TWCERT/CC 資安情資電子報

2023 年 3 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 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

Atlassian 發布 Jira 嚴重漏洞 CVE-2023-22501，並推出修補與暫時解決方案

SaaS 大廠 Atlassian 日前發表資安通報，指出旗下產品 Jira Service Management Server and Data Center 遭發現一個嚴重漏洞 CVE-2023-22501；該漏洞在某些情形下，可導致未授權駭侵者假冒其他用戶登入，並取得遠端連線能力以存取系統。

Atlassian 在資安通報中指出，在對用戶目錄的寫入權限與外送 Email 都為啟用狀況下，Jira Service Management 實例可能會遭到攻擊者使用從未登入的帳號，以傳送給用戶的註冊 token 取得系統存取權限，而駭侵者可以透過兩種方式輕易取得該註冊用 token。

該 CVE-2023-22501 漏洞據 Atlassian 自行評估，其 CVSS 危險程度評分高達 9.4 分（滿分為 10 分），其危險程度評級也高居最危險等級的「Critical」。

Atlassian 指出，這個漏洞所影響的 Jira Service Management Server 和 Data Center 版本為 5.3.0、5.3.1、5.3.2、5.4.0、5.4.1、5.5.0 等。Atlassian 已推出 5.3.3、5.4.2、5.5.1 和 5.6.0 等，將此漏洞修補完成；如果無法立即升級版

本，Atlassian 也備有對應各版本的專屬修補軟體，以做為對應該漏洞的暫時解決方案。

Atlassian 指出，即使用戶的 Jira Service Management Server and Data Center 係布署於不直接連通外網的防火牆內，或透過單一登入 (SSO) 存取外部用戶目錄者，也應立即套用更新。

- CVE 編號：CVE-2023-22501
- 影響產品：Jira Service Management Server 和 Data Center 版本 5.3.0、5.3.1、5.3.2、5.4.0、5.4.1、5.5.0。
- 解決方案：升級至 5.3.3、5.4.2、5.5.1 和 5.6.0 等版本。無法立即升級版本時，可至 Atlassian 下載安裝對應各版本的專屬修補軟體，以做為對應該漏洞的暫時解決方案。

- 資料來源：
  1. Jira Service Management Server and Data Center Advisory (CVE-2023-22501)
  2. Atlassian warns of critical Jira Service Management auth flaw

第 2 章、 國內外重要資安事件

2.1、資安趨勢

資安廠商發表 2022 年勒贖軟體 14 大攻擊目標研究報告

資安廠商 Sophos 日前發表研究報告，指出 2022 遭到勒贖攻擊最嚴重的 14 大目標，分別是媒體、娛樂與休閒產業、零售業、能源與公用事業、物流與運輸、企業與專業服務、醫療產業、高等教育、營建業與物業管理、IT 科技與電信業、中央及聯邦政府、地方與州政府、初級教育、製造業、金融業等。

媒體、娛樂與休閒產業高居 14 大目標的第一位。據統計指出，2022 年這些產業遭勒贖攻擊較前一年上升高達 147%，且在 12 個月內有高達 79% 曾遭勒贖攻擊。第二名的零售業在 2022 年中有 77% 曾遭勒贖攻擊，其中包括瑞典連鎖超市 Coop，曾因勒贖攻擊其收銀系統而被迫關閉 800 家門市達 3 天之久。

第三名是能源與公用事業，2022 年有 75% 業者曾遭勒贖攻擊；最著名的案例就是 Colonial Pipeline 遭駭，造成美國東岸的燃油供應中斷數日之久。第四名的物流與運輸業，在 2022 年有 74% 業者亦曾遭勒贖攻擊；而在 Sophos

的調查中，物流運輸業在支付贖金後，能救回的資料比例也最低，僅能救回 50% 資料。

第五名的企業、專業與法律服務業，也有高達 73% 在去年曾遭攻擊。資安專家指出多數企業未能隨時更新其使用軟硬體，同時也缺乏資安人員，以致經常遭到損失或快速支付贖款。

之後的行業排名與其遭勒贖攻擊比例如下：

其他：69%、醫療產業：66%、高等教育：64%、營建與物業管理：63%、IT、科技與電信：61%、中央/聯邦政府：60%、地方/州政府：58%、初等教育：56%、製造業：55%、金融業：55%。\

各行各業平均遭勒贖攻擊比例高達 66%，可見勒贖攻擊之為害甚烈，幾乎人人都是受害者。

勒贖攻擊的對象已從早期以金融與大企業為主，發展至今可謂無差別攻擊，人人都可能遭到勒贖攻擊；因此建議不論組織或個人都須提高資安防護能力與意識，並且隨時更新所使用的軟硬體至最新版本。

- 資料來源：
  1. Top 14 ransomware targets in 2023 and beyond
  2. The complete guide to ransomware

2.2、新興應用資安

2.2.1、電動車充電樁通訊協定遭發現存有漏洞，可導致遠端關機、資料與電力遭竊

以色列資安廠商 SaiFlow 近日發表研究報告，指出該公司發現多種電動車充電系統的舊版通訊協定，內含兩個資安漏洞，可能導致駭侵者遠端關閉充電樁，甚至用以竊取資料與電力。

被發現存有漏洞的電動車充電通訊協定為 Open Charge Point Protocol (OCPP) 1.6J 版本；該通訊協定使用 WebSocket ，讓電動車充電樁與管理系統 (Charging Station Management System, CSMS) 服務提供者進行溝通。

SaiFlow 指出，OCPP 標準並未明確定義在已啟用與充電樁連線的情形下，CSMS 應如何接受來自充電樁的新連線要求；這種對於多個已啟用連線操作方式缺乏明確定義的情形，導致駭侵者有機會藉由充電樁和 CSMS 間的通訊連線來下手發動攻擊。

SaiFlow 說，攻擊者可以冒充為一個已經建立連線的充電樁，對 CSMS 發動兩種攻擊：在 CSMS 供應商關閉原有連線並建立新連線時，對 CSMS 發動服務阻斷攻擊 (Denial of Service, DoS)、以及侵入並攔截 CSMS 與已連線充電樁之間的連線，以竊取充電中車主的各種個資，包括駕照資訊、信用卡號、CSMS 登入資訊等。

SaiFlow 也指出，新版的 OCPP 2.0.1 已經修補好這兩個漏洞，其做法為當單一充電樁同時進行多個連線時，進行更頻繁的充電樁登入資訊提供要求。

隨著電動車的快速普及，其相關基礎設施的資安也將更為重要。建議公用充電樁業者應加強充電樁暨管理系統的資安防護與軟硬體升級作業，以免成為駭侵攻擊的受害者。

- 資料來源：
  1. Hijacking EV Charge Points to Cause DoS
  2. Is Your EV Charging Station Safe? New Security Vulnerabilities Uncovered

2.2.2、加密貨幣詐騙 App 潛入 Apple App Store 與 Google Play

資安廠商 Sophos 旗下的資安研究人員，近日發表研究報告指出名為「Pig Butchering」（殺豬）的高報酬投資詐騙 App 兼詐騙攻擊活動，成功略過 Apple App Store 與 Google Play 等主流行動應用程式商店的防範，對受害者進行加密貨幣詐騙攻擊。

