TWCERT/CC 資安情資電子報

2023 年 7 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 5 章節：

第 1 章、封面故事：上月 TWCERT/CC 所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第 2 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第 3 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 4 章、TVN 漏洞公告：TWCERT/CC 為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN) 平台之產品漏洞資訊。

第 5 章、資安情資分享概況：將上月份 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

目錄

第 1 章、 封面故事

Toyota 發現更多配置錯誤的雲端伺服器，造成客戶個資外洩長達 7 年

全球汽車製造行銷大廠 Toyota，日前在進行進一步的資安檢測時，發現有兩個配置錯誤的雲端伺服器，造成客戶個資外洩，且時間長達 7 年之久。

這次資安調查與發現是在 Toyota 於 2023 年 5 月發現一台配置錯誤的伺服器洩漏超過 200 萬名客戶所在地資料長達 10 年後，由該公司針對由旗下子公司 Toyota Connected Corporation 管理的雲端環境，進行全面性的深入調查而發現的。

兩台被發現配置錯誤造成資料外洩的雲端伺服器，其中第一台洩漏的是 Toyota 位於亞洲與大洋洲於 2016 年到 2023 年 5 月間的資料；該資料原本只應開放 Toyota 經銷商與服務廠取用，但卻因伺服器配置錯誤而可公開存取；其洩漏的客戶個人資料包括以下欄位：

- 客戶住址；
- 客戶姓名；
- 客戶電話號碼；
- Email；
- 客戶編號；

- 車輛登錄號碼；
- 車輛識別號碼（VIN）。

Toyota 並未對外公布受該伺服器錯誤而遭外洩的受影響客戶人數。

第二台配置錯誤的雲端伺服器，洩露的是約 26 萬名日本 Toyota 客戶車內導航系統的較不敏感資料，包括車內導航裝置的裝置 ID、地圖圖資更新資訊、資料建立日期等；資料外洩期間則自 2015 年 2 月 9 日到 2023 年 5 月 12 日之間。至於受此洩露影響的車輛，以 Toyota 旗下的豪華車品牌 Lexus 為主，受影響車款包括 LS、GS、HS、IS、ISF、ISC、LFA、SC、CT、RX 等。

建議擁有大量客戶與員工個資的中大型企業，對於各種系統的配置與資安防護應更為重視，且定期進行安全測試，並請專業資安團隊進行紅隊入侵測試，以找出弱點予以補強

- 資料來源：
  1. Apology and Notice Concerning Newly Discovered Potential Data Leakage of Customer Information Due to
  2. Toyota finds more misconfigured servers leaking customer info

第 2 章、 國內外重要資安事件

2.1、資安趨勢

零售暨接待服務產業資安調查顯示 91% 業者認為勒贖攻擊是首要威脅

跨國零售暨接待服務產業組織 Retail & Hospitality Information Sharing and Analysis Center（RH-ISAC）日前協同電信業者 Verizon，於 Verizon 日前發表的資安報告 2023 Verizon Data Breach Investigation Report Analysis 中，指出多項該產業的資安現況，包括最常發生的攻擊形態、業者最擔心的資安威脅形式等資訊。

RH-ISAC 針對旗下 242 個來自零售、接待服務與旅宿業者的資安調查，與 2023 Verizon Data Breach Investigation Report Analysis 的廣泛調查結果相比對，得到以下關於該產業資安現況的調查結果：

- 釣魚攻擊、勒贖攻擊、登入資訊竊取等資安攻擊形態，是該產業成員最常發生資安攻擊事件的三大類型；此與 Verizon DBIR 呈現的結果一致；
- 分散式阻斷攻擊（Distributed Denial of Service, DDoS）雖然在 Verizon DBIR 中列為最首要的攻擊型態，但在 RH-ISAC 的調查中並非該產業最常發生的攻擊樣態；
- RH-ISAC 會員在 2022 年針對共用平台上發生的商業電子郵件相關攻擊

（BEC）的討論度有所上升，此與 Verizon DBIR 的調查結果相同；

- RH-ISAC 會員最關切的議題，是針對客戶付款資料的竊取；這也和 Verizon 針對各產業的調查結果一致；
- 高達 91 % 的產業成員最關切勒贖攻擊及其影響；
- 83% 的攻擊源自外部駭侵者；
- 勒贖攻擊佔所有通報資安攻擊的 24%，與先前佔比維持一致；
- 95% 的資安攻擊都有財務誘因；
- 高達 90% 的資安攻擊與 Log4j 漏洞有關。

由於零售、接待服務與旅宿業者手中持有大量客戶相關個資與付款資訊，因此經常成為駭侵攻擊目標。建議相關業者應持續強化資安防護量能。

- 資料來源：

1. 2023 Verizon Data Breach Investigation Report Analysis
2. 2023 Data Breach Investigations Report
3. Industry Insights Report Reveals Top Cyber Threats in the Retail & Hospitality Sector

2.2、新興應用資安

2.2.1、駭侵團體 Lazarus 疑發動 Atomic 錢包竊案，造成 3,500 萬美元損失

區塊鏈金流監控廠商 Elliptic 日前發表研究報告指出，駭侵團體 Lazarus 疑似在近期發動針對 Atomic 錢包的駭侵攻擊行動，竊走高達 3500 萬美元的加密貨幣。

這起針對 Atomic Wallet 發動的攻擊事件發生於 2023 年 6 月初，有許多用戶通報其錢包遭到入侵，存於其中的加密貨幣資金遭竊一空。

加密貨幣分析廠商 ZachXBT 在分析本次攻擊事件時，指出這波攻擊行動總共造成的財務損失，高達 3,500 萬美元，其中單一用戶的最大損失，幾乎佔總體被竊金額的 10%。

Elliptic 的分析則根據多種跡象研判指出，這次攻擊行動的幕後操作者，可能是駭侵團體 Lazarus；這也是該團體在 2023 年犯下的最大金額加密貨幣竊案。

Elliptic 的分析層面包括錢包間的金流流向、洗錢的策略與手法等；這些分析都顯示出與 Lazarus 慣用手法的高度相關。

美國聯邦調查局（Federal Bureau of Investigation, FBI）曾指稱發生於 2022 年 6 月的 Harmony Horizon Bridge 駭侵攻擊事件，也是由 Lazarus 所發

動，當時被竊取的金額高達 1 億美元；而在 2022 年 3 月發生的 Axie Infinity 駭侵攻擊案件，也是由 Lazarus 發動，更造成高達 6.2 億美元的鉅額損失。

資安專家也指出，Lazarus 駭侵團體近年來的攻擊行動，全部精準鎖定各種加密貨幣相關漏洞，主要目的就是竊取大量資金。

建議加密貨幣投資者應妥善保管自己的數位資金，如果資金金額較大，應使用離線的冷錢包儲存，勿儲存於任何線上熱錢包，且應嚴加保管冷錢包的登入資訊與復原密語。

- 資料來源：
  1. North Korea’s Lazarus Group Likely Responsible For $35 Million Atomic Crypto Theft
  2. Lazarus hackers linked to the $35 million Atomic Wallet heist

