TWCERT/CC 資安情資電子報

2023 年 6 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) 平台之漏洞嚴重程度前五的產品漏洞資訊。

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

烏克蘭政府單位遭駭侵者以假冒 Windows Update 指南發動攻擊

烏克蘭電腦緊急應變團隊（Computer Emergency Response Team of Ukraine，CERT-UA）指出，APT 28 （又名 Fancy Bear）駭侵團體近日以偽造的 Windows Update 資安更新指南惡意郵件，大規模攻擊烏克蘭政府各單位。

CERT-UA 指出，APT 28 的駭侵者，以真實人名加上「@outlook.com」結尾的 email 信箱，偽裝為系統管理員，向烏克蘭多個攻擊目標的政府實體人員發送假冒的 Windows Update 更新指南，以魚目混珠的方式來欺騙攻擊對象，使其誤信而感染惡意軟體。

在這些偽造的升級指南中，沒有採取一般常用的方式，亦即透過 Windows 系統內建的升級機制，而是要求使用者執行某些 PowerShell 指令；一但受害者照做，該指令就會下載一個攻擊用的 PowerShell 指令檔，一邊模擬出一個偽造的 Windows Update 更新進度視窗，一邊下載另一個含有惡意指令的 PowerShell 指令檔，使 APT 28 駭侵者得以透過 Mocky service API 竊取受害電腦系統中的機敏資訊。

CERT-UA 建議烏克蘭各政府系統管理者，應加強限制關鍵設備與伺服器主機執行 PowerShell 指令，並強化對於 Mocky API 的監控，以避免機敏資訊遭竊。

另一方面，根據 Google Threat Analysis Group 先前的報告，在 2023 年第一季所有針對烏克蘭發動的攻擊用釣魚郵件中，有 60% 以上來自俄羅斯駭侵團體，而 APT 28 更是其中一大來源。

建議機敏關鍵設備與伺服器的系統管理者，應對 PowerShell 指令的執行加以嚴格限制，並且隨時監控系統各項連外 API 的使用情形，以避免遭到駭侵者竊取資料。

- 資料來源：
  1. Кібератака групи APT28: розповсюдження електронних листів з "інструкціями" щодо "оновлення операційн
  2. Hackers use fake ‘Windows Update’ guides to target Ukrainian govt
  3. Ukraine remains Russia’s biggest cyber focus in 2023

第 2 章、 國內外重要資安事件

2.1、資安趨勢

調查指出多數公司不夠重視資安，將造成嚴重後果

一項由資安廠商 Delinea 針對多國共 2,000 名企業資安技術決策者進行的調查指出，多數公司對於資安的認知與投入相當不足，恐將造成嚴重後果。

這項調查針對位於澳洲、紐西蘭、新加坡、馬來西亞、印度、台灣、香港的 2,000 名企業資安決策人員進行問卷調查，發現多數企業並未將資安視為公司業務策略的一部分。

調查指出，這些企業資安決策人員中，只有 39% 認為所屬公司的領導階層，將資安視為強化公司業務的一環；有 36% 的公司更是只在監管與法規要求之下，才會認真考慮資安。也有 17% 的公司完全不認為資安是該公司的工作重點。

調查也說，雖然有 54% 的公司設有專責資安人員，但只有 48% 的公司會將資安政策與作為以文件方式明文規範，也有 33% 的公司只有在發生資安事件時才會以書面方式進行資安作為與政策的溝通。

對公司內從事資安工作的人員來說，這樣的情況也造成衝擊；有 31% 受訪者表示其資安團隊承受極大的工作壓力，而在近年來全球經濟發展不確定性提高的情況下，有 48% 的受訪者表示，要將資安與公司的發展重點相互結合，也變得更不容易。

由於多數公司對資安的不夠重視，因此導致 35% 公司延遲在資安人員與軟硬體設備方面的投資、34% 公司發生資安策略決策的延遲，更有 27% 公司因而增加了非必要的費用。有 89% 的企業因而發生了資安負面事件，也有 26% 公司遭到更為嚴重的駭侵攻擊。

建議各公司的決策階層人員，能夠更加理解資安和企業業務發展方向結合的重要性，才能有效降低企業面臨的資安風險，避免發生重大資安事件與損失。

- 資料來源：
  1. Cybersecurity often overlooked by business leaders: Delinea
  2. Most firms aren't taking cybersecurity seriously enough - and it could come back to haunt them

2.2、新興應用資安

2.2.1、全新 macOS 惡意軟體 Atomic 竊取 50 種加密貨幣錢包內的數位資產

資安廠商 Trellix 和 Cyble Labs 旗下的資安研究人員，近日發現一個全新 macOS 惡意軟體，稱為 Atomic；該惡意軟體的開發者透過 Telegram 「廉價出租」，供有意使用的駭侵者透過網路散布，以竊取受害者 Mac 電腦內 50 種以上加密貨幣錢包內的數位資產。

據研究報告指出，Atomic 是一種以 Go 開發的 64 位元 macOS 惡意軟體，內含一個易於使用的 web 管理介面，以便於駭侵者「管理」受害者；而其軟體本身也包括 MetaMask 加密錢包的暴力試誤功能、加密貨幣檢查器、DMG 安裝程式介面，並接收放在 Telegram 頻道中的竊取記錄。

研究人員發現 Atomic 的最近版本為 2023 年 4 月 25 日，改版相當活躍，推論這是一個仍在研究開發中的持續性駭侵計畫；該惡意 DMG 檔案也幾乎無法被 VirusTotal 偵測出來；研究人員以 59 種不同的防毒防駭引擎測試，只有一種能夠偵測到 Atomic 的存在。

使用者一旦感染 Atomic，該軟體會先顯示一個假的互動視窗，以騙得使用者輸入的 macOS 系統密碼，取得系統密碼後，Atomic 即可提升自身的執行

權限，以進行進一步的駭侵攻擊活動。接著 Atomic 會試圖讀取 macOS 系統中用以儲存各種密碼的 KeyChain Access，以取得各種機敏資訊，包括如 Electrum、Binance、Exodus、Atomic 等軟體加密貨幣錢包密碼，以及如 MetaMask、Trust Wallet、Jaxx Liberty、Binance Chain 等瀏覽器擴充套件形態的加密貨幣錢包密碼，以及如 Chrome、Firefox、Edge 等瀏覽器本身儲存工的密碼、信用卡資訊，以及電腦本身的各種系統資訊。

建議不論是何種作業系統使用者，要下載任何軟體，均應透過合法可信賴的管道下載，勿於即時通訊、網路論壇、內容農場等危險來源下載安裝任何軟體。

- 資料來源：
  1. PhD. Phuc @phd_phuc
  2. Threat Actor Selling New Atomic macOS (AMOS) Stealer on Telegram
  3. New Atomic macOS info-stealing malware targets 50 crypto wallets

