



TWCERT/CC 資安情資月報

106 年 09 月份

目錄

第 1 章、 摘要	1
第 2 章、 TWCERT/CC 近期動態	3
第 3 章、 國內外重要資安新聞	3
3.1、 國內外資安政策、威脅與趨勢.....	5
3.2、 駭客攻擊事件及手法.....	5
3.3、 軟硬體漏洞資訊.....	18
3.4、 資安研討會及活動.....	22
第 4 章、 本月份事件通報統計	26

第 1 章、摘要

在 TWCERT/CC 近期動態部分，本中心於本月舉辦「台灣資安通報應變年會-您不可不知的資安聯防新思維」。

在資安政策方面，塔林手冊 2.0 出版，彙整出網路戰爭規範，另資安處建立國家級資安聯防架構，預計年底完成各關鍵基礎設施 ISAC。資安威脅方面，有研究指出，Siri、Alexa 與 Cortana 設計上有漏洞，可以人耳聽不見的超高頻率遙控，而藍牙漏洞恐讓上億手機門戶大開，不用配對或設定就能駭入裝置，另首個鎖定 Dirty Cow 漏洞的 Android 惡意程式現身，且系統清理軟體 CCleaner 遭駭客修改免費版程式，如瀏覽器中跳出「找不到 Hoefler Text 字型」視窗，為惡意程式請勿點選更新，而最新木馬「xRAT」，讓你在駭客眼下等於裸奔，它可隨時監控 Wechat、QQ。資安趨勢方面，請當心 IE 臭蟲可能曝露你的上網隱私，另新型 Android 銀行木馬程式 Red Alert 2.0，感染超過 60 種銀行及社交應用軟體。

在駭客攻擊事件方面，德勤會計師事務所遭駭，電子郵件個資外洩，另近期 Equifax 被駭案可能與 Struts 漏洞有關，建議用戶盡快更新。

在軟硬體漏洞部分，Google 及 Microsoft 都發布 8 月之安全更新；Struts2 REST 插件程序的 XStream Handler 反序列化操作，可能遭利用惡意的 XML 內容提升權限；BlueBorne 安全性漏洞隱憂；Apple 釋出 3 項商品之安全更新；VMware 釋出安全更新。

在資安研討會及活動部分，2017 年 10 月 20 日於台北寒舍艾美酒店舉辦「新世代智慧資安研討會」，另 2017 年 10 月 24 日於國泰金融會議中舉辦「指出資安的新衣-2017 發揮設備最大功效研討會」，2017 年 11 月 1 日於台北舉辦「BSI Standards 國際標準管理年會」，

另 2017 年 12 月 7 日至 8 日於台北國際會議中心舉辦「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“ Scanning port” (通訊埠掃描)為大宗。

第 2 章、TWCERT/CC 近期動態

2.1、TWCERT/CC 於 9 月 13 日舉辦「台灣資安通報應變年會-您不可不知的資安聯防新思維」

TWCERT/CC 於 9 月 13 日集思北科大會議中心舉辦「台灣資安通報應變年會-您不可不知的資安聯防新思維」，此次研討會是台灣電腦網路危機處理暨協調中心(TWCERT/CC)自 2015 年國家中山科學研究院承接以來，首次舉辦的大規模的資安研討會議，當天約有 330 人共襄盛舉，是個盛大的資安年會。此次的研討會主題是放在「資安通報應變」，為了因應近年來台灣發生數起重大的資安事件，希望透過此次的會議，讓與會嘉賓能了解資安通報應變的做法、資安支援管道、資安事件處理流程及解決方案等相關資訊。此次研討會議中除了針對資安通報應變為主軸外，也於會議上辦理 TWCERT/CC 協辦的「國家中山科學研究院 神盾盃」頒獎典禮。

行政院資通安全處簡處長也於會中針對「我國資安聯防機制」進行相關分享，國家資安發展關鍵指標主要由完備資安基礎環境、建構國家資安聯防體系、孕育優質資安人才，及推升資安產業自主能量等四個面向來衡量，目前資安處初期已成立針對金融單位的資安服務團，該團成員共有 10 人，並希望能在今年成立 4 個資安服務團。至於資安風險評估面向，則是以早期預警、持續監控、通報應變，及協助改善等四面向，來落實以風險管理為核心的資安防護，其中通報應變是最重要的部分，唯有進行資安事件通報，才能掌握目前狀況，即時應處。

會中特別邀請到台灣 CERT/CSIRT 聯盟成員前來分享「各 CERT/CSIRT 內部運作及提供的服務內容」，目前台灣 CERT/CSIRT 聯盟成員包含政府部門的 TWNCERT、學術網路的 TACERT 及 TWCSIRT、電子商務的 EC-CERT、通傳會的 NCC-CERT、趨勢科技

的 TM-CSIRT 及民間產業的 TWCERT/CC。台灣 CERT/CSIRT 聯盟的目的，是希望能透過台灣的這些 CERT/CSIRT 組織密切合作，即時掌握台灣的資安狀況，並即時處理緊急資安事件。此外，台灣仍有其他 CERT/CSIRT 尚未加入聯盟組織，未來將持續邀請台灣各個 CERT/CSIRT 組織加入聯盟，以擴展台灣 CERT/CSIRT 聯盟規模，並達到全台資安聯防之目的。另外，也於會議上特別邀請 Nippon CSIRT Association Steering Committee Chair Masato Terada 來為大家進行日本在運行 CSIRT 的相關經驗分享。

