TWCERT/CC 資安情資電子報

2023 年 12 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 7 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、資訊安全宣導：針對近期資安議題、TWCERT/CC 服務或配合政府資安政策等進行資安宣導，以提升大眾資安意識。

第 4 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 5 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 6 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 7 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

Microsoft Exchange 新發現 4 個可導致 RCE 與資料竊取的 0-day 漏洞

資安廠商趨勢科技 (Trend Micro) 日前發表研究表告，指出該公司發現 4 個存於 Microsoft Exchange 的 0-day 漏洞，可能造成駭侵者藉以遠端執行任意程式碼，或竊取設備上的機敏資訊。

該公司在發現這批漏洞的 2023 年 9 月初，就立即向 Microsoft 通報這批 0-day 漏洞，這 4 個 0-day 漏洞目前暫無 CVE 編號，但有 Trend Micro 自有的編號 ZDI，分列如下：

- ZDI-23-1578：該漏洞為存於 ChainedSerializationBinder 類別的 RCE 漏洞；該漏洞原因是未能適當驗證使用者資料，駭侵者可以利用該漏洞來對未受信任的資料進行序列化還原（deserialization），並以 Windows 最高執行權限等級 SYSTEM 來執行任意程式碼；
- ZDI-23-1579：存於 DownloadDataFromUri 方法的漏洞，在資源存取前未能有效驗證 URI，可導致駭侵者竊取 Exchange Server 內的機敏資訊；
- ZDI-23-1580：存於 DownloadDataFromOfficeMarketPlace 方法，同樣屬

於 URI 驗證不足的漏洞，可導致未經授權的資訊洩露；

- ZDI-23-1581：存於 CreateAttachmentFromUri 方法中，也屬於 URI 驗證不足漏洞，亦可造成機敏資訊遭竊。

所有漏洞都需要通過使用者身分驗證才能進行，致使其 CVSS 分數較低，約在 7.1 到 7.5 之間（滿分為 10 分）。

為避免駭侵者取得系統存取權並利用此批 0-day 漏洞，建議系統管理者應加強帳密安全性，並使用多重登入驗證機制。

- 資料來源：
  1. (0Day) Microsoft Exchange ChainedSerializationBinder Deserialization of Untrusted Data Remote Code E
  2. (0Day) Microsoft Exchange DownloadDataFromUri Server-Side Request Forgery Information Disclosure Vul
  3. (0Day) Microsoft Exchange DownloadDataFromOfficeMarketPlace Server-Side Request Forgery Information
  4. (0Day) Microsoft Exchange CreateAttachmentFromUri Server-Side Request Forgery Information Disclosure
  5. New Microsoft Exchange zero-days allow RCE, data theft attacks

第 2 章、 資安小知識

10 大常見的資安不安全設定

美國國家安全局（National Security Agency, NSA）與網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）於今年 10 月時，聯名公布該單位旗下紅隊與藍隊共同歸納出的 10 大最常見網路資安設定錯誤，以供各公私單位參考並解決問題。

最常見資安錯誤設定第一名為使用軟體與應用程式的預設組態，包括使用預設登入資訊、使用預設的服務存取權限設定等；駭侵者只要用簡單的搜尋，就能找到各種軟硬體的預設登入帳密，並取得系統的存取權限，甚至進行進一步的駭侵攻擊。

第二名為未適當區隔使用者與管理者權限，這會造成一般低階使用者擁有太多不必要的管理權限，駭侵者只要利用釣魚攻擊等手法取得一般使用者存取權，即可進行各種進階操作，甚至提升己身權限以執行進階駭侵攻擊。

第三名為內部網路監控能力不足，許多單位未對主機和內部網路的流量進行充分的監控，可能導致偵測不到駭侵攻擊活動，或是缺少足夠的資料用以分析或應對資安威脅。

第四名為缺少網路分段作為，這可能導致未經授權的使用者或駭侵者，可以輕易存取關鍵內部網路資源；這種錯誤特別易使勒贖攻擊者輕易取得單

位機敏資訊。

第五名為資安漏洞修補不充分，導致系統存有已知漏洞，容易遭致駭侵者用於攻擊；第六名為可略過的系統存取控制，這將使駭侵者或未經授權者可輕易存取系統，甚至提升執行權限。

第七名為不夠強或錯誤設定的多重登入驗證，包括設定錯誤的智慧卡或代碼產生器，或是缺少能抵抗釣魚攻擊的多重登入驗證程序，都將使取得登入資訊的駭侵者極易入侵系統。第八名是對網路分享資源與服務存取限制不足，駭侵者可輕易使用共享資料夾，或使用未關閉的服務來存取系統。

第九名是密碼管理強度不足，包括易於猜測破解的密碼，甚至是以明文儲存的密碼，都無法有效抵擋駭侵者攻擊；第十名則為未限制的程式碼執行，這使駭侵者只要掌握登入資訊，即可執行各種攻擊用程式碼酬載，嚴重危及系統安全。

建議各單位可以參考此指南，檢視並加強現存的資安防護設定錯誤，以提高資安攻擊的防護能力。

- 資料來源：
  1. NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
  2. NSA and CISA reveal top 10 cybersecurity misconfigurations

第 3 章、 資訊安全宣導

近期偽冒旅遊訂房網站業者發送之詐騙訊息

大型旅遊訂房網站 Booking.com 近日在全球各地都傳出遭駭侵者發動詐騙攻擊的事件，許多客戶在訂房後收到詐騙信件或訊息，然後被導至釣魚網站，導致個人與付款相關資訊遭竊。

據新加坡媒體報導，自今年 1 月起至少已有 30 名受害者，遭詐騙的總額達 41,000 新幣；而在英國、愛爾蘭、紐西蘭、日本、台灣等多國有使用者受害。媒體指出，旅客在 Booking.com 上預訂房間後，會收到由該網站的 App 內聊天室發出的訊息，或以該站網域署名的 email，內容是詐騙者假冒旅館人員，要求消費者在規定時間內「確認」信用卡資訊，否則將取消其訂位。

消費者一旦信以為真，點按了訊息中的釣魚連結，就會被帶到詐騙者設立的假網站，並會被要求輸入個人資訊、銀行帳號或信用卡資訊，以及由金融業者發送的單次有效密碼，隨即其信用卡或帳號就會遭到盜刷或盜領。

資安廠商 Perception Point 指出，駭侵者先利用假稱訂房或社交工程等攻擊手法，入侵各飯店的內部系統後加以控制，因此能取得客戶訂房資訊，也能假冒飯店人員進入其在 Booking.com 的後台，利用 App 內的即時通訊和 email 發送機制，來發送釣魚連結給訂房旅客。

由於訊息是來自 Booking.com 的站內即時通訊或該網域的 email，因此旅客很難在第一時間發現異狀；不過資安專家也表示，駭侵者發送的釣魚連結，並非使用 Booking.com 網域，而是其他試圖魚目混珠的網域，用戶如能仔細觀察，依然可發現異狀。

建議用戶在進行各種電子交易時，對於任何發送給消費者的連結，都必須提高警覺，仔細確認連結所屬網域正確無誤，可大幅降低遭釣魚攻擊的成功機率。

- 資料來源：
  1. More travellers using Booking.com conned by scammers posing as hotel representatives
  2. Warnings over 'scam' Booking.com emails asking travellers to provide bank card details or risk havin
  3. Hotel hackers redirect guests to fake Booking.com to steal cards

第 4 章、 國內外重要資安事件

4.1、資安趨勢

半數企業領袖認為生成式 AI 將影響客戶信賴感

資安廠商 Vanta 在一項針對 2,500 位企業領袖的大規模調查中發現，超過一半的企業領袖認為未經規範且不透明的生成式 AI 運用，可能導致客戶信賴感的降低。

