TWCERT/CC 資安情資電子報

2022 年 5 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

Spring4Shell 0-day 嚴重漏洞已遭駭侵者濫用，建議立即進行更新

0-day 漏洞 Spring4Shell（CVE-2022-22965），雖然原廠已推出更新修補程式，但仍發現該漏洞遭駭侵者大規模用於攻擊。

日前遭發現的嚴重 0-day 漏洞 Spring4Shell（CVE-2022-22965），雖然 VMware 原廠已緊急推出更新修補程式，但包括微軟在內的多家資安廠商，仍發現該漏洞遭駭侵者大規模用於攻擊。

這個稱作 Spring4Shell 的嚴重 0-day 漏洞，是存於 VMware Spring Core Java framework 之中，該程式框架可讓開發者輕鬆且快速開發各種企業級 Java 應用程式，使用範圍非常廣泛，包括 Apache Tomcat 等伺服器或多種個別軟體套件，都使用了 Spring Core Java framework。

Spring4Shell 漏洞的發生原因，是在傳送參數時未能進行安全的反序列化（Deserialization），該錯誤可讓駭侵者遠端執行任意程式碼，且其 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），危險程度評級為最高等級的「嚴重」（critical）等級。

在這個漏洞公開後，多家資安廠商立即在數日內觀測到大量增加的相關駭侵活動。資安廠商 Check Point 指出，在 3 月 31 日時的相關攻擊次數僅有數百次，四天後的 4 月 3 日，相關攻擊次數即暴增至 14,000 件以上；其中最主要的攻擊對象為軟體發行業者，約有 28% 的攻擊都針對該行業進行，原因

可能是用於發動攻應鏈攻擊。

以地域來看，Check Point 指出歐洲的攻擊案件最多，達 20%，攻擊美國的案件則占 11%。微軟也在日前指出，在其雲端服務中觀測到若干利用 Spring4Shell 漏洞的攻擊活動。

資安專家表示，任何使用 Spring Core Java Framework 的服務，都應立即更新至最新版本，確認該漏洞修補完成，以免遭到駭侵者攻擊。

- CVE 編號：CVE-2022-22965
- 解決方案：升級 Spring Framework 至 5.3.18 和 5.2.2 版本，以及 Spring Boot 至 2.5.12 版本，或更高版本。

- 資料來源：
  1. spring4shell
  2. CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression
  3. SpringShell attacks target about one in six vulnerable orgs
  4. Microsoft detects Spring4Shell attacks across its cloud services

第 2 章、 國內外重要資安事件

2.1、資安趨勢

統計指出，勒贖 DDoS 攻擊比例降至近年新低，但應用層 DDoS 攻擊暴增

Cloudflare 發表統計數字指出，過去猖獗的「勒贖 DDoS」攻擊，自今年以來持續大幅下降；三月時，RDDoS 攻擊占所有 DDoS 攻擊次數的比例，已降到兩年來的新低水準。

全球最大網路基礎建設廠商 Cloudflare 的資安部門，近日發表統計數字指出，過去十分猖獗的「勒贖 DDoS」（Ransom Distributed Denial of Service, RDDoS）攻擊，自今（2022）年以來持續大幅下降；至今年三月時，RDDoS 攻擊占所有 DDoS 攻擊次數的比例，已降到兩年來的新低水準。

過 RDDoS 攻擊，是指駭侵者對特定組織或企業發動大規模 DDoS 攻擊，癱瘓其內外網路連線與服務後，向廠商要求贖款或滿足特定要求以解除攻擊，否則持續攻勢的一種資安攻擊方式。有些駭侵者會同時結合傳統的勒贖攻擊，包括竊取企業內部機敏資訊，再加上強力 DDoS 攻擊，以加強攻擊力，逼迫受害單位支付贖款。

根據 Cloudflare 旗下資安單位的統計指出，該公司觀察到的 RDDoS 占所有 DDoS 攻擊次數的比例，在 2021 年 12 月達到高峰（28%）後便一路大幅下降：2022 年 1 月降至 17%，二月降至 6%，三月更降至近兩年最低水準的 3%；和去年相比，降幅多達 52%。

目前 Cloudflare 無法確定今年以來 RDDoS 大幅下降的確實原因。

但是 Cloudflare 也指出，自 2022 年以來，發生在應用層（Application Layer）的 DDoS 攻擊次數卻較往年大增 164%；如以季來看，2022 年第 1 季發生在應用層，針對消費級網通產品發動的 DDoS 攻擊，較上一季暴增 5,086%，針對網路媒體公司發動的 DDoS 攻擊也暴增 2,131%。

- 資料來源：
  1. DDoS Attack Trends for 2022 Q1
  2. Ransom DDoS attacks have dropped to record lows this year

2.2、新興應用資安

2.2.1、去中心化金融交易平台（DeFi）遭駭侵攻擊情況日益嚴重

資安廠商研究報告指出，各種針對加密貨幣的去中心化金融服務平台所發動的駭侵攻擊，在今年第一季財損甚至達到史上最高記錄。

資安廠商 Chainalysis 日前發表研究報告指出，各種針對加密貨幣的去中心化金融服務（Decentralized Finance, DeFi）平台所發動的駭侵攻擊，近年不但日益增加，在今年第一季財損甚至達到史上最高記錄。

以損失金額來說，各種針對加密貨幣平台發動的駭侵攻擊，於去（2011）年達到史上最高記錄，全年的總損失高達 32 億美元，其中針對去中心化金融平台的全年攻擊損失，達到 25.1 億美元。

然而光是在今（2022）年第一季，針對加密貨幣相關服務的攻擊總損失，已來到 13 億美元，而針對去中心化金融平台的單季攻擊損失，就高達 4.3 億美元。

若以各平台的攻擊占比來看，針對去中心化金融平台的全年攻擊損失占比，2020 年約為 30%，2021 年大幅成長到 72%，到了今年第一季更高達 99%。

該報告也指出，在針對加密貨幣相關的攻擊形態上，近年來也發生相當大的變化。在 2020 年時，駭侵者主要是以取得平台或用戶持有的登入資訊來發動攻擊，這種攻擊的比例在 2020 到 2022 年之間占所有攻擊損失額的

35%；但是針對去中心化金融服務平台的攻擊，主要是透過攻擊去中心化金融交易協定所使用的智慧合約，在程式設計上的邏輯漏洞，例如所謂的「閃電貸款」。這種攻擊比例自 2020 年的 10% 左右，上升到 2022 年的近 50%。

報告分析指出，駭侵者主要是攻擊去中心化平台為取得加密貨幣正確價格資料所需的「預測機」（Oracle）機制，最近發生的多起去中心化交易所遭駭事件，都是駭侵者利用預測機的程式邏輯漏洞，進而竊起鉅資。

- 資料來源：
  1. Hackers Are Stealing More Cryptocurrency From DeFi Platforms Than Ever Before
  2. Cryptocurrency DeFi platforms are now more targeted than ever

2.2.2、資安廠商發現漏洞後，Everscale 區塊鏈關閉其 web 版加密貨幣錢包

Everscale 區塊鏈上的加密貨幣錢包，遭資安廠商發現存有嚴重漏洞，可能導致用戶資金遭竊之後，開發公司 Ever Surf 立即關閉停用該加密貨幣錢包的 web 版本。

Everscale 區塊鏈上的加密貨幣錢包，日前遭資安廠商 Check Point 旗下的資安專家發現存有嚴重漏洞，可能導致用戶資金遭竊之後，開發公司 Ever Surf 立即關閉停用該加密貨幣錢包的 web 版本，以免用戶因此漏洞而招致財物損失。

