TWCERT/CC 資安情資電子報

2021 年 9 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 4 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、新興應用資安、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、軟體系統資安議題及軟硬體漏洞資訊。

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、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

多廠牌路由器登入驗證跳過漏洞，現已遭大規模用於攻擊

網通大廠旗下的資安研究團隊，發現一個出現在多廠牌路由器的嚴重資安漏洞，可導致駭侵者跳過登入驗證過程，直接取得路由器的控制權。

全球網通大廠 Juniper 旗下的資安研究團隊，近日發現一個出現在多廠牌路由器的嚴重資安漏洞，可導致駭侵者跳過登入驗證過程，直接取得路由器的控制權；該漏洞且已遭駭侵者大規模用於攻擊。

資安專家指出，該漏洞出現在各廠牌路由器採用的公版 Arcadyan firmware，目前更多現有駭侵者利用此漏洞跳過路由器登入驗證程序，取得路由器控取權限後，在路由器內安裝名為 Mirai 的僵屍網路惡意軟體。

該漏洞的 CVE 編號為 CVE-2021-20090，發生在 Arcadyan 公版路由器韌體程式的 web 控制界面；攻擊者可以利用這個漏洞，在被攻擊的路由器中啟動 telnet 連線，以命令列方式控制受到感染的路由器。

這個 CVE-2021-20090 漏洞的 CVSS 分數高達 9.9 分（滿分為 10 分）；據資安專家表示該漏洞存於 Arcadyan 公版韌體至少有 10 年以上。

據該團隊發表的研究報告指出，目前已知有 17 個廠牌，20 種以上的各廠牌路由器產品內含此一漏洞，其中包括在台灣比較暢銷的品牌 4 款路由器在內（DSL-AC88U、DSL-AC87VG、DSL-AC3100、DSL-AC68VG）。

值得注意的是，Juniper 是在發表了該漏洞的概念驗證攻擊方法後 2 天，開始觀察到有駭侵者利用此漏洞大規模發動攻擊。

由於含有此漏洞路由器的廠牌極多，用戶應隨時注意原廠發表的更新訊息，在原廠發表的韌體更新程式推出後，應立即進行更新。

- CVE 編號：CVE-2021-20090
- 影響產品/版本：詳見 Juniper 資安研究報告中列表

- 資料來源：
  1. Freshly disclosed vulnerability CVE-2021-20090 exploited in the wild
  2. Actively exploited bug bypasses authentication on millions of routers

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、網路服務商記錄到 HTTP DDoS 攻擊強度新高

雲端網路服務商指出，分散式服務阻斷攻擊（DDoS）的強度正在不斷提高；今年記錄到的最高攻擊強度，高達每秒鐘 1,700 萬次連線要求。

雲端網路服務商 Cloudflare 日前發表研究報告，指出分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）的攻擊強度，正在逐年不斷提高；今年記錄到的最高攻擊強度，高達每秒鐘 1,700 萬次連線要求。

Cloudflare 指出，該公司的網路保護系統，稍早記錄到一起全球性的 DDoS 攻擊事件，攻擊規模與強度打破該公司歷年來的觀測記錄；除了攻擊強度高達每秒 1,720 萬次連線要求外，其攻擊次數相較於 Cloudflare 在 2021 年第二季的平均服務能量每秒 2,500 次連線要求，也高達 70%。

Cloudflare 在報告中說，該次攻擊發在生七月，持續不到 1 分鐘，是非常短暫而強烈的攻擊，被攻擊的對象是某家金融產業組織，在短短幾十秒的時間內，遭到了 3 億 3,000 萬次連線要求；其中高達每秒 1,500 萬次以上連線要求的強大攻擊密度維持了 15 秒。

Cloudflare 說，這次駭侵者發動的 DDoS 攻擊，係由一個包括至少 20,000 台裝置的僵屍網路所發動的，其連線要求來自全球各地；以 IP 數量來看，高

達 15% 的攻擊連線來自印尼，其次為印度與巴西（合計達 17%），接著是越南、烏克蘭、柬埔寨、泰國、孟加拉、俄羅斯、南非、波蘭、阿根廷、巴基斯坦、墨西哥與其他國家。

Cloudflare 也說，除了這次攻擊外，近期也經常觀察到其他強烈的 DDoS 攻擊，主要目標係針對亞太區的網路接取服務供應商、電信業者、網站託管業者與遊戲廠商。

- 資料來源：
  1. Cloudflare thwarts 17.2M rps DDoS attack — the largest ever reported
  2. HTTP DDoS attacks reach unprecedented 17 million requests per second

2.1.2、資安廠商公布 SaaS 服務統計，雲端用戶資安設定高達 44% 發生錯誤

資安廠商發表雲端 SaaS 的資安調查報告，發現高達 44% 的用戶資安設定是錯誤的，不當給予過高的操作權限，對 SaaS 用戶的資安造成嚴重潛在風險。

資安廠商 Varonis 日前發表一份關於雲端 SaaS（Software as a Service，軟體即服務）的資安調查報告，發現多種 SaaS 使用者帳號資安設定的錯誤。

Varinos 是利用 DatAdvantage Cloud 服務，收集該公司客戶在使用各種 SaaS 服務，如 Amazon Web Services、Box、GitHub、Google Drive、Jira、Okta、Salesforce、Slack、Zoom 等知名常見 SaaS 服務的資料，經由分析後得到此 SaaS 資安研究報告的統計數字。

在這份報告列舉的多項統計數字中，其中有高達 44% 的 SaaS 用戶，其資安設定是錯誤的；管理者經常不當給予組織成員過高的操作權限，使其可以存取超過其職務所需範圍的資料，或進行不必要的操作；這可能對該 SaaS 使用單位的資安造成嚴重潛在風險。

另外有高達 75% 的約聘工作者使用的 SaaS 帳號，在該約聘人員離職之後，並未立即由管理員進行關閉歸檔的操作，反而持續能夠使用；這種錯誤也很容易造成潛在的資安風險，因為不只是約聘人員可能被駭侵者以各種方法攻擊，造成登入資訊被竊，約聘人員本人也可能竊取之前工作上獲得的資訊。

報告也指出，有 15% 的 SaaS 企業用戶員工，會將自己 SaaS 帳號中的資料或檔案，轉存到個人擁有的裝置或個人雲端服務帳號中。

統計數字也說，在所有 SaaS 雲端服務中，有高達 43% 的帳號處於被放棄的狀態；這些帳號久未使用，但也沒有被各 SaaS 企業用戶的負責管理者將之移除或回收，就此棄之不顧；這對駭侵者來說充滿可趁之機，也對 SaaS 用戶本身造成極大的資安風險。

- 資料來源：
  1. 43% of all cloud identities are abandoned
  2. 2021 SaaS Risk Report Reveals 44% of Cloud Privileges are Misconfigured
  3. 44% of cloud privileges are misconfigured, warns Varonis Featured

2.2、新興應用資安

2.2.1、硬體亂數產生器的嚴重錯誤，將導致數十億台 IoT 裝置面臨資安風險

資安廠商發現普遍應用於 IoT 裝置硬體中的「亂數產生器」存有錯誤，可能因此導致全球數十億台 IoT 裝置面臨嚴重資安攻擊風險。

資安廠商 Bishop Fox 旗下的研究人員 Dan Petro 與 Allan Cecil，日前發現普遍應用於 IoT 裝置硬體中的「亂數產生器」（Random Number Generator, RNG）存有嚴重錯誤，可能因此導致全球數十億台 IoT 裝置面臨嚴重資安攻擊風險。

兩位研究人員在報告中指出，這些有問題的硬體亂數產生器，原本應該在每次運作時都隨機產生無法預測的亂數；但在某些需要頻繁產生亂數的使用情境時，有時會產生僅部分無序的亂數，有時產生的亂數都是 0，甚至還可能造成記憶體初始錯誤。

研究人員指出，由於這個亂數產生器的錯誤發生在硬體層，因此無法以作業系統或軟體方式加以修補；研究人員也說而為 IoT 裝置撰寫的軟體，通常都不會針對亂數產生的結果予以嚴密檢查。

由於在各種 IoT 裝置的資料加密過程中，加密金鑰的生成過程，需要使用硬體亂數產生器產生的亂數；一旦這些加密金鑰是有序的、容易預測，甚至根本就是 0 的話，加密的內容就很容易遭到解密，因而使得加密過程變得無效，影響這些 IoT 裝置的資安。