除了邀請 CERT/CSIRT 外，也非常榮幸邀請到各大資安廠商高階主管、資安社群 TDOH 創辦人沈家生、HITCON 常務理事長 Allen、駭客書院謝副院長、調查局周科長、台灣數位鑑識發展協會林理事長、中科院資安防護組陳組長，以及臺灣科技大學資訊工程系鄭教授前來為我們進行相關資安協處、人才培育，及通報應變等相關分享。

會議可公開簡報下載：

https://twcert-official-file.s3.hicloud.net.tw/1060913_TWCCERT_Conf.rar



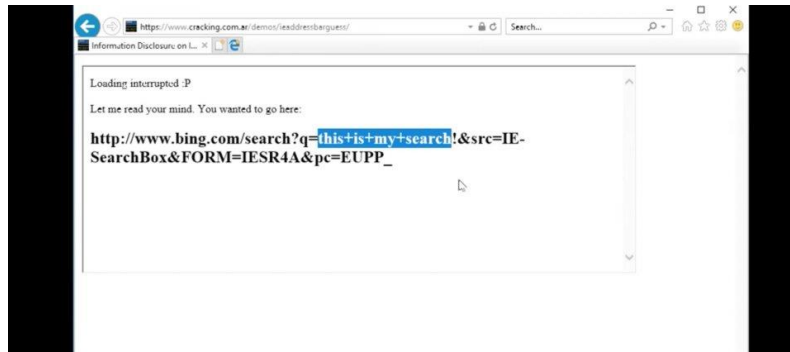


第 3 章、國內外重要資安新聞

3.1、國內外資安政策、威脅與趨勢

3.1.1、當心 IE 臭蟲可能曝露你的上網隱私

安全研究人員 Manuel Caballero 揭露微軟的 Internet Explorer (IE) 瀏覽器出現漏洞，它出現在 IE 的 location 物件中，這個物件讓人存取瀏覽器頁面的 URL 資訊。攻擊需要駭入某個網站在其中埋入一段 HTML 物件標籤，或是透過廣告軟體載入特定 HTML 或 JavaScript 程式碼。其次網頁還要加入 compatibility metatag，這可以讓網站管理員（或攻擊者）選擇相容的 IE 版本。攻擊者嵌入的上述二類標籤再由 IE 載入後，location 物件遭到欺騙，使惡意物件得以存取原本只有主瀏覽器視窗才看得到的資訊，即使用者輸入的所有內容，包括 URL 及查詢關鍵字。

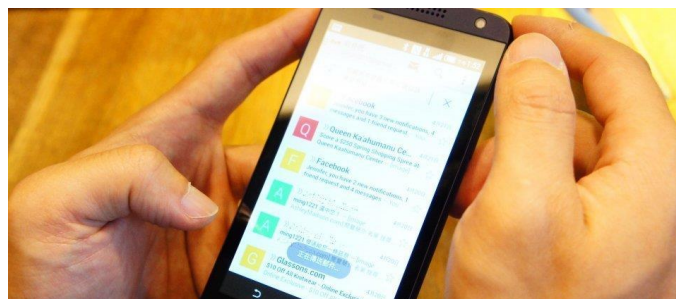


(資料來源：臺灣 iThome)

3.1.2、首個鎖定 Dirty Cow 漏洞的 Android 惡意程式現身

趨勢科技 (Trend Micro) 在本周揭露了首個利用 Dirty Cow 漏洞的 Android 惡意程式家族—ZNIU。該漏洞可允許駭客取得被駭系統的最高權限，雖然自 2007 年釋出的 2.6.22 版便已存在，但一直到去年 10 月才曝光，包括 Linux、 Red Hat、Ubuntu、Debian 與基於 Linux 的 Android 在去年皆已陸續修補。

ZNIU 通常以散布在各個惡意網站的色情程式作為媒介，安裝後它就會與遠端的 C&C 伺服器展開通訊，開採 Dirty Cow 漏洞的 ZNIU 在擴張權限後就能突破系統限制以植入後門，以替未來的遠端攻擊鋪路。Dirty Cow 的攻擊過程，先在惡意網站埋伏，待下載至使用者的 Android 裝置後開採 Dirty Cow 漏洞，連接 C&C 伺服器更新惡意程式，並竊取資料，再假冒用戶的身份和電信商交易謀利，竄改裝置上的資料。



(資料來源：臺灣 iThome)

3.1.3、新型 Android 銀行木馬程式 Red Alert 2.0，感染超過 60 種銀行及社交應用軟體

SfyLabs 的安全研究人員偵測到一種新的 Android 銀行特洛伊木馬，名為 Red Alert 2.0，目前已經有超過 60 款金融和社交相關 App 被感染，木馬程式會透過受害的裝置獲得聯絡人清單，並接管簡訊功能，讓使用者無法接到金融機構相關來電或簡訊，來逃避雙因素身份驗證。

