TWCERT/CC 資安情資月報

106 年 07 月份

臺灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Teams / Coordination Center

目錄

第 1 章、摘要

在 TWCERT/CC 近期動態部分，本中心於本月參與 2017 國際資訊安全組織台灣高峰會及 iThome Security Forum 資訊安全論壇，並於資安論壇中針對勒索軟議題進行發表。

在資安政策方面，資訊資安新法並進，安全基礎下推動台灣數位經濟；南韓外交部要制訂計畫，打擊網路攻擊；新加坡進行代號為「Exercise Cyber Star」的國家網路安全演習，且欲推出道德駭客註冊機制；美網戰司令部，將脫離國安局獨立，且卡巴斯基同意提供程式碼給美國政府；日擬擴編網路防衛隊，強化攻防戰力；法國招聘精通中文的資安特工；柬埔寨也加快制定網路犯罪法腳步；德國設特別指揮中心，嚴防 G20 峰會期間網路襲擊。資安威脅方面，Google 在 Android Play 商店發現 Lipizzan 間諜程式，另駭客可能利用飯店的免費 Wi-Fi 傳送惡意軟體，另 Petya 勒索軟體作者公開解密主密鑰，可以解 Petya 系列但不適用 notpetya (petwrap)。資安趨勢方面，美國聯邦調查局與國土安全部提出警告，核子設施將是駭客鎖定攻擊的目標。

在駭客攻擊事件方面，台灣遭網路間諜集團 BlackTech 鎖定竊取機密技術；網路電台服務 8tracks 遭駭，1800 萬筆帳戶資料遭竊；請小心 Fruitfly 惡意程式，被發現已感染數百台 MAC 電腦；馬來西亞金融公司遭 DDOS 攻擊並勒索比特幣，專家提供 IT 部門相對應行動方案，而義大利聯合信貸銀行遭駭，40 萬筆客戶資料外洩；圖片辨識軟體 CopyFish 的 Chrome 套件遭駭，請盡速移除

在軟硬體漏洞部分，Oracle、Cisco、Joomla!及 Microsoft 都發布 7 月之安全更新；PHP 的多重缺陷將可讓遠端使用者獲得機敏資訊；Apache 網頁伺服器 mod_http2 模組發現弱點，可使駭客發

動阻斷服務攻擊；Fortinet FortiOS 輸入驗證之漏洞將讓駭客使用遠端方式進行跨網站指令碼(Cross-Site Scripting)攻擊；Samba 釋出重大安全更新。

在資安研討會及活動部分，企業面對威脅軟體的自救之道、2017 亞洲跨國黑客松台灣團隊選拔賽、性別駭客工作坊-Line Bot 教學工作坊、HITCON Community、2017 年第二屆 VR 開發者黑客松大賽、CLOUDSEC 2017 企業資安高峰論壇、CISSP®資訊安全系統專家認證、SSCP 資安專業人員認證等活動皆已可開始報名，歡迎大家踴躍參加。

在本月份事件通報統計部分，分別介紹通報來源統計圖、攻擊來源統計圖及攻擊類型統計圖等統計數據。

第 2 章、TWCERT/CC 近期動態

2.1、7 月 11 日至 13 日參加 2017 國際資訊安全組織台灣高峰會

TWCERT/CC 於 7 月 11 日至 13 日參加 2017 國際資訊安全組織台灣高峰會，於會中擺設攤位並介紹 TWCERT/CC 服務內容，另外也向與會聽眾進行相關資安通報流程及作法、資安防護意識等相關宣導作業，另外也於攤位上舉辦抽獎活動，鼓勵與會聽眾填寫問卷並訂閱 TWCERT/CC 每月免費資安月報。

2.2、8 月 1 日及 8 月 10 日參加 iThome Security Forum 資訊安全論壇-企業面對勒索軟體的自救之道

TWCERT/CC 於 8 月 1 日及 8 月 10 日參加 iThome Security Forum 資訊安全論壇-企業面對勒索軟體的自救之道，TWCERT/CC 副主任吳專吉將於會中針對「從 WannaCry 與 Petya 勒索軟體行為，看企業如何因應?」進行相關分享。

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、Google 在 Android Play 商店發現 Lipizzan 間諜程式

日前，Google 安全研究人員發現了一系列名為 Lipizzan 的 Android 間諜程式，可以竊取用戶大量的資訊，包含文字簡訊、電子郵件、語音留言、位址資訊等。推測是由以色列 Equus Technologies 公司開發的，Google 的部落客稱呼他為「網路武器賣家」，透過 Google Play Protect 的協助，Android Play Store 在至少超過 20 種應用程式中發現這個 Lipizzan 間諜程式。

Lipizzan 間諜程式攻擊手法分析，可區分兩個階段：

（1） 第一階段，攻擊者將 Lipizzan 間諜程式偽裝成合法的應用程式，透過 Android Play Store 散佈出去。

（2） 第二階段，一旦使用者在 Android Play Store 安裝了受感染的應用程式，Lipizzan 間諜程式會自動下載「授權憑證」，以確保設備不會發現它的存在。完成驗證後，會透過已知的漏洞，去監控跟竊取受害者的資訊。

此外， Lipizzan 還可以收集特定應用的數據，從而破壞其加密技術，包括 WhatsApp、Snapchat、Viber、Telegram、Facebook Messenger、LinkedIn、Gmail、Skype、Hangouts 和 KakaoTalk 等通訊社群軟體。

