TWCERT/CC 資安情資月報

106 年 10 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

為提升我國民眾資安意識，TWCERT/CC 於每月發布資安情資月報，月報中統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、資安威脅、資安趨勢、駭客攻擊事件、軟硬體漏洞及資安事件通報統計分析等資訊。

TWCERT/CC 近期動態，本中心於本月參加「The Dungeons of Hackers Conference 2017 - 駭客的地下城」研討會。

在資安政策方面，美國國土安全部發布強制命令要求政府網站使用 HTTPS 及電子郵件驗證，另台灣行政院資安服務團，將於明年起進駐中央部會，而立法院籲制定資通安全管理法以提升資安。資安威脅方面，美公開警告能源和工業產業遭駭客鎖定，另經調查發現，政府網站使用 https 比率僅 11.2%，恐危及整體國家資安環境，而民眾不愛換密碼也成資安一大漏洞，另外有超過 73,000 支 IOT 監視器畫面被公開。資安趨勢方面，熱門網站被植入惡意程式 駭客竊取民眾電腦「挖礦」。

在駭客攻擊事件方面，駭客設計 WordPress 假冒防護外掛，而金管會針對遠端銀行客駭事件做說明，另 IBM 公布新型勒索軟體 "Bad Rabbit" 的 IoCs。

在軟硬體漏洞部分， Microsoft 釋出 10 月之安全更新； Apple 釋出 iOS 11.0.2 安全更新；Apache 釋出 Tomcat 安全更新另修補 NTP 及 wget 之漏洞；WPA2 無線通訊協定存在弱點，駭客能操縱 KRACKs 攔截竄改 Wi-Fi 傳輸資料；Adobe 釋出安全更新緊急修補 type confusion 漏洞；Dnsmasq 最新版修補 7 項漏洞；Fortinet FortiMail 釋出升級版本補強 cross-site scripting 弱點；cURL 釋出最新版解決 overread 漏洞；CentOS 釋出安全更新；Node.js 釋出

更新檔修補參數驗證漏洞。

在資安研討會及活動部分，2017 年 11 月 20 日至 23 日於台大集思會議中心、台南成功大學-C-Hub 創意基地、高雄集思會議中心-中庭交誼廳中舉辦「2017 OWASP Taiwan Week」，另 2017 年 12 月 7 日至 8 日於台北國際會議中心中舉辦「HITCON Pacific 2017」。

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，經攻擊特徵分析後，本月以”嘗試 SASL 認證暴力破解”為大宗。

第 2 章、TWCERT/CC 近期動態

2.1、106 年 10 月 14 日 TWCERT/CC 參加「The Dungeons of Hackers Conference 2017 - 駭客的地下城」研討會

TWCERT/CC 於 106 年 10 月 14 日參加「The Dungeons of Hackers Conference 2017 - 駭客的地下城」研討會，此次會議是由學生駭客社群 TDOH 主辦，參與對象主要為學生，針對資安基礎知識、惡意程式分析、無線網路安全、資安社群推廣等項目為研討內容，TWCERT/CC 也於此次研討會上針對 TWCERT/CC 服務內容進行推廣，希望透過此場的推廣，能讓學生對於 CERT 有更進一步的認識。

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、不愛換密碼 成資安大漏洞

台灣社群用戶在行動時代暴露在資安風險的程度越來越高。台灣社群用戶中有超過 25%帳號曾經被盜，而曾遇過周遭親友帳號詐騙問題的用戶更超過 5 成。

台灣用戶對於社群密碼、安全認證碼等防護認識也不足，超過四分之一的用戶曾協助親友收取安全認證碼，且每 10 人中就會有一位曾傳送安全驗證碼或密碼給其他人。若再深入探究台灣用戶的密碼設定習慣，不僅逾 6 成的用戶僅以 1～3 組密碼於各社群帳號間交互使用，且半數以上的用戶從未定期更換密碼以預防資安問題。

- http://www.chinatimes.com/newspapers/20171023000075-260204

（資料來源：臺灣中時電子報）

3.1.2、美公開警告 能源和工業產業遭駭客鎖定

路透社報導，美國國土安全部和聯邦調查局（FBI）共同警告，除了政府實體之外，核能、能源、航空、水利以及其他重要製造業也

成網路攻擊的目標，這些攻擊至少可追溯至 5 月。

報告說，駭客的目的是藉由惡意電郵和中毒的網站，入侵組織網路，以取得進入目標電腦網路的機密資訊。駭客已成功入侵部分目標的網路，但並未透露確切的受害者，或任何遭入侵破壞的案件。

美國當局已經監控這些活動多月，今年 6 月首度發布機密報告，當中詳述初步細節。這項報告由路透率先揭露。報告私下寄給恐遭攻擊風險的企業，說明一套縮小範圍的攻擊活動，瞄準核能、能源和重要的製造業部門。

國土安全部長發言人麥康奈（Scott McConnell）婉拒進一步說明報告內容，以及這次公開的原因。麥康奈說：「這項技術警告提供防止或減低瞄準多個產業惡意網路活動的建議，同時重申我們致力關注新威脅。」FBI 則拒絕對此發表評論。