2.2.2、加密貨幣釣魚「服務」Inferno Drainer 已成功詐騙近五千名受害者

資安廠商 Scam Sniffer 日前發表資安研究報告，指出該公司的研究人員發現一個用來提供加密貨幣釣魚詐騙「服務」的平台 Inferno Drainer；該平台自今年三月底至今已有近 5000 名受害者，詐騙金額超過 590 萬美元。

據 Scam Sniffer 指出，詐騙者自 2023 年 3 月 27 日開始，至少已經利用該平台架設多達 689 個詐騙網站；這些詐騙網站假冒的加密貨幣產業相關知名品牌，數量多達 229 個，其中包括 MetaMask、OpenSea、Collab.Land、LayerZero Labs 等。

這批詐騙網站絕大部分都在今年 5 月 14 日後才上線運作，但已經造成相當規模的損失。Scam Sniffer 的資安研究人員，曾在 Telegram 上看到 Inferno Drainer 的成員展示一張成功詐騙取得 103,000 美元的螢幕截圖，用來強調其詐騙得逞的能力。

該平台稱提供多種加密貨幣詐騙方式，並以此為招徠；這些詐騙方式包括多鏈詐騙（Multichain Fraud）、Aave 代幣與 Art Blocks 耗盡攻擊、MetaMask 代幣核准漏洞攻擊等等。該平台也具備十分現代後的操作後台，甚至還提供免費試用。

該平台向有意使用的駭侵者收取至少 20% 的不法所得；如果需要代客架設詐騙網站，收費則為 30%。

Scam Sniffer 統計自該平台開始運作後的損失，絕大多數的數位資產損失來自以太坊主網（Mainnet），高達 430 萬美元，其餘為 Arbitrum（79 萬美元）、Polygon（41 萬美元）、BNB（39 萬美元），合計高達 590 萬美元。其中單一攻擊損失的最高金額為 40 萬美元。

建議加密貨幣投資人對於各種可疑或利潤明顯不合理的投資機會，必須提高警覺，切勿點按不明連結、安裝不明軟體，也不要將數位錢包的復原短語交付給任何人。

- 資料來源：
  1. $5.9 Million Stolen By Scam as a Service Provider Called Inferno Drainer
  2. Crypto phishing service Inferno Drainer defrauds thousands of victims

2.2.3、Jimbos Protocol 遭閃電貸攻擊，損失超過 750 萬美元

一個架構於 Arbitrum 區塊鏈上的去中心化金融（Decentralized Finance, DeFi）服務專案 Jimbos Protocol，近期遭到駭侵者以「閃電貸」（Flash Loan）攻擊得逞，損失的數位資金高達 4,000 枚以上以太幣，換算超過 750 萬美元。

營運 Jimbos Protocol 的公司在日前於 Twitter 上公開發表遭駭侵攻擊的消息，並表示已向司法單位報案，並已與資安專家合作，以期找出問題並加以解決。

該攻擊發生在 Jimbos Protocol 推出第二版後僅僅 3 天，許多投資人購買了其推出的 Jimbo Token 代幣之後；駭侵者成功竊得的數位資金，高達 4,090 枚以太幣。

雖然 Jimbo Token 具備一種半穩定地板價機制，可由其儲備的其他數位資產與其他機制，來試圖穩定幣價，但在 Jimbos Protocol 遭到駭侵攻擊一事傳出之後，該幣的價格立即暴跌，由原本的一枚 0.238 美元狂跌到僅有 0.0001 美元。

據區塊鏈資安專家指出，由於 Jimbos Protocol 平台缺少「滑點控制」（Slippage control）機制，因此遭到駭侵者以此發動「閃電貸」(Flash Loan）

攻擊，其方法是重覆利用閃電貸，以極快的速度，在同一筆交易中同時借出並償還大量資金，並利用該漏洞來不斷賺取借還之間的價差。

這種利用閃電貸來快速賺取價差的攻擊，過去也頻繁發生在其他 DeFi 平台上過；其中一個比較知名的案例，是發生在 Euler Finnace DeFi 專案的閃電貸攻擊事件，當時的損失高達 1.97 億美元。

建議加密貨幣投資人在選擇投資標的時，應注意該專案的資安是否經過知名第三方資安廠商稽核，且設有投資人保障基金，且應避免高風險的目標。

- 資料來源：
  1. Jimbos Protocol (v2, soon) @jimbosprotocol
  2. Flash loan attack on Jimbos Protocol steals over $7.5 million

2.3、國際政府組織資安資訊

2.3.1、西班牙警方破獲釣魚攻擊犯罪集團，共逮捕 40 人

西班牙警方日前破獲一個金融釣魚攻擊犯罪集團，一共逮捕包括駭侵者和其他協助犯罪者等 40 名不法分子；該犯罪集團的不法獲利所得高達 70 萬歐元，受害者超過 30 萬人。

西班牙警方表示，這個名為「Trintarios」的犯罪集團，主要在馬德里與塞維利亞（Seville）兩大城市進行犯罪活動，以釣魚簡訊與釣魚郵件為工具，針對進行金融詐騙攻擊，竊取受害者的信用卡資訊，用以購買加密貨幣，再換為法定貨幣以獲取不法利益。

警方說，遭到逮捕的 40 人，將遭到下列罪名起訴，包括組織犯罪、銀行詐騙、偽造文書、冒用他人身分、洗錢等。

駭侵者透過假冒為銀行的詐騙簡訊，謊稱受害者的信用卡遭到盜刷，或是銀行帳戶遭到冒領，需要受害者使用簡訊中提供的釣魚網頁連結，提供正確的信用卡或帳戶相關資訊，藉以竊取受害者的金融服務登入資訊、各種個資等機敏資訊。

駭侵者也透過釣魚機制的儀表板，在取得受害者的金融服務登入資訊和各種個資後，立即以竊得的資訊來申請貸款，並將受害者的信用卡與其控制

的加密貨幣錢包連結，以便盜刷並購買加密貨幣。

警方也說，該犯罪集團也透過多種方式進行洗錢，例如僱用人頭戶來收取銀行轉帳、以 ATM 提款，並以虛設行號的 POS 系統偽造交易等方式洗錢。竊得的資金則用來購置該犯罪集團使用的毒品、槍械武器、資助遭到拘押的該集團成員，其餘款項則匯出到多明尼加共和國，供該集團分子在該國購置房地產。

西班牙警方表示，目前除了繼續追緝可能的在逃分子之外，也積極與國際檢警單位合作，盡一切努力以追回贓款。

建議用戶如接獲宣稱銀行或信用卡因盜刷遭停用的簡訊或 Email，切勿點按其中的連結，或開啟附件；應立即與相關銀行聯絡確認。

- 資料來源：
  1. La Policía Nacional desmantela la estructura de financiación de los Trinitarios con la que defraudar
  2. Spanish police dismantle phishing operation linked to crime ring