Google 提供如何保護您的 Android 設備不受駭客攻擊，您可以透過以下的步驟來做好防護措施：

（1） 確保您已經加入 Google Play Protect。

（2） 從官方的 Play 商店下載及安裝程式。

（3） 設定啟用「驗證應用程式」功能。

（4） 用 PIN 碼或密碼鎖保護您的裝置。

（5） 將安裝「未知來源」功能選項保持關閉。

（6） 將設備的安全性更新（含漏洞修補）保持在最新的版本。

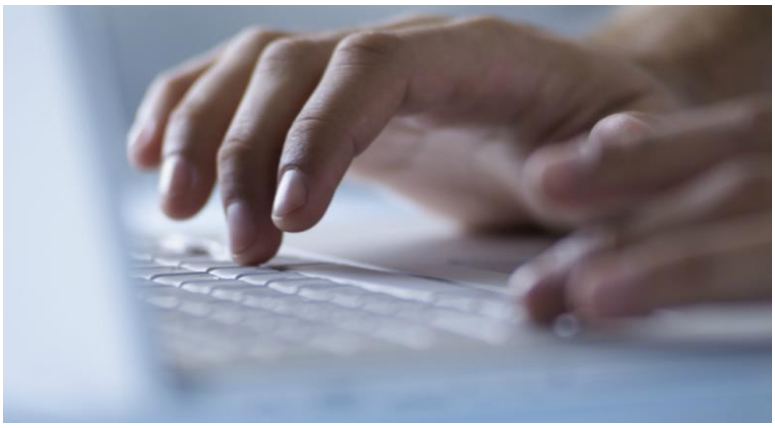
（資料來源：美國 The Hacker News）

3.1.2、駭客可能利用飯店的免費 Wi-Fi 傳送惡意軟體

飯店為了讓顧客自由及方便地在飯店使用網路，通常會提供了免費 Wi-Fi，但這些免費 Wi-Fi 並沒有足夠防禦能力去抵擋駭客的入侵。

有個存在十多年的駭客組織名叫「Dark-Hotel」，最近重新活躍起來，他們會先以實體方式入侵飯店的 Wi-F 設備，接著使用釣魚郵件或社交工程的方式入侵受害者電腦，他們針對住在奢華飯店的商務人士進行攻擊，首先傳送附帶惡意軟體的電子郵件，惡意軟體不會一次傳送完畢，而是分階段傳送，這種分階段傳送的方式可以降低被檢測出來機會，而最後可能會使用一個 word 檔分散使用者注意，同時在後端執行惡意程序。

Dark Hotel 非常小心的隱藏自己的蹤跡，資安公司 Bit Defender 的威脅分析師則指出，考慮到駭客攻擊的複雜性，不排除這是一個由國家支持的駭客組織。



（資料來源：美國 BGR）

3.1.3、南韓外交部要制訂計畫，打擊網路攻擊

南韓政府官員於 23 日表示，外交部近期將制訂一項中期計畫，以提升應對網路攻擊的能力。南韓政府單位和其他公家機構面臨與日俱增的網路威脅。外交部的網站受到駭客的分散式阻斷服務攻擊（DDoS），全球各處也受到勒索軟體的危害。外交部計劃於 8 月和外部的網路安全機構簽訂合約，在今年規劃出 2018 至 2022 年的實行藍圖，一步步提升網路安全。外交部官員表示，此次計畫旨在提升整體資訊安全系統的能力，保護外交電報等重要訊息免受網路攻擊，他亦指出，將對於首爾外交部大樓以及全球 184 個外交使館的網路弱點進行全面性評估。

（資料來源：臺灣聯合新聞網）

3.1.4、新加坡進行代號為「Exercise Cyber Star」的國家網路安全演習

7 月 18 日，新加坡網路安全局（CSA）進行了代號為「Exercise Cyber Star」的國家網路安全演習，有 11 個關鍵資訊基礎設施部門首次在國家網路安全演習中進行了測試，目的是將網路事件管理和應變計劃納入考核。

來自 11 個行業和超過 200 名參與者，其中包括行業主管和 CII 所屬單位，共同參與了此次演習。演習場景涵蓋了不同類型的網路攻擊，包括網頁竄改、大規模資訊外洩、勒索軟體、阻斷服務攻擊和實體安全攻擊，參與者則開發和測試他們的事件管理和修復計劃，以應對這些模擬攻擊。

CSA 首席執行官 David Koh 表示：「這些演習對於將所有關鍵部門整合在一起，更重要的是加強各部門的事件應變計劃和促進跨部門之間的協調。」

（資料來源：新加坡 OPENGOV）

3.1.5、新加坡欲推出道德駭客註冊機制

根據一項等待決議的網路安全法案，新加坡正在為推出「道德駭

客註冊機制」而徵求意見。儘管看似有所限制，但對於從事網路安全行業的道德駭客和相關企業來說，他們都將受益於這項許可政策。

該提案第四部分寫到：「隨著業界對可靠網路安全服務需求的增長、以及網路安全風險變得愈加普遍，該法案旨在為滲透測試和安全服務的運營管理提供授權。授權框架將提振網路安全服務、解決業內的資訊不對稱，以及提升網路安全服務提供商和專業人員的標準」。

如果這項網路安全法案獲得通過，企業將能夠雇用更可靠的人才去修補軟體。對於道德駭客來說，他們也無需再冒著遊走在法律紅線邊緣的風險去尋找和匯報漏洞。

（資料來源：美國 Neowin）

3.1.6、防止網路釣魚攻擊，Google 將對未經驗證的程式秀出警告訊息

Google 已經通過對“未經驗證(unverified app)”的第三方應用程式的新警告，提升了 G Suite 生產力應用程式的安全性，使用者遇到尚未通過驗證的網路程式或 Apps Script 時將會秀出警告訊息，這項新的程序是為了解決今年 5 月所發生的 Google Docs 網路釣魚攻擊事件。

這個“未經驗證”的螢幕畫面，取代了原有使用者看到的“錯誤”

的畫面，透過這項新的告警程序，讓使用者可以藉由更清楚的訊息與更繁複的程序，來降低造訪未授權程式的機會，也減少了受釣魚攻擊事件的風險。

Google 上週也將這項保護措施擴展到 App Script 上，而這項措施也讓開發人員更輕鬆的測試他們的 App。因為使用者會看到告警的螢幕，所以程式開發人員在測試應用程式時，不用先經過使用者授權的流程。這項保護措施一開始會先運用在新建立的程式上，後續將會推廣到現有的應用程式。

（資料來源：美國 PC & TECH AUTHORITY）

3.1.7、美網戰司令部，將脫離國安局獨立

網戰司令部獨立的目的，在於賦予其更多自主權，使其不再受到與國安局共同作業的限制。

美國網戰司令部負責執行網路攻擊暨防禦作戰行動，自二〇〇九年成軍以來隸屬美國國安局，而美國國安局負責監控與蒐集全球電話、網路及其他情資，但這類職掌有時可能與美國對敵對勢力採取的軍事作戰行動牴觸，為了賦予網戰司令部更多自主權，正計畫將其獨立，使其不再受到與國安局共同作業的限制。此外，美國亦決定提升其能力，將網路作戰併入其日常作戰範疇，並規劃網戰司令部獨立為一個

軍事司令部，將使數位空間的作戰與在陸、海、空和太空等傳統範圍的作戰擁有相同基礎。

（資料來源：TAIWAN DAILY）

3.1.8、日擬擴編網路防衛隊，強化攻防戰力

日本《共同社》報導，防衛省正考慮大幅度強化其「網路防衛隊」的規模與能力，預計將擴編 10 倍至千人之譜，且為更有效地因應網路攻擊，可能成立專門研究進行網路攻擊的新部門，作為「假想敵部隊」。