這項調查是資安廠商 Vanta 針對澳洲、法國、德國、英國、美國的 2,500 位企業領袖進行的資安議題問卷調查，以了解企業在面對資安與信賴管理方面面臨的困難與挑戰。

報告指出，超過三分之二的受訪企業領袖，認為自己的企業必須強化資安防護能力與合規程度，另外也有四分之一受訪者表示，自己的企業在組織的資安防護與合規策略上過於被動。

報告也發現企業普遍面臨的新時代資安與信任困境，包括生成式 AI 的使用大幅增加、駭侵攻擊的廣度與深度大幅提升，企業必須大大提高資安方面的投入，但實際上可運用的人力與預算卻是減少的。

在 AI 運用方面，54% 企業領袖認為需要建構一套適當的 AI 使用規範體系，讓企業有所遵循，包括規範本身與生成式 AI 使用的透明度揭露等，否則

將影響客戶對企業的信賴感。

此外，高達 72% 的受訪企業領袖，認為有充分的資安與合規策略，能夠提升企業的經營效率，但只有 41% 的企業進行內部資安稽核，僅有 37% 企業採用第三方的資安稽核，36% 企業完成內部資安問卷調查，平均更有 12% 企業當被問及內部資安策略時無法提供資訊或證明。

建議各大公私單位面對日益嚴峻的資安風險與合規要求，都應認真面對，撥列充足資源加以規畫，以強化資安防護能力與合規程度。

- 資料來源：
  1. The State of Trust Report 2023
  2. Generative AI could erode customer trust, half of business leaders say

4.2、新興應用資安

4.2.1、LastPass 遭竊資訊導致 440 萬美元加密貨幣被盜

區塊鏈專家 ZachXBT 與區塊鏈錢包 MetaMask 的開發者 Taylor Monahan，近期發現日前密碼儲存工具服務 LastPass 於 2022 年發生駭侵事件中外洩的資訊，疑已遭駭侵者用以竊取受害者的加密貨幣資產，損失達 440 萬美元。

該起加密貨幣竊案發生於 2023 年 10 月 25 日，共有 25 名受害者，其加密貨幣錢包中合計約 440 萬美元的各種加密貨幣資產，同時遭駭侵者盜領一空。

ZachXBT 指近期頻繁接獲用戶回報，表示自己的加密資產遭到竊取；在深入追蹤多個案例後，發現這些受害者的共同點，就是都使用了 LastPass 服務。

ZachXBT 表示，如果使用者將自己加密貨幣錢包的復原短語或密碼存在 LastPass 中，而又未曾於 LastPass 遭駭後更改復原短語與密碼，錢包內的數位資產就極可能在一瞬間遭到駭侵者盜領一空。

LastPass 是一個使用者眾多的密碼儲存管理服務，在 2022 年曾兩度發生駭侵事件，當時該服務的程式原始碼、顧客資料、經過加密的使用者儲存密碼、正式版網站備份等資訊都遭到駭侵者竊取。

LastPass 當時指出，雖然使用者儲存在該服務的密碼資訊經過加密儲

存，且只有使用者本人擁有可解密的密碼，但如果使用者密碼本身強度不足，或使用與其他服務相同的密碼，就還是有被駭侵者破解的高度風險。

ZachXBT 指出，現在既然已經發生 LastPass 使用者加密資產遭竊的案例，即表示駭侵者已有能力破解經加密的使用者密碼。加密貨幣投資人應立即把資金撤回冷錢包，並且立即修改熱錢包的密碼或復原短語。

建議加密貨幣投資人應避免將錢包復原短語或密碼存於線上密碼管理平台，資金最好存在離線的冷錢包內，如需存於線上熱錢包，應經常修改熱錢包的密碼或復原短語。

- 資料來源：
  1. ZachXBT @zachxbt
  2. LastPass breach linked to theft of $4.4 million in crypto

4.2.2、駭侵者濫用以太坊功能，竊得 6,000 萬美元加密資金

資安廠商 Scam Sniffer 近期發現有駭侵者濫用以太坊的「Create2」功能，成功略過加密錢包的資安功能並入侵加密貨幣位址，在六個月內竊得高達 6,000 萬美元加密資金，受害者近 10 萬人。

Scam Sniffer 近來發現多起利用相同手法的加密資產竊案，都是利用以太坊提供的「Create2」功能來加以濫用。該功能是於以太坊的「Constantinople」改版時推出，可在區塊鏈上新增智慧合約。這個功能非常強大，可以在布署智慧合約前用來計算錢包位址，讓區塊鏈開發者可用以設計出複雜的智慧合約功能，且可以進行鏈下交易之用。

Scam Sniffer 指出，駭侵者利用 Create2 功能憑空創造出全新的智約合約位址，因其不含任何過往的惡意交易記錄，因此當駭侵者將竊取的資金轉入這些全新的錢包位址時，就不易觸發危險位址交易警示。

最近的一次竊取記錄顯示，某位受害者不慎簽署了駭侵者提供的惡意智慧合約，其相當於 927,000 美元的 GMX 代幣就遭到駭侵者轉入這類預先計算的合約位址內，因而遭到竊取。

也有駭侵者利用 Create2 功能，製作出和受害者個人擁有的位址相當接近的錢包位址，用來混淆受害者視聽，讓受害者以為轉帳目標位址是自己所擁有的錢包，從而竊取資金。

Scam Sniffer 指出，自 2023 年 8 月起，已記錄到 11 起駭侵者利用位址混淆手法進行的加密貨幣詐騙，共計損失 300 萬美元；最大的一筆竊案，損失

金額高達 160 萬美元。

建議加密貨幣持有者在進行轉帳時，務必仔細檢查並確認轉帳目標的錢包位址是否完全正確，否則資金一旦轉出就無法逆轉，恐將蒙受重大損失。

- 資料來源：
  1. Wallet Drainers Starts Using Create2 Bypass Wallet Security Alert
  2. Ethereum feature abused to steal $60 million from 99K victims

4.3、國際政府組織資安資訊

4.3.1、全球 40 國將共同簽署協定，共同拒付勒贖贖金

全球 40 國將於華盛頓召開的第三屆國際反勒贖大會（International Counter-Ransomware Initiative Summit）上簽署協定，共同拒付贖金給勒贖團體，以扼止日益猖獗的勒贖攻擊。

本次大會將於 2023 年 10 月 31 日起在華盛頓舉辦，共有全球共 48 個國家與會，包括歐盟與國際刑警組織 (INTERPOL) 在內。會中將聚焦討論如何阻擋勒贖團體的資金流向，並發展出全球共同合作的架構，以阻擋勒贖團體資金的跨境流動。

合作國家將透過美國財政部共享一分黑名單，內容會包括勒贖團體用以匯款的加密貨幣錢包。

白宮負責資安與發展中科技的國家安全副顧問 Anne Neuberger 在記者會上指出，這次大會希望能成功應對日益嚴重，且全球損失金額屢創新高的勒贖攻擊；其中美國是最大的受害國，光是美國一國的損失，就佔全球勒贖攻擊財務損失的 48%。

Neuberger 也表示，將會利用 AI 技術來分析區塊鏈情資，找出不法資金所在並加以打擊。

據資安廠商 NCC Group 的統計，在 2023 年 9 月共記錄到 514 起勒贖攻擊事件，打破 2023 年 3 月創下的歷來最多勒贖攻擊記錄的 459 次。

而從地理分布上來看，北美是遭到勒贖攻擊最嚴重的地區，佔全球總攻擊量的 50%，其次為歐洲的 30%，再其次為亞洲，佔 9%。

近年來的勒贖攻擊，不只攻擊私人企業，也屢屢針對各國政府官方系統發動攻擊，曾造成政府服務受阻的國家，包括哥斯大黎加、肯亞、波蘭、烏克蘭、英國等。

- 資料來源：
  1. Alliance of 40 countries to vow not to pay ransom to cybercriminals, US says
  2. The US and Its Allies Are Pledging Never to Pay Hacker Ransoms