- https://udn.com/news/story/6809/2771416

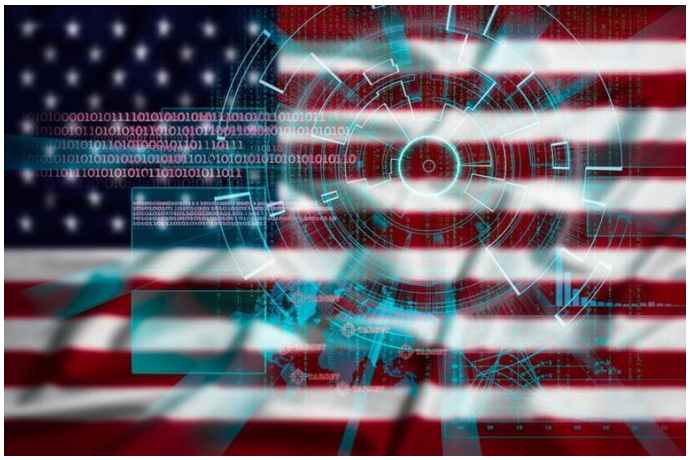
（資料來源：臺灣聯合新聞網）

3.1.3、美國國土安全部發布強制命令要求政府網站使用 HTTPS 及電子郵件驗證

美國國土安全部在 10 月 16 日發布一項緊急命令，要求聯邦政府的各個機關在 90 天內必須建置 DMARC(Domain-based

Message Authentication, Reporting & Conformance)機制以確保有心人士利用聯邦政府郵件伺服器網域寄送廣告及釣魚郵件。全球資安聯盟（Global Cyber Alliance, GCA）的 CEO Phil Reitinger 亦指出，使用 DMARC 並非保護電子郵件本身，而是保護收到信的人，因此只要聯邦政府導入此一機制，就可以防止人民被欺騙，也可為私人企業建立標竿。

另在 120 天內，所有的聯邦政府機關必須在所有的網站上使用 HTTPS（Hypertext Transfer Protocol Secure）協定，以確保使用者能以安全連線瀏覽網站，或以 STARTTLS 等加密協定來確保與聯邦政府網站間的資料來往是安全的。ZDNET 則指出，雖然美國政府已於 2015 年發布僅能使用 HTTPS 之說明文件，但至今仍有 1/4 的政府網站仍不支援 HTTPS 連線。官方亦指出，能讓人民信任所有層級的政府網站是很重要的，他們亦要求所有的聯邦政府機關一個進階資安工具包，以確保可以保障全美大眾的安全。



- https://www.techrepublic.com/article/dhs-orders-federal-agencies-to-bolster-cybersecurity-with-https-email-authentication/

（資料來源：美國 TechRepublic）

3.1.4、超過 73,000 支監視器畫面被公開

研究人員 Mike Olsen 提出警告，Amazon 上販賣的某些產品暗藏了惡意程式。根據 Olsen 的說法，他在調校一批向朋友購買的戶外型監視攝影機時發現攝影機暗藏了惡意程式。而販售的廠商 Urban Security Group (USG)在網路上的評價大致良好，而且還針對了某款 Sony 攝影機提供特惠組合方案。

Olsen 在他的部落格當中詳細說明了攝影機的軟體介面可看到監視畫面，但管理畫面卻看不到其他正常該有的設定功能。Olsen 說：「我只是像其他人一樣，懷疑這應該是 CSS 沒設好，所以就叫出開發人員工具。」但他並未找到他想要的選項，反而發現<body>標籤底下偷偷暗藏了一個<iFrame>標籤。這個 iFrame 會連上一個「看似非常奇怪的」主機名稱。他到 Google 上搜尋後發現，該主機名稱會連上某個專門散布惡意程式的網站。此惡意網站曾在 2009 年遭到關閉，但 2011 年又被人發現它會讓一些網站感染指向惡意網域的 iFrame。發現這件事之後，Olsen 立即向 Amazon 反映，該網站後來向他表示將會聯繫攝影機廠商(USG)。

家用監視攝影機確實是提升居家及工作場所安全的一個不錯工具。但為了即時觀看監視畫面，您必須讓監視攝影機連上網際網路。而且，較新型的攝影機甚至可以從遠端遙控，好讓使用者操控單一攝影機來監視一大片區域。科技智慧化的結果，人們可以很方便地透過網路來查看監視攝影畫面，但這也讓其他連上網路的人都有機會看到。任何未經授權的人，只需具備特殊的工具和專業知識就能辦到。

- https://www.csoonline.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html

（資料來源：美國 CSO）

3.1.5、行政院資安服務團　明年起進駐中央部會

行政院資通安全處長簡宏偉 15 日受訪說，各級政府機關資安人才缺額有 500 多人，行政院正在進行招募外，也正著手成立「資安服務團」，先進駐資安層級度較高的政府機關，包括五院和中央二級機關，協助各部會建立資安防護、資安管理、聯防機制等。

現在政府一方面從各領域培育一些資安人才，不過培育人才需要一些時間，因此另方面政府也同步著手進行成立「資安服務團」，現正在物色服務團成員，希望網羅技術、管理階層等專業人才，並預計明年起一團約 10 人，先成立 2 團，先找一、兩個中央部會機關試辦。

