TWCERT/CC 資安情資電子報

2023 年 4 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)在行政院資通安全處及國家通訊傳播委員會指導下，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 6 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、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養。

第 3 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 4 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 5 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 6 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

Google 於 Samsung Exynos 晶片組中發現多達 18 個 0-day 漏洞

Google 旗下的資安研究團隊 Project Zero 日前發表資安通報指出，該團隊的研究人員在 Samsung 用於行動裝置、穿戴式裝置與汽車中的 Exynos 晶片組，一口氣發現多達 18 個 0-day 資安漏洞。

該團隊是在 2022 年末到 2023 年初之間，在 Exynos 晶片組的 Modem 內發現多個安全漏洞，在 18 個漏洞中有 4 個的危險程度極高，可讓駭侵者自外網入侵裝置的基頻 (Baseband)，並且遠端執行任意程式碼。

據報告指出，這 4 個遠端執行任意程式碼漏洞（其中一個為 CVE-2023-24033，另外三個尚無 CVE 編號），可讓攻擊者在無需任何使用者互動的隱密情形下遠端入侵設備，並遠端執行任意程式碼。

Samsung 也在自行發表的漏洞資安通報中表示，Exynos 晶片組中的基頻軟體未能妥善檢查由 SDP 指定之接受類型的格式，導致駭侵者可在基頻晶片中發動服務阻斷攻擊 (Denial of Service, DoS)，或是遠端執行任意程式碼。

Google Project Zero 的報告也指出，駭侵者只需要擁有受害者的手機電話號碼，即可發動攻擊。

其他 14 個 Exynos 晶片組中的漏洞，其危險程度較低，但仍有一定程度的資安風險；攻擊者需實際操作受害手機，或利用惡意行動網路才能發動攻擊。

受此漏洞影響的行動裝置不限於 Samsung 品牌，只要是採用 Exynos 晶片組的裝置都受到影響，包括：

- Samsung 手機：S22、M33、M13、M12、A71、A53、A33、A21、A13、A12、A04 等系列；
- Vivo 手機：S16、S15、S6、X70、X60、X30 系列；
- Google 手機：Pixel 6、7 系列；
- 採用 Exynos W920 晶片的所有穿戴裝置；
- 所有採用 Exynos Auto T5123 晶片組的汽車。

雖然 Samsung 已經向各品牌廠商提供暫時解決方案，但其修補軟體並未公開，且無法由用戶自行安裝。各用戶可以暫時先停用 Wi-Fi Calling 和 VoLTE 功能，以避免 RCE 漏洞遭到攻擊。

- 資料來源：
  1. News and updates from the Project Zero team at Google
  2. Product Security Update
  3. Google finds 18 zero-day vulnerabilities in Samsung Exynos chipsets

第 2 章、 資安小知識

雲端服務的資安防護與建議

透過雲端部署服務已經逐年成為趨勢，由於雲端服務具有高擴展性、高方便性以及高運算彈性，因此企業透過雲端部署服務的比例逐漸增長。然而駭客逐漸改變攻擊模式，鎖定雲端服務，而雲端服務的漏洞數量也不斷增長，企業在處理雲端安全的議題時，仍以傳統資安架構及防禦模式來處理，因此容易形成資安防禦層面的缺口。

目前雲端服務主要有 Amazon Web Services（AWS）、Google Cloud Platform（GCP）、Microsoft Azure 與阿里雲（Alibaba Cloud），本篇以 Google Cloud Platform 為例，提供企業相關資安防護與建議：

- 啟用多重身份驗證、使用強密碼：由於攻擊者可藉由攔截或竊聽 Google Cloud Platform 的密碼或憑證，建議啟用多重身份驗證，以及使用複雜度較高的密碼原則，並定期修改密碼，以降低資安風險。
- 最小權限原則：企業應採取最小權限原則設定使用者僅能存取他們履行職責所需的內容，而不能存取更多內容，以避免攻擊者竊取密碼後，

能存取安全相關日誌資訊或是 Google Cloud Storage buckets，導致數據被修改、刪除甚至洩漏。

- 存取限制設定：企業應停用 buckets 公用分享設定，並且使用 VPC Service Controls 限制哪些 IP 可以訪問 Google Cloud Storage API，以避免攻擊者若具有足夠的權限，能上傳惡意代碼至 Google Cloud Storage buckets。
- 啟用版本控制功能：在 buckets 上啟版本控制功能，以便可以恢復較早版本。
- 啟用“Data Read”與“Data Write”Log：由於 Google 本身允許個人或團體挖掘其漏洞，故在 zero-day 漏洞是無法避免的，因此建議啟用“Data Read”與“Data Write”Log 利於事件發生後的追蹤。
- 啟用”Access Transparency”功能：由於可能會有 Google 內部人員存取 Google Cloud Storage buckets 的資料造成資料外洩的風險，因此當有 Google Cloud 管理員存取您的內容時，企業可透過近乎即時的記錄檔深入查看存取活動。

- 資料來源：

1. Threat Modelling Cloud Platform Services by Example: Google Cloud Storage

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、資安研究指出：多數單位無法於 1 小時內解決雲端資安威脅

網通廠商 Palo Alto Networks 旗下的資安研究人員發表報告《2023 雲端原生資安狀況報告》(2023 State of Cloud-Native Security Report) 指出，有 90% 單位表示無法自行在 1 小時內發現、處理並解決資安威脅。

報告指出，在 Covid-19 疫情期間，各公私單位擴大雲端服務使用達 25% 以上，但也因此面臨更大的雲端資安挑戰，且雲端應用在開發期間若未注意資安防護，因而產生的資安漏洞，將在應用上線後帶來極大資安威脅。

報告顯示，有 75% 的組織每周會在雲端布署新增或更新的程式碼，甚至有 40% 會每日進行程式碼更新，但沒有任何組織能夠負荷同等的資安防護心力。

報告也指出，許多單位在將應用移往雲端時，仍舊難以完整對應可能帶來的資安威脅與技術困難；有 78% 受訪單位表示將雲端服務的安全責任分散到各單位，而非以單一資安團隊因應，而有 47% 表示旗下員工並不了解對應

的資安責任。

另外，這些單位也難以選用適合的資安防護工具，許多單位都同時採用多種不同的資安防護工具，平均的使用種類達 30 種以上，其中只有 6 到 10 種是專門針對雲端的資安防護。這造成管理人員無法輕鬆了解整體資安防護狀況，有高達 76% 組織指出這麼多種的資安防護工具，反而造成資安防護的盲點。

Palo Alto Networks 在報告中指出，駭侵者利用組織資安漏洞發動攻擊的動作通常十分快速，在雲端服務中曝露在 Internet 下的資料，遭到攻擊得逞的所需時間往往只要數分鐘；即時偵測攻擊發生並立即排除，成為雲端應用資安的一大挑戰。

建議各單位在開始轉用雲端服務時，對於整體資安策略應有通盤性的考量，其解決方案也應考量易用性、可擴充性與可見度，並設置專責資安單位，以強化資安防護層級，並加速遭攻擊時的反應速度。

- 資料來源：
  1. Complexity Challenges Cloud Security, 2023 Survey Shows
  2. Palo Alto Networks: Most Organizations Can’t Resolve Cyberthreats Within an Hour

3.1.2、去年有 55 個 0-day 漏洞遭駭客濫用於攻擊，以 Microsoft、Google、Apple 為主

資安廠商 Mandiant 近期發表 2022 年 0-day 漏洞濫用研究報告，指出駭侵者持續使用 0-day 漏洞發動惡意攻擊；報告指出，2022 年有 55 個 0-day 漏洞遭大規模濫用，其中大部分漏洞來自 Microsoft、Google 和 Apple 產品。

