# TWCERT/CC 資安情資電子報

## 2022 年 10 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 6 章節：

第 1 章、封面故事：主題式資訊安全專題分享。

第 2 章、資安活動紀事：TWCERT/CC 主辦或參與之資安活動及訓練課程等。

第 3 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 4 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 5 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 6 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 ..... 1
節日性與假期性網路釣魚分析 ..... 1
第 2 章、 資安活動紀事 ..... 13
資安防護及案例分享研討會-雲林場 ..... 13
第 3 章、 國內外重要資安事件 ..... 16
3.1、 資安趨勢 ..... 16
3.1.1、 資安專家發現駭侵者利用「影子網域」發動攻擊的案例數量大增 ..... 16
3.1.2、 統計指出，超過 80% 大型網站將用戶搜尋資訊透露給廣告業者 ..... 18
3.1.3、 調查指出，2022 年第一季全球 34% 登入動作為憑證填充攻擊所為 ..... 20
3.1.4、 調查指出高達 68% 製造業未能完全掌握其工業製造系統內外存取情形 22
3.2、 新興應用資安 ..... 24
3.2.1、 多家加密貨幣交易所採用的 npm 軟體套件遭植入惡意程式碼 ..... 24
3.2.2、 荷蘭警方逮捕竊取加密貨幣並且洗錢的犯罪分子 ..... 26
3.2.3、 Lazarus 駭侵團體藉由詐騙 Crypto.com 工作機會，對加密貨幣開發者植入 macOS 惡意軟體 ..... 28
3.2.4、 駭侵者自加密貨幣交易公司 Wintermute 竊走 1.62 億美元等值數位資產 ..... 30
3.3、 國際政府組織資安資訊 ..... 32
3.3.1、 美國資安主管機關下令各單位立即修補已遭用於攻擊之漏洞 ..... 32
3.3.2、 英國警方逮捕涉嫌駭入 Uber、Rockstar 等公司的 17 歲駭侵者 ..... 34
3.4、 社群媒體資安近況 ..... 36
3.4.1、 資安專家發現駭侵者新手法，透過 Microsoft Teams 的 GIF 進行釣魚等多種攻擊 ..... 36
3.4.2、 LinkedIn 的智慧連結，遭濫用於釣魚郵件攻擊 ..... 38
3.5、 行動裝置資安訊息 ..... 40
Google Play 與 App Store 中發現多支廣告軟體，下載安裝次數高達 1,300 萬次 40
3.6、 軟體系統資安議題 ..... 42
3.6.1、 資安廠商發現利用時間相關性取得網域名稱的攻擊方法 ..... 42

3.6.2、 駭侵者自製 SideWalk Linux 版本變種後門惡意軟體，以攻擊學術單位 44
3.6.3、 Uber 疑遭駭侵者透過社交工程攻擊，入侵內部系統 ..... 46
3.6.4、 資安廠商發現針對以色列工業生產控制系統的大規模駭侵活動 ..... 48
3.6.5、 駭侵者透過 YouTube 遊戲破解教學影片散布惡意軟體 ..... 50
3.7、 軟硬體漏洞資訊 ..... 52
3.7.1、 資安專家利用分析工具，發現 Node.js 程式庫內超過 100 個 0-day 漏洞 52
3.7.2、 Apple 推出 iOS、macOS 更新，修復一個已遭駭侵者大規模濫用的 0-day 漏洞 ..... 54
3.7.3、 Microsoft 推出 2022 年 9 月 Patch Tuesday 更新修補包，共修復 63 個漏洞 ..... 56
第 4 章、 資安研討會及活動 ..... 58
第 5 章、 TVN 漏洞公告 ..... 67
第 6 章、 2022 年 9 月份資安情資分享概況 ..... 70

# 第 1 章、 封面故事

## 節日性與假期性網路釣魚分析


- 節日性與假期性之網路釣魚，主要是利用人性的弱點，尤其在假期和節日時分，許多使用者除了會因為放假而鬆懈警戒外，也會因為節日的氛圍，提高了民眾線上購買商品的慾望，而導致大量的網路釣魚趁機攻擊且成功機率更高。
- 尤其隨著網路購物的新興發展，除了過往傳統節日外，越來越多網路購物節的促銷活動紛紛推出，導致在相關時節時，針對線上購物的網路釣魚攻擊大量增加，導致節日性網路釣魚受害者數量隨之驟升。
- 關於節日性與假期性的網路釣魚攻擊，其類型大致分為假冒的銷售與廣告、假冒的網路購物驗證訊息、假冒的訂單商品物流資訊，以及假冒的善心捐款求助等，讓使用者在假日或節日進行購物、瀏覽網頁或社群媒體時，往往一不小心就因此上當受騙。
- 因此，使用網路時為避免不慎受騙上當而遭受損失，應針對節日性與假期性網路釣魚進行基本防護，例如注意自身信用卡或金融卡是否遺失或遭盜刷、養成保留購物證明習慣、經常檢查賬戶交易情形及核對帳單內容等，透過這些基本的節日性與假期性網路釣魚防護，讓減少使用者在節慶期間受騙上當之機率。

一、簡介

節日性與假期性的網路釣魚，主要是利用使用者在假日放鬆或專注於節日的活動時，對釣魚郵件等資訊疏於警戒的心理，例如假日時收到旅遊類型的釣魚資訊，或在情人節時收到折扣極高的禮品等釣魚資訊，甚至利用物流釣魚資訊誘騙假日在家中休息的使用者上鉤。尤其近年隨著 COVID-19 疫情的爆發，導致越來越多人不論是購買假日的食物與日用品，或是送給他人的節日禮物，都會透過網際網路瀏覽及購買。根據台灣網路資訊中心(Taiwan Network Information Center, TWNIC)的統計報告，在國內，2020 年有 59.6%的使用者會透過網路進行購物，平均消費金額為新台幣 3,217 元，較 2019 年增加 556 元。而在這些網路購物過程中的假期與節日促銷廣告、物流通知、匯款通知等資訊，都可以成為攻擊者進行網路釣魚的最佳利器之一。

舉例來說，在 2020 年的雙十一節慶，因網路購物的成熟以及 COVID-19 等因素，造成創辦集團前所未有的高額營收，總共達到 740 億美元，為 2019 年的近兩倍營收。而國外較為熟知的黑色星期五(Black Friday)和網路星期一(Cyber Monday)，也分別創造了 90 億美元和 108 億美元的收益，都比去年成長了 21.6%和 15.1%。然而，許多攻擊者便利用使用者大量網路購物的形勢，進行與之相關的網路釣魚攻擊。由於這些節日都位於 10 月底至 11 月，因此，該月所搜集的網路釣魚攻擊數量急速增加。根據歐洲知名資安新聞網站 Help Net Security 的報導，在近三年期間，全年所有網路購物的數量中，疑似為網路釣魚的數量佔比，以及僅限於每年度從感恩節、黑色星期五，到網路星期一的購物季節期間所有的網路購物數量中，疑似為網路釣魚的數量佔比，如圖 1。