服務團明年進駐單位以 8 大關鍵基礎設施，包括：能源、水資源、交通、通訊傳播、金融、緊急救援與醫院、中央與地方政府機關、高科技園區的主管機關為優先順位。

另外，遠東國際商業銀行日前電腦遭駭，行政院長賴清德已要求

金管會年底前建置金融業資安聯防平台，簡處長表示，資通處去年起就已開始與 8 大關鍵基礎設施的主管機關洽談，除金融業資安聯防平台要在年底前建立，希望其他 7 大等關鍵基礎設施也都加速進行，在年底前成立資安聯防平台。

- http://www.appledaily.com.tw/realtimenews/article/new/20171015/1222911/

（資料來源：臺灣蘋果即時）

3.1.6、政府網站使用 https 比率僅 11.2%，恐危及整體國家資安環境

「立法院數位國家促進會」會長余宛如表示，由於 https 能保護網頁在傳輸過程中不被變造，使得政府資訊不容易在傳輸過程中被竄改，但是，台灣的 1,089 個政府網站中，使用 https 的比率過低，僅有 11.2%，其中更更包括總統府、國安局、外交部的網站皆未使用 https。由於 http 為傳輸網頁的規格，而 https 則是在 http 架構上額外採用加密演算法，使網頁在傳輸過程中有受到保護，讓有心人無法在傳輸過程中擷取網頁並進行竄改。換言之，https 是在傳輸過程中，為資訊加上一層信封；而沒有使用 https，就彷彿寄發明信片般，每個接觸到的人都有機會閱讀，甚至進行惡意竄改，因此，https 可以說是最基本的網站資安防護措施。

目前，同樣主掌國家安全、國際事務的國安局、外交部的相關網站均未使用 https。而且，根據紀錄，2016 年國安局被駭客攻擊超過 63 萬次，比 2015 年大幅成長的情況下，國安局還尚未使用 https，這對於將來面對駭客的攻擊，恐怕造成更令人擔憂的後果。行政院雖然有訂定計畫，要在 2018 年的 12 月底將所有政府網站皆更新為 https，但這樣的期限，在腳步快速的數位時代，實在應該提早至 2017 年 12 月底完成。

余宛如進一步表示，根據調查，政府使用 https 的比率不僅過低，僅有 11.2%，而且調查中的安全指標等級，由安全到不可信任，分為 A 到 T 級的結果。其中，台灣雖然有 67%的機關在防護最高的 A 級，但是做為國家安全掌門人的國防部，安全等級僅有 B 級，而科技龍頭的科技部網站在 10 月份改版前，更是僅達到防護最低的 T 級；至於總統府，則更是除了總統信箱外，皆未使用 https。國發會資訊管理理處處長潘國才、行政院資安處副處長徐嘉臨皆表示，目前行政院確實訂定相關的規畫，並將盡可能將時程縮短。國發會更將在 2018 年開始把 https 納入網站盤點的檢核項目中，也有提供諮詢專線供各單位詢問。科技部資訊處處長薛大勇則表示，科技部新版網站近期上線，已經針對資安部分做出多項改善，將來來也會依照建議「立法院數位國家促進會」，再朝網站資訊設計、使用者體驗優化等方向再強化。國防部通次室資安處代處長廖述煌則表示，國防部的資訊安全絕對會努力往 A 級前進。

https 並非高深的技術，卻足以造成政府資訊被竄改成假新聞等嚴重威脅公共安全的議題，但這方面並沒有專業單位來協助所有部會，進行判斷與統合；而且，國防部本次還是第一次參加資訊安全相關的記者會，更顯示出國家資訊長立法，建立政府具備整合性的資訊掌門人的重要性。

- http://technews.tw/2017/10/05/https-taiwan-government/

（資料來源：臺灣 TechNews）

3.1.7、熱門網站被植入惡意程式 駭客竊取民眾電腦「挖礦」

根據英國廣播公司（BBC）揭露，許多駭客將特殊的程式碼植入各大熱門網站，像是學校、社福機構，甚至是雲端服務網站；只要民眾造訪這些網站，駭客就能悄悄地用民眾的電腦來賺取虛擬貨幣，不過他們並非竊走民眾的虛擬貨幣，而是利用他們的電腦來協助挖礦。

資安研究公司「趨勢科技」（Trend Micro）副總裁佛格森（Rik Ferguson）表示，挖礦的過程須要大量的電腦合作進行運算，駭客只要可以控制越多的電腦，他就可以賺越多的錢。以比特幣（Bitcoin）為例，比特幣的交易須仰賴「礦工」以電腦進行運算，一方面確保了比特幣交易的正確性、避免雙重支付的可能，一方面則讓貨幣來源保持活動狀態，運算成功後，系統便會提供新的比特幣給礦工作為獎勵。

「協助挖礦的惡意軟件並不是新鮮事了」，佛格森補充，隨著既有虛擬貨幣及新推出虛擬貨幣價值的提升，惡意程式碼已經愈來越普遍，如果網站中的這些程式碼是被刻意隱藏起來，可能代表這些程式

碼是遭惡意植入。

BBC 報導指出，資安研究員已經檢視數百萬個熱門網站的程式碼，並連繫了英國數間被查獲網站裝有挖礦程式碼的公司，他們大多都表示不知道程式碼是由誰植入，部分公司現在已經刪掉該程式碼並且升級內部的資安政策。

