TWCERT/CC 資安情資電子報

2019 年 9 月份

目錄

第 1 章、 封面故事

資安專家成功示範以修改過的 Lightning 連接線，透過 iPhone 駭入 Mac

資安專家成功以修改過的 Lightning 連接線連接受害者的 iPhone 和 Mac 後，在用戶不知不覺的情況下，以另一支 iPhone 遙控並駭入用戶的 Mac，並執行任意指令。

由駭客 _MG_ 等人開發的「O.MG Cable」，外觀上看起來和一般的 Lightning 連接線沒有任何差異，甚至在插入 iOS 裝置和電腦時，系統也不會偵測到任何異常。

但只要受害者利用這條連接線連接 iOS 裝置和 Mac 電腦，駭侵者就可以透過網路來控制受害者的 Mac，甚至包括開啟 Terminal 視窗，執行任意程式碼。

開發者指出，在這條 O.MG Cable 上可以預先載入多種指令或程式腳本，也能刪除自身運作的記錄。

- 資料來源：
  1. https://mg.lol/blog/omg-cable/
  2. http://mg.lol/blog/defcon-2019/
  3. https://www.vice.com/en_us/article/evj4qw/these-iphone-lightning-cables-will-hack-your-computer

第 2 章、 資安宣導

近期發生多起假檢警「境外匯款」鉅額詐騙，請小心勿上當

近期多件假檢警「境外匯款」鉅額詐騙，被害人年齡大多在 50 歲以上，事業有成、富有積蓄。接獲歹徒電話後，未加以查證即依照歹徒指示交付現金或(境外)匯款，造成財產損失也增加對自身生活環境之惶恐。

- 近期案例

吳女士(58 歲)家中經營紅外線機具生意，5 月份在家中接獲假銀行行員來電佯稱吳女士證件遭盜用被冒名開戶，表示將協助吳女士轉接檢察官處理，隨後假檢察官謊稱吳女士涉及香港洗錢案、多次傳喚皆未到案，要求被害人提領帳戶存款，交付公證以示清白，被害人信以為真，於 108 年 5 月 20 日至 6 月 25 日期間，分別於四家銀行臨櫃匯款 21 筆至香港（匯豐銀行）帳戶，金額合計美金 244 萬 8,170 元及歐元 70 萬 7,000 元（初估約新臺幣 1 億 187 萬 8,270 元）。

- 詐騙手法

一、歹徒先隨機撥打市內電話或手機門號，假冒醫療院所、電信局或銀行人員名義，以個人資料遭冒用，再轉接假冒警察、檢察官，佯稱被害人涉及刑案、多次傳喚未到，要求配合辦案、監管帳戶、交付現金或(境外)匯款以證明清白，不配合就要收押等。

二、歹徒為避免銀行發現可疑情形，還會以「偵查不公開」為由，引導被害人若有行員詢問領款用途，要以公司購置機具、投資、子女結婚、家中買房子等理由搪塞行員。

三、因民眾對司法程序不甚瞭解，待匯款多筆後，聯繫不到假檢察官，始知受騙。

請民眾不要隨便輕信『假檢警』的詐騙，收到訊息請先查證 165 或相關單位，不要受騙上當

第 3 章、 國內外重要資安事件

3.1、 資安趨勢

3.1.1 研究人員再次發現 Tesla Model S 無線鑰匙漏洞，可竊走車輛

去年發現 Tesla Model S 無線鑰匙可被任意複製的資安研究人員，再次發現另一漏洞，同樣可在車主不知不覺的情形下，以無線方式複製鑰匙並竊走車輛。

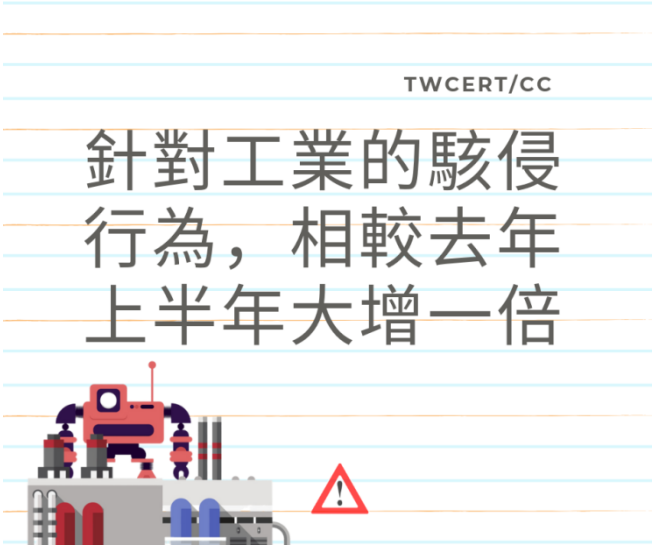
比利時 KU Leuven 大學資安研究人員 Lennert Wouters，日前在亞特蘭大市舉辦的資安學術研討會發表演說，再次指出 Telsa Model S 無線鑰匙存有資安漏洞；駭客能在不接觸到車主持有正版鑰匙的情形下，利用該漏洞破解鑰匙與車輛間的加密通訊，透過無線連結竊取資料，打造出一模一樣的無線鑰匙，從而竊走車輛。

這已是 Lennert Wouters 第二次揭露 Tesla Model S 無線鑰匙系統的漏洞。去年他首次發表此一漏洞時，完整示範了整個破解與複製鑰匙的過程；本次他只提供部分證明，並未完整示範。