資安廠商 Check Point 的研究人員，日前發表研究報告指出，Ever Surf 為 Everscale 區塊鏈開發的加密貨幣錢包，內含一個嚴重資安漏洞；駭侵者可利用此漏洞，輕鬆破解存於瀏覽器本地儲存區中，由用戶持有的私有加密金鑰與錢包存取權復原短語。駭侵者可以藉此完全控制用戶的加密貨幣錢包，並將存於錢包位址內的資金任意轉出，造成用戶的損失。

Check Point 報告說，這個漏洞使得密鑰破解變得十分簡單快速，駭侵者可利用消費級的電腦設備，在幾分鐘內就可以破解用戶私鑰。

Ever Surf 在接獲 Check Point 公司的漏洞通報後，立即關閉了 web 版本加密錢包的服務；該公司在對外的聲明中指出，正在和 Check Point 密切合作，以便解決這個問題。

該公司也強調，這個問題只會發生在 web 介面，不會發生在為行動裝置原生開發的 app（包括 iOS 與 Android 版本），原因是桌面版瀏覽器缺少行動裝置擁有的不重覆裝置識別碼。

該公司要求使用 web 版加密貨幣錢包的用戶，應該改用桌面應用程式版本；截至目前為止，各版本的加密錢包約有 67 萬名用戶，已進行 3,160 萬次交易，但該公司無法估算有多少用戶使用 web 版本的加密貨幣錢包。

- 資料來源：
  1. True Story of Ever Surf for Desktop
  2. Check Point Research detects vulnerability in the Everscale blockchain wallet, preventing cryptocurr
  3. Everscale blockchain wallet shutters web version after vulnerability found

2.2.3、NFT 巨擘 Bored Ape 的 Instagram 帳號遭盜，價值 280 萬美元 NFT 被竊

NFT 大發行商「無聊猿遊艇俱樂部」，發生官方 Instagram 帳號遭駭侵者盜取事件；駭侵者隨即透過該帳號，發布詐騙 NFT 空投活動。

NFT 大發行商「無聊猿遊艇俱樂部」（Bored Ape Yacht Club, BAYC），日前發生官方 Instagram 帳號遭駭侵者盜取事件；駭侵者隨即透過該帳號，發布詐騙 NFT 空投活動，並且成功竊走參與用戶共 91 枚 NFT，總價值高達 280 萬美元。

BAYC 在事件發生後，在 Twitter 發表聲明，要求用戶不要遞交任何作品，不要鑄造 NFT 代幣、不要點按任何連結，也不要連結加密貨幣錢包。

據區塊鏈專業媒體 The Block 指出，當 BAYC 的 Instagram 官方帳號遭挾持後，駭侵者透過該帳號，發布了一個假訊息，詐稱要舉辦一場 LAND 空投；用戶如果想要免費接收空投的 NFT，必須要連結用戶的加密貨幣錢包。許多用戶不疑有他，連結了錢包後，存於錢包內的 NFT 就遭到駭侵者盜領了。

根據區塊鏈掃瞄網站 Etherscan 的資料指出，駭侵者用以接收釣魚盜領 NFT 的加密貨幣錢包，內有 91 個 NFT 代幣，換算其價值，高達 280 萬美元。

BAYC 的共同創辦人也在推特上表示，他們將會接觸受害用戶，進行事後調查；他也強調 BAYC 的官方 Instagram 有開啟二階段登入驗證。

關於 BAYC 的官方 Instagram 帳號存取權是如何遭竊的，目前尚無具體資訊。

在四月上旬，BAYC 也曾發生過其官方 Discord 頻道遭駭，駭侵者也利用該頻道發動釣魚攻擊；不過該次攻擊中，駭侵者只得手了一枚 NFT。

- 資料來源：
  1. Bored Ape Yacht Club @BoredApeYC
  2. Address
  3. Bored Ape Instagram account hacked: NFTs worth $2.8 million stolen

2.3、國際政府組織資安資訊

2.3.1、美國資安主管機關下令修補 WatchGuard 網通設備漏洞

CISA 命令美國政府各民事單位，應立即處理 WatchGuard Firebox 與 XTM 防火牆漏洞，因該漏洞已遭駭侵團體利用於大規模攻擊。

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）日前命令美國政府各民事單位，應立即處理 WatchGuard Firebox 與 XTM 防火牆漏洞，因該漏洞已遭駭侵團體利用於大規模攻擊。

在 CISA 發出的資安通報與命令中指出，駭侵團體 Sandworm 日前利用 Watchguard 家用暨中小企業網通設備中的一個漏洞 CVE-2022-23176，發展出一個名為 Cyclops Blink 的僵屍網路。

CISA 的命令，要求美國聯邦政府各民事單位，必須於命令發布 3 星期內（即 2022 年 5 月 2 日）之前，針對單位使用的 WatchGuard Firebox 與 XTM 網通設備進行資安修補；CISA 同時也強烈建議美國各公私單位，亦應按照該局發布的指引以更新該漏洞。

此外，美國政府也在稍早的今（2022）年 4 月 6 日宣布，成功阻擾了 Cyclops Blink 所設立的僵屍網路，以避免該駭侵團體持續擴大攻擊。

資安專家指出，Cyclops Blink 不只利用 WatchGuard 裝置漏洞進行駭侵攻擊，部分 ASUS 的網通產品也含有同類漏洞，同樣會遭到 Cyclops Blink 感

染，成為其僵屍網路的一分子；ASUS 網通產品用戶亦應提高警覺，立即更新至最新韌體版本，以修補可遭 Cyclops Blink 攻擊的漏洞。

- 資料來源：
  1. BINDING OPERATIONAL DIRECTIVE 22-01- REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIE
  2. CISA warns orgs of WatchGuard bug exploited by Russian state hackers
  3. US disrupts Russian Cyclops Blink botnet before being used in attacks
  4. Cyclops Blink Sets Sights on Asus Routers

2.3.2、美國資安主管機關聯合警告，駭侵者正鎖定工業製造控制系統發動攻擊

多個美國資安主管機關聯合發表資安通報，警告駭侵者已有能力利用新型惡意軟體工具，針對多種工業設備發動駭侵攻擊。

多個美國資安主管機關，包括網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）、國家安全局（National Security Agency, NSA）、聯邦調查局（Federal Bureau of Investigation, FBI）與能源部（Department of Energy），日前聯合發表資安通報，警告駭侵者已有能力利用新型惡意軟體工具，針對多種工業設備發動駭侵攻擊並予以挾持。

該聯合通報指出，已經掌握確切情資，顯示已有與部分國家政府相關的 APT 駭侵團體，利用全新的客製模組化惡意軟體，針對工業控制系統（ICS）與資料取得監控系統（SCADA）發動攻擊並取得控制權。

聯合通報說，這些由 APT 駭侵團體用於攻擊的模組，其架構可以讓駭侵者執行自動化攻擊，而其攻擊模組可直接與目標設備互動，因此即使是低技術水準的駭侵者，亦可操作過去僅有高階駭侵者可進行的攻擊操作。

通報指出，目前已有包括德國施耐德電機（Schneider Electric）生產的 MODICON、MODICON Nano 可程式邏輯控制器（PLC）、日本歐姆龍（Omron）生產的 Sysmac NJ 與 NX 系列 PLC，以及 Open Platform Communications Unified Architecture 伺服器已有遭駭侵者挾持的攻擊記錄。

