TWCERT/CC 資安情資電子報

2022 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 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 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

資安廠商發現數千起駭侵者滲入 Microsoft Teams 群組，散布惡意木馬軟體案例

資安廠商 Avanan 旗下的資安研究人員，近日發現有駭侵者滲入全球眾多企業廣泛採用的工作討論群組服務 Microsoft Teams，並在群組討論中散布惡意軟體，誘使企業員工安裝。

Microsoft Teams 的使用者相當多，據統計全球活躍用戶多達 2.7 億人，因此成為駭侵者眼中極佳的釣魚攻擊目標。

Avanan 指出，該公司的研究人員自今（2022）年起觀察到數千次採用類似手法的 Microsoft Teams 攻擊事件。駭侵者以先前釣魚攻擊或其他手法，取得目標企業員工的 Microsoft 365 或電子郵件登入資訊，即可進入目標企業的 Microsoft Teams 討論群組。

進入群組討論後，駭侵者會在討論群組中分享一個名為「User Centric」的執行檔，實際上內含特洛伊木馬惡意軟體；一旦有企業員工不查，安裝該惡意軟體於電腦上，該惡意軟體即可常駐於系統中，攔截使用者的輸入資訊，並竊取各種機敏資料。

Avanan 在報告分析中表示，由於 Microsoft Teams 本身的資安保護設施有缺陷，惡意連結與檔案的掃瞄不夠徹底，再加上各種防毒防駭軟體，儘管對 Email 等傳統通訊方式有相當程度的保護措施，但對 Microsoft Teams 之類的通訊工具並未提供足夠的防護能力。

Avanan 也說，一般企業員工對於 Email 的資安意識比較牢固，但對於 Micrisoft Teams 之類的群組討論工具，就往往失去戒心；該公司過去針對醫療院所的研究，就發現醫護人員對於在 Email 中分享機密資訊的資安風險較為理解，但對於 Microsoft Teams 之類平台中可能發生的資安風險，其理解程度欠佳，導致駭侵者可輕易受邀入群，甚至在其中散布惡意連結與軟體。

- 資料來源：
  1. Hackers Attach Malicious .exe Files to Teams Conversations
  2. Attackers use Microsoft Teams as launchpad for malware

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、Linux 開發者修補資安漏洞的速度，比其他作業系統業者都快

Google資安團隊指出，Linux開發者修補資安漏洞的速度，比其他主流軟硬體與作業系統業者都快

Google 旗下的資安研究團隊，針對市場主流作業系統、軟硬體業者修補該單位提報資安漏洞的所需時間發表統計報告，指出 Linux 開發者推出資安修補所需日數是最短的。

Google 旗下的資安研究團隊 Project Zero，日前發表一分針對市場主流作業系統、軟硬體業者修補該單位提報資安漏洞所需時間的統計報告；報告中指出 Linux 開發者推出資安修補所需日數是最短的，平均為 25 日。

在這份報告中，Project Zero 統計了 2021 年各大主流作業系統暨軟硬體廠商，針對該單位發現並提報的資安漏洞，推出修補更新所需的日數。首先，各廠商推出修補的平均所需日數為 52 日，較三年前的 80 日大幅加速，顯見各廠商對資安漏洞的修補更加重視，並投入了大量資源。

報告中說，Project Zero 在 2019 到 2021 年間，一共向各廠商提報多達 376 個資安漏洞，並要求這些廠商按該單位設立的標準（90 日）內修復漏洞；其中有 351 個（93.4%）獲得修復、14 個（3.7%）被廠商回報列為不予修復（won’ t fix）、11 個（2.9%）從未修復。

從漏洞修復的速度來看，這三年來各大廠商修復漏洞的速度多半都有加快，從 2019 年到 2021 年所需日數如下所示：

- Apple：71 天、63 天、64 天；
- Microsoft：85 天、87 天、76 天；
- Google：49 天、22 天、53 天；
- Linux：32 天、22 天、15 天；
- 其他：63 天、54 天、29 天。

而在未能於 90 日內修復提報漏洞的比例來看，近三年來比例最高的是 Oracle，有高達 57% 的漏洞都未能於 90 日再加 14 天最後期限的 104 日內修復；而 Apple 與 Micrsoft 則有 5%、Linux 有 4%、Google 有 2%，其他為 7%。

- 資料來源：
  1. A walk through Project Zero metrics
  2. Linux developers patch security holes faster than anyone else, says Google Project Zero

2.1.2、資安廠商 ESET 發表 2021 資安威脅報告

資安廠商 ESET 發表年度資安威脅報告 ESET Threat Report T3 2021；報告總結指出 2021 年最大的資安威脅來源，是來自各種被發現的軟硬體嚴重資安漏洞。

在報告中指出，2021 年各種重大資安威脅中，有許多源於各種軟硬體的研究漏洞，如年初有超過 10 個以上的 APT 駭侵團體，利用 Microsoft Exchange Server 中的 ProxyLogon 嚴重漏洞，對全球目標發動大規模駭侵攻擊；而 Microsoft Exchange Server 中的另一個嚴重漏洞 ProxyShell，則在 2021 年 8 月引發另一波各個駭侵體的全球性攻擊活動。

在 2021 年 12 月底發現的 Log4j 漏洞，則是去年度另一個引發大規模資安危機的軟體漏洞。該漏洞的 CVSS 危險程度評分高度滿分 10 分，且駭侵者可利用此漏洞挾持整個網站，因此也引來各個駭侵團體的大規模濫用。據 ESET 的監控資料指出，Log4j 漏洞攻擊在 2012 年的最後三周內快速暴增，成為全年第 5 大資安攻擊主因，可見其嚴重程度。

ESET 在報告中也指出，RDP 遠端桌面攻擊，延續自 2020 年因肺炎疫情導致的全球封城與在家工作潮，而在 2021 年仍然大幅成長；據該公司的監控資料指出，2021 年全年遭到資安防護軟體阻擋的 RDP 攻擊次數，較 2020 年大幅成長 897%。

另外，透過 Android 平台上的惡意軟體進行的金融詐騙相關攻擊，2021 年的發生次數，也較 2020 年大增 428%。

- 資料來源：
  1. ESET Threat Report T3 2021
  2. THREAT REPORT T3 2021

2.2、新興應用資安

2.2.1、資安廠商發現一個會竊取 Windows 用戶加密貨幣的 Golang 僵屍網路

資安廠商近來發現一個新的僵屍網路 Kraken，會利用一個稱為 SmokeLoader 的後門木馬軟體，在入侵 Windows 裝置後，竊取用戶電腦上各種資訊。

資安廠商 ZeroFox 旗下的研究人員，近來發現一個新的僵屍網路 Kraken。這個僵屍網路會利用一個稱為 SmokeLoader 的後門木馬軟體，在入侵 Windows 裝置後，竊取用戶電腦上各種資訊，還會將用戶加密貨幣錢包中的資產盜領一空。

該公司是在去（2021）年 10 月起開始觀察到 Kraken 的活動；每一次 Kraken 設立一台新的控制伺服器（Command and control server），就會觀察到數百台 Windows 裝置遭駭。

在報告中，研究人員指出這個版本的 Kraken，除了會修改遭駭 Windows 電腦的登錄檔，確保該惡意軟體可以阻擋 Windows Defender 偵測並在電腦中持續常駐執行外，也能收集電腦上的各種資訊、下載並執行軟體、執行 shell 命令、截取畫面，並且竊取用戶加密貨幣錢包中的資金。

在 ZeroFox 觀察到的案例中，受害 Windows 電腦中的 Kraken 惡意軟體，在感染後多半會下載另一個叫做 RedLine Stealer 的惡意軟體，可以用來竊取用戶的密碼、瀏覽器 cookie、信用卡資訊與加密貨幣錢包資訊。

