TWCERT/CC 資安情資電子報

2018 年 8 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、參展 HITCON Community 2018 研討會

7 月 27 日至 28 日 HITCON 已於台北南港展覽館一館 5 樓舉辦 HITCON Community 2018 研討會，TWCERT/CC 此次與往年不同，除了於 HITCON CMT 2018 擺設攤位外，亦配合主辦單位的資安挑戰賽規劃，安排「挖掘受駭 IP CAM-速速通報 TWCERT/CC」的挑戰活動。

這兩天下來，所有參與 TWCERT/CC 攤位活動的挑戰者，總共貢獻了約 60 個有效 IP CAM 受駭單位，這些 IP CAM 都是有弱密碼或漏洞等問題，除了畫面被公開給全世界欣賞外，也有可能被有心人士利用當成殭屍設備進行 DDoS 攻擊等資安問題，會後 TWCERT/CC 將會主動通報這些 IP CAM 受駭的單位，請其更改密碼或修補漏洞。

2.2、協辦 107 年度高中職資安種子教師研習營

8 月 18 日至 19 日「教育部資訊安全人才培育計畫推動辦公室」，及「財團法人國家實驗研究院國家高速網路與計算中心」，已於國家高速網路與計算中心新竹本部電腦教室，共同主辦「107 年度高中職資安種子教師研習營」，此次研習營目的主要是協助培訓資安種子師資，促進資安扎根教育，TWCERT/CC 亦為此次研習營之協辦單位。TWCERT/CC 主任陳永佳受邀擔任講師，講題為：「個資外洩實務案例與防護作法」。

2.3、與「合勤科技」及「台灣賽門鐵克」簽訂合作備忘錄

為了厚植我國資訊安全自我防護能量，並建構資安聯防體系，TWCERT/CC 與合勤科技 (Zyxel Communications Corp.)建立合作機制，由合勤科技於惡意樣本檢測系統中提供技術支援及區域聯防解

決方案，協助實踐我國電腦網路安全防護與危機處理作為，打造安全可信賴的網路空間。

此外，TWCERT/CC 亦與台灣賽門鐵克再次簽訂合作備忘錄，台灣賽門鐵克將提供 TWCERT/CC 惡意樣本分析技術及最新資安情資，並與 TWCERT/CC 互助處理資安事件，共同朝向資安聯防的目標前進。

2.4、TWCERT/CC 將於 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」

TWCERT/CC 將於 10 月 3 日集思台大會議中心舉辦「2018 台灣資安通報應變年會-企業無可避免的資安管理責任」，隨著網際網路與物聯網蓬勃發展，不僅給人們帶來便利的生活，也衍伸出許多資安問題，例如電商業者網站資訊安全防護未完善，而造成客戶資料外洩，引發大量的詐騙事件；或讓有心人士成功入侵電商網站，修改商品價格，而造成電商業者財物重大損失等問題，然而電子商務之資安風險，不再僅僅是客戶資料外洩或財務損失，在新版個資法上線後，將可能影響企業商譽及巨額財務損失。

企業除了面臨上述的資安問題外，另外還有網路攝影機監控畫面外洩、勒索軟體攻擊事件、DDoS 攻擊事件、挖礦程式盛行等，亦是企業頻繁遭遇的資安問題，因此資安在當今的世代已愈來愈受重視，企業在經營時，需考量完善的資安防護，制定並落實資安政策及通報應變標準作業流程，才能即時應對席捲而來的資安威脅。

參與此場會議，可了解以下幾項課題：

(1) 面臨資安管理法的因應之道。

(2) 電子商務資訊安全的重要性及相對應的解決策略。

(3) CERT/CSIRT 任務及服務內容，並了解如何自主建置 CSIRT。

(4) 資安通報的重要性及好處，提高企業資安通報意願。

會議全程皆為免費，歡迎大家共襄盛舉！預計 9 月初開放報名！

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、金管會祭出兩大策略因應金融機構遭駭事件

金融機構遭駭客攻擊事件近年頻傳，金管會金融發展行動方案祭出兩大策略因應，首先是要拉高資安險的投保率，並訂出「資安險未來三年保費收入每年成長率 25%」的目標，建構資安網絡；二是強化投保資安保險資訊揭露，並納為上市櫃公司的公司治理評鑑加分指標項目。

資料來源：

http://www.chinatimes.com/newspapers/20180705000274-260202

3.1.2、PayPal 旗下 Venmo App 可透過其 API 窺探大多數交易

Venmo 是 PayPal 旗下的一個知名的行動支付服務，讓用戶可以使用手機或網頁轉帳給他人，2009 年創辦推出後，2012 年 BrainTree 以 2620 萬美元收購了 Venmo，而一年後 PayPal 以 8 億美元收購了 Braintree，現在 Venmo 是 PayPal 的官方子公司。

該產品的特色為人們可以公開自己的支付行為，有點類似發朋友圈，寫上轉帳事由，並添加一些表情，是美國知名的行動支付服務。然而根據最近對隱私宣導者的調查, 絕大多數的 Venmo 交易記錄在一個公開 API 中，且任何人都可以存取，原因是因為 Venmo 應用程式預設對所有用戶設置為「公開」，除非用戶特地去更改設定，否則他們透過 Venmo 匯款應用程式進行的所有交易都會被記錄下來，並透過 Venmo 公開 API 提供給任何人。

透過此 API 公開的資料包括發件人和收件人的姓名、Venmo 頭像、交易日期、交易相關的評論、交易類型等。發現此問題的隱私權倡導者 Hang Do Thi Duc 表示，他使用此隱私政策查詢 Venmo API 並下載該公司 2017 年公開交易共 207,984,218 筆資料。

並建立了一個名為「Public by Default」的網站，列出了一些相互關聯的 Venmo 付款案例，例如，Duc 追蹤與大麻經銷商、玉米經銷商、部分家庭或隨機的夫婦相關的交易，甚至某女性有關 2,033 次 Venmo 交易的故事。

Duc 也發布有關 Venmo 用戶如何將其個人資料的隱私從公開更改為私人的視覺化說明，用戶也可以訪問連結以查看公開 API 中記錄的最新 Venmo 交易。

●TWCERT/CC 建議，Venmo 用戶如不願公開交易紀錄，應進行隱私設定，以免交易紀錄曝光。

資料來源：

https://www.bleepingcomputer.com/news/security/paypals-venmo-app-exposes-most-transactions-via-its-api/

https://publicbydefault.fyi/

https://publicbydefault.fyi/#venmo

https://venmo.com/api/v5/public

https://venmo.com/api/v5/public?limit=1

3.2、駭客攻擊事件及手法

3.2.1、Adidas 美國網站遭受資料洩露，影響數百萬客戶

知名德國運動服裝公司 Adidas 發布了一項安全警報，警告客戶其美國網站可能遭駭客竊取了客戶資料。

Adidas 證實，該公司在 6 月 26 日發現有未授權單位企圖出售一批 Adidas 客戶資料，可能伺服器遭攻擊者未經授權存取客戶個人資料。 外洩資料包括客戶名稱、地址、電郵地址和加密密碼，但該公司聲稱客戶信用卡或健身資訊未受到影響，並已將資料洩露事件通知執法機構。