遭駭侵者濫用的 0-day 漏洞共有 55 個，其中有 53 個可讓駭侵者在受害裝置上提升其執行權限，或是遠端執行任意程式碼。

以遭攻擊產品而來說，2022 年 Microsoft Windows 共有 15 個 0-day 漏洞遭利用，Chrome 排名第二，有 9 個遭濫用的 0-day 漏洞，iOS 排名第三，有 5 個 0-day 漏洞，macOS 排名第四，有四個 0-day 漏洞。

報告說，由於 0-day 漏洞是在開發者得知或發表修補程式之前，就遭到駭侵者利用的漏洞，因此幾乎沒有任何保護或監控措施可用於保護，因而成為駭侵者樂於使用的攻擊目標。

Mandiant 於 2022 年追蹤 13 個 0-day 漏洞的濫用情形，據其報告指出，駭侵者使用 7 個 0-day 漏洞發動攻擊，主要攻擊作業系統、網路瀏覽器和網路管理產品，以進行網路問諜攻擊為主，佔比達 50%以上。另外有 4 個 0-day 漏洞用於金融方面的攻擊，其中又有 75% 的攻擊屬於勒贖。

在 2021 年，駭侵者利用了 81 個 0-day 漏洞發動資安攻擊入侵，2022 年的數字略有下降；然而，2022 年受到濫用的 0-day 漏洞的數量也比 2021 年之外的年份來得多。Mandiant 預計在 2023 年，這一趨勢將繼續上升。

建議企業和個人用戶應採取以下措施：及時更新作業系統、網路瀏覽器和其他軟體；使用網路安全防護產品，如防火牆和入侵檢測系統，並加強內部網路監控，以便及時發現各種可疑活動，並增強人員的資安意識與教育訓練。

- 資料來源：
  1. Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace
  2. Hackers mostly targeted Microsoft, Google, Apple zero-days in 2022

3.2、新興應用資安

3.2.1、加密貨幣硬體錢包 Trezor 遭駭侵者大規模冒名發動釣魚攻擊

專門製造硬體加密貨幣冷錢包的 Trezor 公司，近日發布資安警訊，指出該公司遭到駭侵者冒名藉以發動釣魚攻擊活動，意圖騙取使用者設定的錢包復原短語，將用戶加密資金盜領一空。

Trezor 等公司製造生產的這類加密貨幣硬體錢包，可以讓用戶離線儲存自己的加密貨幣資產，是比連網的「熱錢包｜更為安全的加密貨幣儲存方式，因此有相當多加密貨幣投資人使用這種裝置儲存數位資產。

用戶在使用這類加密貨幣錢包存入數位資產前，必須先設定一組 12 到 24 個字元組成的「復原短語」；日後要存取數位資產時，必須先將硬體錢包插上電腦的 USB 埠，然後輸入正確的復原短語才能進行。這波針對 Trezor 硬體錢包的攻擊活動，就是以竊取用戶的復原短語為目標。

據 Trezor 指出，從 2023 年 2 月 27 日開始，有許多 Trezor 用戶收到駭侵者發送的簡訊與 Email 訊息，內容指稱該公司因發生駭侵事件導致用戶資料遭竊，影響用戶的資金安全性；駭侵者並在訊息中附上一個釣魚網址，要求用戶連上該網址以確保資金安全。

用戶點按該網址後，會被導至假冒的 Trezor 官方網頁；如果用戶按下網頁中的按鈕，網頁就會要求用戶輸入自己的復原短語；一旦用戶輸入了正確的復原短語，錢包中的加密貨幣資產立即就會被盜領一空。

Trezor 指出，該公司近期並未發生任何被駭事件，也絕不會透過簡訊或電話聯絡用戶；不過 Trezor 並未說明駭侵者如何取得該產品用戶的聯絡方式。

建議加密貨幣投資者應時時提高警覺，除了勿隨意點按不明連結外，也絕對不要將相關冷熱錢包的復原短語告知任何人，以免資產遭到盜領。

- 資料來源：
  1. Trezor @Trezor
  2. Trezor warns of massive crypto wallet phishing campaign

3.2.2、駭侵者攻擊 Euler Finance 借貸協定，竊走 1.97 億美元加密貨幣

由位於英國的 Eular Labs 推出的加密貨幣借貸協定 Euler Finance 於日前遭到駭侵者發動攻擊，多種加密貨幣資產遭竊，總額高達 1.97 億美元。

駭侵事件發生於本（2023）年 3 月 12 日，不明身分的駭侵者，利用該協定閃電貸款 (flash loan) 的漏洞，成功竊取多種加密貨幣資產，包括價值 875 萬美元的 DAI、1850 萬美元的 WBTC、3385 萬美元的 USDC，以及 1.358 億美元的 stETH。

閃電貸是一種去中心化加密貨幣交易所提供的服務，可讓使用者在無擔保，無抵押的情形下快速借出加密資產進行操作；借貸者須在交易資料寫入區塊前的極短時間 (多半在數秒內) 內償還貸款，否則將會取消使用者的貸款。通常用於快速借款投資套利。

這次 Euler Finance 遭到攻擊的部分，就是其閃電貸智慧合約的安全漏洞，在借出資金後竄改借貸額度，在數秒後還款金額遠低於借貸出來的資產金額，藉以獲得極大的不法所得。

資安專家指出，這次攻擊所使用的漏洞，發生在 Euler Finance 在資金驗證機制上未能完整驗證的漏洞。駭侵者同時扮演借貸者與平倉者兩種角色，

透過相互操弄， 以閃電貸借出 3000 萬美元的 DAI，在利用該漏洞後，獲得高達 880 萬美元的不法獲利。

雖然駭侵者使用的以太幣數位錢包已遭到追蹤，理論上可以掌握所有金流，但也有專家指出駭侵者早已先一步使用遭到多國禁用加密貨幣混合服務 Tonardo Cash 來進行洗錢因此仍然難以追蹤。

建議加密貨幣交易協定應更加嚴格審視智慧合約的安全性，並交由專業區塊鏈資安公司進行稽核，以儘量減少這類漏洞的存在。

- 資料來源：
  1. Euler Labs @eulerfinance
  2. Euler Finance Loses $199 Million in Flash Loan Attack
  3. Hackers steal $197 million in crypto in Euler Finance attack

3.3、國際政府組織資安資訊

3.3.1、美國聯邦調查局調查國會人員資料遭竊事件

美國聯邦調查局 (Federal Bureau of Investigation, FBI) 目前正在調查一起與美國國會議員與工作人員相關的個資外洩事件；該起資安事件肇因於一家專門服務美國國會議員、工作人員與家屬的醫療機構 DC Health Link 遭到駭侵攻擊，導致上述人員的個資被竊。

據首先報導本事件的媒體 DailyCaller 指出，美國國會行政單位立即發送電子郵件通報給所有可能遭到影響的人員，在信中表示 DC Health Link 於近日遭到嚴重駭侵攻擊，導致該機構數千名客戶的個人身分可辨識資訊 (Personal Identifiable Information) 遭到外洩。

該信也指出，目前並不清楚這次攻擊的影響範圍有多大，但 FBI 已指出包括國會議員與相關工作人員的個資已遭竊取。

該信也表示，目前的資訊顯示這次攻擊行動並非專門鎖定國會議員進行攻擊。

據資安專業媒體 Bleeping Computer 指出，這批 DC Health Link 的遭竊資料，至少有一部分已經遭到一個稱為 IntelBroker 的駭侵者貼上某駭侵論壇加

以出售；在駭侵者公布的這批資料表頭顯示，這批資料一共包括 17 萬個用戶帳號，資料欄位包括姓名、出生年月日、住址、Email 地址、電話號碼、社會安全碼 (Social Security Number, SSN) 等多達數十種資料。

駭侵者 IntelBroker 要求購買者以難以追蹤金流的 Monero (XMR) 加密貨幣來購買，購買所需金額則沒有透露；駭侵者也說至少已有一個買家購買了該批資料。