不過 ZeroFox 也指出，光是 Kraken 本身就具備竊取加密貨幣的能力，包括 Zcash、Armory、Bytecoin、Electrum、Ethereum、Exodus、Guarda、Atomic、Jaxx Library 等多種加密貨幣錢包，Kraken 都可竊取其中存放的加密貨幣。

據 ZeroFox 觀察，屬於 Kraken 駭侵者的主要錢包，每個月都約有 3,000 美金的轉入。而這些駭侵者也經常「轉移陣地」，關閉運作一段時間的控制伺服器，轉而以全新 IP 設立全新的控制伺服器，以避免遭到鎖定。

- 資料來源：
  1. Meet Kraken: A New Golang Botnet in Development
  2. New Golang botnet empties Windows users' cryptocurrency wallets

2.2.2、加密貨幣平台 Wormhole 遭駭，損失達 3.26 億美元，現已補回

可提供多種加密貨幣互換的跨鏈加密貨幣去中心化金融交易平台 Wormhole 日前遭駭，損失包裝以太幣 120,000 枚。

可提供多種加密貨幣互換的跨鏈加密貨幣去中心化金融（Decentralized Finance, DeFi）交易平台 Wormhole 日前遭駭，損失包裝以太幣（wETH）120,000 枚，現額高達 3.26 億美元；不過一家投資該平台的合作伙伴，已出資彌補用戶的損失。

該起駭侵事件發生於 2022 年 2 月 3 日，當時 Wormhole 的系統遭到不明來源的駭侵攻擊；駭侵者利用該平台智慧合約的漏洞，在其平台上的智慧合約，憑空鑄造出 120,000 枚「包裝以太幣 wETH」（即以 Solana 區塊鏈製作出的加密貨幣，價格鎖定以太幣），接著再換成 93,750 枚以太幣，並將其轉帳到自有的以太坊區塊鏈錢包內。

據區塊鏈相關媒體報導指出，這次攻擊的主因在於 Wormhole 的「保護帳號」（guardian accounts）並未進行驗證，因此導致駭侵者可利用這個漏洞，憑空鑄造出 120,000 枚 wETH，完全零成本。

Wormhole 在發現漏洞遭攻擊後，除了修補漏洞外，同時試圖和駭侵者談判；Wormhole 表示願意提供 1,000 萬美元當做獎金，要求駭客將竊走的 wETH 歸還給 Wormhole；不過截至目前為止，駭侵者竊走的 93,750 枚以太幣，仍然並未轉移到任何錢包之中，該在駭侵者的控制之下。

不過，Wormhole 的投資者之一 Jump Crypto 在事件發生後，立即對 Wormhole 補回 120,000 枚 wETH，因此在這次駭侵事件中，投資人的所有損失都得到彌補。

資安專家指出，Wormhole 使用的 Solana 區塊鏈相關程式碼版本過舊，可能是造成這次攻擊事件的主要破口；一月中旬在 GitHub 上就有針對該平台 Solana 程式碼更新的 Pull request，但程式碼遲到二月才見變更，數小時之後就發生了此次駭侵事件。

- 資料來源：
  1. $325 Million Stolen from Wormhole DeFi Service
  2. Wormhole restores stolen $326 million after major crypto bailout

2.2.3、全球最大 NFT 交易平台 OpenSea 用戶遭釣魚攻擊詐騙，損失達 200 萬美元

OpenSea 日前發生多名用戶遭到駭侵者發動的釣魚攻擊的資安事件，導致高達 200 萬美元以上的 NFT 收藏品遭駭侵者竊走。

全球交易量最大的「非同質性代幣」（Non Fungible Token, NFT）交易平台 OpenSea，日前發生多名用戶遭到駭侵者發動的釣魚攻擊的資安事件，導致高達 200 萬美元以上的 NFT 收藏品遭駭侵者竊走。

據資安廠商 Check Point 指出，駭侵者是利用 OpenSea 即將升級其智慧合約（Smart Contract）系統的時機，對部分 OpenSea 用戶發送詐騙的釣魚信件，內容要求用戶必須在規定時間之內，將其上架於 OpenSea 的 NFT 收藏品搬移（migrate）到新平台上，否則原先上架的 NFT 將會下架，用戶必須另行上架。

一旦用戶按下釣魚信件中的按鈕，就會被導到一個釣魚網站；如果用戶按下了「簽署」的按鈕，其帳號中擁有的 NFT 代幣，就會被轉移到由駭侵者控制的錢包內。

在這次事件中，受害的 OpenSea 用戶一共有 17 名，一共有 250 個以太坊（Ethereum）上的 NFT 代幣遭到竊走，以美元計價，損失高到 200 萬美元左右。

OpenSea 在調查這起事故後，對外聲明表示，這次事件並非利用 OpenSea 平台的系統進行，該公司的平台並沒有發現任何相關漏洞，因此是一次單純的釣魚詐騙案件。

在該起事件曝光後，駭侵者就停止發送釣魚詐騙信件給其他 OpenSea 用戶，因此案情並未繼續擴大。

資安專家呼籲，由於近日 NFT 的交易十分熱門，涉及的轉帳金額也愈來愈大，因而成為資安攻擊的目標；用戶在進行任何帳務相關操作時，務必再三確認，以免成為這類詐騙案件的受害者，蒙受巨大損失。。

- 資料來源：
  1. New OpenSea attack led to theft of millions of dollars in NFTs
  2. OpenSea users lose $2 million worth of NFTs in phishing attack

2.3、國際政府組織資安資訊

2.3.1、烏克蘭國防部、國營銀行遭 DDoS 攻擊

烏克蘭國防部與兩間烏克蘭國營銀行，近日遭到嚴重的分散式服務阻斷（Distributed Denial of Service, DDoS）攻擊，導致正常業務活動受阻。

在烏克蘭國防部方面，該部表示其網站可能因遭受 DDoS 攻擊而無法順利運作。烏克蘭資安主管機關「國家特種通訊與資訊保護局」（State Service of Special Communications and Information Protection）指出，攻擊活動自今（2022）年 2 月 15 日開始，該局並且記錄到數量極為龐大的同時發生連線要求。

而在遭到攻擊的國營銀行方面，受害對象是烏克蘭最大的銀行 Privatbank 以及國營儲蓄銀行 Oschadbank；這兩家銀行的官方網站雖然仍可存取，但用戶無法登入自己在這兩家銀行的帳號，以使用線上金融服務；另外也有部分存戶雖然可以登入帳戶，但帳戶內的餘額與近期交易活動清單資訊均不正確。

該國的另一資安相關單位「烏克蘭安全局」（Security Service of Ukraine），曾在本周稍早時指出該國正在遭逢「大規模混合作戰」的打擊。該局指出，攻擊者的目的在於引發烏克蘭國內的混亂與人心浮動，而該局已成功阻止某些攻擊活動，並且緝獲數個僵屍網路農場；這些僵屍網路針對烏克蘭公民散布炸彈攻擊訊息和各式假訊息，以試圖在烏克蘭境內製造恐慌。

烏克蘭政府旗下的電腦事件緊急反應小組，也指出這些針對該國的多起網路攻擊活動，都由一個名為 Gamaredon 的駭侵團體策畫發動。。

- 資料來源：
  1. Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#3787)
  2. Defence of Ukraine @DefenceU
  3. Ukrainian military agencies, state-owned banks hit by DDoS attacks

2.3.2、美國資安主管機關指出，多家美國國防部包商遭駭侵攻擊

美國三大資安主管機關，日前聯合發布資安通報，指出多家美國國防部承包廠商，自 2020 年起遭駭侵者發動長期攻擊。

美國三大資安主管機關聯邦調查局（Federal Bureau of Investigation, FBI）、國家安全局（National Security Agency, NSA）、網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），日前聯合發布資安通報，指出多家美國國防部承包廠商，自前 2020 年 1 月起，開始遭疑似有幕後資助指揮的相關駭侵者發動長期攻擊。