報導引述政府消息人士表示，防衛省計畫在 2019 年《中期防衛力整備計畫》中，將網路防衛隊規模由目前的 110 人，大幅擴編至 1000 人，並於 2018 年預算中先計入數十人份的必要經費。人員方面，除了從陸自「系統防護隊」、海自「保全監察隊」、空自「系統監察隊」或其他單位調來擁有通資電專長的自衛隊員外，也有雇用民間人員的想法。

另外，由於防衛省認為研究網路攻擊方式有助於防衛能力建構，也將繼續爭取成立專門研究如何進行網路攻擊的新部門。不過自衛隊發動網路攻擊可能侵犯日本憲法保障的通信秘密自由，並違反自衛隊

「專守防衛」的理念，因此在現行規劃中，該部門僅擔任假想敵；未來是否對外來網路攻擊發動自衛權反擊，官員表示，「需要進行個別具體的判斷」。

據悉，新設的攻擊部門僅限於防衛省與自衛隊的網路內，在模擬演習等時負責展開攻擊，攻擊行動的經驗則用於構築防衛能力，政府相關人士強調：「研究攻擊方法對構築恰當的防禦體系來說是不可或缺，防衛隊本身並不是為了進行網路攻擊而存在。」

日本將主辦 2020 年東京奧運和殘障奧運會，因此自衛隊 2014 年 3 月成立網路防衛隊，國會則在 2014 年 11 月通過《網路安全基本法》，讓政府於 2015 年 1 月成立網路安全戰略本部，內閣官房情報安全中心也於同日改組為網路安全中心，強化因應網路攻擊的能力。

（資料來源：臺灣青年日報、臺灣自由時報）

3.1.9、Petya 勒索軟體作者公開解密主密鑰，可以解 Petya 系列但不適用 notpetya (petwrap)

2017 年 6 月 28 日 Not Petya 勒索軟體造成許多國家多種災情，而近日 Petya 勒索軟體的作者(自稱為 Janus Cybercrime Solutions)

則正式公開了他的解密主密鑰，可以用來解密遭到所有 Petya 家族加密的檔案。Petya 家族一共有三個不同的版本，依照被感染後出現紅色、黃色以及綠色的骷髏頭而定。

雖然 NotPetya 是根據 Petya 變種而來，但 NotPetya 用了不同的加密方式，因此這組密鑰無法用來破解 NotPetya 的受害檔案。

（資料來源：美國 Merkle）

3.1.10、美國聯邦調查局與國土安全部提出警告，核子設施將是駭客鎖定攻擊的目標

依據美國聯邦調查局及國土安全部上週發表的聯合報告指出：「自五月以來，駭客持續滲透美國及其他國家經營核電廠與能源產業公司的網路，Wolf Creek 核能公司就是其中一家被攻擊的對象。」

紐約時報揭露，他們已取得相關的報告，這些攻擊事件也獲得網路安全專家的確認。但文件中並未提到有關攻擊動機的資訊（是屬於破壞事件或是網路刺探行為），目前無法得知，攻擊者是否已全般掌握對目標網路的攻擊能力以及獲得這些設施控制系統的存取權限。

攻擊者先針對目標設施採取一連串的偵察活動，蒐集資訊以利採取後續攻擊行動。Wolf Creek 公司對此攻擊事件不發表評論，他們澄清並沒有任何作業系統受到影響，而且公司與設備的網路並未相互連結；調查人員目前無法判別攻擊者使用的是哪種惡意軟體。

目前的攻擊行為並沒有影響到公共安全，大多數攻擊事件都僅限於行政及商業網路的範圍。紐約時報報導：「目前攻擊的對象，鎖定在可以直接存取系統的控制工程師，而非直接攻擊設備，如果這些設備遭到破壞，將導致爆炸、火災或洩漏危險物質。」

專家指出，這些攻擊者屬於國外的 APT 組織，駭客對會存取控制系統的工程師進行釣魚郵件攻擊，透過寄發惡意 word 文件(此處為假借寄發履歷文件)的方式，誘騙這些工程師開啟惡意附件，以植入惡意程式，竊取工程師的憑證，進而取得控制系統的權限，以利他們可以進入目標網路。此外，駭客也透過水坑式攻擊，透過入侵合法網站來散佈惡意軟體。

美國國土安全部認為，針對關鍵基礎設施的網路攻擊事件，將是國家安全面臨到的最大挑戰之一。

（資料來源：美國 MUST READ）

3.1.11、資訊資安新法並進，安全基礎下推動台灣數位經濟

資訊長四法草案已完成一讀，期望能重新定位資安部門，並由資訊總處統一指揮、協調資訊政策並進行跨部會資訊整合。

一直以來政府部門推動資安總是窒礙難行，另一方面，各行業盼

望資訊科技能協助企業轉型，資訊部門能成為帶動企業創新的火車頭時，資訊長的角色也被賦予更高的期待。因此，各界開始呼籲台灣需要設立國家級資訊長，協助推動政府數位治理、邁向數位國家。

有鑒於此，去（2016）年底立委余宛如等人提出資訊長四法草案並完成一讀，包括新增「行政院資訊總處組織法」草案、「政府資訊單位人員設置管理條例」草案，以及修正「中央行政機關組織基準法」和「行政院組織法」部分條文。期望能將資訊部門由現在的幕僚單位重新定位為業務單位，資訊總處統一指揮、協調資訊政策並進行跨部會資訊整合，而政府資訊人員也能做到更好的流動升遷。

余宛如亦比較美國聯邦資訊安全管理法(FISMA)2014 年版與行政院版資安法後，認為以下三大部分後續應更清楚定義並修正以減少爭議：第一、強調市場機制。第二、資安組織架構明確、職責分明。第三、中央目的事業主管機關對非公務機關的監管權過大且自身責任未明。

（資料來源：臺灣資安人）

3.1.12、法國招聘精通中文的特工

為打擊 ISIS 極端組織及網路犯罪，法國情報部門招聘新人，特別是具有電腦或語言能力者，包括中文、俄文及波斯文。

為打擊伊斯蘭國（ISIS）極端組織及網路犯罪，法國情報部門加緊招聘新人，理想人選是具有電腦或語言能力者，包括中文、俄文及波斯文。法國境外安全總局（DGSE）是相當於美國中央情報局或英國軍情六處的情報單位，局長莫羅（Charles Moreau）日前接受路透社採訪時表示，應對 ISIS 武裝分子及網路駭客，對特工新人的能力要求已有所改變。他亦指出，DGSE 不再有興趣招聘像 007 情報員電影主角龐德的人才，而是要求「具備各種電信和訊息技術能力者，包括加密專家到電腦超級怪咖，都是我們有興趣招聘的對象」。