另外，這些 IoT 裝置搭載的作業系統，因為成本和執行效能的考量，大多是簡化的版本，在作業系統層面並未提供軟體亂數產生機制，而這類 IoT 裝置的數量又極多，估計全球約有數十億台已布署的 IoT 裝置。而這些 IoT 裝置在上市後的軟體更新極為困難，因此該錯誤對採用這些 IoT 裝置的公私單位、組織與個人，可能產生嚴重的資安風險。

- 資料來源：
  1. You're Doing IoT RNG
  2. Aug 9, 2021 FUNDAMENTAL FLAW IN RNGS AFFECTS MANY IOT DEVICES By Dennis Fisher
  3. A Critical Random Number Generator Flaw Affects Billions of IoT Devices

2.2.2、數千萬台 IoT 裝置內含嚴重資安漏洞，可導致駭侵者取得監看監聽資訊

資安專家發現一個嚴重資安漏洞，存於數千萬台使用 Kalay IoT 雲端平台與開發工具的 IoT 產品中，可導致駭侵者取得這些 IoT 裝置產生的監控資訊。

資安廠商 Mandiant 旗下的資安專家，在 2020 年底發現一個嚴重資安漏洞，存於數千萬台使用 Kalay IoT 雲端平台與開發工具的 IoT 產品中；這些 IoT 產品主要是連網監視裝置，該漏洞可導致駭侵者遠端取得這些 IoT 裝置產生的監控資訊，甚至於裝置控制權。

該漏洞的 CVE 編號定為 CVE-2021-21873，發生在提供給 IoT 裝置廠商用以開發軟體所需的開發工具（SDK）內的 Kalay protocol；其 CVSS 危險程度評分高達 9.6 分（滿分為 10 分）。

資安專家指出， 各種支援 Kalay protocol 的 IoT 裝置，只需要提供一個裝置的不重覆識別碼（UID），即可註冊使用 Kalay 雲端服務，並且把監控資料儲存到其雲端伺服器內；而該裝置的用戶在使用 Kalay 提供的行動 app 或 web 界面時，也只需提供該 UID，即可取得存在雲端的監控資料。

由於驗證過程的安全性很薄弱，因此攻擊者可以透過提供 UID，以偽造身分的方式，即可自 Kalay 雲端服務中輕易取得監控畫面或錄音的資料，甚至還能進一步結合其他漏洞，完全控制監裝置。

Mandiant 的資安專家以此漏洞為基礎，發展出的攻擊概念證明程式，可以透過此漏洞掃瞄裝置、註冊並取得 UID、遠端連線到該裝置並登入其控制界面，最終取得監控的畫面與音訊資料。

此漏洞已經緊急推出暫時解決方案，美國資安主管機關 CISA 也發表資安通報，提供技術指導與處理建議。

- 資料來源：
  1. Please Update the SDK Version to Minimize the Risk of Sensitive Information Being Accessed by Unauth
  2. ICS Advisory (ICSA-21-229-01) ThroughTek Kalay P2P SDK
  3. Critical bug impacting millions of IoT devices lets hackers spy on you

2.2.3、去中心化交易協定 Poly Network 遭駭，被竊資金高達 6.11 億美元

跨鏈加密貨幣交易平台 Poly Network 發生加密貨幣駭侵案件；該協定在數個區塊鏈的流動性池同時遭到駭侵攻擊，損失金額高達 6.11 億美元。

提供跨區塊鏈加密貨幣交易轉換的交易平台 Poly Network，日前發生加密貨幣史上最大的駭侵案件；該協定在數個區塊鏈的流動性池，在同一時間遭到駭侵攻擊，被竊取的損失金額高達 6.11 億美元。

Poly Network 提供的服務，是在不同的區塊鏈上轉換加密貨幣，包括比特幣、以太幣與 Ontology。據區塊鏈專業媒體 The Block 的研究人員 Igor Igamberdiev 指出，Poly Network 被攻擊的原因是出在加密問題之上。

這次 Poly Network 被竊事件，同時發生在多個區塊鏈協定上；據目前的估計，Poly Network 在以太坊上被竊的以太幣資金多達 2.73 億美元、在幣安智慧鏈 (Binance Smart Chain）上損失的幣安幣（BNB）也高達 2.53 億美元、而在 Polygon Network 區塊鏈上損失的 USDC 穩定幣則為 8,500 萬美元。

值得一提的是，在這起駭侵事件發生後，管理集中化穩定幣泰達幣（USDT）的 Tether 公司，立即將等值 3,300 萬美元的泰達幣加以鎖定，使得駭客無法進行轉帳洗錢。

不過，幣安交易所的創辦人則在 Twitter 上指出，該公司雖然知道這次攻擊事件，也盡全力提供各式協助，但因為幣安智慧鏈與以太坊都是高度去中心化的區塊鏈，沒有人能夠完全控制該鏈上的活動，因此無法保證任何事，只能在其能力範圍能盡力協助。

目前幣圈各界正在密切注意被竊資金的流向，但駭客很可能透過隱密性較高的門羅幣等其他加密貨幣進行洗錢。該案後續發展仍有待觀察。

- 資料來源：
  1. At least $611 million stolen in massive cross-chain hack
  2. Over $600 million reportedly stolen in cryptocurrency hack

2.2.4、日本加密貨幣交易所 Liquid 遭駭，損失高達 9,400 萬美元以上

日本加密貨幣交易所 Liquid，日前發生嚴重駭侵攻擊事件，其熱錢包遭攻擊，損失高達 9,400 萬美元以上。

日本加密貨幣交易所 Liquid，日前發生嚴重駭侵攻擊事件；該交易所用來儲存用戶帳號加密貨幣資產的熱錢包遭到攻擊，目前已知的損失高達 9,400 萬美元以上。

Liquid 是全球規模最大的加密貨幣 / 法幣交易所之一，擁有八十多萬名註冊用戶，這些用戶的全球分布超過 100 個國家；且該交易所每天的加密貨幣交易額超過 11 億美元。

Liquid 在駭侵攻擊事件發生後，隨即在官方的 Twitter 帳號發布公告，承認其熱錢包遭到駭侵者挾持；該公司立即將尚未遭竊的加貨貨幣資產轉移到較安全的冷錢包中，同時暫停所有加密貨幣相關交易。包括加密貨幣的買賣與轉帳，在調查活動完成之前都無法進行，但法幣的交易與存提款不受影響。

Liquid 也說，被竊取的 9,400 萬美元加密貨幣資產，總共包括 69 種不同的加密貨幣；這些加密貨幣在未經授權的情形下，被轉出到其他加密貨幣交易所或去中心化交易所 (DeFi Swap) 中。

被竊加密資產依各幣種區分，分別為以太幣（ETH） 3,090 萬美元、瑞波幣（XRP）1,290 萬美元、比特幣（BTC）480 萬美元、各種穩定幣 770 萬美元、Tron 20 萬美元、其他代幣共計 3,740 萬美元。

加密貨幣資安專家指出，由於有高達 4,500 萬美元的以太幣，被轉入去中心化交易所如 Uniswap 與 Sushiswap，因此難以追查竊取者的身分，以及其金流動向。

資安專家多次呼籲加密貨幣持有人，儘可能避免將自己的加密貨幣資產，存在風險極高的交易所管理熱錢包中；應轉帳回自己持有的冷錢包中妥善存放，以降低遭竊風險。

- 資料來源：
  1. Liquid Global Official @Liquid_Global
  2. Liquid cryptocurency exchange loses over $90 million following hack

2.2.5、駭客假冒 OpenSea 交易所客服人員，竊走求助用戶的加密貨幣與 NFT 收藏

NFT 交易所 OpenSea 遭駭侵者假冒為其客服人員，藉機竊走求助用戶存於錢包內的加密貨幣與 NFT 收藏。

NFT 交易所 OpenSea 近日遭駭侵者在社群平台 Dischord 上假冒為其客服人員，藉機竊走求助用戶存於錢包內的加密貨幣與 NFT 收藏。

據資安專業媒體 BleepingComputer 報導，最近有不明身分的駭侵者，在 NFT（Non-Fungible Token 非同質性代幣）交易網站 OpenSea 在新興社群網站 Dischord 上設立的討論群組中，假冒為 OpenSea 的客服人員，藉以詐騙竊取求助用戶的加密貨幣與 NFT 收藏品。

駭侵者的詐騙手法，是在 OpenSea 的官方 Dischord 頻道中觀察用戶貼文，一旦發現有用戶提出相關問題，便假冒為 OpenSea 官方客服人員，傳遞私訊給貼文用戶，假稱可以解決用戶在 OpenSea 的各種使用問題。受害者往往會因其親切的「服務態度」等話術而受騙上當。