目前已知受影響者主要是 adidas[.]com/US 線上購物的客戶，該公司正在向這些客戶通報此事件，並聲明正在與領導品牌的資料安全公司和執法部門合作調查這個問題。

●TWCERT/CC 建議，如近期曾於 Adidas 美國網站購物之客戶，可能會成為魚叉式網路釣魚攻擊活動的目標，如接獲任何疑似來自 Adidas 之電郵，請務必確認來源，切勿輕易點選信件連結或附件，除儘速透過官網服務更改密碼 (儘可能不要透過信件提供之變更密碼連結)並應對可能的攻擊保持警惕，以免遭有心人士利用。

資料來源：

https://www.hackread.com/hackers-steal-millions-of-customers-data-from-adidas-us-website/

https://securityaffairs.co/wordpress/74001/data-breach/adidas-security-breach.html

https://news.softpedia.com/news/adidas-hacked-customer-data-exposed-521764.shtml

https://www.cyberscoop.com/adidas-data-breach/

https://wepro180.com/tech-news/%E3%80%90%E9%BB%91%E5%AE%A2%E5%85%A5%E4%BE%B5%E3%80%91adidas-%E9%81%8E%E8%90%AC%E5%AE%A2%E6%88%B6%E8%B3%87%E6%96%99%E5%A4%96%E6%B4%A9%EF%BC%81/

https://www.adidas-group.com/en/media/news-archive/press-releases/2018/adidas-alerts-certain-consumers-potential-data-security-incident/

3.2.2、Typeform 備份文件遭駭客獲取，敏感資料外洩

總部位於西班牙巴賽隆納的知名線上問卷製作服務網站 Typeform 宣布遭受未知的攻擊者下載了包含敏感客戶資訊的備份文件導致資料洩露。

備份文件包含直到 2018 年 5 月 3 日由 Typeform 客戶透過調查和線上表格收集的資料，該公司稱攻擊者從 Typeform 的伺服器獲取的備份文件中不包含 Typeform 密碼和用戶信用卡資訊。

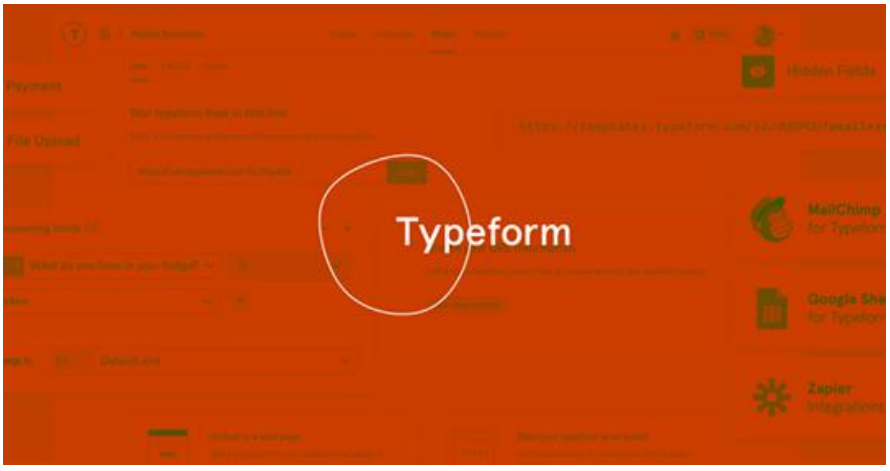
該公司表示，攻擊者利用漏洞後導致事件發生，但 Typeform 並沒有透露是什麼漏洞，僅稱已確實修補其安全漏洞。

根據事件的時間表，Typeform 表示，其員工在 6 月 27 日星期三的 14:00 CET 發現了入侵行為，並在 30 分鐘後恢復受影響的伺服器的安全，而兩天後正式宣布了這一消息。

Typeform 表示只有收到電郵通知的客戶才會受到影響，這表明備份文件可能沒有包含所有客戶的資訊，但只包含少數選定的客戶。

然而 Typeform 的客戶之一，Monzo 銀行則聲明 Typeform 洩漏事件導致其大約 2 萬位在其網站上進行調查的使用者的資料已被曝光，並表示正在徹底調查此事，且結束與 Typeform 的關係。

Monzo 銀行發布其外洩資料包括姓名、電郵地址、城市、年齡區段、薪金級別、郵政編碼、舊銀行名稱、Twitter 用戶名和所使用電郵地址、所屬大學及其電郵地址等。



資料來源：

https://www.bleepingcomputer.com/news/security/typeform-announces-breach-after-hacker-grabs-backup-file/

https://www.typeform.com/data-breach-june-2018/

https://securityaffairs.co/wordpress/74016/data-breach/typeform-security-breach.html

https://thehackernews.com/2018/06/typeform-survey-software.html

https://www.theregister.co.uk/2018/07/02/typeform_breach/

https://monzo.com/blog/2018/06/29/typeform-breach/

3.2.3、知名 APP Timehop 遭駭，資料外洩影響 2100 萬用戶

Timehop 宣布了一項安全漏洞，影響了超過 2100 萬用戶的整個用戶群。該 APP 主要功能是整合許多社群媒體，分析過去貼文或圖片用以回顧使用者歷史的今天。

該公司表示，駭客獲取了對其基礎設施的存取權限並竊取了其用戶的詳細資訊，包括用戶名、電郵、電話號碼和存取密鑰，但並非所有用戶都在其帳戶中附加了電郵地址或電話號碼。2100 萬用戶群中只有 22% (大約 470 萬用戶)在其帳戶中附加了電話號碼。此外，並非所有用戶名都包含用戶的真實姓名。

儘管如此，駭客竊取了所有 2100 萬用戶的存取密鑰。這些存取密鑰用以將 Timehop 帳戶鏈接到各種社交媒體帳戶，Timehop 並能從這些帳戶中提取過去的社交媒體貼文和圖像。

Timehop 表示，已對所有帳戶進行身分證，因此駭客將無法使用任何這些存取密鑰從用戶的第三方社交媒體帳戶 (如 Facebook、Facebook Messenger、Twitter 或 Instagram)檢索資料。