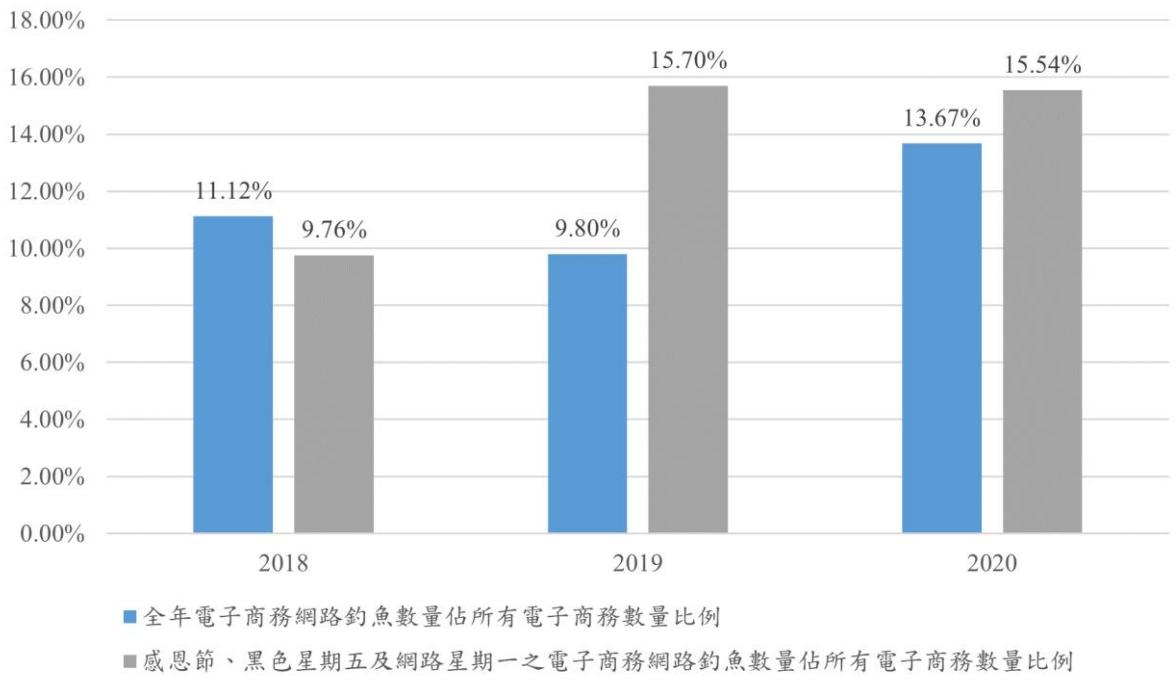



圖 1、2018 年至 2020 年之全年與購物季節網路釣魚比例統計。

從圖 1 中可以見得，從 2018 年到 2019 年期間，雖然全年的網路釣魚比例有所下降，但針對購物季節期間的網路釣魚比例，卻明顯快速增加了 5.94%，顯示攻擊者開始將無目標且大量發送的網路釣魚攻擊，開始轉而著重於假日及節日使用者大量進行網路購物的時節進行攻擊。而在 2020 年，全年的網物購物之網路釣魚比例快速上升，而整個購物季節雖有小幅度的下降，但仍維持著相當高之比例，甚至在購物季節期間，有 37%的網路購物消費者表示疑似遭到與 COVID-19 方面的網路釣魚攻擊，顯示著仍有諸多攻擊者將特殊購物時節作為目標，進行相關的網路釣魚攻擊。

除了網路購物之外，許多傳統節日也成為攻擊者的最佳目標之一，例如許多攻擊者會利用情人節送禮給另一半的習慣，進行販售花卉、酒、珠寶等禮品，以及假冒情人的網路釣魚攻擊，誘騙使用者上當後，竊取其個資和金融資訊。根據美國 FBI 的網路犯罪投訴中心統計，在 2019 年，因為類似的浪漫騙局而受騙的受害者，其損失總金額高達 4.75 億美元。並且除了常見的節慶假日外，像是報稅季節，也是許多攻擊者喜愛的目標，尤其在網際網路越發方便的現在，網路報稅的功能及便利性增加，許多攻擊者便偽冒政府機

關，以退稅理由進行網路釣魚，誘導使用者提供個資，或是告知使用者欠繳稅金，要求必須透過預付卡、禮品卡或電匯等方式補繳，否則威脅將可能遭到逮補。

在假期或節日中，大量的網路釣魚攻擊發生，使用者因假日放鬆一時不察容易上當，因而此期間網路釣魚的成功率提升許多。一般而言，網路釣魚的類型大致如下：

1. 假冒之銷售與廣告：隨著網路購物可減少時間花費，且可瀏覽大量各類的物品，網路購物已經成為隨處可見的購物方式，眾多商家為提升自身的熱度及能見度，除了會販售各式各樣的商品外，更會透過如社群媒體、網頁置入或寄送電子郵件等方式投放廣告。然而，攻擊者便會利用相關各式各樣的商品，針對各個節日、假日，假冒商家販售與之相對應的商品，並到處投放相關廣告，甚至經常假藉名義提供大量的優惠，讓使用者被其優惠吸引，一時不察而上當。

2. 假冒之網路購物驗證訊息：在進行網路購物時，許多使用者為提升便利性，往往會透過信用卡進行款項支付，減省需前往特定場所或與物流人員進行款項支付確認等耗時費力的實體程序。然而，攻擊者便可利用此模式，告知使用者其必須點擊惡意連結方能針對其信用卡的支付進行確認，而使用者往往便不疑有他，點擊惡意連結後，提供相關資訊，讓攻擊者得以取得使用者的相關金融資訊，並進行後續惡意行為。

3. 假冒之訂單商品物流資訊：隨著網路購物的興起，使用者放假不需出家門，即可線上購買所需物品，因此攻擊者便利用網路購物透過物流公司寄送之模式，寄送偽冒物流資訊，讓使用者收到後點擊惡意連結，甚至進入偽冒的電商或物流頁面，進而竊取使用者個資隱私資料。

4. 假冒之善心捐款求助：在大眾歡愉的節慶時節，許多攻擊者利用大眾的善心，偽冒弱勢族群或災難受災戶等，要求使用者提供相關資金以度過佳節，而動了惻隱之心的使用者便會點擊惡意連結，或是提供金融資訊，以便將資金匯給攻擊者，導致相關資訊外洩。

由上可知，在假日或節慶時節，使用者往往會因放鬆而降低戒心或一時難以應付突發狀況，甚至受到時節相關商品的促銷吸引，導致受騙上當而得不償失。因此，不論是何種時節，使用者都應針對可疑的、不確定的資訊保持戒心，則可避免輕易受騙上當。

二、節日性與假期性網路釣魚案例

隨著網路購物的普及性及便利性的增加，除了使用者的大量增加外，網路釣魚的數量同樣也與日俱增；此外，網路釣魚的模式逐漸從一開始的大量、無目標的攻擊，逐漸轉變成目標性鎖定，在分析使用者的行為模式之後，以最佳成功率方式進行網路釣魚攻擊。而網路購物往往是在假日或節慶時被使用的最為頻繁，自然成為攻擊者的一大目標。

## (一)假期性網路釣魚案例

在現代人難得悠閒的放假時節，許多人為減少實地購物所花費的時間和精力，往往選擇透過網路購物去購置必需品及相關產品。然而，卻有許多攻擊者利用此習慣，在假日使用者往往放鬆戒心時，透過節日相關或日常必須的相關商品，加上誇張的便利性及優惠，誘騙使用者上當後，成功竊取其個資。針對假日的網路釣魚攻擊逐漸增加的同時，國內也發生不少相關案例，茲統整列表如下。

表 1、假期性網路釣魚案例統整表

| 網路釣魚類型 | 網路釣魚主題 | 網路釣魚媒介 | 網路釣魚手法 | 網路釣魚受害情形 |
|---|---|---|---|---|
| 假冒之銷售與廣告 | Facebook貼文提供電影優惠 | Facebook與Line等社群媒體 | 貼文留言後，要求加入Line群組後竊取Line個資 | Line個資外洩，並被販賣給廣告商 |
| 假冒之網路購物驗證訊息 | 旅遊優惠信用卡登入提醒信 | 釣魚郵件與仿冒信用卡之釣魚網站 | 假意提醒信用卡被登入，並要求使用者登入後提供個資 | 於釣魚網站中提供的個資和信用卡資訊外洩 |
| 假冒之訂單商品物流資訊 | 告知包裹遭退貨，需點擊連結後查看資訊 | 手機簡訊與仿冒物流公司之釣魚網站 | 告知包裹被退回，導致使用者點擊連結進入釣魚網站後下載惡意apk檔案 | 行動裝置的控制權、個資遭竊，以及發送釣魚簡訊的電信費用損失 |
| 假冒之善心捐款求助 | 假冒知名餐飲集團，轉發貼文即捐助對應費用給受災戶 | Line等社群媒體 | 偽冒知名餐飲集團，告知使用者轉發Line文章，便會捐助費用給水患受災戶，卻是搜集轉發者個資 | Line個資外洩，並被販賣給廣告商 |

在假日時節，是許多人難得進行長時間網路活動的時間，也是大眾放鬆身心的日子。然而，攻擊者卻利用許多人假日放鬆警戒的機會，假冒成他人，騙取使用者的個資、金融資訊，甚至個人財務，使得使用者一時的不察或善意遭到利用，反而造成自身極大的困擾和損失。

## (二)節日性網路釣魚案例

越來越多的網路購物節日推陳出新，導致每年的網路購物節日營收逐漸增加，成為一種新興的購物熱潮。然而，卻有許多攻擊者利用此習慣，將帶有惡意的訊息包裝成購物的商品等資訊，透過節日相關的訊息，誘騙使用者上當後，成功竊取其個資。在針對節日的網路釣魚攻擊逐漸增加的同時，國內也發生不少相關案例，列表如下：