2.2.2、盜版超級瑪利歐遊戲內含加密貨幣挖礦惡意軟體

資安廠商 Cyble 近日發表資安研究報告，指出該公司旗下的資安研究人員於最近發現一個早在 2003 年就推出的知名老遊戲 Super Mario 3：Mario Forever，近來遭到駭侵者在其安裝程式中植入後門惡意軟體，用於駭侵攻擊之用。

Super Mario 3：Mario Forever 雖然早在 2003 年就在 Windows 平台上推出，但該遊戲的開發廠商 Buziol Games 最近將這個遊戲翻新，推出了新版本，更新遊戲畫面和音效，因此又引發一股熱潮。

Cyble 的資安研究人員指出，駭侵者在多個遊戲相關討論區、社群平台中的社團或各式網路廣告「推廣」這個含有惡意軟體的遊戲，以吸引玩家安裝遊玩。

由 Cyble 資安研究人員截獲的惡意版本 Super Mario 3：Mario Forever，是內含 3 個可執行檔的壓縮檔；除了主程式 super-mario-forever-v720e.exe 是沒有問題的遊戲檔案之外，另兩個分別名為 java.exe 和 atom.exe 的檔案，都含有惡意程式碼。

其中 java.exe 內含的是專門用來挖掘 Monero 加密貨幣的 XMR 惡意軟體；而 atom.exe 則內含一個名為 SupremeBot 的惡意軟體，除了會自我隱藏

外，還會從控制伺服器中下載額外的惡意軟體 Umbral Stealer。

Umbral Stealer 是自 2023 年 4 月起出現在 GitHub 上的開源 C# 資訊竊取惡意軟體，會竊取受害電腦中瀏覽器內儲存的密碼、cookie、工作階段 token、加密貨幣錢包、Discord、Minecraft、Roblox、Telegram 等熱門網站與遊戲的登入認證 token。

建議遊戲愛好者應避免從不明管道下載安裝任何遊戲軟體，對於以「破解版」、「免費暢玩」、「註冊機」為號召的程式更需提高警覺。

- 資料來源：
  1. Trojanized Super Mario Game Installer Spreads SupremeBot Malware
  2. Trojanized Super Mario game used to install Windows malware

2.2.3、全新 macOS 惡意軟體 JokerSpy 攻擊日本加密貨幣交易所

資安廠商 BitDefender 和 Elastic Security Labs 旗下的資安研究人員，最近發現一個全新的 macOS 惡意軟體 JokerSpy，且發現該惡意軟體鎖定日本某家加密貨幣交易所發動攻擊。

資安研究人員指出，該惡意軟體使用一個內含 Mach-O 檔案的 xcc 二進位碼，可同時在 Intel 與 Apple Silicon 處理器架構上運作，而該檔案也會檢查 Mac 電腦中的 TCC 資料庫，以規避系統內建的資安防護措施。

xcc 在執行時會將受害 Mac 的各項系統資訊回傳給駭侵者設立的控制伺服器，並且建立一個以 Python 程式語言撰寫的後門，用以下載後續的惡意程式碼酬載，執行進一步的攻擊。

BitDefender 表示，目前該公司掌握到的 JokerSpy 攻擊案例並不多，但可確定的是，JokerSpy 在今年五月末開始發動第一步的駭侵攻擊，入侵受害者的 Mac 電腦後，於 6 月 1 日起開始載入新的 Python 惡意軟體酬載 Swiftbelt；而 Elastic 掌握到的攻擊活動，則是鎖定日本一家大型加密貨幣交易所。

資安專家指出，目前還不清楚 JokerSpy 的攻擊造成多大程度的影響，但如果第一個案例就是資安防護相對較嚴密的加密貨幣交易所，表示駭侵者在技術的成熟度上不可輕忽。

專家也表示，雖然和 Windows 相比，macOS 因為裝機量較少，使得該作業系統上的惡意軟體較少，但也出現了像 JokerSpy 這樣的 macOS 平台專屬惡意軟體，值得 macOS 使用者注意。

雖然 macOS 普遍擁有較佳的安全性，但使用者仍不可大意，絕對應避免安裝使用來路不明的應用程式，或任意點按不明連結。

- 資料來源：
  1. New mysterious macOS malware infiltrates crypto exchange
  2. Initial research exposing JOKERSPY

2.3、國際政府組織資安資訊

2.3.1、瑞士政府針對進行中的 DDoS 攻擊與資料外洩發出警訊

瑞士政府最近針對一起鎖定 IT 服務商進行的勒贖攻擊發出警訊，指出不僅受攻擊者可能發生資料外洩的風險，更可能遭到 DDoS 攻擊。

瑞士政府於 6 月 6 日發出警訊，表示瑞士政府旗下多個部門，因其 IT 供應商 Xplain 遭到勒贖攻擊，造成多個政府單位的服務受到影響。

Xplain 服務的瑞士政府部門相當廣泛，包括多個部級單位、行政組織與瑞士軍方等。

Xplain 是在今年 5 月 23 日起遭到 Play 勒贖軟體發動攻擊，攻擊者宣稱已經取得 Xplain 內部多種包含隱私、機密資訊、財務、稅收相關的檔案；而在 6 月 1 日時，由於未能順利取得贖款， Play 勒贖團體便對外釋放出所有被竊檔案內容。

瑞士政府指出，正在針對這些遭到外洩的資料進行調查，而攻擊者釋放出來的文件檔案，可能是屬於瑞士聯邦政府部分單位所有。

瑞士政府近日又發表一項資安警訊，指出部分政府入口網站與聯邦行政網站的線上服務，已經因遭到分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）而受到影響。

據報，這次 DDoS 攻擊是駭侵團體「NoName」，該駭侵團體自 2022 年起就針對北大西洋公約組織（NATO）會員國與其在歐洲、烏克蘭、北美設立的各個實體發動各式駭侵攻擊。

瑞士政府表示，在今年 6 月 12 日當天，許多該國聯邦行政單位的網站出現無法存取的問題，經查後證實是遭到 DDoS 攻擊所致。該國現已調派專家進行處理與調查，並將盡速恢復正常服務。

建議各政府單位或公用事業如有使用外包廠商服務，應確實監督並要求廠商加強資安防護，避免機敏資訊外洩。

- 資料來源：
  1. Federal Administration also impacted by Xplain hack
  2. Swiss government warns of ongoing DDoS attacks, data leak

2.3.2、LockBit 勒贖軟體在美國發動 1,700 起攻擊，共勒贖 9,100 萬美元

美國與世界各國的資安主管機關，近期針對惡名昭彰的 LockBit 勒贖攻擊，聯合發表警示報告；報告指出該勒贖軟體自 2020 年起針對美國境內各公私組織，總共發動近 1,700 起勒贖攻擊，所獲的不法勒贖金額合計高達近 9,100 萬美元。

發表這份警示指引的，除了包括美國資安最高主管機關網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）之外，還包括澳大利亞、加拿大、英國、德國、法國與紐西蘭的資安主管機關。