四個單位也在資安通報中說，這些有國家勢力支持的駭侵者，同時也擁有能鎖定執行 Windows 系統的 ASRock 主機板的 CVE-2020-15368 漏洞，針

對採用上述軟硬體組合的 IT 或 OT 環境，發動遠端執行任意程式碼攻擊。

通報建議系統管理者立即針對系統用戶套用多重登入驗證（MFA）流程，務必更改預設密碼，並且強化資安防護。

- 資料來源：
  1. APT Cyber Tools Targeting ICS/SCADA Devices
  2. CVE-2020-15368 Detail
  3. US warns of govt hackers targeting industrial control systems

2.3.3、伊朗國營電視台宣稱，當局破獲大型資安攻擊

伊朗國營電視台日前發布新聞，新聞內容宣稱伊朗當局近日破獲一起針對該國境內多個公私單位的大型資安攻擊行動。

該則新聞是在上周日發布於伊朗國營電視台，新聞內容指出，伊朗政府破獲的資安攻擊行動，意圖針對該國境內 100 個以上的公營和民營單位發動駭侵攻擊。

新聞並未明確指出遭到鎖定攻擊的單位有哪些，不過根據新聞報導，這些單位在近期都曾遭到駭侵攻擊。

新聞也說，目前尚未確實掌握發動攻擊的駭侵者真實身分，但可以確定的是，這些攻擊的來源，係來自西方國家。

值得注意的是，在去（2021）年 10 月時，曾經發生過一場針對伊朗能源供應系統的大規模駭侵攻擊行動，造成該國全國各地的加油站運作陷入癱瘓；加不了油的車輛在加油站外大排長龍，引起民怨達數日之久。

此外，去年 7 月時，伊朗也曾發生一起針對該國鐵道系統的駭侵事件，也造成伊朗國內鐵道運輸秩序大亂，許多列車無法順利開行或發生嚴重誤點。

伊朗由於核子武器開發問題，長期以來與西方國家處於對立狀態；該國在 2000 年代後期，遭到 Stuxnet 惡意軟體嚴重駭侵攻擊後，開始將各政府機關的基礎電腦系統設施切離 Internet，以避免再次遭到攻擊而無法運作。

- 資料來源：
  1. State TV Says Iran Foiled Cyberattacks on Public Services
  2. State TV says Iran foiled cyberattacks on public services
  3. Iran Suspects Israel and US Behind Fuel Cyber Attack

2.4、社群媒體資安近況

惡意軟體 FFDroider 專門竊取 FB、IG、Twitter 等社群與電商平台帳號

資安廠商 Zscaler 發現一個新惡意軟體，命名為 FFDroider。該惡意軟體會藏身在各種正版軟體破解工具、免費軟體或遊戲中。

資安廠商 Zscaler 旗下的資安研究人員，近日發現一個新惡意軟體，命名為 FFDroider。該惡意軟體會藏身在各種正版軟體破解工具、免費軟體或遊戲中，用戶一旦安裝這些軟體，FFDroider 即會竊取受害者的各種社群與電商平台的登入資訊。

資安專家指出，FFDroider 和其他多數的惡意軟體相同，也是透過許多用戶會想要下載的破解版軟體、免費遊戲等，常以 torrent 的形態透過 P2P 下載傳散。

據專家表示，用戶如果下載了含有 FFDroider 的軟體或遊戲，除了用戶下載的軟體外，FFDroider 也會下載並安裝到系統上，並且假冒為 Telegram 通訊軟體的桌面版應用程式，以逃避防毒軟體的偵測。

用戶一旦執行了 FFDroider，該惡意軟體會在 Windows 登錄檔中新增一個名為「FFDroider」的機碼，接著該惡意軟體會檢查系統上已安裝的網頁瀏覽器，接著竊取特定社群網站的 cookie 與登入資訊，並將這些竊得的資訊傳送到駭侵者設置的控制伺服器。

會遭 FFDroid 竊取 cookie 和登入資訊的瀏覽器，包括 Google Chrome（以及所有基於 Chromium 開發的其他相容瀏覽器）、Mozilla Firefox、Internet Explorer 與 Microsoft Edge。

至於 FFDroider 竊取的登入資訊，包括 Facebook、Instagram、Amazon、eBay、Etsy、Twitter、WAX Cloud wallet 入口等。

- 資料來源：
  1. FFDroider Stealer Targeting Social Media Platform Users
  2. New FFDroider malware steals Facebook, Instagram, Twitter accounts

2.5、行動裝置資安訊息

2.5.1、Android 金融惡意後門 Fakecalls，會攔截打到銀行客服專線的求助電話

資安廠商 Kaspersky 近期發現 Android 金融後門惡意軟體；該惡意後門具備前所未見的強大攔截功能，能夠直接攔截用戶撥打給銀行客服專線的求助電話。

資安廠商 Kaspersky 旗下的資安專家，近期發現一個 Android 金融後門惡意軟體；該惡意後門具備前所未見的強大攔截功能，能夠直接攔截用戶撥打給銀行客服專線的求助電話，導向到駭侵者處，接著對用戶進行各式金融詐騙。

Kaspersky 是在去（2011）年時發現這個罕見的金融惡意軟體開始活動，並將之命名為「Fakecalls」；Fakecalls 除了具備典型後門惡意軟體的各種監控與資料竊取功能外，更能假冒銀行客服專線。

Kaspersky 在報告中指出，Fakecalls 主要是假冒南韓兩大知名銀行 Kookmin Bank 與 KakaoBank 的行動 App，該後門會要求用戶授予多項存取權限，包括存取通訊錄、麥克風、攝影鏡頭、地理座標、撥接電話等等。而在畫面上顯示的客服電話號碼，確實是各該銀行真實的客服電話專線號碼；。

當用戶透過 Fakecalls 的假冒銀行 App 撥打客服支援專線時，該後門會產生假冒的電話撥打介面；這時 Fakecalls 會直接把用戶導向到駭侵者設立的假客服中心，由駭侵者與受害者直接通話，或是播放一段假冒真實銀行的預錄客戶關懷語音。

Kaspersky 也指出，Fakecalls 主要以南韓用戶為攻擊對象，因此其假冒的撥號介面僅支援韓文；若用戶將手機切換到其他語系，在 Fakecalls 假裝撥打至銀行客戶電話時，用戶就會發現異常。

資安專家指出，為避免遭到這類惡意軟體攻擊，手機用戶應避免下載不明來源的應用軟體，只從官方合法管道安裝 App，且應注意 App 要求的存取權限是否過多。

- 資料來源：
  1. Fakecalls: a talking Trojan
  2. This Android Malware Can Hijack Phone Calls to Customer Support

2.5.2、多支惡意 Android 應用程式使用資料竊取 SDK，下載多達 4,500 萬次

TWCERT/CC

資安廠商 AppCensus 發現多支可自 Google Play Store 中下載的 Android 應用程式，使用了可竊取用戶機敏資訊的第三方 SDK 進行開發。

資安廠商 AppCensus 旗下的資安研究人員，近來發現多支可自 Google Play Store 中下載的 Android 應用程式，使用了可竊取用戶機敏資訊的第三方 SDK 進行開發；這些惡意軟體的下載次數合計超過 4,500 萬次，受害者相當多。

資安專家表示，該 SDK 可竊取 Android 用戶的各種個人機敏資訊，包括剪貼簿內容、GPS 地理座標、email 地址、手機門號、以及用戶手機內數據機（Modem）的 MAC 地址與無線網路 SSID 等資訊。