表 2、節日性網路釣魚統整表

| 網路釣魚類型 | 網路釣魚主題 | 網路釣魚媒介 | 網路釣魚手法 | 受害情形 |
|---|---|---|---|---|
| 假冒之銷售與廣告 | 情人節浪漫信件，下載附件查看詳細資訊 | 釣魚郵件與多種惡意程式 | 情人節時，透過相關愛情內容，誘騙使用者下載帶有惡意程式的附件 | 主機遭惡意程式攻擊除了個資外洩，還可能遭攻擊者操控及勒索 |
| 假冒之網路購物驗證訊息 | 雙11期間出現未購買商品的訂購通知，提供個資以取消訂單 | 釣魚郵件與偽冒大型零售商的釣魚網站 | 告知使用者一筆未下訂、金額不菲的訂單資訊，一旦使用者欲取消訂單，會進入釣魚網站後被要求填寫個資和金融資訊 | 使用者填寫的個資和金融資訊外洩 |
| 假冒之訂單商品物流資訊 | 雙11購買的貨物寄送失敗，需前往網站填寫資訊以驗證身份 | 釣魚簡訊與偽冒物流公司之釣魚網站 | 告知使用者送貨失敗，在使用者點擊簡訊中連結，並填寫相關資訊後，將會被開啟小額支付，並被盜刷多筆費用 | 個資以及小額支付的掌控權遭盜用，支付盜刷費用致金錢損失 |
| 假冒之善心捐款求助 | 春節購物即捐款部分收益給弱勢族群 | 購物平台及社群媒體 | 告知使用者在春節期間購物，會將部分收益捐給弱勢族群，卻在收到款項後不聞不問 | 損失購物的費用 |

在節慶期間，攻擊者將假冒的產品提供較大折扣，藉以誘引消費者購買，或利用與節慶相關的聳動文字，吸引消費者前往該網站瀏覽，甚至在消費者購物後，假冒為購物相關商家或物流人員，藉口優惠秒殺、網路抽獎等理由，迫使消費者於不假思索情況下便提供個資，甚至提供相關金融資訊，讓攻擊者得以利用節日，竊取更多資訊、獲取更多不法利益。

## 三、節日性與假期性網路釣魚防護

隨著網際網路的普及化，以及網路購物的興起，許多民眾在假日時為節省出門購物的時間和精力，會選擇透過網際網路購買所需物品。尤其是在節慶時節，許多與節日相關的產品紛紛推陳出新，增加民眾的購買慾望。更遑論近幾年大量的網路購物節日紛紛推出，產生極為驚人的經濟效益。然而，也有越來越多的攻擊者倚賴網路購物的發展，藉此賺取更多的不法利益。這些攻擊者往往會利用大折扣、特殊產品、仿冒知名商家的商品，或假冒網路購物的物流公司，要求使用者提供個資方進行運送。以及假冒為金融企業，告知使用者其使用的支付方式未成功，需利用攻擊者的方式重新支付，導致這些消費扣款落入攻擊者手中。甚至透過行善的名義，要求民眾提供資金或

提升購物意願，實質上卻是讓攻擊者輕易獲取不正當的金錢利益。

因此，為避免在假日或節日時，因一時的疏忽導致蒙受額外損失，使用者在每個節日、假期時，除提高警戒外，應採取下述防範措施[16]：

1. 注意自己的金融卡與信用卡：注意自己在購物時，所拿出的卡片位置，以及是否有遭他人掃描、盜用，甚至竊取其中的資訊。

2. 保留購買證明：在進行購物時，應保留任何購買的收據、購買證明及金流證明等資訊，一旦有任何問題，可以作為證據以保障自身權益。

3. 經常檢查賬戶及帳單：使用者必須經常檢閱信用卡相關的帳單和支付內容、數額，並且保留相關紀錄，避免遭他人利用盜刷而不自知。

4. 確認網站的真實性：許多攻擊者會透過與真網站相似的網址和網頁呈現欺騙使用者，只要使用者不仔細檢查便難以分辨該網站的真假，讓使用者以為該網址為真正的企業網站，事實上反而是誤入釣魚網站。以及在進行善心捐款時，應確定捐款對象的真實性，以及透過可信任之協募款商家進行愛心捐獻。

5. 維持注意網站安全性的習慣：許多偽冒的釣魚網站或臨時架設的假網站，鮮少會注意並耗費精力使用 HTTPS，因此，使用者在進行連網行為時，可多加留意該網站是否為 HTTPS，一旦沒有使用 HTTPS，就必須多加注意，並且減少提供個人資訊進行金融交流等行為。

6. 確認與追蹤貨物的物流狀況：使用者應選擇足以信任的物流公司進行商品配送，且時時注意配送狀態，避免被假冒的送貨資訊欺騙，使得重要貨物落入攻擊者手中。

7. 注意過高的折扣：對於一些不太合理、過度優惠折扣，甚至不合常理的價格，必須多加留意過濾。例如知名品牌的智慧型手機，終年不予以折扣，卻在某

些商家中提供頗高的優惠價格，則該產品品質、來源，甚至真假，都必須多加留意，避免購買後財物兩空。

在美好的假期及節日時分，是大眾歡慶、購物及放鬆的日子，但往往會出現惡意人士利用這些美好，藉由各種網路釣魚手法，從民眾身上獲取不法利益，導致美好的日子變調。因此，在這些特殊的日子裡，使用者在進行網路行為時，務必謹慎小心，對於任何可疑的訊息一概不全盤接受，並且盡量透過可信的管道進行購物或金流交換等行為，除了保障自身的權益不受損外，，也避免無端受到任何有心人士打擾，安心歡度美好的假期及節日。

四、結論與建議

1. 節日與假期，是許多人放鬆警戒及較常使用網路購物等行為的時節，導致越來越多攻擊者會透過針對節日與假期的網路釣魚攻擊，來增加其網路釣魚的成功機率。較常出現的類型為假冒的銷售與廣告、網路購物驗證訊息、訂單商品物流資訊，以及善心捐款求助等，讓在假日及節日時常進行網路行為的使用者防不勝防。

2. 為避免遭受節日與假期性的網路釣魚攻擊，雖然在購物前，使用者就必須慎之又慎，避免受騙上當，但在決定購買後也應留有萬一被詐騙之後減少損失的餘地。因此建議使用者在進行網路購物時，盡量不使用金融卡或轉帳方式付款，而是透過非當場扣款的信用卡，或是透過如 PayPal、Apple Pay 等可信第三方支付管道進行款項支付，一旦確認遭受詐騙，仍可向信用卡公司或支付管道進行投訴，以取回部分或全數消費金額。

3. 在進行購物時，不論是金融卡還是信用卡，都是許多人支付款項的喜好選擇。然而，這些卡片上的資訊一旦遺失或外洩，則其中的資金可能都轉為攻擊者所有。而這些攻擊者一旦取得相關資訊，為了不打草驚蛇，往往會以小額支

付方式，多筆交易後以取得較大資金。雖然在進行任何交易時，使用者都必須小心謹慎，但就怕一時疏忽導致資訊外洩，因此，使用者最好替自身金融卡或信用卡，設定輸入次數上限，一旦在同樣系統中購物超過該次數，將會被鎖定且提供警示，如此，萬一不小心被竊取資訊，仍可防堵攻擊者透過大筆數的小額購物，累積消費大量的金額。

4. 在節日時分，使用者往往會收到大量的廣告訊息，但點擊進入後的購買系統類型不盡相同，例如有些透過電商平台、有些自創網站，甚至有些要求使用者下載應用程式進行購物。因此建議使用者，盡量避免在檢閱廣告後，下載任何檔案，不論是廣告宣傳檔案或應用程式下載，因為在這些檔案中，難以辨別是否有惡意程式潛藏於其中。即便該應用程式為透過 App Store 或 Google Play Store 等合法管道下載，但仍需仔細檢閱其要求之權限，以及隱私條款，避免在下載並進行購物後，自身所提供的相關訊息，遭到惡意使用。

5. 在假期期間，許多人會外出使用公共 WiFi 或電腦，然而，在節慶時分，會有許多攻擊者藉由不安全的網路或電腦，竊取使用者的資訊。因此，建議使用者一旦使用公共且不保證安全的 WiFi 和電腦時，盡量減少進行購物或金流交換等行為，避免攻擊者透過不安全的網路和不安全的電腦，竊取使用者的個資和資金。

6. 在節日與假期時節，不論是購物或捐款的支付方式都相當多，而近期流行、預先付款的禮物卡、預付卡與點數卡等，更是便利且受歡迎的支付方式，由於事先已確認其價值且便於攜帶，甚至會配合店家有相對應的優惠，使得此種類型的支付方式越來越受大眾歡迎。但正如其名，此種支付模式經常被作為贈送用途，尤其愈來越多的禮品卡不需透過實體交易，僅需告知序號即可

使用及支付款項，且難以追回，導致越來越多的攻擊者會要求使用者透過禮物卡進行交易。因此，建議使用者若收到任何支付訊息，不論是購物還是善心捐款，一旦對方要求透過禮物卡進行支付，多半都屬於網路釣魚較多，務必多加留心，避免上當。