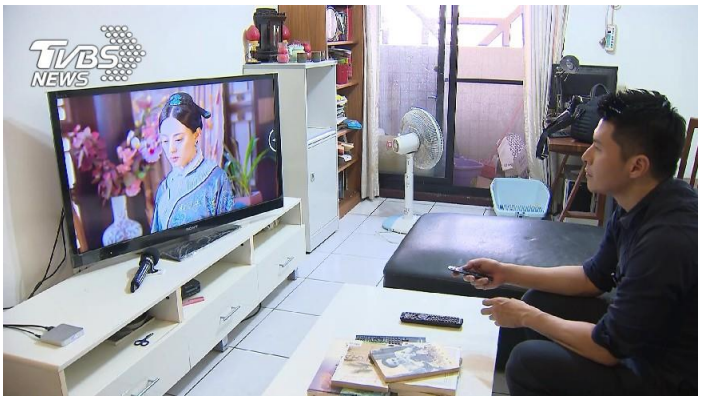
- http://news.ltn.com.tw/news/world/breakingnews/2218283

（資料來源：臺灣自由時報）

3.1.8、立法院籲制定資通安全管理法 提升資安

預算中心指出，國內資安法規未臻健全，在公部門雖有資通安全推動單位與相關遵行法令，其中屬法律者，規範目的各異，而適用時或僅就實害結果進行處罰，或其保護客體僅以特定類型的資料為限，並非整體考量資通安全管理。其餘規定對資通安全管理雖定有較細節的規範，但位階較低，且規定分散，適用上難免不足，相關單位不易落實；另適用於非公務機關的規定，因立法目的不同，其適用範圍、保護客體與規範對象亦有差異，無法作為各非公務機關共通遵循標準，難以帶動整體資通安全能量。民生與工業基礎設施聯網後，成為駭客攻擊新目標，近年來國內外接連發生重大資安事件，已造成政府聲譽

及企業財產損失，駭客零時差攻擊風險遽增，資安儼然成為國家安全之重要一環，關鍵基礎設施資安防護亟待強化。因此，政府宜儘速完成「資通安全管理法」立法程序 ，賦予各機關資通安全維護義務的法源，提升資通安全能量。



- http://news.tvbs.com.tw/politics/782250

（資料來源：臺灣 TVBS）

3.2、駭客攻擊事件及手法

3.2.1、駭客設計 WordPress 假冒防護外掛，並植入後門

資安專家發現一種偽冒知名 WordPress 反垃圾郵件工具外掛「WP-SpamShield Anti-Spam」，名為「X-WP-SPAM-SHIELD-PRO」。

下載「X-WP-SPAM-SHIELD-PRO」的用戶會感染後門程式，並關閉其他外掛，甚至用來竊取資料和添加隱藏的管理員帳戶。

資安專家分析發現該假外掛具有合法的資料結構和檔案名，但其所有內容都是假的，皆是用於達成攻擊者目的駭侵工具。

假外掛的作者還實作了一個更新功能，允許攻擊者可以上傳任何檔案到該站點。例如可以上傳 ZIP 存檔，將其解壓縮到系統，然後刪除存檔。

這款外掛未出現在官方 WordPress 外掛庫中，而是在其它地方提供下載來源。駭客利用手段誘使用戶擔心自己的網站安全，進而騙取受害者下載該偽冒外掛。

● *TWCERT/CC 建議 WordPress 使用者務必僅安裝官方 WordPress 庫的外掛程式，切勿於第三方下載安裝，以免遭駭客利用。*

- https://blog.trendmicro.com.tw/?p=52746

3.2.2、金管會對遠東銀行發生電腦駭客事件說明

遠東國際商業銀行(下稱遠東銀行)發生電腦病毒入侵，經該行檢視發現疑似駭客入侵 SWIFT 系統產生虛偽交易之情形，金管會說明如下：

依遠東銀行清查因屬虛偽交易，不是從個別客戶帳戶匯出資金，故客戶沒有損失。未來若有損失，全額由該行承擔，故客戶權益不受影響。金管會已要求該行立即強化網路安全防禦。

金管會於 10 月 5 日接獲遠東銀行通報 SWIFT 系統異常後，已請其他銀行進行清查；依其他銀行回報結果，SWIFT 系統均屬正常。

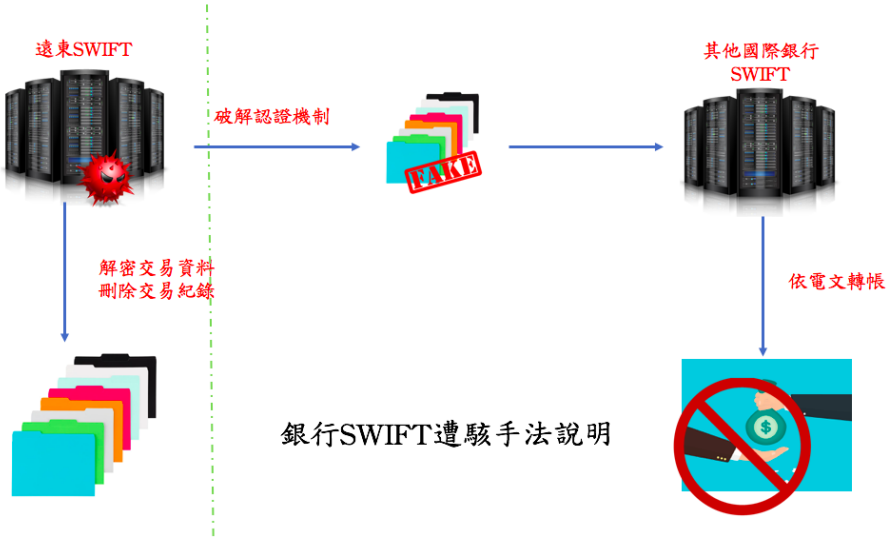
為加強金融機構資訊安全維護，金融機構除應依「金融機構辦理電子銀行業務安全控管作業基準」等規定辦理外，金管會並要求各銀行在連續假期應注意以下事項：