2.3.2、美國資安主管機關警示：政府單位應檢視是否因 Barracuda 0-day 漏洞而遭攻擊

美國資安主管機關網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），日前發表資安警訊，要求美國聯邦政府旗下單位立即檢視並調查是否因 Barracuda 日前修補的 0-day 漏洞遭駭侵攻擊。

該 0-day 漏洞的 CVE 編號為 CVE-2023-2868，發生在 Barracuda Email Security Gateway 應用程式中，該產品廣為全球 200,000 個公私單位採用，包括大型企業如 Samsung、Mitsubishi、Kraft Heinz、Delta Airlines 以及各國政府機構。

據 CISA 指出，該漏洞已遭駭侵者廣泛利用於攻擊，因此 CISA 除將此 0-day 漏洞列入其指定資安漏洞列表之外，也要求美國聯邦政府各民事執行單位（Federal Civilian Executive Branch Agencies，FCEB）必須依其 BOD 22-01 具強制力的作業指引，在期限之前更新或應對該 0-day 漏洞。

不過，Barracuda 原廠也表示，該公司已在前一周周末期間透過強制更新機制套用兩個針對此 0-day 漏洞的修補程式，因此該 0-day 漏洞已經在 5 月 21 日時自動修補完成。

不過根據 Barracuda 建議，雖然漏洞已經自動修補完成，但採用該公司 ESG 產品的客戶，其系統管理者仍應檢視其應用環境是否有遭到駭侵攻擊得

逞的跡象；CISA 也對此發出相同的建議，聯邦單位仍應檢視是否曾遭攻擊。

雖然 CISA 的強制性資安檢測修補命令僅適用於美國聯邦政府單位，但仍建議所有公私單位隨時注意並遵守 CISA 發表的最新資安警示與作業指引。

- 資料來源：
  1. CISA Adds One Known Exploited Vulnerability to Catalog
  2. Barracuda Email Gateway Defense Updates

2.4、社群媒體資安近況

2.4.1、Twitter 工程師發現 Android 版 WhatsApp 閒置時經常存取手機麥克風，Meta 指該問題為 Android 系統錯誤造成

一名 Twitter 工程師發現廣為使用的通訊軟體 WhatsApp 的 Android 版本，會在閒置時頻繁存取 Adnroid 裝置的麥克風，引發資安與隱私疑慮；但 WhatsApp 的開發者 Meta 在回應該問題時表示，該問題為 Android 系統內的錯誤所造成。

發現問題的 Twitter 工程師 Foad Dabiri，日前在 Twiiter 上發表一張截圖，表示安裝在其 Google Pixel 7 Pro 手機上的 WhatsApp 通訊軟體，從清晨 4 時左右頻繁使用該手機的麥克風；但該時間 Foad Drbiri 仍在睡眠中，並未使用 WhatsApp 進行語音通訊。

在該篇 Twitter 文章之後，陸續也有其他 WhatsApp 用戶通報相同的問題，不只會發生在 Google 品牌手機上，也會發生在 Samsung 手機上，包括 Samsung Galaxy S22 與 Galaxy S23。

在該推文下方也有不少用戶加入討論，分享其發現的狀況；有用戶注意到在未使用 WhatsApp 時，其 Android 手機右上角的通知區內，也會頻繁出現綠色小亮點（表示手機的敏感性硬體裝置，如相機或麥克風正在使用中）。

在相關討論愈來愈多時，WhatsApp 官方帳號也貼文回應，表示已與推文原作者的 Twitter 工程師聯絡並了解狀況。WhatsApp 也強調，當用戶授予手機麥克風的存取權限後，WhatsApp 僅在會使用者進行語音通話、視訊通話或錄製語音訊息時，才會使用裝置上的麥克風，且所有通訊內容皆以端對端加密進行傳輸。

WhatsApp 也表示，該問題可能是來自 Android 系統在隱私儀表板中發生的屬性錯誤，且已通報 Google 調查並解決該問題。

由於 Android 系統上較常出現要求過多權限的惡意軟體，因此建議用戶在授予 App 存取權限時應特別注意，且如果發現不正常的相機與麥克風存取情形，應特別提高警覺並移除可疑軟體。

- 資料來源：
  1. WhatsApp claims consistent microphone access is an Android bug
  2. Elon Musk Slams Meta’s WhatsApp for Unauthorized Access to Microphones

2.4.2、Facebook 發現專門竊取平台帳號與資料的惡意軟體 NodeStealer

Facebook 旗下的資安防護研究團隊，日前新發現一個專門竊取資訊與各平台帳號的惡意軟體 NodeStealer；該惡意軟體會以竊取瀏覽器 cookie 的方式，來挾持使用者在多個平台的帳號所有權。

Facebook 資安團隊在報告中指出，該團隊的資安研究人員，在 2023 年 1 月下旬時發現 NodeStealer 的活動跡象，當時該惡意軟體主要攻擊越南境內的 Meta 旗下服務使用者；當時距離 NodeStealer 的初次布署於攻擊僅有兩個星期。

Facebook 在報告中表示，NodeStealer 是以 JavaScript 撰寫，並透過 Node.js 框架來執行，因此可在 Windows、macOS 和 Linux 等不同作業系統跨系統運作；且 VirusTotal 上多數的防毒防駭引擎，當時都無法偵測出 NodeStealer。

NodeStealer 是一個偽裝成 PDF 檔或 Excel 試算表檔案的 Windows 可執行檔，且在散布時會使用讓使用者感興趣的檔名，以引誘使用者開啟該檔案；在使用者執行了 NodeStealer 後，該惡意軟體便會竊取使用者設備上安裝的 Chromium 瀏覽器（包括 Google Chrome、Microsoft Edge、Brave、Opera 等等）中的 Cookie，並竊取其中的 Facebook、Gmail、Outlook 登入資訊。

資安專家指出，竊取瀏覽器中的 cookie 已經成為新發現駭侵攻擊活動中常用的攻擊手法，原因是這樣可以直接取得受害者的帳號控制權，無需取得登入資訊，也不會被二階段登入驗證程序所阻擋。

建議使用者應避免自不明來源下載安裝任何可疑應用軟體，或開啟可疑檔案，以避免惡意軟體伺機入侵。

- 資料來源：
  1. The malware threat landscape: NodeStealer, DuckTail, and more
  2. Facebook disrupts new NodeStealer information-stealing malware

2.5、行動裝置資安訊息

2.5.1、Apple 於 2022 年共封鎖 170 萬個存有隱私與資安問題的 App

Apple 日前發表 App Store 統計數字報告，在報告中指出該公司在 2022 年間除了封鎖 170 萬個存有隱私、資安與違反內容政策問題的 App 之外，也防止超過 20 億美元疑似詐騙的交易。

