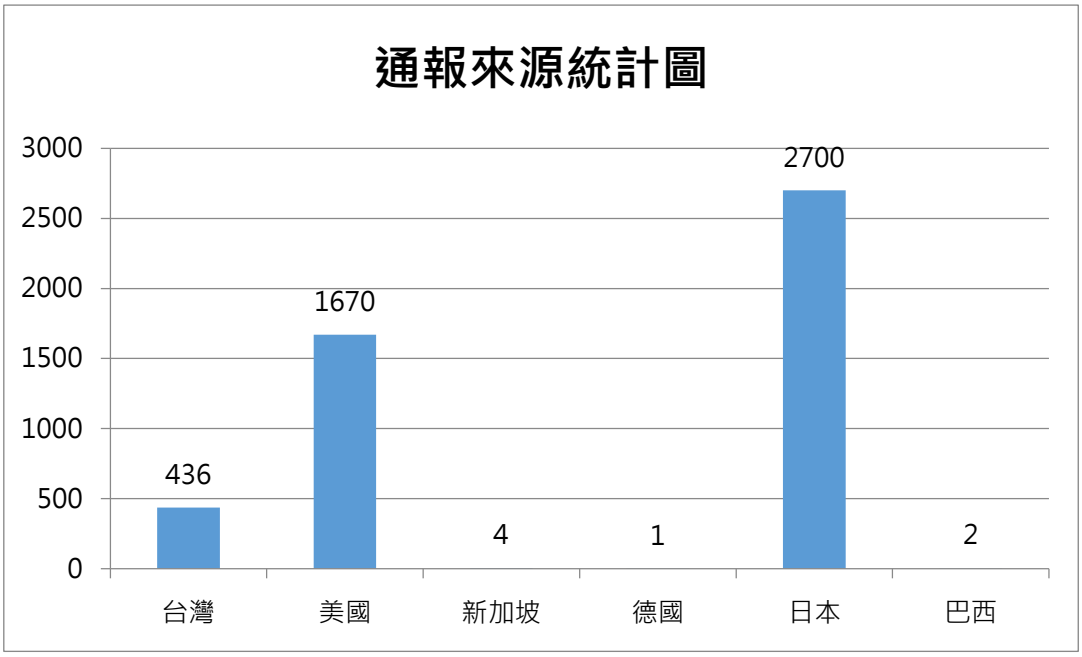


圖 1、通報來源統計圖

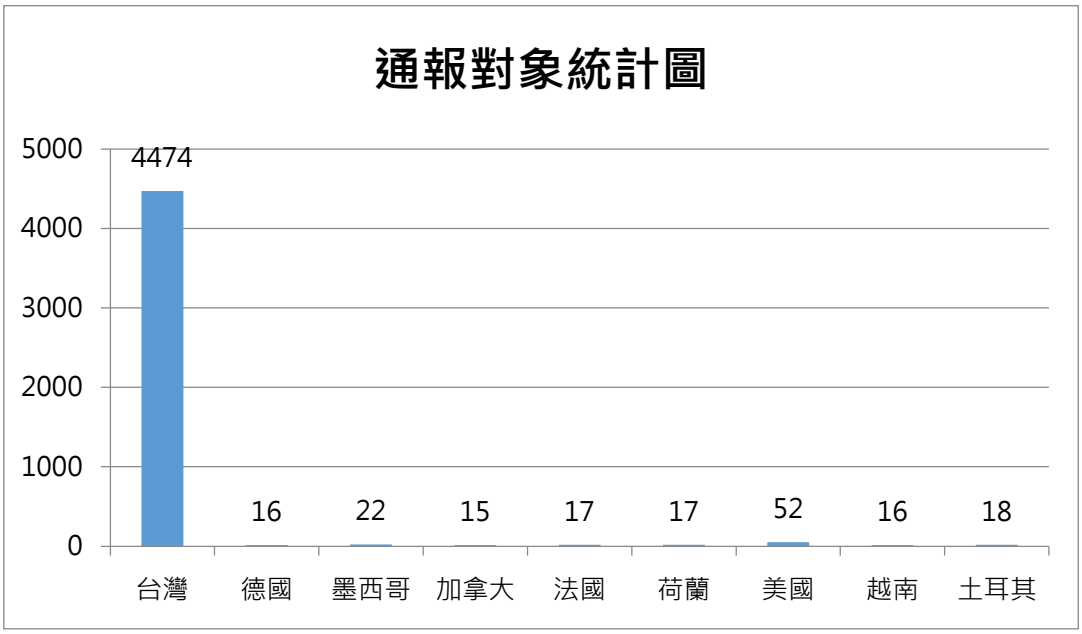


圖 2、通報對象統計圖

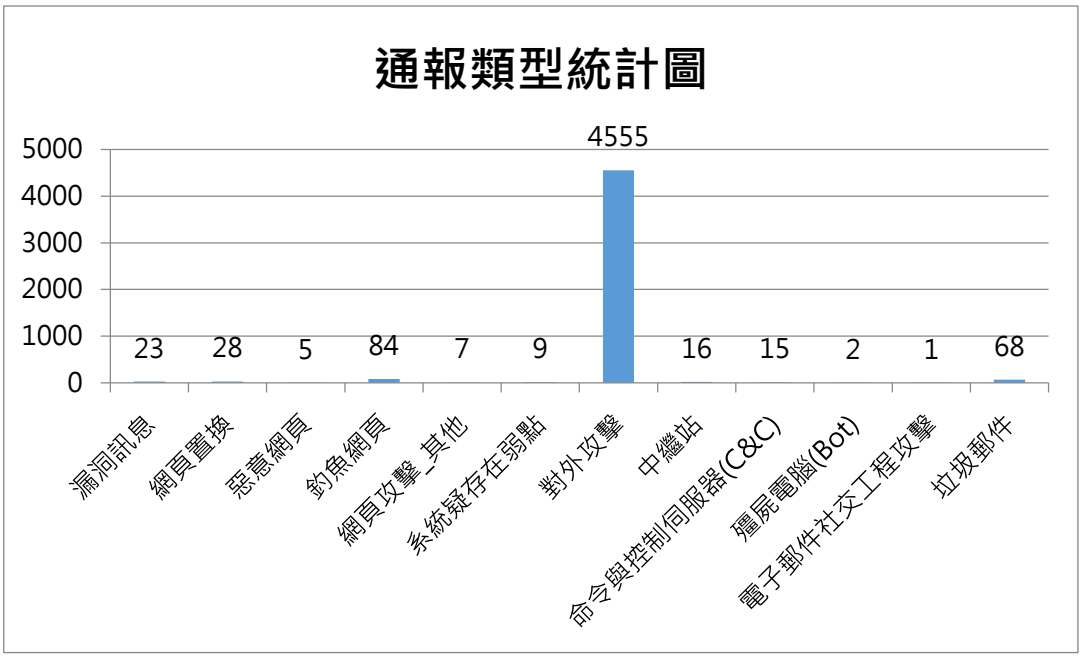


圖 3、通報類型統計圖

通報案件中，TWCERT/CC 於本月接獲美國 US-CERT 通報，由美國國土安全部與聯邦調查局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，其中台灣受影響之 IP 有 16 個。Joanap 通常是經由網頁掛馬攻擊或受害者不慎開啟惡意郵件附檔，會蒐集受害者重要資訊，如主機 IP 位址、主機名稱、現有系統時間等；而 Brambul 則是 32-bit 的 Windows SMB 蠕蟲。以暴力破解密碼方式存取受害者系統，再以電子郵件傳送受害電腦的 IP、主機名稱、用戶名稱及密碼資訊給 Hidden Cobra。

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[3]。

受影響平台為微軟作業系統，建議可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，建議處理措施如下：

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如下：

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。

參考連結：

[1]https://www.us-cert.gov/ncas/alerts/TA18-149A

[2]https://www.us-cert.gov/ncas/analysis-reports/AR18-149A

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

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 6 月 9 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。