Sophos 在報告中指出，這個 Pig Butchering 詐騙活動，主要針對社群平台 Facebook 與交友平台 Tinder 上的男性受眾為主要攻擊對象，先以竊取來的照片設立假的女性用戶帳號，加上許多出入高級餐廳、休閒娛樂場所、一流旅遊景點、貴重物品商店的照片來取信潛在受害者；在得到受害者信任後，接者以該假帳號告知受害者，有親友在金融投資分析機構任職，邀請受害者加入加密貨幣投資計畫，並以高額報酬利誘，誘使受害者到 Apple App Store 或 Google Play 下載詐騙惡意 App。

報告也說明駭侵者成功略過 App Store 和 Google Play 的手法。惡意軟體開發者會先開發一個功能一切正常的 App，建置兩台介面相同的伺服器，但只有其中一台含有惡意程式碼。惡意軟體開發者接著上傳 App 送審，此時該 App 只會連到不含惡意程式碼的伺服器，以通過審查並成功上架；上架後再將 App 連線指向含有惡意程式碼的伺服器，以改變 App 功能。

受害者開啟變造過的 App 後，會看到一個來自惡意伺服器的加密貨幣交易介面，其中所有資料全是假的，以引誘受害者入金進行投資。

這類以高額獲利與美女引誘受害者進行詐騙的手法，自古以來皆十分有效；建議加密貨幣投資人應對來自社群媒體的可疑互動保持高度警覺，以免遭受損失。

- 資料來源：
  1. Fraudulent “CryptoRom” trading apps sneak into Apple and Google app stores
  2. Crypto scam apps infiltrate Apple App Store and Google Play

2.2.3、駭侵者以 16 個 NPM 詐騙測速程式套件來挖掘加密貨幣

資安廠商 CheckPoint 旗下的資安研究人員，近日發現一組共 16 個冒充為網路速度測試工具的 NPM 程式套件，表面上無害，但實際上會盜用受害電腦的資源，為駭侵者挖掘加密貨幣。

NPM 是網路上著名的開源 JavaScript 程式庫，內含 220 萬種以上的開源 JavaScript 程式套件，提供開發人員自由使用，以加速程式開發的速度。

CheckPoint 是在 2023 年 1 月 17 日時發現這些惡意程式套件，全都由一個用戶名稱為「trendava」的 NPM 帳號上傳到 NPM 程式庫中；該公司立即通報 NPM，NPM 則在隔日將這 16 個惡意程式套件下架。

這 16 個惡意 NPM 程式套件，名稱大多和網路速度測試有關，列表如下：

lagra、speedtesta、speedtestbom、speedtestfast、speedtestgo、speedtestgod、speedtestis、speedtestkas、speedtesto、speedtestrun、speedtestsolo、speedtestspa、speedtestwow、speedtestzo、trova、trovam。

CheckPoint 指出，這 16 個惡意軟體，雖然目的都是挖掘加密貨幣，但每個套件中惡意程式碼使用的手法都略有不同。CheckPoint 認為，駭侵者可能是要藉以觀察哪種方式比較不容易遭到防毒防駭機制發覺阻擋。

鑑於這類開放程式庫中經常混入駭侵者上傳的惡意套件，建議程式開發者在利用這些方便的套件前，必須先仔細檢視其 source code，以辨識其中是否夾帶惡意程式碼。

- 資料來源：
  1. Check Point CloudGuard Spectral detects malicious crypto-mining packages on NPM – The leading regist
  2. NPM packages posing as speed testers install crypto miners instead

2.3、國際政府組織資安資訊

2.3.1、美國資安主管機關 CISA 警示 Windows 與 iOS 0-day 漏洞已遭用於資安攻擊

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）日前發表資安通報，公告有 4 個分別屬於 Windows 與 iOS 的 0-day 漏洞，由於設備採用數量眾多，目前已遭駭侵者用於攻擊行動；該告也通令美國聯邦各單位機關，須於三週內完成資安修補。

這次由 CISA 公告的 4 個 0-day 漏洞，前兩個是發生在 Microsoft Windows 系統中，其一 CVE-2023-21823 存於 WIndows Graphics Component，可用以遠端執行任意程式碼；其二 CVE-2023-23376 是存於 Windows Common Log File System Driver 中，駭侵者可藉以提升自身執行權限。

CISA 公告的第三個 0-day 漏洞 CVE-2023-21715 同樣針對 Microsoft 產品，是發生在 Microsoft Office 中的 Microsoft Publisher 中，屬於資安防護功能略過漏洞。而第四個 0-day 漏洞 CVE-2023-23529 則發生在 Apple iOS、iPadOS、macOS 中的 WebKit，是一種型別混淆漏洞，可用於執行任意程式碼。

發生在 Microsoft 產品的 3 個 0-day 漏洞，已在本月 Microsfot Patch Tuesday 資安修補包中修復；而 Apple iOS、iPadOS、macOS 的 0-day 漏洞也已推出更新版本予以修復。

根據公告於 2021 年 11 月的具約束力操作指引 (binding operational directive) BOD 22-01 規定，在 CISA 公布新的已遭用於攻擊漏洞時，所有美國聯邦政府民事機關，都必須針對相關漏洞進行處理。

關於本次公布的四個 0-day 漏洞，CISA 要求各機關須於三個星期內完成修補工作，最遲不可超過 2023 年 3 月 7 日。此外，雖然 CISA 的規定只生效於美國聯邦機關，但該單位強烈建議所有公私單位，都應該依照 CISA 的指引，立即修補漏洞，以免遭到攻擊。

建議各公私單位的系統管理員與個人用戶，都應隨時注意所用系統軟硬體的更新訊息，儘速更新到最新版本，以避免駭侵者利用未及時更新的已知漏洞發動攻擊。

- 資料來源：
  1. KNOWN EXPLOITED VULNERABILITIES CATALOG
  2. CISA Cyber @CISACyber
  3. CISA warns of Windows and iOS bugs exploited as zero-days

2.3.2、荷蘭警方破解 Exclu 加密通訊平台，成功逮捕多名嫌犯

荷蘭警方於近日公開表示，成功駭入並破獲犯罪者愛用的 Exclu 加密通訊平台，透過監控其上通訊活動，結合多國警方通力合作，跨國逮捕多名嫌犯到案。

荷蘭警方說，該行動實際上包括兩波調查，分別在 2020 年 9 月與 2022 年 4 月進行；警方一共進行 79 次目標搜索行動，執行範圍遍及荷蘭、德國、比利時，一共逮捕 42 名嫌犯。

參與這次行動的，還包括歐洲檢察官組織 (Eurojust)、歐洲刑警組織 (Europol)，以及義大利、瑞典、法國、德國警方，有賴歐洲各國警力與檢調機關通力合作，才能成功緝獲這些犯罪份子。

在被捕的 42 人中，有兩人是該加密通訊平台 Exclu 的擁有人與營運者，其餘 40 人則是該平台的用戶，其中有人開設毒品製造地下工廠，不但擁有大量毒品，甚至還有許多槍械彈藥，以及高達 400 萬歐元的現金。

僅在荷蘭一地，警察就對 22 個地點發動搜索行動，逮捕 11 人。

荷蘭警方表示，Exclu 為完全會員制的加密通訊平台，半年使用費為 800 歐元，讓用戶可以透過加密方式互傳訊息與媒體檔案；由於該平台宣稱具備較熱門通訊服務更強的隱私保護，因此吸引許多需要秘密通訊的用戶，除犯