報告指出，光是去年一年之內，針對美國各級政府單位（包括州、地方行政單與各級司法單位）的勒贖攻擊中，有 16% 的攻擊行動是透過 LockBit 來發起。

報告同時指出，自 2020 年 1 月起，駭侵者也利用 LockBit 來攻擊各種領域、不同大小的關鍵基礎設施，例如金融服務、食品與農產、教育、能源、政府單位、緊急服務、醫療、生產製造、交通運輸等領域。

報告中也詳列多達 30 種 LockBit 勒贖駭侵者，在發動攻擊時會使用的免費與開源軟體工具，以及多達 40 種發動攻擊時使用的手段、技巧與程序（tactics, techniques and procedures, TTPs）。

報告同時列舉多個 LockBit 駭侵攻擊時經常使用的各種漏洞之 CVE 編號，以及自 LockBit 於 2019 年 9 月出現以來的演進路線分析。

美國 FBI 建議所有組織應仔細閱讀該報告，並且實作報告中的各種應對指引，以降低遭 LockBit 攻擊的風險與損害。

建議各公私單位皆應參考該報告，找出所有潛在資安弱點予以解決，並依建議加強防護能力。

- 資料來源：
  1. Understanding Ransomware Threat Actors: LockBit
  2. CISA: LockBit ransomware extorted $91 million in 1,700 U.S. attacks

2.3.3、CISA 要求美國政府單位立即修補可能造成間諜軟體攻擊的 iPhone 資安漏洞

美國資安最高主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA）日前通令全美聯邦政府下轄各單位，應即刻修補發生在 iPhone 上的兩個 0-day 資安漏洞 CVE-2023-32434 與 CVE-2023-32435。

這兩個漏洞由資安廠商 Kaspersky 發現，與其相關的攻擊活動命名為「Operation Triangulation」；Kaspersky 是在該公司莫斯科與全球多處辦公室所屬員工持有的 iPhone 上發現該攻擊活動。據報該攻擊活動自 2019 年起就開始進行，且一直持續至今。

Apple 也在上周三緊急發表資安更新，修補包括這兩個 0-day 漏洞在內的多個 iOS 資安漏洞；Apple 也表示已經獲知這兩個漏洞已遭大規模用於針對 iOS 15.7 之前版本的攻擊之上。

受這兩個漏洞影響的 Apple 產品，包括 iPhone 8 和後續機型、iPad Pro（所有機型）、iPad Air（第 3 代）和後續機型、iPad（第 5 代）和後續機型，以及 iPad mini（第 5 代）和後續機型。

CISA 已將這兩個漏洞，連同其他近期發布的多個嚴重漏洞加入其 KEV 名單中，所有美國聯邦政府轄下民事與執行單位，都應在 7 月 4 日前完成修補。

建議建議各公私單位參考 CISA 不定期發布的最新 KEV 名單進行資安修補，以避免遭駭侵者透過已知但未及修補的各式資安漏洞發動攻擊。

- 資料來源：
  1. 關於 iOS 16.5.1 和 iPadOS 16.5.1 的安全性內容
  2. Dissecting TriangleDB, a Triangulation spyware implant
  3. Known Exploited Vulnerabilities Catalog

2.3.4、歐洲刑警組織破獲 EncroChat 加密通訊平台，緝得不法資金 9.8 億美元

歐洲刑警組織（Europol）近日宣布破獲加密行動通訊平台 EncroChat，除使其停止運作外，另也逮捕相關嫌疑人近 6,600 人，緝獲相關不法資金高達 9.8 億美元。

Encrochat 是一個特製的全球行動通訊平台，擁有自行研發的客製化 Android 系統與專屬手機，強調具有強大且無法破解的加密通訊功能、匿名性和不可追蹤性；該服務亦提供可自動刪除的通訊服務、緊急手機清空機制、不受篡改的裝置啟動流程（booting）、抗暴力破解法的 FIPS 140-2 認證硬體加密引擎等，因此受到許多犯罪分子的青睞，許多不法之徒以每半年 1,500 歐元的價格租用該服務，專屬特製手機的售價則為 1,000 歐元，且可遠端清空所有內容。

歐洲刑警組織自 2020 年起發動一場大規模的執法行動，順利破解並潛入 EncroChat 平台之內，自此掌握了該平台上 6 萬名用戶、高達 1.15 億則通訊內容，最後由法國和荷蘭警方協同發動搜捕行動，一共逮捕 6,558 名該平台用戶，其中包括 197 名重要犯罪分子在內。

此外，Europol 根據掌握的通聯記錄內容，一共緝獲多達 270 噸的不法藥物與毒品、971 台各式車輛、271 處地點、923 挺各式武器、68 枚各式爆裂物、40 台飛機、83 艘船隻，以及高達 8.07 億美元現金，並凍結 1.68 億美元

存款。

Europol 指出，多數 EncroChat 的使用者中，有 34.8% 為組織犯罪成員、33.3% 涉及毒品走私，另有 14% 涉及洗錢、11.5% 涉及謀殺、6.4% 涉及武器走私。所有被捕成員遭司法控訴合計的徒刑刑期長達 7,134 年。

- 資料來源：
  1. Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR
  2. EncroChat Bust Leads to 6500 Arrests in Three Years

2.4、社群媒體資安近況

2.4.1、駭侵者假冒加密貨幣新聞記者，盜用社群帳號竊得 300 萬美元

資安廠商 Scam Sniffer 發現一個被稱為「Pink Drainer」的駭侵團體，以假扮為加密貨幣新聞記者的方式，透過釣魚信件盜用受害者的 Discord 與 Twitter 社群媒體帳號，成功竊得近 300 萬美元。

根據 ScamSniffer 的鏈上監機器人觀測到的駭侵活動，Pink Drainer 在這次攻擊行動 中，成功竊得的總金額高達 2,997,307 美元的等值加密貨幣；受害者人數多達 1,932 人，單一受害者最大損失高達 327,000 美元，而遭到攻擊的區塊鏈網路則包括以太坊、Arbitrum、Polygon、BNB 和 Optimism。

資安專家指出，Pink Drainer 主要透過社交工程攻擊來竊取受害者的社群帳號，其手法十分細緻。駭侵者會先假冒為知名加密貨幣相關媒體如 Cointelegraph 與 Decrypt 等旗下的新聞記者，詐稱要對受害者進行專訪；得到受害者的信任之後，駭侵者會要求受害者進行所謂的 KYC（Know Your Customer）認證流程以證實其身分無誤，並將受害者導向用來竊取其 Discord 登入憑證的釣魚頁面。

Pink Drainer 將受害者導入的釣魚頁面中，含有惡意軟體 Carl verification bot，會以「Drag Me」指示，要求受害者將含有惡意 JavaScript 程式碼的按鈕

加入瀏覽器的書籤中，藉以執行程式碼並竊取受害者的 Discord 登入憑證。

如果竊得的 Discord 帳號本身擁有許多追蹤者，駭侵者還會對這些追蹤者發動攻擊，利用假冒的加密貨幣贈與活動、鑄幣活動，或以釣魚網頁等其他詐騙方式，進一步進行詐騙。