這些美國國防部的承包廠商（U.S. Cleared defense contractors, CDCs），主要負責生產或提供服務的範圍，包括指令、控制、通訊與戰鬥系統；情報、監控、偵搜、定位；武器與飛彈研製；車輛與飛行器設計製造，以及軟體開發、資料分析、電腦系統與物流等等。

通報指出，這些針對多家國防部承包商的駭侵攻擊行動，有些持續長達六個月，且定期竊取數百份機密文件、郵件與其他類型資料。

通報表示，在這波駭侵攻擊中，駭侵者主要嘗試駭入各該承包商使用的軟體與雲端服務，特別是廣為使用的 Microsoft 365 環境。

通報也指出，這些遭駭的承包廠商服務對象遍及美國軍方各單位，包括美國陸軍、空軍、海軍、太空軍、國防部，以及各情治單位。

通報說，敵對勢力取得這些文件、郵件和資料後，將可據以調整其軍事計畫與重點，加速相關技術開發進程，並且與其盟友分享資料，對美國國家

利益影響至鉅。

- 資料來源：
  1. Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive
  2. US says Russian state hackers breached defense contractors

2.3.3、FBI 警示：BlackByte 勒贖攻擊已駭入多個美國關鍵基礎設施內網

美國聯邦調查局日前發布資安通報，指出一個名為 BlackByte 的勒贖團體，過去三個月來已入侵至少三個美國關鍵基礎設施機關的內部網路。

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前發布資安通報，指出一個名為 BlackByte 的勒贖團體，過去三個月來已入侵至少三個美國關鍵基礎設施機關的內部網路。

這份由 FBI 與美國特勤局（U.S. Secret Services）共同發表的資安通報中指出，截至去（2021）年 11 月止，BlackByte 攻擊至少三個美國關鍵基礎設施，包括政府機關、財政，以及食物暨農產品機關，以及多家外國企業。

報告也指出，BlackByte 勒贖團體是個「勒贖即服務」（Ransomware as a Service, RaaS）平台，專門攻擊各種實體或虛擬的 Windows host 系統。

報告中也提供「駭侵攻擊指標」(Indicators of Compromise），供系統管理者評估，及早發現遭駭跡象，並立即應對防範。這些跡象包括在某些指定目錄內出現的特定資料夾及檔案，這些是 BlackByte 駭入後會新增的檔案與資料夾。

報告內也詳列上述新增檔案的 MD5 雜湊值列表，供系統管理員比對之用。

報告建議所有系統管理者，應對系統實施定期完整的備份措施，包括異地備份、離線並以密碼保護備份檔案，且在原系統更新、修改或受攻擊時亦

應確保備份檔不受影響。

此外，也應確保系統之間的相互隔離，無法直接存取，並定期在所有裝置上安裝並更新必要的防毒防駭軟體與作業系統；也應密集檢查網域、目錄伺服器或各裝置上是否出現不明新帳號。未使用的 RDP 與遠端遙控界面也應全數關閉，並禁止在 Email 中顯示可點按的連結等。

- 資料來源：
  1. Indicators of Compromise Associated with BlackByte Ransomware
  2. CRITICAL INFRASTRUCTURE SECTORS

2.4、社群媒體資安近況

Meta 與金融科技公司 Chime 聯合控告透過 Facebook、Instagram 發動釣魚攻擊的駭客

前身為 Facebook 的 Meta 公司，日前與金融科技業者 Chime 聯合控告兩名奈及利亞籍駭侵者，指控他們在 Facebook 與 Instagram 上假冒 Chime，對用戶進行釣魚攻擊。

兩名遭到控告的駭侵者，涉嫌利用至少 5 個 Facebook 假帳號、800 個以上 Instagram 假帳號，假冒 Chime 公司的人員，試圖騙取用戶的 Chime 帳號控制權。

用戶一旦上當受騙，就會被導向至兩名駭侵詐騙者設立的 Chime 詐騙登入頁面；該頁面會要求用戶輸入 Chime 帳號登入所需的 Email 與密碼，以及電話號碼、社會安全號碼等個資。

用戶如果輸入正確的帳號密碼，其存在 Chime 內的存款，即會遭到兩名駭侵者盜領一空。

在 Meta 與 Chime 聯合控告該兩名駭侵者的起訴書中指出，該兩名嫌犯於 2020 年 3 月至 2021 年 10 月之間，長期以上述的詐騙釣魚手法來進行詐騙攻擊活動；Meta 公司旗下的 Facebook 於 2020 年 6 月 5 日起開始針對該詐騙行動進行防範，包括移除嫌犯使用的 Facebook 與 Instagram 假帳號、在 Facebook 與 Instagram 中阻擋假冒 Chime 公司服務使用的網域，並且對假帳號發送警告信。

但這些手法並沒有辦法遏阻嫌犯繼續利用 Facebook 和 Instagram 設立假帳號繼續進行詐騙攻擊活動，嫌犯在 2021 年 10 月時仍能繼續利用上述服務發動釣魚攻擊。

- 資料來源：
  1. DRAFT 2-7-2022
  2. Meta and Chime sue Nigerians behind Facebook, Instagram phishing

2.5、行動裝置資安訊息

會竊取各種資訊並發動金融詐騙攻擊的 Android 惡意軟體 Medusa 正在大舉感染中

一個名為 Medusa 的 Android 金融特洛伊木馬，目前正在全球各地大幅感染 Android 行動裝置用戶。

一個名為 Medusa 的 Android 金融特洛伊木馬，目前正在全球各地大幅感染 Android 行動裝置用戶；該惡意軟體會竊取用戶手機中的金融服務登入資訊，並用於金融詐騙攻擊，用戶應提高警覺。

Medusa（又稱 TangleBot）木馬並不是最近才發現的新惡意軟體，過去就曾在北美洲與歐洲肆虐；不過資安廠商 ThreatFabric 旗下的資安研究人員，在一份最近推出的研究報告中，詳細描述了新版 Medusa 的運作方式。

研究人員在報告中指出，這次 Medusa 仍然和之前一樣，使用相同的 FluBot 惡意軟體發送平台，來執行其簡訊釣魚攻擊活動。

報告也指出，Medusa 是利用 Android 系統中的「輔助使用」指令引擎來進行各種攻擊活動，包括在手機上執行特定操作或手勢、擅自擷取螢幕畫面、自行開啟通知、鎖定畫面、點按畫面上的元件等。

ThreatFabric 在報告中指出，Medusa 能夠以極高的效率，記錄用戶在手機上的鍵盤輸入、進行影音即時盜錄、也能遠端遙控手機，因此能用以竊取用戶手機中的各種金融服務登入資訊。

Medusa 主要是夾帶在遭到仿冒的熱門應用程式，例如 DHL、Purolator、Android Update、Flash Player、Amazon Locker 與各種影音播放程式等；用戶如果不在官方應用程式商店取得這些軟體，而是自不明來源自行下載安裝 APK 檔，就很容易成為這類惡意軟體的受害者。

- 資料來源：
  1. Partners-in-crime: Medusa and Cabassous attack banks side-by-side
  2. Medusa malware ramps up Android SMS phishing attacks

2.6、軟體系統資安議題

2.6.1、為防範 ASUSTOR NAS 遭 DeadBolt 勒索病毒攻擊，建議用戶立即進行資安防護

因應 DeadBolt 勒索病毒攻擊，ASUSTOR Inc. 目前暫時停止 EZ-Connect 、ASUSTOR EZ Connect、ezconnect.to 服務，並研究勒索病毒的根源與解決方案。