罪分子外，也有一些律師、醫師、調查人員等使用該平台。

警方表示這次出擊係利用各種駭侵破解技術，成功掌握 Exclu 上的所有通訊內容，再加以一一查核，才能成功逮捕多名犯嫌；但非犯罪份子的通話記錄也同時為警方掌握，引發隱私外洩疑慮。荷蘭警方說，Exclu 上的正常用戶可向警方申請，自伺服器上刪除其相關內容。

小型加密通訊平台或相關社群論壇，經常成為犯罪份子利用的工具；建議平台經營業者應思考如何避免成為犯罪工具，並以適當機制，在不影響用戶隱私的前提下，提早發現不法活動的跡象並及早通報。

- 資料來源：
  1. Politie leest opnieuw mee met criminelen
  2. Police hacked Exclu 'secure' message platform to snoop on criminals

2.3.3、歐洲刑警組織破獲「執行長詐騙」駭侵團體

歐洲刑警組織 (Europol) 日前宣布破獲一個由法國人與以色列人共同組成的駭侵團體，該團體透過企業 Email 攻擊，偽裝多家公司執行長發信指示員工匯款，進而騙取巨額不法所得。

Europol 指出，在該團體犯下的多起案件中，其中一件針對單一公司的攻擊不法所得就高達 3,800 萬歐元，約合 4,030 萬美元。

駭客為避免金流遭到追蹤，使用多重洗錢手法；不法所得輾轉經由歐洲、中國轉匯，最後匯到以色列進行提領。Europol 一共執行 8 次搜索行動，一共逮捕 6 名法國人和 2 名以色列人，查緝 510 萬歐元的銀行存款與 35 萬歐元加密貨幣。

Europol 表示，這次能夠順利破案，有賴 Europol 與多國警方與相關執法人員通力合作，包括 Eurupol 本身、法國、克羅埃西亞、匈牙利、葡萄牙、西班牙等國的檢警人員與資安專家都參與偵辦。

Euporol 指出，駭侵者發動的攻擊活動，屬於企業電子郵件攻擊 (Business Email Compromise, BEC)；駭客駭入目標企業的個人裝置或電子郵件系統，並監視公務通訊內容，當發現有大額轉帳付款時，便偽裝成企業執行長或該企業的客戶，並指示經辦人員將款項轉匯到駭侵者控制的銀行帳戶內。

2021 年 12 月時，這個駭侵團體也曾假冒法國一家大型治金工廠的執行長，成功將高達 30 萬歐元的款項以詐騙手法轉至匈牙境內的銀行帳戶；數日後該駭侵者試圖再次進行詐騙 50 萬歐元時，因該公司已報警而遭到攔截。

建議各公司行號的出納經辦人員，在收到可疑的轉帳目標改變命令時，務必提高警覺，於第一時間向主管與資安單位報告確認，以免發生巨額資金損失。

- 資料來源：
  1. Franco-Israeli gang behind EUR 38 million CEO fraud busted
  2. Europol busts ‘CEO fraud’ gang that stole €38M in a few days

2.3.4、挪威警方破獲大型 Axie Infinity 駭侵集團，查緝不法加密貨幣高達 580 萬美元

挪威警方 (Økokrim) 日前宣布破獲 Lazarus 駭侵團體在去年針對熱門區塊鏈遊戲 Axie Infinity 漏洞發動攻擊所竊得的大量加密貨幣資產，總值為 6000 萬克朗，相當於 580 萬美元。

Økokrim 指出，這筆加密貨幣贓款是由 Lazarus 駭侵團體，針對發行熱門區塊鏈邊玩邊賺遊戲 Axie Infinity 的發行公司 Sky Mavis，在 2022 年所進行的攻擊不法所得。Lazarus 於去年 3 月攻擊該遊戲的 Robin bridge 協定，對其部分區塊驗證者取得控制權後，隨即偽造兩筆未經授權的巨額交易，總損失金額高到 6.2 億美元。

Økokrim 說，這是在挪威緝獲的史上最高額贓款；在該局偵辦人員鍥而不捨地全力偵辦，查出不法分子的洗錢路徑，最後終於破獲部分該案被竊款項。

美國聯邦調查局 (Federal Bureau of Investigation) 指出，Lazarus 駭侵團體是在該案發生前數個月，以魚叉式釣魚攻擊手法，在求職網站上針對 Sky Mavis 員工展開假冒的挖角攻擊，要求受挖角員工填寫含有惡意程式碼的假冒履歷文件，使該駭侵團體可以入侵 Sky Mavis 的內部系統。FBI 說，這是 Lazarus 進行加密貨幣竊取攻擊的慣用手法。

Økokrim 表示，這次成功破案，有賴於多國警政與資安單位合作，才能順利破案；其中包括美國 FBI 專家支援追蹤駭客的加密貨幣轉帳路線。緝獲的贓款將交由 Sky Mavis 補償蒙受損失的用戶。

建議在金融業、加密貨幣產業或其他機敏事業單位工作的員工，需隨時對各種不明的郵件、檔案或連結提高警覺，以免成為魚叉式釣魚攻擊的對象，造成所屬組織與其用戶的巨額損失。

- 資料來源：
  1. Rekordhøgt kryptobeslag i Axie-saka
  2. Norwegian police recover $5.8M crypto from massive Axie Infinity hack

2.4、社群媒體資安近況

2.4.1、美國最高資安外交官的 Twitter 帳號遭駭

美國新任命的最高資安外交官 Nate Fick 日前表示，其個人使用的 Twitter 帳號遭到駭入；他稱此事為「因工作而帶來的威脅」。

Nate Fick 是由現任美國總統 Joe Biden 於去年 6 月宣布提名為新成立的「網路空間與數位政策局」(Bureau of Cyberspace and Digital Policy)，該單位直屬於美國國務院，由美國副國務卿擔任其主管，主要推動三方面的政策宣導與國際合作，包括國際資安 (International Cyberspace Security)、國際資訊與通訊政策 (International Information and Communication Policy) 以及數位自由 (Digital Freedom)。

目前尚不清楚駭侵者的身分、動機與背景，也沒有駭侵者利用遭駭 Twitter 帳號擅自發送貼文的跡象；不過 Nate Fick 指出他很少使用個人 Twitter 發文，如有必要發文，通常都使用美國國務院申請的單位官方帳號來發表推文。

Nate Fick 是美國海軍陸戰隊退役軍人，也曾擔任某民間資安公司執行長；目前是網路空間與數位政策局的局長。他在 2022 年 9 月上任，成為美國首位網路空間與數位政策無任所大使。

據 CNN 指出，該局的目標是結合美國的外交政策，在網路上提倡各種數位人權議題，以對應極權國家在網路上日漸擴張的聲量。

社群媒體帳號的安全性總有多種漏洞存在，也可能因各種原因遭到駭入或挾持，建議用戶避免在社群媒體上透漏各種機敏資訊。

- 資料來源：
  1. Nate Fick @ncfick
  2. America’s top cyber diplomat says his Twitter account was hacked

2.4.2、駭侵者侵入 Reddit 竊走原始碼與內部資料

美國大型社群論壇網站 Reddit 日前傳出遭到駭侵攻擊。據 Reddit 指出，駭侵者以高度目標釣魚手法，取得員工對內部系統的登入資訊後，入侵 Reddit 後台系統，取得部分內部資料與程式碼。