建議存有大量用戶機敏資訊的單位，應全面加強各項資訊系統的資安防護層級，並將資料庫內的資訊加密儲存，以免遭竊後造成機敏資訊外洩。

- 資料來源：
  1. Henry Rodgers @henryrodgersdc
  2. FBI investigates data breach impacting U.S. House members and staff

3.3.2、烏克蘭警方破獲以冒充遊戲程式進行木馬植入的駭侵者

烏克蘭網路警察宣佈逮捕一名涉嫌製作遠端存取木馬（RAT）惡意軟體的開發者；該惡意軟體對外冒充為遊戲應用程式，已感染多達一萬多台電腦設備。

警方指出，該惡意軟體開發者將其惡意軟體偽裝為電腦遊戲；在警方捕獲該嫌犯時，該駭侵者已可即時存取 600 台遭感染的電腦，且能自受害者處下載檔案，竊取各種安全憑證、植入各種惡意軟體酬載、遠端安裝或刪除任何程式、竊取螢幕截圖，並攔截電腦麥克風和攝影機取得的聲音或影片。

駭侵者竊得這些資料後，也存取受害者的帳戶，以竊取「電子資金」，但目前還不清楚被竊的是網路銀行存款還是加密貨幣資產。

警方在搜索駭侵者住處時，發現了該駭侵者用於操作惡意軟體並發動工具的電腦系統；這些裝置目前已遭警方沒入並展開進一步的調查。目前還不清楚受害者是否僅限於烏克蘭境內，或包括其他國家的電腦與使用者。

烏克蘭警方並未提供有關駭客如何散布惡意軟體的詳細資訊。以往類似的惡意軟體，多半以透過 YouTube 影片來宣傳其偽造的遊戲外掛模組、作弊工具，也會藉由 Google 關鍵字廣告、惡意廣告、社群媒體行銷活動、直接訊

息傳遞和電子郵件等方式來進行散布。

被捕嫌犯現在面臨刑事控告，罪名是違反烏克蘭犯罪法第 361 條第 5 段之未經授權進行（自動化）資訊、電子通訊、資訊和通訊系統以及電子通訊網路的干擾。上述最高刑責為 15 年有期徒刑。

烏克蘭警察持續在努力應對日漸猖獗的網路犯罪活動，破獲多起網路犯罪案件，包括僵屍網路、勒贖團體，以及針對該國政府與能源基礎設施的多起攻擊事件。

鑑於假冒為遊戲或付費應用程式破解版的惡意軟體愈來愈多，各用戶應完全避免安裝來路不明的所謂破解版、註冊機或外掛程式，以確保不受惡意軟體植入。

- 資料來源：
  1. Кіберполіція викрила жителя Хмельниччини у створенні «вірусу» для викрадення даних користувачів
  2. RAT developer arrested for infecting 10,000 PCs with malware

3.4、社群媒體資安近況

3.4.1、全新惡意 ChatGPT Chrome 擴充套件，會盜走 Facebook 帳號控制權

資安廠商 Guardio 旗下的資安研究人員，近期發現一個正常的 Google Chrome 擴充套件 ChatGPT for Google，遭到駭侵者植入惡意程式碼，以竊取用戶的 Facebook 帳號控制權。

研究人員發現這個 Google Chrome 擴充套件，在 Google Chrome web store 上相當受歡迎，目前已有超過 9000 次以上的下載安裝次數。

研究人員指出，該擴充套件首次於 2023 年 2 月 14 日上架到 Chrome Web Store，但一個月後才開始在 Google 搜尋頁面投放關鍵字廣告，之後每天都有上千次下載安裝數量。

研究人員發現該擴充套件在使用時，會連線到先前已遭 Google 移除的惡意擴充套件相同的伺服器；該惡意擴充套件同樣也是宣稱以提供 ChatGPT 功能為號召，因此研究人員認為新的惡意擴充套件是與舊版相同的攻擊活動。

用戶點按搜尋引擎上顯示的廣告後，會連到一個假冒的詐騙 ChatGPT for Google 頁面，再導向到該套件在 Chrome Web Store 上的安裝頁面；用戶安裝該套件後，雖然確實可以使用 ChatGPT 提供的服務，但套件中的惡意程式碼

會試圖竊取用於存在瀏覽器中的 Facebook session cookie，導致駭侵者取得受害者的 Facebook 帳號控制權。

駭侵者隨即會竄改使用者設定的登入密碼，導致用戶無法再次存取自己的 Facebook 帳號，甚至還會把用戶的個人顯示名稱與大頭貼改掉。

鑑於 ChatGPT 等生成式 AI 工具近期引發的熱潮，許多駭侵者以此名目進行冒名詐騙攻擊，投放各式假冒 App、擴充套件或釣魚網站；建議用戶在搜尋使用這類工具時，必須提高警覺，避免使用非官方出品的 App、擴充套件或網站。

- 資料來源：
  1. “FakeGPT”: New Variant of Fake-ChatGPT Chrome Extension Stealing Facebook Ad Accounts with Thousands
  2. Facebook accounts hijacked by new malicious ChatGPT Chrome extension

3.4.2、資安專家遭駭侵者於 LinkedIn 鎖定發動惡意軟體植入攻擊

資安廠商 Mandiant 近日發表研究報告指出， UNC2970 駭侵團體近來針對美國和歐洲境內的資安研究人員與媒體發動攻擊，手法是透過 LinkedIn 發送詐騙工作機會給攻擊對象，藉以植入全新惡意軟體。

據 Mandiant 的報告指出，駭侵者先在 LinkedIn 假裝為獵才中的人力資源人員，以相當優渥的工作機會和薪酬，引誘被列為攻擊目標的對象與其聯絡，在雙方「相談甚歡」後，再引誘對方改用 WhatsApp 進行溝通，然後對受害者投放三種全新的惡意軟體，以進一步入侵受害者服務中的單位。

Mandiant 表示，觀察到駭侵者會冒用許多知名公司（如紐約時報）來發送工作說明書 Word 檔案給受害者；而該 Word 檔的巨集會執行遠端範本注入，自某個遭到挾持用以當作駭侵控制伺服器的 WordPress 網站中，取得一份已經遭到修改為木馬的 TightVNC，將其改名為「LidShift」安裝在受害者的電腦上。

接著 LidShift 會載入一個修改自 NotePad++ 外掛程式的加密 DLL （稱為「LidShot」）作為惡意軟體下載安裝工具，將其安裝到系統記憶體中，接著載入另一個全新的客製化惡意軟體安裝工具「TouchShift」，偽裝成合法的

Windows 二進位檔，接著就利用各種惡意軟體模組來進行鍵盤記錄、螢幕擷取、隧道通訊、後門監控，還能進一步下載更多惡意軟體模組。

建議各企業員工在 LinkedIn 上應對不正常高薪酬的工作機會提高警覺，當對方要求到其他防護能力較差的社群平台上溝通時，應立即拒絕並斷絕溝通往來，同時切勿開啟任何對方傳送的不明檔案與連結。

- 資料來源：
  1. Stealing the LIGHTSHOW (Part One) — North Korea's UNC2970
  2. Security researchers targeted with new malware via job offers on LinkedIn

3.4.3、駭侵論壇 Breached 因擔心遭 FBI 鎖定而關閉

駭侵攻擊相關論壇 Breached 近日宣布關閉，不再提供交流，原因是管理者認為該網站的伺服器很可能已遭司法單位掌握。

Breached 駭侵論壇過去專門提供駭侵者放置竊自各企業、政府單位或其他組織的資料，供駭侵者展示並販賣。由於這些功能，Breached 吸引了各式網路犯罪分子，包括勒贖團體、資料竊取者、資安研究人員、黑帽駭客、或是對網路犯罪技術有興趣的各色人等。

過去有許多著名的駭侵攻擊行動，包括資料竊取、勒贖攻擊等，都與該網站有關，受害者包括許多大型公司，例如 DC Health Link、Twitter、RobinHood、Acer、Activition 等。