DGSE 目前每年招聘 500 到 600 名特工，預計在 2019 年增加到 7,100 名。網路時代的來臨，各行業對電腦人才需求趨急，對此，莫羅表示，想要找到這樣的人才並不容易，競爭激烈，但是「我們不能坐在這裡等他們上門，而是要主動出擊，找到這些人才」。另外，莫羅也意識到語言對情報工作的重要性，必須招聘語言專家，特別是精通俄文及中文的人，以及為了打擊 ISIS 所需要的阿拉伯語及波斯語人才。

（資料來源：臺灣大紀元）

3.1.13、柬埔寨加快制定網路犯罪法腳步

為了因應層出不窮的網路威脅，柬埔寨政府將加速完成新的網路犯罪法草案。6 月 30 日，柬埔寨政府在金邊招開了 4G LTE 國際會議，

會中亦針對資安對策進行討論。網路犯罪法的草案是由資通訊安全部所支援，並由內政部監督，兩個部門目前正在針對美國的資安法架構進行研究。

資通訊安全部的官員指出，目前資安法案還在制定中，因此國民應該對於網路犯罪更加小心，特別是利用網路進行交易的電子商務廠商。網路犯罪的法律還不存在，因此對於某些交易行為是不是有犯罪意圖，目前還很難定義。

（資料來源：日本 BUSINESS PARTNERS）

3.1.14、卡巴斯基同意提供程式碼給美國政府

過去幾天，美國政府傳出提案禁止軍方使用卡巴斯基(Kaspersky)產品的消息，以避免該公司向俄羅斯政府提供美國蒐集到的漏洞或情資訊息。

卡巴斯基的發言人對此表示聲明，指出卡巴斯基身為私人企業，並不隸屬於任何政府組織，卡巴斯基也從未或是將要幫助進行網路間諜行為的政府。卡巴斯基的 CEO Eugene Kaspersky 則在 7 月 2 日時向報社指出，卡巴斯基願意將程式碼提供給美國政府，並證明他們的產品並沒有任何惡意行為，卡巴斯基也願意做任何事以取得信任。

俄羅斯政府同樣的也對數個美國公司提出檢查程式碼的要求，

Cisco、IBM、Hewlett Packard Enterprise、McAfee 及 SAP 已經同意提供防火牆及防毒軟體等產品的程式碼，而 Symantec 則表示由於涉及產品風險，因此不願意提供。

不論對於美國或是俄羅斯政府來說，當私人企業將產品程式碼提供給政府，代表政府可能會有機會找到程式碼中的漏洞，並利用漏洞將產品做不當使用，這則是政府及私人企業都必須斟酌考量的議題。

（資料來源：美國 Gizmodo）

3.1.15、德國設特別指揮中心，嚴防 G20 峰會期間網路襲擊

據報導，全球 20 個主要經濟體的領導人定本月 7 日和 8 日齊聚德國漢堡召開峰會。德國網路安全監管部門聯邦資訊安全局局長 Arne Schoenbohm 表示，當局要嚴防與外國政府有關聯的駭客組織對峰會發動網路攻擊，為此已設立了一個特別指揮中心，全天候防範網路襲擊。Arne Schoenbohm 指出，德國當局雖未收到任何襲擊情報，但為防萬一，展開了多次「滲透測試」，通過模擬駭客可能採用的攻擊技術，來評估峰會使用的電腦網路是否存有弱點或漏洞，以便及時修補，提升其安全性。當局也安排數十名網路專家隨時待命，嚴防駭客發動襲擊。

報導稱，預料此次峰會將引來數以萬計示威者，當局將出動大約兩萬名警察，在警犬、馬匹和直升機的支援下，防範示威者鬧事。

Arne Schoenbohm 亦指出，示威也可能在網路上進行，示威者「無需從 100 公里或 1000 公裡外的地方來到這裏，只要在網路空間啟動程序，速度比現實世界里還要快」。目前，德國和與會國包括美國的網路安全部門保持密切聯繫，共同保護峰會使用的電腦網路、監視攝像機和其他安保配備。德國去年曾挫敗俄羅斯駭客組織 APT28 的網路襲擊，這個組織與俄羅斯政府有關聯，當時它們的襲擊對象是德國國會、政黨和智庫。Arne Schoenbohm 表示，這類襲擊仍未停止，對方顯然是要搜集相關信息，以影響德國九月舉行的全國大選。

另德國聯邦資訊安全局上周宣布，發現新一波的魚叉式網路釣魚攻擊(spearphishing attack)，其手法是誘使政府和商業機構的電郵用戶點擊會下載惡意軟體的鏈接。Arne Schoenbohm 表示，當局正與德國政黨及國會議員攜手合作，提升他們的網路安全意識。他表示，儘管加強網路安全，但威脅仍然存在。例如他剛得知政府為選舉開發的一個電腦程序並不安全，接下來幾周內將進行安保檢討。

（資料來源：臺灣新浪新聞）

3.2、駭客攻擊事件及手法

3.2.1、網路電台服務 8tracks 遭駭，1800 萬筆帳戶資料遭竊

網路電台服務 8tracks 於上周遭受攻擊，包含姓名、雜湊密

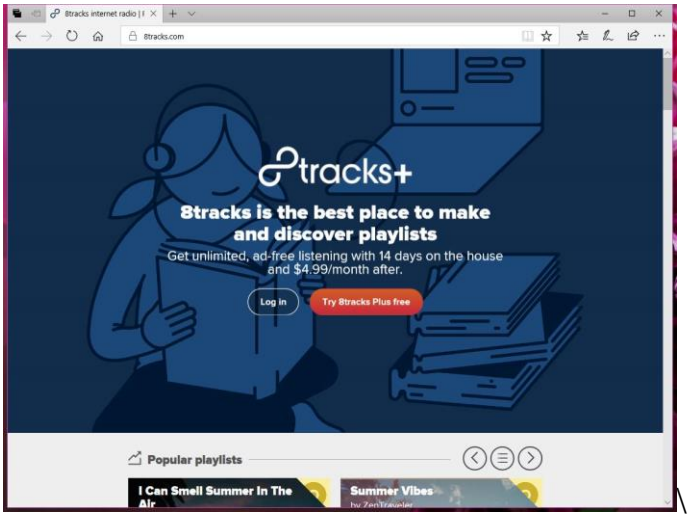
碼與電子郵件等超過 1800 萬筆資料遭竊。

8tracks 已確認此事並表示主因為員工的 Github 帳戶密碼未使用雙因子驗證機制所導致。8tracks 解釋影響範圍僅限於以電子郵件登入的客戶，其他以 Google 或 Facebook 等方式登入者則不受影響。所幸遭竊帳戶密碼以使用雜湊演算法混淆，但為安全起見，8tracks 仍強烈建議使用者變更密碼。