建議加密貨幣投資人對於各種不請自來的邀約，包括投資機會、交友、訪問等，均應提高警覺，切勿接受不明邀請、連結與檔案，以免遭駭而蒙受損失。

- 資料來源：
  1. Pink Drainer steals $3M from multiple hack events including OpenAI CTO, Orbiter Finance
  2. Hackers steal $3 million by impersonating crypto news journalists

2.4.2、Reddit 二月攻擊事件駭侵者揚言公布所竊資料

於今年 2 月對美國大型社群討論平台 Reddit 發動攻擊的 BlackCat（ALPHV）勒贖團體，最近揚言要公開當時自該平台竊得的 80 GB 資料。

Reddit 在今年 2 月 9 日對外揭露該平台在 2 月 5 日時遭到駭侵攻擊，遭竊的資料包括各種內部文件、軟體源程式碼、員工資料、部分該平台廣告委刊客戶資料等。

當時 Reddit 在進行內部調查後指出，駭侵者係透過取得僅僅一位員工的內部網路登入資訊，即取得該平台部分內部業務系統、控制面板與部分文件檔案和程式碼的存取權限。

Reddit 在當時否認有任何生產系統遭到駭入，也沒有任何用戶相關個資如密碼、帳號或信用卡資訊外流。

不過在近日，一位資安專家發現 BlackCat（ALPHV）駭侵團體現在宣稱自己就是 Reddit 於 2 月 5 日遭到駭侵攻擊的發動者；該團體宣稱手上掌握的該公司內部檔案與資料多達 80 GB，且曾在 4 月 13 日和 6 月 16 日兩度接觸 Reddit，要求高達 450 萬美元的贖金，但 Reddit 均未回應。

該團體宣稱當時正在等候 Reddit 宣布 IPO（股票首次上市），但近來由於 Reddit 因其公開 API 即將開始收費，造成平台大量用戶與開發者不滿，正在威脅撤離 Reddit，該團體認為這又是威脅 Reddit 支付贖金的好機會，因此

再次威脅公開所竊資料。

建議手上擁有大量用戶個資的平台，針對日益嚴重的勒贖攻擊，應確實加強資安防護能力，特別是以社交工程或釣魚攻擊取得員工持有的系統登入資訊。

- 資料來源：
  1. Hackers breach Reddit to steal source code and internal data
  2. Reddit hackers threaten to leak data stolen in February breach
  3. BlackCat claims they hacked Reddit and will leak the data

2.4.3、駭侵者利用 OnlyFans 成人圖片散布資料竊取惡意軟體

資安廠商 eSentire 發現近來又有駭侵者利用成人社群訂閱制網站 OnlyFans 中的成人內容，來誘使受害者安裝能夠遠端存取的 DcRAT 資料竊取惡意軟體，甚至可用來發動勒贖攻擊。

OnlyFans 是全球知名的訂閱制社群內容創作網站，平台上最大宗的內容是成人限制級影音與文字；過去該平台中的訂戶限定內容，就經常成為各種駭侵者用來吸引受害者的誘餌，因為總有許多人想要免費一探究竟。

eSentire 指出，該公司發現的這波攻擊行動，最早開始於 2023 年 1 月，主要透過各種方式如地下論壇貼文、即時通訊、廣告或假網站等通路，來對受害者聲稱可免費觀賞 OnlyFans 中的付費限制級內容，然後藉機散布一個內含惡意 VBScript 的 zip 壓縮檔。

eSentire 分析該 VBScript，指出其為 2021 年另一場攻擊活動所用 VBScript 的小幅修改版本，在載入受害 Windows 電腦後，最終會注入一個名為 DcRAT 的惡意特洛伊木馬軟體；這是 AsyncRAT 的修改版本，可以在受害的 Windows 電腦上進行鍵盤輸入側錄（keylogging）、監控系統連接的 webcam 畫面、任意存取並變更檔案內容，也可以連上網路並竊取受害者的各種系統登入資訊、瀏覽器 cookie 等。

此外，DcRAT 還可以載入一個勒贖攻擊模組，可將所有非系統檔案全面加密，並加上 .DcRAT 的副檔名。

建議網路使用者應對這類「好康」訊息提高警覺，勿隨意點按不明來源的連結，也不應開啟任何來路不明的檔案。

- 資料來源：
  1. OnlyDcRatFans: Malware Distributed Using Explicit Lures of OnlyFans Pages and Other Adult Content
  2. Hackers use fake OnlyFans pics to drop info-stealing malware

2.5、行動裝置資安訊息

2.5.1、內含間諜軟體 SpinOK 的 Android App 在 Google Play 中下載超過 4 億次

資安廠商 Dr. Web 旗下的研究人員，近日發現一個新的 Android 惡意軟體出現在多個上架於 Google Play Store 的 App 中，合計下載次數超過 4 億次。

這個命名為 SpinOK 的惡意軟體，本身是個廣告 SDK；資安研究人員發現 SpinOK 會以看似無害，每天提供各種獎勵和抽的迷你小遊戲或每日任務來吸引用戶安裝使用，但實際上 SpinOK 會擅自使用用戶 Android 手機裝置上的感測器資料，包括陀螺儀、磁力計，來確認自己不是在沙箱環境內執行，以避免誤入惡意軟體偵測工具布置的「蜜罐」(honeypot）。

一旦確認執行環境「安全」後，SpinOK 就會一邊從伺服器上下載各種小遊戲給用戶玩，一邊掃瞄、搜尋並上傳用戶存於手機資料夾中的檔案，包括用戶的私密照片、影片和文件檔，或是竊取並取代剪貼簿的內容，並上傳到駭侵者設定的伺服器內。

Dr. Web 發現在 Google Play 中一共有 101 個 App 內含 SpinOK，總下載次數合計高達 4.21 億次以上，下載次數最多的 App 包含 Noizz（1 億次）、Zapya（1 億次）、VFly（5000 萬次）、MVBit（5000 萬次）、Biugo（5000

萬次）、Crazy Drop（1000 萬次）、Cashzine（1000 萬次）、Fizzo Novel（1000 萬次）、Cash EM: Get Rewards（500 萬次）、Tick: Watch to earn（500 萬次）。

Google Store 已在 Dr.Web 公開 SpinOK 相關情形前，將包含 SpinOK 的 App 全數下架；必須在確認 App 內不再含有 SpinOK 後才能再次上架。不過目前無法確認各開發者是否知道這些 App 內含 SpinOK。

建議下載過這些 App 的用戶，應立即刪除並進行完整的系統掃毒；此外即使在 Google 官方 Play Store，下載任何 App 前也應先閱讀評價與留言，避免下載可疑 App。

- 資料來源：
  1. Android apps containing SpinOk module with spyware features installed over 421,000,000 times
  2. Android apps with spyware installed 421 million times from Google Play

2.5.2、超過 6 萬種 Android App 內含惡意廣告軟體

羅馬尼亞資安廠商 Bitdefender 日前發表研究報告，指出該公司旗下的資安研究人員，發現過去半年以來，共有超過 60,000 種不重覆的 Android App，表面上看來是正常的手機應用程式，但卻內含惡意廣告軟體。