Timehop 在一份聲明中表示，沒有證據表明未經授權就存取過任何帳戶，並正與執法部門和網路安全公司合作，以追查入侵者並保護其基礎設施。

根據調查的初步證據，入侵發生在 2017 年 12 月 19 日，當時駭

客獲得對 Timehop 雲端基礎設施的管理員帳戶的存取權限。Timehop 表示，因無法使用多因素身分驗證來保護該帳戶，從而使攻擊成為可能。

駭客在 2017 年 12 月和 2018 年 3 月和 6 月的四個不同日期登錄此帳戶，在此期間進行了偵察作業，直到 7 月 4 日，當入侵者開始公開資料庫時，入侵才被發現。

Timehop 表示檢測到這個駭侵活動後，在兩小時十九分鐘便切斷了駭客的存取，現在透過多因素身分驗證保護所有帳戶，以防止進一步的入侵。並且正在採取其他安全措施。

資料來源：

https://www.bleepingcomputer.com/news/security/timehop-security-breach-affects-the-company-s-entire-21-million-userbase/

https://www.zdnet.com/article/timehop-breach-hits-21-million-users-due-to-a-lack-of-2fa-on-cloud-services/

3.2.4、新加坡最大的醫療保健集團遭駭，150 萬名患者紀錄被盜

SingHealth 是新加坡最大的醫療集團，擁有 2 家三級醫院、5 家國家級專科醫院和 8 家綜合診所，根據新加坡衛生部 (Ministry of Health, MOH)發布的一份報告，駭客竊取了大約 16 萬名患者的「門診配藥」資訊，其中包括新加坡總理李顯龍和少數部長。

MOH 表示，「2018 年 7 月 4 日，綜合健康資訊系統 (Integrated Health Information Systems, IHiS)資訊庫管理員在 SingHealth 的

一個 IT 資訊庫中檢測到異常活動。他們立即採取行動」，被盜資訊包括患者的姓名、地址、性別、種族、出生日期及國家註冊身分證(National Registration Identity Card, NRIC)號碼，並特別針對總理的「門診配藥」個人資訊進行蒐集。 到目前為止，沒有證據表明這次襲擊主謀是誰，但 MOH 表示此網路攻擊「不是任意駭客或犯罪集團的工作」，媒體也猜測這可能是國家級駭客所為

新加坡網路安全局 (Cyber Security Agency of Singapore, CSA)和 IHiS 的調查也證實，「這是一次蓄意、具有針對性，且精心策劃的網路攻擊」，新加坡政府向其公民保證，沒有醫療紀錄被篡改或刪除，並且沒有診斷、檢測結果或醫生的紀錄在攻擊事件中被盜，在接下來的五天內，醫療機構會聯繫所有受影響的患者。

而於今年 5 月 1 日正式成立的名為智慧國家及數位政府工作團隊 (Smart Nation and Digital Government Group, SNDGG) 因此次事件，新加坡政府為了讓 SNDGG 全盤審查政府系統的網路安全措施，並在必要時實施任何額外的保護措施，將「暫停」推出新的資訊通信技術系統。新加坡政府表示，目前為暫停性評估，並強調 Smart Nation 專案仍將逐步實施，沒有具體的專案存在實質性的停止風險。

由於醫療保健行業是國家關鍵基礎設施的一部分，除水、電和運輸外，它已成為一個對駭客具有強烈吸引力的目標。

SingCERT 因應此事件，提出建議的安全措施，並強烈建議企業審查其系統並對可疑活動保持警惕。

以下是企業可採取的直接措施：

(1) 查看網域管理員帳戶：域管理員可以完全控制網域。應查看並嚴格管理網域管理員帳戶，禁用已不再使用之非活動帳戶。

(2) 禁用標準工作站的 PowerShell：攻擊者可利用 PowerShell 執行惡意命令和腳本。如果標準用戶工作站不需要，請考慮禁用

PowerShell。

(3) 監控未授權的遠程存取或資料庫存取：請留意可疑的 SQL 查詢，特別是那些返回與資料庫大小相關的大量資訊的查詢。遠程存取應具有強大的登錄密碼，並且僅限於授權用戶。

(4) 加強對長期運行或退役端點的控制：監控長時間運行的端點是否存在感染跡象。退役端點應於不再使用時離線，因為攻擊者可能利用這些可能已過時的軟體和病毒定義的端點。

(5) 採用強大的端點保護：考慮為標準用戶提供企業範圍的應用程式白名單。白名單將標準用戶限制為已批准的應用程式列表，同時阻止所有其他應用程式運行，包括防毒軟體可能沒有定義的惡意軟體。

(6) 使系統保持最新狀態：應用軟體更新和安全修補程序，以便修復可能被攻擊者或惡意軟體利用的已知漏洞。

SingCERT 提到，網路攻擊仍然是一種普遍的威脅。企業需要提高警惕，以應對不斷變化的網路威脅，並採取預防措施來保護其公司的資料。

作為商業推動者，網路安全不應該是事後的想法。透過採用六個「要點」來加強組織的網路防禦：

(1) 瞭解組織資產：識別並瞭解組織的網路元件，以防止和偵測未經授權的資產存取。

(2) 只允許授權軟體運作：實現與防毒集成的應用程式控制，以便只允許授權的軟體運作。

(3) 及時修補和更新：及時修補和更新作業系統、韌體和應用程式，以減少系統已知的漏洞，從而將網路攻擊降至最低。

(4) 給出正確的管理「通行證」: 限制管理員許可權，以免給攻擊者特權來破壞系統。

(5) 及時檢測違規情況：透過使用啟用的審核跟蹤/安全性紀錄檔，記錄設置連續監視，儘快檢測違規情況。

(6) 存取控制：透過實施多因素身分驗證，確保僅授權存取。

資料來源：

https://thehackernews.com/2018/07/singapore-healthcare-breach.html

https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

https://www.bleepingcomputer.com/news/security/hackers-stole-a-third-of-singapores-healthcare-data-including-prime-ministers/

https://www.reuters.com/article/us-singapore-cyberattack/cyberattack-on-singapore-health-database-steals-details-of-1-5-million-including-pm-idUSKBN1KA14J?feedType=RSS&feedName=technologyNews

https://www.securityweek.com/singapore-health-database-hit-major-cyberattack

https://www.tripwire.com/state-of-security/security-data-protection/data-of-1-5-million-people-breached-in-singapores-worst-digital-attack/

https://www.facebook.com/125845680811480/posts/1957979740931389/
https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/7/minister-in-charge-of-cybersecurity-convenes-committee-of-inquiry
https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data
https://www.csa.gov.sg/gosafeonline/~/media/csa/documents/publications/be_safe_online/be_safe_online_infographic_english.pdf?la=en