專家說，用戶放入剪貼簿中的資訊，極有可能是十分敏感的個資，例如用以取回加密貨幣錢包控制權的恢復短語、各種密碼、信用卡卡號、郵寄地址等；這些資訊一旦被竊且辨識出其擁有者與用途，可能導致十分嚴重的後果，例如加密資產或登入資訊被盜。

資安廠商表示，目前共發現 11 種 Android 應用程式使用該 SDK，分別為 Speed Camera Radar、AI-Moazin Lite、WiFi Mouse、QR & Barcode Scanner、Qibla Compass Ramadan 2022、Simple weather and Clock Widget、Handcent Next SMS - Text w/MSS、Smart Kit 360、AI Quran mp3、Full Quran MP3、Audiosdroid Audio Studio DAW 等，合計的下載次數超過 4,500 萬次。

資安廠商於 2021 年 10 月向 Google 通報後，這些應用程式均遭 Google Play Store 下架；不過有部分開發者在移除有問題的 SDK 後，重新將新版應用程式上架到 Google Play Store 中。

- 資料來源：
  1. The Curious Case of Coulus Coelib
  2. Android apps with 45 million installs used data harvesting SDK

2.5.3、部分 Android 裝置內 ALAC 音訊解碼器，內含遠端執行任意程式碼漏洞

資安廠商 Check Point 發現採用 Qualcomm 與 MediaTek 處理器的 Android 裝置，內建的 ALAC 音訊解碼器實作方案含有資安漏洞，駭侵者可藉以遠端執行任意程式碼。

資安廠商 Check Point 旗下的資安專家，日前發現採用 Qualcomm 與 MediaTek 處理器的 Android 裝置，內建的 Apple Lossless Audio Codec（ALAC）音訊解碼器實作方案含有資安漏洞，駭侵者可藉以遠端執行任意程式碼。

Apple Lossless Audio Codec 是由 Apple 開發的無損音訊壓縮格式，在 2011 年開放源碼；專家指出，雖然 Apple 經常針對 ALAC 推出更新與資安修補，但並非所有採用 ALAC 的廠商，都會立即套用這些更新。

這次 Check Point 資安專家發現的漏洞，即出在世界最大的兩家 Android 晶片供應商 Qualcomm 與 MediaTek 上；駭侵者可以利用特製的音訊檔案，來誘發採用 Qualcomm 與 MediaTek 的 Android 裝置發生錯誤。駭侵者可以讀寫邊界外的記憶體內容，並且用戶不知情的情形下，遠端執行任意程式碼。

這三個資安漏洞的 CVE 編號與 CVSS 危險程度評分，分別為 CVE-2021-0674（5.5 分）、CVE-2021-0675（7.8 分），以及 CVE-2021-30351（9.8 分）。

Qualcomm 與 MediaTek 已於去（2021）年 12 月修復這批漏洞，但由於 Android 手機的更新，往往必須等到手機品牌原廠推出更新才能進行，更有許多中低價位手機，在上市一兩年後，原廠就停止提供韌體更新服務，因此用

戶必須提高警覺；除了一有更新就須立即套用外，也應避免在 Google Play Store 以外處下載安裝任何手機應用程式。

- 資料來源：
  1. Largest Mobile Chipset Manufacturers used Vulnerable Audio Decoder, 2/3 of Android users' Privacy ar
  2. Critical bug in Android could allow access to users' media files

2.6、軟體系統資安議題

2.6.1、駭侵者鎖定攻擊 Microsoft Exchange Server 以散布 Hive 勒贖軟體

資安廠商 Varonis 發現 Hive 勒贖軟體相關駭侵團體，鎖定未曾修補 ProxyShell 漏洞的 Microsoft Exchange Server 發動攻擊。

資安廠商 Varonis 旗下的研究人員，近來發現 Hive 勒贖軟體相關駭侵團體，鎖定未曾修補 ProxyShell 漏洞的 Microsoft Exchange Server 發動攻擊，用以自我散布，並植入各種惡意軟體，例如 Cobalt Srtike 等。

Varonis 也指出，該駭侵者也會竊取 Microsoft Exchange Server 上的管理者登入資訊與有價值的資料，最後再發動檔案加密的勒贖攻擊。

Hive 惡意軟體本身屬於一種「勒贖即服務」（Ransomware-as-a-service）駭侵活動，有意發動勒贖攻擊者，可以「租用」Hive 來發動攻擊。最早發現於去（2021）年 6 月，當時主要的攻擊對象，以全球範圍的醫療單位、非營利組織、零售商、能源供應商等為主。

據 Varonis 的報告指出，Hive 會先尋找未曾修補 ProxyShell 相關漏洞的 Microsoft Exchange Server 進行，成功入侵之後就在 Exchange Server 可共用存取的資料夾中放置惡意後門指令檔；該指令檔可以利用系統權限來執行惡意 PowerShell 程式碼。

接著，Hive 使用該 PowerShell 程式碼，自遠端控制侵服器下載 Cobalt Strike 程式碼，並在受感染的電腦記憶體中執行；然後利用系統權限開始掃瞄

內網中的機敏資料，特別是檔名中含有「password」的檔案內容。

已知被利用的漏洞為 CVE-2021-34473、CVE-2021-34523 和 CVE-2021-31207，這些漏洞 Microsoft 於 2021 年皆已修補完成。

資安專家呼籲所有 Microsoft Exchange Server 管理者，應立即更新至最新版本，修復 ProxyShell 及各種已知漏洞，以免伺服器與內網裝置遭類似攻擊。

- 資料來源：
  1. Hive Ransomware Analysis
  2. Upgrade Exchange to the latest Cumulative Update
  3. Microsoft Exchange servers hacked to deploy Hive ransomware
  4. Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: April 13, 202
  5. Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: May 11, 2021

2.6.2、會將用戶導向惡意網站的重導服務，影響超過 16,500 個網站

資安廠商 Avast 近期發現一個名為 Parrot 的流量導向系統，實際上是由駭侵團體所控制，並且會將用戶重新導至釣魚網站或含有惡意軟體的網站。

資安廠商 Avast 旗下的研究人員，近期發現一個名為 Parrot 的流量導向系統（Traffic Direction System, TDS），實際上是由駭侵團體所控制，並且會將用戶重新導至釣魚網站或含有惡意軟體的網站；使用該服務的網站超過 16,500 個。

Avast 資安研究人員指出，Parrot TDS 的惡意攻擊，會在用戶符合某些條件（例如所在地區、語言、作業系統、瀏覽器類型）的組合時，將用戶導向到某些特定的釣魚網站，或讓用戶前往含有惡意軟體的網頁或下載檔案。

該公司的研究人員發現 Parrot TDS 涉及一起稱為「FakeUpdate」的惡意攻擊活動；該攻擊活動會將用戶導向到假冒的 Google Chrome 軟體更新網站，假稱用戶的 Chrome 瀏覽器版本過舊，要求用戶按下更新按鈕；當用戶照做後，則會下載安裝一個內含遠端遙控木馬（Remote Access Trojan, RAT）的惡意軟體。