Bitdefender 指出，該惡意廣告軟體約在 2022 年 10 月開始出現，假扮為各種不同型式的 Android App 吸引用戶下載，類型包括假冒為資安防護軟體、遊戲破解工具、遊戲作弊工具、VPN 連線軟體、Netflix 串流影片觀賞工具、各種第三方網站的原生 App 等等。

Bitdefender 指出，這些內含廣告惡意軟體的 App，並非上架到官方的 Google Play Store，而是在許多第三方網站中，透過 Google Search 來接觸潛在受害者，吸引他們以側載（Sideloading）方式自行安裝 APK 檔，以規避 Google Play Store 的惡意軟體防護機制。

當受害者在其 Android 手機上安裝這些 App 後，不會立即自我設定為自動執行，因為這會需要額外權限；反之，這些 App 會走正常的 Android 軟體安裝流程，然後在安裝完成前要求用戶開啟 App。此外，這些 App 不但沒有圖示，也沒有一般會顯示在圖示下方的 UTF-8 名稱標籤，所以用戶也很難在手機中找到這些惡意 App。之後這些惡意 App 就會在受害者手機上大量顯示蓋版廣告。

據 Bitdefender 指出，這波惡意攻擊主要受害者以美國 Android 用戶為主，比例達 55.27%，其次為南韓（9.8%）、巴西（5.96%）、德國（2.93%）、英國（2.71%）、法國（2.56%）等。

建議 Android 手機用戶不要在 Google Play Store 官方以外的來源安裝任何來路不明的 APK 檔案，以避免安裝到內含惡意軟體的 App。

- 資料來源：
  1. Tens of Thousands of Compromised Android Apps Found by Bitdefender Anomaly Detection Technology
  2. Over 60,000 Android apps secretly installed adware for past six months

2.5.3、Anatsa Android 木馬惡意軟體大規模竊取美英等國使用者銀行資訊

資安廠商 ThreatFabric 旗下的資安研究人員，近日發現一個命名為 Anatsa 的全新 Android 木馬惡意軟體，自今年 3 月起開始攻擊位於美國、英國、德國、奧地利、瑞士等國境內使用者，竊取取銀行相關資訊。

據研究人員指出，這個 Anatsa 木馬軟體藏身在多個於 Google Play Store 中上架的 Android 應用程式內，且總下載安裝次數已超過 30,000 次。

ThreatFabric 指出，這並不是 Anatsa 木馬軟體第一次的活動，先前的攻擊活動發生自 2021 年 11 月，當時有超過 300,000 萬次下載安裝次數。

該公司於 2023 年 3 月偵測到 Anatsa 開始再次活動，與前一次 Anatsa 的活動相同，木馬惡意程式都藏身在如 PDF 檢視編輯工具等辦公室應用與生產力工具類的 App 內，且當 ThreatFabric 通報 Google 並由 Google 將惡意 App 自 Google Play Store 中下架後，駭侵者總能很快再上架新的惡意 App 到 Google Play Store 中。

另一方面，ThreatFabric 也說，上架到 Google Play Store 的軟體，原先都不含惡意程式碼，以逃避 Google 的上架審查；但在使用者安裝到手機中後，便會更新並載入惡意程式碼。

ThreatFabirc 指出，在這次的攻擊行動中，Anatsa 會竊取多達十多家銀行與網路券商的金融相關資訊，包括登入帳號密碼、信用卡詳細資訊、付款資訊等，而竊取手法包括利用釣魚網頁畫面覆疊等。

建議 Android 用戶即使在 Google 官方 Play Store，於下載應用程式前也應仔細閱讀用戶評價，且如果 App 要求多種顯非必要的存取權限，應立即關閉並移除該 App。

- 資料來源：
  1. Anatsa banking Trojan hits UK, US and DACH with new campaign
  2. Anatsa Android trojan now steals banking info from users in US, UK

2.6、軟體系統資安議題

紐約市近 45,000 名學生個資因 MOVEit 資安漏洞而遭外洩

美國紐約市教育局（New York City Department of Education, NYC DOE）日前指出，有駭侵者透過 MOVEit 資安漏洞入侵該局一台伺服器，竊取多達 45,000 學生的個人機敏資訊。

NYC DOE 指出，這 45,000 名學生的資料，係在伺服器間轉檔的過程中，遭到駭侵者利用 CVE-2023-34362 MOVEit 漏洞竊得。雖然 NYC DOE 在該漏洞公開後立即予以修補，但駭侵者是在該漏洞仍為 0-day 漏洞期間就利用該漏洞竊得資料。

NYC DOE 表示，目前正在與紐約市資安相關單位合作調查本次個資外洩事件；就目前掌握的資訊來看，遭到不當存取的伺服器中文件約有 19,000 筆，除了有 45,000 名學生的個資遭到外洩，另有若干 DOE 員工和相關服務廠商人員的資料也遭到竊取。

NYC DOE 說，受此次駭侵攻擊影響而外洩的資料類型，包括社會福利號碼（Social Security Number）和員工編號等。NYC DOE 也說，由於 MOVEit 漏洞的影響和攻擊活動相當廣泛，目前美國聯邦調查局（Federal Bureau of Investigation）正在擴大偵辦。

據資安專家指出，Clop 勒贖團體已開始利用藉由 MOVEit 漏洞攻擊所取得的資料，對多個對象進行勒贖要脅；受到該團體勒贖的單位，包括殼牌石油（Shell）、喬治亞大學（University of Georgia）、喬治亞大學系統（University System of Georgia）、Heidelberger Druck、聯合健診學生資源（UnitedHealthcare Student Resources）等公私單位在內。

建議各公私單位應立即修補 MOVEit（CVE-2023-34362）漏洞，並調查在漏洞修補之前是否發生入侵事件，以了解資料是否遭竊並予以應對。

- 資料來源：
  1. Alert Regarding Data Incident
  2. Hackers steal data of 45,000 New York City students in MOVEit breach

2.7、軟硬體漏洞資訊

Microsoft 推出 2023 年 6 月 Patch Tuesday 每月例行更新修補包

Microsoft 日前推出 2023 年 6 月例行資安更新修補包「Patch Tuesday」，共修復 78 個資安漏洞；特別的是其中含有 38 個屬於遠端執行任意程式碼（RCE）的漏洞。

本月 Patch Tuesday 修復的漏洞數量有 78 個，較上個月（2023 年 5 月）的 38 個資安漏洞增加許多；而在這 78 個漏洞中有多達 38 個屬於遠端執行任意程式碼類型，其中有 6 個的危險程度評級達到「嚴重」等級（Critical）。

這次的 Patch Tuesday 也是自 2022 年 3 月以來，首次沒有任何 0-day 漏洞的例行性更新。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：17 個；
- 資安防護功能略過漏洞：3 個；
- 遠端執行任意程式碼漏洞：32 個；
- 資訊洩露漏洞：5 個；
- 服務阻斷（Denial of Service）漏洞：10 個；