4.3.2、加拿大政府外包業者遭駭，導致政府雇員資料被竊

加拿大政府日前發表資安通報，指出兩家為加拿大政府處理員工轉調手續的外包廠商，日前遭到勒贖攻擊，致使加拿大政府雇員的多種個資外洩。

據加拿大政府的通報指出，兩家協助該國政府員工轉調手續的廠商，分別是 Brookfield Globla Relocation Services (BGRS) 與 SIRVA Worldwide Relocation & Moving Services，兩家公司自 1999 年起即承辦加拿大政府員工調任的相關事宜。

加拿大政府雖然沒有在通報中詳細說明兩家公司遭駭的詳情，但勒贖團體 LockBit 在其官網中表示是該組織犯下對 SIRVA 公司的勒贖攻擊；LockBit 也揚言已經取得該公司多達 1.5TB 的資料，並向該公司要求高達 100 萬美元的贖金，但 SIRVA 並未支付，因此該批被竊資料就遭到 LockBit 公開在暗網中。

另一方面，加拿大政府於 2023 年 10 月 19 日接獲兩家外包廠商遭駭的通報後，立即向該國資安主管機關加拿大資安中心（Canadian Centre for Cyber Security）與隱私保護官辦公室（Office of the Privacy Commissioner）通報事故。

在加拿大政府對外公開的資安通報中，並未提供本次事件的受害人相關資訊，包括潛在的加拿大政府雇員受害者人數在內；不過由於 BGRS 和

SIRVA 兩家公司自 1999 年開始就承接相關業務，因此包括個人資訊財務資訊遭竊的受害者人數可能不在少數。包括加拿大皇家警察（Royal Canadian Mounted Police）、加拿大空軍與多個政府單位從業人員都受到影響。

加拿大政府表示，已針對受害者提供信用監控服務，並對有需要的人員重新核發有效護照等證件；加拿大政府也將在案件調查告一段落後盡快公布調查報告。

建議各政府單位協力外包廠商，應加強資安防護能力，避免政府所屬各種機密文件與人員相關資料遭竊。

- 資料來源：
  1. Message to current and former public service employees and members of the Canadian Armed Forces and
  2. Canadian government discloses data breach after contractor hacks

4.3.3、Royal 勒贖團體要脅 350 個受害者支付 2.75 億美元贖金

美國聯邦調查局（Federal Bureau of Investigation, FBI）與網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），日前聯合發表資安通報，指出一個名為 Royal 的勒贖團體，自 2022 年 9 月起犯下多起勒贖攻擊，總共要求的贖金高達 2.75 億美元。

FBI 在通報中更新了於 2023 年 3 月發出的資安指引，指出自 2022 年 9 月以來，Royal 勒贖團體的攻擊行動，至少有 350 個以上受害個人或團體。

如同其他勒贖團體的攻擊手法，Royal 勒贖團體會先竊取受害者的資料，然後再將其加密並要求高額解鎖贖金；如果受害者拒付贖金，被竊的資料就會遭到 Royal 公開在其網站上。

兩個單位也指出，Royal 勒贖團體最常用於入侵受害者電腦系統的手法，是藉由釣魚郵件來騙取受害者的系統登入資訊。

資安廠商 RedSense 旗下的資安專家也指出，Royal 在今年 9 月時更名為 BlackSuit，並放棄原先使用的駭侵工具與組織架構；新的組織架構更加企業化，更接近其來源駭侵團體 Conti2 的組織與運作方式。

今年 3 月時 FBI 與 CISA 已經在針對 Royal 勒贖團體發布的資安通報中，提供防範該團體進行駭侵攻擊的指引，包括該團體典型的攻擊手法、流程等詳細資訊，以協助各單位阻擋其攻擊，並且攔截進行攻擊用的惡意程式碼酬載。

- 資料來源：
  1. #StopRansomware: Royal Ransomware
  2. FBI: Royal ransomware asked 350 victims to pay $275 million

4.3.4、多國檢警合作破獲大型勒贖集團，受害者遍及全球 71 國

歐洲刑警組織（Europol）、歐洲檢察官組織（Eurojust）日前會同七國執法單位，在烏克蘭境內多處同步執行搜索，成功破獲一個大型勒贖集團，遭該集團攻擊的受害者多達 1,700 個，分布遍及全球 71 國。

超過 20 名來自挪威、法國、德國、美國的調查人員，在行動開始前夕於烏克蘭首都基輔會合，並在荷蘭設立協調行動用的虛擬指揮中心，會同烏克蘭警方於該國境內 30 處以上地點，於 2023 年 11 月 21 日同步展開執法行動。展開搜索行動的城市包括 Kiev、Cherkasy、Rivne、Vinnytsia 等地。

警方行動大有斬獲，不只成功逮捕該勒贖集團的 32 歲首腦，同時也逮捕其他四名集團成員，並扣押多種犯罪相關工具與證物，包括電腦系統、多片 SIM 卡與大量電子犯罪記錄等。

據 Europol 發表的新聞稿指出，該勒贖團體同時利用多種不同的勒贖工具進行攻擊，使用的惡意軟體包括 LockerGoga、MegaCortex、HIVE、Dharma 等；在進行攻擊後，該團體會要求受害企業以比特幣將贖款匯款到指定的加密貨幣交易所帳號，以換取解密用的金鑰。

Europol 也指出，該團體通常先透過暴力試誤法與 SQL 注入攻擊，以及夾帶惡意軟體附檔的釣魚信件，來取得受害企業系統的登入資訊，之後再利用 TrickBot、Cobalt Strike、PowerShell Empire 等惡意軟體來操控受害企業的

內網，再啟動勒贖軟體。所有受害企業合計有超過 250 台伺服器遭到加密攻擊，損失高達數億歐元。

建議各公私單位必須強化資安防護與人員教育訓練，避免勒贖團體利用資安漏洞或釣魚成功，因而遭到攻擊，蒙受重大損失。

- 資料來源：
  1. Ransomware group dismantled in Ukraine in a major international operation supported by Eurojust and
  2. Понад 3 мільярди гривень збитків: кіберполіція та слідчі Нацполу викрили хакерів, які атакували пров

4.4、社群媒體資安近況

4.4.1、Discord 檔案連結將改為暫時有效，以遏止駭侵者置放惡意軟體

全球大型社群討論平台 Discord 日前發布新聞稿指出，該平台將在今年年底之前改用暫時性連結來提供檔案下載服務，以防駭侵者使用其 CDN 服務來放置惡意軟體。

Discord 在回覆資安專業媒體 BleepingCompter 的採訪時指出，該平台正在調整存於其 CDN 中檔案 URL 連結的實作方式，以加強資安防護，提供使用者更安全的使用環境。Discord 指出，新措施將可逐漸減少存放在該平台上的惡意軟體檔案數量，且讓該平台的資安團隊更有效地限制經使用者檢舉的檔案連結。

Discord 即將推出的暫時性檔案連結 URL，在今年年底全面實施後，URL 的有效期限將限縮在 24 小時以內，且檔案連結 URL 會新增三種參數，以強化對 URL 的控制。

資安專家指出，Discord 的新做法是外部期待已久的改變，因為有愈來愈多的駭侵者，利用 Discord 的檔案分享功能來置放其惡意軟體檔案，將 Discord 的 CDN 服務變成惡意檔案擴散平台；特別是進行金融詐騙或由國家力量幕後支援的惡意檔案，數量佔比最高。