1. 加強各類異常情形之監控，包括資訊系統異動、防毒防駭事件警訊、internet 存取紀錄、派版軟體及病毒碼更新設備等之監控處置。

2. 原則禁止遠端連線。即禁止由外部連線至銀行內部營運區進行系統維護作業，若真有緊急需要，應加強監控管理，例如身分驗證、授權人工確認等。

3. 防止駭客透過內部系統入侵，將交易系統設定與 SWIFT 系統脫鉤(即自動化介接機制改為人工處理)。

4. 為加強管控通匯交易，交易金額大於一定金額以上者，要求 call back 確認。 金管會表示，資訊安全是金融機構須面對並重視之課題，金管會將持續督促金融機強化資訊安全防護。



- https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201710060005&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News

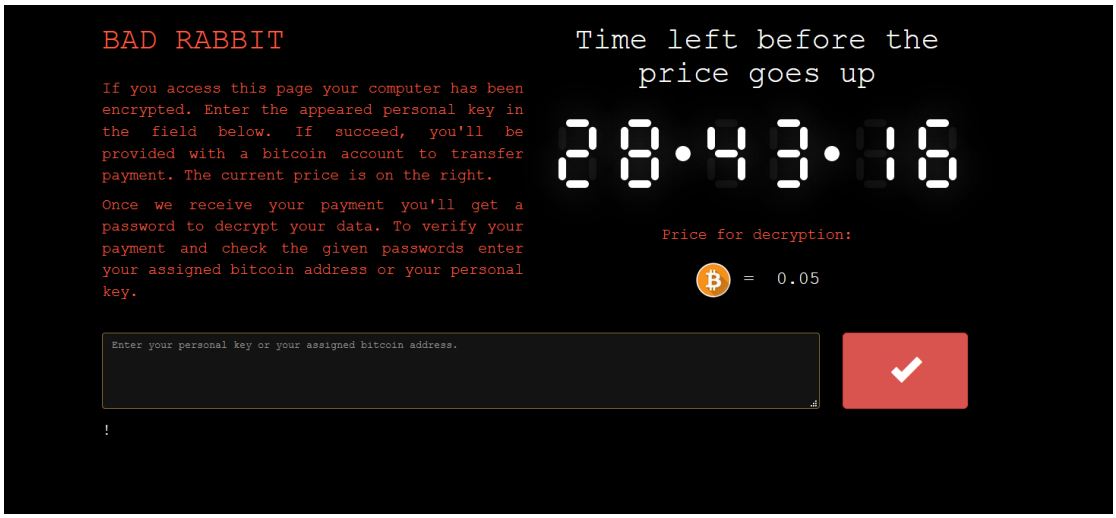
3.2.3、IBM 公布新型勒索軟體 "Bad Rabbit" 的 IoCs

根據有關報告，近期發現一種標記為 "Bad Rabbit" 的新型勒索軟體變種，初始分析顯示是透過偽冒的 Flash Player 更新模組進行感染。

一旦被感染，檔案即遭加密，並要求使用解密密鑰的費用為 0.05 比特幣(約 280 美元)，而目前沒有跡象顯示支付贖金是否會產生有效密鑰，以正確解密受害者的檔案。

資安公司表示，烏克蘭運輸業成員以及政府機構和俄羅斯媒體 Interfax 和 Fontanka 等，都是這次襲擊事件的受害者，部分報導表示，土耳其，保加利亞和德國也發生過攻擊。

●TWCERT/CC 建議，確保防毒軟體和相關的特徵檔是最新的，並於瀏覽網頁時，如該網頁信任度不高，盡可能不要安裝 Flash Player 更新。



- http://www-01.ibm.com/support/docview.wss?uid=swg22010367

3.3、軟硬體漏洞資訊

3.3.1、微軟釋出 10 月份安全更新

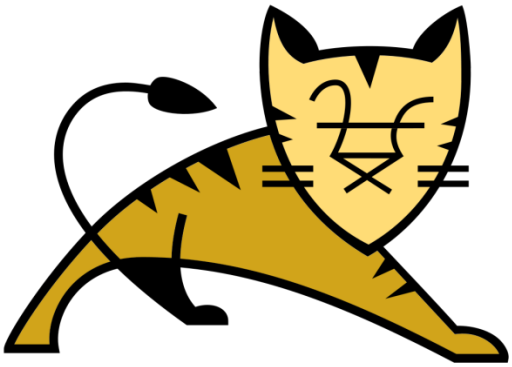
Microsoft 多款軟體存在弱點，駭客可藉此取得遠端系統控制權，該公司就相關版本軟體提供對應之安全更新，及提供更新檔清單對照參考。