Avast 的觀察報告指出，主要的攻擊活動似乎從 2022 年 2 月起開始進行，不過早在 2021 年 10 月起就有 Parrot 的活動跡象。

Avast 說，使用 Parrot TDS 服務的不知情網站，高達 16,500 個以上，其中有不少網站是屬於大學、地方政府、成人內容平台或個人部落格等。

該公司也發現一些 Parrot TDS 重新導向的目標網站，實際上是用來騙取 Microsoft 360 雲端服務登入資訊的釣魚網站。

在 Avast 的報告中也指出，光是 2022 年 3 月 1 日至 29 日，該公司的資安服務一共阻擋多達 600,000 次 Parrot TDS 的攻擊，險遭攻擊的用戶以巴西最多，其次為印度和美國。

- 資料來源：
  1. Parrot TDS takes over web servers and threatens millions
  2. Malicious web redirect service infects 16,500 sites to push malware

2.6.3、風力發電大廠 Nordex 遭 Conti 勒贖攻擊，IT 系統與風機管理系統停擺

德國風力發電設備製造廠 Nordex 遭到 Conti 駭侵團體勒贖攻擊，造成其 IT 系統與遠端風機管理系統無法運作。

全球最大的德國風力發電設備製造大廠，在全球擁有 8,500 名員工的 Nordex，日前證實遭到惡名昭彰，曾涉入多起重大勒贖攻擊的 Conti 駭侵團體勒贖攻擊，造成其 IT 系統與遠端風機管理系統無法運作。

Nordex 是在本月 2 日對外證實，該公司正遭到嚴重的資安攻擊，並在偵測到攻擊行動的第一時間關閉 IT 系統，以避免災情擴大。

該公司在對外發表的聲明中指出，在遭到攻擊的初期就立即採取行動，且為防範攻擊範圍擴大，該公司主動關閉跨越多地分公司、多單位使用的 IT 系統。

不過資安專業媒體 BleepingComupter 則指出，該刊於 3 月 31 日時即接獲情資指出，Nordex 因為遭到 Conti 勒贖攻擊，因此造成公司所有系統被迫離線；該情資也指出 Nordex 當時雖然啟動調查，但是並不知道攻擊來自何方。

BleepingComputer 指出，Conti 勒贖團體於 4 月 14 日宣示，該團體主導了此次對 Nordex 的攻擊。該刊也說，目前尚未發現該團體洩漏任何來自 Nordex 的機敏資料，該刊推測 Nordex 可能正在私下和 Conti 進行談判。

在 Nordex 最近發表的聲明中指出，該公司進一步的調查指出，所有本次資安攻擊，影響的都是該公司內部的設備，並無任何客戶的資料遭到外洩，攻擊也沒有影響到客戶擁有的資產。

Nordex 也說，該公司已和相關主管機關暨內外部資安專家合作，詳細調查整起攻擊事件。

- 資料來源：
  1. Update on cyber security incident
  2. Wind turbine firm Nordex hit by Conti ransomware attack

2.6.4、駭侵團體宣稱駭入可口可樂，竊得大量機敏資訊

可口可樂日前遭到某個駭侵團體對外宣稱對該公司發動駭侵攻擊；該公司目前正在進行相關調查，以便釐清是否有資料遭到竊取。

全球最大的軟性（無酒精）飲料製造廠可口可樂，日前遭到某個駭侵團體對外宣稱對該公司發動駭侵攻擊；該公司目前正在進行相關調查，以便釐清是否有資料遭到竊取。

一個名為 Stormous Ransomware 的駭侵團體，日前在某駭侵攻擊相關論壇上貼出告示，表示該團體已經駭入可口可樂公司所屬的內部網路與伺服器，並且竊得多達 161GB 的資料。

Stormous Ransomware 的貼文也說，可口可樂公司是該團體的第一個攻擊目標，目前已將這批 161 GB 的資料放在暗網上出售；如果有人願意購買，該團體也會先提供小批資料，讓買家驗證該批資料確實來自可口可樂公司。

這批資料目前在暗網站開價為 1.65 枚比特幣，換算為約為 64,000 美元。

據了解，駭侵者提供的竊得檔案，內容包括壓縮過的文件檔、內附管理者相關資訊的文字檔、電子郵件、密碼、客戶名單等多種機敏資訊。

Stormous Ransomware 團體的運作方式相當奇特，首先，這次針對可口可樂的攻擊事件，似乎並未將該公司系統內的檔案予以加密；另外，該團體也在暗網上公開要求其他駭侵團體停止為支援烏克蘭而向俄羅斯發動駭侵攻擊，否則該團體將對這些團體發動報復性攻擊。

再者，Stormous Ransomware 團體也曾在暗網上對其追蹤者發出調查表單，以決定該團體要先攻擊哪一家公司；投票結果中，可口可樂以 72% 票數高居首位，其次為玩具大廠 mattel.com、線上學習平台 Blackboard.com、奇異航空 geavation.com、綜合科技集團 danaher.com 等。

可口可樂公司目前並未對外證實資料遭竊，但該公司回覆資安媒體採訪時指出，目前正在與司法單位配合進行調查。

- 資料來源：
  1. Coca-Cola investigating claims of hack after ransomware group hawks stolen data
  2. Coca-Cola investigates hackers' claims of breach and data theft

2.6.5、三家德國風電產業相關廠商，疑遭駭侵團體攻擊

三家位於德國的風力發電產業相關廠商，近日疑似遭到駭侵團體發動駭侵攻擊，造成公司運作和生產受阻。

被攻擊的德國風電產業相關公司，其中的 Deutsche Windtechnik AG 是專精於風力發電機風扇葉片檢修的公司；該公司的遠端控制系統於四月初開始遭到攻擊，造成近 2,000 組德國境內的風力發電機組無法運作。

風力發電機組製造廠 Nordex SE 則在三月底起遭駭侵攻擊，迫使該公司關閉 IT 系統。

另一家風力發電機組製造廠 Enercon GmbH 則對外表示，該公司的衛星公司自二月開始遭到駭侵攻擊；攻擊造成該公司共 5,800 組風電機組無法順利控制，僅能在自動操作模式下運作。

據華爾街日報報導指出，在烏克蘭遭俄羅斯入侵之後，親俄羅斯駭侵團體，針對西歐各國的攻擊活動就開始升高；該報也表示，由於德國與其他西歐國家，在戰事開始後，準備在各方面降低對俄國進口石油與天然氣的依賴，因此這批針對風力發電產業的攻擊活動，很可能是為了阻礙各國尋求替代能源的努力。

據位於布魯塞爾的歐洲風力發電產業組織 WindEurope 發言人表示，由於攻擊發生的時機敏感，因此該攻擊很可能與烏俄戰爭事件有關。

受害廠商 Deutsche Windtechnik AG 的高層則表示，該產業需要更高的 IT 資安防護標準，因為對可再生能源的需求不斷提高，該產業遭到駭侵攻擊的可能性也日益增加。

- 資料來源：
  1. European Wind-Energy Sector Hit In Wave Of Hacks
  2. THE WALL STREET JOURNAL European Wind-Energy Sector Hit in Wave of Hacks

2.7、軟硬體漏洞資訊

2.7.1、Microsoft 發布 2022 年 4 月份資安更新包 Patch Tuesday

Microsoft 發布 2022 年 4 月份的例行性資安更新包，共修復多達 119 個資安漏洞。

Microsoft 日前發布 2022 年 4 月份的例行性資安更新包（Patch Tuesday）；在這次發表的資安更新包中，一共修復多達 119 個資安漏洞，包含 2 個 0-day 漏洞，更有 10 個漏洞屬於嚴重（Critical）等級。