3.2.5、越南多家銀行及主要網路基礎設施遭攻擊

越南電腦緊急事件應處小組 (Vietnam Computer Emergency Response Team, VNCERT)發出警告，近期越南國內多家銀行及主要網路基礎設施遭惡意程式攻擊，且攻擊者事前對於此些機構有詳盡的研究，利用高階技術以規劃整起事件並竊取資訊。VNCERT 副主任 Nguyễn Khắc Lịch 提出警告，政府、金融、電信、電力、航空、運輸等各領域單位皆應做好準備以防範攻擊。

有關此次攻擊事件，目前可確認之訊息如下：

C&C Server IP 列表：

(1) 38.132.124[.]250

(2) 89.249.65[.]220

惡意程式列表：

(1) syschk.psl (318KB (32624 bytes))

- MD5:26466867557F84DD4784845280DA1F27
- SHA-1:ED7FCB9023D63CD9367A3A455EC94337BB4862

8A

(2) hs. exe (259 KB (265, 216 bytes))

- MD5:BDA82F0D9E2CB7996D2EEFDD1E5B41C4
- SHA-1:FF715209D99D2E74E64F9DB894C114A8D13229A

●TWCERT/CC 建議相關單位可先行將惡意 IP 及程式加以阻擋，避免遭受攻擊。

2. Ra quet he thong va xoa cac thư mục và tập tin mã độc có kích thước tương ứng:

a) syschk.ps1 (318 KB (326,224 bytes))

- MD5: 26466867557F84DD4784845280DA1F27

- SHA-1: ED7FCB9023D63CD9367A3A455EC94337BB48628A

b) hs.exe (259 KB (265,216 bytes))

- MD5: BDA82F0D9E2CB7996D2EEFDD1E5B41C4

- SHA-1: 9FF715209D99D2E74E64F9DB894C114A8D13229A

3. Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xoá tập tin chứa mã độc trong Phụ lục kèm theo.

4. Sau khi thực hiện, yêu cầu các đơn vị báo cáo tình hình về Cơ quan điều phối ứng cứu sự cố quốc gia (Trung tâm VNCERT) theo địa chỉ email: ir@vncert.gov.vn /điện thoại: 0869100319 trước 12h ngày 26/7/2018.

5. Trên đây là những mã độc rất nguy hiểm, có thể đánh cắp thông tin và phá huỷ hệ thống thông tin, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- PGĐ Nguyễn Khắc Lịch
- Các chi nhánh, phòng: CNHCM, CNĐN, KTHT, NCPT, TV&BDNV;
- Lưu VT, ĐPƯC.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch

資料來源：

http://www.vncert.gov.vn/baiviet.php?id=100

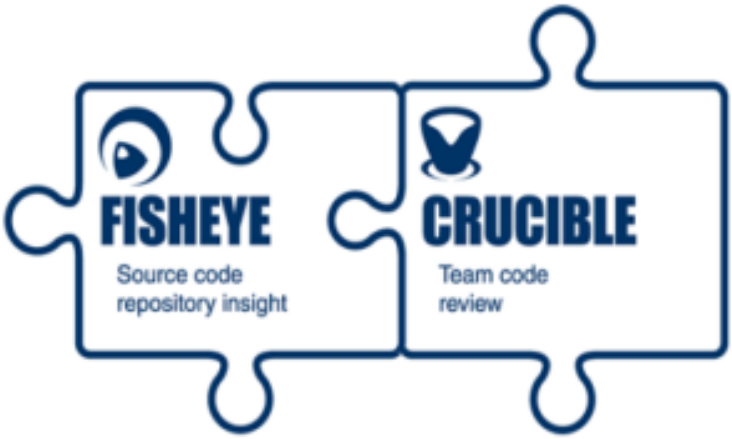
https://vietnamnews.vn/society/462371/vncert-warns-of-malicious-code-targeting-banks-and-govt-offices.html#B4OKMGzPfVp7MkR2.97

3.3、軟硬體漏洞資訊

3.3.1、軟體開發輔助工具 FishEye 及 Crucible 出現造訪路徑攻擊弱點

澳洲 Atlassian 公司為程式設計者及專案經理開發輔助工具軟體，旗下商品魚眼 (FishEye)係版本控制軟體，搜尋引擎可抽出程式碼資

產中豐富的有益資訊，於報表呈現改版差異；另熔爐 (Crucible)為協作開發工具，適用多人非同步複審程式碼之聯合設計情境。FishEye 與 Crucible 皆為網頁介面，被檢測出高風險造訪路徑攻擊(Directory Traversal)瑕疵，囿於 Attachment Review 元件對輸入字串值中路徑符號「../../..」無法檢驗剔除，攻擊者經由程式探勘，可突破路徑存取權限制，不當獲取機密檔案內容，Atlassian 已公告升級後版本。



資料來源：

https://jira.atlassian.com/browse/CRUC-8212

https://exploit.kitploit.com/2018/06/atlassian-fisheye-and-crucible-cve-2017.html

3.3.2、小心三星手機，新版 Messages APP 無預警外流隱私照片

數日前三星電子智慧手機內建簡訊軟體更新後，眾多用戶驚覺，圖庫區存放個人照片圖檔，竟在不知情下外傳，流向郵件聯絡人所列名單，三星電子表示，因豐富通訊服務 (Rich Communications Services, RCS)之 SCHEDULED TEXT 功能錯誤，故導致無端送出用戶個資事件，新版 Messages APP 尚有其他潛在異常狀況，建議暫緩安裝，待三星電子修補成功再行安裝，若然已安裝瑕疵版本，可透過設定 Messages，禁止存取儲存空間，並清除既有 Cache 資料及訊息，重新安裝以保無虞。