為避免用戶遭 DeadBolt 勒索病毒攻擊而造成損失，建議立即採取以下措施：

- 更改預設 ADM 8000 及 8001 等連接埠，以及 Web 服務 80 及 443 等連接埠。
- 關閉 EZ-Connect 服務。
- 立即進行備份。
- 若不須使用 SSH、SFTP 服務，請將其停用。

為降低用戶遭勒索病毒攻擊的風險，請點此連結參考更詳細的安全措施。

若用戶發現自己的 NAS 遭到 DeadBolt 勒索病毒攻擊，建議先拔除網路線與關機(請按 3 秒電源開關，聽到嗶聲)，並請至 DeadBolt 勒索軟體技術支援處留下資訊，該公司的技術人員會盡快進行聯繫。

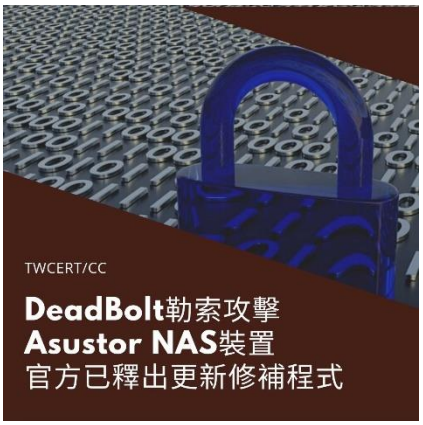
- 資料來源：

1. 立即採取資安防護行動，防範 DeadBolt 勒索病毒

2. 面對 Ransomware 加密勒索與網路攻擊應有的觀念、措施與備份策略

3. DeadBolt 勒索軟體技術支援

2.6.2、DeadBolt 勒索攻擊 Asustor NAS 裝置，官方已釋出更新修補程式



日前傳出 Asustor NAS 裝置遭 DeadBolt 勒索軟體攻擊，Asustor 已於 2 月 24 日下午緊急推出更新，以阻止攻擊。

當裝置遭 DeadBolt 勒索軟體攻擊得逞後，除了所有檔案都會加密，並且加上「.deadbolt」的副檔名外，裝置管理介面的登入畫面，也會被替換成一個警告頁面；在該頁面中，駭侵者會向受害者勒贖比特幣，才能解開所有檔案。

Asustor 官方在支援論壇中指出，該公司目前正在調查整起案件，已暫停 myasustor.com 的 DDNS 服務，同時建議用戶，一旦發現 NAS 裝置可能遭到 DeadBolt 攻擊時，採取下列步驟：

- 拔除乙太網路埠上的網路線。
- 按下電源鍵三秒以上，將 NAS 安全關機。
- 切勿開機，以免資料遭到刪除。
- 填寫服務表單，技術人員會盡快與用戶連絡。

如果用戶的 Ausutor NAS 尚未遭到攻擊，該公司也建議用戶立即採取以下行動，以避免裝置遭駭，造成資料損失：

- 立即變更外部連入使用的埠號，如 8000、8001、80、443。
- 停用 EZ Connect。

- 立即備份所有檔案，並定期進行備份。
- 若不須使用 SSH、SFTP 等服務，請停用。

此外，該公司已經推出最新 ADM 版本供用戶下載，以對應 Deadbolt 攻擊，建議所有用戶立即套用更新至最新版本，有啟用自動更新的用戶會自動作背景更新。

- 資料來源：
  1. ADM 4.0.4.RQO2 (2022-02-24)
  2. Protecting Yourself from Deadbolt
  3. Mitigating Ransomware Risks
  4. DeadBolt ransomware now targets ASUSTOR devices, asks 50 BTC for master key
  5. 立即更新 ADM 至最新版本，保護 ASUSTOR NAS 免於勒索軟體危害
  6. DeadBolt 勒索軟體技術支援

2.6.3、國際紅十字會所屬伺服器自上月起遭駭

國際紅十字會（The International Committee of the Red Cross）日前表示，自上個月起，該組織所屬的伺服器，開始遭到疑似由國家幕後支持的駭侵團體攻擊。

在這次攻擊中，駭侵者不僅成功入侵紅十字會所屬的伺服器，也竊走多種個人機敏資料；被竊的資料包括個人姓名、所在地、連絡方式，受害者則是參與「重建家庭連繫」（Restoring Family Links）計畫的成員，人數多達515,000。

資安專家調查事件後指出，駭侵者係利用一種名為「資安攻擊專用」（Designed for offensive security）的客製化駭侵工具，這種工具通常與「進階持續性資安威脅」（Advanced Persistent Threat, APT）相關。

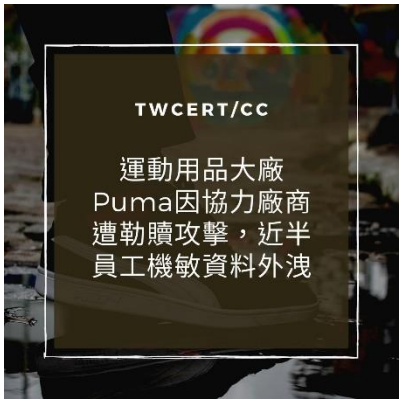
資安專家說，駭侵攻擊發生於去（2021）年 11 月 9 日，直到 70 天後才遭發現；而駭侵者是利用紅十字會伺服器中一個尚未修補的嚴重資安漏洞「Zoho」（CVE-2021-40539）來發動攻擊。該漏洞存於 Zoho 的 ManageEngine ADSelfService Plus 企業用密碼管理系統解決方案中，駭侵者無需通過登入驗證，即可利用此漏洞，遠端執行任意程式碼。

紅十字會也說，駭侵者利用此漏洞滲透後，即可偽裝成合法的系統使用者或管理者，布署各種後續駭侵工具，並且竊取各種資料，甚至包括加密過後的資料在內。

網路設備大廠 Palo Alto Networks 旗下的資安研究人員指出，在過往的駭侵攻擊記錄中，曾經利用 Zoho 漏洞發動駭侵攻擊的 APT 團體是 APT27；而德國國內調查機關也曾發現該團體利用同一漏洞，攻擊德國的商業組織。

- 資料來源：
  1. Cyber-attack on ICRC: What we know
  2. Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite
  3. Red Cross Hack Linked to Iranian Influence Operation?

2.6.4、運動用品大廠 Puma 因協力廠商遭勒贖攻擊，近半員工機敏資料外洩



全球知名運動用品製造大廠 Puma，日前其北美地區的人資行政管理協力廠商 Kronos 遭到勒贖攻擊，造成該公司近半數員工相關資料遭到不當存取。

Puma 在北美地區用於員工與行政管理的雲端服務廠商 Kronos，於去（2021）年 12 月遭到不明來源的勒贖攻擊，造成 Puma 在北美地區近半數的數千名員工資料同時遭到駭侵者不當存取。

Puma 使用的 Kronos 服務，包括 Workforce Central、Workforce TeleStaff、Enterprise Archive、TeleTimeIP、Extensions for Healthcare 與 FMSI 環境等，都託管於 Kronos 的雲端伺服器。

據稍早的報導指出，在 Kronos 於去年底遭攻擊後，使用 Kronos 系統服務的客戶，其行政作業都大大受阻，甚至必須退回到紙本文書作業模式長達數周之久。

據受理 Puma 資安事件的美國緬因州總檢查署指出，在此次事件中個資遭竊的 Puma 員工，人數為 6,632 人；除了員工個人姓名外，遭到外洩的個資還包括員工的社會安全號碼（Social security number）。

Puma 本身尚未針對這起事故提供任何詳細情報，不過 Kronos 在寄發給可能受害員工的信件中表示，正在進行事件調查，該公司也將提供資料外洩員工兩年免費的 Experian IdentityWorks 個資濫用監測服務，以及高達 100 萬美元的個資外洩保險。