研究人員發現，Red Alert 2.0 以 500 美元的低價出租木馬程式，主要針對金融機構的網站及應用程式實施攻擊，現用 Android 6.0 作業系統的行動裝置也會受到感染；此外，Red Alert 的作者仍致力於將 SOCKS 和 VNC 模組添加到受感染設備的遠程控制功能，從而形成具有類似 RAT 功能的木馬程式。



(資料來源：美國 BLEEPINGCOMPUTER)

3.1.4、系統清理軟體 CCleaner 遭駭客修改免費版程式，建議用戶更新

知名系統清理軟體 CCleaner，主要用來清理垃圾程序和廣告 cookies 的軟體，功能受大眾喜愛。Piriform 在部落格證實 CCleaner v5.33.6162 和 CCleaner Cloud v1.07.3191 被駭，建議用戶下載無毒新版本。這些遭駭的版本包含遠程管理工具，企圖連接幾個未註冊網頁，可能會下載其他未經許可的程式。

Piriform 表示 CCleaner 不會自動更新，所以安裝有問題的版本

的每個人都需要刪除它並安裝新的版本。



(資料來源：美國 The Hacker News)

3.1.5、彙整網路戰爭規範 塔林手冊 2.0 出版

WannaCry 等勒索病毒前陣子讓全世界陷入混亂，加上全球強權紛指控敵國使用網路攻擊干預國內政治，全球唯一闡述網路空間法律的「塔林手冊」亦在近期發布最新版本。

網路衝突安全會議 (Cycon) 最早於 2009 年由北約卓越合作電腦防衛中心 (Cooperative Cyber Defence Center of Excellence) 在愛沙尼亞首都塔林召開，今年的 Cycon 中亦有來自全球各地的 500 多名資訊科技安全專家，齊聚北大西洋公約組織 (NATO) 在塔林召開的網路衝突安全會議 (Cycon)，並對塔林手冊展開熱烈討論。「塔林手冊 1.0」(Tallinn Manual 1.0) 於 2013 年由 19 名專家團隊彙整而成，由劍橋大學出版社 (Cambridge University Press) 出版。然而隨著網際網路技術與日俱增，網路規則也亟需同步更新，因此「塔林手冊 2.0」(Tallinn Manual 2.0) 因應而生。

塔林手冊編撰團隊的領導人英國艾克斯特大學 (University of Exeter) 教授施密特 (Michael Schmitt) 說，「塔林手冊 2.0」是關於網路衝突法律的獨特選集。教授亦指出，他旗下團隊的任務為開墾伴隨網路空間出現的「數位蠻荒地帶」，並希望這本書能成為次要法

律來源，目的在解釋法條而非制訂法律，因為法律是由國家制訂。



(資料來源：台灣中央社)

3.1.6、資安處建立國家級資安聯防架構，預計年底完成各關鍵基礎設施 ISAC

行政院資通安全處長簡宏偉於 9 月 13 日參與臺灣資安通報應變年會指出，為了能夠增強政府機關的防護，今年資安處新增資安協防員與資安服務團的角色，進駐 8 大關鍵基礎設施來建立完善的資安架構，落實各機關單位的資安防護，以及協助應變及通報。目前資安處初期已成立針對金融單位的資安服務團，該團成員共有 10 人，簡處長希望能在今年成立 4 個資安服務團。

簡處長認為，資安不是固若金湯的城牆，無法滴水不漏地防護所有的資安威脅，資安是一種風險管理的概念，需要控制可能產生的資安風險，政府透過早期預警、持續監控、通報應變，以及協助改善等 4 大面向，來落實以風險管理為核心的資安防護，其中通報應變是最重要。他舉例表示，去年一銀發生 ATM 盜領事件時，也遭到 DDoS 攻擊，其他遊戲業同時遭受一樣攻擊，但這些事件需要透過通報才能知道實際情況，更凸顯出資安問題不是一銀出現狀況後，僅解決金融資安單一條線的問題，而是也有其他面向需要處理，甚至可以瞭解整體臺灣資安環境來對症下藥。

資安處提供資安服務團協助 8 大關鍵基礎設施建立資安架構，來

完成資安處提供 4 大面向資安防護，進一步建立情報驅動 (Intelligence-base) 導向的國家層級資安聯防架構。簡處長也表示，預計要在年底前成立各機關 ISAC，之後把所有情報整合傳送到國家層級 N-ISAC 跟國際資安資訊分享。



(資料來源：臺灣 iThome)

3.1.7、藍牙漏洞恐讓上億手機門戶大開，不用配對或設定就能駭入裝置

安全公司 Armis Labs 研究人員揭露一項針對藍牙漏洞進行的攻擊手法，使開啟藍牙連線的行動裝置可能被駭客植入惡意程式。

攻擊者只要接近目標受害者，透過藍牙連線取得其 MAC 位置，即可藉由目標裝置的藍牙漏洞入侵，研究人員因此稱這項攻擊手法為 BlueBorne。在這類攻擊中，受害者只要開啟藍牙即可，不需與攻擊者裝置做過配對，不須任何設定，甚至不需設為「可尋找」模式，此外也不需要使用者介入就能入侵。

BlueBorne 基本上影響所有使用藍牙連線的裝置。根據估計，包括現代化手機、電腦、電視、汽車及醫療器材，今天這類裝置高達 82 億個。研究人員表示，藍牙連線裝置等往往是網路上防護最弱的終端，感染速度極快，且藍牙對所有作業系統具有最高權限，也提高 BlueBorne 攻擊的危險性。