7. 為避免在節日與假期時，遭到相關網路釣魚攻擊，許多企業、組織及網站都會定期公佈那些可疑或確實有進行惡意行為的網站及公司，建議使用者在進行任何購物或款項支付前，都應前往這些網站查詢，確認目標支付對象並非可疑或詐騙者。但若使用者仍不幸遭到網路釣魚攻擊，則建議使用者應立即通報相對應的組織，採取進一步的防範措施，促其加強整體網路資安能量以防堵攻擊蔓延。

- 資料來源：

1. 2020 台灣網路報
2. Online holiday sales grow north of 45% in 2020
3. A record-breaking Cyber Week 2020: Online shopping steals the show
4. Holiday shopping season fraud stats revealed
5. Seasonal Scams: Valentine's Day Edition
6. Steer clear of IRS imposter scams
7. Holiday Phishing Attacks
8. 【「想看電影嗎？」詐騙粉專也搭上《復仇者聯盟 4》熱潮】
9. 日本出現偽裝「樂天信用卡」通知信的釣魚詐騙，大家要小心
10. 【詐騙】郵寄包裹涉嫌違規操作退回？核對退貨地址？危險簡訊
11. 《詐騙快訊》「南部淹水，民眾分享 10 人，集團捐款千元」王品集團遭冒用

防詐達人呼籲民眾愛心別被利用

12. 病毒提前過情人節?看到「Love you 」附件別亂點! 垃圾信夾帶惡意 JavaScript, 散播勒索病毒 挖礦程式,台灣列全球第五大感染區
13. 詐騙新手法:取消訂單,信用卡反而被盜!
14. 「查包裹」 假中華郵政奪個資 盜刷 AppStore
15. 網拍詐騙近來激增，近 900 人匯款後未收到貨！
16. 7 Tips to Help Protect You from Holiday Fraud

# 第 2 章、 資安活動紀事

## 資安防護及案例分享研討會-雲林場


活動時間：111.09.02(五) 14:00~16:30

活動議程：

| 時　間 | 議程內容 |
|---|---|
| 13:30 ~ 14:00 | 活動報到 |
| 14:00 ~ 14:30 | TWCERT/CC 服務範疇及案例分享<br>TWCERT/CC 專業講師 |
| 14:30 ~ 16:20 | 製造業如何因應資安威脅<br>瑞思資訊股份有限公司<br>鄭閔聰 專案經理 |
| 16:20 ~ 16:30 | Q & A |

由 TWNIC、TWCERT/CC 主辦的資安防護及案例分享研討會於 9 月 2 日假雲林縣斗六市公所 2 樓第二會議室舉辦。臺灣遭受資安攻擊事件高於全球平均值，因應惡意程式攻擊及勒索軟體攻擊日以俱增，製造業於內外部之圖檔與文檔等資料，面臨資安漏洞風險威脅，希望透過本次研討會介紹台灣電腦網路危機處理暨協調中心(TWCERT/CC)免費資安通報的服務內容，並邀請專業講師探討「製造業如何因應資安威脅」，企業透過提升端點安全才能有

效降低惡性攻擊之防護管道。

研討會首先由 TWCERT/CC 曲承則工程師講授 TWCERT/CC 服務範疇及資安事件案例分享，首先與企業人士分享各類型資安威脅案例，包含釣魚網站、DDoS 與殭屍網路、重大更新提醒、勒索攻擊案例等，特別針對案例分享美國燃油管道系統遭受 DarkSide 勒索攻擊，系統檔案遭受加密並盜取近 100G 資料要脅，甚至導致美國東岸近 18 州的燃油管道作業停擺而進入緊急狀態。由此可見，在網路時代下資安即國安已成事實，曲工程師建議大家面對勒索攻擊可有以下措施：首先一定要使用防毒軟體並即時更新系統、實施網路分段區隔並監控流量、僅在需要時啟用 Microsoft Office 巨集、必須要加密重要或敏感資料、更需要安排定期進行檔案備份。接續曲工程師特別針對 TWCERT/CC 服務說明詳細說明：企業遭受資安事件通報的流程與方法、網路釣魚通報、漏洞揭露通報、惡意檔案檢測服務以及加入 TWCERT/CC 資安聯盟好處，企業可取得資安情資優先預警的資訊，鼓勵企業訂閱情資電子報等服務內容。

接著研討會特別邀請瑞思資訊股份有限公司鄭閔聰專案經理，講授主題為「製造業如何因應資安威脅」。首先針對台灣製造業資安現況介紹，點出近 95%製造業廠商仍為資安入門生，僅有設置基本防護，整體仍缺乏資安觀念。然而製造業資安難以落實的原因，根據工研院統計，多數來自內部技術能量不足、公司對於資安投資報酬率缺乏了解，以及內部員工缺乏資安意識所導致。另一因素更是來自於對企業主而言導入資安其效果難以量化，僅能以遭受攻擊後停機停工時間之損失進行量化，而非增加企業營業額或製程效率等。鄭經理提出製造業三大資安需求：1.跨廠區管理需求，2.設備聯網與遠端連線需求，3.IT 及 OT 混合環境下 OT 資安解決方案，更藉由舉例 2018 年某企業產線資安事件僅因為人員疏失未遵守標準 SOP，進行新機上線前隔離掃毒，造成產線停擺損失高達幾十億元。鄭經理最後強調員工資安意識將是因應資安威脅最初步的防護方式，因製造業資安與工安不同並無專法規定，建議參考公部門資安法相關應辦事項、上市上櫃公司資通安全管控指引，製

造業可從管理面、技術面、人員認知開始著手。

最後議程 Q&A 時段，與會人士踴躍提出詢問：首先第一個問題詢問「因為公司有兩個廠區，想請教講師關於跨廠區的資安，建議要如何做起，因為目前許多資料都是透過網路來共享連線，如果要導入相關制度的話公司能不能自行處理，還是會建議由資安公司進廠輔導協助導入呢？」鄭閔聰經理回覆建議將外網串成大內網會相對安全，建議委由資安公司來進行，因為串大內網是相對複雜，另外建議聘請講師至場內對人員上資安觀念課程，提升廠內每一位人員資安意識是更加落實的做法。第二個問題詢問「目前公司沒有機聯網的部分，公司資料都是使用內網，請問是否表示廠區內就沒有所謂的資安威脅了呢？還有其他的潛在威脅？」鄭閔聰經理答覆：確實公司若是多使用內網是相對安全，但通常資安事件遇到最大的問題是 USB、光碟、網站等問題，且經常遇到的破口是在於人員的疏失上，且公司一定會有一個在對外窗口的外網電腦，這就必須是重點注意與防護的地方。

本場研討會為實體與線上同步舉辦共 58 人與會，經由兩位專業講師的資安探討，與會人員皆受益良多，以及認識 TWCERT/CC 詳細的服務內容。經統計會後問卷調查統計，對於本次雲林資安研討會內容、講師專業度及場地滿意度等表達為滿意。

# 第 3 章、 國內外重要資安事件

## 3.1、資安趨勢

### 3.1.1、資安專家發現駭侵者利用「影子網域」發動攻擊的案例數量大增


**全球網通產品大廠 Palo Alto Networks 旗下的資安威脅研究團隊「Unit 42」，近日發表調查報告指出，近來透過「影子網域」（domain shadowing）手法發動駭侵攻擊的案例數量，較過去大為提升。**

報告指出，該團隊利用網路掃瞄的方式進行分析，在 2022 年 4 月到 6 月之間就發現了 12,197 個影子網域案例。

資安專家表示，影子網域是一種 DNS 挾持攻擊的類型；駭侵者以各種手法取得某個網域名稱的控制權後，在該網域下新增一個子網域，指向自己能夠控制的主機，來進行各種駭侵攻擊活動。

這種攻擊手法由於沒有更動主網域與其下屬其他子網域，因此不容易遭到發現；而用戶在接收到駭侵者冒用遭挾持為影子網域主機所發送的釣魚信

件，或連上惡意網站時，由於仍會顯示合法真實的網域名稱，所以不但能夠通過防毒防駭程式的監控，用戶也會降低其戒心。

Unit 42 指出，影子網域的偵測極為困難，必須使用高度的自動化機器學習技術，才能快速精準分析大量的 DNS 記錄資料；在 VirusTotal 中也僅僅記錄了 200 個影子網域的案例，少於 Unit 42 找到的 12,197 個案例。

在 Unit 42 針對某個影子網域的駭侵攻擊案例分析中，可以看到該駭侵者挾持了 16 個分屬澳洲、俄羅斯和美國的私營企業、教育單位網域，並在其下設立了 649 個影子網域，來進行各種駭侵攻擊；其中有個澳洲企業所屬的網域，遭駭侵者私設影子網域的時間，長達 19 年。

由於這類透過影子攻擊的手法難偵測並防範，因此各單位的網域管理者，必需經常檢視自己擁有的網域是否出現異常；一般用戶在進入疑似釣魚頁面時，也應提高警覺，即使網域名稱無誤，也不要任意輸入自己的登入資訊。