該公司在報告中說，在 2022 年有超過 420,000 個開發者帳號因涉及詐騙或惡意行為而遭停權； 且有超過 2.82 億個用戶帳號亦因類似原因而遭停權。

Apple 也說，有 150,000 個開發者帳號在申請註冊時就因偵測到可疑活動而遭到中止；也有接近 400,000 個 App 因為內含試圖在未告知用戶的情形下獲取用戶個資，因而遭到 App Store 審核人員拒絕上架。

另外，也有 153,000 個 App 因為試圖誤導用戶，或因抄襲現有其他 App 而遭到拒絕上架；也有 29,000 個 App 因為含有未載明或隱藏的功能，也遭拒絕上架到 App Store 內。

App Store 也表示，2022 年中有多達 24,000 個 App 因為試圖以假功能先引誘用戶安裝，之後再出現惡意功能，因而遭到該團隊封鎖。

而在 App Store 的支付方面，該團隊一共封鎖了 20.9 億美元的詐騙交易，破歷年新高紀錄，亦有 714,000 個假帳號因涉及詐騙交易而遭封鎖，無法再次進行交易。

App Store 在去年一年之中，也封鎖了近 390 萬張遭到盜刷，試圖在 App Store 中進行詐騙交易的信用卡。

此外，App Store 在去年也刪除了超過 1.47 億則詐騙 App 評價，以防用戶受到假冒評價誤導而下載到不符所需的 App。

建議用戶下載手機 App 時，應避免在非官方管道下載或進行測載；即使在官方 App Store 下載，也應仔細閱讀其他用戶評價，以避開資安風險。

- 資料來源：
  1. App Store stopped more than $2 billion in fraudulent transactions in 2022
  2. Apple blocked 1.7 million apps for privacy, security issues in 2022

2.5.2、新發現 Android 惡意軟體 Fleckpe 已於 Google Play 下載 62 萬次

資安廠商 Kaspersky 旗下的研究人員，近日發表研究報告指出，在 Android 應用軟體官方下載服務 Google Play Store 中，發現一個全新的 Android 惡意軟體 Fleckpe；該惡意軟體會偽裝成多種實用軟體，但私下擅自訂閱高價服務，造成用戶損失。

Kaspersky 指出，在 Google Play Store 中至少發現 11 個偽裝成實用 App 但內含 Fleckpe 惡意軟體的 App，其偽裝成的 App 包括多種照片後製、影像編輯、照片存檔、進階版桌面圖片等等不同類型，吸引用戶下載安裝。

據報告統計指出，這 11 種 App 的總下載次數，合計已達 62 萬次之多。

Kaspersky 說，Fleckpe 和過去曾大量出現的 Jocker 和 Harley 等「訂閱」型 Android 軟體一樣，都會在用戶不知情的情況下，訂閱多種高價付費服務，以不法手段賺取服務分潤的暴利；也有一些付費服務根本就是駭侵者提供的，這樣駭侵者就能取得全額訂閱費用。

據報告指出，Fleckpe 主要的 Android 系統受害者，多分布在泰國、馬來西亞、印尼、新加坡、波蘭，但也有少量的受害者分布於全球其他國家。

據 Kaspersky 表示，在該公司公布這份資安通報時，所有 Google Play Store 中含有 Fleckpe 惡意軟體的 App 已全數遭到下架；但是 Kaspeskey 也強調，可能仍有未被發現的 Fleckpe 惡意 App 仍在架上可供下載，駭侵者也可能製作新的惡意 App 上架到各種應用程式商店，使用者仍需提高警覺。

建議 Android 使用者除需安裝防毒防駭軟體外，即使在官方 Google Play Store 中下載軟體，仍需提高警覺，在安裝前仔細查看其他使用者提供的評價。

- 資料來源：
  1. Not quite an Easter egg: a new family of Trojan subscribers on Google Play
  2. New Fleckpe Android malware installed 600K times on Google Play

2.5.3、資安研究人員分析行動裝置間諜軟體 Predator Android 版本的駭侵方式

資安廠商 Cisco Talos 和 Citizen Labs 旗下的資安研究人員近日發表研究報告，分析一個商業化的 Android 間諜惡意軟體 Predator 與其載入器 Alien，指出其資料竊取能力與其他操作細節。

Predator 是由一家以色列公司 Intellexa 開發並發售的商業化行動平台間諜軟體，同時支援 iOS 與 Android 平台；該惡意軟體已證實與多起針對媒體記者、歐洲政治人物，甚至 Meta 公司高階主管的駭侵事件有關。

在 Android 裝置上，Predator 能夠盜錄受害者的來電語音通話、自即時通訊軟體中收集資訊，甚至隱藏安裝在手機上的應用程式，同時阻止該程式的執行。

2022 年 5 月時，Google 旗下的資安研究團隊 Google TAG 就發現了 Predator 用以入侵並植入其載入程式 Alien 的 0-day 漏洞；Alien 載入程式是注入一個名為 zygote64 的 Android 程序，然後下載並啟用附加的間諜軟體程式碼；Alien 是從一個外部位址取得並啟動 Predator 組件；如果發現新版 Predator，也會進行更新。

當 Alien 偵測到自己在 Samsung、Huawei、Oppo 或 Xiaomi 手機上執行時，就會以遞迴方式窮舉列出存有用戶資訊、電子郵件、即時通訊內容、社

群媒體、瀏覽器 App 資料的目錄並竊取其內容，也會竊取用戶通訊錄與媒體資料夾中的私人媒體檔案，包括音訊、圖片和影片等。

各平台手機用戶應對不明連結或檔案隨時提高警覺，避免自不明來源安裝或開啟可疑檔案。

- 資料來源：
  1. Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware
  2. Predator: Looking under the hood of Intellexa’s Android spyware

2.6、軟體系統資安議題

2.6.1、新出現的「Greatness」釣魚攻擊服務，簡化 Microsoft 365 釣魚攻擊流程

網通大廠 Cisco 旗下的資安研究單位 Cisco Talos，其資安專家發現一個全新的釣魚攻擊「服務」（Phishing-as-a-Service, PhaaS）平台「Greatness」，在多個國家廣泛用於發動針對 Microsoft 365 的釣魚攻擊活動中。

由於 Microsoft 365 雲端生產力服務的全球使用者為數眾多，包括各式大中小型企業、政府單位與個人，因此這類 PhaaS 攻擊可能造成的影響層面甚廣。

Cisco Talos 在報告中指出，「Greatness」PhaaS 平台最初是在 2022 年中推出，其活動在 2022 年 12 月第一次達到高峰；在 2023 年 3 月又再次開始活躍；受該平台發動釣魚攻擊所影響的受害者遍及全球，主要分布在美國、加拿大、英國、澳洲與南非。