3.3.2、Apple 釋出 iOS 11.0.2 安全更新

Apple iOS 11.0.2 經察存在弱點，駭客可藉此取得遠端系統控制權，及造成資料清除、服務阻斷、詐騙攻擊、加密失敗等事件，該公司就相關版本軟體提供對應之安全更新。

3.3.3、Apache 釋出較高安全性之 Tomcat 9.0.1 及 8.5.23

Apache 多版 Tomcat 存在共同弱點，HTTP PUTs 運作時，servlet 預設組態中"read-only"初始化參數設定為 false，駭客可藉此取得遠端伺服器控制權，並執行任何程式碼，Apache 就相關版本軟體提供對應之安全更新。



3.3.4、WPA2 無線通訊協定存在弱點，駭客能操縱 KRACKs 攔截竄改 Wi-Fi 傳輸資料

目前 Wi-Fi 商品無所不在，而弱點在於 WPA2 無線通訊協定本身，非僅涉及特定作業系統或裝備，駭客可佔據 client 與 AP 之中間人位置，執行 KRACKs(Key Reinstallation Attack，即金鑰重安裝攻擊)，取得控制權及機敏資料，甚而假手受害者實行網路犯罪，其影響不容小覷，各原廠業者已陸續提供安全更新。

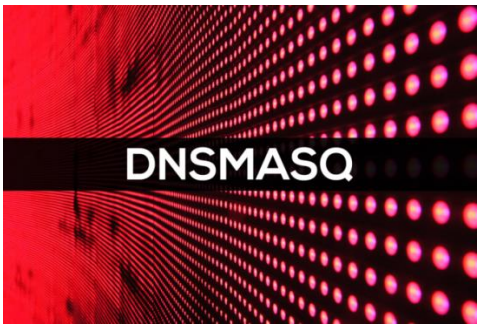
3.3.5、Adobe 釋出安全更新緊急修補 type confusion 漏洞

Adobe Flash Player 系列產品存在弱點，駭客藉此執行遠端程式碼，散佈 FinFisher 間諜程式，取得遠端系統控制權，FinSpy 是惡名昭彰的隱密監視型惡意軟體，透過各種媒介，採魚叉式釣魚以垃圾信夾帶微軟 Office 文件(尤其是 Word)來散佈，遭感染設備會監視私人

通訊及側錄影音，Adobe 提供最新版軟體免除漏洞。

3.3.6、Dnsmasq 最新版修補 7 項漏洞

廣泛運用的 open-source 網路功能軟體 Dnsmasq，全球約 110 萬線上使用個案，經查存在 7 項弱點，駭客可變造過的 DNS 封包、RA 訊號、DHCPv6 請求等，造成 Buffer Overflow、DoS，亦可竊取機敏資料，新版軟體發布以解決相關安全問題。



3.3.7、Fortinet FortiMail 釋出升級版本補強 cross-site scripting 弱點

Fortinet FortiMail 客製化 Webmail 登入頁面，存在輸入驗證瑕疵，駭客能透過受害者瀏覽器進行 XSS 攻擊，執行惡意程式碼，取得受害者資料並竄改，Fortinet 提供修補後版本。

3.3.8、cURL 釋出最新版解決 overread 漏洞

cURL 函式庫 libcurl，特定 proces 接收 IMAP(Internet Message Access Protocol)回應資料為"0"時有風險，駭客可送回特製 IMAP FETCH 回應，藉此取得機敏資料，及造成系統當機，cURL 提供最新版修補漏洞。

3.3.9、Apache 釋出安全更新修補 HTTPD 組態解析錯誤

HTTPd (HTTP daemon)為伺服器領域自由軟體，系對"Allow"及"Deny"2 項參數列的註解內容可能無法正常解析，駭客可藉此繞過安全限制，任意取得遠端系統資源，業者就相關版本軟體提供對應之安全更新。

3.3.10、CentOS 釋出安全更新修補 NTP 及 wget 之漏洞

CentOS 系列軟體存在 NTP(Network Time Protocol)相關漏洞，異常組態設定指令能當掉主機 ntpd 服務或造成 NTP server 片段錯誤；另外部檔案拿取工具 wget 存在緩衝區溢位漏洞，影響 fd_read_body()與 kip_short_body()運算過程，駭客可藉此中斷系統服務，及執行任意程式碼，CentOS 就相關版本軟體提供對應之安全更新。

3.3.11、Node.js 釋出更新檔修補參數驗證漏洞

伺服器端網頁開發工具 Node.js 存在 windowBits 參數驗證弱點，整數”8”若用在 windowBits 參數，Node zlib 將之視作不合規則而當掉或者拋出 exception，駭客可藉此造成 DoS，Node.js 提供對應之安全更新。