- 資料來源：
  1. Domain Shadowing: A Stealthy Use of DNS Compromise for Cybercrime
  2. Domain shadowing becoming more popular among cybercriminals

## 3.1.2、統計指出，超過 80% 大型網站將用戶搜尋資訊透露給廣告業者


**資安廠商 Norton 旗下研究單位 Norton Labs 的資安專家，近期發表研究報告指出，有超過 80% 的大型網站，會將網友在其網站上搜尋站內資訊時輸入的關鍵字，透露給如 Google 之類的網路廣告業者；這種行為可能造成用戶隱私侵害問題。**

Norton Labs 為研究用戶瀏覽網站受到阻礙的情形，開發出一個網頁爬蟲程式，首先模擬真人用戶進行站內搜尋，並在搜尋框內輸入「JELLYBEANS」當做搜尋關鍵字，然後收集網站所有網路流量進行分析，結果發現分析目標的 100 萬個網站中，有高達 81.3% 網站與第三方網站之間的連線要求的後續傳送資料中出現了「JELLYBEANS」這個關鍵字，足證用戶輸入的站內搜尋關鍵字，被傳送到第三方網站中；而這些第三方網站中，絕大多數都是網路廣告相關業者的伺服器。

藉由分析這些連線要求封包標頭中的資訊，Norton Labs 可以掌握取得「JELLYBEANS」關鍵字的，是哪些第三方網站；Norton 同時也發現用戶輸入的站內搜尋關鍵字，有 75.8% 透過 Referer header 來傳送，也有高達 71% 透過 URL 的後綴參數來傳送。

Norton 指出，雖然各大網站都備有大篇幅的隱私保護政策，但真正有在其隱私保護政策中明確說明會將用戶的搜尋內容傳給第三方的網站，僅佔 13%；其他 75% 網站都只用概括性的描述「與第三方分享用戶相關資料」輕輕帶過。

針對網站把用戶輸入的關鍵字傳送給第三方網站的做法，目前沒有太多防範措施；不過為了避免這些輸入資訊與個人可追蹤身分連結起來，導致用戶隱私進一步的侵害，建議用戶可使用工具來阻擋網頁中埋入的跨站追蹤機制，或使用具備跨站追蹤阻擋功能的瀏覽器，例如 Safari、Firefox 等。

- 資料來源：
  1. 8 in 10 Websites leak your search terms
  2. Over 80% of the top websites leak user searches to advertisers

## 3.1.3、調查指出，2022 年第一季全球 34% 登入動作為憑證填充攻擊所為


**資安廠商 Okta 日前發表調查報告，指出在本（2022）年第一季中全球網路的登入流量中，有高達 34% 為駭侵者發動的憑證填充（Credential Stuffing）攻擊；在某些地區這類攻擊的流量甚至高於正常登入流量。**

所謂憑證填充攻擊，多為駭侵者透過僵屍網路對目標伺服器發動大規模登入嘗試，在每次登入時都會使用竊取而來的登入資訊，試圖登入目標伺服器或網路服務。如果某一組登入資訊可以成功登入，駭侵者就能進入系統，進行進一步的攻擊；如果一直無法登入，目標伺服器也可能因為短時間的大量登入連線要求，造成系統不堪負荷，導致正常服務受阻。

Okta 報告指出，該公司長期監測網路登入流量並進行分析，發現 2022 年以來，透過憑證填充攻擊的案例數量較往年大幅上升；以全球登入流量來看，已佔 34%，亦即超過三分之一的登入都是憑證填充攻擊。

報告也指出，在全球某些地區如東南亞和美國，憑證填充攻擊的流量佔比還更高，遠超過正常登入的流量佔比。如以攻擊目標所屬行業別來看的話，最常遭到憑證填充攻擊的是零售/電商網站，此外教育、能源、金融服

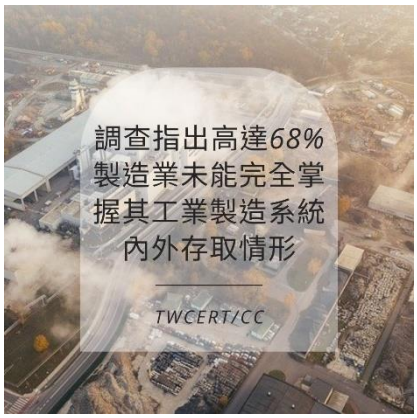
務、軟體/SaaS 網站也是這類攻擊集中發動的目標類型。

另外 Okta 也指出，這類攻擊的特徵是會集中火力在短期間內大量發動登入攻擊，有案例是登入連線要求暴增 10 倍以上，因此往往造成伺服器巨大負荷，影響正常運作。

建議網站營運管理者應採取行動防範憑證填充攻擊，包括使用各種偵測方式辨認非正常登入要求、採用 proxy 偵測系統，且將可疑帳號予以停權等；用戶則應避免在不同服務之間使用同一組密碼，並且務必啟用二階段登入驗證。

- 資料來源：
  1. Top Insights From Our 2022 State of Secure Identity Report
  2. Okta: Credential stuffing accounts for 34% of all login attempts

## 3.1.4、調查指出高達 68% 製造業未能完全掌握其工業製造系統內外存取情形




**資安廠商 SecureLink 日前發表調查報告指出，製造業在管理其連網工業製造控制系統上，面臨重大資安風險；其中有高達 68% 廠商表示，對於其製造系統內外相關帳號的存取權限無法完全掌控。**

報告指出，製造業在邁向數位轉型與工業 4.0 的過程中，導入多種智慧與數位技術，以控制生產流程，提高生產效率；然而這些新導入的相關系統，如營運科技（Operational technology, OT）、工業控制系統（Industrial control systems, ICS）和可程式化邏輯控制器（Programmable logic controller, PLC）等系統，原本並非設計為與外部網路互連。許多製造業者為求便利，讓這些系統可對外連線時，未能同步加強其資安防護能力，就帶來諸多威脅。

調查也指出，超過 50% 製造業者自陳未能加強其製造系統資安防護的原因有三，一是無法完全掌握、監控內外所有相關帳號的連線與其權限，二是治理方面的缺失，三是缺乏應對相關資安風險的處理能力。

調查報告也揭露，有高達 42% 製造業者並未針對第三方對其工業系統的連線工作階段進行任何監控，甚至未對第三方可進行的連線與存取權限加以

限制，直接視同內部員工的連線存取，因而給予過多不必要的存取權限與資源。

報告也顯示製造業者對於帳號管理過於鬆散的事實，有 41% 業者沒有移除無需再次連線的帳號，也沒有控管登入資訊共享的情形；這導致駭侵者可以輕易利用各種方法取得登入資訊，進而駭入公司內網與其工控系統。

建議製造業應大幅加強工控系統的資安層級，除避免工控系統直接曝露於外網之外，更應仔細盤點各種不同層級連線者的存取權限，予以嚴格限制；且應即時清除無需再次連線的帳號。

- 資料來源：
  1. Lack of Access Management Is Causing Data Breaches
  2. How to Solve Third-Party Remote Access Problems in Manufacturing

## 3.2、新興應用資安

### 3.2.1、多家加密貨幣交易所採用的 npm 軟體套件遭植入惡意程式碼


**資安廠商 Mend 旗下的資安專家，日前發現由許多加密貨幣交易所採用的部分 npm 軟體套件，近日遭駭侵者植入可用於資訊竊取的惡意程式碼。**

這些遭植入惡意程式碼的 npm 套件，經查係由 dYdX 交易所的員工所上傳；dYdX 是一個架構在以太坊區塊鏈上的去中心化加密貨幣交易所（Decentralized Exchange, DEX），提供包括比特幣與以太幣等 35 種以上熱門加密貨幣的永續合約交易，每日交易量超過 10 億美元。

資安專家指出，目前確定含有惡意程式碼的 npm 軟體套件有 @dydxprotocol/solo 0.41.1、0.41.2 和 @dydxprotocol/perpetual 1.2.2、1.2.3 等。另外稍早時候證實亦遭植入惡意軟體的 @didxprotocol/node-server-base-dev，目前則已下架。

資安專家指出，在 Github 中至少有 44 個專案使用了 @dydxprotocol/solo 套件，而這些專案則分屬多個加密貨幣交易平台所有。因此可以想見有多家加密貨幣交易平台，可能使用了這些內含惡意軟體的程式碼套件來進行開

發。

分析指出，植入的惡意程式碼，一旦安裝到受害電腦上，即會自受害者在 Amazon AWS instance 上竊取 IAM 登入資訊，以及用戶在 Github 上的 token、SSH key、環境變數與對外 IP 等資訊。

dYdX 在收到其上傳程式碼內含惡意軟體的通報後，對外表示已立即自 npm 中移除多個程式套件，並表示該平台的網站、App 均未遭到攻擊，該平台資金安全無虞，且該惡意軟體不會攻擊其智慧合約。