在受影響業種方面，主要的受害者分布於製造業、醫療保健業、科技產業、教育、房地產、營建業、金融業、企業服務等等。

報告指出，「Greatness」PhaaS 平台幾乎包辦一切發動釣魚攻擊所需的要素；欲發動攻擊的駭侵者，只要使用 Greatness 的管理控制台來使用其 API

key，並且提供攻擊目標的 email 地址，並且指定釣魚信件的標題與部分內容即可；其餘包括用來發送釣魚信件的伺服器、惡意 HTML 附件的產生等，都由 Greatness PhaaS 平台一手包辦。

受害者一旦開啟 Greatness 釣魚信中的附件，就會看到一個冠上受害者公司 logo 的 Microsoft 365 假登入對話框，用以竊取受害者輸入的 Microsoft 365 登入資訊；接著該惡意頁面就會中繼受害者和真正 Microsoft 365 之間的通訊內容，竊取各種機敏資訊。

建議各機關或個人都應加強對釣魚郵件的警覺，切勿任意開啟來路不明郵件中的附件。

- 資料來源：
  3. New phishing-as-a-service tool “Greatness” already seen in the wild
  4. New 'Greatness' service simplifies Microsoft 365 phishing attacks

2.6.2、全球各地發生多起以假 QR Code 問卷、停車票卡竊取受害者資金事件

QR Code 已成為通用全球的便利工具，使用者可利用智慧型手機掃瞄 QR Code 後，快速存取各種網路資源；但近來在全球各地傳出多起不法分子利用 QR Code 假冒會員問卷、停車票卡，實則埋藏惡意連結，造成各種損害。

新加坡海峽時報日前報導指出，一名 60 歲左右的婦人，在一家珍珠奶茶店，以智慧型手機掃瞄了貼在店面牆上的會員問卷 QR Code，想要填寫會員問卷以獲贈一杯免費的飲料，結果不幸遭到駭侵者惡意攻擊。

報導說，婦人以其 Android 手機掃瞄該惡意 QR Code 後，便下載了一個第三方 App 在手機上；婦人以該 App 填寫完問卷資料後，當天半夜突然接獲銀行通知，帳戶已遭盜領達 20,000 美元。資安專家指出，該惡意軟體顯然竊取了受害者手機中的網路銀行登入資訊。

新加坡警方指出，光在 2023 年 3 月，類似案件就有 113 起，共造成 445,000 美元的財損。

此外，在美國與英國各地，近來也頻頻發生類似的攻擊事件。許多將車輛停在停車場內的車主，會遭到駭侵者將假冒的停車計時票卡夾在擋風玻璃上；以發生在美國舊金山的案例而言，駭侵者偽造舊金山交通局（San Francisco Municipal Transportation Agency, SFMTA）製作的停車票卡；車主若

以手機掃瞄偽造票卡上的 QR Code，就會進入駭侵者製作偽造 SFMTA 官方網站，其外觀和真實的 SFMTA 官網極為類似，用以詐騙受害者誤將停車費繳交到駭侵者設立的帳戶中。

在英國的案例則是受害者掃瞄假 QR Code 後，會進入釣魚網站並輸入自己的信用卡資料，造成卡片資料外洩並被盜刷。

建議用戶以手機掃瞄 QR Code 後，如果被要求下載軟體，應提高警覺，仔細判斷軟體真偽，且不應授予過多權限；若被導到網站，應仔細觀察網址是否正確無誤，以免遭到釣魚攻擊而造成資安風險。

- 資料來源：
  1. Woman who scanned QR code with malware lost 20k to bubbl tea survey scam while she was sleeping
  2. Fraud , Fake Parking Ticket PSA
  3. QR codes used in fake parking tickets, surveys to steal your money

2.6.3、美國 MCNA Dental 因勒贖攻擊外洩 890 萬病患資料

美國政府資助牙醫暨口腔醫療保險服務 Managed Care of North America (MCNA) Dental，日前在其官網發表資安通報，表示因遭到勒贖攻擊，造成超過 890 萬名美國病患個資遭到外洩。

MCNA Dental 於上周五發表資安通報，指出該單位現已獲悉其電腦系統於 2023 年 2 月到 3 月間遭到未經授權人士入侵；調查指出駭侵者在 2023 年 2 月 26 日起取得 MCNA Dental 內部網路的存取權限。

在駭侵者活動期間，近 900 萬名病患的資料遭到不當存取，遭竊的資料包括以下欄位：

- 病患全名；
- 住址；
- 出生年月日；
- 電話號碼；
- Email；
- 社會安全號碼（Social Security Number）；

- 駕照號碼；
- 政府核發身分證件號碼；
- 醫療保險（方案資訊、保險公司、會員編號、醫療保健 ID 等）；
- 牙齒保健資料（就診次數、牙醫師姓名、醫師姓名、就醫記錄、X 光片存檔、用藥記錄、診斷書資料等）。

據美國緬因州總檢察署辦公室指出，因此勒贖攻擊而造成資料外洩的受害者人數為 8,923,662 人，MCNA Dental 已告知這些受害者資料外洩一事，且 MCNA 已採取所有行動來處理資安設置，以防類似事件再次發生。

勒贖團體 LockBit 在其網站中宣稱，針對 MCNA Dentel 的攻擊是由他們發動的；LockBit 說整個資料量高達 700GB，並要求 MCNA Dentel 支付 1,000 萬美元贖金，否則就要公開這批資料。LockBit 也在其網站中公布了部分資料。

建議擁有大量機敏資訊的公私單位，務必加強資安防護能力，避免因各式資安攻擊造成資料外洩，造成大量受害者權益受損。

- 資料來源：
  1. Data Breach Notifications
  2. Notice of Data Breach
  3. MCNA Dental data breach impacts 8.9 million people after ransomware attack

2.7、軟硬體漏洞資訊

2.7.1、駭侵者利用已公開的 WordPress 外掛程式漏洞發動大規模攻擊

資安廠商 Patchstack 近期發現一個 WordPress 外掛程式漏洞 CVE-2023-30777，在該廠商公布相關漏洞資訊後短短 24 小時，就開始遭到駭侵者藉以大量發動攻擊。

該漏洞 CVE-2023-30777 存於一個獲得廣泛採用的 WordPress 外掛程式（Plugin）Advanced Custom Fields，屬於高危險性的跨站指令碼攻擊（Cross-site scripting, XSS）漏洞；未經授權的攻擊者可透過該漏洞竊取機敏資訊，並且在受到攻擊的 WordPress 網站中提升自身的執行權限。