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
106/11/20-11/23	2017 OWASP Taiwan Week	【資安研討會】2017 OWASP Taiwan Week 主辦單位：台灣雲端安全聯盟 日期:2017 年 11 月 20 日 (一) ~ 2017 年 11 月 23 日 (四) 地點:台大集思會議中心、台南成功大學-C-Hub 創意基地、高雄集思會議中心-中庭交誼廳 線上報名連結：https://csa.kktix.cc/events/owasp2017 資料來源：https://csa.kktix.cc/events/owasp2017 活動概要： OWASP(Open Web Application Security Project)為全球主要針對開放網頁應用程式安全進行研究的非營利組織，目前已有超過 45,000 名的志願參與者，針對頁應用程式相關的資安問題，進行關鍵的研究並發佈相關的研究成果，對於現今以網頁程式運作為主的資訊環境，更顯得 OWASP 正扮演著舉足輕重的角色;今年 OWASP 重新啟動台灣分會的運作，希望以更積極主動的方式，將國際間的熱鬧資安議題，以及研究的成果，透過社群活動、大型會議等方式，分享給國內的參與者，OWASP 台灣分會依循全球一致的原則，以中立的角色連結產管學研界，希望凝聚國內資安社群的能量，以接軌國際資安社群，能夠同步發佈全球已公開的研究資料，將有助於改善與提昇國內的資安防禦技能與產業環境。
106/12/4-12/6	HITCON Training	【資安訓練課程】HITCON Training 課程時間：2017 年 12 月 4 日-12 月 6 日 受訓地點：台北 課程網站 : https://hitcon.org/2017/pacific/training.html 課程費用：付費 線上報名： https://hitcon.kktix.cc/events/hitcon-winter-training-2017 資料來源 : https://hitcon.org/2017/pacific/training.html 課程簡介：

時間	研討會/課程名稱	研討會相關資料
		共分為六類課程，包含 Malware、Exploitation Technique、Incident Response、Web Security、Windows Security 及 SCADA Security。
106/12/7-12/8	HITCON Pacific 2017	會議時間：2017 年 12 月 7 日-12 月 8 日 會議地點：台北國際會議中心 （台北市信義區信義路五段） 會議網站：http://hitcon.org/2017/pacific/ 會議票價： ●超級早鳥報名 2017.10.09 - 10.20 : NT$ 9,000 ●早鳥報名 2017.10.21 - 11.24 : NT$ 11,000 ●一般票報名 2017.11.25 - 現場 : NT$ 16,000 ●圓桌套票 Round-Table Combo Pass NT$3,000 首屆 HITCON Round Table，由 HITCON 精選議題深入交流，限額 50 名，購買任一票種，即可以 NT$3,000 升級為圓桌套票，參加 12/7 12:00 - 15:00 HITCON Pacific Round Table。 線上報名連結： https://hitcon.kktix.cc/events/hitcon-pacific-2017 資料來源：https://hitcon.org/2017/pacific/index.html 活動概要： 繼 HITCON CMT Mission: Regain The Initiative 的前哨站，悄悄揭開了台灣年度資安盛會 HITCON Pacific 的序幕，我們可以看到今年整個攻擊的手法與規模都趨於泛化，表示威脅將越來越貼近大眾的日常生活，從水電、交通運輸到工廠生產系統、關鍵基礎設施及銀行等，或具有聯網能力之 IoT 設備，其遭受網路攻擊的機會大幅增加。 資安不再是發生在新聞中的實境秀，所有人都身在其中。去年我們邀請許多國際資安專家談論資安戰略與發展進程，今年 HITCON Pacific 的主題將是 Cyber Force Awakens。我們將呼籲政府、企業乃至於公民等各界取得數位資產的主動權，建立網路力量與資安產業生態系。並邀請國內外專家從資安技術、政策與法規面，探討「數位國土」所面臨的威脅與防禦，為聽眾帶來國際最新的資安觀點及因

時間	研討會/課程名稱	研討會相關資料
		應對策。 會議中除了有重量級講師，將與國際 CTF 全球 10 強攻防總決戰共同舉辦，我們企盼您加入這項行列，與世界級 CTF 選手共同點亮台灣資安軟硬實力。

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 544 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、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，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；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。