一旦用戶上鉤，駭侵者就會要求受害者連上假冒的「客服系統」伺服器，並且要求用戶開啟電腦畫面分享權限；用戶照做後，駭侵者就會要求用戶「重新同步」通用加密貨幣錢包軟體 MetaMask 的手機版應用程式與桌面版 Google Chrome 瀏覽器外掛程式，並在畫面上顯示含有 MetaMask 用戶設定錢包復原密語的 QR code 畫面。

駭侵者此時即可擷取該 QR code，利用此 QR Code 取得受害用戶的 MetaMask 錢包控制權，輕鬆竊走受害者存於錢包內的加密貨幣與 NFT 收藏

品。

OpenSea 表示獲悉用戶遭詐騙一事，但沒有提供受害金額與受害者人數等資訊；該公司呼籲用戶在求助時，應利用該公司官方網站上提供的客服連絡方式，切勿使用如 Dischord 或 Twitter 等社群平台，以免給予駭侵者可乘之機。

- 資料來源：
  1. jeffnicholas.eth @_jeffnicholas_
  2. Nate Chastain (natec.eth) @natechastain
  3. Fake OpenSea support staff are stealing cryptowallets and NFTs

2.3、國際政府組織資安資訊

美國資安主管機關 CISA 聯手 Google、Amazon、Microsoft 以打擊勒贖攻擊

美國 CISA 公布一項計畫，結合公部門與民間力量防制勒贖攻擊等資安威脅；首波民間合作單位包括 Amazon、Google、Microsoft 等多家企業。

美國資安主管機關資訊安全與基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA），日前公布一項名為「聯合資安防護協作」（Joint Cyber Defense Collaborative，JCDC）的合作計畫；該計畫旨在結合公部門與民間力量，共同防制勒贖攻擊等各種資安威脅。

該專案的目的，是讓 CISA 可以發展各種資安協同防護計畫，結合美國各級政府（聯邦、州與地方政府）以及民間企業或組織的力量，以發揮整體防護戰力，對抗日益猖獗的資安攻擊，保護可能遭到攻擊的各種關鍵基礎設施。

在 JCDC 發表的首波民間合作單位，即包括 Amazon Web Services、Google Cloud、Microsoft、AT&T、Crowdstrike、FireEye Mandiant、Lumen、Palo Alto Networks、Verizon 等多家企業，其業務範圍包括資安防護、雲端服務、電信服務等資安相關的重要關鍵基礎設施。

已經加入 JCDC 計畫的美國各級政府單位，則包括美國國防部、國家安全局、司法部、聯邦調查局、美國網路作戰司令部、國家情報總監辦公室（Office of the Director of National Intelligence）等。

CISA 總監 Jen Esterly 在 JCDC 的新聞稿中指出，同意加入 JCDC 的產業合作伙伴，將與 CISA 和各相關政府單位並肩作戰，共同對抗各種針對美國發動的資安攻擊事件，並且同步發展新的解決方案。

- 資料來源：
  1. CISA LAUNCHES NEW JOINT CYBER DEFENSE COLLABORATIVE
  2. CISA teams up with Microsoft, Google, Amazon to fight ransomware

2.4、社群媒體資安近況

求職社群網站 LinkedIn 遭發現漏洞，任何人均可冒名任何公司發布職缺訊息

資安專家發現全球熱門求職求才社群網站 LinkedIn 的流程漏洞：任何人均可冒名任何公司張貼虛假求才訊息。

資安專家 Herman Singh 近曰發現全球熱門求職求才社群網站 LinkedIn，在張貼職缺的流程中存有一個嚴重漏洞，導致任何人均可冒名任何公司張貼虛假求才訊息，不但能取得求職者的詳細資訊，也能夾帶各種惡意檔案，進一步發動各種駭侵攻擊。

據資安專業媒體 BleepingComputer 的測試，LinkedIn 在張貼求才職缺訊息的流程中，預設情形下並未限制僅能由求才公司所屬的帳號來張貼職缺訊息，因此任何人都能「代替」任何公司，在 LinkedIn 上張貼職缺；而且用這種方式張貼出來的職缺，看起來和被冒名公司開出的職缺，幾乎沒有差別。

資安專家指出，LinkedIn 在張貼職缺公告的這個漏洞，將可導致嚴重的資安風險；一來會有很多不知情的求職者，針對虛假的大公司熱門職缺投遞個人履歷，駭侵者可藉以收集大量求職者的機敏個資，包括姓名、性別、Email、照片、工作經歷、連絡方式等資訊，另外還可以在求職訊息中夾帶各式可用來進行駭侵攻擊的元件，例如植入惡意軟體的檔案、將求職者導向惡意網站，以發動釣魚攻擊的連結等等。

BleepingComputer 指出，在 LinkedIn 網站上，並未提供驗證張貼者真實資格的流程，也沒有選項可讓公司行號限制只有哪些帳號可以張貼連結；

BleepingComputer 去函微軟公司旗下的 LinkedIn 資安團隊，也沒有得到具體的解釋。

資安專家建議各大公司的人資部門人員，在 LinkedIn 針對此問題提出解決方案前，應該提高警覺，定期巡查自己公司在 LinkedIn 上的相關內容，並且透過搜尋功能，檢視有無任何冒名張貼職缺的情況，發現後即刻回報 LinkedIn 進行處理。

- 資料來源：
  1. The Fake Job Offer Scam on LinkedIn
  2. You can post LinkedIn jobs as almost ANY employer — so can attackers

2.5、行動裝置資安訊息

2.5.1、Google Play Protect 僅能偵測出 31% 的 Android 追蹤監控惡意軟體

資安廠商發表研究報告，指出 Google Play Store 內建的 Google Play Protect 惡意軟體偵防機制，僅能偵測到 31% 的 Android 追蹤監控惡意軟體。

資安廠商 Atlas VPN 旗下的資安研究人員日前發表研究報告，指出 Google Play Store 內建的 Google Play Protect 惡意軟體偵防機制，在測試中表現不佳，僅能偵測到 31% 的 Android 追蹤監控惡意軟體（Stalkerware），成功偵測的比例，遠低於市售商業防毒防駭軟體的一般表現。

Atlas VPN 的資安專家說，該單位會同獨立研究機構 AV-Test，以常見的 29 種 Stalkerware 來測試市售常見的 18 種 Android 專用防毒防駭軟體，結果 Google Play Protect 的表現敬陪末座，29 種追蹤監控惡意軟體，只能成功偵測出 9 種，比例為 31%。

同樣表現不佳的 Android 防毒防駭軟體，還包括由 Norton 推出的 NortonLifeLock Norton 360；29 種惡意軟體中僅偵測出 17 種，成功偵側比例僅為 58.6%。

表現最佳的 Android 防毒防駭軟體有三款，分別是 Antiy AVL、Bitdefender Mobile Security、Trend Micro Mobile Security；這三種軟體都 100% 偵測出全部 29 種追蹤監控惡意軟體。

兩種來自知名資安廠商 ESET 與 Kaspersky 的產品 SET Mobile Security 與 Kaspersky Internet Security for Android，表現也相當優秀，僅有 1 支惡意軟體沒有偵測到，成功率達 96.6%。

有鑑於 Android 平台上的惡意軟體為數眾多，建議 Android 手機用戶務必安裝實際有效的防毒防駭軟體，以降低各種遭到駭侵攻擊的風險。

- 資料來源：
  1. Google Play Protect on Android Failed Against Malware-Detecting Apps From Avast, McAfee, More: AV-Te
  2. Google Play Protect detects only 31% of Android stalkerware
  3. (Atlas VPN) Google Play Protect detects only 31% of Android stalkerware

2.5.2、Google 自 Play Store 中下架多個假冒雲端挖礦 app

Google 自 Googe Play Store 中下架 8 個蓄意假冒為雲端挖礦服務，實際上會進行各種詐騙的惡意 app。

Google 近期自其 Googe Play Store 中下架 8 個蓄意假冒為雲端挖礦服務，實際上會進行各種詐騙的惡意 Android app；然而資安廠商趨勢科技旗下的資安專家指出，在 Google Play Store 上，仍有多個同類惡意 app 並未遭到下架。

這些被 Google 下架的惡意雲端挖礦 app，假借幫用戶在雲端挖掘比特幣等加密貨幣為理由，下載安裝這些 app；這些 app 甚至還會鼓勵用戶付費取得更多挖礦算力，分得更多加密貨幣。實際上用戶不但得不到任何加密貨幣分潤，甚至還會被植入大量廣告，或是在不知情的情況下，訂閱昂貴的數位服務。