Lennert Wouters 表示，新漏洞和去年相比，其可操作的範圍較小，距離車身必需近一點，花費複製時間也較長，但同樣有效。Tesla 原廠已得知該漏洞，並將在近期透過無線方式進行更新推播，以修補此漏洞。

- 資料來源：
  1. https://www.wired.com/story/hackers-steal-tesla-model-s-key-fob-encryption/

3.1.2 針對工業的駭侵行為，相較去年上半年大增一倍



IBM 轄下的資安研究單位 X-Force IRIS 日前發表研究報告，指出過去半年以來，針對工業和製造業的駭侵次數，和去年上半年相比，大幅增加了一倍。

IBM 的報告指出，該單位發現製造業被列為駭侵攻擊對象的比例，近年來大幅增加；近半年來有一半左右的駭侵事件，都是針對工業製造部門發動的。

這些駭侵行動最主要的攻擊手法，仍是透過釣魚郵件、發動水坑攻擊，或是駭入企業的第三方合作單位，以取得入侵所需的登入資訊。

有些駭侵團體會先在企業內網中潛伏數月之久，盡量搜刮所需的檔案；但也有駭侵行動在入侵之後就立刻展開。

IBM 估計，大型企業每次遭到攻擊，平均會有 12,000 台電腦遭到破壞；企業至少要花 512 小時才會發現遭到駭入，復原所需時間更長達 1,200 小時。

- 資料來源：
  1. https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/
  2. https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/

3.1.3 專家研製偵測軟體 Bluetana，抓到竊取信用卡資訊的假冒藍牙刷卡機

資安公司 Krebs 與美國大學共同合作，開發出一支能夠偵測出假冒藍牙刷卡機的 App，可以用來遏止信用卡資料竊盜事件。

Krebs on Security 發表專文指出，該單位與加州大學聖地牙哥分校、伊利諾大學香檳城區分校，共同開發出一支稱為 Bluetana 的手機 App，希望能夠找出各種透過藍牙傳輸資料的假冒信用卡刷卡機。

這類假的藍牙刷卡機經常被歹徒放在美國各地自助加油站的刷卡機旁，當不知情的顧客刷卡時，信用卡資料就有被竊取的風險。

研究單位表示，他們讓 44 位志願者使用 Bluetana 偵測全美六個州的 1,185 個加油站，一年來發現了 64 個假冒刷卡機。

Bluetana 將有助於加油站管理者與警察更快速找到可疑的假冒刷卡機，減少信用卡資料竊取與盜刷造成的巨大損失。

- 資料來源：
  1. https://krebsonsecurity.com/2019/08/meet-bluetana-the-scourge-of-pump-skimmers/

3.1.4 單眼相機也可能被勒贖軟體攻擊

資安研究單位 Check Point 發表研究報告，指出單眼相機也可能成為勒贖軟體的攻擊目標。

Check Point 的資安專家指出，單眼相機用來傳送相片資料的 PTP 傳輸協定，存有易被駭客攻擊的漏洞；駭客可利用 PTP 在相機中植入勒贖軟體。

Check Point 使用 Canon EOS 80D 進行攻擊示範，透過相機的 Wi-Fi 相片傳輸功能，將勒贖軟體植入相片，並且將記憶卡中的所有影像資料加密，讓用戶無法存取相片或影片。

Check Point 在今年三月發現這個漏洞，並且通報 Canon；Canon 也於日前推出安全更新。攝影愛好者除了應該立即更新，並應避免使用未加密的無線網路傳輸照片；而在相片傳輸完成後應立即關閉相機的 WiFi 功能。

- 資料來源：
  1. https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera/
  2. https://global.canon/en/support/security/d-camera.html
  3. https://www.theverge.com/2019/8/11/20800979/check-point-canon-eos-80d-dslr-malware-ransomware-cybersecurity

3.1.5 美國政府警告，2020 總統大選恐遭勒贖攻擊

美國政府官員指出，2020 總統大選時，駭客可能會加強攻擊選民資料庫；尤其是勒贖攻擊。

據路透社報導指出，美國政府已著手規畫針對 2020 大選選民資料庫的資安強化作業，各項新保護措施預計在一個月內就會上線。

美國官員指出，該資料庫曾在 2016 年遭俄羅斯駭客入侵，當時駭客的目的僅為竊取資料；但 2020 年可能發生的駭侵行為，其動機將會是操弄、干擾選舉或破壞資料。

美國國土安全部旗下的網路基礎架構安全局（CISA）特別針對勒贖攻擊的威脅發出警告；過去半年來已有多個美國大小城市，因勒贖攻擊而造成市政系統全面癱瘓。

CISA 已經開始會同 2020 大選各相關單位，共同研擬遭到各種攻擊時的反應計畫，同時加強對各式網路攻擊的防範準備。

- 資料來源：
  1. https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-u-s-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222