由於這類在公開的開源程式套件庫中植入惡意軟體的供應鏈攻擊案件，近來發生次數日益增加，因此程式開發者在採用這類程式庫時，務必提高警覺，並做好對應防範措施，以免遭到攻擊。

- 資料來源：
  1. Maciej Mensfeld @maciejmensfeld
  2. dYdX @dYdX
  3. npm packages used by crypto exchanges compromised

## 3.2.2、荷蘭警方逮捕竊取加密貨幣並且洗錢的犯罪分子


**荷蘭警方近日宣布，於今（2022）年 9 月 6 日前逮捕一名 39 歲男子，該男子涉嫌竊取數千萬歐元等值加密貨幣並且進行洗錢。**

荷蘭警方表示，在接獲該國與義大利受害者報案後，警方與該國中央網路犯罪偵辦單位協力合作，監控特定比特幣交易後，終於找到該名犯罪分子的行蹤，並於一個叫 Veenendaal 的小村將其逮捕。

警方在聲明中說，該名嫌犯所有透過犯行得到的不法獲利，目前均以加密貨幣形式遭到警方扣押；該嫌犯雖然在 9 月 8 日獲釋，但警方對其犯罪行為的調查仍在繼續進行中。

警方在聲明中指出，該嫌犯係利用植入惡意程式碼的更新版加密貨幣錢包 Electrum Wallet 來竊取受害者的加密貨幣。Electrum 是一個開源比特幣數位錢包，可以用來儲存用戶的加密貨幣資產。

警方目前尚未提供關於此案駭侵手法的詳細說明，不過荷蘭警方向媒體表示，嫌犯是透過釣魚攻擊來散布植入了惡意程式碼的 Electrum 錢包；嫌犯極可能在 Electrum 中植入了可竊取受害者電腦資訊的惡意程式碼，或是利用釣魚攻擊誘騙受害者輸入機敏資訊，因此能夠掌握受害者用以復原加密貨幣錢包的復原短語。

只要輸入正確的復原短語，駭侵者即可在自己的設備上，完全存取受害者加密貨幣錢包，並且輕易竊走錢包內的加密貨幣資產。

加密貨幣投資者應特別注意資產安全，避免將加密貨幣儲存在可透過網路連線存取的「熱錢包」，避免自不明來源下載相關軟體，同時絕不將復原短語告知任何人。

- 資料來源：
  1. Man verdacht witwassen tientallen miljoenen euro’s aan cryptovaluta [English below]
  2. Police arrest man for laundering tens of millions in stolen crypto

## 3.2.3、Lazarus 駭侵團體藉詐騙 Crypto.com 工作機會，對開發者植入惡意軟體


**資安廠商 Sentinel One 近日發表調查報告，指出該公司的資安研究團隊，發現 APT 駭侵團體 Lazarus，近日透過假冒 Crypto.com 的多個工作機會，對應徵的加密貨幣相關開發者投放含有惡意軟體的 macOS 檔案。**

Crypto.com 是全球知名的大型加密貨幣企業，除了提供加密貨幣交易外，也提供 NFT、質押賺息、DeFi 服務等多項功能；該公司大手筆買下洛杉磯 Staple Center 球場冠名權，同時贊助多項運動比賽，因此成為駭侵者假冒的對象。

Lazurus 過去就曾有假冒加密貨幣業者在 LinkedIn 上「徵才」，然後以私訊傳送惡意軟體，用以駭入加密貨幣相關從業人員電腦的記錄。這次 Sentinel One 發現的攻擊活動，可謂故技重施；駭侵者透過 LinkedIn 私訊傳送一份 26 頁的 PDF 檔給應徵的加密貨幣開發者，檔案內容看似為 Crypto.com 的所有職缺說明，但內藏一個可在 macOS 執行的惡意軟體 Mach-O 二進位檔，接著進一步安裝酬載，並連接到駭侵者設立的控制伺服器。

由於在 Sentinel One 調查期間，Lazarus 已經關閉其控制伺服器，因此暫時未能查明會有哪些資料遭竊；不過 Lazarus 長期以來都鎖定加密貨幣相關業者與從業人員進行攻擊，過去也曾成功竊取受害公司與個人的加密貨幣資產。

建議加密貨幣相關工作者在求職轉職時，務必確認自己看到的職缺與聯絡窗口的真偽，對於對方寄送來的相關檔案也應小心謹慎，勿隨意開啟；各加密貨幣業者也應經常巡查 LinkedIn 等求職平台，檢視是否有不明帳號冒充官方帳號進行不法活動，如有則應立即檢舉。

- 資料來源：
  1. Lazarus ‘Operation In(ter)ception’ Targets macOS Users Dreaming of Jobs in Crypto
  2. Lazarus hackers drop macOS malware via Crypto.com job offers

## 3.2.4、駭侵者自加密貨幣交易公司 Wintermute 竊走 1.62 億美元等值數位資產


**數位資產交易公司 Wintermute 日前發布資安通報，指出該公司的去中心化金融業務（DeFi）遭到駭侵者攻擊，高達 1.62 億美元的數位資產遭竊。**

Wintermute 的主要業務是在多達 50 個以上的加密貨幣交易所與交易平台中提供流動性，亦即投入加密貨幣資金，以賺取利息或其他收益；與 Wintemute 合作的大型加密貨幣交易所，包括 Binance、Coinbase、Kraken、Bitfinex 等。

雖然 Wintermute 沒有提供任何本次駭侵攻擊的細節，僅表示公司資產充裕，運作一切正常，不過加密貨幣專家推測指出，駭侵者可能是利用個人化以太幣錢包位址產生器 Profanity 的一個已公開漏洞來發動此次攻擊，並且成功竊取大筆資金。

資安專家指出，由於 Profanity 充許用戶在位址中使用自訂 16 進位數字組合來產生自訂錢包位址，因此給駭侵者透過暴力試誤法來產生私鑰的空間；據估計，駭侵者只要使用 1000 個 GPU 運算 50 天，即可產生 7 位數自訂位址的所有私鑰組合。而許多加密貨幣礦場使用的 GPU 數量都遠大於此。

資安專家也表示，由於以太坊自需要大量算力的工作量證明（PoW）共識協定，改版至不需要算力的權益證明（PoS）共識協定，造成許多以太幣礦工投下巨資購置的礦機，此後陷於無用武之地的困境；這些礦機也可能遭駭侵者取得用來進行 Profanity 位址破解運算，用來獲取暴利。

建議加密貨幣投資者，如果將數位資產存在由 Profanity 產生的錢包位址，應盡速將資產轉移其他錢包內；最好使用不連接網路的冷錢包來儲存資產，且絕對不要將錢包恢復短語告知外人，或存在易遭破解的網路服務內。

- 資料來源：
  1. wishful cynic @EvgenyGaevoy
  2. Hackers steal $162 million from Wintermute crypto market maker

# 3.3、國際政府組織資安資訊

## 3.3.1、美國資安主管機關下令各單位立即修補已遭用於攻擊之漏洞


**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）日前下達命令，要求聯邦政府旗下各單位必須在限期之內修補新加入「已知遭攻擊漏洞」清單（Known Exploited Vulnerabilities, KEV）的 12 個以上資安漏洞，其中包括 Google Chrome 0-day 漏洞。**

這些漏洞多半已經遭到各大駭侵團體大規模用於攻擊，其中包括已在 9 月 2 日推出修補版本的 Google Chrome 0-day 漏洞 CVE-2022-3075、已經發生大規模 Deadbolt 勒贖攻擊的網通產品漏洞 CVE-2022-27593，以及遭到 Mirai 以及 Moobot 僵屍網路大規模攻擊的兩個嚴重漏洞 CVE-2022-28958 與 CVE-2022-26258 等。

其他於此次列入清單中的漏洞，還包括 Apple iOS、iPadOS、macOS 的輸入驗證漏洞（CVE-2022-9934）、Oracle WebLogic Server 的不明漏洞（CVE-2018-2628）、Android OS 權限提升漏洞（CVE-2011-1823）等。

根據 CISA 指出，在該局將最新漏洞加入其「已知遭攻擊漏洞」清單後，所有聯邦旗下的民事相關單位，都必須依照於去（2021）年 11 月頒布的強制操作指引（Binding Operational Directives, BOD) 22-01 之規定，限期完成新加入漏洞的修補作業。

以這次的情形而言，各聯邦所屬單位將有三星期的時間完成各項修補作業，最遲應於 11 月 29 日前全部完成。

雖然美國 CISA 這類命令只對美國聯邦政府旗下單位具有約束力，但仍建議我國各公私營單位密切注意 CISA 發布的各項資安通報與修補命令，參考其資安防護指引修補漏洞，並強化自身的駭侵攻擊防禦能力。