- 假冒詐騙漏洞：10 個；
- Edge -Chromium 漏洞：1 個。

雖然本月的 Patch Tuesday 沒有任何已遭大規模濫用的 0-day 漏洞，但仍有幾個值得用戶注意，可能已遭駭侵者用於攻擊的漏洞如下：

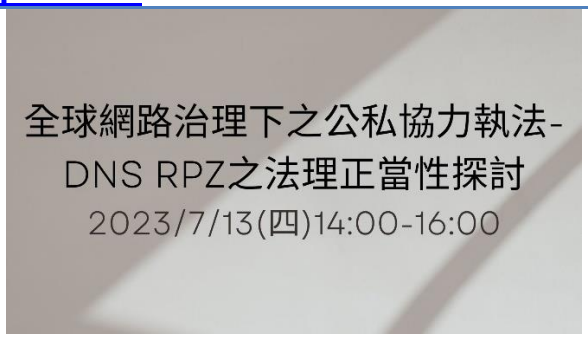
第一個是 CVE 編號為 CVE-2023-29357 的 Microsoft SharePoint Server 權限提升漏洞；該漏洞存於 Microsoft SharePoint 之中，可讓駭侵者將自身執行權限提升到任何用戶等級，包括管理員等級在內。

第二個值得注意的漏洞是 CVE-2023-32031，是存於 Microsoft Exchange Server 中的遠端執行任意程式碼漏洞。

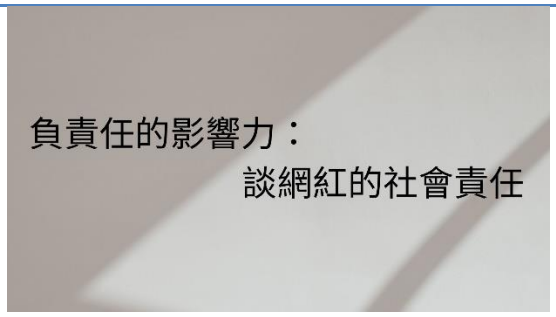
- CVE 編號：CVE-2023-29357、CVE-2023-32031 等
- 影響產品(版本)：Microsoft 旗下多種軟體，包括 Windows、Office、Exchange 等。
- 解決方案：建議系統管理者與 Microsoft 用戶應立即依照指示，盡速套用 Patch Tuesday 與不定期發表的資安更新，以避免駭侵者利用未及更新的漏洞發動攻擊。

- 資料來源：
  1. Microsoft SharePoint Server Elevation of Privilege Vulnerability
  2. Microsoft Exchange Server Remote Code Execution Vulnerability
  3. Microsoft June 2023 Patch Tuesday fixes 78 flaws, 38 RCE bugs

第 3 章、 資安研討會及活動

全球網路治理下之公私協力執法-DNS RPZ 之法理正當性探討	
活動時間	**2023 年 7 月 13 日(四)14:00-16:00**
活動地點	**張榮發國際會議中心 703 會議廳(台北市中正區中山南路 11 號)/網路同步**
活動網站	**https://www.twtechlaw.org.tw/webpage/conference_content.php?CONF_ID=329&conf_type=active**
活動概要	 **主辦單位：財團法人台灣網路資訊中心、國立陽明交通大學科技法律學院、台灣科技法學會** 活動方式：台北實體班 / 網路同步班(線上聽講，自行準備電腦、筆電、手機、PAD 等，連上網路即可觀看) 內容說明： 主持人 / 國立陽明交通大學科技法律學院 陳銘雄院長 =>DNS RPZ 之執行現況以及實際需求 主講人 / 黃勝雄執行長 =>DNS RPZ 相關措施之法律性質 主講人 / 蔡志宏庭長 =>令狀原則及其例外於 DNS RPZ 之應用 =>各類行政執法與 DNS RPZ

	財團法人台灣網路資訊中心 黃勝雄執行長 台灣士林地方法院 蔡志宏庭長(台灣網路治理論壇理事) 台灣嘉義地方檢察署 陳昱奉檢察官(查緝詐欺及資通犯罪督導中心專案檢察官) 內政部刑事警察局科技研發科 莊明雄代理科長 司改會民間 e-ID 律團召集人/執行委員 林煜騰律師 報名日期：2023 年 06 月 27 日(二) ~ 2023 年 07 月 11 日(二) 參加對象說明：社會大眾

負責任的影響力：談網紅的社會責任	
活動時間	**2023 年 07 月 14 日(五) , 14:00-16:00**
活動地點	**IEAT 國際會議中心 8 樓綜合教室/Webex 會議室** ******本活動採實體與線上同步進行******
活動網站	**https://www.twsig.tw/20230714/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 按讚、訂閱、開啟小鈴鐺並定期收看（聽），也許再 donate 一下，似乎已成為許多人生活的日常。我們從泛稱為「網紅」的部落客、YouTuber、IG 紅人、Tik Toker、Podcaster 身上，獲得遊戲攻略，了解世界大事、投資理財重點；又或學習語言、彩妝與穿搭，也經常依其建議決定買下某個推薦的某個昂貴 3C 產品或育兒用品，並認同他們對爭議性話題的個人看法。特別是數位原生族群的 Z 世代，他們越來越著迷於在社群平台上分享自己或觀看他人的故事，也更願意支持或追隨網紅，並將網紅視為重要的資訊來源。收看網紅的內容，似乎比看電視影集還更稀鬆平常。 也因此，當國內出現某些網紅賣假貨、揹著嬰兒滑雪為代言產品、大鬧超商或北歐家具店、推銷醫療產品、散播陰謀論等狀況時，網友們撻伐的音量也不小，要求這些具有影響力的網紅們注意自己的言行，也應該要為自己的影響力負起一定的社會責任。

美國聯邦貿易委員會 (FTC) 和廣告標準局，以及英國的競爭和市場管理局 (CMA) 已制定有關網紅應該在其貼文中誠實揭露其與品牌間關係的規則；法國也出現由廣告機構所發展的「負責任的影響力證書」（Responsible Influence Certificate），發給在廣告透明度滿足特定要求的網紅，據報導，在問世 18 個月內，這張證書已發出 150 張，且還有越來越多的品牌，會將該證書列為選擇合作網紅之必要條件。

本場講堂活動邀請到國內專家及網紅，探討建構負責任的影響力的方式，又，在整個網紅社群媒體的生態系統中，包括網紅、廣告主、平臺業者、甚至是廣大網友在內的不同利害關係人，又應該扮演妥自己的角色？

議程

14:00-14:05 活動介紹

14:05-15:45 焦點座談

主持人 - 劉昱均 執行秘書 (iWIN 網路內容防護機構)

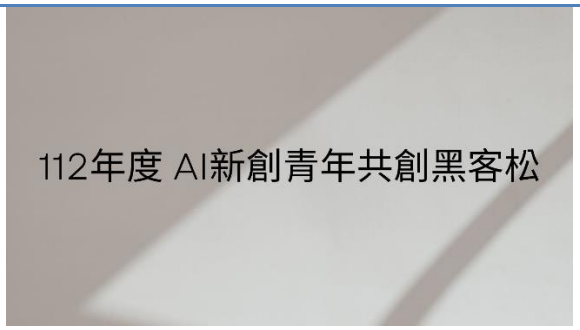
與談人 -

張裕昌 總經理 (世紀奧美公關顧問)