3.1.6 McAfee 指出：2019 年第一季，每分鐘就有 504 次駭侵攻擊

資安廠商 McAfee 發表統計數字，指出 2019 年上半年各種駭侵攻擊的統計數字。

根據 McAfee 的報告，2019 年第一季的全球駭侵活動仍持續上升，平均每分鐘就觀測到高達 504 次各式駭侵活動。其他重要的觀測統計數字如下：

- 與去年同期相較（以下同），勒贖攻擊增加了 118%，駭侵的進行策略與技術都有所提升；
- 超過 20 億組帳號的登入資訊被盜，且在暗網中流通；
- 愈來愈多針對公司行號進行的駭侵攻擊，以魚叉式網路釣魚（Spearphishing）為初始攻擊手法；
- 意在挖掘新虛擬貨幣的挖礦惡意軟體攻擊增加 29%；
- 針對亞太區的網路攻擊增加 126%。

詳細的報告資料，可參考 McAfee 的報告全文。

- 資料來源：
  1. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

3.2、國際政府組織資安資訊

3.2.1 最新統計指出，倫敦每月平均遭到近一百萬次網路攻擊

資安研究單位指出，今年前三個月的統計，倫敦平均每月遭到近一百萬次網路攻擊，較去年提高 90%。

資安研究單位「資訊自由」（Freedom of Information）發表研究報告，指出 2019 年第一季，倫敦一共遭到 280 萬次各式網路攻擊事件，平均一個月就有近一百萬次。

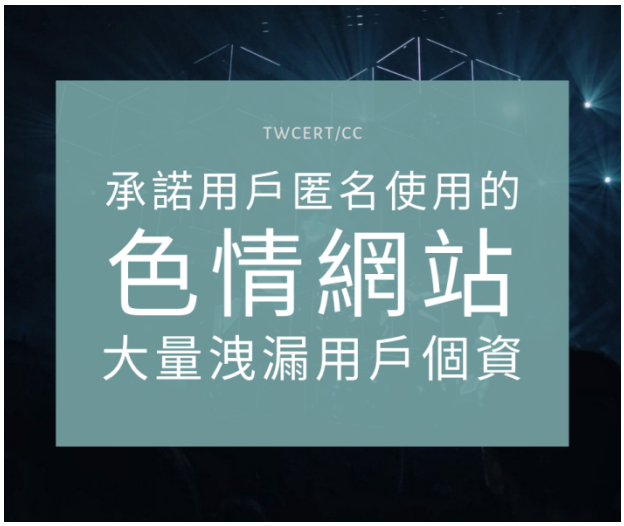
和 2018 年四月到十二月的攻擊統計相比，身為英國金融中心的倫敦，遭網路攻擊的次數上升了 90%；資安單位認為一方面是因為攻擊次數確實有所增加，但也可能是因為攻擊偵側技術的進步所致。

在去年四月以來的 720 萬次網路攻擊中，垃圾郵件佔絕大多數，達 690 萬次；其次是釣魚詐騙信件，有近 25 萬次，和惡意軟體相關的攻擊也有近兩萬起。

- 資料來源：
  1. https://www.infosecurity-magazine.com/news/city-of-london-one-million/

3.3、 行動裝置資安訊息

3.3.1 承諾用戶匿名使用的色情網站，大量洩漏用戶個資



一個名為 Luscious.net 的色情網站，承諾讓用戶匿名使用，然而卻發生大量用戶個資外洩事件。

據資安專家指出，該網站的用戶資料庫被發現公開在外部網路上，而且沒有任何保護措施；外洩的個資包括 110 萬名用戶的用戶名稱、email、使用記錄、性別、所在地等資料欄位。

另外，像是用戶自己上傳的相片和影片內容、留言、貼文、喜愛的內容、追蹤的帳號等資料也在外洩之列。

這個色情網站的內容，以變態和動漫的色情內容為主，雖然名氣不大，但據 Alexa 統計，其流量位居全美五千大網站之列。

資安專家和 TechCrunch 試圖和該網站連絡，以通報個資外洩事件，但都沒有得到任何回應。

- 資料來源：
  1. https://www.vpnmentor.com/blog/report-luscious-data-breach/
  2. https://techcrunch.com/2019/08/19/anonymous-luscious-hentai-manga-porn-security-lapse/

3.4、 行動裝置資安訊息

3.4.1 Apple iPhone 的 AirDrop 功能可能洩漏手機門號等資訊

資安研究單位證實，透過低功率藍牙協定進行廣播連線的 Apple iPhone AirDrop 功能，可能洩漏包括手機門號在內的各種資訊。

據資安研究單位 Hexway 的報告指出，非常方便的 iPhone AirDrop 功能，可能洩露包括手機門號、電池容量、裝置名稱、無線網路連線狀況、iOS 版本號碼等資訊。

蘋果的 Mac 和 iPhone、iPad 等產品，有極為方便的「接續互通」功能，讓用戶可以簡單地透過無線方式傳送檔案，或在另一台設備上完成工作；這些功能係透過低功率藍牙和 Wi-Fi 無線連結完成，特別是低功率藍牙的廣播功能。

Hexway 分析 iPhone 發出的低功率藍牙資料封包，發現手機門號資訊係以 SHA256 進行加密傳送；然而駭客只要針對某一區域的所有手機門號預先以 SHA256 加密，得到一個對照表後，再用 iPhone 發出的門號 SHA256 雜湊值查表比對，即可找出你的門號。

Hexway 的報告中，也分析了運用 SHA256 查表法取得用戶 Wi-Fi 密碼或其他資訊的可能手法。

- 資料來源：
  1. https://hexway.io/blog/apple-bleee/
  2. https://arstechnica.com/information-technology/2019/08/apples-airdrop-and-password-sharing-features-can-leak-iphone-numbers/