資安專家指出，在這 8 個遭下架的 app 中，都內建了 1 到 2 個如 FakeMinerPay 或 FakeMinerAd 之類的惡意軟體；其中一個名為 BitFunds 的惡意 app，下載安裝次數突破 100,000 次以上，有兩支 app 甚至還需要付費安裝。

資安專家也說，這些 app 實際上沒有任何挖礦功能，卻會顯示計數器之類的畫面，以愚弄用戶，以為真的正在進行挖礦賺錢的過程；有些 app 還會慫恿用戶付費取得更強大的挖礦能力，賺取更多加密貨幣，「服務費用」從 14.99 美元到高達 189.99 美元不等。

趨勢科技也說有兩支假冒挖礦 app，會對用戶顯示大量廣告；這些 app 會要求用戶觀看廣告，廣告結束後才能繼續挖礦，或是加快挖礦速度；有些 app 甚至還會在背景進行假冒廣告點擊的詐騙活動。

趨勢科技說，雖然 Google 此次移除了 8 個假冒挖礦 app，但在 Google Play Store 中以「cloud mining」（雲端挖礦）來搜尋，仍有非常多可疑的 app 存在，用戶必須提高警覺，避免因一時貪念，下載安裝這類詐騙挖礦 app。

- 資料來源：
  1. Fake Cryptocurrency Mining Apps Trick Victims Into Watching Ads, Paying for Subscription Service
  2. Bogus Cryptomining Apps Infest Google Play

2.5.3、數千 Facebook 帳號資訊遭全新 Android FlyTrap 惡意軟體竊取

資安廠商發現全新的 Android 惡意軟體 FlyTrap，會藉由提供折價券或有獎徵答遊戲，吸引用戶下載安裝並注入惡意木馬軟體。

資安廠商 Zimperium 旗下的研究團隊，日前發現一個全新的 Android 惡意軟體 FlyTrap，會藉由提供折價券或有獎徵答遊戲，吸引用戶下載安裝並注入惡意木馬軟體 FlyTrap，以竊取用戶的 Facebook 帳號相關資訊。

根據 Zimperium 的研究報告指出，FlyTrap 會以簡單的社交工程手法，騙取用戶信任以下載其惡意軟體，並且在該 App 中登入 Facebook 帳號以參加抽獎或其他活動，例如 Netflix 專用折價券或 Google AdWords 的折價券等；受害者依其 App 指示登入其 Facebook 帳號後，該惡意軟體中的木馬程式即可透過內建的 JavaScript 注入以竊取用戶的 Facebook cookie、用戶帳號詳細資訊、所在地、IP 位址等。

FlyTrap 收集到這些資訊後，即會上傳到駭侵者設立的控制伺服器；Zimperium 的資安專家發現該控制伺服器的漏洞並入侵後，取得了該批駭侵者竊得的資料。分析該批資料後，發現感染 FlyTrap 惡意軟體的 Android 手機超過 10,000 台以上，分布遍及全球 144 國，受害的 Facebook 用戶有數千名之多。

值得注意的是，包含 FlyTrap 惡意軟體的 Android App，其用戶介面設計十分精良，且在 Google Play Store 與多個第三方 Android 行動應用程式商店均有上架；雖然在 Zimperium 通報 Google 後，這些惡意軟體已自 Google Play

Store 下架，但仍在其他第三方 Android 行動應用程式商店中保持上架狀態。

- 資料來源：
  1. FlyTrap Android Malware Compromises Thousands of Facebook Accounts
  2. FlyTrap malware hijacks thousands of Facebook accounts

2.5.4、美國行動通訊服務商 T-Mobile 發生大規模客戶資料外洩事件

美國行動通訊服務商 T-Mobile 有近億顧客資料，日前被放上網路待價而沽；T-Mobile 也證實這批資料被竊，目前正在進行調查作業。

美國大型行動通訊服務商 T-Mobile，日前發生嚴重資安事件；有近億顧客資料日前被放上網路待價而沽；T-Mobile 也證實這批資料被竊，目前正在進行調查作業。

據資安專業媒體 BleepingComputer 報導指出，有駭侵者成功入侵 T-Mobile 的多台資料庫主機，竊得近 1 億名 T-Mobile 用戶的多種個資，並放上駭侵相關網站求售。

BleepingComputer 取得駭侵者的說法，指出該批資料包括用戶使用行動裝置的 IMEI 與 IMSI 編號、電話號碼、顧客姓名、裝置安全密碼（PIN）、社會安全碼、駕照號碼與出生年月日等。

駭侵者也說，這批資料中的 IMEI 號碼，最遠可溯及 2004 年。

該批資料是在約兩星期前的一波駭侵攻擊中取得。據 BleepingComputer 報導，駭侵者係透過 ssh 連線到 T-Mobile 所屬內部資料中心的 Oracle Database Server，進而取得這批資料。

而當 BleepingComputer 向 T-Mobile 針對此事進行採訪時，T-Mobile 證實該公司發生了駭侵攻擊事件，也證實該公司所屬的伺服器，確實發生過外界不當存取事件，且有部分資料外洩；但該公司說「目前尚未確認是否有顧客

個資遭到竊取」。

T-Mobile 在聲明中說，該公司已經會同專家與司法單位，針對此次資料外洩事件積極展開調查；目前也已經關閉駭侵者攻擊使用的進入點；但該公司也說，在調查行動告一段落之前，無法確認外界宣稱的受影響者人數。

- 資料來源：
  1. 100m T-Mobile Customer Records Purportedly Up for Sale
  2. T-Mobile confirms servers were hacked, investigates data breach

2.6、軟體系統資安議題

2.6.1、避免 Synology NAS 產品遭駭客攻擊，建議用戶強化帳密安全設定

群暉科技 Synology 近日接獲數起使用者詢問，觀察到有異常數量 IP 企圖嘗試登入 NAS 產品，經產品安全團隊調查，確認為駭客使用暴力密碼破解手法，而非利用特定系統安全性弱點。Synology 也呼籲使用者毋須恐慌，同時建議使用者持續加強帳號權限與密碼設定，以阻斷駭客入侵的可能。

經 Synology 產品安全團隊分析攻擊樣本，這次事件為知名惡意程式 StealthWorker 的攻擊，該駭客組織利用暴力密碼破解手法登入受害裝置，植入惡意程式後進行資料加密勒索，再利用受害裝置進一步探索並攻擊更多弱密碼裝置，可能被攻擊的對象包括一般 Linux 主機及市面上各廠牌 NAS。

目前 Synology 已與國內外相關資安 CERT 單位展開協作，透過 TWCERT/CC 對國外通報惡意程式的 C&C Server(Command and Control Server)的 IP，並請相關單位將其關機，以儘快結束此次攻擊事件。

「Synology 將確保您的系統與資料安全視為首要之務，我們不僅成立專責產品安全團隊(PSIRT)，也透過與相關資安單位協作，確實管理並快速回應資安事件。」Synology 安全事件應變組經理林涵恩表示，「資安攻擊手法日新月異，我們也呼籲所有 Synology 使用者透過 DiskStationManager(DSM)內建的各項帳號與密碼管理設定，持續加強 NAS 的安全性，以防範惡意攻擊。」

Synology 建議使用者採取以下行動來加強 NAS 系統安全性：

- 於控制台>使用者帳號新增一組具管理員權限的帳號，並停用系統預設的「admin」帳號
- 加強所有帳號密碼的複雜性，並啟用多步驟驗證(如 OTP 一次性密碼)或是 SecureSignIn 為帳號提供多一道安全防護

此外，若您擔心設備因使用弱密碼而已遭到攻擊，可以透過下列方式進行檢查：

1. 登入 DSM，至控制台>任務排程表檢查是否被建立異常的程式碼。您也可以透過日誌中心搜尋「ScheduledTask」。
2. 檢查 FileStation 是否有檔案被加密(副檔名可能已被修改)。
3. 如有上述提及的任何狀況，請備份您的資料並重新安裝最新正式版本 DSM 來確保系統完全乾淨。

若有其他不確定性的異狀，建議直接聯絡 Synology 原廠獲取技術支援：

4. 請至 DSM 中的技術與支援中心>支援服務>勾選啟用遠端存取，並提供技術支援識別碼與暫時的 DSM 帳號密碼。

關於 Synology 對安全性的努力，歡迎您透過產品安全性總覽瞭解更多。

- 資料來源：
  1. 群暉科技 Synology®關心您的資料安全，建議所有使用者強化帳號與密碼安全設定
  2. 防範勒索病毒的方法
  3. 如何提升 SynologyNAS 安全性？