他們相信 BlueBorne 手法可被用以發動各種型態攻擊，包括遠端執行程式碼以取得裝置控制權、存取公司資料或網路、滲透進企業內網而感染鄰近裝置，或是進行中間人(man-in-the-middle)攻擊。

微軟在本週的安全修補已經修補所有 Windows 版本的藍牙漏洞。iOS 10 也已修補了這些漏洞。也就是說，全球約 20 億 Android 裝置，以及舊版 iOS 裝置用戶仍然曝露於風險之中。雖然 Google 已經針對 Marshmallow 及 Nougat 釋出更新版，但受到 Android 現有版本及更新機制分歧的限制，勢必仍有眾多的 Android 裝置，因此從 Google Pixel、Samsung Galaxy、LG Watch Sport 到汽車音響可能都還未修補。



(資料來源：臺灣 iThome)

3.1.8、隨時監控 Wechat、QQ 最新木馬「xRAT」，讓你在駭客眼下等於裸奔

LookOut 工程團隊從 60 幾個 xRAT 的樣本中發現，有許多相似之處強烈顯示 mRAT 和 xRAT 來自同一個團體所開發。這些相似之處包括都有中文殘留在程式碼內，結構、解密金鑰也都極為類似。工程師 Michael Flossman 表示儘管三年前就被攤在陽光下，mRAT 至今仍非常活躍於行動裝置之中，並成為 xRAT 的更新基礎。

xRAT 多半以 PDF 檔案作為偽裝，能直接以管理員權限運行，這代表你的手機等於在駭客面前脫光光。除了具監控 Wechat、QQ 等

監控與自動刪除等能力以外，xRAT 還能竊取瀏覽器紀錄、設備的型號、ID，SIM 卡號碼，簡訊、聯繫名單，通話記錄，Wi-Fi 資料與電子郵件登入密碼，地理定位資料，可說手機裡的重要資料無一不包了；自動刪除也不限於本機，就連 SD 卡的資料也能一次完全清空。不僅如此，甚至連打開麥克風、攝影機，把錄影錄音內容發送出去，xRAT 都做得到。

目前還不清楚這種木馬的詳盡感染途徑，而且它也具備了先進的自動銷毀能力，不僅僅能將軟體本身從手機中刪除，並且會盡可能的刪除手機內的腳本資訊，就連技術人員都無從得知這個木馬曾經在手機內存在過，這也代表僅僅刪除 Wechat 或 QQ 並沒有用；若真想 100% 避免 xRAT，建議 Wechat 或 QQ 連碰都不要碰，或是用台專門使用 Wechat 或 QQ 備用機，並不要留下敏感資料或記錄。



(資料來源：臺灣 IN SIDE)

3.1.9、研究：Siri、Alexa 與 Cortana 有設計漏洞，可以人耳聽不見的超高頻率遙控

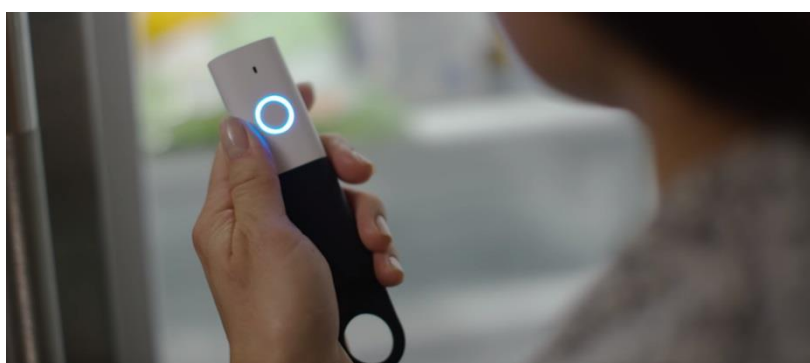
中國浙江大學的 6 名研究人員近日發表了一篇研究論文，指出市場上的各種數位語音助理皆含有設計漏洞，駭客只要將語音命令轉成人耳聽不見的超高頻率，以悄悄地要求裝置執行命令，研究人員把這

類的攻擊命名為「海豚攻擊」(DolphinAttack)。

DolphinAttack 的攻擊原理來自於一般人可以聽到介於 20 到 2 萬赫茲之間的聲音頻率，於是駭客製造了高於 2 萬赫茲的超高聲音頻率 (Ultrasonic Frequency)，人耳聽不見，但上述數位語音助理卻聽得見，於是駭客便可在使用者聽不見的狀態下秘密釋出指令。

被點名的數位語音助理包括蘋果的 Siri、Google Now、Samsung S Voice、華為的 HiVoice、微軟的 Cortana，以及 Amazon 的 Alexa。攻擊的方式也許是呼叫內建 Alexa 的 Echo 裝置開啟智慧鎖，或者是呼叫手機上的 Siri 撥打任意號碼，也能要求 Mac 上的 Siri 造訪惡意網站，甚至是改變 Audi Q3 汽車上導航系統的目的地。