3.4.2 駭客公開最新 iOS 12.4 越獄破解資訊

由於 Apple 未在最新版 iOS 12.4 中修補過去已經修補過的漏洞，致使駭客得以發布針對 iOS 12.4 的越獄（Jailbreak）方法。

針對最新版 iOS 的越獄方法，已經很久沒有在網路上公開發表過；這次駭客之所以能對最新版 iOS 發表越獄方法，其實是因為 Apple 未在 iOS 12.4 修補一個已在 iOS 12.3 中解決的安全漏洞。

不少用戶照著公開的方法，也成功破解安裝了 iOS 12.4 的 iPhone。

資安專家指出，過去資安研究者甚少發表 iOS 的破解方法，是因為這些破解方法非常值錢，往往可以賣到幾百萬美元之譜；一旦公布，Apple 很快就會推出更新軟體修補漏洞，讓破解方法失效。

用戶破解 iPhone 主要是希望能讓手機更加個人化（例如使用自定系統字體）、破解系統限制，或是執行某些未在 App Store 中發行的應用軟體；然而這可能帶來相當大的資安風險。

- 資料來源：
  1. https://www.vice.com/en_us/article/qvgp77/hacker-releases-first-public-iphone-jailbreak-in-years

3.5、 軟體系統資安議題

3.5.1 英國爆發生物辨識資安事件，百萬人指紋、面孔與帳密未加密存放

英國爆發有史以來最嚴重生物辨識資訊資安事件，計有超過一百萬人的臉部、指紋圖像資料、登入帳密等個資，存放在未經加密的公開資料庫中，可任人隨意取用。

以色列資安專家 Noam Rotem 和 Ran Locar 日前發現，英國保全公司 Suprema 旗下的 Biostar 2 生物辨識門禁系統，將其辨識資料庫放在網路上，而且未經加密；只要針對其 Web 管理界面的 URL 略經修改，即可進入資料庫中。

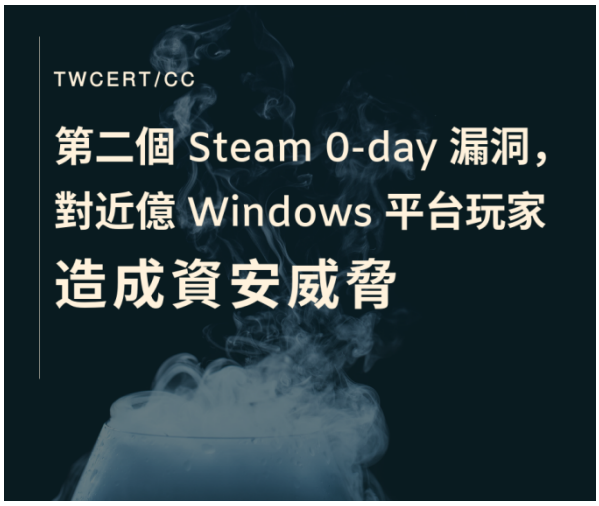
專家指出，資料庫中一共有兩千七百八十萬筆資料，檔案大小高達 23GB，內含資料欄位包括指紋和面部掃瞄資料、面部相片、用戶帳號與密碼、進出記錄、安全控管權限層級等個資，影響人數超過一百萬人。

Biostar 2 與其相關系統的用戶遍布全球，共有 83 國、超過五千七百家公私單位採用該系統。受影響單位包括英國倫敦警察廳、英國各國防相關單位等。

資安專家進一步指出，這個資料庫不但完全未經加密，甚至連基本的權限控管也付之闕如；他們可以任意在資料庫中新增用戶或更改資料。

- 資料來源：
  1. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

3.5.2 第二個 Steam 0-day 漏洞，對近億 Windows 平台玩家造成資安威脅



俄羅斯資安研究員連續公布兩個遊戲平台 Steam 的 Windows 0-day 漏洞，其中第二個漏洞對近一億名 Windows 平台遊戲玩構成嚴重威脅。

被俄羅斯資安研究員 Vasily Kravets 公布的 Steam Windoes 0-day 漏洞，不但能夠提升執行權限，也可用來執行任意程式碼，對該平台上九千六百萬名 Windows 玩家的資安造成嚴重威脅。

Kravets 和另一名資安研究員，日前發現一個 Steam 平台的 0-day 漏洞，同樣可以用來執行任意程式碼，但 Steam 無意修補，兩人於是公開該漏洞資訊。Steam 平台隨即將兩人自其 HacketOne 資安漏洞獎金計畫中除名；Keavets 隨即公布第二個 0-day 漏洞。

Steam 表示，這兩個 0-day 漏洞都必須實際在受害者用戶電腦上進行實體操作，無法遠端進行駭侵操控，這也是 Steam 認為兩位研究者不符 HackerOne 參賽資格的主因；這兩個資安漏洞也已透過更新修補完成。

- 資料來源：
  1. https://amonitoring.ru/article/onemore_steam_eop_0day/
  2. https://www.bleepingcomputer.com/news/security/second-steam-zero-day-impacts-over-96-million-windows-users/

3.5.3 企業內的 IoT 裝置，是俄羅斯大規模攻擊的目標

微軟發表研究報告，指出該公司發現俄羅斯支持的 APT28 駭侵團體，以企業內的 IoT 裝置做為攻擊跳板。

微軟的資安研究單位 Microsoft Threat Intelligence Center 日前指出，該單位觀測到來自俄羅斯支持的 APT28 駭侵團體（又名 Strontium 或 Fancy Bear），近來對企業的駭侵攻擊，係以企業內的各種連線裝置為目標。