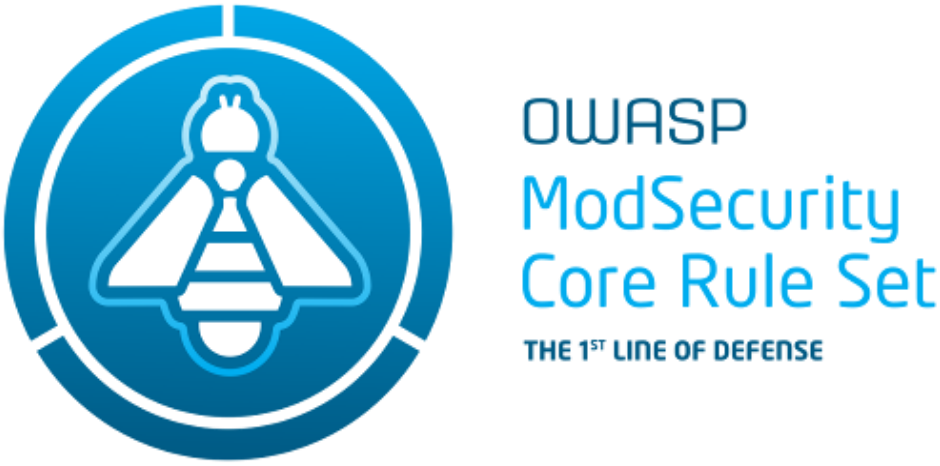
資料來源：

https://us.community.samsung.com/t5/forums/v3_1/forumtopicpage/board-id/GalaxySNineQandA/thread-id/5854/page/1

https://www.bleepingcomputer.com/news/mobile/glitch-in-samsung-messages-app-sends-photos-to-random-contacts/

3.3.3、網頁程式防火牆 ModSecurity 暗藏 XSS 缺陷

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)，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，經研究員 Adipta Basu 分析原始碼，IMG 元件之 onError 變數出現跨站台腳本攻擊弱點，攻擊者可注入 <img src=x onError=prompt(document.cookie)> 或類似結構之惡意標籤，但 ModSecurity 無法過濾且當成正常 HTML 程式碼執行，探勘實務在 Mac OS High Sierra 環境多機測試，證實 XSS 漏洞的確存在，然因 XSS 僅在非套用 Core Rule Set 環境發生，故對該漏洞是否成立仍有疑義。



資料來源：

https://hackings8n.blogspot.com/2018/07/cve-2018-13065-modsecurity-300-has-xss.html

https://www.exploit-db.com/exploits/44970/

3.3.4、亞太電信魔速方塊基地台出現雙破綻：XSS、擴權登入

亞太電信為強化特定場域信號強度，提供微型基地台，號稱魔速方塊，設備由富士康 (Foxconn)研發，據資策會資安所資安檢測鑑識實驗室 (CFL)分析指出，魔速方塊韌體設計 2 項缺失，首先是使用者帳號設定介面，於「username」欄位注入之 Script 程式碼未遭安全機制阻擋，可發動 XSS 攻擊；另外內建帳密「admin/admin」極易猜測，儘管權限低，卻成為入侵突破口，且管理系統僅靠密碼辨識帳號合法性，只要帳號有效，Cookie 內容真偽則無法驗證，駭客僅需惡意變更 Cookie 內容，將「mode=LOW」轉換成「mode=ENG」，即可接獲得工程師等級最高授權，比照高階管理者帳號 foxconn，行使完整管控，設定全部組態參數，省下暴力破解時間。CFL 已通報上述兩家鴻海集團所屬企業，韌體已修補完成。

資料來源：

https://gist.github.com/ChuanYuan-Huang/a92b8b32980123d5fa9bf5a8299114bf

3.3.5、醫療監控儀 MyCareLink Patient Monitor 二缺失，影響病患與裝置安全

知名大型醫療科技公司 Medtronic，營售 MyCareLink Patient Monitor，是用於監測病患生命跡象的看護監控儀器，經測試設備作業系統，察覺兩項缺失，一是寫死的密碼可擴權操縱作業系統；二是該監控儀 Debug Port 可連接專屬介面，攻擊者透過短距感應之通訊協定，讀寫身旁患者心律調整器之記憶體內容，恐怕干擾心臟病患脈搏，Medtronic 獲告此事，已著手修補，近期將啟動無線更新設備，居家使用該型醫材之病患及家屬，請關注更新進度。

資料來源：

https://ics-cert.us-cert.gov/advisories/ICSMA-18-179-01

https://nvd.nist.gov/vuln/detail/CVE-2018-8868

3.3.6、媒體播放器 VLC 測出 Use-After-Free 漏洞

法國非營利組織 VideoLAN 所開發 VLC (初始命名 VideoLAN Client)，係免費開源之跨平台多媒體播放器，支援多種媒介來源 (CD、DVD、硬碟)與視訊格式 (WMV、MP3、MKV)，經研究指出，該軟體具有 Use-After-Free 弱點，無論在 32 位元或 64 位元環境安裝 VLC，若攻擊者將特製 MKV 視訊檔拖曳至 VLC 介面，則有機率觸發任意程式碼執行事件，或者直接導致 DoS，VideoLAN 已升級程式版本公開下載。

資料來源：

http://seclists.org/fulldisclosure/2018/Jul/28

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11529

3.3.7、更新 VMware Tools，抑制 out-of-bounds read 缺陷

虛擬主機業者 VMware，為提升虛擬機中客體作業系統的管理效能，強化互動便利性，供應 VMware Tools 模組，然 VMware Tools 之共用資料夾驅動程式 Hgfs 存在越界讀取記憶體弱點，該弱點針對啟用檔案共享的客體 Windows 作業系統，成功探勘後可能取得系統資料內容，成為 VM 內作業系統管理者身分，VMware 已釋出新版 Tools，解決記憶體配置與邊界管理失誤。

資料來源：

https://www.vmware.com/security/advisories/VMSA-2018-0017.html

https://securitytracker.com/id/1041291

3.3.8、注意 LFI 破綻，撈取 VelotiSmart WiFi 攝影機密碼檔

無線網路攝影機 VelotiSmart WiFi B-380，採用 Unix 環境，且內部建置 uc-http service 1.0.0，囿於 uc-httpd 先天具有 local file inclusion (LFI)及造訪路徑攻擊兩類弱點，經 Miguel Méndez Zúñiga 分析，確認該型攝影機存在典型的本機檔案包含漏洞，攻擊者可直接經通信埠 80，附掛特定字串「/../../etc/passwd」，對設備所在 IP 攻擊，採取「http://192.168.x.x:80/../../etc/passwd」或類似方式，能撈取密碼檔、系統組態、無線網段掃描結果等資料，Veloti 公司暫無安全更新公告。