Reddit 在近日發表的資安通報中表示，該網站在 2 月 5 日稍晚發現遭到駭侵攻擊。駭侵者以高度成熟的釣魚攻擊手法，複製了 Reddit 內部專用系統的頁面，因此成功從某一 Reddit 員工處取得內部系統的登入資訊與二階段登入驗證碼，隨即取得 Reddit 的部分內部文件、程式碼，以及某些後台儀表板和管理系統資訊。

Reddit 表示，在該名員工主動通報後，該公司立即展開行動與調查，以防受害範圍擴大。目前沒有跡象顯示用戶的帳號與密碼遭竊，而 Reddit 產品系統(即用以執行 Reddit 主要功能並儲存多數資料的主機系統) 也並未遭受攻擊。

Reddit 也指出，在被竊的內部資料，可能包括數百名員工的個人資訊，以及某些廣告客戶的相關資料，但不包括信用卡、密碼與廣告績效表現等資料在內。該公司在經過內部調查後，目前認為並沒有任何公眾相關資料遭到駭侵者存取。

Reddit 指出，該公司認為這次攻擊的手法類似先前 Riot Games 遭到攻擊的事件；在該事件中，Riot Games 最熱門的「英雄聯盟」(League of Legends) 原始程式碼也遭到竊取，駭侵者很快要求該公司支付 1000 萬美元贖金，但遭到 Riot Games 拒絕。隨後 League of Legends 程式碼就出現在駭侵相關論壇中求售。

針對企業員工發動社交或釣魚攻擊，以取得內部系統登入資訊的攻擊手法日漸普遍，因此建議各單位組織除了須加強內部系統的資安防護層級外，也應加強員工、供應商等的資安教育訓練，避免成為攻擊破口。

- 資料來源：
  1. We had a security incident. Here’s what we know.
  2. Hackers breach Reddit to steal source code and internal data

2.4.3、Twitter 取消免費用戶簡訊二階段登入驗證，資安專家提供建議替代措施

大型社群平台 Twitter 日前宣布將逐步取消對未付費用戶以簡訊發送二階段登入驗證碼，僅有付費用戶可以透過 Twitter 直接收到簡訊驗證碼；為此資安專家提供多種更為安全的替代方案，以讓廣大的未付費 Twitter 用戶擁有更高的安全性。

Twitter 於日前在官方部落格發表的公告中指出，該平台將在 2023 年 3 月 20 日起，全面取消未持有 Twitter Blue 認證標誌用戶以簡訊收取二階段登入驗證碼的服務；未來只有付費取得 Twitter Blue 認證標誌的用戶，才可透過簡訊收取二階段登入驗證碼。

Twitter 執行長 Elon Musk 在自己的推文中指出，Twitter 每年因為假帳號產生的簡訊驗證碼費用高達 6,000 萬美元。

為維持用戶登入安全，Twitter 另外提供兩種替代方案，分別是採用軟體產生隨機二階段登入驗證碼，以及使用硬體安全金鑰。

資安專家指出，雖然很多人可能會批評 Twitter 取消簡訊驗證碼發送的措施，但從資安角度來看，這反而提高了用戶的帳號安全性。主因在駭侵者可透過多種方式，輕易攔截用戶接收的簡訊驗證碼，例如 SIM-Swap 攻擊，或透過用戶裝置中的惡意軟體來獲取驗證碼。

專家建議用戶可採用具備雲端備份功能的 Authy 或 Microsoft Authenticator 來產生 Twitter 專用的二階段登入碼，這樣即使手機遺失，也不會失去帳號的存取權限。

根據 Twitter 發表的帳號安全報告指出，在 2021 年 7 月到 12 月間，僅有 2.6% 的 Twitter 用戶啟用二階段登入驗證，比例極低；而在這批用戶中，有 74.4% 使用簡訊接收登入驗證碼，28.9% 使用驗證碼產生軟體，0.5% 採用硬體安全金鑰。

簡訊驗證碼的安全性較低，建議用戶可趁此機會改用 Authy 或 Microsoft Authenticator 等具雲端備份功能的二階段驗證碼產生工具，以提高帳號的資安防護能力。

- 資料來源：
  1. An update on two-factor authentication using SMS on Twitter
  2. Twitter gets rid of SMS 2FA for non-Blue members — What you need to do

2.5、行動裝置資安訊息

2.5.1、近 1,900 種釣魚個資竊取 Android 手機畫面覆疊模組，在駭侵論壇中出售

資安廠商 Cyble 旗下的資安研究人員，近來發表研究報告指出，該公司發現在俄羅斯駭侵相關論壇中，有一組名為「InTheBox」的駭侵團體，在論壇上出售一批多達 1,894 種網頁注入型手機惡意畫面覆疊模組；這些惡意畫面覆疊專門用於在 Android 手機上假冒各式服務官方網站，用以竊取用戶各類機敏資訊。

報告指出，這些假冒官網的覆疊畫面，主要用以竊取用戶在各大銀行、加密貨幣交易所或電子商務網站輸入的機敏資訊為主。

這批為數龐大的假冒網站惡意畫面覆疊和多種惡意軟體相容，包括有 814 種相容於 Alien、Ermac、Octopus、MetaDroid 惡意軟體（要價 6,512 美元）、495 種相容於 Cerberus 惡意軟體（要價 3,960 美元）、585 種相容於 Hydra 惡意軟體（要價 4,680 美元）。該駭侵者也提供單一網頁注入覆疊畫面銷售，一個要價 30 美元。

據 Cyble 的分析報告指出，InTheBox 的惡意畫面覆疊模組包含一個 App 用 PNG 圖檔，以及內含可竊取用戶機敏資訊 JavaScript 指令的 HTML 檔案。在大多數情形下，這些覆疊模組會蓋掉正牌官網的登入或資料輸入畫面，並

且竊取用戶輸入的資訊；該段 JavaScript 甚至能夠驗證用戶輸入的信用卡資訊是否有效。

Cyble 也指出，InTheBox 販售這類惡意覆疊畫面已有相當長的時間，這些惡意畫面也曾用於多次攻擊行動，最近一次是在 2023 年 1 月針對西班牙的銀行。

鑑於 Android 系統上這類假冒官網畫面覆疊的攻擊十分頻繁，建議 Android 用戶在點按任何連結或安裝應用程式時，都應特別提高警覺，檢查連結的正確性，並且避免下載來路不明或評價偏低的 App。

- 資料來源：
  1. ‘InTheBox’ Web Injects Targeting Android Banking Applications Worldwide
  2. Over 1,800 Android phishing forms for sale on cybercrime market

2.5.2、駭侵者利用假冒 ChatGPT App 植入 Windows、Android 惡意軟體

資安專家 Dominic Alvieri 日前發現，有駭侵者利用近來熱門的「生成式人工智慧軟體」(Generative AI software) ChatGPT 的熱潮，推出假冒 ChatGPT 的惡意 Windows 與 Android 軟體，以攻擊上當受騙的使用者，在其裝置中植入惡意程式，或是將使用者導向釣魚網頁。

由人工智慧新創公司 OpenAI 於日前公開發表的 ChatGPT，引發了全球性的 AI 熱潮，光在 2023 年 1 月就吸引超過 1 億名用戶試用。為了減少計算資源與頻寬的大量支出，OpenAI 推出每月收費 20 美元的進階版本 ChatGPT Plus，原先免費試用的版本則開始限制其可用次數。