被列入攻擊目標的企業連網裝置，包括 VoIP 電話、網路印表機、網路影音解碼器等。

微軟說，許多企業要不是沒有更新這些裝置的韌體，以修補資安漏洞，就是連這些裝置的預設登入帳密都沒有改掉，給了駭侵團體可乘之機。

一旦駭侵團體透過這些裝置侵入企業內網，就有可能進行更進一步的駭侵行為，鎖定電腦或伺服器進行正規攻擊。

- 資料來源：
  1. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
  2. https://www.bleepingcomputer.com/news/security/russian-apt-abuses-iot-devices-to-infiltrate-corporate-targets/

3.5.4 跨國共享工作空間 WeWork，全球各地使用相同的易猜測 Wi-Fi 密碼

資安專家指出，WeWork 共用工作空間提供的 Wi-Fi 十分不安全，不但使用非常容易猜到的密碼，這套密碼竟然在全球各地的 WeWork 辦公空間均可使用。

WeWork 是最近聲量很高的跨國共享工作空間服務商，最近高調申請股票掛牌上市，然而被資安專家指出其辦公空間提供的無線網路，存有各種安全問題。

首先，在美國與全球各處一共 528 個 WeWork 辦公空間提供的 Wi-Fi，竟然使用非常容易猜測的密碼來進行保護，而且各辦公空間的 Wi-Fi SSID 名稱與密碼都完全相同。

其次，WeWork 的 Wi-Fi 沒有使用更嚴密的加密協定，僅使用非常容易破解的 WPA2 個人版；密碼更是長久未曾更換。這使得任何曾經租用過 WeWork 空間或知道密碼的人，都能輕鬆進入其無線網路，對網路中的其他電腦發動中間人攻擊，或是以相同的 SSID 與密碼誘拐用戶連進其自行設定的無線網路。

- 資料來源：
  1. https://www.fastcompany.com/90391748/weworks-wi-fi-network-is-easy-to-hack
  2. https://twitter.com/seancaptain/status/1164184574148120581

3.5.5 台灣資安公司揭露多家企業級 VPN 服務漏洞後，駭客用來攔截流量

台灣資安廠商戴夫寇爾（DevCore）公布若干大型企業 VPN 服務商的資安漏洞後，隨即傳出有駭客利用這些已公開的漏洞，駭入兩家 VPN 服務。

台灣著名的資安廠商戴夫寇爾（DevCore），日前在 Black Hat 國際資安研討會上發表研究報告，公開了數家大型企業級 VPN 服務廠商的多項資安漏洞與駭侵測試報告；被點名的其中兩家 VPN 服務商 Pulse Secure VPN 與 FortiGate VPN 隨即傳出被駭的消息。

據報，駭客利用了 DevCore 發表的部分技術細節與概念實作方法，先在 Internet 上掃瞄具有資安漏洞的主機，駭入之後隨即取得這兩家 VPN 的系統相關檔案。

利用取得的檔案資料，駭客即可偽裝成受信任的連線裝置，連入其 VPN 網路。

- 資料來源：
  1. https://devco.re/blog/2019/08/28/Pulse-Secure-SSL-VPN-advisory/
  2. https://devco.re/blog/2019/08/09/Fortigate-SSL-VPN-advisory/
  3. https://www.zdnet.com/article/hackers-mount-attacks-on-webmin-servers-pulse-secure-and-fortinet-vpns/

3.6、 軟硬體漏洞資訊

3.6.1 Google 資安團隊 Project Zero 一口氣發現多個 iOS 安全漏洞

Google 的資安團隊 Project Zero 最近一口氣公開六個該團隊發現的 iOS 安全漏洞，其中有些漏洞可讓駭客在用戶不知情的情況下侵入系統，甚至執行任意程式碼。

這六個被發現的漏洞，第一個是 CVE-2019-8646，駭客可利用這個漏洞遠端讀取裝置中的資訊；因為沒有任何用戶互動，所以用戶難以發現。

第二個漏洞是 CVE-2019-8660，與記憶體管理有關；駭客可利用特殊設計的程式碼引發記憶崩潰（memory corruption），藉以造成應用程式停止運作或執行任意程式碼。其他漏洞說明，詳見參考連結。

上述的六個資安漏洞，其中的四個已在七月 22 日發行的 iOS 12.4 中修補完成，但仍有兩個漏洞尚未完成修補。

- CVE 編號：
  - CVE-2019-8646
  - CVE-2019-8647
  - CVE-2019-8660
  - CVE-2019-8641
  - CVE-2019-8662
  - CVE-2019-8624
- 影響產品：iOS 12.4 之前版本
- 解決方案：升級至 iOS 12.4 以上版本
- 資料來源：
  1. https://bugs.chromium.org/p/project-zero/issues/detail?id=1858
  2. https://www.securityweek.com/google-researchers-find-remotely-exploitable-vulnerabilities-ios
  3. https://twitter.com/natashenka/status/1155941108553175041

3.6.2 Intel 處理器再次發現嚴重資安漏洞

Intel 各型處理器，繼去年年初被發現其分支預測執行單元存有稱為「Spectre」和「Meltdown」的嚴重資安漏洞後，近日又被發現另一個類似的資安漏洞，可導致在 CPU 內存取的敏感資料遭到竊取。