因為有使用 SSH 公/私密鑰對應所保護，8tracks 認為駭客並非入侵到主要伺服器與資料庫，而是備份系統與資料庫，8tracks 表示已進行審核所有的安全措施，並變更儲存系統密碼、在備份系統新增存取紀錄、Github 上使用雙因子認證以及限制存取權限和改善密碼加密強度等。

值得注意的是，8tracks 除使用者名稱、密碼、電子郵件等資料外，並未儲存其他機敏資料如信用卡號碼、電話號碼或家住地址等。

●TWCERT/CC 建議 8tracks 使用者儘速變更帳戶密碼，若該密碼亦使用在其他網路服務，請務必同時變更，並應養成不同網路服務使用不同之登入密碼之習慣。



3.2.2、台灣遭網路間諜集團 BlackTech 鎖定竊取機密技術

資安專家發現一起名為「PLEAD」行動的 APT 攻擊事件，並和 Shrouded Crossbow (暗弩) 以及近期的 Waterbear (水熊)有相當關聯，可能同屬駭客團體 BlackTech。

BlackTech 從 2012 年在東南亞地區活躍至今，除日本和香港地區外，尤其針對台灣，並專門竊取機密文件，曾經攻擊台灣的政府機關和民間機構。

資安專家表示，根據其幕後操縱 (C&C) 伺服器的 mutex 和網域名稱來看，BlackTech 的行動主要是竊取攻擊目標的機密技術。

此活動主要透過電子郵件， 並以 RTLO（從右至左覆蓋）技術欺騙目標收件者，比如將檔案名稱 xxx.fdp.scr 顯示成 xxx.rcs.pdf。

RTLO 技術是利用支援由右到左書寫語言的 Unicode 字元，攻擊者透過 RTLO 的攻擊模式可以在檔名的中間插入轉碼字元，使惡意檔案在系統上看似正常。

資安專家研析發現：相同的 C&C 伺服器、彼此配合的攻擊行動、類似的工具、技巧和目標，因此推測這些行動背後都是由同一個組織所掌控。

資安專家分析，PLEAD 的後門程式可讓歹徒：

（1） 蒐集瀏覽器和電子郵件用戶端 (如 Outlook) 所儲存的登入憑證。

（2） 列出系統上的磁碟、執行程序、開啟的視窗以及檔案。

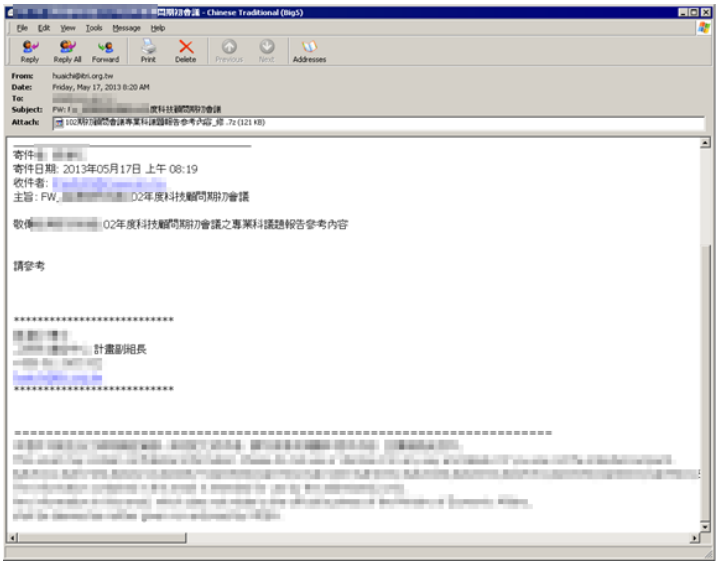
（3） 開啟遠端指令列介面。

（4） 上傳目標檔案。

（5） 透過 ShellExecuteAPI 執行應用程式。

（6） 刪除目標檔案。

●TWCERT/CC 建議，切勿任意開啟電子郵件夾帶檔案，如寄件者來自熟悉帳號，亦應確認信件是否正常，以免遭有心人士利用。



3.2.3、馬來西亞金融公司遭 DDOS 攻擊並勒索比特幣，專家提供 IT 部門相對應行動方案

馬來西亞網路安全部門證實，截至上週五（2017 年 7 月 7 日）為止，已經有 4 間金融公司遭到 DDOS 攻擊，早先的報告指出，這些攻擊是緊接在近期 WannaCry 及 Petya 病毒威脅事件之後，目標鎖定在幾家線上的交易商(攻擊日期約在 7 月 5 日到 7 月 7 日之間)。馬來西亞金融安全專家告訴當地媒體，這些攻擊來自於一個叫做 Armada Collective 的組織，雖然他也不排除是由其他模仿者所採取的攻擊行為。

攻擊者要求在 7 月 13 日前交付 10 比特幣的贖金，不然將會發動下一波的攻擊行動。目前受影響的公司正透過 Clean Pipe 及流量清洗的方式來解決問題。這樣的事件告訴我們，駭客不管組織的大小、型態，都會對其發動攻擊行為。

資安專家提出警告說：「這些攻擊者，可能針對醫療、觀光服務甚至於是水、電、能源、交通運輸等國家關鍵基礎設施採取網路攻擊行為。」

根據 Corero 去年的調查顯示，運用 DDOS 攻擊實施勒索的情形已經相當普遍，常見的攻擊手法大概可以區分三種：

（1） 第一種是以龐大的網路流量塞爆頻寬，影響正常的服務申請。

（2） 第二種是透過系統漏洞攻擊，也是最危險的一種攻擊行為。

（3） 第三種是藉由操縱 TCP、UDP 等通訊協定，造成攻擊。

5.針對上述的攻擊事件，馬來西亞網路安全部門提出警告，並提出以下幾項建議作為：

（1） 各個組織應採取事先防範作為，避免後續造成更大的影響。

（2） 如果遭受 DDOS 攻擊，應立即求助 ISP 業者協助解決。

（3） 除了 ISP 業者以外，受攻擊者也可以向從事 DDOS 問題處理的系統商尋求解決。

（4） 檢查 Geo-IP Blocking 的可能性，如果你的客戶主要來自馬來西亞或鄰近的國家，你可以設定該地區 IP 位址的優先權或阻擋其他地區的 IP，當發生攻擊時，依據這樣的設定可以確保網路使用的安全。