各種 Microsoft 軟體產品的用戶與系統管理員，應立即按照指南進行更新，以減少遭駭侵者利用已知漏洞發動資安攻擊的風險。

這次 Microsoft Patch Tuesday 更新修復的漏洞，依漏洞類型區分如下：

- 執行權限提升漏洞：47 個；
- 遠端執行任意程式碼漏洞：47 個；
- 資訊洩露漏洞：13 個；
- 分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）漏洞：4 個；
- 詐騙（Spoofing）漏洞：3 個；
- Edge（Chromium）瀏覽器組件漏洞：26 個。

這次修復的兩個 0-day 漏洞分別如下：

- CVE-2022-26904：存於 Windows User Profile Service 的執行權限提升漏

洞，該漏洞證實已遭外界駭侵者大規模濫用於發動攻擊。

- CVE-2022-24521：存於 Windows Common Log 檔案系統驅動程式之中；該漏洞是由 Crowdstrike 與美國國家安全局（National Security Agency, NSA）發現。

資安專家指出，駭侵者經常利用已公開但未經修補完成的漏洞發動攻擊，因此各類微軟產品的用戶，應該立即依指示更新至最新版本，以免未及修補的漏洞，成為駭侵攻擊的破口。

- 解決方案：立即更新至最新版本。

- 資料來源：
  1. Security Update Guide
  2. Microsoft's April 2022 Patch Tuesday tackles two zero-day vulnerabilities
  3. Microsoft April 2022 Patch Tuesday fixes 119 flaws, 2 zero-days

2.7.2、Apache HTTP 伺服器漏洞揭露，QNAP 要求 NAS 用戶採取行動

QNAP 發表資安通報，要求該品牌 NAS 產品用戶，立即針對一組嚴重 Apache HTTP 伺服器揭露的漏洞採取行動。

由於 QNAP NAS 採用 Apache HTTP Server，QNAP 日前發表資安通報，要求該品牌 NAS 產品用戶，立即針對一組嚴重 Apache HTTP 伺服器揭露的漏洞採取行動，檢查設定值，以避免駭侵者利用該批漏洞發動攻擊。

台灣專業網路儲存設備廠 QNAP（威聯通），日前發表資安通報，要求該品牌網路儲存裝置（Network Attached Storage, NAS）產品用戶，立即針對一組嚴重 Apache HTTP 伺服器漏洞採取行動，檢查裝置內的相關設定值，以避免駭侵者利用該批漏洞發動攻擊。

通報指出，如果用戶保持原出廠設定值，QNAP NAS 並不受弱點影響。有兩個嚴重漏洞 CVE-2022-22721 與 CVE-2022-23943，存於 Apache HTTP server 2.4.52 與先前版本內；據 NVD 資安專家分析指出，駭侵者可以利用這兩個漏洞，以相當簡單的方式發動攻擊，且用戶難以查覺。

QNAP 指出，CVE-2022-22721 影響的是 32 位元的 QNAP NAS 裝置，而 CVE-2022-23943 則影響在其 Apache HTTP server 中啟用 mod_sed 的用戶。

這兩個漏洞的 CVSS 危險程度評分為 9.8 分（滿分為 10 分），危險程度評級為「嚴重」（critical）等級；且目前 QNAP 尚未推出正式的修補更新；不過在資安通報中，QNAP 提供了暫時解決方案。該通報建議用戶進行下列操作：

- 將 LimitXMLReuerstBody 參數保持預設值「1M」，以對應 CVE-2022-22721 漏洞；
- 停用 mod_sed 功能，以對應 CVE-2022-23943 漏洞。

QNAP 表示，在出廠設定中，mod_sed 原本就是關閉狀態；如果用戶無法確認是否維持在預設值，應立即檢視 Apache 設定，有必要時應關閉 mod_sed。

QNAP 也指出，目前正在調查這兩個漏洞造成的影響，並將儘快推出解決這兩個漏洞的韌體更新，請用戶密切注意，有更新應立即套用。

- 資料來源：
  1. Investigating Multiple Vulnerabilities in Apache HTTP Server
  2. QNAP asks users to mitigate critical Apache HTTP Server bugs

2.7.3、超過百款聯想筆電內含 UEFI 漏洞，建議立即更新

Lenovo 針對旗下一百款以上的筆記型電腦推出資安更新，修復 3 個存於 UEFI 韌體驅動程式內的資安漏洞，建議用戶立即更新。

全球市佔率相當高的 PC 大廠 Lenovo（聯想），日前針對旗下一百款以上的筆記型電腦推出資安更新，修復 3 個存於 UEFI 韌體驅動程式內的資安漏洞，用戶應立即更新。

這三個漏洞是於去（2021）年由資安廠商 ESET 旗下的資安研究人員發現，並於該年 10 月通報給原廠；含有這三個漏洞的筆電款式甚多，包括 Lenovo IdeaPad 3、Legion 5 Pro-16ACH6 H 與 Yoga Slim 9-14IYL05 等系列，全球使用者人數可能多達數百萬人。

三個漏洞中，有兩個（CVE-2021-3971 和 CVE-2021-3972）漏洞，可讓駭侵者關閉針對 SPI 快閃記憶體的機制，而 SPI 快閃記憶體係用以儲存 UEFI 韌體程式碼；這樣駭侵者即可在電腦啟動（boot）期間執行非由原始製造廠（Original Equipment Manufacturer, OEM）提供簽署的程式碼。

另一個漏洞 CVE-2021-3970 則可讓本地端的駭侵者，利用此漏洞提升執行權限，並且於本土端執行任意程式碼。

聯想除了於近日提供新版韌體，修復上述三個漏洞外，也在官網提供所有含有上述漏洞的筆記型電腦形號清單；所有使用 Lenovo 品牌筆記型電腦的用戶，應立即核對自己使用的產品是否列名於清單內，同時立即升級至最新版本韌體，以免遭駭侵者利用這三種已知漏洞發動攻擊。

- CVE 編號：CVE-2021-3970、CVE-2021-3971 和 CVE-2021-3972
- 影響產品：詳見聯想官網清單。
- 解決方案：依指示更新至最新版本韌體。

- 資料來源：
  1. When “secure” isn’t secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer la
  2. Lenovo Notebook BIOS Vulnerabilities
  3. Product Impact:

2.7.4、Google Chrome 緊急修復已遭濫用於攻擊的 0-day 高危險漏洞

Google 推出新版 Google Chrome 瀏覽器版本 100.0.4896.127，修復一個證實已遭駭侵者濫用於資安攻擊的 0-day 漏洞 CVE-2022-1364。

Google 日前緊急推出新版 Google Chrome 瀏覽器版本 100.0.4896.127，修復一個證實已遭駭侵者濫用於資安攻擊的 0-day 漏洞 CVE-2022-1364；廣大 Google Chrome 用戶應立即升級至最新版本。

目前關於 CVE-2022-1364 這個漏洞的公開資訊並不多，僅知該漏洞存於 Google Chrome 的 V8 JavaScript 引擎內，屬於一種「類型混淆」（type confusion）漏洞；這種漏洞一旦發生，通常會導致瀏覽器崩潰，駭侵者進而可以讀寫超出緩衝區漏洞的記憶體內容，並且進一步執行任意程式碼。

該漏洞的 CVSS 危險程度評分為 8.8 分（滿分為 10 分），危險程度評級為「高」（high）；本漏洞是由 Google 旗下的威脅分析小組資安專家 Clément Lecigne 發現並提報至 Google Chrome 團隊，該團隊在一天以內即推出了漏洞修復新版。