駭侵者可利用這個資安漏洞，以「旁路攻擊」（Side-channel attack）方式濫用一種稱為 SWAPGS 的指令，取得處理器核心記憶體中的敏感資料，例如密碼、token、加密密鑰等。

這個漏洞雖然和先前的 Spectre、Meltdown 很類似，但先前各作業系統廠商發行的資安修補程式，對此一漏洞是無效的，必須另行安裝新的更新修補程式。

微軟表示，已在七月發行的更新包中修補了這個漏洞，各 Windows 版本用戶應立即安裝此一更新。

- CVE 編號：CVE-2019-1125
- 影響產品(版本)：Intel 2012 年後推出的各型 x86 處理器。
- 解決方案：安裝各作業系統廠商推出的最新軟體更新套件。
- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1125
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1125
  3. https://www.infosecurity-magazine.com/news/new-intel-swapgs-flaw-spells-bad/

3.6.3 Adobe Acrobat 與 Adobe Reader 被發現多個安全漏洞

這這批安全漏洞總數達到 60 個以上，以資料洩漏和任意程式碼執行的資安風險為主，而且受影響的平台不只 Windows，也包括 Mac 版本。

Adobe 已針對這些重要安全漏洞發行更新，請所有 Adobe Acrobat 和 Adobe Reader 的用戶盡速更新，以修補漏洞。

- CVE 編號：多個 CVE 編號，詳閱參考連結。
- 影響產品(版本)：Adobe Acrobat 與 Adobe Reader Windows/Mac 多個版本，詳閱參考連結之文件內列表
- 解決方案：安裝 Adobe 發行之最新安全更新軟體即可
- 資料來源：
  1. https://helpx.adobe.com/security/products/acrobat/apsb19-41.html

3.6.4 老舊聯想筆電被發現另一嚴重資安漏洞

資安研究單位 Pen Test Partners 發表研究報告，指出已經不再支援的聯想 Lenovo Solution Center 軟體，存有另一嚴重資安漏洞；駭侵者可藉此漏洞提升自身權限至管理者或系統階層權限，並且執行任意程式碼。

Lenovo Solution Center 是先前預載在所有聯想筆電的系統管理程式，由於先前曾經爆發另一嚴重資安問題，聯想已經停用該程式且停止支援；但可能仍有相當數量的老舊聯想筆電，仍在執行這個程式。

聯想已經針對這個資安漏洞發布資安通報，並且建議所有還在執行 Lenovo Solution Center 的老舊聯想電腦用戶，盡速升級至新版的 Lenovo Vantage 軟體。

- CVE 編號：CVE-2019-6177
- 影響產品：Lenovo Solution Center 03.12.003
- 解決方案：升級至 Lenovo Vantage。
- 資料來源：
  1. https://threatpost.com/bug-found-in-pre-installed-software/147657/
  2. https://nvd.nist.gov/vuln/detail/CVE-2019-6177
  3. https://support.lenovo.com/tw/zh/solutions/len-27811

3.6.5 SanDisk SSD Dashboard 管理程式存有資安漏洞

資安專家 Martin Rakhmonov 在日前發表研究報告，文中指出全球儲存裝置大廠 SanDisk 推出的電腦端 SSD 管理程式存有兩個資安漏洞。

首先是 CVE-2019-13466，這個資安漏洞在於把用來保護用戶資訊的加密密鑰，以明碼寫死在程式碼中，而且非常容易破解。

其次 CVE-2019-13467 的問題更加嚴重：該軟體與 SanDisk 伺服器透過網路傳輸資料時，仍使用未經加密的 http 協定，而非加密的 https，因此非常容易遭到中間人攔截攻擊。

在作者向 SanDisk 通報這兩個問題後，SanDisk 做了相對應的調整：目前不再將用戶資料自動上傳到其伺服器，改為由用戶在通報問題時手動上傳，另外傳輸協定也改為 https。

- CVE 編號：CVE-2019-13466、CVE-2019-13467
- 影響產品：SanDisk SSD Dashboard 2.5.1.0 之前版本
- 解決方案：升級至 SanDisk SSD Dashboard 2.5.1.0 起之新版
- 資料來源：
  1. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/sandisk-ssd-dashboard-vulnerabilities-cve-2019-13466-cve-2019-13467/
  2. https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=25983

3.6.6 D-Link DVA-5592 路由器存有資安漏洞

D Link DVA-5592 無線路由器的 Web 管理界面，存有中等嚴重程度的資安漏洞。

透過此漏洞，駭客可以跳過帳密認證程序，直接進入管理界面，並且取得用戶的敏感資訊，例如 Wi-Fi 密碼或用戶的手機門號。

發現這個漏洞與本機其他安全漏洞的資安研究人員表示，已在一個多月前將漏洞資訊提報給 D-Link 的資安通報專線，但目前仍未看到 D-Link 推出修補程式。

- CVE 編號：CVE-2019-6969
- 影響產品：D-Link DVA-5592
- 解決方案：截稿前尚無
- 資料來源：
  1. https://rhaidiz.net/2019/02/27/dribble-router-vulns-dlink-alcatel-cve-2019-6969-cve-2019-6968-cve-2019-7163/
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6969