資安專家指出，有多組駭侵者利用 ChatGPT 近來的熱潮，假冒其名義推出免費使用進階版本 ChatGPT Plus 的「服務」，藉以引誘用戶安裝內含惡意程式碼的假冒軟體。Dominic Alvieri 就發現名為 Chatteo AI Chat GPT 和 Smart AI Chatbot 的可疑 App 出現在 Google Play Store 和其他第三方 Android App Store 中，甚至刊登廣告，企圖混淆視聽，誘使用戶下載。

資安廠商 Cyble 也指出一個叫做 chatgpy-go.online 的網頁，也假冒成 ChatGPT，但實際上內含會竊取 Windows 剪貼簿內容的惡意程式碼，甚至含有一個名為 Aurora Stealer 的資訊竊取惡意軟體。

Cyble 進一步指出，根據該公司的統計，有超過 50 個以上的惡意 App 假冒 ChatGPT 的圖示，並使用類似名稱以魚目混珠，以在用戶裝置上安裝各種惡意軟體，用戶不可不防。

目前 ChatGPT 只有一個官方網址 chat.openai.com，而且未提供任何作業系統版本的桌面或行動 App；建議想使用 ChatGPT 的用戶必須特別提高警覺，勿使用任何不明來源網頁或應用程式，以免遭到駭侵攻擊。

- 資料來源：
  1. Dominic Alvieri @AlvieriD
  2. The Growing Threat of ChatGPT-Based Phishing Attacks
  3. Hackers use fake ChatGPT apps to push Windows, Android malware

2.5.3、Samsung 推出新防護機制，防止暗藏惡意程式碼的檔案以零互動方式感染 Galaxy 手機

南韓行動裝置大廠 Samsung 近日為旗下 Galaxy 系列行動裝置推出全新防護機制「Samsung Message Guard」，能夠阻擋聊天軟體傳來含有惡意程式碼的檔案，以「零互動」方式觸發裝置漏洞進行攻擊。

Samsung 指出，「Samsung Message Guard」功能，可立即分析透過各種訊息傳送過來的檔案是否具有資安威脅性，並在其造成破壞之前先行封鎖。

所謂「零互動」攻擊方式是一種複雜成熟的攻擊技巧，透過攻擊某些軟硬體漏洞，以完全不需要以螢幕顯示或操作來和用戶互動的方式，自動執行後續的攻擊行動，例如植入惡意軟體進行監控、資料竊取、大量顯示廣告、訂閱高價服務或發動釣魚攻擊等。

零互動攻擊一個有名的案例，是透過 NSO 的 Pegasus 間諜軟體，利用 Apple iMessage 的 KISMET 和 FORCEDENTRY 漏洞，來針對多國政治人物與媒體記者進行監控。

針對這種攻擊方式，Apple 於 iOS 16 中引進「鎖定模式」(lockdown mode)，讓高危險攻擊對象可採用這種模式，限制各種軟硬體資源的存取，藉以提高資安防護能力。

而 Samsung 推出的「Samsung Message Guard」則是一種在手機中與系統隔開的虛擬空間， 透過訊息程式傳來的 PNG、JPG、JPEG、GIF、ICO、WEBP、BMP、WBMP 檔會先存放於該空間內進行檢測，如果發現可能內含惡意軟體，這樣檔案就會遭到封鎖，無法與裝置作業系統進行互動。

Samsung 指出，Samsung Message Guard 會以背景方式在手機中自動執行，無需用戶手動啟用。此一新資安防護機制已於 Galaxy S23 機種上推出，日後會陸續於執行 Samsung One UI 5.1 與後續版本的其他 Samsung Galaxy 裝置上推出。

鑑於零互動攻擊對手機用戶往往造成嚴重資安威脅，Samsung 行動裝置用戶應隨時注意更新消息，在該機制可用時立即進行更新。

- 資料來源：
  1. Samsung Message Guard Protects You From New and Invisible Threats
  2. Samsung adds zero-click attack protection to Galaxy devices

2.5.4、Google 計畫透過強化韌體安全機制，加強 Android 資安防護能力

Google 近期開始研究在韌體層面強化 Android 作業系統安全性的各種做法，包括處理器以及其單晶片系統上的其他元件，如無線通訊、媒體運算、安全防護等模組，試圖補強過去飽受詬病的各種 Android 系統資安防護弱點。

Google 表示，過去已有大量攻擊與駭侵案例，係經由 Android 裝置中的次要處理元件之韌體與漏洞來發動攻擊。近期該公司密集與 Android 生態系中的合作夥伴進行合作，以改善系統元件與韌體在和 Android 系統溝通過程中的安全機制，包括以下重點：

- 在編譯器層級的安全加強：在程式碼編譯過程中加強安全性，以減少各種程式碼執行作業中發生崩潰或其他漏洞所衍生的資安問題；
- 記憶體安全問題的加強：加強 Android 系統中在記憶體層面的安全性，以減少因記憶體崩潰、釋放後使用、虛無指標 (null pointer) 等問題。Google 也說將在 App 開始使用記憶體前，先將記憶體內容以 0 填滿，以免記憶體內含先前使用過的資料。

不過，資安專家也指出雖然 Google 此計畫的立意相當好，卻可能造成裝置效能的大幅下降，因為裝置需花費更多資源來進行額外的資安防護檢驗；另外，對於使用非標準元件以達成特定功能的 Android 裝置來說，由於未必能享有與主要處理器相同的安全資源，問題可能更為嚴重。

Google 對此指出將致力於這類資安防護機制運作效能的最佳化，以減輕其對 Android 系統運作效能的影響。該公司也說，未來將會擴大於其韌體程式碼中使用 Rust 來實作所有功能，這是一種可確保記憶體運作安全性的程式語言。

由於 Android 系統的先天架構，以及其在市場上有眾多生產廠商的複雜性，使其資安防護功能一向較為薄弱；建議 Android 系統用戶應隨時注意更新軟體與韌體，避免下載不明來源 App，並在原廠停止支援該裝置的安全更新後，盡速汰舊換新。

- 資料來源：
  1. Hardening Firmware Across the Android Ecosystem
  2. Google is making your Android phone safer with hardened firmware

2.6、軟體系統資安議題

駭侵團體攻擊印度某醫療、能源研究領域與供應鏈以竊取情報

資安廠商 WithSecure 日前發表研究報告，指出該公司旗下的資安研究人員，發現 Lazarus 駭侵團體涉嫌於 2022 年第四季針對印度公私立醫療、科技與能源研究單位和其供應鏈發動駭侵監控攻擊，其主要目的推定為情報收集分析。

報告詳細描述 WithSecure 觀察到的駭侵程序；首先是以 Zimbra mail server 軟體中已知的漏洞 CVE-2022-27925 和 CVE-2022-37042 侵入受駭單位的內部網路，並利用另一個已知漏洞「pwnkit」 CVE-2021-4034 來提升自我執行權限到 root 等級。

接著駭侵者利用 shelf webshell 和自製駭侵工具來安裝 proxy、tunnel 和連線中繼工具，並利用受駭者 Windows 網域中使用老舊作業系統 Windows XP 的主機來進一步安裝其他駭侵工具如 Grease、Minikatz 和 Cobalt Strike 等。駭侵者最後取得約 100GB 資料傳送到其設立的控制伺服器，但沒有進行任何破壞行為。