該漏洞的 CVSS 危險程度評分為 7.1 分（滿分為 10 分），危險程度評級為「高」（High）；Patchstack 於 2023 年 5 月 2 日發現此漏洞，並在 3 天後的 5 月 5 日公布漏洞相關細節與攻擊用的概念驗證（proof of concept）。Advanced Custom Fields 外掛程式的開發者則是在 Patchstack 推出概念驗證前一天完成該外掛程式的修復，並且推出更新版本 6.1.6。

然而根據網路基礎建設業者 Akamai 旗下資安團隊的報告指出，該團隊自 5 月 6 日起開始觀察到大量使用 Patchstack 攻擊概念驗證程式碼發動的攻擊活

動；報告指出駭侵者直接拷貝了 Patchstack 撰寫的程式碼，針對眾多 WordPress 網站發動攻擊。

據估計，目前仍在使用舊版未更新 Advanced Custom Fields 外掛程式的 WordPress 網站，高達 140 萬個之多，因此給駭侵者很大的攻擊空間。

- CVE 編號：CVE-2023-30777
- 解決方案：建議使用 Advanced Custom Fields 外掛程式的 WordPress 網站管理員，應立即將該外掛程式更新到 5.12.6、6.1.6 或後續版本，以避免遭到攻擊。

- 資料來源：
  1. Reflected XSS in Advanced Custom Fields Plugins Affecting 2+ Million Sites
  2. The Race to Patch: Attackers Leverage Sample Exploit Code in Wordpress Plugin

2.7.2、Microsoft 推出 2023 年 5 月 Patch Tuesday 每月例行更新修補包，共修復 38 個資安漏洞，內含 3 個 0-day 漏洞

Microsoft 日前推出 2023 年 5 月例行資安更新修補包「Patch Tuesday」，共修復 38 個資安漏洞，其中有 6 個是屬於「嚴重」(Critical) 危險程度的漏洞，另有 3 個 0-day 漏洞也獲得修復，這些漏洞已知遭用於攻擊活動。

本月 Patch Tuesday 修復的漏洞數量僅有 38 個，較上個月（2023 年 4 月）的 97 個資安漏洞少了很多，可說是歷來修補漏洞數量最少的一次；其中 6 個屬於嚴重等級的漏洞，分類上全部屬於遠端執行任意程式碼類型，也是各種軟體漏洞中危害最大的一類。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：8 個；
- 資安防護功能略過漏洞：4 個；
- 遠端執行任意程式碼漏洞：12 個；
- 資訊洩露漏洞：8 個；
- 服務阻斷（Denial of Service）漏洞：5 個；
- 假冒詐騙漏洞：1 個。

本月修復的 0-day 漏洞共有 3 個，第一個是 CVE 編號為 CVE-2023-29336 的 Win32K 權限提升漏洞；該漏洞存於 Win32K Kernel driver 之中，可讓駭侵者將自身執行權限提升到最高等級的 SYSTEM 等級。

第二個 0-day 漏洞是 CVE-2023-24932，屬於開機安全功能略過漏洞；該漏洞已遭駭侵者利用 BlackLotus UEFI bootkit 用於攻擊；Windows 系統中的韌體會遭寫入惡意軟體，且防毒防駭軟體無法偵測。

第三個 0-day 漏洞是 CVE-2023-29325，存於 Windows OLE 系統中，為遠端執行任意程式碼漏洞。

- CVE 編號：CVE-2023-29336、CVE-2023-24932、CVE-2023-24932
- 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，以最快速度套用 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. Win32k Elevation of Privilege Vulnerability
  2. Secure Boot Security Feature Bypass Vulnerability
  3. Windows OLE Remote Code Execution Vulnerability
  4. Microsoft May 2023 Patch Tuesday fixes 3 zero-days, 38 flaws

2.7.3、Apple 修復 3 個可用以駭侵 iPhone、iPad、Apple Watch、Apple TV 與 Mac 的 0-day 漏洞

Apple 近日修復 3 個可讓駭侵者用以攻擊 iPhone 與 Mac 等多款 Apple 產品的 0-day 漏洞 CVE-2023-32409、CVE-2023-28204、CVE-2023-32373。iPhone 與 Mac 使用者應儘速更新，以降低遭駭侵者以已知漏洞發動攻擊的風險。

據 Apple 這三個漏洞都存於跨平台的 WebKit 瀏覽器引擎。頭一個漏洞 CVE-2023-32409 為一個沙箱跨越漏洞，可讓遠端駭侵者跳過 Web 內容沙箱的侷限，影響到沙箱以外的操作環境。

至於另外兩個漏洞，駭侵者都可以利用特制的網頁內容來觸發。其中一個屬於越界讀取錯誤（out-of-bounds read），駭侵者可藉以取得機敏資訊；另一個則是屬於釋放後使用（use-after-free）的錯誤，駭侵者可透過此漏洞遠端執行任意程式碼。

受到此漏洞影響的裝置相當多，包括 iPhone 6s（所有機型）、iPhone 7（所有機型）、iPhone SE（第 1 代）、iPad Air 2、iPad mini（第 4 代）、iPod Touch（第 7 代）、iPhone 8 與後續機型、iPad Pro（所有機型）、iPad Air（第 3 代與後續機型）、iPad（第 5 代與後續機型）、iPad mini（第 5 代與後續機型）、所有執行 macOS Big Sur、Monterey 與 Ventura 的 Mac 電腦、Apple Watch Series 4 與後續機型、Apple TV 4K（所有機型）、Apple TV

HD。

Apple 在新推出的 iOS、iPadOS 16.5、macOS Ventura 13.4、tvOS 16.5、watchOS 9.5、Safari 16.5 中強化了邊界檢查、輸入驗證和記憶體管理，解決了這 3 個 0-day 漏洞。

- CVE 編號：CVE-2023-32409、CVE-2023-28204、CVE-2023-32373
- 影響產品(版本)：iPhone 6s（所有機型）、iPhone 7（所有機型）、iPhone SE（第 1 代）、iPad Air 2、iPad mini（第 4 代）、iPod Touch（第 7 代）、iPhone 8 與後續機型、iPad Pro（所有機型）、iPad Air（第 3 代與後續機型）、iPad（第 5 代與後續機型）、iPad mini（第 5 代與後續機型）、所有執行 macOS Big Sur、Monterey 與 Ventura 的 Mac 電腦、Apple Watch Series 4 與後續機型、Apple TV 4K（所有機型）、Apple TV HD。
- 解決方案：立即升級到 iOS、iPadOS 16.5、macOS Ventura 13.4、tvOS 16.5、watchOS 9.5、Safari 16.5。

- 資料來源：
  1. About the security content of iOS 16.5 and iPadOS 16.5
  2. Apple fixes three new zero-days exploited to hack iPhones, Macs