該論壇是在一個已遭破獲的駭侵論壇 RaidFuroms 之後成立的，RaidForums 也和許多大規模資料竊取案件有關，並於去（2022）年 4 月遭到美國聯邦調查局 (Federal Bureau of Investigation, FBI）破獲，其創辦人 Omnipotent 在倫敦落網。

Breached 論壇是在上周五開始停止服務，原因是其創辦人兼擁有者 Pompompurin 在三月中遭到 FBI 逮捕，罪名為協助他人販賣未經授權的存取

工具。

在 Pompompurin 被捕後，該網站管理人員 Baphomet 曾試圖先關站，然後將論壇網站搬遷到另一難以追蹤的網路主機，以逃避司法追緝；但 Baphomet 後來表示連該主機都可能遭到司法單位掌握，因此取消了復站計畫。目前論壇上的參與者都轉往 Telegram 頻道上繼續互動。

建議擁有各種機敏資訊的單位，應加強資安防護能力，以免其機敏資訊遭到竊取後，被放上這類網站外洩或販賣。

- 資料來源：
  1. Breached hacking forum shuts down, fears it's not 'safe' from FBI
  2. Alleged BreachForums owner Pompompurin arrested on cybercrime charges

3.5、行動裝置資安訊息

3.5.1、Android 更新修復 60 個資安漏洞，包括 2 個嚴重遠端任意程式碼執行漏洞

Google 日前推出 2023 年 3 月 Android 資安更新，共修復多達 60 個資安漏洞，其中包括 2 個嚴重等級的遠端任意程式碼執行漏洞，影響 Android 11、12、13 等版本。

這次的更新以兩波推出，分別是 2023-03-01 與 2023-03-05；第一波包括 31 個 Android 元件如 Framework、系統與 Google Play 的更新；第二波則包括 29 個位於 Android 核心與 MediaTek、Unisoc、Qualcomm 等第三方廠商元件的更新。

Google 指出，在第一波更新中，有一個存於 Android 系統的漏洞最為嚴重，可在無需用戶互動，也不需提升執行權限的情形下，遠端執行任意程式碼；另有兩個危險程度評級為「嚴重」等級的遠端執行任意程式碼漏洞 CVE-2023-20951、CVE-2023-20954，Google 為了避免其遭駭侵者利用，未提供相關資訊。

而在第二波更新中兩個嚴重等級的漏洞 CVE-2022-33213 與 CVE-2022-33256，則是存於 Qualcomm 未公開源碼的元件，分別發生在 Qualcomm 的

Data Modem 與 Multi-code Call Processor 中。這兩個漏洞將由 Qualcomm 另行提供說明與更新方式。

第二波中其他來自 Qualcomm、MediaTek 和 Unisoc 的漏洞，Google 在其資安通報中也表示，解決方案也將由各由各原廠自行提供。

Android 裝置用戶可按下「設定」-> 「系統」->「系統更新」->「檢查更新」或「設定」->「安全性與隱私」->「更新」->「安全性更新」等來進行更新，以修補已知漏洞。至於 Android 10 用戶，由於該系統已結束其生命周期，因此將無法取得安全性更新；建議升級至搭載最新版本 Android 系統的裝置。

- 資料來源：
  1. Android Security Bulletin—March 2023
  2. March 2023 Security Bulletin

3.5.2、資安廠商發現「拼多多」官方 App 利用 Android 0-day 漏洞竊取用戶機敏資訊

資安廠商 Lookout 近期發表研究報告，指出該公司旗下研究人員發現電商網站「拼多多」在第三方應用程式商店上架的官方 Android App，內含數個 0-day 漏洞；資安研究人員指出拼多多涉嫌利用這些 0-day 漏洞竊取並監控用戶。

資訊技術網站 Ars Technica 報導引用 Lookout 資安研究人員提供的資訊，指出至少有兩個非 Google、Apple 官方應用程式商店中的拼多多官方 App，含有可利用 Android 0-day 漏洞 CVE-2023-20963 的惡意程式碼。該漏洞已在本（2023）年三月初由 Google 發行的 Android 資安更新中完成修復。

Lookout 的資安研究人員指出，駭侵者可利用此漏洞來提升執行權限，並自控制伺服器中下載額外的惡意程式碼，以提升過後的權限來執行。Lookout 也指出，用以簽署兩個遭發現含有惡意程式碼拼多多官方 App APK 的私鑰，也用在該公司上傳到 Google Play Store 中不含惡意程式碼的 App 簽署。

在 Ars Technica 報導 Lookout 的發現數日之前，Google 便已接獲多個資安研究人員反應，指出包括拼多多在內的多家電子商務網站，在第三方應用程式商店上架的 App 版本均內含惡意程式碼；Google 因而在其 Android 裝置的資安防護機制 Google Play Protect 中新增對這些應用程式的阻擋，用戶將無

法安裝這些 App；已安裝者也會收到刪除通知。

由於在中國境內無法存取 Google 官方 Play Store，因此拼多多 Android App 在如三星、華為、Oppo、小米等第三方應用程式商店中上架。

建議 Android 手機用戶除應盡可能避免在不明來源下載任何 App 外，也應隨時依原廠更新通知進行手機作業系統更新。

- 資料來源：
  1. Android app from China executed 0-day exploit on millions of devices
  2. Android app from China executed 0-day exploit on millions of devices

3.6、軟體系統資安議題

3.6.1、ChromeLoader 惡意軟體以假冒任天堂與 Steam 破解版遊戲攻擊玩家

南韓資安廠商 AhnLab Security Emergency Response Center (ASEC) 日前發表研究報告，指出該公司最近偵測到一個針對遊戲玩家的全新一波攻擊活動，以假冒任天堂與 Steam 破解版遊戲虛擬主機硬碟檔 (Virtual hard disk, VHD) 的形式來散布；玩家如不慎安裝，會遭到植入 ChromeLoader 惡意軟體，遭到駭侵者以多種方式發動後續攻擊。

ASEC 的報告中指出，ChromeLoader 是在 2022 年發現的瀏覽器挾持惡意軟體，原本的功能是竊取各種登入資訊，但在多次改版之後，加入更多攻擊可能性；除了竊取機敏資訊以外，也能布署惡意軟體，或是在系統中投擲「解壓縮炸彈」，導致用戶嚴重損失。

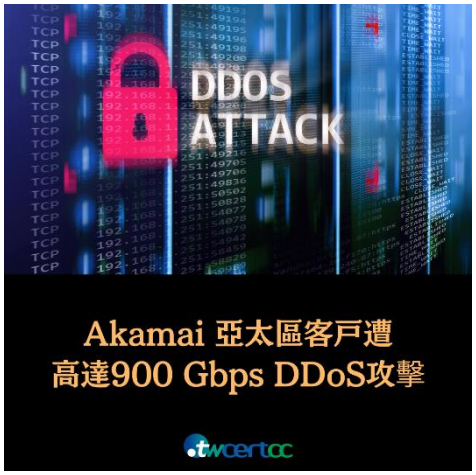
ASEC 指出，這波攻擊以各種熱門 Nintendo 與 Steam 平台上遊戲的破解版為誘餌，吸引想免費玩遊戲大作的玩家上鉤；遭到冒名的遊戲包括「艾爾登法環」(Elden Ring)、黑暗靈魂三 (Dark Souls III)、碧血狂殺二 (Red Dead Redemption 2)、極速快感 (Need for Speed)、決勝時刻 (Call of Duty)、薩爾達傳說：曠野之息 (The Legend of Zelda: Breath of the Wild)、瑪利歐賽車 8 豪華版 (Mario Kart 8 Deluxe)、超級瑪利歐 奧德賽 (Super Mario Odyssey) 等，甚至