（5） 盡快與負責網路安全的政府機構聯絡，請求協助；另外，我們強烈建議您不要支付相關的贖金。

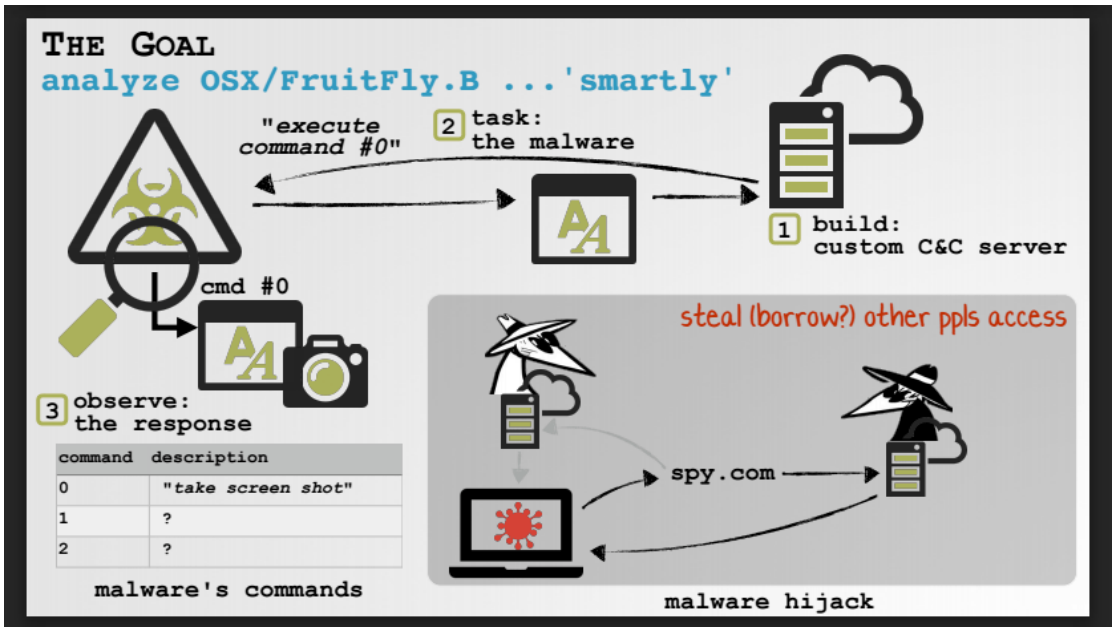
3.2.4、請小心 Fruitfly 惡意程式，被發現已感染數百台 MAC 電腦

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。

根據 Synack 資安公司研究員 Patrick Wardle 表示，通常這些惡意程式都會在政府或國家使用的軟體中被發現，但 Fruitfly 卻針對一般的使用者，駭客將後門程式植入目標電腦後，便與自建的命令控制伺服器(C&C)連線，下達竊取用戶畫面或鍵盤輸入紀錄等命令，以取得敏感資訊(例如信用卡卡號)，詳細技術報告 Patrick Wardle 將在 2017 年的 Black Hat 大會說明。

●TWCERT/CC 提醒蘋果 OSX 用戶參考以下 VirusTotal 連結，若有檔案名稱為 fpsaud，應盡速刪除，並且保持作業系統及防毒軟體有最新的安全更新。

根據 9to5mac 報導，蘋果已於 2017 年 1 月時，發布安全更新，建議用戶更新至 El Capitan 之後的版本



3.2.5、義大利聯合信貸銀行遭駭，40 萬筆客戶資料外洩

聯合信貸銀行（UniCredit）總部設於米蘭，歐洲最大的銀行集團之一，有著超過 2800 萬用戶，業務遍及 19 個國家。

該銀行發佈官方聲明承認其伺服器近期被駭客入侵，有大約 40 萬名客戶的資訊被洩漏。

早在 2016 年 9 月、10 月間即曾經遭受過第一次駭侵，第二次發生在今年 6 月、7 月間，並由公司資安部門發現，才引發深入調查。

UniCredit 表示，此外洩事件可能是透過第三方處理與個人貸款有關的客戶資料。

因此外洩資料可能包含客戶姓名、地址和 IBAN 號碼等資訊。然而客戶密碼並沒有被洩露，目前也未發現未經授權的交易。

該銀行已立即採取補救行動，並設法檢測未經授權的存取，以阻絕駭客並升級該銀行系統，以防止進一步的違規行為。

●如有要了解即時資訊之 UniCredit 客戶，請聯繫 UniCredit

專用免費電話 800 323285 或其分行客戶服務。

另外，UniCredit 將透過特殊管道與受影響的客戶聯繫，不包括電子郵件或電話，因此如客戶接收到相關通知，請確認來源，以免遭駭客利用。

3.2.6、圖片辨識軟體 CopyFish 的 Chrome 套件遭駭，請盡速移除

Copyfish 是一款免費的 Chrome 擴充套件，它能夠從圖像、影片、以及 PDF 檔案等內容中提取文字並作出翻譯。

該開發團隊於昨日(7/30)對外公告，團隊成員於 7/28 遭駭客以社交工程方式成功騙取團隊的 Google 開發帳號。

一位小組成員收到了來自 “Google” 的電子郵件，表示需要更新 Chrome 擴充功能 (Copyfish)，否則將從商店中刪除，再以「請點擊開啟更多資訊」誘騙員工打開 “Google” 密碼對話框，不幸的，團隊成員因此輸入了開發者的帳號及密碼。

在該所屬公司毫不知情下， CopyFish 在第二天「被」升級至「2.8.5」 版，因該駭客已將特製的 CopyFish 透過竊得之帳密傳送

至 Google 商店，由於 Chrome 擴充功能會自動更新而無需知會使用者，因此使用 CopyFish 的大多數用戶將收到「更新」的版本。

2017 年 7 月 30 日的開始出現抱怨回報，表示 Copyfish for Chrome 在網站上顯示廣告和垃圾郵件，開發團隊才驚覺有異。

經檢查 Google 開發人員帳號顯示，攻擊者不僅上傳了擴充功能的惡意版本，還將擴充功能移到了自己的帳戶，這意味著 Copyfish 開發團隊在此時無法存取該擴充功能。更無法更新它，攻擊者可能會推出另一個版本的擴充功能到用戶群。

由於 Chrome 擴展程序會自動更新，只能暫時移除 Chrome 擴充功能 CopyFish ，所幸 Firefox 版擴展檔案 Copyfish 則不受影響。