雖然 Google 在更新通報中指出，該公司已獲悉有駭侵團體使用此漏洞進行攻擊的情報，但 Google 認為應該要等多數用戶都完成更新後，再對外透露更詳細的資訊，因此目前對於此類攻擊的泛濫程度尚不得而知。

本 0-day 漏洞也是今（2022）年至今 Google Chrome 修復的第 3 個 0-day 漏洞。

鑑於 Google Chrome 是世界上占有率最高的瀏覽器，用戶數量眾多且跨及多個作業系統平台，因此用戶恐處於極大風險之下。包括 Windows、macOS、Linux 作業系統的 Google Chrome 用戶，都應立即更新至最新版本，以避免潛在的資安攻擊風險。

- CVE 編號：CVE-2022-1364
- 影響產品：Google Chrome 100.0.4896.127 之前各作業系統（Windows、macOS、Linux）版本。
- 解決方案：更新至 Google Chrome 100.0.4896.127 或其後續版本。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google Chrome < 100.0.4896.127 Vulnerability
  3. Google Chrome emergency update fixes zero-day used in attacks

第 3 章、 資安研討會及活動

工研院【網路資安工程師國際雙證培訓班】	
活動時間	**2022-05-10(二) ~ 2022-06-17(五) 09:00 ~ 16:00**
活動地點	**台灣高雄市前鎮區一心一路 243 號 4 樓之 1 高雄學習中心**
活動網站	**https://www.accupass.com/event/2204050753431500876000**
活動概要	 **主辦單位：工研院產業學院** 企業競爭力的核心，就是資訊！ 提早佈局資安策略，保障經營命脈，避免駭客傷害！公司營運，在網路世紀大不易， 2021 上市櫃公司重大資安事件高達 16 家， 病毒攻擊、資訊外洩.....， 嚴重影響企業經營，需要挺身捍衛， 和 AI 人才一樣吸金，資安專業現在有更多展現能力的機會！ 數位之境，由你守護！工研院【網路資安工程師國際雙證培訓班】 高雄場初次開班，用鍵盤就能完成的生涯規劃等著你實現！

第 3 屆 ICANN APAC-TWNIC Engagement Forum 暨第 37 屆 TWNIC IP 政策資源管理會議	
活動時間	**2022 年 5 月 12-13 日**
活動地點	**台北福華大飯店 B2 福華廳**
活動網站	**https://forum.twnic.tw**
活動概要	 **主辦單位：ICANN、TWNIC** 3rd ICANN APAC-TWNIC Engagement Forum with 37th TWNIC IP Open Policy Meeting 網際網路名稱與號碼指配組織（ICANN）與台灣網路資訊中心（TWNIC）共同舉辦第 3 屆 ICANN APAC-TWNIC Engagement Forum，暨第 37 屆 TWNIC IP 政策資源管理會議，即將於 5 月 12、13 日以實體及線上直播同步登場！ 盛大邀請產、官、學各界利害關係人以及全球社群，藉此交流機會，重新見解網路本質，在全球要跨入網路世界的下個維度前，可以深度討論全球域名系統、網路位址政策及網路安全等關鍵議題，讓本就於亞太區擔任關鍵要角的台灣，能藉此機會實際面對全球網路議題，進一步建構更安全穩定的網路使用環境。 本次活動特別邀請嘉賓網路之父 Vinton Cerf 一齊與會，引領大家從

	網際網路的本質啟動探討，其他重量級講者及與會貴賓還包含：DotAsia 亞洲域名註冊機構行政總裁暨 ICANN Board 董事鍾宏安、日本 JPNIC 網路發展部門總經理暨 ICANN 董事 Akinori Maemura、網際網路協會 (ISOC) 總裁兼執行長 Andrew Sullivan、丹麥奧胡斯大學：媒體與資訊研究國際傳播政策系名譽教授 Wolfgang Kleinwaechter、亞太網路資訊中心（APNIC）總裁 Paul Wilson、行政院政務委員唐鳳、國家通訊傳播委員會鄧惟中委員、臺灣網路治理論壇理事長吳國維、網際網路與司法管轄政策網路組織之域名管轄部門總監 Elizabeth Behsudi 等，集結國、內外多位專家學者，針對網路公共政策、網路治理、隱私、網路安全等議題進行深入探討，期盼借力國際重量級嘉賓的知識及觀點交流，激發深度有價值對話，進一步推動台灣網路資訊的產業穩定及安全發展。

【資安學院】資通系統防護基準實務課程	
活動時間	**5/26-5/27 09:00 ~ 17:00**
活動地點	**中華民國資訊軟體協會 訓練教室** **（台北市大同區承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/2742**
活動概要	數位轉型 軟協與您共行 中華民國資訊軟體協會 CISA Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 課程說明：因應網際網路及其他資通科技快速發展與普及，為保障障國家安全，維護社會公共利益，並建立以風險管理為核心的機制，行政院於 108 年 1 月 1 日起正式實施資通安全管理法，而為了確保資通訊系統之安全，亦於同年 8 月 26 日修正發布附表十之資通系統防護機準，各機關需依系統等級施行「資通系統防護基準」。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

【資安學院】資安事故處理實務演練	
活動時間	**6/22-6/23 09:00 ~ 17:00**
活動地點	**中華民國資訊軟體協會 訓練教室** **（台北市大同區承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/2753**
活動概要	數位轉型 軟協與您共行 中華民國資訊軟體協會 CISA Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 課程說明：近期政府企業遭受勒索病毒、APT 攻擊等資安事故頻傳，當資安事件發生時，應如何正確因應、處理及保全數位證據，成為政府企業必須正面以對之嚴肅課題。本課程將說明政府企業於發生資安事故時，應如何迅速釐清受害範圍、清除惡意程式及阻斷可疑之中繼站連線，進而回復至正常運作。 本課程並以 Window 模擬環境為例，解析駭客入侵之情境，搭配實作解說資安事件處理流程，調查入侵事件的樣貌，而做出正確的因應。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布漏洞嚴重程度前五名之漏洞資訊如下表：

ASUS RT-AX88U - Format String	
TVN / CVE ID	TVN-202203007 / CVE-2022-26674
CVSS	9.8 (Critical)
影響產品	ASUS RT-AX88U firmware pre v3.0.0.4.386.4606
問題描述	ASUS RT-AX88U 存在 Format String 漏洞，遠端攻擊者不須權限，即可利用此漏洞寫入任意記憶體位址，進行遠端程式碼執行，對設備進行任意操作或中斷服務。
解決方法	Update RT-AX88U firmware version to 3.0.0.4.386.46065
公開日期	2022-04-22
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6043-0f72c-3.html

ASUS Control Center - SQL Injection	
TVN / CVE ID	TVN-202203002 / CVE-2022-26669
CVSS	8.8 (High)
影響產品	ASUS Control Center v1.4.2.5
問題描述	ASUS Control Center 存有 SQL Injection 漏洞，遠端攻擊者在取得一般使用者權限後，可利用特定 API 參數注入 SQL 指令，取得資料庫結構或資料。
解決方法	Update version to 1.4.3.2
公開日期	2022-04-26
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6056-b0d90-3.html