- 資料來源：
  1. Data Breach Notifications
  2. Puma hit by data breach after Kronos ransomware attack

2.6.5、英國休閒食品公司 KP Snacks 遭 Conti 勒贖攻擊，且延燒至供應鏈

英國大型休閒食品製造商 KP Snacks 遭 Conti 勒贖軟體攻擊，除了導致該公司產品生產受阻之外，受害災情也延燒到經銷其商品的多家大型超市。

KP Snacks 是英國的相當知名的休閒食品製造廠。這次針對該公司的攻擊行動，首先是在 2022 年 1 月 28 日發動的；當時 KP Snacks 公司旗下的多個 IT 設備發生異常，使得該公司的生產活動受到影響。

在該周周末時，KP Snacks 的 IT 人員會同第三方資安專家，開始針對事件進行調查與處理；當時即確認該公司部分資料已可能遭竊。

進入二月後，勒贖災情繼續擴大到與該公司產品相關的下游供應鍊；據資安媒體掌握的情報指出，KP Snacks 在發送給下游大型通路商 Nisa 超市的信中指出，該公司確認其 IT 系統因遭勒贖攻擊受到影響，因此無法處理該超市發送的訂單；該公司也表示，目前無法預期何時可以恢復正常。

資安廠商 DarkFeed 也掌握到 Conti 駭侵集團發給 KP Snacks 的勒贖信，要求該公司在 5 日之內支付不明數額的贖金，否則 Conti 就會公開竊自 KP Snacks 公司的各種機敏資訊。

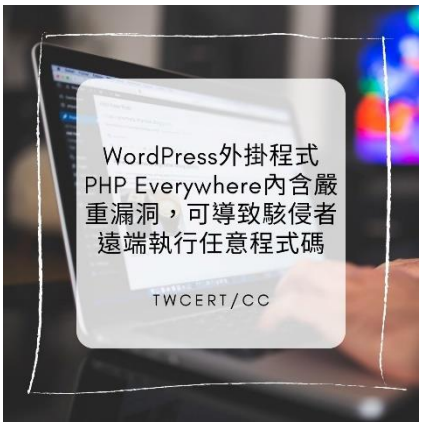
據報導指出，Conti 公布了一部分竊得的資訊，當做該團體手上握有 KP Snacks 機敏資訊的證據；遭到公開的資訊包括信用卡刷卡單、附有員工住址與電話號碼的試算表、各種機密合約和文件等。

資安專家表示，Conti 勒贖團體近期的活動日益猖獗，近來的受害者包括印尼中央銀行、愛爾蘭衛生部、大型行銷公司 RR Donnelly 等，各廠商應加強資安防護能力並提高警覺。

- 資料來源：
  1. KP Snacks supply chain shut down by Conti ransomware attack
  2. DarkFeed @ido_cohen2
  3. KP Snacks giant hit by Conti ransomware, deliveries disrupted

2.7、軟硬體漏洞資訊

2.7.1、WordPress 外掛程式 PHP Everywhere 含漏洞，可導致駭客遠端執行任意程式碼



資安廠商 Wordfence 旗下的研究人員，日前發現一個在 WordPress 中廣為使用的外掛程式 PHP Everywhere，內含三個嚴重漏洞，可導致駭侵者遠端執行任意程式碼。

PHP Everywhere 是一個相當實用的 WordPress 外掛程式，可以在網站的部落格文章與頁面的內文、邊欄、區塊編輯器中的任何區塊中插入 PHP 程式碼，以便動態顯示所需的內容。

這三個被發現的漏洞都是遠端執行任意程式碼漏洞，分述如下：

- CVE-2022-24663：這個漏洞可讓任何 WordPress 的訂閱者，只要發送一段含有「shortcode」參數的連線要求給 PHP Everywhere，即可遠端執行任意 php 程式碼。
- CVE-2022-24664：這個漏洞可讓 WordPress 網站擁有作者（contributor）權限的用戶，在新增的文章中插入 PHP 程式碼方塊並且預覽，以執行該程式碼。
- CVE-2020-24665：這個漏洞可讓 WordPress 網站擁有作者（contributor）且具有編輯文章權限的用戶，利用區塊編輯器新增 PHP Everywhere 的區塊；該權限應設為僅有系統管理者可使用此功能，但並未如此設定。

這三個漏洞的危險程度評級都是最高的「嚴重」等級，CVSS 危險程度得分均高達 9.9 分（滿分為 10 分），所有 WordPress 版本，只要安裝了 PHP Everywhere 2.0.3 及先前版本，均受這三個漏洞影響。

由於此三個漏洞的嚴重性極高，所有使用該外掛程式的 WordPress 網站管理員，均需立即升級 PHP Everywhere 至最新版本（目前為 3.0.0），以免網站曝險。

- CVE 編號：CVE-2022-24663、CVE-2022-24664、CVE-2022-24665
- 影響產品：安裝有 PHP Everywhere 2.0.3 及先前版本的所有 WordPress 各版本。
- 解決方案：升級 PHP Everywhere 至 3.0.0。

- 資料來源：
  1. Critical Vulnerabilities in PHP Everywhere Allow Remote Code Execution
  2. PHP Everywhere

2.7.2、WordPress 強制更新 UpdraftPlus 外掛程式的嚴重資安漏洞

WordPress 日前強制針對裝有 UpdraftPlus 外掛程式的網站進行強制更新，以修補一個嚴重漏洞 CVE-2022-0633，受影響網站超過 300 萬個。

這個漏洞讓網站內容訂閱戶，可以輕易下載網站最新的備份檔案，而在備份檔案中往往會包括許多可資辨識身分的個人資料。

UpdraftPlus 是個可以簡化網站備份與還原流程的 WordPress 外掛程式，可以進行排程備份，也可以將備份檔案自動寄到可信賴的 Email 信箱中。

不過，該漏洞讓任何執行權限的登入用戶，都能利用特製的連結來下載網站的備份檔，藉以竊取網站資料庫中的任何機敏資訊。

這個漏洞由於操作並不困難，因此依 CVSS 危險程度分級列為「高度危險」（high）等級，其危險程度評為為 8.5 分（滿分為 10 分）。

該漏洞是 WordPress 開發廠商 Automattic 旗下的資安研究人員於本（2022）年 2 月 14 日所發現的，並且立即通報給外掛程式開發廠商；開發者很快就完成漏洞修補，WordPress 於 2022 年 2 月 16 日開始強制裝有此外掛程式的三百多萬個 WordPress 網站升級；這在 WordPress 來說是相當罕見的。

UpdraftPlus 存有此漏洞的版本，自 1.16.7 至 1.22.2；開發者推出 1.22.3 與 2.22.3（付費專業版），以修復此漏洞。

UpdraftPlus 開發者在幾天後，又再度推出新版，強化漏洞修補，目前最新版本為 1.22.4；建議所有 UpdraftPlus 用戶，儘速更新到此最新版本。

- CVE 編號：CVE-2022-0633
- 影響產品：1.16.7 至 1.22.2。
- 解決方案：升級至 1.22.3（付費版為 2.22.3）與後續版本。

- 資料來源：
  1. UpdraftPlus security release – 1.22.3 / 2.22.3 – please upgrade
  2. WordPress force installs UpdraftPlus patch on 3 million sites

2.7.3、Microsoft 推出 2022 年 2 月 Patch Tuesday 資安修補包

Microsoft 近日推出 2022 年 2 月 Patch Tuesday 資安修補包，一共修補 48 個資安漏洞；各種 Microsoft 產品用戶，應立即套用更新。

本次的資安修補包修復的 48 個資安漏洞之中，並無列為「嚴重」等級的漏洞；各漏洞的類型如下：

- 16 個執行權限提升漏洞；
- 3 個資安防護功能跳過漏洞；
- 16 個遠端執行任意程式碼漏洞；
- 5 個資訊洩露漏洞；
- 5 個服務阻斷漏洞；
- 3 個詐騙假冒漏洞。