據資安廠商 Trellix 的統計，至少有 10,000 個以上的駭侵攻擊活動，使用置放於 Discord CDN 服務的惡意軟體下載 URL 來散播惡意軟體檔案，或是將第二階段的惡意軟體酬載放在 Discord 平台上。

包括 RedLine Stealer、Vidar、AgentTesla、zgRAT、Raccoon Stealer 等惡意軟體，都會使用 Discord 來放置惡意檔案或指令檔。

建議使用者應避免任意點按不明來源傳來的連結，以免遭惡意軟體攻擊或植入。

- 資料來源：
  1. Discord, I Want to Play a Game
  2. Discord will switch to temporary file links to block malware delivery

4.4.2、Bloomberg Crypto 官方 X 帳號遭盜，用以進行 Discord 釣魚攻擊

全球大型財經媒體彭博新聞（Bloomberg News）所屬的加密貨幣子頻道，其在 X 平台上官方帳號日前遭竊，稍後該官方帳號即遭駭侵者用於進行詐騙，將讀者導向至釣魚網站，以騙取受害者的 Discord 平台登入資訊。

根據加密貨幣詐騙觀察家 ZachXBT 指出，駭侵者在該帳號的個人檔案中，放入了一個原本就有 14,000 個成員的 Telegram 聊天頻道連結；該連結會將點按者導向到一個有 近 34,000 名成員的假冒 Bloomberg Discord 聊天室。

據 ZachXBT 指出，Bloomberg 原本的 Telegram 頻道，其使用者名稱為 @BloombergNewsCrypto；在 2023 年 10 月時，該頻道更名為 @BloombergCrypto，但原先使用的舊名因不明原因遭到駭侵者取得，並用來發動釣魚攻擊。

受害者如果進入該舊 Telegram 頻道後，會看到由機器人自動發送的訊息，要求使用者前往其在 Discord 上的聊天室；而使用者在點按該連結後，會先被導到一個假冒的 Discord 使用者身分驗證服務釣魚網站，要求使用者輸入其 Discord 登入資訊，從而竊取使用者的帳密。

資安專家指出，由於許多加密貨幣投資者都使用 Discord 社群服務，因此 Discord 帳號資訊經常成為駭侵者的攻擊目標；駭侵者可利用竊得的 Discord 帳號來推廣加密貨幣詐騙或釣魚攻擊，甚至竊取使用者的加密貨幣資金。

為防範釣魚攻擊，建議加密貨幣投資人避免點按任何不明連結，並採用多階段登入驗證，不在任何可疑網站中提供任何帳密等個人資訊。

- 資料來源：
  1. ZachXBT @zachxbt
  2. Bloomberg Crypto X account snafu leads to Discord phishing attack

4.5、行動裝置資安訊息

4.5.1、Google Play 開始為 Android VPN App 標示資安稽核標章

Google Play 日前開始在上架到該平台的 VPN（虛擬私人網路） App 欄位中，新增一個資安稽核標章，可顯示該 App 與其服務平台是否通過第三方的獨立資安認證。

Google 指出，要能在 Google Play 的 App 說明欄位中獲得此標示，App 與其服務平台必須符合 Mobile App Security Assessment (MASA) 的標準；而 MASA 則是由 App Defense Alliance (ADA) 制訂出的行動 App 資安認證標準。

MASA 的標準要求 App 與其服務平台，在資料儲存、資料隱私、加密、存取認證和工作階段管理 (session management)、網路通訊、平台互動與程式碼品質方面，都有相當嚴格的要求。

Google 會選擇 VPN App 作為首度導入 App 資安稽核標章的先導應用程式類型，主要原因是 VPN 應用程式對於使用者的資安與隱私保護深度相關，且會涉及使用者機敏資訊存取；在 Google Play 中顯示該標章的 App，即表示通過獨立第三方以 MASA 標準進行的資安認證，可為使用者提供多一層的保護與信任。

第三方資安認證廠商，會以 MASA 標準來對 App 的源碼、伺服器設定與配置進行稽核，並且試圖發現 App 中的資安錯誤與弱點，來判斷該 App 是否

符合 MASA 標準，可以獲頒認證合格標章。

由於 Google Play 是屬於 Android 系統的官方 App Store，因此這個標章的推廣，對於強化 Android 平台的安全性，可以帶來正面的影響。

Google 目前要求所有在 Google Play 上架的 VPN App，都必須通過該認證；目前已通過第三方 MASA 認證且獲得認證標章的 VPN app，包括 Nord VPN、Google One、ExpressVPN 等。

未來 Android 使用者在 Google Play 下載各類 App 時，建議可以選擇具有該資安認證標章的 App，以提升安全性。

- 資料來源：
  1. More ways for users to identify independently security tested apps on Google Play
  2. 行動應用程式安全性評估
  3. Google Play adds security audit badges for Android VPN apps

4.5.2、美國 FCC 推新規定防制 SIM-swap 與門號攜碼攻擊

美國聯邦通訊委員會（Federal Communication Commission, FCC）日前推出新規定，強制要求各家電信業者強化 SIM 卡補發或攜碼轉換電信業者作業申請的安全驗證流程，以保護消費者免於日益嚴重的 SIM-swap 攻擊。

FCC 旗下的「隱私與資料保護工作小組」（Privacy and Data Protection Task Force）在 2023 年 7 月研擬推出新規定，以強化消費者與電信業者對 SIM-swap 攻擊的防護能力。所謂 SIM-swap 攻擊是指駭侵者假冒消費者要求補發手機 SIM 卡或申請攜碼至其他電信業者以取得新 SIM 卡，藉以竊取消費者的手機門號控制權。

駭侵者取得新 SIM 卡後，即可以該門號來進行進一步的攻擊活動，例如配合竊得的用戶登入資訊，以該門號接收二階段登入驗證簡訊，取得消費者各種社群與金融服務帳號的控制權，或是假冒消費者身分使用或申請各種服務，以散布惡意連結或惡意軟體等，為害甚大。

FCC 本次新規定修改了與「消費者專屬網路資訊」（Customer Proprietary Network Information，CPNI）與「本地門號可攜性」（Local Number Portability）的相關規定，強制要求電信業者在接獲消費者進行新 SIM 補發或攜碼至其他電信業者服務時，必須進行額外的使用者身分驗證，並且明確通知用戶。

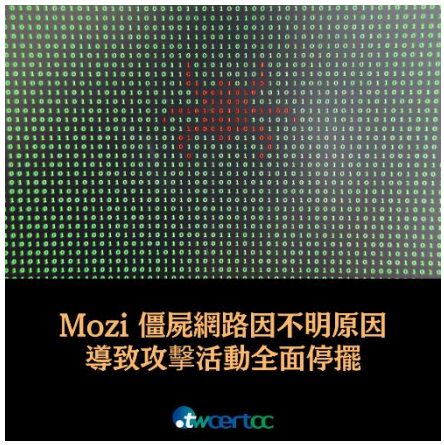
FCC 表示，新規定強化了電信業者對消費者的安全保護責任，期可大幅提高 SIM-swap 的攻擊難度，減少這類攻擊的得逞。

由於在台灣申請這類電信服務均需出示雙證件，因此國內的 SIM-swap 攻擊較為少見；但消費者如果擁有國外電信門號，務必提防這類攻擊。

- 資料來源：
  1. FCC ADOPTS RULES TO PROTECT CONSUMERS' CELL PHONE ACCOUNTS
  2. FCC adopts new rules to protect consumers from SIM-swapping attacks

4.6、軟體系統資安議題

4.6.1、Mozi 僵屍網路因不明原因全面停擺



資安廠商 ESET 日前發表研究報告指出，一個名為 Mozi 的惡意軟體僵屍網路，在今年 8 月時突然大幅減少惡意攻擊活動；在 9 月底時更有一不明酬載上傳，因而全面停擺。