第 3 章、 資安研討會及活動

【資安學院】6/14 雲端服務資訊安全及管控措施	
活動時間	**2023-06-14 09:30 ~ 16:30**
活動地點	**中華民國資訊軟體協會-大同辦公室 D01 大會議室** **（台北市中山區中山北路 3 段 22-1 號新設工大樓 5 樓 C 區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/3955**
活動概要	中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 協會聯絡窗口： 02-2553-3988 分機 388　廖資深專員 security(at)cisanet.org.tw 報名截止： 2023-06-09 近年資訊及網路科技騰飛，國內外雲端服務提供商林立，為節省設備、人員及技術成本，越來越多企業選擇雲端，處理其資料儲存和運算等作業，但也衍生出相關資訊安全的議題及風險。 本課程引用國際準則及法規要求，講解目前業界之實務作法，介紹雲端資料傳輸、資訊儲存等之必要之控制，雲端服務委外管理及資安事故回報等機制。採用互動式教學，以提升學員雲端資安風險分析及管理的能力。

D Forum ESG 系列：企業資安論壇(實體、線上同步)	
活動時間	**2023/6/16**
活動地點	**t.hub 內科創新育成基地 1F 102 會議室**
活動網站	**https://www.digitimes.com.tw/seminar/DForum_20230616/**
活動概要	 **主辦單位：DIGITIMES** 調整資安體質 布局欺敵戰術 企業隨著數位轉型風浪一波波拍打上岸， 浪中挾帶更多資安汙泥。 擁抱新興的科技工具協助了企業治理， 但隨資料上雲遁地，凡走過都是曝險部位， 迫使企業資安長被駭妄想敏感體質症狀加劇。 企業面對資安恐慌切記步步為營，掌握威脅情資只是起手式， 堅守零信任安全思維，善用環境分段技術， 避免群聚感染、徹底清零暗網黑手！ 當供應鏈上下游信任協議機制已成為共好的依靠， 你的資安不只是你的資安， 企業需要共築資安的堡壘。 詳細活動議程及報名方式請參閱活動官網。

機器學習與資安異常診斷實務	
活動時間	**112 年 6 月 27 日，週二，09:10~16:00**
活動地點	**台灣金融研訓院芬恩特創新聚落(南海路 3 號 4 樓)**
活動網站	**https://web.tabf.org.tw/page/407020/course9.htm**
活動概要	 **主辦單位：台灣金融研訓院** 課程等級：初階/中階 參加對象： -各金融機構〈含金控、銀行、證券、保險、信合社、農漁會、投信、投顧等〉從業及資訊安全管理人員。 -對本課程有興趣，欲提升資訊安全知識者。 課程內容： ● 機器學習概論 ➢ 機器學習簡介 ➢ 機器學習步驟與過程 ➢ 模型效能分析與評估方式 ➢ 監督與非監督式模型簡介 ➢ 集成式模型架構 ● 異常診斷機制與模型 ➢ 異常診斷簡介 ➢ 異常診斷發展趨勢與挑戰 ➢ 監督式異常診斷模型 ➢ 半監督式異常診斷模型 ➢ 異常診斷模型建置示範

	*主辦單位保留活動內容調整之權益。 詳細課程內容及報名方式請參閱活動官網。

從國際安全標準看物聯網安全	
活動時間	**112 年 7 月 4 日，週二，09:10~16:00**
活動地點	**台灣金融研訓院芬恩特創新聚落(南海路 3 號 4 樓)**
活動網站	**https://web.tabf.org.tw/page/407020/course10.htm**
活動概要	 **主辦單位：台灣金融研訓院** 課程等級：初階 參加對象： -各金融機構〈含金控、銀行、證券、保險、信合社、農漁會、投信、投顧等〉從業及資訊安全管理人員。 -對本課程有興趣，欲提升資訊安全知識者。 課程內容： ● 物聯網簡介與安全概論 ➢ 資訊安全概論 ➢ 物聯網安全簡介 ➢ 物聯網資訊安全趨勢與合規測試 (SSDLC) ● 物聯設備安全測試初探 ➢ 物聯網測試國家標準與法規 ➢ 影像監控系統物聯網設備安全測試 ➢ 物聯網設備藍芽安全 *主辦單位保留活動內容調整之權益。 詳細課程內容及報名方式請參閱活動官網。

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布之資安漏洞，漏洞嚴重程度前五名之漏洞資訊如下表：

仲琦科技 Hitron CODA-5310 - Using default credentials	
TVN / CVE ID	TVN-202304004 / CVE-2023-30603
CVSS	9.8(CRITICAL)
影響產品	Hitron CODA-5310 v7.2.4.7.1b3
問題描述	仲琦科技 CODA-5310 的 telnet 功能使用預設帳號和密碼，且未提醒使用者修改，導致遠端攻擊者不須權限即可利用該帳號密碼取得管理者權限，進行查看與修改，造成系統服務中斷。
解決方法	仲琦科技已提供解決問題版本給網路營運商並告知升級，如有任何問題請聯繫網路提供業者。
公開日期	2023-05-02
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7085-13321-3.html

仲琦科技 Hitron CODA-5310 - Broken Access Control	
TVN / CVE ID	TVN-202304005 / CVE-2023-30604
CVSS	9.8(CRITICAL)
影響產品	Hitron CODA-5310 v7.2.4.7.1b3
問題描述	仲琦科技 CODA-5310 未對所有系統設定網頁進行權限驗證，導致遠端攻擊者不須身分驗證就可以存取特定的系統設定介面，並對系統進行任意操作或中斷服務。
解決方法	仲琦科技已提供解決問題版本給網路營運商並告知升級，如有任何問題請聯繫網路提供業者。
公開日期	2023-05-02

相關連結	https://www.twcert.org.tw/newepaper/cp-151-7086-35622-3.html

固特斯 SGUDA U-Lock 遠端八合一電子鎖 - Broken Access Control	
TVN / CVE ID	TVN-202211008 / CVE-2022-46307
CVSS	8.8 (High)
影響產品	聯繫固特斯詢問受影響產品及版本
問題描述	SGUDA U-Lock 電子鎖中控服務之管理電子鎖功能未作有效的授權控管，遠端攻擊者以一般權限登入後，即可調用 API 取得其他電子鎖資訊，並控制終端電子鎖，或使電子鎖無法正常使用。
解決方法	聯繫固特斯進行漏洞修補
公開日期	2023-05-11
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7099-e8897-3.html

威德網頁設計 FANTSY - Broken Acesss Control	
TVN / CVE ID	TVN-202304001 / CVE-2023-28698
CVSS	9.8 (Critical)
影響產品	威德網頁設計 FANTSY v2.1.8
問題描述	FANTSY 未適當進行權限控管，使遠端攻擊者不須權限，即可修改 URL 參數，取得系統管理者權限，任意操作系統，並終止服務。
解決方法	聯繫威德網頁設計進行漏洞修補
公開日期	2023-05-11
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7101-f88db-3.html