●TWCERT/CC 建議，已安裝 Copyfish 的 Chrome 用戶盡速從 Chrome 瀏覽器中刪除該擴充功能，直至問題獲得解決。

3.3、軟硬體漏洞資訊

3.3.1、PHP 的多重缺陷將可讓遠端使用者獲得機敏資訊

在 PHP 的報告中指出了多點漏洞，部分漏洞是藉由 PHP INI API 觸發 stack overflow，可讓遠端的使用者可在目標系統中執行任意代碼(Arbitrary Code)，其他漏洞也可能導致拒絕服務(Deny Service)，或在目標系統中獲得機敏的資訊。

駭客可能利用這種漏洞攻擊方式，透過 PHP INI API 觸發 stack overflow 漏洞，進而執行任意代碼(Arbitrary Code)，獲取機敏資訊。

3.3.2、Apache 網頁伺服器 mod_http2 模組發現弱點，可使駭客發動阻斷服務攻擊

本次安全更新修補了 Apache 漏洞，該漏洞是由 mod_http2 模組記憶體存取錯誤之弱點，將導致阻斷服務攻擊。

駭客利用 HTTP/2 多重連線之功能觸發 mod_http2.c 模組造成記憶體存取錯誤以達成阻斷服務的條件。

3.3.3、Samba 釋出重大安全更新

Samba 釋出重大安全更新，其更新包含了 4.0.0 之後的所有版本資訊，該漏洞可

讓駭客利用此漏洞得到系統之控制權。

當駭客利用中間人攻擊(MITM)的手法時可於網域中在回應或授權時偽裝成受信任之主機並藉此提高存取權。

3.3.4、Oracle 釋出安全公告(July 2017)

Oracle 發布 2017 年 7 月的重大安全更新，以解決多個產品中的 308 個漏洞。這些漏洞中將可嚴重的足以讓駭客利用遠端攻擊的方式控制受影響的系統。

此次更新所涵蓋的產品包含：Oracle Database Server、Oracle Enterprise Manager、Oracle E-Business Suite、Oracle Fusion Middleware, Oracle Hyperion、Oracle Industry Applications, Oracle Primavera、Oracle Java SE、Oracle、Solaris、Oracle VM VirtualBox 及 MySQL 等計 97 項產品。

3.3.5、Cisco 釋出安全更新(July 20,2017)

此次更新主要是用以修復 Web 安全設備 WSA(Web Security Appliance)的漏洞。 駭客可利用此漏洞獲取管理者(root)權限得以控制系統。

此漏洞是由於 Web 界面上用戶輸入的驗證不足(insufficient validation)，駭客可利用此漏洞對受影響的設備略過 Web 界面的認證機制以通過身份驗證並執行命令，進而將權限從管理員(administrator)提升至最高權限(root)。

3.3.6、Joomla! 發表安全更新[20170704]

本次安全更新修補了 Joomla! 2 個安全漏洞及超過 50 個錯誤並解決了 Joomla! CMS (Content Management System)安裝程式在安裝過程中因缺乏網路空間使用者的權限將可讓使用者增加權限，進而控制整個網站的嚴重漏洞。

此次更新只針對新安裝 Joomla!的安裝程式，並不影響已安裝完成之 Joomla!網站。

3.3.7、Fortinet FortiOS 輸入驗證之漏洞將讓駭客使用遠端方式進行跨網站指令碼(Cross-Site Scripting)攻擊

Fortinet 發布了 FortiOS 的幾個漏洞，駭客可利用此漏洞進行跨網站指令碼(Cross-Site Scripting)攻擊，駭客可用遠端方式使用被攻擊者之暫存檔（包括身份驗證 cookie），透過 Web 表單提交的資料連線至 Fortinet 設備，進而登入 Fortinet 設備。

此次更新影響了" FortiView Application filter "(CVE-2017-3131), "FortiToken activation"(CVE-2017-3132)和"SSL VPN Replacement Messages" (CVE-2017-3133) 建議 Fortienet 的使用者盡快將 FortiOS 更新至 5.6.1 版。

3.3.8、Microsoft 釋出 Outlook 安全更新(July 2017)

Microsoft 釋出安全更新以解決 Office 產品的漏洞，駭客攻擊時將建立個特別的檔案引誘使用者開啟該檔，駭客則可使用該漏點損害受駭的電腦或電腦內的資料。

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
106/09/06	CLOUDSEC 2017 企業資安高峰論壇	主辦單位：趨勢科技 日期：2017 年 9 月 6 日 (三) 8:00 - 16:50 地點：TICC 台北國際會議中心(台北市信義區信義路五段 1 號) 線上報名連結：https://www.cloudsec.com/event-registration/?event=8052 資料來源：https://www.cloudsec.com/tw/ 活動概要： 現在，企業體系、政府組織和個人都面臨多樣化且不確定的駭客威脅。在這樣的世代，企業因應的解決方案都必須重新評估重新定義，企業、政府甚至個人所建立的防禦等級一定要 Level UP。邁入第七年亞太區資安大會『CLOUDSEC 2017 企業資安高峰論壇』，今年要帶領您從更高的角度了解：未知威脅在哪裡？潛在風險怎麼評估？真正的防禦和程序要如何進行？最重要的是協助您全面提升威脅防禦能力。
106/09/09 -10/07	CISSP®資訊安全系統專家認證	主辦單位：MasterTalks 日期：2017 年 09 月 09 日 (六) 09:00 ~ 2017 年 10 月 07 日 (六) 18:00 地點:台北市中正區市民大道三段 2 號 (三創數位生活園區) 線上報名連結：http://www.accupass.com/event/register/1707080744251449780826 資料來源：http://www.accupass.com/event/register/1707080744251449780826

時間	研討會/課程名稱	研討會相關資料
		活動概要： 依據 Cybersecurity Trends Spotlight Report 資訊安全專家 CISSP 認證為最有價值的 IT 認證，且在資安法即將通過前夕以及資訊安全日益重要的今日，各大企業無不爭相徵求 CISSP 資訊安全專家的加入，以保護公司重要的資訊資產並應對各種新型態的威脅。現在就開始準備 CISSP 證照取得，提升自己的競爭力與專業形象。
106/09/09-10/07	SSCP 資安專業人員認證	主辦單位：MasterTalks 日期：2017 年 09 月 09 日 09:00 ~ 2017 年 10 月 07 日 18:00 地點:台北市中正區市民大道三段 2 號 (三創數位生活園區) 線上報名連結： http://www.accupass.com/event/register/1707080753499245532020 資料來源： http://www.accupass.com/event/register/1707080753499245532020 活動概要： 參加本課程，除能強化您在存取控制、安全作業管理、資安風險識別/監控與分析、安全事故回應與復原、密碼學及網路與通訊安全等領域之專業知識外，亦可在課堂上透過精心設計的演練案例及實務分享獲取實作經驗，讓你在取得證照的同時，回到工作崗位上也能夠實地上手，展現您的工作績效與訓練成果。