Mozi 是一個知名的分散式阻斷服務攻擊（Distributed Denial of Service, DDoS）惡意軟體僵屍網路，2019 年開始其攻擊行動，主要攻擊目標是各種 IoT 裝置，例如網路路由器、數位攝影機等各種聯網裝置。

Mozi 的典型進攻方式，是利用各種 IoT 設備的資安弱點，例如使用預設登入帳號密碼、未經修補的已知資安漏洞等等，來植入惡意軟體，使裝置成為點對點（peer to peer）僵屍網路的節點之一，再透過 BitTorrent 的 DHT 協定來協同，對特定目標發動 DDoS 攻擊用封包。

據 ESET 的報告指出，Mozi 的活動於 2023 年 8 月 8 日起開始大幅減少，首先是停止了其在印度的所有攻擊活動，之後於 8 月 16 日也停止了在中國的所有攻擊活動；最後在 9 月 27 日時，有一個 UDP 訊息發送給所有的 Mozi 僵屍網路節點，要求節點透過 HTTP 下載一個更新檔，結果造成整個 Mozi 惡意軟體活動的全面停止。

該更新檔甚至也停用了部分受植入裝置的系統服務、阻擋部分連接埠等。

ESET 分析該更新檔後指出，更新檔雖然停止了 Mozi 的攻擊活動，但並沒有完全刪除該惡意軟體，而且遭感染的裝置仍可對遠端伺服器執行 ping，以確認裝置中的 Mozi 惡意軟體仍可接受操控；這表示本次停止活動是受到刻意監控下進行的。

建議各種 IoT 設備的使用者與管理人員，應在有資安更新可用時立即套用更新，並且避免使用預設登入帳號密碼；未使用的連接埠也應全面關閉。

- 資料來源：
  1. Who killed Mozi? Finally putting the IoT zombie botnet in its grave
  2. Mozi malware botnet goes dark after mysterious use of kill-switch

4.6.2、勒贖攻擊導致獨立遊戲 17,000 位玩家資料全遭刪除

資安媒體報導，近日一次勒贖攻擊造成獨立遊戲 Ethyrial: Echos of Yore 中所有 17,000 玩家的帳號資料，以及帳號中儲存的遊戲中寶物與進度全部遭到刪除。

Ethyrial: Echos of Yore 是由獨立遊戲開發廠商 Gellyberry Studios 開發的多人線上角色扮演遊戲，提供使用者免費遊玩；但玩家也可以選擇每月付費以支持遊戲開發。該遊戲仍在早期開發階段，最近開始在 Steam 遊戲平台上開始提供「搶先體驗」版，提供玩家嘗鮮體驗，然而卻在近日遭到勒贖攻擊。

在遭到攻擊後，Gellyberry 於官方 Discord 聊天室發表公告，指出該遊戲在上周五清晨突然遭到不明來源攻擊，伺服器中所有的資料和備份檔都遭到加密鎖定，駭客並要求支付數額不明的比特幣贖金；該公司鑑於多個案例在支付贖金後仍無法取得解鎖密鑰，因此決定不予支付，並且將手動重建伺服器，並且建立新的帳號與遊戲角色資料庫。

Gellyberry 表示，受到影響的 17,000 名玩家，其帳號與儲存的遊戲進度、遊戲內寶物都將復原，並且還會獲得一個進階版的遊戲寵物，以感謝玩家對這段期間不便之處的支持與體諒。

Gellyberry 也表示，為防範這類攻擊再度影響玩家權益與遊戲開發運作，今後會提高遊戲資料庫的離線備份頻率，同時要求所有連線到開發伺服器時必須使用 P2P VPN，並且限制可存取的 IP 網段。

受到影響的玩家須註冊一個新帳號，然後要求平台進行手動資料復原。

服務大批用戶的平台營運者，必須強化資安防護措施，以免因各類攻擊造成服務中斷，或是使用者機敏資訊外洩。

- 資料來源：
  1. Discord
  2. Ransomware attack on indie game maker wiped all player accounts

4.6.3、斯洛維尼亞最大電力公司 HSE 遭勒贖攻擊

東歐國家斯洛維尼亞最大電力公司 Holding Slovenske Elektrarne (HSE)，日前遭到勒贖攻擊，導致該公司部分系統與檔案遭到破壞；但該公司表示供電並未受到影響。

HSE 的電力供應，占斯洛維尼亞國內電力消費的 60% 以上，因此算是該國關鍵基礎設施之一。該公司係於 2001 年由斯洛維尼亞政府設立，目前屬於政府持有的國營企業；其發電方式相當多樣，包括水力發電、火力發電、太陽能發電，甚至還擁有煤礦。HSE 同時也在義大利、賽爾維亞與匈牙利設有分支機構。

據當地媒體報導，攻擊事件係發生於 2023 年 11 月 22 日，該公司於 11 月 24 日發現攻擊事件後，隨即通報斯國資安主管機關，並與警察單位、第三方資安業者與專家合作處理，避免災情擴大到斯洛維尼亞其他機構與系統。

據 HSE 在官方聲明中表示，該公司尚未接獲任何支付贖款的要求，且受到影響的系統，目前侷限於 Sostanj 火力發電廠與 Velenje 煤礦；該公司的供電能力與供電系統運作保持正常。

當地的資安專家指出，這次攻擊事件很可能與 Rhysida 勒贖團體有關；美國資安主管機關 FBI 與 CISA 日前曾針對 Rhysida 勒贈團體的攻擊技術、策略與手段發布資安警訊。

資安專家表示，由於 Rhysida 在攻擊後，通常只會以 Email 來通知受害者，要求受害者以信內提供的密碼，到該團體在暗網設立的網站登入以「協商」贖款，在 Email 中不會有贖金相關金額的資訊。

建議各關鍵基礎設施應加強各類資安防護能力，避免因勒贖或其他型態的資安攻擊，而導致資料外洩，甚至無法正常運作。

- 資料來源：
  1. Kibernetski napad na skupino HSE: 'Zahteve po odkupnini ni, a tudi dostopa ne'
  2. Slovenia's largest power provider HSE hit by ransomware attack

4.7、軟硬體漏洞資訊

4.7.1、Microsoft 推出 2023 年 11 月 Patch Tuesday 每月例行更新修補包

Microsoft 日前推出 2023 年 11 月例行資安更新修補包「Patch Tuesday」，共修復 58 個資安漏洞；其中含有 5 個是屬於已遭駭侵者用於攻擊的 0-day 漏洞。

本月 Patch Tuesday 修復的漏洞數量僅有 58 個，較上個月（2023 年 10 月）的 104 個資安漏洞大為減少；而在這 58 個漏洞中，僅有 3 個屬於「嚴重」等級，另有 5 個是屬於已知遭到駭侵者用於攻擊的 0-day 漏洞，另外還有 15 個遠端執行任意程式碼 (RCE) 漏洞。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 執行權限提升漏洞：16 個；
- 資安防護功能略過漏洞：6 個；
- 遠端執行任意程式碼漏洞：15 個；
- 資訊洩露漏洞：6 個；
- 服務阻斷（Denial of Service）漏洞：5 個；
- 假冒詐騙漏洞：11 個。

本月的 Patch Tuesday 有 5 個 0-day 漏洞，其中有 3 個已遭大規模濫用的兩個，分別如下：

第一個 0-day 漏洞是 CVE 編號為 CVE-2023-36036，存於 Windows Cloud Files Mini Filter Driver 中，屬於執行權限提升漏洞；駭侵者可透過此漏洞，提高自身的執行權限到 SYSTEM 等級，但駭侵者是如何運用此漏洞發動攻擊的，目前仍屬未知狀態。