第 4 章、 資安研討會及活動

2019 CYBERSEC 101	
活動時間	2019/9/6(五)、9/20(五)、10/25(五)、11/8(五)、11/29(五)
活動地點	台北市松山區敦化南路一段 108 號 B2
活動網站	https://cybersec101.ithome.com.tw/
活動概要	 CYBERSEC 101 為全新系列研討會，藉由定期舉辦，持續對資安實務做更全面更深入的探討與交流，期能擴大 IT 與資安人員的資安視野，精進資安防禦技能，持續提升企業組織的資安防禦水平。 2019 年 CYBERSEC 101 資安實務研討會的第一場次，將以當前全球最受企業與政府矚目的「NIST Cybersecurity Framework」為主題，透過此一完整涵蓋企業五大防禦構面的資安藍圖，由資安專家帶領 IT 與資安人員，以每個月一個子題的節奏，依序探討 NIST Cybersecurity Framework 的五大資安防禦功能（Identify、Protect、Detect、Respond、Recover），完整檢視企業資安防禦的全貌，為企業資安防禦奠定持續改善的基礎。

CDX2.0 推廣活動	
活動時間	2019/09/10(二) 13:00~16:00
活動地點	臺北市和平東路二段 106 號 4 樓
活動網站	https://nchc-cdx.kktix.cc/events/cdxactivity-0910
活動概要	 雲端資安攻防平台（Cyber Defense Exercise，CDX）為科技部指導國家高速網路與計算中心（國網中心）執行「資訊安全開放資料平台研發與惡意程式知識庫維運（II）」計畫之一，平台採用雲端服務的架構進行規劃與設計，主要用以改善傳統攻防平台受限於軟硬體限制、管理與使用不易等問題，以虛擬化的架構實現攻防演練場景快速部署的可行性，提供多人多場景同時進行攻防演練之環境，並可提供模擬真實的網路環境用於攻防技術相關研究，讓參與者能夠熟悉與掌握以往曾經發生過的資訊安全事件，並從中學習資訊安全的檢測與分析技巧。

Cyber Attack Taipei Series 2019	
活動時間	2019/09/17 (二) 8:00~17:00
活動地點	台北市中山區中山北路二段 39 巷 3 號
活動網站	https://www.eventbrite.com/e/cyber-attack-taipei-series-2019-tickets-68951581035

活動概要	 **Threat Intelligence, Cybersecurity, Digital Investigation, Cyber Forensics, Artificial Intelligence, IoT, Machine Learning, BigData, Fintech** **About this Event** WHO SHOULD ATTEND • Administrators • Chief Information Security Officers (CISO) • Chief Information Officers (CIO) • Chief Technology Officers (CTO) • IT Directors • Cyber Security Heads • Senior Executives in Security • Technology and Risk Officers • Network and Information Profiles

9 月台北例會-物聯網時代的資安與隱私風險管理	
活動時間	2019/09/24 (二) 14:30~16:30
活動地點	台北市信義區基隆路一段 143 號 3 樓
活動網站	https://www.caa.org.tw/newsdetail-15994.html
活動概要	中華民國電腦稽核協會 Computer Audit Association **1.物聯網產品資安與隱私風險管理框架介紹** **2.組織採用物聯網設備之風險與管理措施** **3.組織物聯網設備管理成熟度評鑑方法介紹**

	主講講師： 姓名：李冠樟 機構：安侯企業管理股份有限公司 單位：資訊科技諮詢服務 職稱：經理 證照：CISA、CISM、CEH、ISO 27001 LA、BS 10012 LA、ISO 20000 LA、ISO 22301 LA、ITIL Foundation 專長：資訊安全管理、資訊系統稽核、個人資料與隱私保護、資訊服務管理、營業秘密保護

9 月新竹例會-機敏資料管理實務講座	
活動時間	2019/09/25 (三) 09:30~12:30
活動地點	新竹市光復路二段 153 號 2 樓
活動網站	https://www.caa.org.tw/newsdetail-15990.html
活動概要	中華民國電腦稽核協會 Computer Audit Association **1.營業秘密與智慧財產的法制要件** **2.新版營業秘密法對企業之影響** **3.營業秘密的侵害與救濟** **4.案例說明與企業應有之防護佈局** **講師：** 張紹斌 中華民國電腦稽核協會理事長/合盛法律事務所主持律師 證照 - 中華民國律師、司法官、BS 10012

第 5 章、 2019 年 8 月份事件通報概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資通報，以下為各項統計數據，分別為通報地區統計圖及通報類型統計圖。

通報地區統計圖為本中心所接獲之通報中，針對通報事件責任所屬地區之通報次數比率，如圖 1 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比率，如圖 2 所示。