4. 如何透過 HyperBackup 將資料備份至遠端 SynologyNAS 或檔案伺服器？

5. 如何使用 HyperBackup 將資料備份至雲端服務？

2.6.2、資安專家再次發現 Windows Print Server 嚴重漏洞

雖然微軟針對 PrintNightmare 0-day 嚴重漏洞進行修復，但資安專家再度發現嚴重漏洞，可透過特製的印表機驅動程式，取得 Windows 系統權限。

雖然日前微軟針對 PrintNightmare 0-day 嚴重漏洞進行修復，但資安專家日前再度發現與 Windows 列印子系統相關的嚴重資安漏洞；駭侵者可透過一個特製的印表機驅動程式，讓任何人輕易取得 Windows 系統權限。

資安專家 Benjamin Delpy 最近針對 Windows 列印子系統中的多項資安漏洞，陸續發表研究報告；最新的一份報告是可以藉由一個特製的印表機驅動程式，進而提升受限 Windows 用戶的權限至系統權限。

Delpy 展示了一種概念證實攻擊方式。他設置了一個放在網路上的列印服務，任何人都可以點擊該連結，然後在其 Windows 系統上安裝一個特製的印表機驅動程式；該驅動程式執行後，會觸發一個漏洞，自動以系統權限執行一個 DLL 檔；該 DLL 即可用系統權限於 C:\Windows\System32 寫入一個必須擁有系統權限才能寫入的 log 檔。

之後 Delpy 稍稍修改該 DLL，只要安裝他提供的特製印表機驅動程式，即可執行該 DLL，並且以系統權限叫出命令列輸入行；因此任何人都可以透過這個漏洞，直接取得系統權限並執行任意程式碼。

資安媒體 BleepingComputer 測試該特製的印表機驅動程式時，發現該 DLL 可以關閉 Windows 內建資安防護軟體 Windows Defender，因此能順利提升執行權限。

資安專家建議 Windows 用戶，在微軟針對此問題推出資安修補程式前，可暫時停止 Windows Print Spooler 的運作，或是在防火牆上設定，阻擋來自外部的 SMB 與 RPC 連線要求；也可以在 Windows Server 上設定 PackagePointAndPrintServerList 的群組原則，只允許擁有 admin 權限的用戶安裝印表機驅動程式。

- 資料來源：
  1. Benjamin Delpy @gentilkiwi
  2. Remote print server gives anyone Windows admin privileges on a PC

2.6.3、Exchange Server ProxyShell 漏洞報告發表後，有駭客進行惡意掃瞄

台灣資安廠商研究員在一場學術會議上發表關於 Microsoft Exchange 的資安漏洞相關報告後，即有駭侵者開始利用這些漏洞進行掃瞄。

台灣資安廠商 DEVCORE 研究員蔡政達（Orange Tsai），在近期的一場學術會議 Black Hat talk 上發表關於 Microsoft Exchange 的資安漏洞相關報告後，即有駭侵者開始利用這些漏洞，針對網路上的 Microsoft Exchange Server 進行掃瞄，意圖利用這些漏洞發動攻擊。

駭侵者掃瞄並欲加以利用的一組三個 MS Exchange Server 漏洞，被合稱為 ProxyShell 漏洞，分別是 CVE-2021-34474、CVE-2021-34523 與 CVE-2021-31207，這三個漏洞的組合，可讓駭侵者不需要經過登入驗證，即可在 Microsoft Exchange Server 上遠端執行任意程式碼。

台灣資安廠商 DEVCORE 的首席研究員蔡政達，因為發現這三個漏洞而獲得今年四月 Pwn2Own 2021 駭侵測試的大獎，而這些漏洞也在今年四月到五月之間，由 Microsoft 官方發布的資安修補程式予以修復。

在蔡政達於在 Black Hat talk 上發表研究成果，並解釋 ProxyShell 漏洞可以如何運作後，另有兩位資安研究專家發表了相關技術研究報告，指出如何實作該漏洞的攻擊後，就有另一位資安專家 Kevin Beaumont 發現有駭侵者試圖偵測他設立的 Microsoft Exchange Server 是否有該漏洞可入侵，在進一步追查後，發現有駭侵者開始大規模掃瞄網路上的 Microsoft Exchange Server，以利用 ProxyShell 漏洞發動攻擊。

Kevin Beaumount 指出，雖然微軟早在四月就針對 ProxyShell 相關漏洞發表更新，但據信整個 Internet 上還有 50% 的 Microsoft Exchange Server 尚未套用這些更新。

- 資料來源：
  1. ProxyLogon is Just the Tip of the Iceberg: A New Attack Surface on Microsoft Exchange Server!
  2. Kevin Beaumont @GossiTheDog
  3. Kevin Beaumont @GossiTheDog CVE-2021-34473

2.6.4、駭客詐騙網站管理員，以含惡意 BazaLoader DDoS 軟體的工具清理網站

有駭侵者對網站管理員寄發詐騙訊息，假稱其網站內含有惡意 DDoS 程式碼，需用其特製工具清除，實則利用此假工具植入 BazaLoader DDoS 惡意軟體。

近來有駭侵者對多個網站管理員寄發詐騙訊息，假稱其網站程式碼內含有惡意 DDoS（分散式服務阻斷攻擊，Distributed Denial of Service）程式碼，需用其特製工具清除，否則將對其提告；網站管理員如果不疑有他，利用此假工具清理其網站，就會被植入 BazaLoader DDoS 惡意軟體。

網站開發者 Brian Johnson 指出，他有兩名客戶在最近收到可疑的法律通知信，指稱其所營運的網站遭到駭侵者植入 DDoS 惡意軟體，並對 Intuit、Hubspot 等大型網路服務業者發動 DDoS 攻擊。該信件威脅網站營運者，若不在時限之內，利用信中隨附連結的清理工具，清除其網站內的惡意程式碼，就將面臨後續的司法控告。

該威脅信件中，還附有一個 Google 文件的連結；詐騙者指稱該連結內有目標網站發動 DDoS 攻擊的「證明」，以及指定採用的「清理程式」。

資安專家分析該「清理程式」，發現該清理程式內含一個名為 Bazaloader 的 DDoS 惡意軟體；收到威脅信件的網站管理者，如果真的安裝使用該程式，其網站伺服器反而會被植入 BazaLoader DDoS 惡意軟體，並且從駭侵者設立的控制伺服器中下載如 Cobalt Strike 之類的惡意軟體模組，成為其僵屍網路的一部分。

資安專家也說，除了以網站遭 DDoS 程式感染之外，這類駭侵者也會以其他的理由來詐騙網站管理者，例如假稱該網站內含有侵害著作權的影音或圖片等等，要求網站管理員以其工具進行侵權檔案掃瞄與移除，進而詐騙網站管理員下載安裝同樣的 BazaLoader DDoS 惡意軟體。

- 資料來源：
  1. Fake DDoS Attack Email
  2. Matthew Mesa @mesa_matt
  3. Fake DMCA and DDoS complaints lead to BazaLoader malware

2.6.5、微軟示警數千 Azure 用戶可能曝險於 Cosmos DB 嚴重資安漏洞

微軟向數千名 Azure 雲端服務用戶示警，指出一個存於 Cosmos DB 的嚴重資安漏洞，可能導致用戶的資料庫遭駭侵者不當存取。

微軟日前向數千名 Microsoft Azure 雲端服務的用戶發出資安警訊，指出一個存於 Cosmos DB 的嚴重資安漏洞，可能導致用戶的資料庫遭駭侵者遠端不當存取。

Azure Cosmos DB 是一個全球使用率相當普及的 NoSQL 資料庫服務，大品牌用戶包括 Mercedes-Benz、Symantec、Coca-cola、Exxon-Mobil、Citrix 等。

該漏洞是於 2021 年 8 月初由資安廠商 Wiz 旗下的研究人員發現，並將此漏洞命名為「ChaosDB」；駭侵者可以用 Cosmos DB 內一個用來幫助用戶進行資料可視化的工具 Jupyter Notebook 功能內的一系列錯誤，來誘發此漏洞，即可取得 Cosmos DB 的用戶登入資訊，包括主要讀寫金鑰；駭侵者這樣可以在無需任何前置作業的情形下，利用此漏洞完全掌控 Azure 用戶的帳號與資料庫內容。