也包括工作用軟體 Microsoft Office 與 Adobe Photoshop 在內。

為避免電腦遭到惡意軟體植入發動攻擊，建議各單位與個人應避免自不明來源處下載號稱破解版的軟體或遊戲，也不要下載使用所謂「註冊機」。

- 資料來源：
  1. ChromeLoader Disguised as Illegal Game Programs Being Distributed
  2. ChromeLoader Malware Targeting Gamers via Fake Nintendo and Steam Game Hacks

3.6.2、Akamai 亞太區客戶遭高達 900 Gbps DDoS 攻擊



網路基礎建設供應商 Akamai 日前表示，該公司某一位在亞太地區的客戶，日前遭到強大的分散式服務阻斷 (Distributed Denial of Service, DDoS) 攻擊，攻擊強度峰值最高達 900.1 Gbps 以上，所幸 Akamai 成功阻擋該次攻擊，未造成該客戶網路服務中斷。

DDoS 攻擊方式為針對目標網站，在短時間內發動大量垃圾連線請求，受害者的網路伺服器難以負荷之下，造成服務中斷、App 停止運作等攻擊效果；駭侵者通常會因為各種原因如政治訴求、報復、地緣政治因素或對受害者進行勒贖等原因而發動攻擊。

Akamai 指出，這次攻擊活動發生在本 (2023) 年 2 月 23 日，持續時間約 1 分鐘左右，攻擊量高達 900.1 Gbps，每秒的資料封包數量高達 1.582 億個，成為該客戶有史以來遭到最強烈的 DDoS 攻擊行動。

據 Akamai 的分析結果指出，這波攻擊行動由該公司的流量清洗網路成功化解，主要的流量被清洗到該公司設於香港、東京、聖保羅、新加坡、大阪等地的中心。

Akamai 也表示，這波攻擊中有 48% 的惡意 DDoS 流量由其亞太區的流量清洗機制承受，但該公司全球 26 個流量清洗中心都參與攻擊對抗，沒有任

何一個流量清洗中心承受的流量超過總流量的 15%。

Akamai 指出，該目標客戶的網路服務在攻擊之下仍正常運作，並未受到直接或間接的影響。

到目前為止發生過的 DDoS 攻擊中，流量最大的是發生在 2021 年 11 月時，針對 Mircrosoft Azure 亞洲區發動的攻擊，當時的瞬間最大流量高達 3.47 Tbps。

有鑑於 DDoS 的強度日益提高，除了各易受攻擊的組織應有因應方案之外，建議一般用戶也應注意自身裝置的資安防護，以免遭惡意軟體植入，成為發動 DDoS 的僵屍網路一環。

- 資料來源：
  1. Akamai mitigates record-breaking 900Gbps DDoS attack in Asia
  2. Akamai Mitigates Record DDoS Attack in Asia-Pacific (900 Gbps)

3.7、軟硬體漏洞資訊

3.7.1、新發現 2 個 TPM 2.0 漏洞，可讓駭侵者竊取 PC 主機上的加密金鑰

資安廠商 Quarkslab 旗下的資安研究人員，近日發現 PC 主機板上的硬體安全機制 TPM 2.0 含有兩個安全漏洞，可讓駭侵者取得電腦中如加密金鑰之類的機敏資料，甚至加以覆寫。

TPM 2.0 是 Windows 11 在系統啟動時必須存有的硬體加密機制，可以加密儲存一些重要的加密金鑰、密碼與其他重要機敏資料，以供 Measured Boot、Device Ecnryption、Windows Defender System Guard (DRTM)、Device Health Attestation 等 Windows 內建的資安防護機制使用，以加強 Windows 系統的安全性。

Quarkslabs 發現的這兩個漏洞，分別為 CVE-2023-1017 與 CVE-2023-1018；CVE-2023-1017 屬於越界讀取漏洞，而 CVE-2023-1018 則是越界寫入漏洞。這兩個漏洞都源自某些 TPM 指令在進行參數特殊處理的錯誤，可讓未經授權的本地攻擊者以發送特製指令的方式，誘發這兩個漏洞發生錯誤，進而透過 TPM 來執行程式碼，藉以竊得機敏資訊，甚至提高執行權限。

開發 TPM 機制的 Trusted Computing Group 組織，針對這兩個漏洞推出新版 TPM 標準，分別如下：

- TMP 2.0 v1.59 Errata 1.4 或後續版本
- TMP 2.0 v1.38 Errata 1.13 或後續版本
- TMP 2.0 v1.16 Errata 1.6 或後續版

- CVE 編號：CVE-2023-1017、CVE-2023-1018
- 影響產品(版本)：各廠商具備 TPM 2.0 晶片之主機板。
- 解決方案：建議用戶應儘量避免讓不明人士操作主機，且僅使用具備可信賴原廠安全簽章的應用程式，並在主機製造商推出新版韌體時立即更新。

- 資料來源：
  1. TPM 2.0 library memory corruption vulnerabilities
  2. TPM 2.0 Vulnerabilities
  3. New TPM 2.0 flaws could let hackers steal cryptographic keys

3.7.2、Google Pixel 手機遭發現多達 120 個資安漏洞

據 Cybersecurityhelp 網站近期發布的 Google Pixel 安全漏洞通報指出，近期 Google Pixel 系列手機共發現多達 120 個資安漏洞。

這批多達 120 個資安漏洞中，以其危險程度評級來說，並沒有被列為「嚴重」(critical) 等級的資安漏洞；列為「高」(high) 等級的有 7 個、「中」(medium) 的有 1 個，其餘的都屬於「低」(low) 危險等級資安漏洞。

屬於「高」危險等級的有以下數個漏洞較值得注意：

- CVE-2023-21054：本漏洞屬於遠端執行任意程式碼漏洞，存於 Pixel 手機的 Modem 子元件未能針對輸入進行妥善檢查；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。
- CVE-2023-24033：本漏洞和上個漏洞同樣屬於遠端執行任意程式碼漏洞，存於 Pixel 手機的 Modem 子元件未能針對輸入進行妥善檢查；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。
- CVE-2023-21058：本漏洞和上個漏洞同樣屬於遠端執行任意程式碼漏

洞，存於 Pixel 手機的 Cellular 韌體子元件未能針對輸入進行妥善檢查；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。

- CVE-2023-21057：本漏洞和 CVE-2023-21058 同樣存於 Pixel 手機的 Cellular 韌體子元件，亦是未能針對輸入進行妥善檢查的漏洞；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。
- CVE-2023-42499：本漏洞存於 Pixel 手機的 modem 子元件，亦是未能針對輸入進行妥善檢查的漏洞；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。
- CVE-2023-42498：本漏洞存於 Pixel 手機的 Cellular 韌體子元件內，同樣也是未能針對輸入進行妥善檢查的漏洞；駭侵者可誘使用戶開啟特製檔案誘發此漏洞，遠端執行任意程式碼。
- CVE-2023-43043：本漏洞屬於 parse.c 和式中的整數溢位錯誤；駭侵者可將特製的資料傳入該應用程式內誘發此漏洞，遠端執行任意程式碼，並且完全控制受害裝置。

- CVE 編號：CVE-2023-21054、CVE-2023-24033、CVE-2023-21058、CVE-2023-21057、CVE-2023-42499、CVE-2023-42498 及 CVE-2023-43043 等
- 影響產品(版本)：使用 2023 年 3 月 1 日前韌體版本的 Google Pixel 手機。
- 解決方案：建議 Google Pixel 手機用戶應立即更新手機到最新版本，以修補這些漏洞。

- 資料來源：
  1. Multiple vulnerabilities in Google Pixel
  2. Dangerous Android phone 0-day bugs revealed – patch or work around them now!