但要執行海豚攻擊必須在距離聲控裝置 1.8 米的範圍內，且這些聲控裝置是隨時開啟的，此外，大部份的聲控裝置在接收到指令時通常會發出聲音而讓使用者有所警覺。研究人員則建議語音數位助理的開發商可限制相關技術所能接收到的聲音頻率，例如直接拒絕人耳收不到的頻率以避免遭到駭客濫用。



(資料來源：臺灣 iThome)

3.1.10、翁浩正：駭客揪團 形成黑色產業

台灣駭客協會常務理事、戴夫寇爾執行長翁浩正表示，現在的駭

客已經不像過去是幾個小朋友的單兵作戰，而是走向組織化，甚至形成一個「黑色產業」。企業必須提高資安層級，資安不再只是公司網管人員的事，老闆應該帶頭做，才能把資安意識擴及全公司。

翁浩正以「勝兵先勝—駭客攻防新趨勢」為題發表演講，一開場，他引述孫子兵法中「勝兵先勝，而後求戰。敗兵先戰，而後求勝」。提醒企業面對資安威脅，應該先做好準備再去打仗，才容易得勝，否則很容易被壓著打。

網路攻擊的手法不斷推陳出新，經常我們面對資安，就是不斷蓋城牆，想擋住駭客入侵，殊不知人家可能已經在開飛機攻擊，舊方法根本擋不住。「資安就是資訊不對稱」的問題，駭客其實是中性的，有壞駭客、也有好駭客。台灣駭客協會的目的，就是希望從駭客的角度傳授心法，讓大家知道駭客怎麼想？了解駭客的手法、工具、行為，才能防禦。



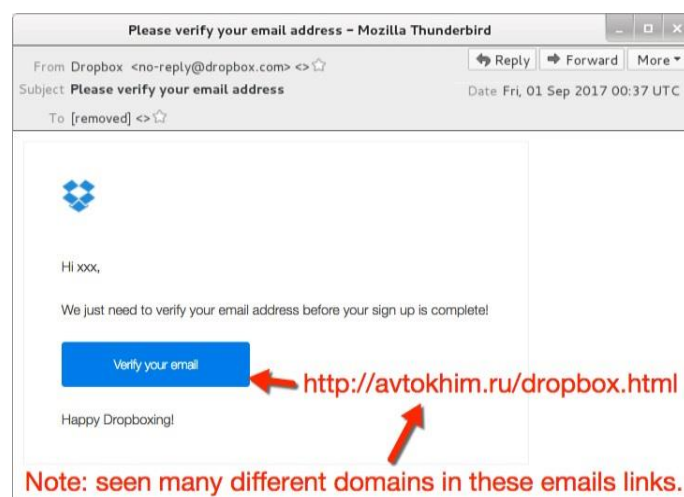
(資料來源：臺灣 iThome)

3.1.11、瀏覽器中跳出「找不到 Hoefler Text 字型」視窗，為惡意程式請勿點選更新

資安研究人員 Brad Duncan 警告，近期發現假冒的 Dropbox 網頁訊息誘騙使用者點選，在瀏覽器(Chrome 與 Firefox)開啟後跳出「找不到 Hoefler Text 字型」(The 'HoeflerText' font wasn't

found) 的提醒視窗並誘導更新，不過更新後即會下載一個偽裝成字型的 JavaScript 檔案，帶來的可能是 NetSupport Manager 遠端存取工具 (RAT) 或 Locky 勒索軟體。

此一惡意活動同時影響 Chrome 與 Firefox 瀏覽器，並未波及微軟的 IE 或 Microsoft Edge。



(資料來源：美國 SANS ISC)

3.1.12、不良的安全習慣與有風險的應用程式讓破壞性的網路攻擊以破紀錄的速度散播

全球高效能網路安全領導廠商 Fortinet (NASDAQ: FTNT) 在第二季的網路威脅報告中顯示，全球的網路安全習慣與有風險應用程式的使用情況惡化，讓破壞性的蠕蟲類攻擊以破紀錄的速度利用熱門漏洞。網路罪犯花很少的時間在研究突破的新方法，相對地他們專注於利用自動化和以意圖為基礎的工具來滲透，對企業營運的持續性帶來更大的衝擊。

有效的網路安全習慣對類蠕蟲攻擊至關重要：犯罪即服務 (Crime-as-a-Service) 基礎架構和自主攻擊工具，讓網路罪犯能夠在全球範圍內輕鬆進行操作。像 WannaCry 此類的威脅，他們的散播

速度和針對廣泛產業進行滲透的能力是非常卓越的。然而，若更多的企業組織能貫徹一致的網路安全習慣，它們就可以被大幅地扼阻。不幸的是，網路罪犯在利用熱門漏洞進行攻擊時，仍然取得很大的成功，這些系統都還沒有進行修補或更新。更糟糕的是，一旦特定的威脅自動化之後，攻擊者就不再局限於針對特定產業，因此它們的影響和運用範圍只會隨著時間不斷地增加。

使用預警威脅風險的技術：隨著應用程式、網路和設備等技術的使用和配置的發展，網路罪犯在殭屍網路的策略、漏洞的攻擊和惡意軟體，也同時不斷地在發展。網路罪犯已經準備妥當，能充份利用這些新技術或服務的弱點與機會。特別是業務有疑慮的軟體使用，以及超連接(hyperconnected)網路因而易受攻擊的 IoT 設備，皆代表潛在的風險，因為它們沒有得到持續一致的管理、更新或更換。