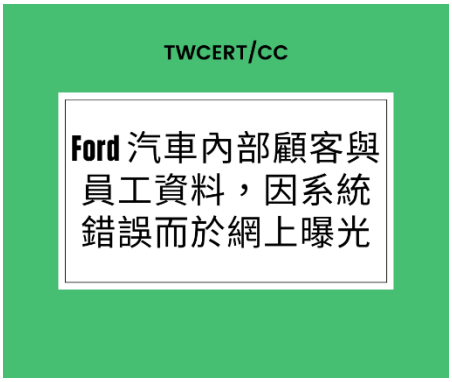
微軟表示，在接獲來自資安廠商的漏洞提報資訊後，該公司已於 48 小時內關閉該漏洞的進入點，藉以封鎖駭侵者使用此漏洞的路徑；雖然該漏洞已於近日得到修復，但微軟在近期又針對 30% 的 Cosmos DB 用戶發出資安警訊，表示這些用戶可能於 8 月 26 日遭到大規模針對此漏洞發動的駭侵攻擊行動。

Wiz 也指出，駭侵者很可能在該公司發現此漏洞並提報給微軟的數個月之前，就積極利用此一漏洞發動攻擊活動。

微軟也針對其 Azure 用戶提供此漏洞的暫時解決方案，用戶可以依其指南，重新製作不同的資料庫讀寫主要金鑰，並定期更換金鑰；微軟也建議 Azure 用戶考慮使用 Azure Cosmos DB 防火牆服務，並且整合其他虛擬系統，以提高安全性。

- 資料來源：
  1. CHAOSDB
  2. Secure access to data in Azure Cosmos DB
  3. Microsoft warns Azure customers of critical Cosmos DB vulnerability

2.6.6、Ford 汽車內部顧客與員工資料，因系統錯誤而於網上曝光



美國 Ford 汽車公司，由於內部客服管理系統的設定錯誤，造成部分員工與顧客的相關資料在網路上曝光可供存取。

美國 Ford （福特）汽車公司日前發生資料安全控管事件，由於內部客服管理系統的設定錯誤，造成部分員工與顧客的相關資料在網路上曝光，可供有心人士直接存取，甚至取得帳號權限。

資安研究人員在美國 Ford 汽車官方網站中發現一個漏洞，可以經由此漏洞進入 Ford 內部伺服器上執行的 Pega Infinity 顧客互動管理系統內，取得諸如用戶資料庫、員工各項記錄與內部派工單等機敏資訊。

研究人員利用 Pega Infinity 一個錯誤設定的漏洞（CVE-2021-27653），透過 Pega Infinity 的客服人員線上對談控制台，即可利用此漏洞存取 Ford 內部的各種系統與資料庫。

研究人員指出，透過這種方法可以取得相當多個人可識別（Personally Identifiable Information, PII），包括以下項目：

- 顧客與員工記錄
- 金融服務帳號
- 資料庫名稱與表格
- OAuth 存取 token
- 內部支援工單

- 附有組織名稱的用戶檔案
- 內部操作介面
- 搜尋列的搜尋記錄

研究人員指出，這些資料外洩可能會對該公司帶來極大衝擊；有心人士可以利用此漏洞，發動進一步的資安攻擊，例如植入更多惡意軟體，以及取得系統控制權之外，外洩的個人可辨識資料，也可用於進一步的釣魚攻擊。

研究人員說，他們在 2021 年 2 月時就向 Pega 提報該漏洞的存在，也透過 HackerOne 漏洞公開計畫提報給 Ford。

- 資料來源：
  1. Ford Breach, August 2021 Disclosure
  2. Pega CVE-2021-27653, March 2021
  3. Ford bug exposed customer and employee records from internal systems

2.7、軟硬體漏洞資訊

2.7.1、Razer 電競產品驅動程式 0-day 漏洞，插入裝置即可取得系統管理權限

資安專家發現電競品牌 Razer 的驅動程式內含嚴重 0-day 資安漏洞，插入 Razer 品牌的鍵盤或滑鼠，即可取得系統管理權限。

資安專家發現電競遊戲控制周邊裝置品牌 Razer 的 Windows 驅動程式，內含嚴重 0-day 資安漏洞；駭侵者只需插入 Razer 品牌的鍵盤或滑鼠，即可輕鬆取得 Windows 10 的系統管理權限。

發現這個漏洞的資安專家是 johhat，他在 Twitter 上公布這個發生於 Razer Windows 驅動程式的 0-day 漏洞；當用戶在 Windows 10 或 Windows 11 電腦上插入任何 Razer 品牌的鍵盤或滑鼠裝置，Windows 會自動從 Razer 的伺服器下載這些裝置的驅動程式 Razer Synapse Software；此時 Razer Synapse Software 會自 Windows 系統取得管理者權限來進行驅動程式的安裝，並且詢問用戶要把驅動程式安裝在哪個資料夾。

這時用戶只需在對話盒內按下鍵盤上的 SHIFT+滑鼠右鍵，出現的快速選單中，會有一個「Open PowerShell window here」的選項；由於這個 PowerShell 視窗是由具有系統管理員權限的 Razer Synapse Software 所啟動，因此 PowerShell 視窗也具有系統管理員的執行權限。

利用這個方法取得系統管理員執行權限後，有心人士即可在近端系統上為所欲為，包括存取 Windows 系統中的所有檔案，或是安裝任何應用程式，

甚至惡意軟體。不過要誘發這個漏洞，駭侵者必須能夠實體存取目標的 Windows 電腦裝置，實體插入 Razer 設備才行。

資安專家 jonhat 在發現這個漏洞後，隨即提報給 Razer 原廠。之後 Razer 表示將儘快推出更新版本，修復此漏洞。

- 資料來源：
  1. jonhat @j0nh4t
  2. Razer bug lets you become a Windows 10 admin by plugging in a mouse

2.7.2、微軟推出 8 月 Patch Tuesday 資安修補包，修復 44 個資安漏洞

微軟推出例行性的 2021 年 8 月份 Patch Tuesday 資安修補包，一共修復 44 個資安漏洞，包括 3 個 0-day 漏洞在內；微軟各種產品用戶，應立即更新此修補包。

微軟近日推出例行性的 2021 年 8 月份 Patch Tuesday 每月資安修補包，一共修復微軟多種軟體系統共 44 個資安漏洞，其中更包括 3 個 0-day 漏洞在內；微軟各種產品的用戶，應立即透過系統更新功能，更新此修補包，以降低遭到駭侵攻擊的風險。

在這次推出的資安修補包中，除了 3 個 0-day 資安漏洞外，以資安漏洞的危險程度評及來看，共有 7 個列為「嚴重」（Critical）等級，37 個列為「重要」等級（Important）；若以漏洞性質與錯誤類型來看，共有 13 個屬於可讓駭侵者遠端執行任意程式碼的 RCE 漏洞，8 個屬於資料外洩漏洞，2 個屬於服務阻斷（DoS）漏洞，4 個屬於詐騙（Spoofing）漏洞。

值得一提的是，3 個 0-day 漏洞中，已經有一個遭到駭侵者大規模濫用；這個漏洞是 CVE-2021-36948，是發生在 Windows 10 與 Windows Server 系統中的 Windows Update Medic Service 中的執行權限提升漏洞；駭侵者可以先以較低權限入侵系統，然後利用這個漏洞提升自身的執行權限，在未經授權的情形下執行任意程式碼，發動進一步的攻擊。

另兩個得到修復的 0-day 漏洞是 CVE-2021-36939 與 CVE-2021-36942；前者是發生在 Windows Print Spooler 的遠端執行任意程式碼漏洞，後者是 Windows LSA Spoofing 漏洞。目前這兩個漏洞都還沒有遭到駭侵者大規模濫

用。

- CVE 編號：CVE-2021-36948、CVE-2021-36939、CVE-2021-36942
- 解決方案：立即透過系統更新功能進行更新修補。

- 資料來源：
  1. Windows Update Medic Service Elevation of Privilege Vulnerability
  2. Microsoft Patch Tuesday: Windows Flaw Under Active Attack
  3. Microsoft August 2021 Patch Tuesday fixes 3 zero-days, 44 flaws

2.7.3、國內網通設備大廠修補無線路由器產品的 RCE 漏洞

國內網通設備大廠於 2021 年 7 月 13 日接獲 HITCON ZeroDay 漏洞通報平台之資安漏洞通報，修復其無線路由器 DIR-819 之遠端程式碼執行(Remote Code Execution, RCE)漏洞。