在這 48 個漏洞之中，有一個值得注意的 0-day 漏洞。該漏洞為 CVE-2022-21989，存於 Windows Kernel 之中，駭侵者可藉以提升自身的執行權限。

雖然這個 0-day 漏洞尚未傳出遭大規模用於駭侵攻擊的情報，不過資安專家表示，目前已有根據這個漏洞發展出的駭侵攻擊概念證實程式（Proof of concept），因此可以預見將會有透過此漏洞發展出的駭侵攻擊活動，用戶不

可掉以輕心。

除了上述 Patch Tuesday 的資安修補之外，Microsoft 也同時針對 Microsoft Edge 瀏覽器推出多達 22 個 Chromium 漏洞的修補更新。

由於微軟產品廣為使用，用戶或系統管理者應立即套用最新推出的資安更新，以免系統中存有的老舊未修補漏洞，給予駭侵者可趁之機。

另外，除了 Microsoft 之外，近日也有多家資訊產品大廠推出 2022 年 2 月資安修補包，包括 Android 的漏洞更新，以及 Cisco、SAP 的資安修補工具等。如有使用這些產品的用戶與系統管理員，均應立即套用更新。。

- CVE 編號：CVE-2022-21989 等多個
- 影響產品：微軟各產品，包括 Windows 各版本、Office 各版本、Microsoft Edge 等。
- 解決方案：套用最新更新軟體。

- 資料來源：

1. 2022 年 2 月 8 日 —KB5010358 (OS Build 10240.19204)
2. Security Update Guide
3. Microsoft February 2022 Patch Tuesday fixes 48 flaws, 1 zero-day

2.7.4、Google 修復 Android 系統遠端權限提升漏洞

Google 日前釋出 2022 年 2 月 Android 資安修補程式，修復多個漏洞，其中包括一個可讓駭侵者遠端提升執行權限，且危險程度為最高等級「嚴重」(Critical）的漏洞。

這個嚴重漏洞的 CVE 編號為 CVE-2021-39675，僅存於最新版本的 Android 12 中，可以在用戶不知情的情形下，遠端提升惡意軟體的執行權限。

這類漏洞通常會被用於手法純熟的惡意軟體發行者，不過 Google 表示並未見到該漏洞遭到大規模濫用於攻擊活動的跡象。

在這波漏洞修補中，還有另一個嚴重漏洞 CVE-2021-30317 也得到修補；該漏洞主要影響 Qualcomm 的封閉原始碼組件，也僅有使用 Qualcomm 零組件的 Android 裝置會受到影響。

另外，這次 Google 釋出的軟體修補包中，除了上述 2 個「嚴重」等級的漏洞之外，另外還有三十餘個屬於「高度」危險等級的漏洞，分別存於 Android system framework、media framework、系統組件、媒體播放系統，以及協力廠商 Amlogic、MTK、紫光、Qualcomm 等相關組件。

值得注意的是，由於市面上的 Android 裝置，其作業系統與資安更新，多半是由裝置製造商提供，無法直接套用 Google 推出的 Android 資安更新包（Google 自行推出的 Pixel 系列與少數第三方機種除外）；因此用戶應密切注意裝置製造廠的更新情報，在對應的更新推出後立即套用。如果因裝置老

舊，製造商已不提供更新服務的話，應淘汰老舊設備。

- CVE 編號：CVE-2021-39675
- 影響產品：Android 10、11、12。
- 解決方案：密切注意裝置製造商的更新提供。

- 資料來源：

1. 2022 年 2 月 8 日 —KB5010358 (OS Build 10240.19204)
2. Security Update Guide
3. Microsoft February 2022 Patch Tuesday fixes 48 flaws, 1 zero-day

2.7.5、Apple 修復已遭駭侵者濫用的 0-day 漏洞

Apple 日前釋出新版 iOS、iPadOS、macOS，修復一個可能已遭駭侵者廣為利用的 0-day 漏洞 CVE-2022-22620，用戶應立即更新各裝置作業系統至最新版本。

這個漏洞存於上述各種作業系統的內建瀏覽器核心 WebKit 內，屬於使用已釋放之記憶體的資安漏洞；駭侵者可利用特製的網頁內容誘發此漏洞，造成作業系統崩潰，並且在受害裝置上遠端執行任意程式碼。

Apple 在產品更新說明中也指出，該公司已接獲此漏洞可能已遭駭侵者大規模濫用於駭侵攻擊的報告。

受此漏洞影響的 Apple 產品如下：

- iPhone 6s 與後續各型機種；
- iPad Pro 全機種；
- iPad Air 2 與後續各型機種；
- iPad 第 5 代與後續各型機種；
- iPad mini 第 4 代與後續各型機種；
- iPod Touch 第 7 代；
- 執行 macOS Monterey 的 Mac 電腦全機種。

Apple 表示，在新推出的 iOS 15.3.1、iPad OS 15.3.1 與 macOS Monterey 12.2.1 中，針對記憶體管理機制進行改善，從而修復此一漏洞。

資安專家指出，雖然目前接獲的情資顯示，此漏洞僅遭駭侵者使用於目標定向駭侵攻擊，尚未出現目標較廣泛的資安攻擊行動，但仍建議擁有上述裝置的用戶，應立即透過系統更新功能，將裝置上的 iOS、iPadOS、macOS 更新至最新版本，以避免潛在的資安攻擊風險。

- CVE 編號：CVE-2022-22620
- 影響產品：iPhone 6s 與後續各型機種、iPad Pro 全機種、iPad Air 2 與後續各型機種、iPad 第 5 代與後續各型機種、iPad mini 第 4 代與後續各型機種、iPod Touch 第 7 代、執行 macOS Monterey 的 Mac 電腦全機種。
- 解決方案：升級至 iOS 15.3.1、iPad OS 15.3.1 與 macOS Monterey 12.2.1 或後續版本。

- 資料來源：
  1. About the security content of iOS 15.3.1 and iPadOS 15.3.1
  2. About the security content of macOS Monterey 12.2.1
  3. Apple Says WebKit Zero-Day Hitting iOS, macOS Devices

2.7.6、新版 Google Chrome 緊急修復一個已遭濫用於攻擊的 0-day 漏洞

Google 日前緊急推出 Google Chrome 瀏覽器最新版本 98.0.4758.102，修復一個已經遭到外部駭侵者廣泛濫用以發動攻擊的 0-day 漏洞 CVE-2022-6069。

這次推出的新版 Google Chrome，包括 Windows、Mac 與 Linux 全作業系統版本，使用舊版 Google Chrome 的用戶，應立即透過 Chrome 內建的更新機制，儘速更新至最新版本。

在 Google 發表的資安通報中，並未詳細說明該 0-day 漏洞的運作方式與細節，僅說明該漏洞為一種「釋放後使用」（use after free）型漏洞。

該漏發生於 Google Chrome 的動畫（Amination）組件中，其 CVSS 危險程度評分為 6.0 分（滿分為 10 分），危險程度分級為「高」（high）等級。

據 vuldb.com 網站指出，駭侵者可以利用未知的輸入，誘發此漏洞並產生記憶體崩潰；該網站也估計使用此漏洞進行駭侵攻擊的價碼，約在 5,000 美元到 25,000 美元之間。

據資安專家指出，這類「釋放後使用」的漏洞，多半是用來未曾更新的 Chrome 瀏覽器上執行任意程式碼，或是讓惡意程式碼有機會突破沙箱（Sandbox）的封鎖，以取用外部資源，或攻擊外部的組件。

這個漏洞是 Google 在今（2022）年首次修復的 0-day 漏洞，然而在 2011 年 Google Chrome 一共修復多達 16 個 0-day 漏洞，其中許多都遭駭侵者大規