(資料來源：台灣網管人)

3.1.13、提報漏洞卻被當詐騙集團，資安專家提醒企業三種反應決定「漏洞」傷害程度

漏洞通報平台 Hitcon ZeroDay 發言人翁浩正在第十三屆台灣駭客年會 (HITCON) 上對企業呼籲，並點出企業因應資安漏洞的三大反應將直接決定漏洞對企業的傷害程度。

最好的情況是，企業網站上提供資安通報窗口，且窗口的層級夠高，能夠迅速回應、討論修復方式並修復完成，有些甚至會主動給予通報者獎金。

其次的情況是，面對漏洞提報的敏感度不夠高的企業，通常反應不積極，就曾有一企業在收到漏洞提報後，稱他們看不出有漏洞，讓翁浩正相當無奈，只能苦笑：「這不是漏洞，難道是功能嗎？」但最讓他們感到難過的是，有些企業會認為他們視為惡意的詐騙集團。除了態度消極，這類企業也多會有屢次修不好，和修補時間過長等狀況，甚至還會盲目使用防火牆設備阻擋。要繞過防火牆對駭客來說並不難，企業明確把漏洞修補好才是治本。

最糟的狀況，還是當他們向企業提報漏洞後，企業完全沒有回應，而且可怕的是這個比例在 Hitcon ZeroDay 平台剛發布時，甚至高達了五成。

為什麼會有這麼多漏洞？資安專家林昆立認為，主因就是「複製貼上工程師」太多，包含知名程式問答網站 Stack Overflow、程式教學書籍的範例、學校課程等，許多程式碼範例本身就有漏洞，因此開發者若照單全收，系統自然會有漏洞。



(資料來源：台灣數位時代)

3.2、駭客攻擊事件及手法

3.2.1、近期 Equifax 被駭案可能與 Struts 漏洞有關，建議用戶盡快更新

Apache 軟體基金會在 2017 年 9 月 5 日釋出的 Struts 2.5.13，修補當中一個自 2008 年就存在的重大安全漏洞(CVE-2017-9805)，此漏洞可能允許駭客自遠端執行任意程式。

Quartz[.]com 宣稱 Equifax 是因為此漏洞而遭入侵，但 Apache 在 2017 年 9 月 9 日聲明澄清美國消費者信用報告業者 Equifax 遭駭導致 1.43 億筆個資外洩的事件目前與釋出的漏洞補丁(CVE-2017-9805)無關，9 月 14 日在外部安全業者的協助下，證實此事件是因為 Apache Struts CVE-2017-5638，建議用戶務必更新。

●TWCERT/CC 提醒用戶：

影響平台： Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10 建議更新至 Struts 2.3.32 或 Struts 2.5.10.1

請確認網站主機是否使用 Apache Struts 2 的網頁應用框架，可透過檢查網站主機目錄中「WEB-INF\lib\」資料夾內的 Struts2.jar 檔，確認當前使用的版本。

如所使用的 Apache Struts 2 為上述(2.3.5 至 2.3.31 或 2.5 至 2.5.10)受影響之版本，則請更新官方 Github 所釋出最新之 Apache Struts 2.3.32 或 Struts 2.5.10.1 的版本。



3.2.2、德勤會計師事務所遭駭，電子郵件個資外洩

全球四大會計師事務所之一的德勤公司在 9 月 25 日傳出遭到駭客竊取機密文件的消息。該公司約有 5 百萬封電子郵件存在雲端，這些電子郵件內的個資恐遭外洩。攻擊主要目標以美國地區為主，而目前德勤也已向德勤的 6 名客戶表示他們的資料受到影響。

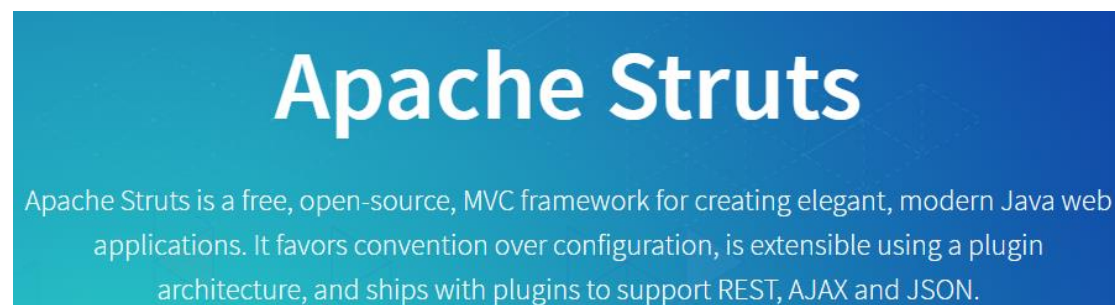
根據英國《衛報》報導，德勤早在今年 5 月就發現駭客攻擊的跡象，駭客更在 2016 年的 10 月或 11 月就造訪過德勤的系統。除了許多機密電子郵件外，駭客更掌握潛在進入管道與許多用戶的個人資料，例如密碼、IP 位置、商務或健康資料等。機密郵件中也包含許多敏感的安全議題與細節。