資料來源：

https://medium.com/@s1kr10s/velotismart-0day-ca5056bcdcac

https://cxsecurity.com/issue/WLB-2018070173

3.3.9、締奇 360 智慧清潔家電現存 RCE 與更新機制瑕疵，駭客可窺探物主隱私

中國大陸締奇智能公司主打智能物聯網設備、機器人產銷業務，其中一款吸塵器「締奇 360 攝影智能掃地機器人」，裝配 Wi-Fi、攝影鏡頭、手機操控等科技功能模組，除清潔地板外，尚可用於關懷居家老幼、夜間防盜錄影等生活需求，歐洲跨國資安設備開發商 Positive Technologies，分析出締奇 360 智慧家電現有 2 個漏洞，Wi-Fi 程式更新函數 REQUEST_SET_WIFIPASSWD 因 RCE，攻擊者可運用預設帳密 admin/888888 建立攻擊鏈，針對 MAC Address 送出 UDP Request 封包，執行任何指令；另因韌體更新程序固定搜尋 microSD 卡內 upgrade_360 資料夾檔案 upgrade.sh，駭客置換偽冒腳本檔後重開機，設備自動執行惡意程式碼，若探勘成功，將以 root 身分採取竊聽、盜錄、偷取隱私等間諜行為，該公司其他販售設備品牌，如戶外型監控器、DVR、智慧門鈴等，若配備有相同錄影模組者，亦有類似風險，不但危及屋主，恐成為殭屍網路幫兇，進行 DDoS 干擾其他 IoT 設備，此事件乃繼 LG 智慧家電弱點後第二宗類案，目前締奇智能僅承認瑕疵存在，尚未對修補方案做出回應，然使用者可旋轉機體外殼隱私保護蓋，遮蔽鏡頭。

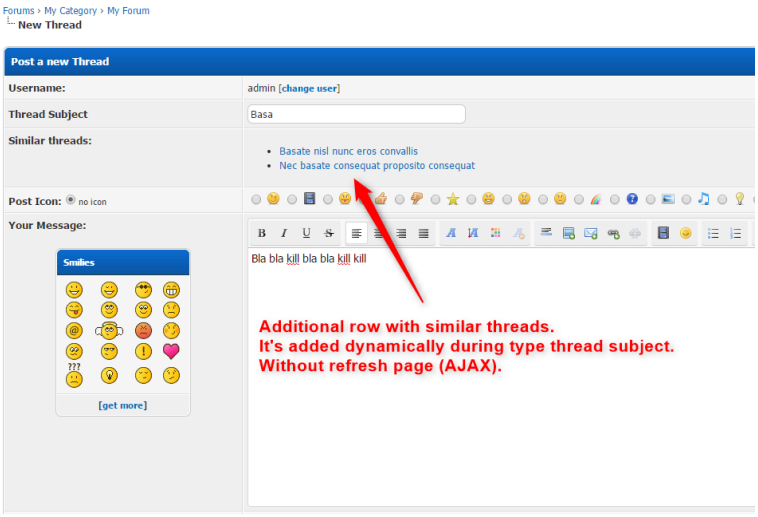
資料來源：

https://www.ptsecurity.com/ww-en/about/news/293957/

https://www.bleepingcomputer.com/news/security/flaws-in-diqee-360-smart-vacuums-let-hackers-spy-on-their-owners/

3.3.10、MyBB 釋出新版 New threads 外掛以消彌 XSS 風險

國外免費開源的論壇軟體 MyBB，使用 PHP 及 MySQL 開發，經某化名 0xB9 之駭客測試，其外掛程式 New Threads 可發動跨站台腳本攻擊，採用簡單的「<script>alert('XSS 入侵')</script>」模式，即可成功探勘發帖功能介面之標題欄位，在論壇索引網頁發生攻擊效果，MyBB 已更新該 Plugin 版本並公開下載。



資料來源：

https://community.mybb.com/mods.php?action=changelog&pid=1143

https://cxsecurity.com/issue/WLB-2018070199

3.3.11、Bluetooth SIG 更新藍牙技術規格，杜絕 MITM 攻擊

藍牙技術聯盟 (Bluetooth Special Interest Group)跨國組織，本身不負責藍牙裝置設計生產，係負責認證授權製造商，制定規範與推動技術為其宗旨，以色列研究員指出，Bluetooth SIG 所建議技術規格，未強制要求檢查雙機連線時收到的公鑰，欠缺把關機制致使底層 Elliptic Curve Diffie–Hellman 金鑰交換程序出現破綻，此瑕疵衝擊藍牙 Secure Simple Pairing 及 low energy Secure Connections 兩項功能，若兩台弱點藍牙機雙向連線，攻擊者在無線通訊距離內採取中間人 (Man-in-the-Middle, MITM)攻擊，可能攔截雙方互送公

鑰，運算出橢圓曲線加密演算之共享金鑰，而後截收後續流量並解密，甚至提供雙方假訊息，迄今無具體事證顯示該漏洞被成功探勘，Bluetooth SIG 已更新藍牙技術規格，亦通知 Apple、Broadcom、Intel、QUALCOMM、Microsoft、Android、Google、Linux Kernel 等，陸續完成各廠產品修補。

資料來源：

https://www.bluetooth.com/news/unknown/2018/07/bluetooth-sig-security-update

https://www.kb.cert.org/vuls/id/304725

3.3.12、閱讀軟體 Foxit Reader 多項錯誤恐觸發 Use-After-Free 及 Type confusion

福昕軟體公司研發數款 PDF 閱讀工具，其特色在體積小、速度快，經測試後，公開桌機 Windows 平台之 PhantomPDF、Reader 版本漏洞狀況，不當重複使用已釋放 buffer 之物件指標將導致當機；而開啟 PDF 時解析轉換 JPG 格式及執行 GetAssociatedPageIndex() 函數時，皆觸發越界存取記憶體；呼叫 addAdLayer()及函數解析 ColorSpace 元件有機會衍生類型混淆；匯出資料功能之 JavaScript 未過濾檔案型態，導致任意檔案寫入事件；而濫用大量緩衝區配置將耗損資源而 crash，上述漏洞伴隨特定函數及參數運用時發生，故使用 Foxit 軟體，出現 Remote Code Execution 機率頗高，亦有機會洩漏系統資訊，Foxit 就相關版本軟體進行升級並公告。

資料來源：

https://www.foxitsoftware.com/support/security-bulletins.php

https://securitytracker.com/id/1041353

3.3.13、防毒軟體 ClamAV 三種漏洞皆能引發 DoS

以 C 語言編輯的 Clam AntiVirus (ClamAV)，係思科及推廣者社群開發，開放原始碼且軟體與病毒碼免費更新，主要應用在 Unix-like 系統架設的 mail server 掃毒，也移植到 Windows 與 Mac OS X 平台，特色是能透過文字介面下運作，且非即時掃描器，但可被其他應用程式即時呼叫執行掃描，經測試 ClamAV 具三項弱點，均導致服務阻斷，駭客變造惡意檔案，在解析 HWP 文件時可觸發 parsehwp3_paragraph()函數之整數溢位，造成無限迴圈；而解析特製 PDF 物件時，恐因過度耗時而擱置全部程序；另在 Windows 環境內 parser.c 程式演算法無法防止參數 entity 產生無限遞迴，目前已推出升級版改善上述缺陷。