- 資料來源：
  1. KNOWN EXPLOITED VULNERABILITIES CATALOG
  2. CISA RELEASES DIRECTIVE ON REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES

## 3.3.2、英國警方逮捕涉嫌駭入 Uber、Rockstar 等公司的 17 歲駭侵者


**英國警方宣布逮捕一名英國籍 17 歲嫌疑犯，該嫌疑者涉及日前發生於 Uber、Rockstar 等公司的駭侵案件。。**

倫敦市警察局稍早發表聲明，指出該局於本（2022）年 9 月 22 日於地點 Oxfordshire 逮捕該名 17 歲嫌疑犯，目前正在進行偵訊。調查與逮捕行動係會同英國國家刑事局（National Crime Agency）與國家網路犯罪單位（National Cyber Crime Unit, NCCU）共同進行。

由於嫌犯仍未成年，因此警方沒有公布其姓名。

雖然倫敦警方沒有提供關於駭侵案件的詳細說明，不過資安專家認為該案件與 Lapsus$ 駭侵團體高度相關；資安界普遍認為該駭侵團體與近期發生的 Uber、Rockstar Games、2K 等公司的駭侵事件有關。

在去（2021）年，資安專家曾懷疑 Lapsus$ 犯下的一系列大公司駭侵案，就是由一名被稱為「White」或「BreachBase」的 16 歲英國駭侵者指揮，受害的公司包括 Microsoft、Cisco、NVIDIA、Samsung 和 Okta 等。

今年 4 月時，倫敦警方也曾逮捕 7 名駭侵者，年齡自 16 歲到 21 歲不等，其中包括一名 17 歲的主犯；不過警方很快就讓其中兩人保釋，主要是因

為其並非主要犯嫌。

數日前一個自稱「Teapotusbehacker」的駭侵團體，在網路上公開未上市大型遊戲「俠盜獵車手 6」（Grand Theft Auto 6）的部分開發中遊戲片段影片，以及 GTA 5（ 已上市）與 GAT 6 的部分程式碼片段。

這類針對大型公司的駭侵案件日益普遍，往往造成未上市產品遭到提前公開，因此各企業應加強資安防護與演練，避免員工和有弱點的系統成為遭駭破口。

- 資料來源：
  1. City of London Police @CityPolice
  2. UK Police arrests teen believed to be behind Uber, Rockstar hacks

## 3.4、社群媒體資安近況

### 3.4.1、資安專家發現駭客新手法，透過 Microsoft Teams 的 GIF 進行釣魚等多種攻擊


**獨立資安研究人員 Bobby Rauch 近期發現一種針對工作社群討論軟體 Microsoft Teams 的全新攻擊手法，可利用 Microsoft Teams 的一系列資安漏洞，透過特製 GIF 圖檔來發動釣魚攻擊、資料竊取等多種駭侵攻擊。**

專家指出，這種攻擊手法主要是利用一個稱為 GIFShell 的惡意軟體組件，利用 Microsoft Teams 一系列資安漏洞，在受害電腦中建立起「反向殼層」（Reverse Shell），並以此反向殼層來傳送夾帶惡意指令，以 base 64 編碼的 GIF 檔案。

為建立這種攻擊模式，駭侵者首先要設法讓 Microsoft Teams 工作群組中的某個成員，在其電腦中安裝一個可用以執行駭侵指令的惡意 stager，同時在該工作群組中設立一個駭侵者自己控制的帳號。

接下來，駭侵者可以利用 GIFShell 將含有惡意指令的特製 GIF 檔傳送到群組中，受害者電腦上的 Microsoft Teams 會將該圖檔存在 log 檔中；由於任

何低執行權限的人都可以查看該 log 檔，因此 stager 也會監視並接收存在 log 檔 GIF 圖檔內的惡意指令，並將之解碼成文字指令，再交由 GIFShell 惡意軟體來執行；駭侵者便可以此流程發動各種駭侵攻擊，包括釣魚攻擊、資料竊取等等。

Bobby Raush 是在今（2022）年 5 月到 6 月之間發現這種攻擊手法，並立即通報 Microsoft，不過根據資安專業媒體 BleepingComupter 的報導，Microsoft 並未立即修正可導致這種攻擊手法的一系列資安漏洞，而是指出這種攻擊手法的運用必須先要有用戶遭駭入，只要用戶能夠提高自己的資安防護能力與意識，該公司認為沒有立即危險，將會在未來的版本再行修復相關漏洞。

不論一般用途或工作使用的社群溝通軟體，建議用戶都應避免自不明連結下載安裝任何應用程式，也勿輕率點按不明連結，以降低遭這類攻擊鎖定的機率。

- 資料來源：
  1. “GIFShell” — Covert Attack Chain and C2 Utilizing Microsoft Teams GIFs
  2. GIFShell attack creates reverse shell using Microsoft Teams GIFs

## 3.4.2、LinkedIn 的智慧連結，遭濫用於釣魚郵件攻擊


**資安廠商 Cofense 近日發布研究報告，指出該公司發現有駭侵者大規模在釣魚郵件攻擊中濫用 LinkedIn 的智慧連結（Smart Link），跳過 Email 軟體中的資安防護功能，將用戶導至釣魚網頁，以竊取金融相關機敏資訊。**

Smart Link 是 LinkedIn 專為 LinkedIn Sales Navigator 與企業用戶提供的功能，可以透過單一連結，一次傳送 15 個檔案，也提供網路行銷人員各種數據分析資訊。

Cofense 發現的釣魚駭侵行動，主要針對斯洛伐克用戶進行；駭侵者假冒斯洛伐克國營郵局發送通知信件給目標用戶，要求用戶支付包裹遞送費用。駭侵者除了使用假冒的信件標頭，讓發信者看起來像是真正的國營郵局外，在信件中的確認按鈕中，也埋設了 LinkedIn 的 Smart Link。

由於該連結是由 LinkedIn 製作發出，因此不會觸發 Email 軟體中的資安防護警訊機制，用戶一旦點按，就會被導到駭侵者設立的釣魚網站，要求支付 2.99 歐元的包裹運費；不過駭侵者真正的目標，是用戶在頁面中輸入的各項信用卡資訊，包括卡號、持卡人姓名、卡片到期日、背面 CVV 驗證碼等。

用戶一旦送出這些資訊，甚至還會透過手機收到確認繳費的假簡訊，以讓用戶更加不疑有他。

資安專家指出，這類利用 LinkedIn Smart Link 的駭侵攻擊手法，目前雖然只針對斯洛伐克用戶，但受害者範圍的擴大也只是時間問題，很快就會有其他國家用戶遭到類似手法的攻擊。

資安專業媒體 BleepingComputer 就此向 LinkedIn 採訪，LinkedIn 表示內部團隊積極防制任何釣魚攻擊行動，並鼓勵用戶開啟二階段驗證功能，並在遇到疑似釣魚網頁時提出檢舉。

由於釣魚郵件的攻擊手法日新月益，且愈來愈難偵測，建議用戶在任何網頁輸入機敏資訊時，務必提高警覺，在確認後才予以輸入，以求自保。

- 資料來源：
  1. Threat actors abuse LinkedIn slink (Smart Link) to bypass Secure Email Gateways (SEGs)
  2. LinkedIn Smart Links abused in evasive email phishing attacks

## 3.5、行動裝置資安訊息

### Google Play 與 App Store 中發現多支廣告軟體，下載安裝次數高達 1,300 萬次


**資安廠商 HUMAN 旗下的資安情報團隊 Satori Threat Intelligence team，日前在兩大行動作業系統 Android 與 iOS 的官方應用程式商店 Google Play 與 App Store 中，發現多支廣告惡意軟體，總下載次數高達 1,300 萬次。**

這類廣告惡意軟體通常會常駐在用戶手機中，在幕後或幕前顯示大量廣告，甚至會製造假點擊，以詐騙手法賺取廣告分潤。有些還會在用戶不知情的情形下，冒用用戶名義訂閱高價服務或軟體，讓用戶蒙受相當損失。

據該團隊報告指出，這次發現的廣告惡意軟體，有一部分屬於一波名為「Scylla」的全新詐騙廣告攻擊活動；該團隊也認為「Scylla」是同一駭侵團體發動的第三波詐騙廣告攻擊，之前的兩波分別為 2019 年 8 月的「Poseidon」與 2020 年底的「Charybdis」。

報告說，這次在兩大平台上發現的廣告軟體，軟體所屬分類以手機遊戲為主；在 iOS App Store 中共有 10 個，包括 Loot the Castle、Run Bridge、

Shinning Gun、Racing Legend 3D、Rope Runner、WOod Sculptor、Fire-Wall、Ninja Critical Hit、Tony Runs 等。