面對遭駭入的消息，德勤公司表示，只有少部分的用戶資料受到影響，對於雲端上有多少封電子郵件有被駭入的風險，德勤公司拒絕回應。德勤的發言人表示，將會出動內外的網路安全顧問與人員，對公司進行徹底的調查。

3.3、軟體漏洞資訊

3.3.1、Struts2 REST 插件程序的 XStream Handler 反序列化操作，可能遭利用惡意的 XML 內容提升權限，建議更新至最新版

Struts2 REST 插件使用帶有 XStream 程序的 XStream Handler 進行未經任何代碼過濾的反序列化操作，這可以在反序列化 XML 有效載荷時引導遠程代碼執行任意攻擊者都可以構造惡意的 XML 內容提升權限。



3.3.2、Google 發布 Chrome 之安全更新

Google 近日發布 Chrome 的安全更新，更新包含了錯誤及漏洞的修復和功能的改善，部分漏洞可能導致緩衝區溢位。



3.3.3、Microsoft 發布 9 月之安全更新

Microsoft 近日發布了 9 月安全更新，以解決多項產品中的多個漏洞，駭客可利用遠端方式攻擊以控制受影響的系統，請使用者盡快更新至最新版本，以取得最新的支援。



3.3.4、BlueBorne 安全性漏洞隱憂，請務必即時更新設備

安全公司 Armis 發現了一個藍牙傳輸漏洞，統稱為 BlueBorne，這個漏洞組合甚至允許惡意攻擊者在完全不觸碰到你的設備的狀態下就能造訪你的系統，包含筆記型電腦、手機與家用 IoT 設備皆有可能成為攻擊目標，請用戶隨時留意你的系統是否有安全性更新。



3.3.5、Apple 釋出 3 項商品之安全更新

Apple 旗下數項產品存在弱點，駭客可藉此取得遠端系統控制權，及造成 Cookies、密碼明文、Apple ID 外流，或者硬體資源不足時中斷程式，Apple 就相關版本軟體提供對應之安全更新。



3.3.6、VMware 釋出安全更新

VMware 多項產品出現 3 類弱點，影響等級高，為阻駭客藉此取得遠端系統控制權，VMware 就各系列、版本軟體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
106/11/01	2017 BSI Standards 國 際標準管理年 會	主辦單位：DIGITIMES 日期：2017 年 11 月 01 日 (三) 09:00-16:45 地點：台北市中正區徐州路 2 號 4 樓 (臺大醫院國際會議 中心 401 會議室) 線上報名連結： https://www.accupass.com/event/1709111322331775999769 資料來源： https://www.accupass.com/event/1709111322331775999769

時間	研討會/課程 名稱	研討會相關資料
		活動概要： BSI 英國標準協會年度盛會，根據全球管理趨勢、企業需求與時事議題訂定「資訊安全」與「永續經營」的相關研討議題，並邀請產官學研界的菁英專家進行分享，協助國內企業組織互相交流、接軌國際。
106/10/24	指出資安的新衣-2017 發揮設備最大功效研討會	主辦單位：資安人 日期：2017 年 10 月 24 日 (二) 09:00-17:30 地點：國泰金融會議中心 1 樓 線上報名連結： https://www.informationsecurity.com.tw/seminar/isevent20171024/register.aspx 資料來源： https://www.informationsecurity.com.tw/edm/IS_EDM_170930/ 活動概要： 希望提供給您們明確的答案與方向，將資安產品使用得更好，將產品設備的效能發揮極限。
106/10/20	新世代智慧資安研討會	主辦單位：Microsoft 日期：2017 年 10 月 20 日 (五) 09:30-16:30 地點：台北寒舍艾美酒店 3 樓 翡翠珍珠廳 線上報名連結： https://www.microsftevents.com/profile/form/index.cfm?PKformID=0x24639405039 資料來源： https://www.microsoft.com/taiwan/events/2017fall_cy

時間	研討會/課程 名稱	研討會相關資料
		bersecurity/ 活動概要： 「新世代智慧資安研討會」由台灣微軟和趨勢科技兩大資安巨頭聯合主辦，將展示最創新、最先進的管理與智慧化技術，以及在平台、應用程式與安全方案的整合應用。
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

時間	研討會/課程 名稱	研討會相關資料
		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 978 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。