資料來源：

https://blog.clamav.net/2018/07/clamav-01001-has-been-released.html

https://secuniaresearch.flexerasoftware.com/secunia_research/2018-12/

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
2018/10/03	2018 台灣資安通報應變年會-企業無可避免的資安管理責任	【資安研討會】2018 台灣資安通報應變年會-企業無可避免的資安管理責任 日期：2018 年 10 月 3 日 (三) 地點：集思台大會議中心 (台北市羅斯福路 4 段 85 號 B1) 參與對象：中小企業組織及團體 主辦單位：台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 報名費用：全程免費，預計 9 月初開放報名！ 參與此場會議，可了解以下幾項課題： 1.面臨資安管理法之因應之道。 2.電子商務資訊安全的重要性及相對應的解決策略。 3.CERT/CSIRT 任務及服務內容，並了解如何自主建置 CSIRT。 4.資安通報的重要性及好處，提高企業資安通報意願。 活動概要： 隨著網際網路與物聯網蓬勃發展，不僅給人們帶來便利的生活，也衍伸出許多資安問題，例如電商業者網站資訊安全防護未完善，而造成客戶資料外洩，引發大量的詐騙事件；或讓有心人士成功入侵電商網站，修改商品價格，而造成電商業者財物重大損失等問題，然而電子商務之資安風險，不再僅僅是客戶資料外洩或財務損失，在新版個資法上線後，將可能影響企業商譽及巨額財務損失。 企業除了面臨上述的資安問題外，另外還有網路攝影機監控畫面外洩、勒索軟體攻擊事件、DDoS 攻擊事件、挖礦程式盛行等，亦是企業頻繁遭遇的資安問題，因此資安在當今的世代已愈來愈受重視，企業在經營時，需考量完善的資安防護，制定並落實資安政

時間	研討會/課程名稱	研討會相關資料
		策及通報應變標準作業流程，才能即時應對席捲而來的資安威脅。
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。
2018/08/24	2018 數位政府高峰會	【資安研討會】2018 數位政府高峰會 日期：2018 年 08 月 24 日 (五) 地點：台北富邦國際會議中心 B2 (台北市敦化南路一段 108 號) 主辦單位：iThome 線上報名連結： https://egov.ithome.com.tw/index.html 活動概要： 「2018 數位政府高峰會」特別邀請產官學研各界專家，多位中央、地方政府機關與專家來分享數位國家、數位治理、公私協力、服務創新、智慧城鄉與資安威脅防禦等實務經驗，一同探討數位政府與數位公

時間	研討會/課程名稱	研討會相關資料
		務員應具備的新能力，協助臺灣在數位轉型浪潮掌握契機。 此外，有鑑於總統府帶頭舉辦社會創新黑客松的創舉，本屆數位政府高峰會亦特別邀請總統盃黑客松五組得獎團隊現身說法，分享這段公私協力共同創新政府服務的成果，並將如此寶貴的經驗推廣給更多的公務同仁，一起參與推動政府進步創新的行列。 本屆數位政府高峰會，內容不僅多元且豐富，對於身為數位政府一員的您，絕對不能錯過！
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

時間	研討會/課程名稱	研討會相關資料
		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
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：

時間	研討會/課程名稱	研討會相關資料
		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
2018/09/19-20 2018/09/26-27	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(第二梯)	【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 07 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 7 月收到通報計 3847 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。