其它與談代表-邀約中

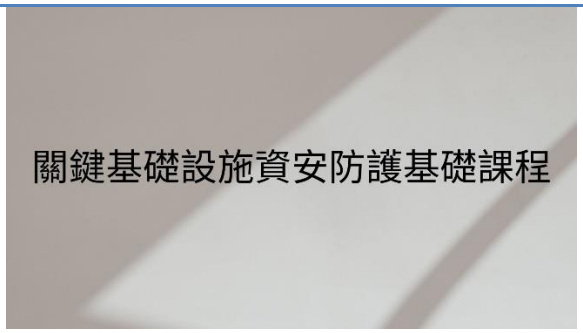
(依姓名筆劃順序排列)

15:45-16:00 現場問答

112 年度 AI 新創青年共創黑客松	
活動時間	**2023/08/01 00:00 ~ 2023/08/31 23:59**
活動地點	**線上活動**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2145**
活動概要	 **主辦單位：數位發展部數位產業署** 活動內容 / Event Details： AI 新創青年共創黑客松透過工作坊促成參賽團隊與新創攜手合作，提出具可行性、實用性、創新性、完整性、社會影響力等的解決方案，對接產業及社會需求，並透過專家審查，遴選出 15 組進入成果發表會之參賽團隊，向投資者、產業界及學術界人士和與會來賓展示黑客松的解決方案和產品，並評估每項解決方案之優缺點以及市場潛力；藉由開發者與產業人士交流與評估過程，有助於深入解決方案，並且也能夠讓產品開發者了解市場反饋和需求。 盼透過本計畫，促進青年學子提出能實際解決市場及社會需求之 AI 應用解決方案，有效培育 AI 種子人才！ 活動聯絡人 / Contact Us： Tiffany Gao　tiffanygao@nycu.edu.tw　02-25700363

InfoSec Taiwan 2023 國際資安組織大會	
活動時間	**2023/08/01(周二) 09:00 ~ 2023/08/03(周四) 18:00**
活動地點	**台北文創大樓 6 樓 / 110 台北市信義區菸廠路 88 號**
活動網站	**https://csa.kktix.cc/events/infosectaiwan2023**
活動概要	 **主辦單位：TWCSA** 智慧聯網的時代來臨，許多應用都與資訊安全相關，2020 年更因 COVID-19 影響，資安議題需求持續增加，歷經 COVID-19，大家改變了學習方式和生活購物的模式，因此近來幾次大型網路攻擊事件，不論國內外都引起了許多人的憂心，不論是近來經常發生的勒索攻擊威脅，或是網站遭到資料的竊取，這些都已成為全球性的資安問題，如何因應新興的資安問題所帶來的資安風險，成為我們所關注的重要話題。疫情、氣候變遷更是加速了各國推動 ESG 的發展，美國道瓊永續指數從 2018 年開始已經把許多資訊安全相關內容都納入企業要求，以強化 ESG 在風險管控的完整性。資訊安全將是台灣與全球都需要面對的課題與挑戰！ 國際資訊安全組織台灣高峰會，由台灣數位安全聯盟主辦，同步接軌 Cloud Security Alliance、The Honeynet Project 與 OWASP 等國際資訊安全組織最新研究成果，透過國際資安社群有助於掌握全球發展趨勢，高峰會可協助與會人員掌握全球資訊安全發展趨勢與產業脈動，內容涵蓋雲端服務安全、誘捕欺敵資安技術、網站應用程式安全、事

	件掌握與應變、企業安全防禦等重要議題。 高峰會：由「OWASP AppSec Taiwan 2023」、「HoneyCon 2023 台灣誘捕網路技術研討會」以及「CSA Taiwan Summit 2023 雲端安全聯盟台灣年會」聯合高峰會議，Full Pass 高峰聯票可參與 8/2-3 兩日會議。 Full Pass 高峰聯票含：「大會手冊、高峰會議包、餐點、高峰會抽獎資格、講師簡報檔」。 8/1 Workshop 實作課程：依課程需求選擇，為確保上課品質，每堂課程皆有人數上限，名額已滿之課程將不再開放報名。 協辦單位、活動推廣和媒體採訪須使用優惠代碼購買。

關鍵基礎設施資安防護基礎課程	
活動時間	**第一梯次：2023/8/3 13:00-16:00** **第二梯次：2023/8/11 13:00-16:00**
活動地點	**臺南市歸仁區歸仁十三路一段 6 號(沙崙資安服務基地 1 樓：攻防教室)**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2129**
活動概要	 **主辦單位：數位發展部數位產業署** 活動內容 / Event Details： 【關鍵基礎設施資安防護基礎課程】招生囉～ 駭客威脅持續猖獗，多數 OT 組織仍成網路犯罪者重點攻擊目標，資安風險與威脅更甚以往！ 名額有限～還不加緊腳步來報名！「關鍵基礎設施資安防護基礎課程」將是你提升工控資安意識最好的機會！ 我們將結合沙崙資安服務基地工控實測場域，針對油、水、電相關關鍵基礎設施系統操作從業人員、資安服務相關從業人員，探討工業控制系統並說明工控系統可能入侵到 OT(營運技術)網段之管道，也配合資安處的法規要求，設計場域訓練稽核，以評估控制系統的資安等級及討論資安防護措施，以提升業者實務防護能力！ 課程對象：油、水、電相關關鍵基礎設施系統操作從業人員、資安服

	務相關從業人員 課程大綱： 1. 工控系統資安環境認知說明 2. 資安防護基準與防護措施說明 3. 工控系統基礎和測試平台介紹 含石化(Emerson DCS)/天然氣(三菱 PLC+SCADA)/電驛系統(SEL, ABB and ARCTEQ)資安攻防實機展演 主辦單位保有開課與否及課程內容調整之權利。 活動聯絡人 / Contact Us：李小姐　doralee@iii.org.tw　02-6607-3299

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布之資安漏洞資訊如下表：

Openfind Mail2000 - XSS (Reflected Cross-site scripting)	
TVN / CVE ID	TVN-202306001 / CVE-2023-28705
CVSS	5.4 (Medium)
影響產品	Openfind Mail2000 V7(含)以前版本
問題描述	Openfind Mail2000 未過濾信件內容中的特殊字元，遠端攻擊者可利用此漏洞，以帶有注入 JavaScript 語法之惡意網頁的釣魚郵件進行攻擊。導致一般使用者進入系統開啟郵件後，觸發 XSS (Reflected Cross-site scripting)攻擊。
解決方法	Update Openfind Mail2000 version to V8
公開日期	2023-06-09
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7158-751a6-3.html**

L7 Networks InstantScan & InstantQoS - Arbitrary File Upload	
TVN / CVE ID	TVN-202306002 / CVE-2023-32752
CVSS	9.8 (Critical)
影響產品	L7 Networks InstantScan IS-8000 & InstantQoS IQ-8000
問題描述	InstantScan 和 InstantQoS 網頁介面之上傳功能未對上傳檔案進行檢查限制，導致遠端攻擊者不須權限，可以利用此漏洞上傳任意檔案，進而執行任意程式碼控制伺服器。
解決方法	聯繫 L7 Networks 進行漏洞修補
公開日期	2023-06-16
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7159-d1383-3.html**