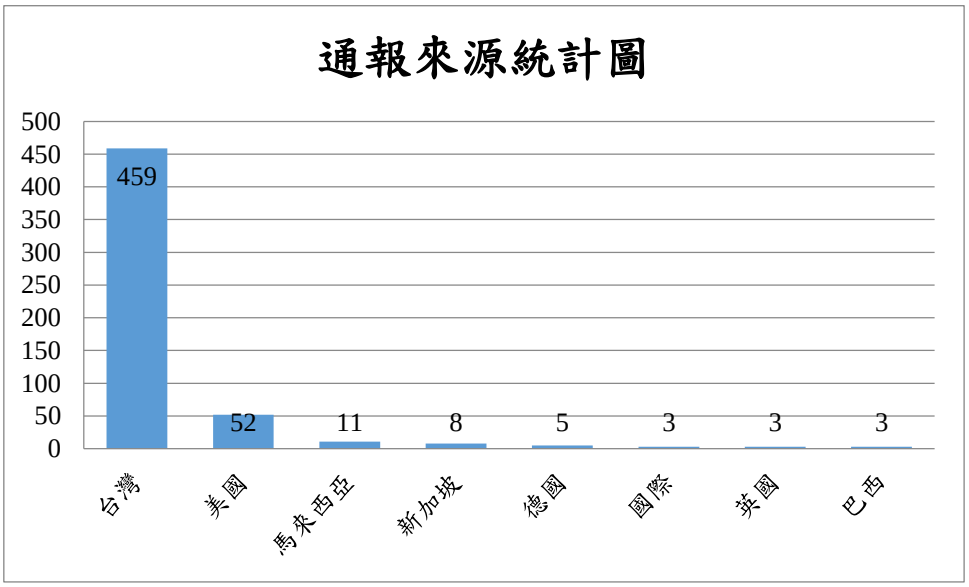


圖 1、通報來源統計圖

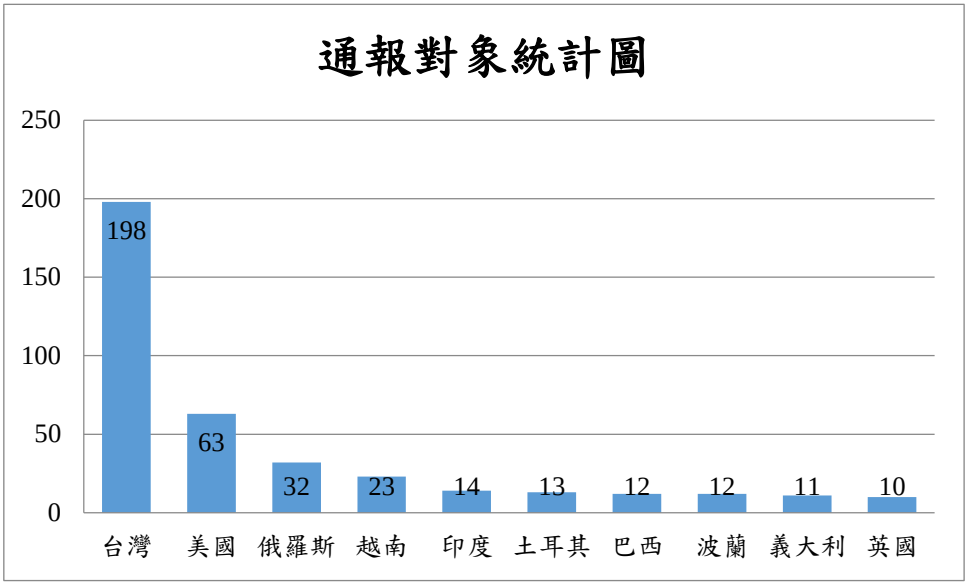


圖 2、通報對象統計圖

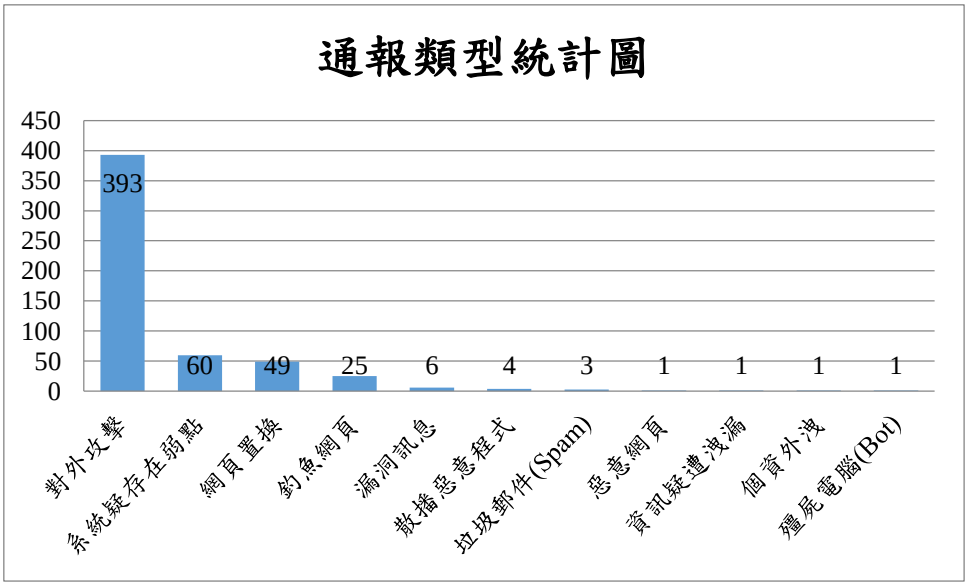


圖 3、通報類型統計圖

本月通報主要來源來自國內特定大專院校提供之情資，攻擊特徵經分析後，本月以”嘗試 SASL 認證暴力破解”為大宗，

SASL 為簡單認證與安全層(Simple Authentication and Security Layer)，一種在既有網路協定中認證機制的框架與標準，為

管理 POP、IMAP 或 SMTP 用戶端向伺服器證實自己身份時所用之機制(參考自 Wikipedia)。郵件伺服器常被利用為主要侵入突破點，進行偽冒郵件或內部網路擴散等攻擊，應列為各單位重要之資訊資產，並嚴加防護。企業平時除應定期弱點掃瞄、安裝修補程式，並在主機端安裝防毒軟體、加強主機端防護外，針對”SASL Force Login”防護應定期檢視郵件伺服器相關活動日誌並強化郵件伺服器安全防護設定，如限制信件代轉設定、郵件過濾機制、郵件管制臨界值等設置。

除通報至 G-ISAC 外，本中心亦針對 zone-h 情資以電子郵件或電話方式通知相關單位進行處理，本月約有 28%單位完成修正，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 11 月 10 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。