廠商已於 2021 年 8 月 5 日釋出 beta 版韌體來修正此資安漏洞；擁有這類裝置的用戶，應立即進行更新，以免遭有心人士利用已知的漏洞發動攻擊而造成損失。

相關訊息請點此參考廠商發布之韌體修補更新公告。

- 影響產品/版本：無線路由器 DIR-819 型號，韌體版本 v1.06 及先前之版本。
- 解決方案：根據廠商釋出之 beta 版韌體進行更新；待正式版發布後，請依照官方提供之更新公告，將產品更新至已修復版本。

- 資料來源：
  1. (non-US) DIR-819 :: HW:A1 :: FW v1.06 :: Remote Code Execution (RCE)

2.7.4、Mirai 僵屍網路利用晶片 SDK 漏洞，多廠牌無線裝置可能遭植入

資安專家發現採用台灣網通大廠之硬體與其 SDK 的無線連網裝置，含有一系列嚴重資安漏洞，且該漏洞已遭 Mirai 僵屍網路鎖定，發動大規模感染。

資安廠商 IoTInspector 旗下的資安專家，發現採用台灣網通大廠無線網路硬體晶片 RTL819xD 與其 SDK 解決方案的眾多無線連網裝置，含有一系列嚴重資安漏洞，且該漏洞已遭 Mirai 僵屍網路鎖定，發動大規模感染；造成數千萬台各廠牌連網裝置曝露於遭植入僵屍惡意軟體的資安風險。

被發現的漏洞共有 4 個，其 CVE 編號為 CVE-2021-35392 到 CVE-2021-35395，存於 SDK 開發組件中的多個元件；其中最嚴重的漏洞為 CVE-2021-35395，CVSS 危險程度評分高達 9.8 分（滿分為 10 分）；該漏洞存於裝置的 Web 管理界面，可讓駭侵者遠端執行任意程式碼，並且取得裝置控制權。

由於該公司的無線網路晶片受到業界廣泛採用，因此這一系列漏洞的影響範圍甚廣；估計有 65 個品牌、200 以上不同款式無線路由器、IP 攝影機、智慧家電等 IoT 裝置含有此漏洞，裝置台數可能超過數千萬台。

雖然該公司在接獲通報後，很快就在 8 月 13 日發布資安更新，但資安廠商 SAM Seamless Network 觀察到惡名昭彰的 Mirai 僵屍網路，很快就針對這個新發現的漏洞進行版本更新。根據 SAM 的觀察報告，Mirai 自 8 月 18 日起開始在網路上掃瞄尚未修補此漏洞的受影響裝置；SAM 也指出被掃瞄次數最多的裝置，包括 Netis E1+ 無線網路延伸器、Edimax N150、N300 無線路由器、Repotec RP-WR5444 無線路由器等。

- 解決方案：

  1. 建議 IoT 裝置用戶檢視產品供應商是否已進行漏洞修補並推出更新檔。
  2. 若產品供應商已推出更新檔，建議用戶應立即進行更新，以免 IoT 裝置遭植入惡意軟體。

- 資料來源：

  1. Realtek AP-Router SDK Advisory
  2. Multiple attempts to exploit Realtek vulnerabilities discovered by our researchers
  3. Advisory: Multiple Issues in Realtek SDK Affects Hundreds of Thousands of Devices Down the Supply Ch
  4. Botnet targets hundreds of thousands of devices using Realtek SDK

第 3 章、 資安研討會及活動

金融資安論壇	
活動時間	**2021 年 9 月 17 日（ 五 ）13:25 PM ~ 17:10 PM**
活動地點	**財團法人張榮發基金會 國際會議中心 8 樓 801 會議廳**
活動網站	**https://docs.google.com/forms/d/e/1FAIpQLSeI88ffRxt-Z7yiGWHH5hqkwomBhLwREH5zx6PZOm4hPlRDnQ/viewform**
活動概要	 **主辦單位：ZUSO Generation** 協辦單位：中華民國電腦稽核協會 決策者與執行者提升資安治理與雙向防禦 為強化金融業資安防護能力，金管會自 2020 年起開始推動「金融資安行動方案」，包含監理、治理、作業韌性與聯防功能之四大面向。ZUSO Generation 與中華民國電腦稽核協會共同攜手於 9 月 17 日，邀請國內重磅貴賓講師群齊聚一堂，分享從國家政策、案件剖析、高層決策、防禦手法、國際標準、風險控管與稽核等各個面向的資安治理議題。內容精彩可期，歡迎您前來與我們互動交流。誠摯歡迎您報名參加！ 活動日期：2021 年 9 月 17 日（ 五 ） 報到時間：13:00 PM ~ 13:25 PM 活動時間：13:25 PM ~ 17:10 PM

2021 TWNIC IPv6 暨資安推廣講座活動 2	
活動時間	**110 年 9 月 17 日(週五)13:30-17:00**
活動地點	**Google Meet 線上視訊會議**
活動網站	**https://docs.google.com/forms/d/e/1FAIpQLSdtxecPujfgQUn5CyvBXgNM1ZiBFM6byHDiyNrr-1jo_3GuvQ/viewform**
活動概要	**主辦單位：TWNIC、TWCERT/CC** 活動聯絡人: 洪子淩小姐，07-6011000 ext 34102，email: jscheng@nkust.edu.tw 活動議程: PM 1:30~1:45 報到 PM 1:45~2:10 來賓致詞 台灣網路資訊中心 董事暨執行長 黃勝雄 博士 台南市電腦公會 吳進雄 理事長 國立成功大學電機系 李忠憲 教授 (ISC)2 台北分會 黃建笙 理事長 PM 2:10~2:40 主題演講 講題:國內外 IPv6 發展現況及應用服務介紹 講者:高雄科技大學資管系 鄭進興 老師 PM 2:40~3:20 主題演講 講題:資安威脅情資分享與防護 講者:台灣網路資訊中心網安資訊組組長林志鴻博士 PM 3:20~3:30 中場休息 PM 3:30~4:30 主題演講 講題: IPv6 網路安全探討 講者: 安華聯網科技股份有限公司協理 林敬皇 博士 PM4:30~5:00 座談會交流 主題: 建置支援 IPv6 網路服務經驗分享 主持人: 鄭進興 老師 林敬皇 博士 林志鴻 博士 課程免費(for ICP 業者、受邀請公司、人員)，名額有限，請於 9/14 前報名，謝謝。

資訊軟體稽核	
活動時間	**9/29 09:30-16:30（共計 6 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0OA==**
活動概要	CISA 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** ● 課程大綱： 1、SSDLC 程式開發安全 2、資訊系統委外開發 RFP 資安需求 3、網站攻防實務 ● 課程對象： -參與系統或軟體開發之相關人員 -軟體專案經理、系統架構師、系統分析師 -程式設計師、軟體測試人員 -以上人員需具備 1 年以上系統軟體開發經驗 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 -每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 -以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

第 36 屆 TWNIC IP 政策資源管理會議	
活動時間	**2021/10/6(三) 9:00 ~ 17:00**
活動地點	**線上研討會**
活動網站	**https://opm.twnic.tw/36th/index.html**
活動概要	 **主辦單位：TWNIC** 第 36 屆 TWNIC IP 政策資源管理會議以創造及促進 IP 相關產業發展為目標之會議，提供各界有關網路技術研究、產業發展之溝通交流平台。本次會議議題將針對台灣及全球的新興網路服務的重要關鍵技術及應用服務的發展趨勢進行研討交流。 會議議程： 09:00 - 09:15 開幕致詞 09:15-09:45 專題演講 Keynote Speech 1 BGP Security Threats and Challenges 09:45-10:20 專題演講 Keynote Speech 2 10:40-12:00 網際安全特別興趣小組 Cyber Security SIG 13:30-14:50 國際合作特別興趣小組 Cooperation SIG 15:10-15:50 政策與法規特別興趣小組 Policy SIG 15:50-16:50 IPv6 佈建發展特別興趣小組 IPv6 Deployment SIG

【資安學院】政府受駭案例與反思	
活動時間	**10/21 18:30-21:30（共計 3 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NQ==**
活動概要	CISA 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** ● 課程大綱： -政府企業資安威脅種類 -資安攻擊入侵思維 -實際案例 1：我國重要油品事業近期遭勒索病毒案 -實際案例 2：其它政府機關遭駭客入侵案 -個人資安防護議題 ● 課程對象： -企業資訊部門 -提供資訊安全服務之業務、專案、技術與決策等主管及人員 -對本課程有興趣，欲提升資安專業知能者。 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 -每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 -以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