第二個已遭用於攻擊活動的 0-day 漏洞是 CVE-2023-36033，是存於 Windows DWM Core Library 中的執行權限提升漏洞，駭侵者可利用此漏洞獲得 SYSTEM 權限。

第三個已用於攻擊之中的 0-day 漏洞為 CVE-2023-36025，存於 Windows SmartScreen 中，屬於資安防護機制略過漏洞；駭侵者可利用特製的 Internet shortcut 來跳過資安檢測程序與警示訊息顯示。

- CVE 編號：CVE-2023-36036、CVE-2023-36033、CVE-2023-36025
- 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. Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
  2. Windows DWM Core Library Elevation of Privilege Vulnerability
  3. Windows SmartScreen Security Feature Bypass Vulnerability

4.7.2、Google Chrome 緊急推出 0-day 漏洞更新

Google 於近日針對 Chrome 瀏覽器中的一個 0-day 漏洞 CVE-2023-6345 發表緊急更新，廣大 Google Chrome 使用者均應立即更新瀏覽器。這是 Google Chrome 今年第六個被發現的 0-day 漏洞。

這個 0-day 漏洞 CVE-2023-6345 存於 Skia 開源 2D 繪圖程式庫中，屬於整數溢位錯誤；駭侵者可利用此漏洞來誘發系統崩潰，進而執行任意程式碼。該漏洞所在的 Skia 繪圖引擎程式庫，同樣也使用於多種軟體如 ChromeOS、Android 與 Flutter 中。

該漏洞是由 Google Threat Analysis Group (Google TAG) 旗下的資安專家所發現；Google TAG 長期以來就擅於發現各種 0-day 漏洞；而該單位發現的 0-day 漏洞，經常會遭到駭侵團體用於攻擊各種重要人士。

Google 也在相關資安通報中指出，該公司已接獲 CVE-2023-6345 已遭駭侵者廣泛用於攻擊活動的情資。這個漏洞的 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)。

- CVE 編號：CVE-2023-6345
- 影響產品(版本)：這個漏洞對所有平台的 Google Chrome 都造成影響，包括 Windows、macOS 和 Linux 平台；Google 也已在 Stable Desktop channel 中推出更新，使用應立即在 Chrome 中選取更新功能，將其 Chrome 瀏覽器更

新到 Windows 版 119.0.6045.199/.200、macOS 與 Linux 版更新至 119.0.6045.199。

- 解決方案：建議 Chrome 使用者應立即將 Chrome 瀏覽器更新到 Windows 版 119.0.6045.199/.200、macOS 與 Linux 版更新至 119.0.6045.199。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google Chrome emergency update fixes 6th zero-day exploited in 2023

4.7.3、全新發現的 BLUFFS 攻擊，可挾持藍牙連線並竊聽通訊內容

Eurocom 旗下的資安專家，近日發現針對藍牙連線通訊的全新攻擊方法 BLUFFS；這些攻擊手法可以介入裝置間的藍牙加密通訊，除可假扮成連線對象裝置外，還可發動各種中間人攻擊（Man-in-the-middle attacks）。

BLUFFS 一共包括六種攻擊手段，其運作原理係應用四個不同的藍牙標準漏洞（其中兩個是未被發現的新漏洞）；這些漏洞發生於裝置間進行藍牙連線時的連線階段解密金鑰的交換流程。

利用這些漏洞的組合，BLUFFS 可以產生出長度較短、較易預測出來的 SKC 金鑰，接著再利用暴力試誤法來試圖解碼藍牙通訊的內容，以便假扮藍牙通訊中的通訊方，進而發動後續的中間人攻擊。

Eurocom 的研究人員不只發展出理論上的攻擊手法，同時也開發出概念驗證工具，可實際進行模擬攻擊；由於該漏洞存於藍牙通訊的基礎架構上，因此不分硬體製造商，所有從 Bluetooth 4.2 到 2023 年 2 月方才發布的最新版本 Bluetooth 5.4，都含有此漏洞。

Eurocom 在研究報告中也提供了對多種市售藍牙晶片與裝置的攻擊結果，各大廠牌推出的各種產品中的藍牙晶片幾乎無一倖免，全部可以使用 BLUFFS 中的六種攻擊手法加以攻擊得逞。

- 解決方案：藍牙標準制定者 Bluetooth SIG 已接獲 Eurocom 的通報，並建議廠商在實作藍牙連線時提高加密金鑰長度限制，並使用 Mode 4 Level 4，並在裝置配對時使用 Secure Connection Only 模式，即可避免遭到 BLUFFS 攻擊。

- 資料來源：

1. BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses
2. Bluetooth SIG Statement Regarding the “Bluetooth Forward and Future Secrecy Attacks and Defenses

第 5 章、 資安研討會及活動

2023 物流與供應鏈資安研討會	
活動網站	https://www.accupass.com/event/231129032054194239023 6
活動概要	 活動資訊：物聯網數位新時代，供應鏈的運作變得日益複雜，亦面臨外部資訊安全的諸多威脅，資安已是另類新形態的「恐怖攻擊」，尤其勒索與癱瘓企業運作屢見不鮮相信，您我深知保障企業數據和系統安全的重要性，因此本會與東吳大學特別邀請來自新加坡及台灣在資安界頗具盛名之專家，分享最新資安議題與解決方案。歡迎各界參加，錯過只能持續面臨資安恐攻! 活動時間：112 年 12 月 12 日(二) 09:00(報到) - 11:40 活動地點：東吳大學城中校區第五大樓 5117 哲名廳 (台北市貴陽街一段 56 號) 主辦單位：東吳大學資安卓越中心 協辦單位：台灣全球商貿運籌發展協會 活動議程：請參閱活動網站 備註：活動免費 聯絡人：秘書處 謝家軒先生 02-25997287

從沙崙資安基地眺望 2024 資安未來研討會

活動網站	https://nds.kktix.cc/events/hackermeetup2023
活動概要	 2023 年全球都在關注的網路安全零信任轉型，現在不只企業組織相當重視，經過三年新冠疫情，讓多國政府也大力提倡【網路安全零信任】。世界各國幾乎都在推廣零信任網路安全策略，主要原因是在 APT 攻擊猖獗、BYOD 與遠端存取需求高漲之下，傳統網路安全策略聚焦邊界防護的作法頻頻遭到不同形式的突破，為了大幅降低企業發生資料外洩災情，以及減少橫向移動攻擊的影響網路安全零信任變成最值得相信的資安服務與產品。另外，台灣資安社群與資安競賽蓬勃。本次活動邀請過去參與過資安社群活動經驗豐富的資安社群團隊與白帽駭客與大家交流，針對目前資安從業人員最關心技術問題與職場議題進行交流。 有鑑於此，主辦單位特別在歲末年終舉行【從沙崙資安基地眺望 2024 資安未來研討會】邀請資安專家及資深白帽駭客分享最新研究觀察，期待讓與會者得到自主研究的全新視野，歡迎對此主題有興趣者報名參加本活動。 指導單位：國家科學及技術委員會、教育部 主辦單位：財團法人國家實驗研究院國家高速網路與計算中心 執行單位：NDS 次世代創新數位安全協會 合作社群：UCCU、若渴計畫、Women Code Tech 社群 時　　間：2023 年 12 月 14 日（四）- 2023 年 12 月 15 日（五）