佳元科技 電子郵差 Web Fax - SQL Injection	
TVN / CVE ID	TVN-202305003 / CVE-2023-28701
CVSS	9.8 (Critical)
影響產品	聯繫佳元科技詢問電子郵差 Web Fax 受影響版本
問題描述	電子郵差 Web Fax 存在 SQL Injection 漏洞，遠端攻擊者不須權限，即可於登入頁面欄位注入 SQL 指令，即可任意操作系統或中斷服務。
解決方法	佳元科技已於 3/29 釋出更新版本
公開日期	2023-05-30
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7145-1a0d4-3.html**

第 5 章、 2023 年 5 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。

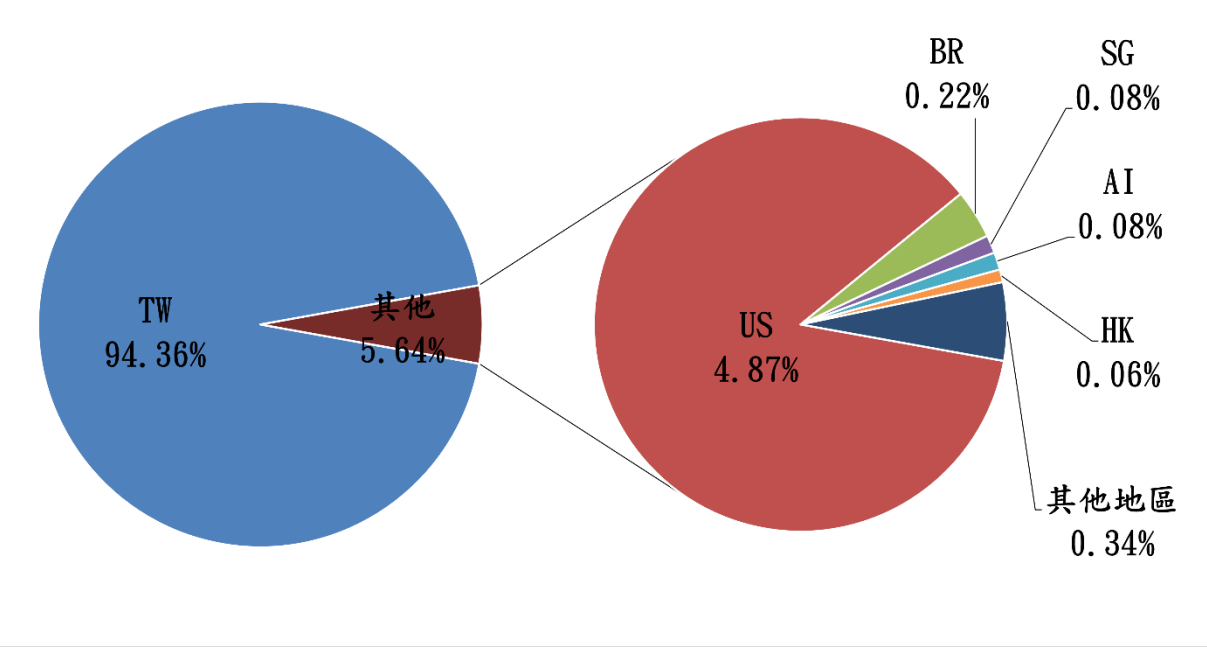

圖 1、分享地區統計圖

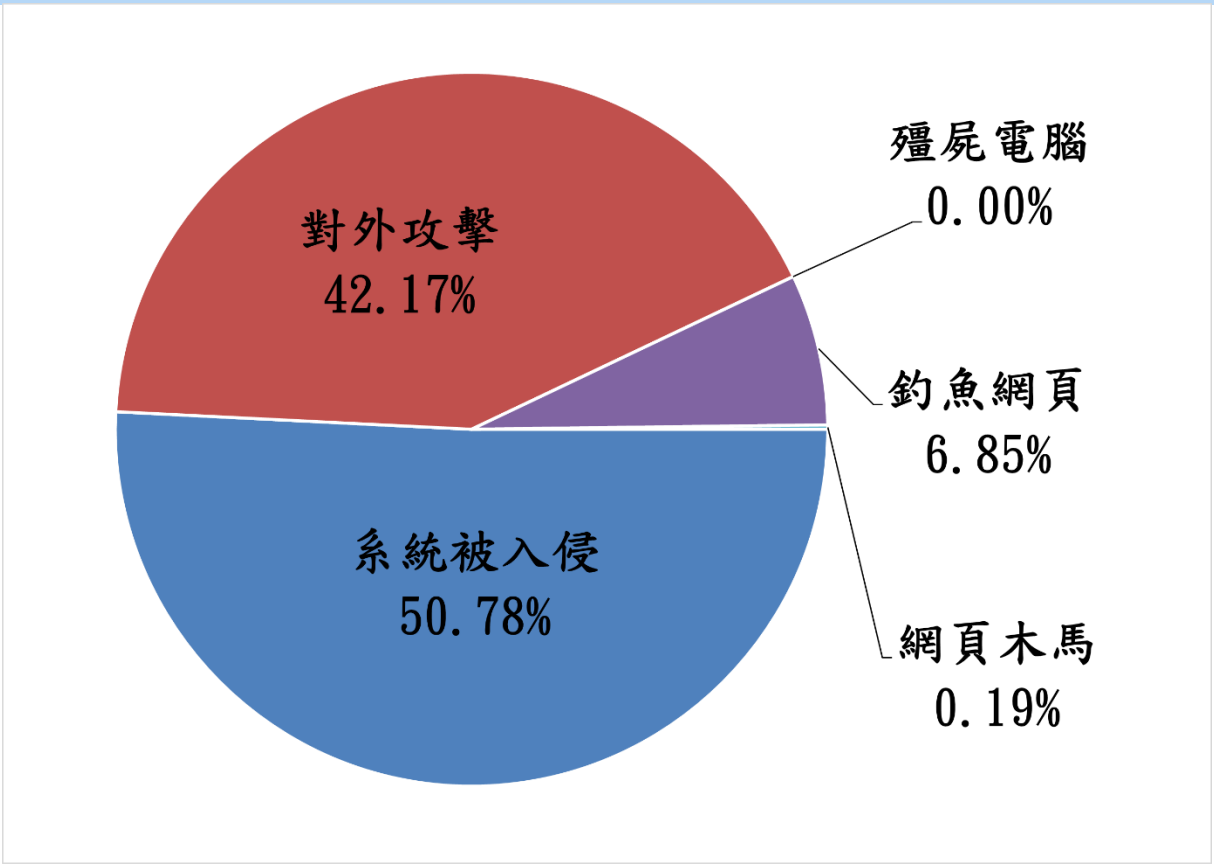

圖 2、分享類型統計圖

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 6 月 9 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**