整個駭侵過程自 2022 年 8 月 22 日起，到 2022 年 11 月 11 日為止，約近三個月時間。

WithSecure 的報告指出，由駭侵者的作案手法與駭侵過程途中犯下的各種錯誤，研判後認定該駭侵活動 Lazarus 駭侵團體有高度相關性。

由此份報告中可獲知，駭侵者均使用各種軟硬體的已知漏洞進行攻擊，因此各公私單位的系統管理者，必須隨時更新使用中的各種軟硬體到最新版本，並列入定期維護的標準作業程序，以防駭侵者利用已知漏洞發動攻擊。

- 資料來源：
  1. North Korean Hackers Exploit Unpatched Zimbra Devices in 'No Pineapple' Campaign
  2. No Pineapple! –DPRK Targeting of Medical Research and Technology Sector

2.7、軟硬體漏洞資訊

2.7.1、Microsoft 推出 2 月 Patch Tuesday 每月例行更新修補包，修復 77 個資安漏洞

Microsoft 日前推出 2023 年 2 月例行資安更新修補包「Patch Tuesday」，共修復多達 77 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 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 修復的漏洞數量較上個月（2023 年 1 月）的 98 個資安漏洞略少一些，但也達 77 個；其中 9 個屬於嚴重等級的漏洞，分類上均為遠端執行任意程式碼類型。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：12 個；
- 資安防護功能略過漏洞：2 個；
- 遠端執行任意程式碼漏洞：38 個；
- 資訊洩露漏洞：8 個；
- 阻斷服務（Denial of Service）漏洞：10 個；
- 假冒詐騙漏洞：8 個。

本月修復的 0-day 漏洞共有 3 個，其中第一個是 CVE 編號為 CVE-2023-21823 的 Windows 繪圖組件漏洞，屬於遠端執行任意程式碼 (RCE) 漏洞。Microsoft 指出駭侵者可以透過系統權限執行任意程式碼。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-2023-21715 的 Windows Publisher 漏洞，屬於資安防護功能略過漏洞。Microsoft 指出駭侵者可以透過特製的 Publisher 檔案加入惡意巨集程式，借用用戶的權限來發動攻擊。

第三個是 CVE 編號為 CVE-2023-23376 的 Windows Common Log Flie System Driver 漏洞，屬於權限提升漏洞。Microsoft 指出駭侵者可以透過此漏洞取得系統權限。目前已知該 0-day 漏洞已遭駭侵者廣泛用於攻擊活動。

- CVE 編號：CVE-2023-21823 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，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 February 2023 Patch Tuesday fixes 3 exploited zero-days, 77 flaws

2.7.2、Apple 修復新發現的 WebKit 0-day 漏洞 CVE-2023-23529

Apple 日前緊急推出新版 iOS、iPadOS、macOS，以修補一個新發現的 WebKit 0-day 漏洞 CVE-2023-23529；該漏洞可讓駭侵者用於執行任意程式碼。

編號 CVE-2023-23529 的這個全新 0-day 漏洞，是一個存於 WebKit 瀏覽器引擎的錯誤，駭侵者可利用特製的網頁內容來誘發此錯誤發生，並且執行任意程式碼，以發動進一步的駭侵攻擊。

Apple 在資安通報中也表示，該漏洞可能已經遭到廣泛濫用於駭侵攻擊。該漏洞存內建 WebKit 引擎且執行舊版作業系統的 iPhone、iPad 和 Mac 電腦。

目前尚無此 CVE-2023-23529 的 CVSS 危險程度評分與評級相關資訊。

為修補此一漏洞，Apple 緊急發表新版 iOS 16.3.1、iPadOS 16.3.1、macOS Ventura 13.2.1；適用機種十分廣泛，包括 iPhone 8 與所有後續機型、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，以及所有執行 macOS Ventura 的 Mac 電腦。

在這次發行的更新版 iOS、iPadOS、macOS 中，除了上述的 CVE-2022-23529 外，Apple 也同時修補另一個漏洞 CVE-2023-23514；該漏洞存於記憶

體管理機制中，屬於使用已釋放記憶體漏洞，可讓駭侵者以核心權限執行任意程式碼。

- CVE 編號：CVE-2023-23529、CVE-2023-23514
- 影響產品(版本)：iPhone 8 與所有後續機型、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，以及所有執行 macOS Ventura 的 Mac 電腦。
- 解決方案：升級到 iOS 16.3.1、iPadOS 16.3.1、macOS Ventura 13.2.1。

- 資料來源：
  1. About the security content of iOS 16.3.1 and iPadOS 16.3.1
  2. About the security content of macOS Ventura 13.2.1
  3. Apple fixes new WebKit zero-day exploited to hack iPhones, Macs

第 3 章、 資安研討會及活動

IT EXPLAINED 數位轉型攻略 V 透過現代化端點管理實現混合辦公，提升企業資安防護實力刻不容緩！	
活動時間	**2023/03/14 14:30 ~ 15:20**
活動地點	**線上**
活動網站	**https://webinar.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 大家沒想到，後疫時代，象徵的並非疫情前的平靜、正常，而是一波波海嘯洶湧而至。 此時最苦惱的人正是 IT 主管，只因為挑戰實在太多。例如隨著零接觸、遠距互動成為日常，必須建構長治久安的混合辦公環境。此外眼看別人家數位轉型推得火熱，面對雲原生、大數據、AI/ML、AR/VR 都能純熟運用，自己豈能停滯不前？ 或是當 ESG、淨零碳排、永續經營等課題，從道德層次昇華到合規層次、經濟層次，任何企業為求生存發展，當然要正面應對這些議題；隨之而來的碳盤查、能源管理等重擔，又落在 IT 部門的身上。而當企業邁向混合辦公、高度數位化、淨零轉型新境界，IT 環境高度開放，這時候又得提防虎視眈眈的駭客攻擊，壓力非常大。 為此 iThome 將在 2023 推出「數位轉型攻略 V：啟動 IT 新戰略」全方位攻略的線上研討會，深入探討多雲機器學習、勒索攻擊防禦、DevSecOps 等關鍵議題，幫助企業 IT 人員在錯綜變局中充實新知、理出頭緒，順利推展 IT 新戰略。

2023/03/14 14:30 ~ 14:40 2023 開發管理新思維：平臺工程

有不少企業招募 SRE 技術人才，但用來負責服務內部顧客，將內部團隊需要的常用功能、共用系統、通用模組等都服務化（或者微服務化），變成一套平臺，改用產品角度來管理和維運。去年，國外出現了一個專有名詞，來形容這種非典型 SRE 的做法，就稱為 Platform Engineering（平臺工程）。

2023/03/14 14:40 ~ 15:20 透過現代化端點管理實現混合辦公，提升企業資安防護實力刻不容緩！（英語演講，中文字幕）

後疫情混合辦公成為企業新常態，員工在家工作的同時卻也帶給 IT 人員新的挑戰。面對快速大量部署、裝置管理與資安維護等挑戰，企業提升 IT 實力刻不容緩！歡迎報名此場線上研討會，帶您了解 Microsoft 如何透過軟硬整合達到簡化部署和端點管理，以及最現代化的 Surface 裝置如何幫助您節省 IT 成本與時間。

當天研討會也邀請到 Microsoft 技術專家進行線上 Q & A。在混合辦公的新常態下資安需求勢不可擋，別讓公司暴露在數以萬計的資安威脅下！敬請鎖定此場研討會！