	地　　點：國科會資安暨智慧科技研發大樓 1F 國際會議廳（台南市歸仁區歸仁十三路一段 6 號） 活動議程請參閱活動網站。

智慧製造產業跨域資安人力高峰論壇	
活動網站	https://isipevent.kktix.cc/events/f2ce8bcc-copy-4
活動概要	 【活動介紹】 教育部先進資通安全實務人才培育計畫與台灣資安主管聯盟及 CIO IT 經理人雜誌，在 2023 年 12 月 15 日（星期五）14:00-17:00，聯合主辦「智慧製造產業跨域資安人力高峰論壇」，希望落實資安觀念向下扎根，並鼓勵更多年輕學子投入資訊安全領域，本次邀請智慧製造產業資安主管分享智慧製造產業端對於資安人才的需求。趕緊手刀手報名吧！錯過可惜！ 【活動資訊】 活動名稱：智慧製造產業跨域資安人力高峰論壇 指導單位：教育部資訊及科技教育司 主辦單位：CIO IT 經理人雜誌、台灣資安主管聯盟、教育部先進資通安全實務人才培育計畫 協辦單位：輔仁大學資訊工程學系、臺灣科技大學資訊工程系、中央大學資訊工程學系、臺北科技大學資訊工程系 參與方式：索取免費票券 活動日期：2023 年 12 月 15 日（星期五） 14:00-17:00 報到時間：13:30-14:00

活動地點：集思北科大會議中心 2 樓感恩廳

【活動時程表】

13:30-14:00 報到

14:00-14:10 開場致詞

14:10-14:25 教育部先進資通安全實務人才培育計畫 概況介紹

14:30-15:30 智慧製造產業資安發展趨勢與職能需求

廣達電腦 林家弘副處長

華碩電腦 劉諭聰經理

廣運機械 黃世昌資安長

(依上台次序排序)

15:35-15:50 中場休息、茶敘交流

15:50-17:00 座談時間

廣達電腦 林家弘副處長

華碩電腦 劉諭聰經理

廣運機械 黃世昌資安長

(依上台次序排序)

【報名規則】

本活動為免費報名，請留意報名時間，活動當天請準時出席。

報名時請妥善填寫真實資料。

活動需簽到和簽退，參加證明僅提供給事先報名並完成簽到退且具學生身分者。未簽到退者，將不予以發放。簽到退時間異常，也可能導致無法取得參與證明。

線上資安專題講座-管窺資訊安全產品研發與人力需求	
活動網站	https://isipevent.kktix.cc/events/098efec3-copy-1
活動概要	 【活動介紹】 教育部先進資通安全實務人才培育計畫在 2023/12/16（六） 14:00 - 16:00，舉辦「線上資安專題講座」，希望落實資安觀念向下扎根，並鼓勵年輕學子投入資訊安全領域，本次邀請 TXOne Threat Research Director 高迦南先生擔任講者，將分享「管窺資訊安全產品研發與人力需求」的專題，趕緊手刀手報名吧！錯過可惜！！ 【活動資訊】 活動名稱：線上資安專題講座-管窺資訊安全產品研發與人力需求 指導單位：教育部資訊及科技教育司 主辦單位：教育部先進資通安全實務人才培育計畫 參與方式：索取免費票券 活動日期：2023/12/16（六） 14:00 - 16:00 報到時間：13：30 - 14：00 活動地點：線上舉辦（活動前一天會提供會議連結至報名者的電子信箱） 【活動時程表】 13:30 - 14:00 講師、與會者報到入場 14:00 - 14:05 活動開場

	14:05 - 15:30 專題講座 15:30 - 15:50 QA 座談時間 15:50 - 16:00 結語 【報名規則】 本活動為免費報名，請留意報名時間，活動當天請準時出席。 報名時請妥善填寫真實資料。 活動需簽到和簽退，參加證明僅提供給事先報名並完成簽到退且具學生身分者。未簽到退者，將不予以發放。簽到退時間異常，也可能導致無法取得參與證明。

【資安學院】12/19-12/20 NIST 網路安全框架建置訓練課程

活動網站	https://www.cisanet.org.tw/Course/Detail/3971
活動概要	 費用： 原價：NT 22,500 元/人 軟協會員：NT 20,000 元/人 費用含稅、教材及完課證明 活動日期：2023/12/19-12/20 09:00~17:00 活動地址：中華民國資訊軟體協會-大同辦公室 D01 大會議室（台北市中山區中山北路 3 段 22-1 號新設工大樓 5 樓 C 區） 活動內容 / Event Deails： 2013 年初美國總統歐巴馬指示國家標準暨技術研究院（National Institute of Standards and Technology, NIST）與全球自願開發網路安全框架的相關利害關係人合作；在過去的五年中，對關鍵基礎設施的威脅及發生之可能性一再增加，建立在其上的 NIST 框架和網路安全戰略也變得越來越重要。 透過參加為期兩天的課程，您將了解如何使用 NIST 網路安全框架來幫助組織預防、偵測和回應網絡攻擊；此外還將了解如何將 NIST 網路安全框架與其他管理系統整合，特別是 ISO / IEC 27001 及附錄 A 的控制措施。課程進行方式包含講師解說，小組討論和課堂學習。

	聯絡窗口： 02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw 報名截止： 2023-12-11

【資安學院】12/25 金融資安威脅與區塊鏈課程	
活動網站	https://dtu.cisa.tw/course.php?id=80
活動概要	 費用： 原價：NT 6,900 元/人 早鳥價：NT 6,200 元/人(課程前一個月報名) 軟協會員：NT 5,600 元/人 費用含稅、教材及完課證明 活動日期：2023-12-25 09:00~16:00 活動地址：中華民國資訊軟體協會-大同辦公室 D01 大會議室（台北市中山區中山北路 3 段 22-1 號新設工大樓 5 樓 C 區） 活動內容 / Event Deails：近期針對金融機構的資安攻擊頻傳，包含釣魚簡訊詐騙、客戶密碼撞庫攻擊等事件層出不窮，本課程除研析過往金融資安發生的實際案例外，亦探討企業在運用 AI 人工智慧、區塊鏈、雲端運算及大數據分析等金融科技時可能遇到之資安威脅。 聯絡窗口： 02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw 報名截止： 2023-12-18

第 6 章、 TVN 漏洞公告

TWCERT/CC 上月份發布之嚴重程度前五資安漏洞資訊如下表：

中華電信 NOKIA G-040W-Q-Improper Input Validation	
TVN / CVE ID	TVN-202311011 / CVE-2023-41355
CVSS	9.8 (Critical)
影響產品	NOKIA G-040W-Q: G040WQR201207
問題描述	中華電信 NOKIA G-040W-Q 的防火牆功能未阻擋 ICMP redirect 請求，未經驗證攻擊者可利用此漏洞進行 DoS 攻擊或是造成流量外洩。
解決方法	更新韌體版本至 G040WQR231013
公開日期	2023-11-03
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7505-a0c94-3.html

中華電信 NOKIA G-040W-Q - Broken Access Control	
TVN / CVE ID	TVN-202311007 / CVE-2023-41351
CVSS	9.8 (Critical)
影響產品	NOKIA G-040W-Q: G040WQR201207
問題描述	中華電信 NOKIA G-040W-Q 存在 Authentication Bypass 漏洞。未經驗證的遠端攻擊者能以任意使用者身份(包含管理者)bypass 驗證機制，以特殊 URL 登入系統。若攻擊者以管理者身份登入系統，則能執行任意系統指令，對系統進行控制，並中斷服務。
解決方法	更新韌體版本至 G040WQR231013

公開日期	2023-11-03
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7501-6155a-3.html

中華電信 NOKIA G-040W-Q - Weak Password Requirements	
TVN / CVE ID	TVN-202311009 / CVE-2023-41353
CVSS	8.8 (High)
影響產品	NOKIA G-040W-Q: G040WQR201207
問題描述	中華電信 NOKIA G-040W-Q 存在弱密碼管理機制。遠端攻擊者可以一般使用者身分登入設備後，利用設備資訊推測管理者密碼，進而利用此漏洞取得管理者權限。
解決方法	更新韌體版本至 G040WQR231013
公開日期	2023-11-03
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7503-a27ed-3.html