模用於攻擊。

由於未修補的舊版 Chrome 很容易成為駭侵者的攻擊目標，建議所有 Google Chrome 用戶，一定要勤於更新，才能避免成為受駭者。

- CVE 編號：CVE-2022-0609
- 影響產品：Google Chrome 98.0.04758.102 之前各作業系統版本，包括 Windows、Mac、Linux。
- 解決方案：升級至 Google Chrome 98.0.04758.102 與所有後續版本。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. GOOGLE CHROME PRIOR 98.0.4758.102 ANIMATION USE AFTER FREE

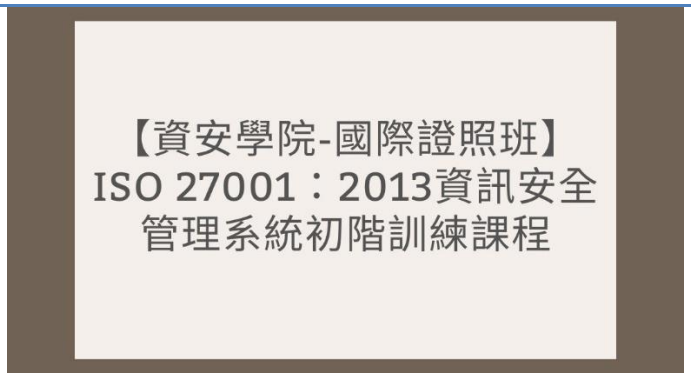
第 3 章、 資安研討會及活動

2022 OT 工控資安年會	
活動時間	**2022 年 3 月 24 日 09:00~17:00**
活動地點	**臺北文創 (台北市菸廠路 88 號 6 樓)**
活動網站	**https://cs.ezmail.com.tw/news/read/id/sy621df5c1680c7**
活動概要	 **主辦單位：資安人媒體** **IT/OT 疆界逐漸模糊，OT 資安隨 IoT、5G、邊緣發展更為吃重** 這兩年許多台灣許多重要的製造商遭受攻擊, 每次的損失都不容小覷, 不只在財務上受到損失, 客戶資料被竊取, 重要的是商譽也會受到嚴重的質疑。資安人也觀察到，公領域推動智慧城市概念、 私領域因為疫情的關係加速數位轉型建置, 許多的應用環境加入了聯網設備，如工業物聯網、車聯網、醫聯網...等。這些場域 IT 與 OT 的界定日漸混淆, 也多了許多網路犯罪的攻擊破口。 IoT、5G、邊緣、雲端運算的技術勢必將會更普遍, 台灣又是全球晶片與資通訊產業的製造基地。以目前 OT 場域與 IT 技術勢必融合的趨勢下，企業組織單位應儘早意識到風險，並且轉變過去「OT 即內網所以安全」的防禦思維，佈署適當的資安管理與控制，才能確保 OT 的數位轉型，安全無虞。

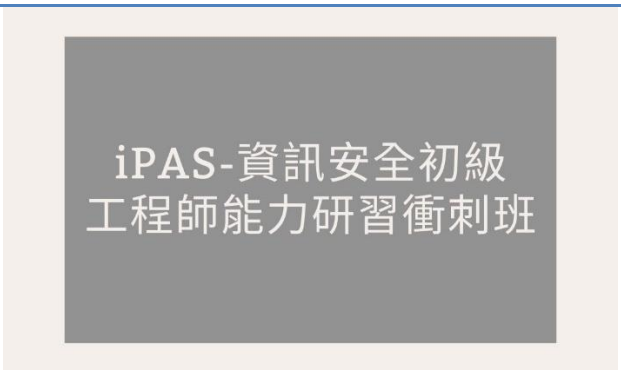
	【2022 OT 資安年會】以「跨越 OT/IT 疆界，提升資安防禦力」為主題，從基礎的網路架構到 ICS 系統, 藉由多面向的主題探討與方案展示, 讓用戶理解最新的技術方案，找到落地作法，達到最有效益的防護投資。

AWS 雲世代資安長戰略峰會	
活動時間	**2022 年 3 月 29 日 (二) 9:00 AM 至 4:00 PM (8:30 AM 開放入場)**
活動地點	**台北 W Hotel 風尚廳 (台北市信義區忠孝東路五段 10 號 8F)**
活動網站	**https://reurl.cc/44Vjd3**
活動概要	 **主辦單位：AWS** 資安議題變得日益重要，去年底（2021）金管會正式發佈施行新版「公開發行公司建立內控制度處理準則」，規定凡是資本額破 100 億元、或名列市值前 50 大的上市櫃公司，不論處於哪個產業類別皆無例外，皆須設置資安長及資安專責單位。當然，這絕對是「資安長」（CISO）擴及到各個產業領域的重要起點，新世代資安長的再定義時候到了。 然而有資安長，不代表這家企業就能做好資安。如何正確地設置資安長，給予足夠的支持與授權，以及資安長如何權衡資源投入與風險控制，幫助企業在安全無虞前提下擁抱數位創新等議題，相信是此刻多數企業十分關切的重要題目。再者，資安準則雖由資安長制定，但要確切落實則需要每位同仁相互配合。資安防護觀念及工具皆需要滾動式調整，才能與時俱進並達到最強地企業資安防護。 為此，AWS 台灣團隊將於 2022 年 3 月 29 日（二）舉行《AWS 雲世代資安長戰略峰會》，預計邀請國際重量級資安解決方案專家、企業風險諮詢顧問服務等資安夥伴與相關單位一起舉辦這場盛會，針對「資安長應具備哪些能力」、「資安長與資訊長的權責劃分」，乃至

	「資安長如何兼顧創新與安全 」等等重大議題進行深入探討。 *活動會視台灣疫情狀況調整舉辦方式。

【資安學院-國際證照班】ISO 27001：2013 資訊安全管理系統初階訓練課程	
活動時間	**4/14（四）~4/15（五）**
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/Course/Detail/2741**
活動概要	 **主辦單位：中華民國資訊軟體協會** 課程說明：資訊（Information）可說是現今最為重要的無形資產，也是企業成功的基礎與命脈。如何確保客戶與公司內部資訊的安全性、完整性及可用性是當今最熱門的課題之一。資訊安全管理系統正是因應維護資訊安全而發展出來的重要標準，在十倍速的資訊時代，您更不能忽略它存在的重要性。本課程可進一步了解 ISO 27001 資訊安全管理系統條文，以精準解讀資訊安全管理系統標準的要求。 課程大綱： ➢ 資訊安全管理系統詮釋 ➢ 管理責任詮釋 ➢ 內部資訊安全稽核詮釋 ➢ 資訊安全管理審核詮釋 ➢ 資訊安全管理系統改善詮釋 ➢ 資訊安全控制措施詮釋 課程對象：資訊安全人員、欲從事 ISO 27001 顧問人員、公司內部導入 ISMS 系統的人員、IT 人員、稽核部門人事。

	活動聯絡人：廖資深專員 Email: maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 講師：SGS 合格之講師授課 學員可藉由此門課瞭解 ISO 27001 資訊安全管理系統之架構，及對條文有進一步之認識。本課程將於結束後，將由 SGS 授與「上課證明」

iPAS-資訊安全初級工程師能力研習衝刺班	
活動時間	**4/23（六）、4/30（六）兩日共計 12 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/Course/Detail/2751**
活動概要	 **主辦單位：中華民國資訊軟體協會** 課程說明：本課程設計將使學員瞭解資訊安全管理與技術專有名詞及其代表意義，並具備資訊安全管理基礎知識，如資產與風險管理、存取控制、身分認證、事故管理、營運持續、法規遵循與資訊倫理等。另亦統整資訊安全技術之基礎知識，如網路安全、通訊安全、作業系統安全、應用程式安全、資安維運技術與新興科技資安管理等。透過講師授課，將協助學員掌握 iPAS 考題方向及技術解析，讓應考更佳輕鬆！ 課程大綱： -資訊安全管理概論 1.資訊安全管理概念 2.資產與風險管理 3.存取控制、加解密與金鑰管理 4.事故管理與營運持運 5.法規遵循與資訊倫理