沛盛資訊 OMICARD EDM - Arbitrary File Upload	
TVN / CVE ID	TVN-202306003 / CVE-2023-32753
CVSS	9.8 (Critical)
影響產品	聯繫沛盛資訊詢問受影響版本
問題描述	沛盛資訊 OMICARD EDM 行銷發送系統檔案上傳功能未對上傳檔案進行檢查限制，導致遠端攻擊者不須權限，即可利用此漏洞上傳任意檔案，進而執行任意程式碼或中斷系統服務。
解決方法	聯繫沛盛資訊詢問相關修補建議
公開日期	2023-06-16
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7160-20ac9-3.html

思考軟體科技 Efence - SQL injection	
TVN / CVE ID	TVN-202306004 / CVE-2023-32754
CVSS	9.8 (Critical)
影響產品	思考軟體科技 Efence 1.2.59 DB.ver 36
問題描述	Efence 之登入功能未對使用者輸入的參數進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	Update Efence version to 1.2.59 DB.ver 41
公開日期	2023-06-16
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7161-3e7c9-3.html

第 5 章、 2023 年 6 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

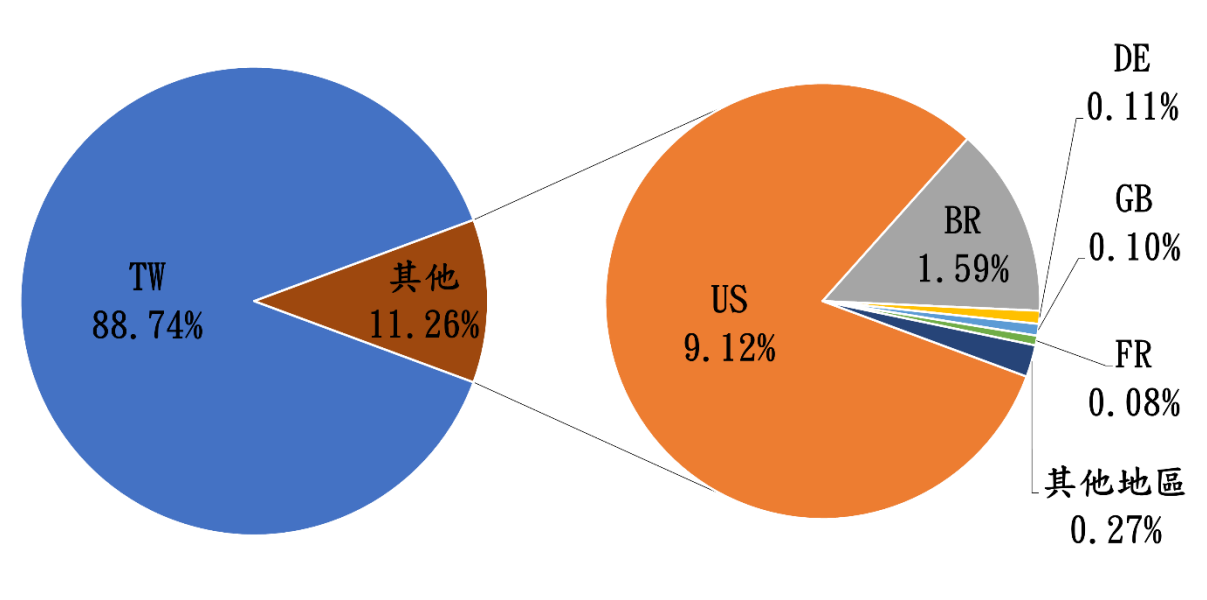


圖 1、分享地區統計圖

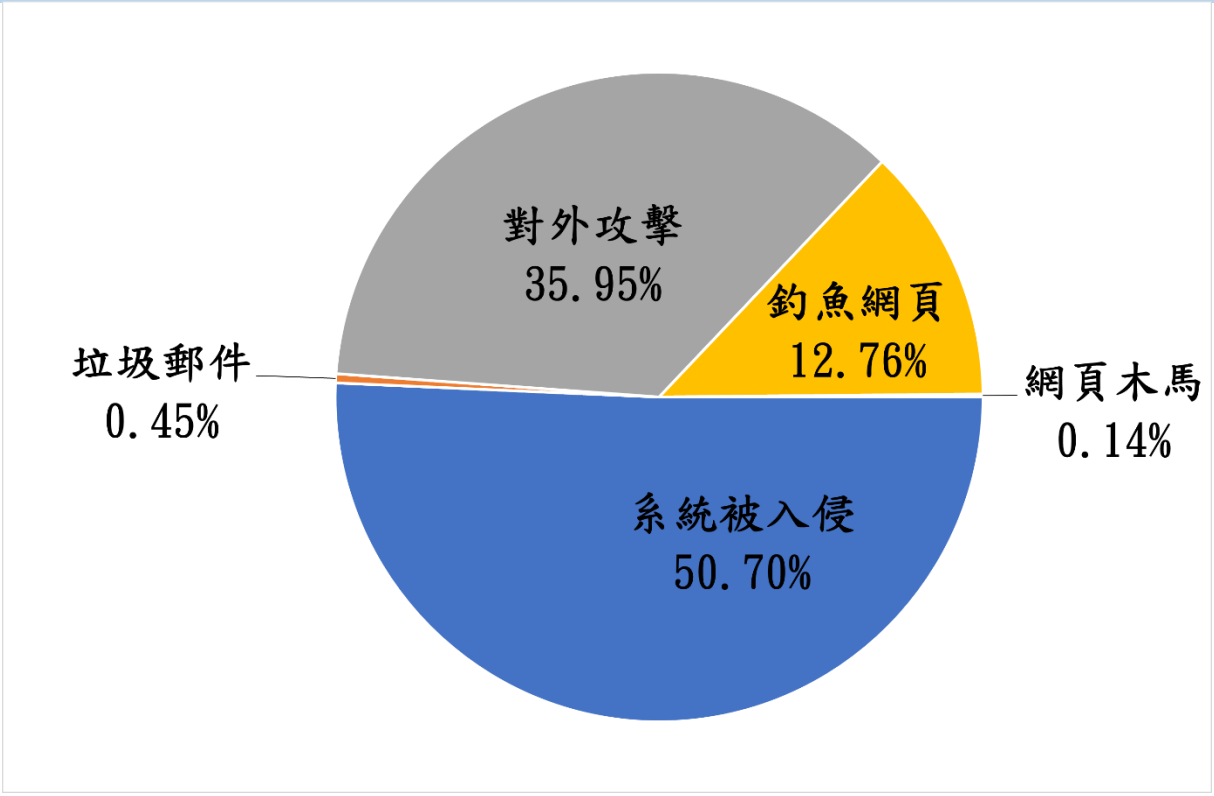


圖 2、分享類型統計圖

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：**2023 年 7 月 10 日**

編輯：**TWCERT/CC 團隊**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

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

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

Twitter：**@TWCERTCC**