3.7.3、Microsoft 推出 2023 年 3 月 Patch Tuesday 每月例行更新修補包

Microsoft 日前推出 2023 年 3 月例行資安更新修補包「Patch Tuesday」，共修復多達 83 個資安漏洞，其中有 9 個是屬於「嚴重」(Critical) 危險程度的漏洞，另有 2 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 修復的漏洞數量較上個月（2023 年 2 月）的 77 個資安漏洞略多一些，達 83 個；其中 9 個屬於嚴重等級的漏洞，分類上包括遠端執行任意程式碼、分散式服務阻斷 (Distributed Denial of Service, DDoS)，以及權限提升類型。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：21 個；
- 資安防護功能略過漏洞：2 個；
- 遠端執行任意程式碼漏洞：27 個；
- 資訊洩露漏洞：15 個；
- 服務阻斷（Denial of Service）漏洞：4 個；
- 假冒詐騙漏洞：10 個；

- Edge - Chromium 漏洞：1 個。

本月修復的 0-day 漏洞共有 2 個，其中第一個是 CVE 編號為 CVE-2023-23397 的 Windows Outlook 漏洞，屬於權限提升 (Elevation of Privilege) 漏洞。Microsoft 指出駭侵者可以透過特製的 Email 誘發此漏洞，強制受害裝置連線到遠端 URL 並傳輸該機的 Windows 帳號 Net-NTLMv2 雜湊值，讓駭侵者中繼到其他系統，並以此雜湊值通過驗證，並竊取系統內特定帳號的 Email 。目前已知該 0-day 漏洞已遭駭侵者廣泛用於攻擊活動。

第二個是 CVE 編號為 CVE-2023-24880 的 Windows SmartScreen 漏洞，屬於資安防護功能略過漏洞。Microsoft 指出駭侵者可以用這個漏洞來製作惡意檔案，該檔案具備跳過 Windows Mark of the Web 的安全防護功能。

- CVE 編號：CVE-2023-23397 等
- 影響產品(版本)：Microsoft 旗下多種軟體，包括 Windows、Office、Exchange 等。
- 解決方案：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. Security Update Guide
  2. Microsoft March 2023 Patch Tuesday fixes 2 zero-days, 83 flaws

3.7.4、Apple 修復舊款 iPhone 上的 WebKit 0-day 漏洞

Apple 近日發表 iOS 15.7.4 與 iPadOS 15.7.4，其中針對舊款 iPhone 與 iPad 上已遭大規模濫用於攻擊的一個 0-day 漏洞進行修復。

這個 CVE-2023-23529 0-day 漏洞發生在 WebKit 瀏覽器子系統中，屬於類型混淆漏洞；駭侵者可利用特製的網頁內容來誘發此漏洞，造成作業系統崩潰，進而取得足夠權限，在受害的 iPhone 或 iPad 上執行任意程式碼，也可以取得該系統控制權。

本漏洞的 CVSS 危險程度評分高達 8.8 分（滿分為 10 分），危險程度評級為「高」（high）等級。

在此次更新中，Apple 強化了類型檢查的強度，以避免此漏洞的發生。

Apple 在 iOS 15.7.4 與 iPad 15.7.4 的發行註記說明中表示，該公司已得知此漏洞已遭大規模用於駭侵攻擊的情報；不過在該說明中並未明確指出攻擊活動的相關情報。

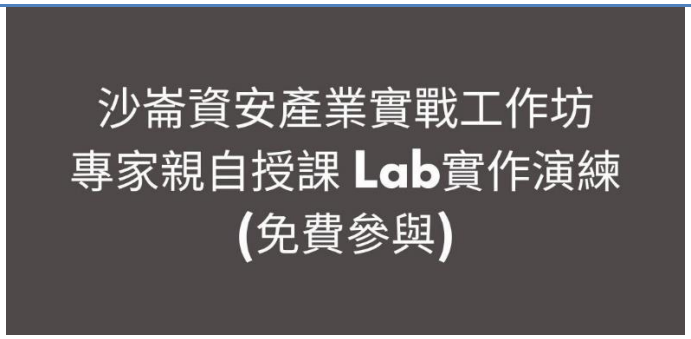
這個漏洞影響的 Apple iPhone 與 iPad 機型，以舊款為主，包括 iPhone 6s 所有機型、iPhone 7 所有機型、iPhone SE（第 1 代）、iPad Air 2、iPad mini（第 4 代）、iPod Touch（第 7 代）等。

除了上述的 CVE-2023-23529 0-day 漏洞外，Apple 在這次發行的 iOS 15.7.4 與 iPadOS 15.7.4 更新中，也修復了另外 15 個資安漏洞。

- CVE 編號：CVE-2023-23529
- 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）等。
- 解決方案：由於各款受影響 iPhone 與 iPad 仍有廣大使用者，建議用戶應立即進行系統軟體更新，以修補這些已發現的漏洞。

- 資料來源：
  1. About the security content of iOS 15.7.4 and iPadOS 15.7.4
  2. Apple fixes recently disclosed WebKit zero-day on older iPhones

第 4 章、 資安研討會及活動

【沙崙資安產業實戰工作坊】專家親自授課 Lab 實作演練	
活動時間	**3/23 (四)-3/24(五)、4/6 (四)-4/7(五)、4/17 (一)**
活動地點	**資安暨智慧科技研發大樓 A122 會議室** **(台南市歸仁區歸仁十三路一段 6 號 1 樓)**
活動網站	**https://www.acw.org.tw/News/Detail.aspx?id=3275**
活動概要	 **主辦單位：ACW** 進入雲端服務的世代，如何建立強固的資安防護邊界，已成為在目前面對資安威脅的重要課題，本次規劃三場 Wrokshop 將從防守到攻擊，再由下(基層員工)至上(高階主管)，進行縱深防禦，建立資安防護的認知，掌握駭客思維建立資安防線；並搭配沙崙資安基地示範場域觀摩，展示實地佈建的資安產品與服務解決方案。 第一場：網路封包分析實務 凡走過必留下痕跡，帶你解密封包分析 2023/3/23 (四)-3/24(五) 9:00~16:00 (每日 6 小時，總課程時數 12 小時) 本課程將介紹網路通訊中常用通訊協定原理介紹、分析與應用，課程包含上機實作，透過課程教學與實務操作，解說資安分析工具詳細操作與使用，使學員熟悉封包擷取、BFP 過濾器及常用操作技巧，研判網路封包等行為。 ★ 適合網管設備維運人員、對網路除錯、網路安全、惡意程式分析有

興趣者。

第二場：網頁弱點分析實務 網頁被綁架!!學會網頁弱點分析就有救

2023/4/6 (四)-4/7(五) 9:00~16:00 (每日 6 小時，總課程時數 12 小時)

本課程將著重在網站應用服務，探討相關的安全性議題，介紹 OWASP Top 10 2021 所挑選出來的十大風險，同時搭配 Lab 實作環境學員學習如何評估一個網站的安全性，探討如何做好基本的網站應用程式安全防範，以降低網站被入侵的風險。

★ 適合網頁開發從業人員、執行弱點檢測/滲透測試人員、對網頁安全及 OWASP Web 相關有興趣者

第三場：重大資安事件根因分析與處理 資安主管必修，預防勝於治療

2023/4/17 (一) 9:00~16:00 (總課程時數 6 小時)

探討企業發生資安事件的根因，遇到資安事件時將如何快速應變及對策，從建立企業所需之資安意識，再到提升企業強化資安防護，需雙管齊下以擘劃安全的數位未來。

★ 適合資安主管、資安長

【注意須知】

1. 本活動參加者需自備筆電(windows 或 mac 皆適用)