叡揚資訊 Vitals ESP - Arbitrary File Upload	
TVN / CVE ID	TVN-202311014 / CVE-2023-41357
CVSS	8.8 (High)
影響產品	Vitals ESP: 6.1 and prior
問題描述	叡揚資訊 Vitals ESP 的特定參數為未進行妥善驗證，遠端攻擊者以使用者權限登入後，可利用此漏洞繞過檔案檢查機制，將腳本上傳至任意系統目錄後執行，藉以操作系統或中斷服務。
解決方法	請聯繫叡揚資訊，以完成升級或修復事宜。
公開日期	2023-11-03
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7508-6d1ef-3.html

ASUS RT-AX55 - command injection - 1	
TVN / CVE ID	TVN-202311002 / CVE-2023-41345
CVSS	8.8 (High)
影響產品	RT-AX55: 3.0.0.4.386.51598
問題描述	華碩 RT-AX55 與驗證相關的產生 token 功能未對特殊參數作過濾，經驗證之遠端攻擊者可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令，並導致阻斷系統與終止服務。
解決方法	更新版本至 3.0.0.4.386_51948
公開日期	2023-11-03
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7496-96e2c-3.html**

第 7 章、 2023 年 11 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。

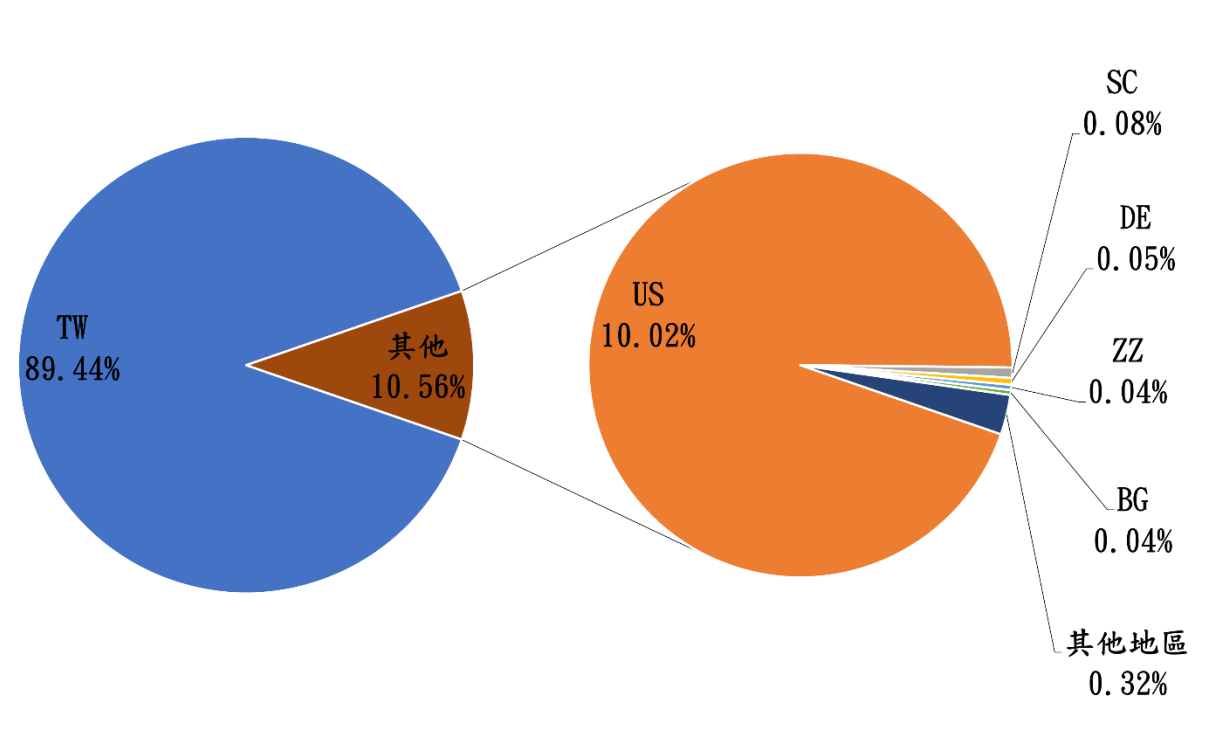


圖 1、分享地區統計圖

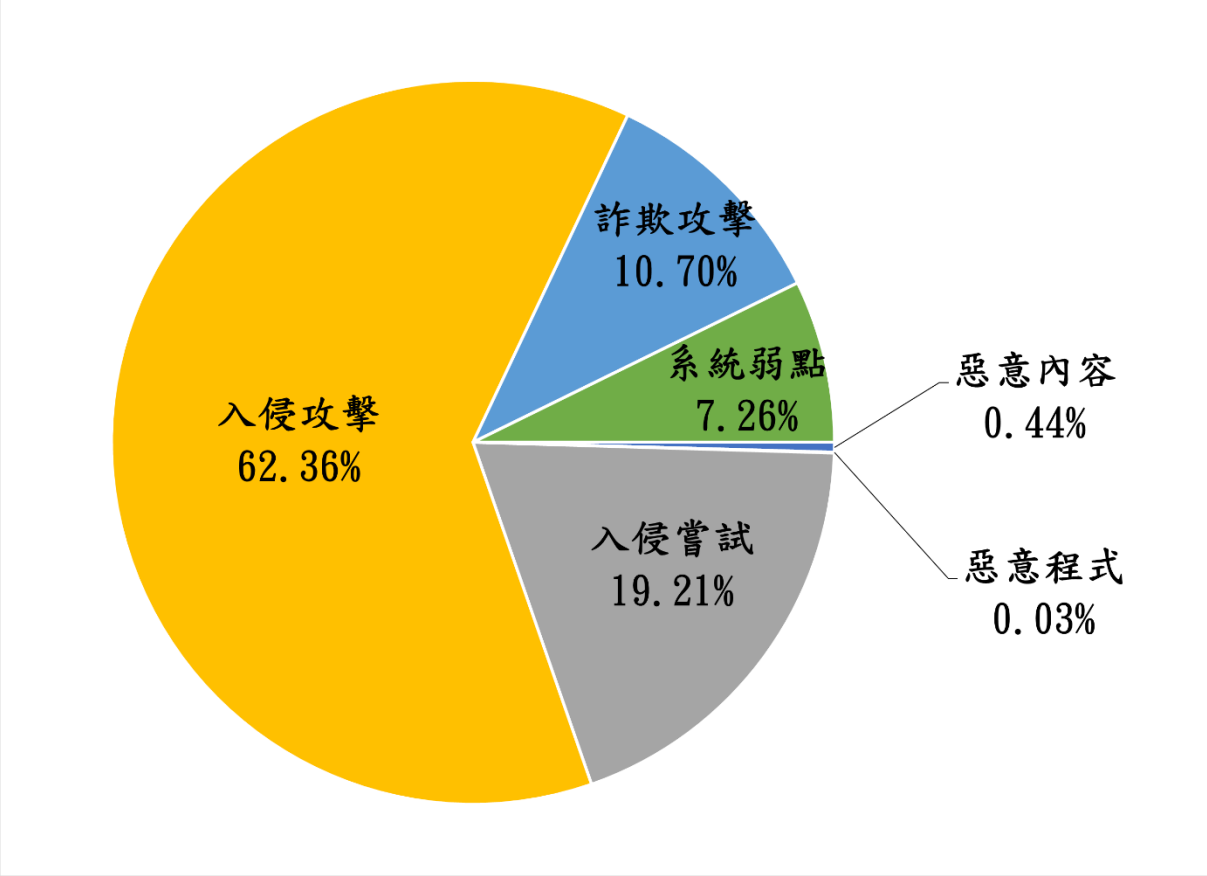


圖 2、分享類型統計圖

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 12 月 8 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**