第 4 章、本月份事件通報統計

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，本月共收到通報共 1517 筆，以下為本中心所蒐整之各項統計數據，分別為通報來源統計圖、攻擊來源統計圖及攻擊類型統計圖。

通報來源統計圖為各國遭受網路攻擊，且發起攻擊之 IP 為我國所有之 IP，並向本中心進行通報之次數，如圖 1 所示；攻擊來源統計圖為本中心所接獲之通報中，我國各單位遭受來自各國之攻擊次數，如圖 2 所示；攻擊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。

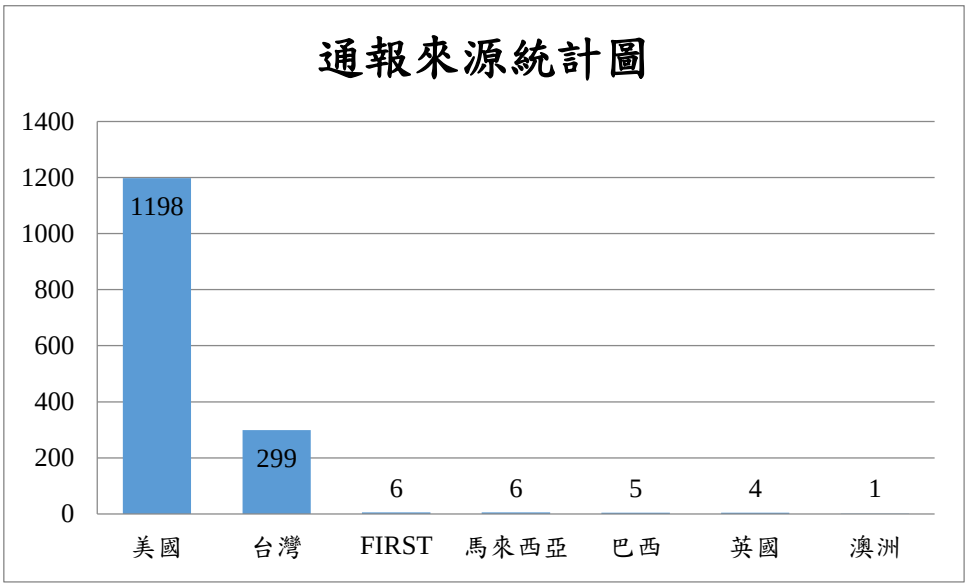


圖 1、通報來源統計圖

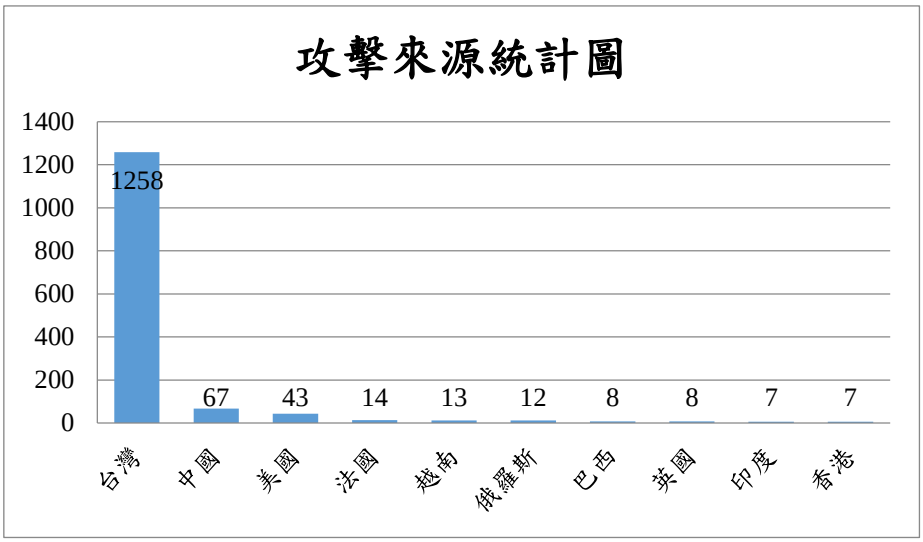


圖 2、攻擊來源統計圖

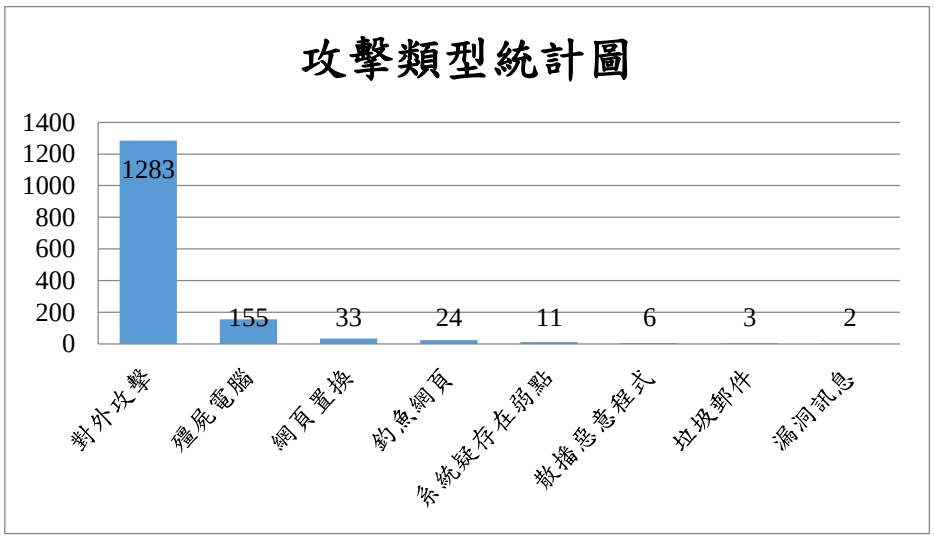


圖 3、攻擊類型統計圖

除通報至 G-ISAC 外，本中心亦已電子郵件或電話方式通知相關單位進行處理，本月約有 50%單位回覆相關處理情形，建議大家應於平常保持良好之防護習慣，於事前勤更新相關弱點及漏洞，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

資料日期：106 年 8 月 8 日

編　　輯：曾佩雅

服務電話：03-4115387

市話免付費電話：0800-885-066

電子郵件：twcert@cert.org.tw

網　　址：https://www.twcert.org.tw/

Facebook：https://www.facebook.com/twcertcc

若有任何問題或建議，請通知我們，也歡迎您的不吝指教。