-資訊安全技術概論

1.重要資安概念與理論

2.網路與通訊安全

3.作業系統與應用程式安全

4.資安維運技術

5.新興科技安全

6.複習與試題演練

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。

以上人員需具備 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、內容資訊，主辦單位保留最終變更及調整之權利。

如欲參加考試，需自行上網報名；111 年第一次初級資訊安全工程師能力鑑定考試資訊：

考試日期：2022/05/28 ~ 2022/05/28、報名日期：2022/01/15 ~ 2022/04/18

詳細報名資訊，請參考 iPAS 官網

第 4 章、 2022 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。

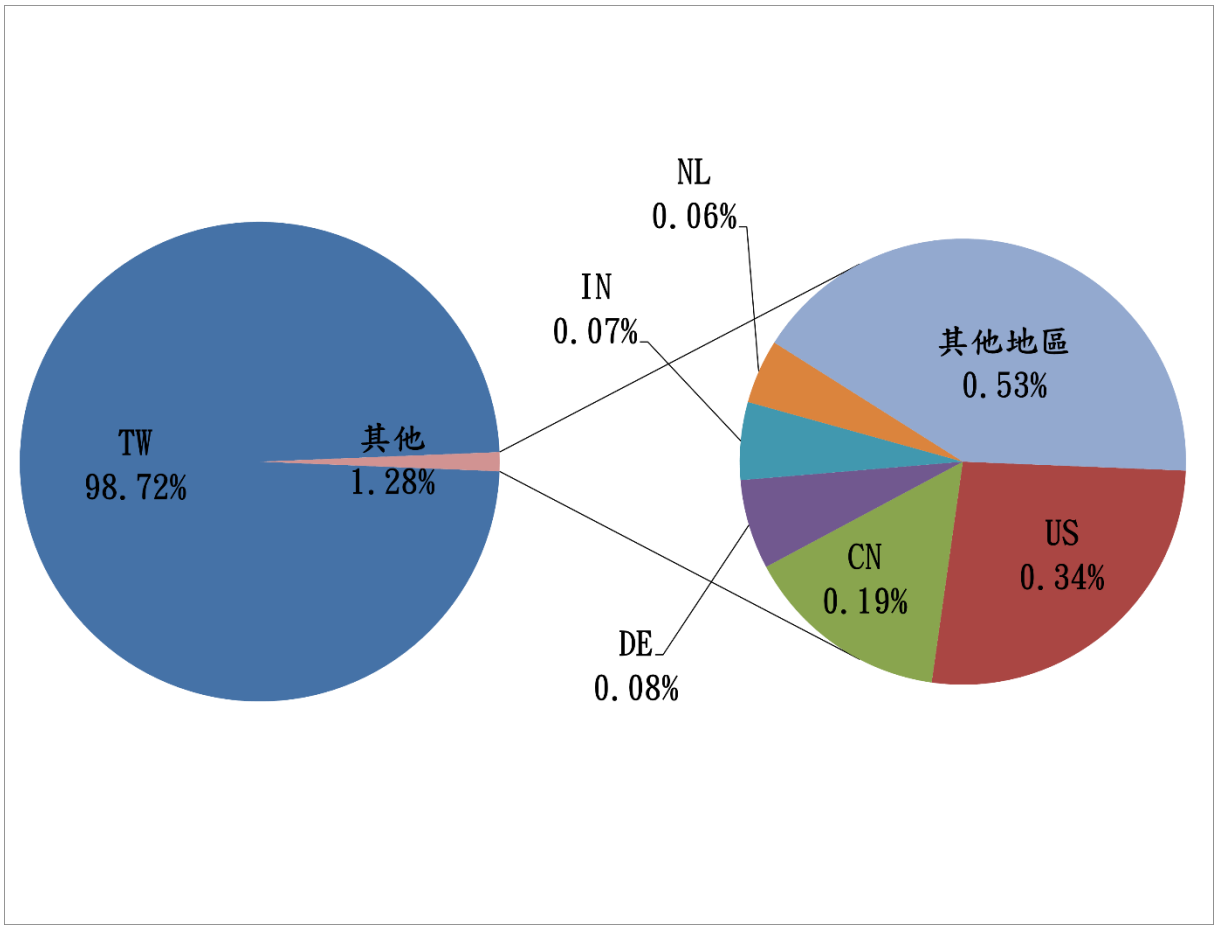


圖 1、分享地區統計圖

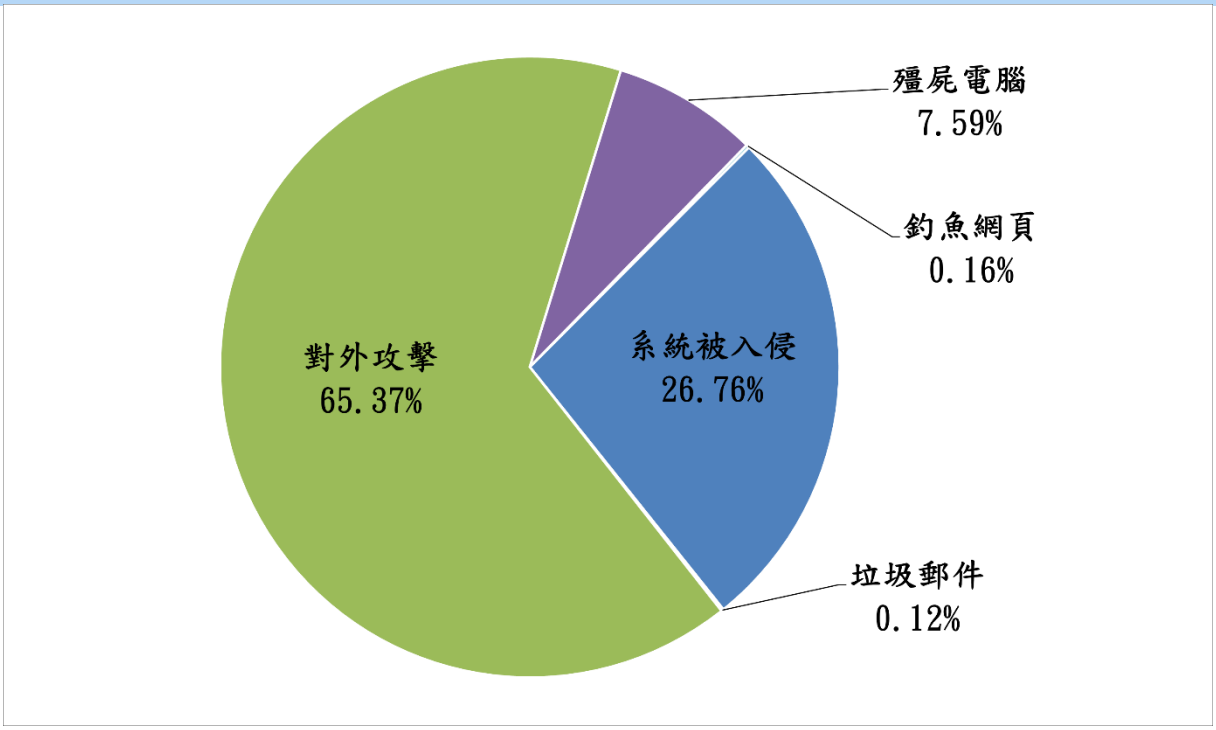


圖 2、分享類型統計圖

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：**2022 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**