參加研討會您將會學到：

- 如何從雲端進行裝置管理：組織的裝置管理總是讓 IT 人員耗腦傷神？Microsoft Intune 為您實現從遠端管理跨平台裝置，更可以集中管理與監控所有 Surface 裝置！
- 公司如何利用 Windows Autopilot 簡化部署：每當有新同事們加入團隊時，IT 人員總要耗費大量時間逐一部署裝置。傳統的部署方式缺乏效率， Windows Autopilot 為您實現從雲端零接觸的進行大量一次性裝置部署，為您省時又省煩惱！
- Surface 從晶片到雲端的完整安全防護：Surface 除了搭載資安晶片 TPM 2.0 之外，還有 Windows Hello 生物辨識讓您快速安全的無密碼登入，更能完美整合 Microsoft Intune 從雲端監控裝置安全與健康，達到層層的安全防護。

IT EXPLAINED 數位轉型攻略 V 後疫情時代的資安挑戰 - 零信任”應”加速實施	
活動時間	**2023/03/16 14:30 ~ 15:20**
活動地點	**線上**
活動網站	**https://webinar.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 2023/03/16 14:30 ~ 14:40 CIO 必看 2023 十大趨勢 竄紅的 ChatGPT 引爆了各界對 AI 的新熱潮，但台灣企業 CIO 今年要注意的科技新趨勢，可不只是對話型生成式 AI，平臺工程、永續 IT、資料治理、顧客大數據、OMO 在今年都是重要議題，我們整理出了 CIO 必看的 2023 年十大趨勢。 王宏仁 iThome 副總編輯 2023/03/16 14:40 ~ 15:20 後疫情時代的資安挑戰 - 零信任”應”加速實施 基於後疫情時代形成的混合辦公型態，以及企業開始加速上雲佈署，使得駭客針對虛擬私人網路 (VPN)等上網方式攻擊比例提高，甚至企業在雲端網路錯誤配置也將增加更多外部入侵內部系統風險；台灣二版將在此次議程中，談到企業應如何加快採用零信任策略，同時整合資安視野，藉此抵禦更多威脅。 盧惠光 台灣二版 高級產品經理

【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	**第一場：2023/3/23 (四)-3/24(五) 9:00~16:00** **第二場：2023/4/6 (四)-4/7(五) 9:00~16:00** **第三場：2023/4/17 (一) 9:00~16:00**
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

2023 OT 資安年會	
活動時間	**2023 年 3 月 30 日(四) / Am 9:30 – Pm 16:30**
活動地點	**臺北文創 6F 會議室**
活動網站	**https://www.informationsecurity.com.tw/Seminar/2023_OT/edm/**
活動概要	 **主辦單位：資安人媒體** 物聯網零疆界 工控資安零信任 近兩年, 數位轉型已成全球高科技產業的主旋律, 台灣是全球的製造基地, 許多廠商也在也積極數位化, 聯網並 AI 化、投入智慧廠房的建置, 而在邁向智慧化的過程中, 必須更全面的去檢視資安, 除了過去的 IT 環境, 更應改變資安的管理思維。 另一方面, 從 2022 年的一連串政治效應, 也提醒我們必須檢視關鍵基礎設施的防護, 特別是 OT 在 CI 裡面所佔的比例相對之高, 這是不可忽視的重要議題。 從政府近期的相關法令的規範, 高科技的供應鏈資安管理的趨勢, 與資安長的設置, 物聯網與 5G 普及下, 高度聯網的工控資安看起來是急需重視的項目。 資安人要從管理面透過 NIST 的框架一起思考 OT 的資安, 對於資安長與主管來說這也是必須面對的重要課題, 同時在零信任的概念下, OT 會有不同的思考策略, 還有面對勒索事件的頻傳, 如何在這樣的架構下重新思考防禦策略, 唯有把 OT 資安一起重視, 才能實現真正的防護網, 發揮數位化下的資安韌性。 相關議題 • 資安主管應該用 NIST CSF 框架檢視資安風險

- 如何落實 OT 端的零信任
- 工業 4.0 的工控資安如何落實
- OT 產線面對勒索猖獗如何因應
- 工安應該包含 OT 資安
- 5G 合網的智慧工廠資安佈署
- 如何落實工控零信任
- 落實 IEC 62443 確保工控物聯網安全
- 產線安全應該思考的 OT 資安

合適聽眾

企業與單位決策層:總經理/副總經理、執行長 CEO、營運長 COO、資訊長 CIO、資安長 CISO、風控長、高階經營管理層廠長/副廠長、處長/副處長、課長/科長/股長、 資安主管、資訊協理、資訊組組長/副組長

OT 現場管理相關人員:製造課長、產品整合工程師、OT 設備工程師、工程經理、系統開發處主管、壓合課長、生管主管、生產製造課長、物聯網事業部/處主管、智慧聯網部/處主管

IT 維護及管理相關人員:IT 專案管理師、軟體應用程式設計師、技術服務組組長、硬體工程師、技術師、硬體設計工程師、技監、程式設計師、系統工程師、資料庫管理員、系統分析師、資訊工程師、系統程式員、網管人員、系統網管工程師、 網管工程師、高級工程師、高級分析師

活動洽詢: Yoyo.Pan@taiwan.messefrankfurt.com / 02-8729-1087 潘小姐

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** **報名截止日：2023/04/17**
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：到工研院產業學院官網報名 / 02-2370-1111 分機 609 或 306 黃小姐

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：

HGiga PowerStation - Information Leakage	
TVN / CVE ID	TVN-202302006 / CVE-2023-24838
CVSS	9.8 (Critical)
影響產品	HGiga PowerStation firmware version < x64.6.2.165
問題描述	PowerStation 特定功能存有 Information Leakage 漏洞，遠端攻擊者不須權限，連線至伺服器時，系統即回傳含有管理員明文帳號密碼的伺服器設定檔，進而對系統進行控制，並中斷服務。
解決方法	Update PowerStation firmware version to x64.6.2.165, then reboot PowerStation.
公開日期	2023-02-24
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6957-d8f67-3.html**

HGiga MailSherlock - Command Injection	
TVN / CVE ID	TVN-202302009 / CVE-2023-24841
CVSS	7.2 (High)
影響產品	HGiga MailSherlock 系統版本：v4.5 系統套件：iSherlock-sysinfo-4.5 <= 4.5-132
問題描述	MailSherlock 連線紀錄查詢功能未對參數值進行特殊字元過濾，遠端攻擊者以管理者權限登入後，即可利用此漏洞進行 Command Injection 攻擊，執行任意系統指令，進而對系統進行控制，並中斷服務。

解決方法	更新 MailSherlock 之 iSherlock-sysinfo 系統套件至 iSherlock-sysinfo-4.5-133.386.rpm
公開日期	2023-02-24
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6960-fc2fe-3.htmlq

瑞賦科技 IOT Wall - Broken Access Control	
TVN / CVE ID	TVN-202302013 / CVE-2023-25017
CVSS	8.1 (High)
影響產品	瑞賦科技 IOT Wall v.22
問題描述	瑞賦科技 IOT Wall 未適當進行權限控管，使遠端攻擊者以一般使用者權限登入後，即可利用此漏洞操作系統管理者權限才能執行之電商整合功能，對所有電商資料進行查看與修改。
解決方法	程式面強化所有 ajax 權限檢查並版更至 IOTWall v.30
公開日期	2023-02-24
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6962-34ac1-3.html