2. 活動提供午餐及簡易茶點

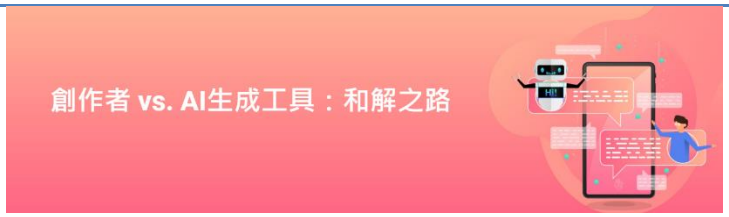
3. 3/24、4/7、4/17 課程結束將安排資安示範場域參訪

※ 活動聯絡人：06-3032260 分機 537 鄭小姐 / katrina@itri.org.tw

資安情資蒐集與分析實務班	
活動時間	**112 年 4/19-4/20，週三、四白天 9:30 ~12:00,13:00~16:30**
活動地點	**工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準**
活動網站	**https://college.itri.org.tw/Home/LessonData/B5466FB5-AC0D-4323-8626-8600A05BB798**
活動概要	 **主辦單位：工業技術研究院** 課程介紹：網路攻擊時有所聞，特別是 APT 組織與駭客集團經常使用惡意程式，繞過各種資安防護偵測系統，潛伏躲藏於被害人的內部網路。網路活動與惡意程式都會透過網路封包進行通訊傳輸，如何有效分辨異常網路封包活動(行為)?就需要培養網路封包分析能力，在巨量網路封包資料中，分析惡意程式與正常通訊封包的差異。 課程特色/目標：本計畫課程規劃以資安威脅情資所需實務技術進行介紹，並且搭配實際操作強化學員實作能力。 課程規劃內容以資安發展趨勢研析，所需要之背景知識為基礎，加上各式新型態應用服務為技術核心，能因應現今熱門之重點應用領域。 課程對象：資訊/資安技術人員、系統/網路安全工程師、資安決策技術主管/中高階主管 課程注意事項：請學員自備筆電上課 報名方式： 線上報名：到工研院產業學院官網報名

	課程洽詢：02-2370-1111 分機 609 或 306 黃小姐 報名截止日：2023/04/17

企業資安實務研討會	
活動時間	**112 年 4 月 19 日(三) 13:25-16:30 (13:00 開始報到)**
活動地點	**高雄軟體科技園區會議中心南區綜合大樓 A 棟 1 樓(中庭交誼廳)** **(806 高雄市前鎮區復興四路 12 號 A 棟)**
活動網站	**https://docs.google.com/forms/d/e/1FAIpQLSelgGSrWOtTaukU7uEEunR2G2BYtvwCthNUb32oGW5hlKne4Q/viewform**
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 隨著智慧製造的興起，為製造業帶來了高效率且靈活的生產模式，然資安問題成為了製造業面臨的重大挑戰。智慧製造系統需要在生產線上收集、儲存與傳輸大量的數據，若資料落 入未經授權的人員手中，可能導致重大損失。因此，智慧製造業者必須採取措施保障資安。這包括加強數據的加密、設置多重驗證機制、監測和紀錄系統活動、建立應變計劃等。藉由透過台灣電腦網路危機處理暨協調中心(TWCERT/CC) 及專業資安講師的案例分享與相關檢測介紹，強化智慧製造資安意識與防護，降低遭受駭客攻擊的風險。 注意事項： 1、請進入活動網頁進行報名。(研討會免費參加，全程參與者可開立研習證明) 2、即日起開始報名，實體與線上會議並行。 3、聯絡窗口：許小姐(07)5254346，E-mail：isrc@mail.nsysu.edu.tw

創作者 vs. AI 生成工具：和解之路	
活動時間	**2023 年 04 月 20 日 , 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/20230420/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 活動背景： 美國著作權局在今年 2 月 21 日的一封信函中表示，圖像式小說（graphic novel）中使用人工智慧（AI）工具 Midjourney 所產生的圖畫，不應受到著作權的保護；這也是首次針對 AI 生成作品著作權保護範圍提出裁定，在該裁定中認定一本名為「Zarya of the Dawn」作品的作者僅擁有該作品的部分著作權，由非人類創作的圖畫部分則排除在外，這些圖畫也不受著作權保護。臺灣的知名作家吳淡如也在年初於社群媒體貼出一張「電腦繪圖」作品，卻被網友揭穿該作品是 AI 生成繪圖，意外引發藝術創作者、網友對於著作權歸屬的討論。 無論是圖像、文字，或甚至由 ChatGPT 對話框中所生成的詩歌與故事劇本，到底 AI 所生成的作品算不算是原創作品，是否也可主張著作權，隨著生成式 AI 工具的熱度激增，也成為討論焦點。有看法認為，這些 AI 生成作品是由機器生成的，缺乏人類的創造性和主觀性，算不上是原創作品，也不該享有著作權；也有人主張，這些作品仰賴人類創作者提供設計想法，還是具備一定的獨創性，儘管 AI 在過程中可能提供了超越人類設計的想像與其他創意，不過人類創作者的主導與創造才是關鍵。

	美國著作權局日前所做出的認定，是否會成為普世價值或共識，目前還不得而知；但就在越來越多的新創公司募資數億美金投入相關應用開發之際，也出現越來越多的支持者與批評者以非常關切的語氣問道：這真的合法嗎？ 議程： 14:00-14:05 活動介紹 14:05-15:45 焦點座談 主持人 - 蔡志宏　庭長（台灣士林地方法院） 與談人 - 林思翰導演（Group.G 共同創辦人） 陳家駿理事長（台灣資訊智慧財產權協會） 馮震宇教授（政治大學科技管理與智慧財產研究所） 15:45-16:00 現場問答

物聯網資安韌性的基石-威脅與安全技術暨物聯網資安事件案例分享	
活動時間	
活動地點	
活動網站	**https://reurl.cc/1eG9E8**
活動概要	 **主辦單位：數位發展部數位產業署** 為讓學員能充份瞭解物聯網面臨之威脅與有效地建置物聯網安全相關技術。課程由簡介物聯網資安規範開場，學員先概括了解目前國內已制定完成的物聯網設備安全規範。接著藉由簡述過往所發生許多相關資安事件案例，強化學員物聯網安全威脅意識，並以如何有效運用安全技術建置物聯網設備安全功能為課程主軸。 (一)活動主題：物聯網資安韌性的基石-威脅與安全技術暨物聯網資安事件案例分享 (二)參加對象：物聯網相關領域企業中的開發人員、資訊人員或網管人員及一般民眾 (三)課程時間： ● 第一場(南部場)：2023/04/28(五) 08:30-12:30 (總課程實數 4 小時) / 台南沙崙 ● 第二場(中部場)：預計 7 月開課 (總課程實數 3 小時)。 ● 第三場(北部場)：預計 9 月開課 (總課程實數 3 小時)。

課程主軸：物聯網概論 / SBOM 檢測 / 裝置安全檢測指引

課程方式：實體&線上並行 (報名名額有限)

● 實體：資安暨智慧科技研發大樓 1 樓-A122 會議室 (台南市歸仁區十三路一段 6 號)

● 線上：Google Meet 線上授課 (上課前 5 日提供連結，寄發 email 給成功報名之學員)

報名截止時間：即日起至 4 月 21 日止 (全程完成研習課程並確實簽到者，結訓即頒發結業證明 4hr)

報名費用：免費參與

【注意須知】

1. 本次課程提供簡易茶點

2. 課程結束將安排 研習證明頒發 暨 資安示範場域參訪

3. 線上網址連結問題排除：連結若發生失效，請隨時留意信件寄發的更新連結

如有相關問題，請逕洽本案聯絡人：林怡夙小姐 07-525-0558

第 5 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：

桓基科技 HGiga OAKlouds - Arbitrary File Upload	
TVN / CVE ID	TVN-202303001 / CVE-2023-25909
CVSS	9.8 (Critical)
影響產品	桓基科技 HGiga OAKlouds OAKSv2 桓基科技 HGiga OAKlouds OAKSv3
問題描述	桓基科技 HGiga OAKlouds 上傳功能未對上傳檔案進行檢查限制，導致不須登入的遠端攻擊者可以上傳任意檔案，進而執行任意程式碼或中斷系統服務。
解決方法	- 更新入口網版面配置模組套件 OAKlouds-layout-2.0 到 OAKlouds-layout-2.0-10 - 更新入口網版面配置模組套件 OAKlouds-layout-3.0 到 OAKlouds-layout-3.0-10
公開日期	2023-03-02
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6973-45872-3.html**