【資安學院】資安事故處理實務	
活動時間	**10/27（三） 09:00-17:00（共計 7 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NA==**
活動概要	CISA 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** ● 課程說明：本課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務。 ● 課程大綱：端點勒索軟體與 APT、網站入侵、雲端線上服務、行動與物聯網裝置、資料庫和資料外洩等事故案件解析、報告撰寫。 本課程需自備筆電、並具備 VMware 環境 ● 課程對象： 資安(訊)主管、資訊安全管理人員、系統管理人員、網路管理人員 具備 1 年以上實務操作經驗與資安事件調查知識尤佳 ● 活動聯絡人：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

台灣駭客年會 HITCON Training 2021	
活動時間	**11/2（二）~ 11/6（六）（報名時間：至 10/18（一）23:59）**
活動地點	**台北市境內，如已達開課人數標準，主辦單位將儘快公布地點。**
活動網站	**https://hitcon.kktix.cc/events/hitcon-training-2021**
活動概要	 **主辦單位：台灣駭客協會** 舊生、已報名 HITCON 2021、HITCON Pacific 2021 享 9 折優惠 ： ➢ 凡是舊生及已報名 HITCON 2021、HITCON Pacific 2021 會眾，持課程邀請碼報名即享有 9 折優惠。 ➢ 請至優惠價資格申請表填寫相關資料，審核通過並使用邀請碼完成購票。 學生 7 折優惠： ➢ 學生票驗證資格說明： ■ 「學生身分」須年齡為 24 歲以下，且必須符合兩點者： ■ 持「學生證」（含研究所），須蓋 110 學年度上學期「註冊章」（包含應屆畢業生）。 ■ 持「身分證、護照」等任一有照證件入場，且須為民國 86 年 9 月後出生，例如國中、準高中職學生、準大學生、準研究生。 ➢ 敬請留意： ■ 學生票現場驗票說明：每位持學生票者雙證件驗證，需提供本人學生證以及上述有照片證件。 ■ 未帶證件或不符資格者，一律以「一般身份」需補票進場。 聯絡信箱：團體報名或對於本活動有任何問題，歡迎寫信至： training@hitcon.org，我們有專人與您聯繫。

第 4 章、 2021 年 8 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。

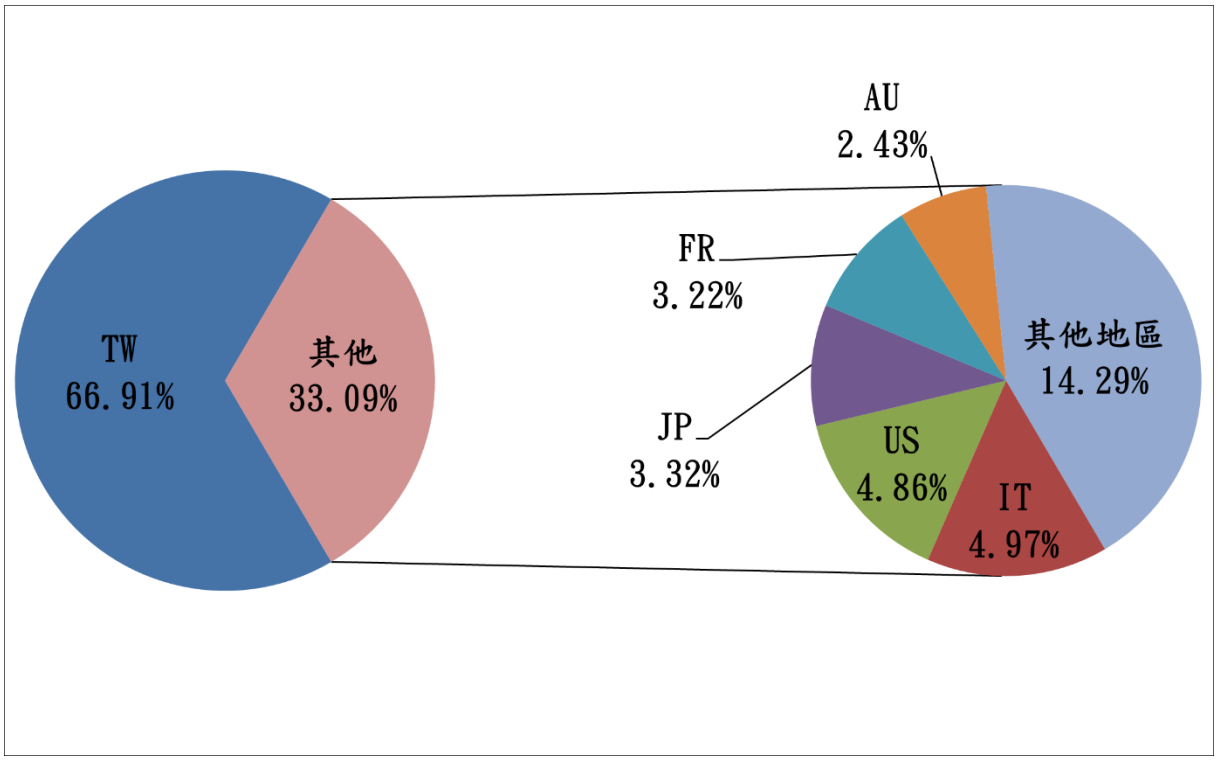


圖 1、分享地區統計圖

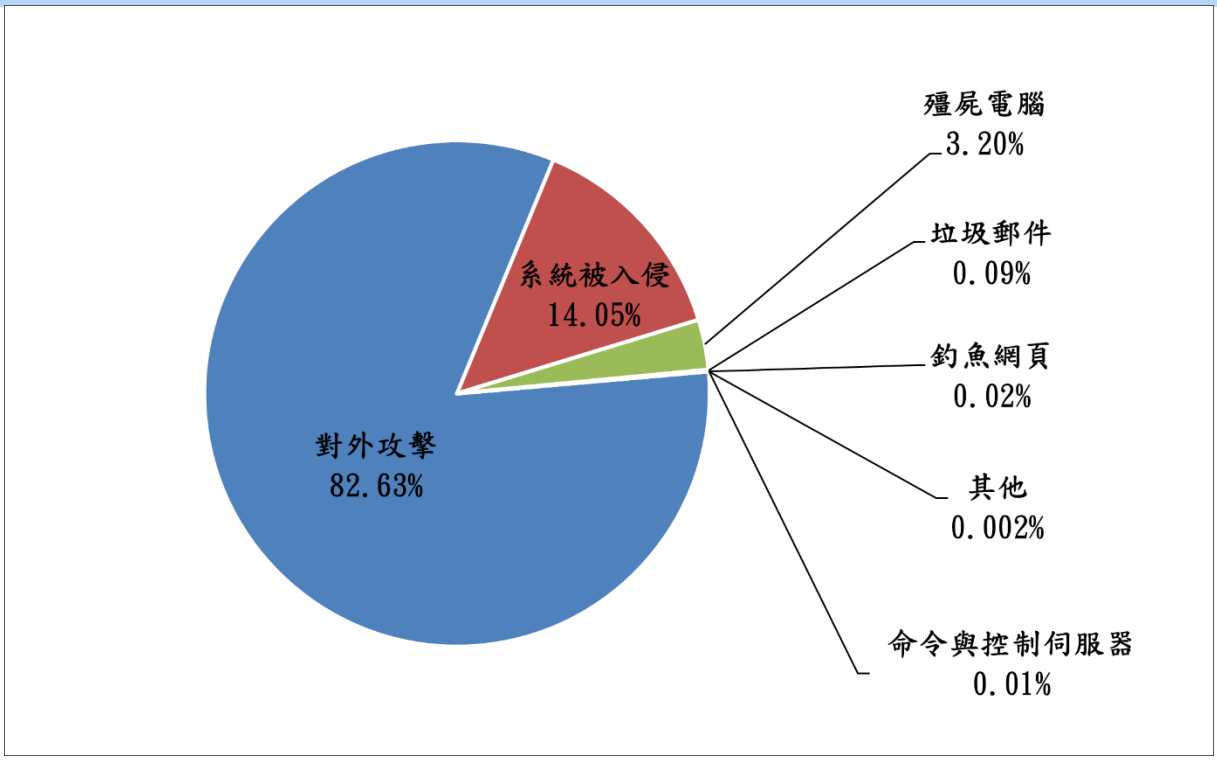

殭屍電腦
3.20%
垃圾郵件
0.09%
釣魚網頁
0.02%
其他
0.002%
命令與控制伺服器
0.01%
系統被入侵
14.05%
對外攻擊
82.63%

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：**2021 年 9 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**