中華數位科技 SPAM SQR 全方位郵件過濾平台 - Code Injection	
TVN / CVE ID	TVN-202302003 / CVE-2023-24835
CVSS	7.2 (High)
影響產品	中華數位科技 SPAM SQR 全方位郵件過濾平台 2.221231 以前版本
問題描述	中華數位科技 SPAM SQR 的進階編輯使用者設定檔功能含有 Code Injection 漏洞，遠端攻擊者以管理者權限登入後，可以利用此漏洞執行任意程式碼，藉以控制系統或中斷服務。
解決方法	請更新至 2.221231(含) 以上版本；若無法開啟自動更新，亦請

	妥善保護您的管理者密碼，避免使用預設密碼以符合密碼強度原則。
公開日期	2023-02-24
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6955-c7612-3.html

HGiga MailSherlock - SQL Injection	
TVN / CVE ID	TVN-202302008 / CVE-2023-24840
CVSS	7.2 (High)
影響產品	HGiga MailSherlock 系統版本：v4.5 系統套件：iSherlock-query-4.5 <= 4.5-167
問題描述	MailSherlock 信件查詢功能未對使用者輸入之參數進行驗證，遠端攻擊者以管理者權限登入後，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	更新 MailSherlock 之 iSherlock-query 系統套件至 iSherlock-query-4.5-168.386.rpm
公開日期	2023-02-24
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6959-cdecb-3.html

第 5 章、 2023 年 2 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。

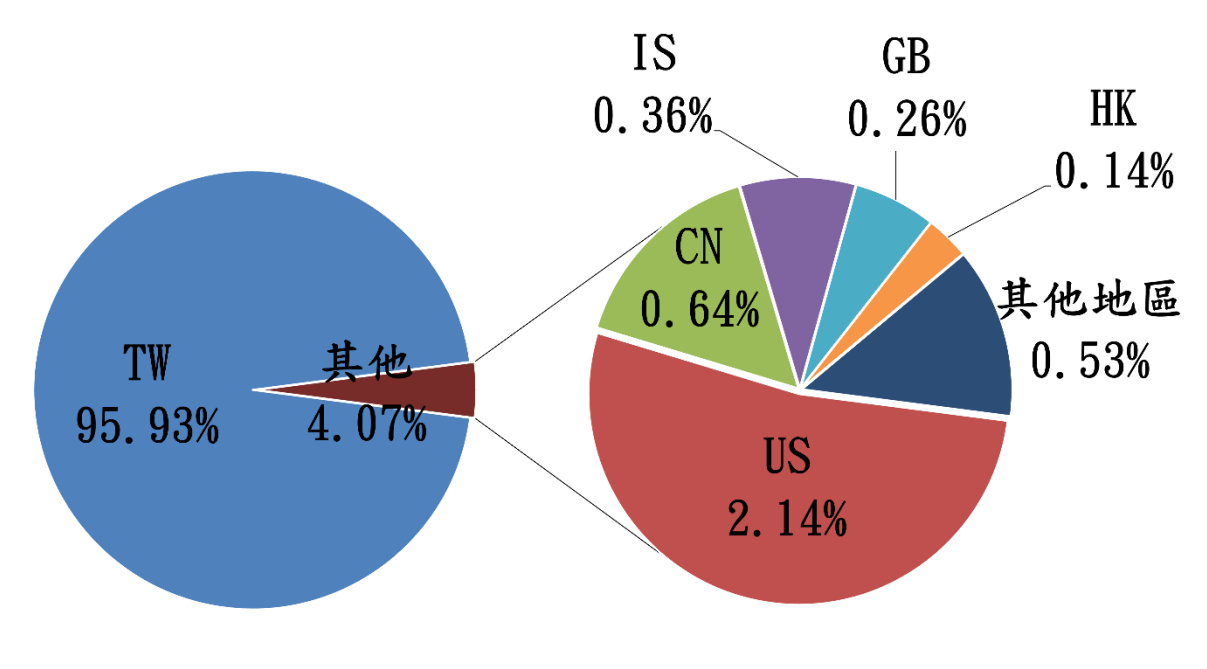

圖 1、分享地區統計圖

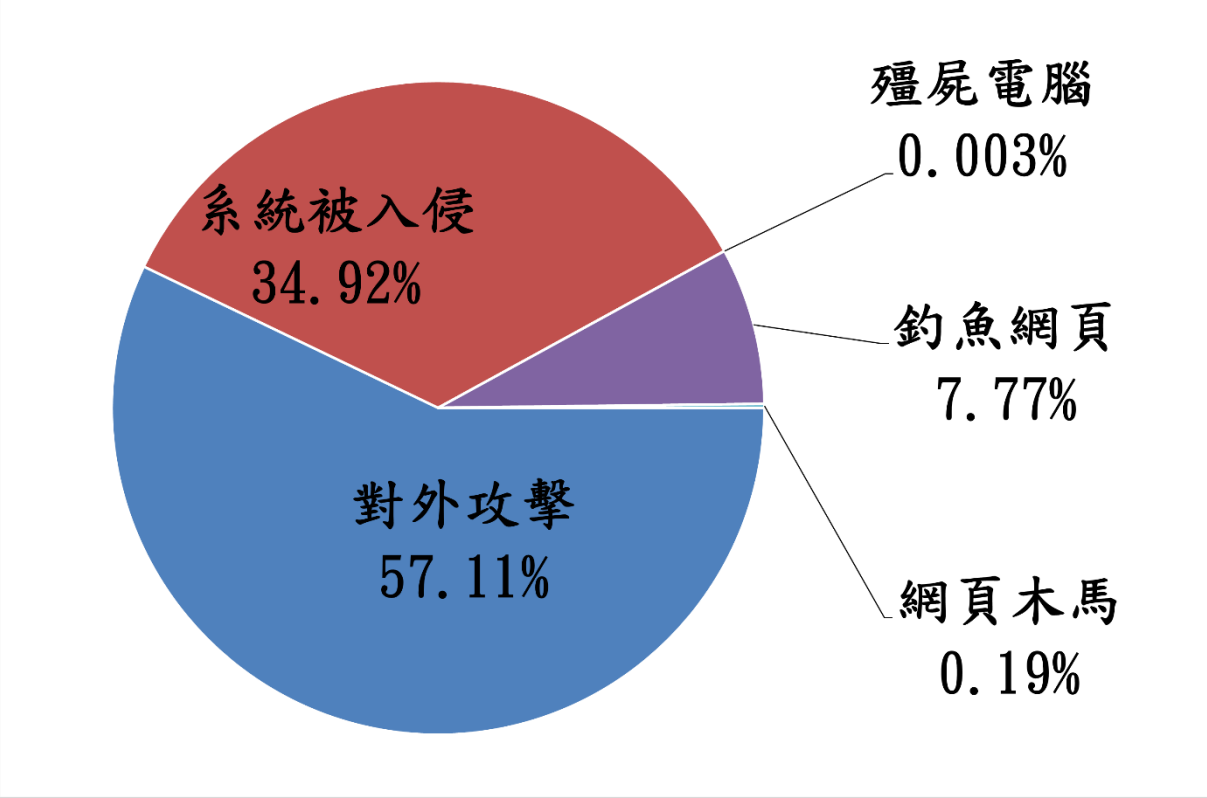

圖 2、分享類型統計圖

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 3 月 10 日**

編輯：**TWCERT/CC 團隊**

服務電話：**0800-885-066**

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**