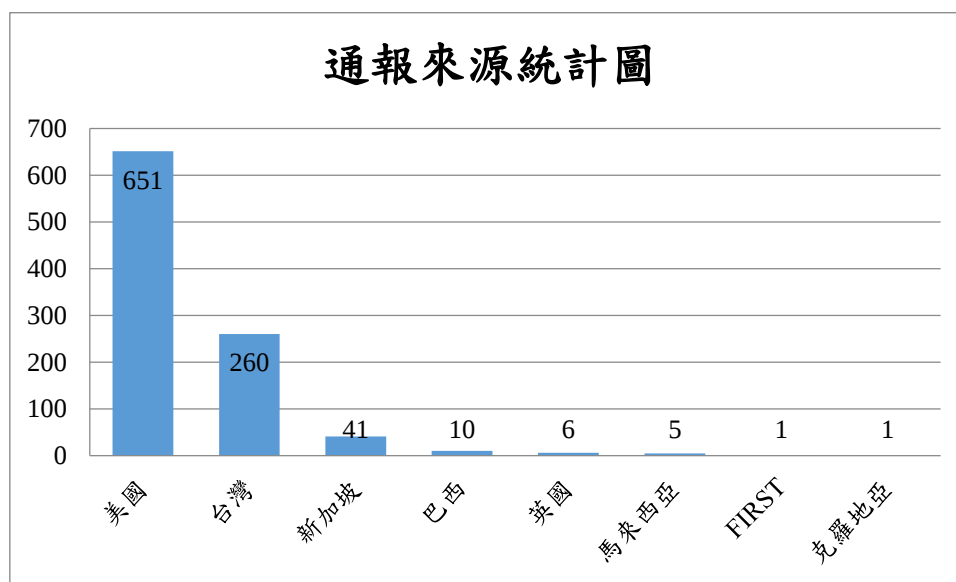


圖 1、通報來源統計圖

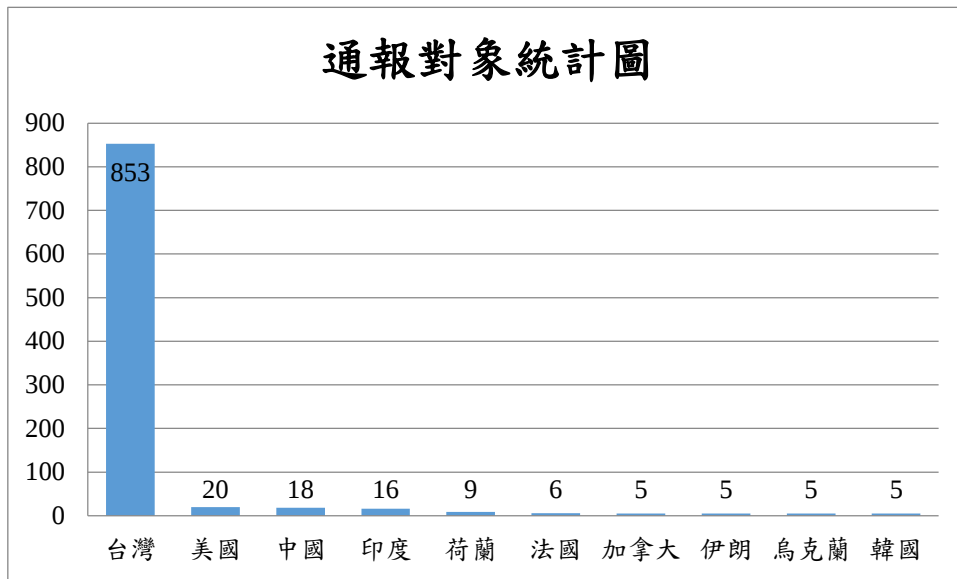


圖 2、通報對象統計圖

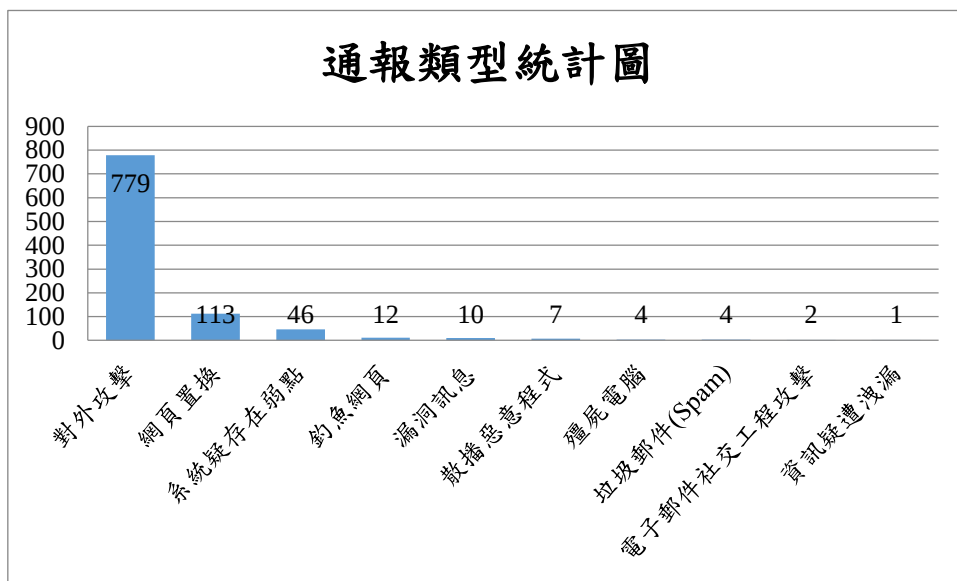


圖 3、通報類型統計圖

本月通報主要來源來自與國際組織合作獲得之情資，攻擊特徵經分析後，本月以“ Scanning port”（通訊埠掃描）為大宗，是駭客用

來尋找電腦或網路的漏洞的一種技術。駭客藉以偵測電腦上有哪些開放通訊埠。根據開放通訊埠資訊，可實作未經授權的存取(參考自 symantec)。企業平時除應定期弱點掃描、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“ Scanning port” 防護應保持關掉不必要的網路服務和軟體功能，並在防火牆增加規則，阻擋例外連線。

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 46%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 10 月 11 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。