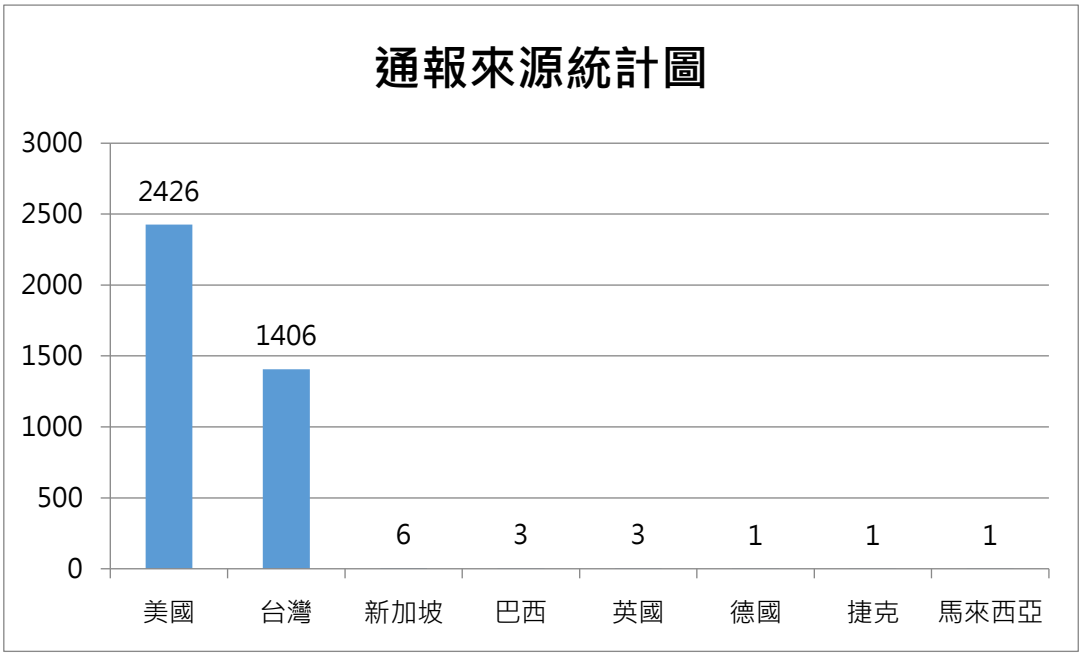


圖 1、通報來源統計圖

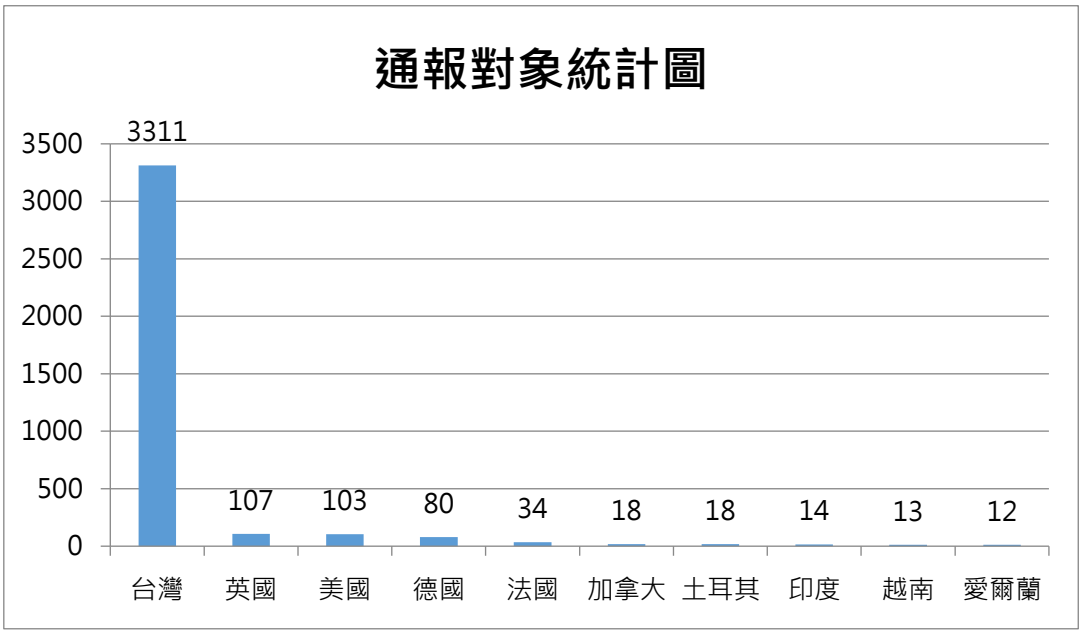


圖 2、通報對象統計圖

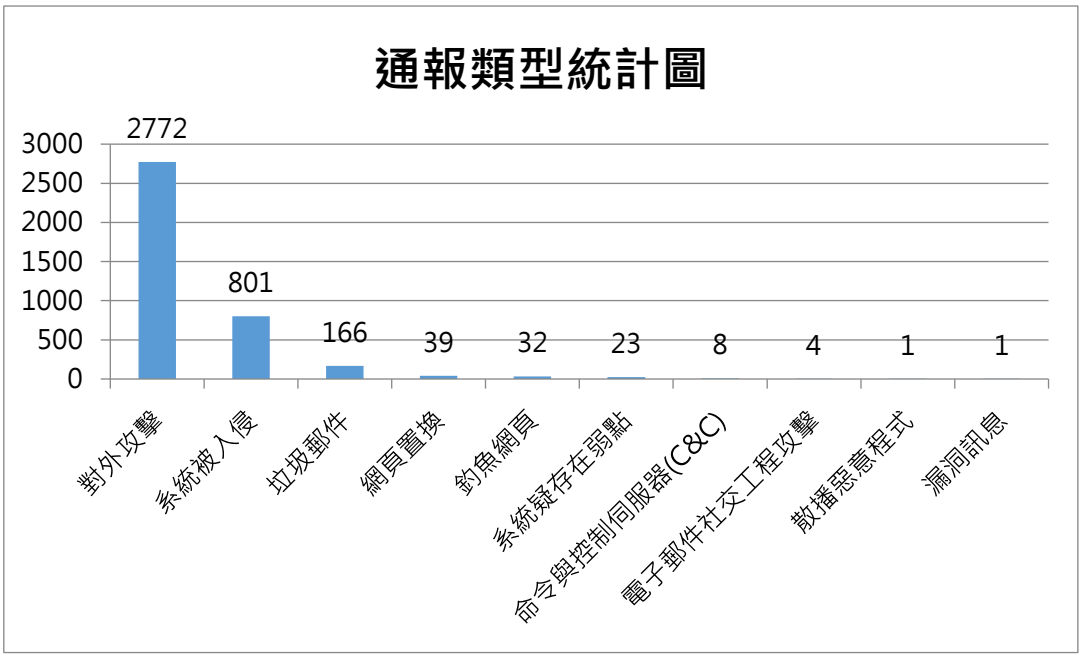


圖 3、通報類型統計圖

本月通報案件中以「蘋果電腦系統惡意程式果蠅 (Fruit Fly)」事件屬特殊案件。近期被發現的針對 Mac 系統的後門程式 Fruitfly，可被攻擊者取得系統控制權進而監控 Mac 的網路攝影機、鍵盤和其他

敏感資源，目前已知感染了 Mac 至少五年，受害人數近 400 人以上，據了解，這個惡意程式可能已經活躍了超過 10 年。

美國司法部 (Department of Justice, DOJ)在 2018 年 1 月 10 日正式起訴 Mac 惡意程式 Fruitfly 的作者 Phillip Durachinsky，Durachinsky 雖然只有 28 歲，但他從 2003 年到 2017 年間利用 Fruitfly 感染了數千台 Mac，這些 Mac 隸屬於個人、企業、學校、警察局及政府組織，之後 Durachinsky 便可存取這些 Mac 上的資料、上傳檔案、拍攝與下載螢幕截圖、側錄鍵盤，或是打開 Mac 上的攝影機與麥克風、竊取受害者的個人資料，諸如登入憑證、稅務紀錄、醫療紀錄、照片、金融紀錄。

資安業者 Malwarebyte Labs 直至 2017 年 1 月才發現 Fruitfly 的存在，當時 Malwarebyte 即判斷 Fruitfly 是很早以前就寫好，因為 Fruitfly 參考的是老舊的文件，使用老舊的程式碼與技巧，而且很容易就被偵測到，也能很快移除它。因此若能將 Mac 作業系統更新至 El Capitan 之後的版本，將可降低遭植入 Fruitfly 的風險。

●TWCERT/CC 提醒蘋果 OSX 用戶參考以下 VirusTotal 連結，若有檔案名稱為 fpsaud，應儘速刪除，並且保持 Mac 作業系統及防毒軟體有最新的安全更新。目前至少有 29 款防毒程式可以偵測到 Fruitfly 惡意程式(OSX.Backdoor.Quimitchin)。 根據 9to5mac 報導，蘋果已於 2017 年 1 月時，發布安全更新，建議用戶更新作業系統至 El Capitan 之後的版本，以避免遭植入 Fruitfly 惡意程式。

● Fruitfly 的 VirusTotal 檢測結果：https://www.virustotal.com/zh-tw/file/befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271/analysis/

●參考連結：

[1] http://securityaffairs.co/wordpress/61342/breaking-news/fruitfly-macos-backdoor.html

[2] http://mashable.com/2017/07/24/mac-malware-fruitfly-beware/?utm_campaign=Feed:+Mashable+(Mashable)&utm_cid=Mash-Prod-RSS-Feedburner-All-Partial&utm_source=feedburner&utm_medium=feed#GQF_f7i_JmqL

[3] https://9to5mac.com/2017/07/25/mac-malware-teenager-theory/

[4] https://twcert.org.tw/subpages/securityInfo/hackevent_details.aspx?id=844

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 8 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。