ASUS WebStorage - Use of Hard-coded Credentials	
TVN / CVE ID	TVN-202203005 / CVE-2022-26672
CVSS	7.3 (High)
影響產品	ASUS WebStorage Android version <= 3.10.1
問題描述	ASUS WebStorage 之 API Token 以明文方式 Hard-code 於 APP 原始碼中，導致遠端攻擊者不須權限，即可利用該 Token 建立連線，針對一般使用者，進行嘗試登入攻擊行為，如果成功可取得該使用者權限，藉以查看、修改與刪除個人資訊。
解決方法	ASUS WebStorage Android version >= 3.10.2
公開日期	2022-04-22
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6041-7bd67-3.html

ASUS Control Center - Broken Access Control	
TVN / CVE ID	TVN-202203001 / CVE-2022-26668
CVSS	7.3 (High)
影響產品	ASUS Control Center v1.4.2.5
問題描述	ASUS Control Center 之 API 功能允許遠端攻擊者在不須登入的情況下，透過調用特定 API 功能，藉以操作部分系統功能或導致服務異常。
解決方法	Update version to 1.4.3.2
公開日期	2022-04-26
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6055-c6500-3.html

Realtek USB FE/1GbE/2.5GbE/5GbE NIC Family - Buffer Overflow	
TVN / CVE ID	TVN-202202008 / CVE-2022-21742
CVSS	6.2 (Medium)
影響產品	Realtek USB FE/1GbE/2.5GbE/5GbE NIC Family 受影響版本如下： Windows 10 平台：10.28 - 10.39 Windows 8 平台：8.49 - 8.60 Windows 7 平台：7.42 - 7.53
問題描述	Realtek USB 驅動程式之 API 功能未作參數長度驗證，導致 Buffer Overflow 漏洞。區域網路內的攻擊者不須權限，即可利用該漏洞中斷服務。
解決方法	Update version to v10.50
公開日期	2022-04-26
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6057-1cd0d-3.html**

第 5 章、 2022 年 4 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。

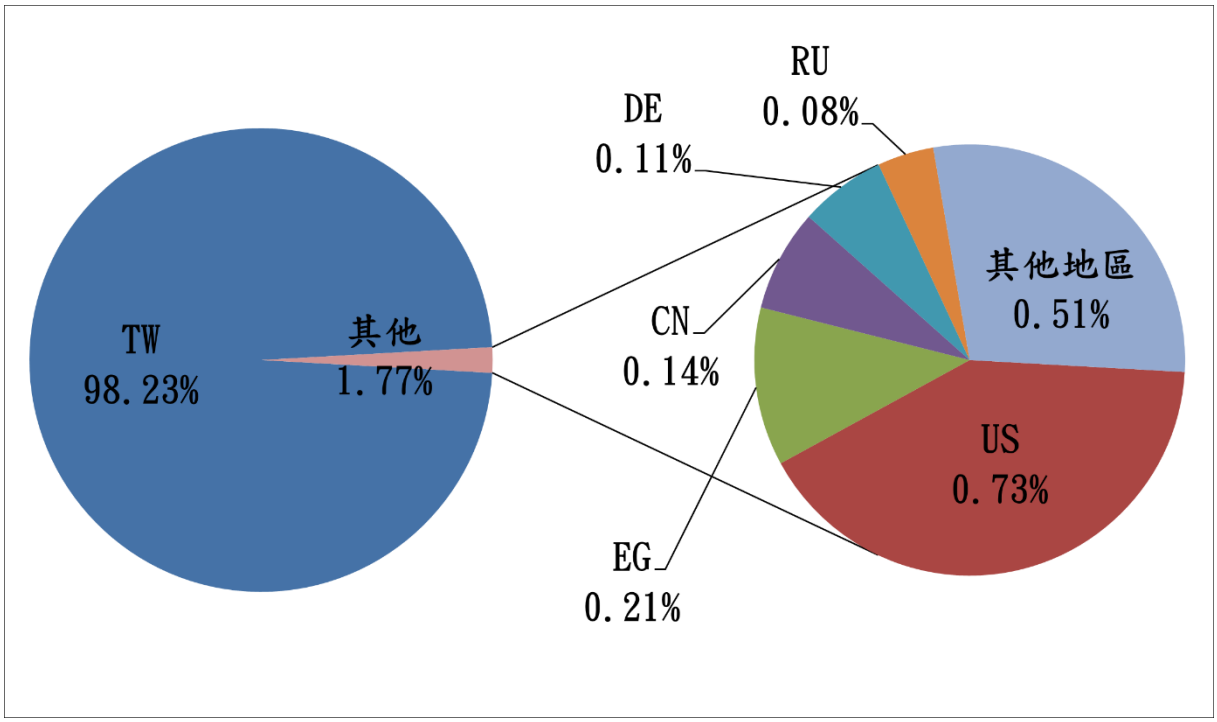

圖 1、分享地區統計圖

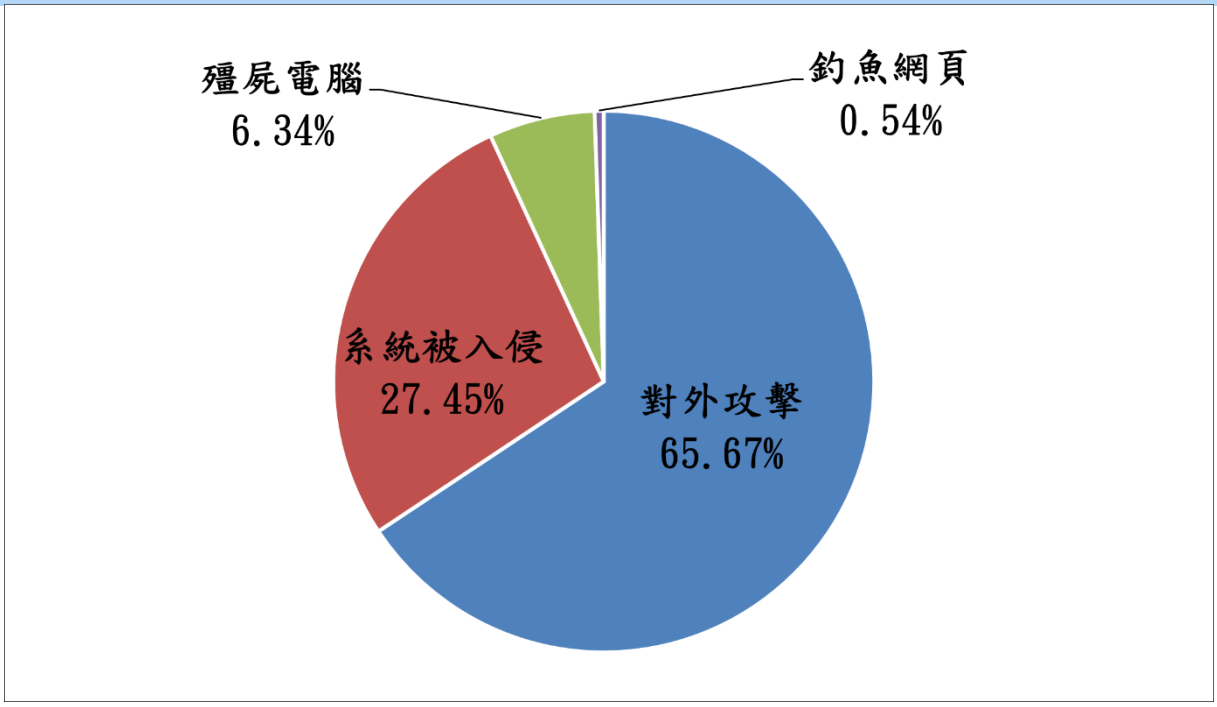

圖 2、分享類型統計圖

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：**2022 年 5 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**