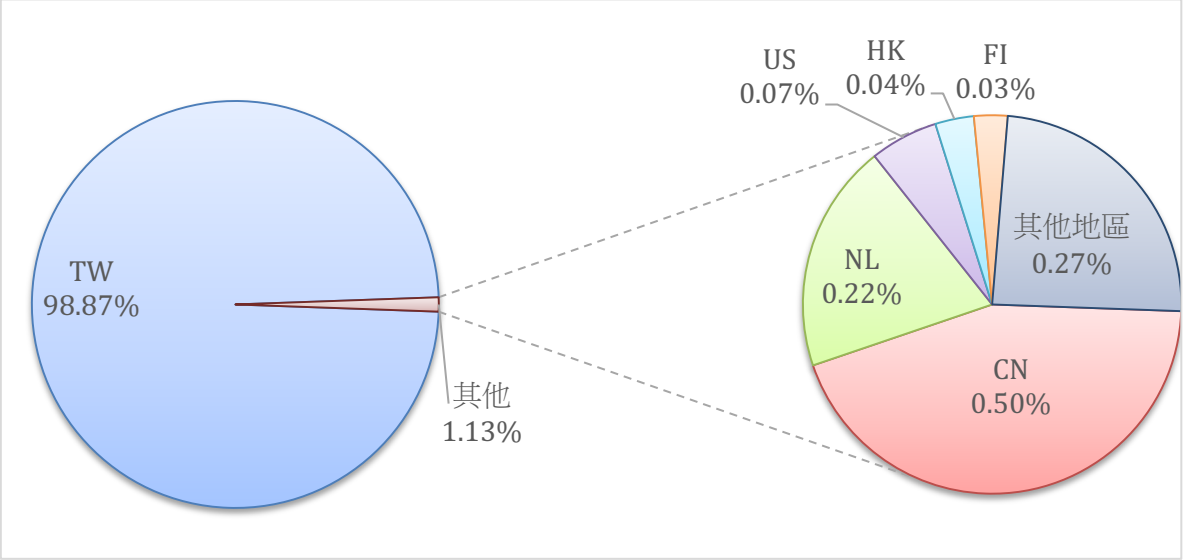


圖 1、通報地區統計圖

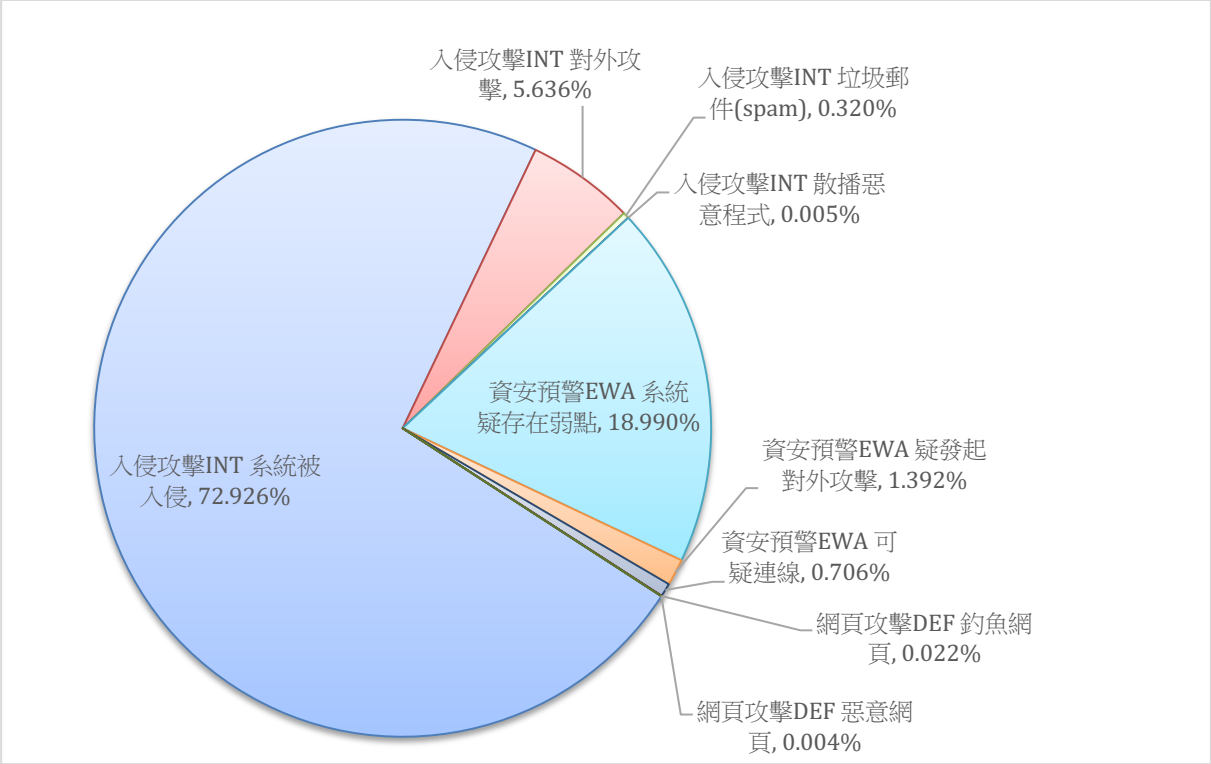

入侵攻擊INT 對外攻擊, 5.636%
入侵攻擊INT 垃圾郵件(spam), 0.320%
入侵攻擊INT 散播惡意程式, 0.005%
資安預警EWA 系統疑存在弱點, 18.990%
資安預警EWA 疑發起對外攻擊, 1.392%
資安預警EWA 可疑連線, 0.706%
網頁攻擊DEF 釣魚網頁, 0.022%
網頁攻擊DEF 惡意網頁, 0.004%
入侵攻擊INT 系統被入侵, 72.926%

圖 2、通報類型統計圖

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：2019 年 9 月 10 日

編輯：林克容、江奕昉、張洛瑀

服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官網：https://twcert.org.tw/

Facebook 粉絲專頁：https://www.facebook.com/twcertcc/

Instagram：https://www.instagram.com/twcertcc/

Twitter：@TWCERTCC