四零四科技 MiiNePort E1 - Broken Access Control	
TVN / CVE ID	TVN-202303002 / CVE-2023-28697
CVSS	9.8 (Critical)
影響產品	Moxa MiiNePort E1 v1.7.2 Build 13012810
問題描述	Moxa MiiNePort E1 未適當進行權限控管，使遠端攻擊者不須權限，即可利用此漏洞進入系統設定介面，進行查看、修改或終止服務。
解決方法	MiiNePort E1 已於 2016 年釋出的 v1.8 中修復此弱點，請更新 MiiNePort E1 版本至 v1.8 以上。
公開日期	2023-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7021-eb43a-3.html

育碁數位科技 a+HRD - Deserialization of Untrusted Data	
TVN / CVE ID	TVN-202302011 / CVE-2023-20852
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD v6.8.1039V844
問題描述	育碁數位科技 a+HRD 之 MSMQ 解譯功能存在 Deserialization of Untrusted Data 漏洞，遠端攻擊者不須權限，即可利用此漏洞執行任意系統指令，藉以控制系統與終止服務。
解決方法	升級至 eHRD6.8.1039V920 以上版本
公開日期	2023-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7023-8368b-3.html

育碁數位科技 a+HRD - Deserialization of Untrusted Data	
TVN / CVE ID	TVN-202302012 / CVE-2023-20853
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD v6.8.1039V844
問題描述	育碁數位科技 a+HRD 之 MSMQ 非同步訊息處理功能存在 Deserialization of Untrusted Data 漏洞，遠端攻擊者不須權限，即可利用此漏洞執行任意系統指令，藉以控制系統與終止服務。
解決方法	升級至 eHRD6.8.1039V920 以上版本
公開日期	2023-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7024-bdefe-3.html

全景軟體 MOTP 行動動態密碼系統 - Path Traversal	
TVN / CVE ID	TVN-202303003 / CVE-2023-22901
CVSS	4.9 (Medium)
影響產品	全景軟體 MOTP 行動動態密碼系統 v3.11 以前版本
問題描述	全景軟體 MOTP 之參數存在 Path Traversal 漏洞，遠端攻擊者以管理者權限登入後，即可利用此漏洞繞過身分認證機制，讀取任意系統檔案。
解決方法	聯繫全景軟體進行版本更新
公開日期	2023-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7022-2cbe0-3.html

第 6 章、 2023 年 3 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。

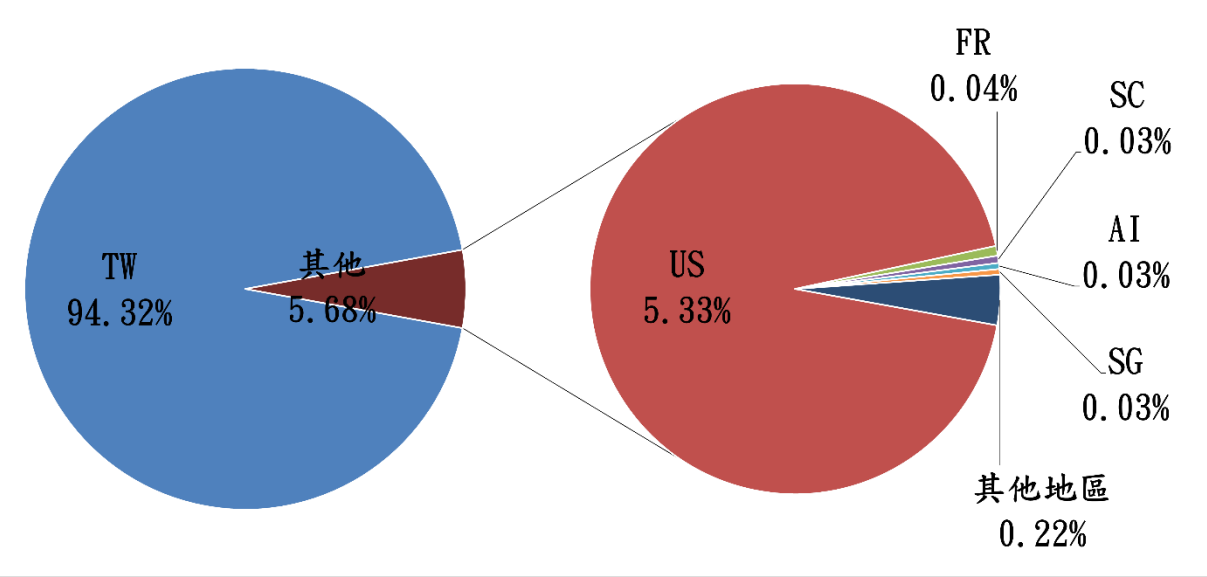


圖 1、分享地區統計圖

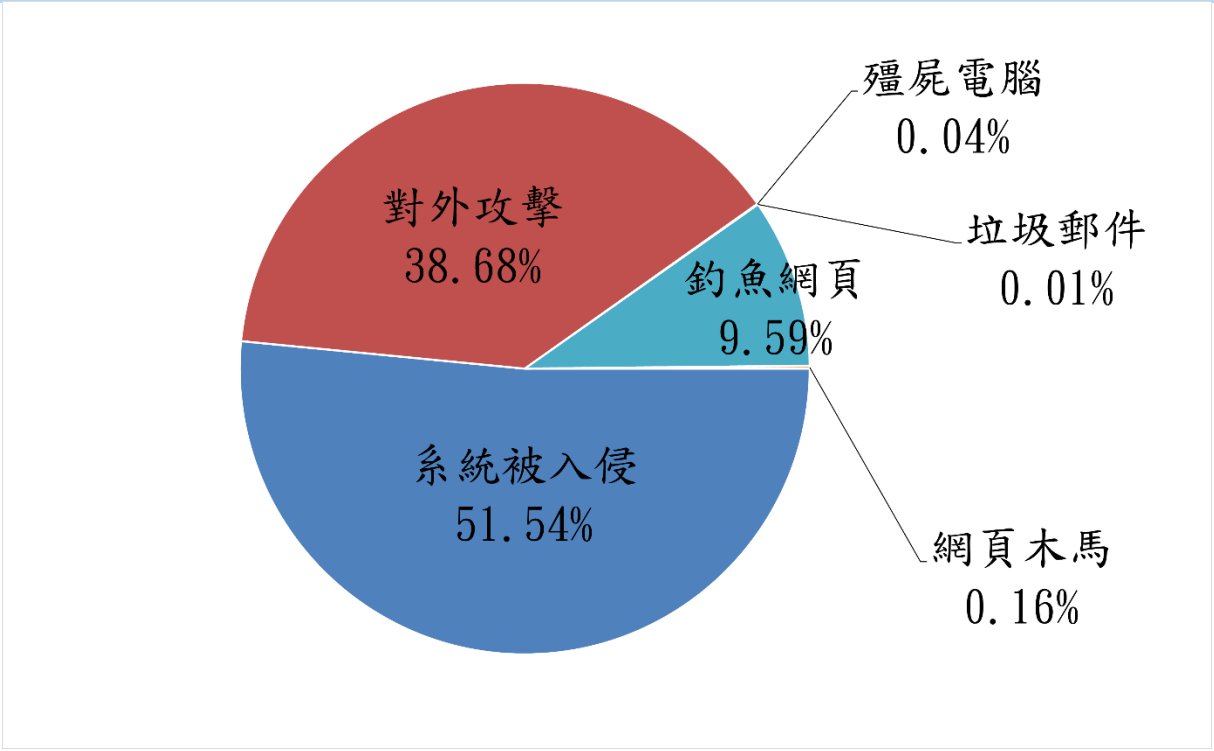


圖 2、分享類型統計圖

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 4 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**