在 Android Google Play Store 中則有多達 75 個惡意軟體，其中下載量超過 100 萬次者如下：Super Hero - Save the World!、Spot10 Differences、Find 5 Differneces、Dinosaur Legend、One LIne Drawing、Shoot Master、Talent Trap - NEW 等。

由於這些惡意 App 都存於官方 App Store，因此不易防範；用戶在下載前應仔細檢視 App 相關評價與評論，如有異常，應避免下載安裝。

- 資料來源：
  1. Poseidon’s Offspring: Charybdis and Scylla
  2. Adware on Google Play and Apple Store installed 13 million times

# 3.6、軟體系統資安議題

## 3.6.1、資安廠商發現利用時間相關性取得網域名稱的攻擊方法


**資安廠商 PT SWARM 日前發表研究報告，指出該公司發現一種利用憑證透明度（Certificate Transparency, CT）機制發動攻擊的手法，可以利用「時間相關性」攻擊，可以一次取得大量網域。**

報告指出，當代的網站為了避免安全憑證過期而造成網站無法存取，多會利用自動化的 TLS 憑證核發與更新機制，例如企業用的 DigiCert、民用的 Let’s Encrypt 與 ZeroSSL 等。

PT SWARM 發現在這種憑證核發的過程中，存有弱點可進行攻擊；任何人都可以利用這種方法，大量取得登記在同一台伺服器上的所有網域名稱；由於許多憑證核發單位都在同一時間更新憑證，該公司因而發現可以利用這種「時間相關性」弱點來發動攻擊。

該公司的研究人員，是在追蹤駭侵者大量設立的多個釣魚網站的網址設立流程中，意外發現這種攻擊方法：研究人員利用工具查詢某個惡意網站獲得 Let’s Encrypt 核發 SSL 憑證的時間戳記，然後以此戳記在 Censys 網站上查詢在同一時間獲得 SSL 憑證核發的網站，就能獲得大量公開甚至未曾公開

的網域名稱。

研究人員雖然用這種方法，找出由單一駭侵者設立，將用於惡意釣魚網站的網域名稱，但這種方法同樣也能用來發現一般正常網站使用的網址；駭侵者也有可能利用這種簡單的方法，來找出目標網站擁有的所有網址，並且伺機發動攻擊。

建議網站管理員應勤於檢查 CT 記錄檔，就有機會發現遭受這類攻擊的跡象，並且及早因應。

- 資料來源：
  1. PT SWARM @ptswarm
  2. Discovering Domains via a Time-Correlation Attack on Certificate Transparency

## 3.6.2、駭侵者自製 SideWalk Linux 版本變種後門惡意軟體，以攻擊學術單位


**資安廠商 ESET 旗下的資安研究人員，近期發現一種新出現的 SideWalk Linux 版後門惡意軟體；該後門和駭侵團體 SparklingGoblin 與 APT41 關係密切，用以攻擊學術研究單位。**

ESET 在報告中指出，新發現的 SideWalk 後門 Linux 版本，過去原本是針對 Windows 電腦而開發的 Windows 版本，原先於 2020 年由資安廠商奇虎 360 旗下的資安研究單位 360 Netlab 發現，後來其他資安廠商陸續發現，該惡意後門軟體被 APT41/SparklingGoblin 駭侵團體於 2020 年 5 月，用以攻擊香港某一所大學的研究單位。

在 ESET 的報告中指出，這次發現的 SideWalk Linux 版本與 Windows 版本的 SideWalk 可謂系出同源，程式碼與架構有許多極為相似之處；包括兩個版本都使用 ChaCha20 加密演算法，且同時使用一個初始值為 0x0B 的計數器，而這是 SideWalk 的一個特徵。

另外 ESET 也發現 Linux 版的 SideWalk 後門軟體，和 Windows 的版本使用相同的密鑰，對送往控制伺服器的所竊得資料進行加密傳送。這也間接證實兩者間的密切關係。

ESET 指出，SparklingGoblin 近期使用 SideWalk Linux 版攻擊的對象，是當時在 2020 年入侵的同一所大學；該團體成功入侵該校多台伺服器，包括一台印表機伺服器、一台 Email 伺服器，以及一台用來管理學生行事曆與選修課程的伺服器。

由於這類由國家支持的 APT 駭侵團體，其駭侵技術十分先進成熟，因此各個可能成為其潛在攻擊目標的單位，都必須嚴加防範，徹底加強資安防護能力與意識。

- 資料來源：
  1. You never walk alone: The SideWalk backdoor gets a Linux variant
  2. Chinese hackers create Linux version of the SideWalk Windows malware

## 3.6.3、Uber 疑遭駭侵者透過社交工程攻擊，入侵內部系統


**共享乘車與送餐服務大型業者 Uber，於本（2022）年 9 月 15 日發布資安通報，指出該公司發生內部系統遭駭侵者以社交工程攻擊手法入侵的資安事件；目前該公司調查查無用戶個人隱私資訊遭到不當存取的證據。**

Uber 於 9 月 15 日發表的資安通報，僅指出該公司正在應對一起資安事故，且已會同司法單位進行事件調查。接著，該公司又於 9 月 16 日再次發表資安通報，指出目前查無用戶機敏資訊（如用戶乘車行經路徑）外洩的證據，且該公司旗下所有服務，包括 Uber、Uber Eats、Uber Freight、Uber Driver App 等都維持正常運作。

不過據紐約時報指出，這次攻擊事件可能肇因於某位員工遭到一名年僅 18 歲的駭侵者，透過社交攻擊手法取得該公司內部系統的登入資訊。

紐約時報進一步指出，該名駭侵者為了取得兩步驟登入驗證密碼，更透過大量發送垃圾通知的手法讓該名遭駭員工不斷收到推送通知，接著再於 WhatApp 上假冒 Uber IT 人員和該員工對話，進而取得兩步驟驗證碼的存取權。

資安專家也指出，該名駭侵者在取得兩步驟驗證碼後，隨即進入 Uber 內部網路，同時很快就在其內網的某個檔案中找到許多具有極高權限的登入資訊；該名駭侵者立即使用這些登入資訊存取 Uber 內部各項系統，包括產品系統、企業 EDR 控制台、Uber 內部的 Slack 管理介面等等。

駭侵者甚至還公開 Uber 各個內部系統的螢幕擷圖，甚至包括內部財務系統的報告畫面，以及 Uber 透過 HackerOne 舉辦漏洞發現懸賞的多份報告在內。資安專家擔憂駭侵者可能會將這些漏洞資訊對外販售。

建議各企業應加強員工資安宣導，防範員工成為社交攻擊破口；內部系統的重要存取密碼也需善加保護，以免遭駭侵者輕易取得，用於發動進一步攻擊。

- 資料來源：
  1. Uber Says It's Investigating a Potential Breach of Its Computer Systems
  2. ber Claims No Sensitive Data Exposed in Latest Breach… But There's More to This
  3. Security update
  4. vx-underground @vxunderground

## 3.6.4、資安廠商發現針對以色列工業生產控制系統的大規模駭侵活動


**專攻工業資安防護領域的資安廠商 Otorio，近日發表研究報告，指出該公司發現針對以色列境內製造業所屬工業控制系統（ICS）發動的大規模攻擊活動；鑑於這類系統的資安防護能力普遍薄弱，易遭駭侵攻擊並嚴重影響工業生產，產業界應強化這類系統的資安防護能力。**

Otorio 在報告中指出，一個名為「GhostSec」的駭侵團體，於本（2022）年 9 月 4 日，在其社群媒體與 Telegram 平台宣稱成功駭入以色列境內多家製造業者所使用的 55 台 Berghof 可程式化邏輯控制器（Programmable Logic Controller, PLC）裝置。

GhostSec 公布了多段影片和畫面截圖，顯示該團體成功駭入受害 PLC 的管理介面，以及其連動的生產設備人機介面（Human-Machine Interface, HMI），以及某台 PLC 停止運作，導致相關生產流程停擺的畫面。

約在一周後，Otorio 再次發布資安通報，指出 GhostSec 於 9 月 10 日成功駭入另一家廠商的淨水設施；自該團體公布的畫面中可以看見，該團體取得某廠淨水系統的 PLC 控制權，可以任意設定用水 pH 值與氯含量。這個案例中遭駭的系統為 ProMinent 生產的 Aegis II 控制器。

在這兩次針對 ICS 與 PLC 的駭侵攻擊分析中，Otorio 發現這些曝露在 Internet 上的 PLC 非常容易透過 Shodan 搜尋引擎予以發現定位，其中更有許多裝置仍使用出場預設的登入帳密即可進入。研究也指出，進入 PLC 系統後雖然無法直接控制個別生產流程，但駭侵者仍可擁有某些功能的完整權限，因此仍可影響工業生產。

資安專家指出這類製造系統的資安防護普遍相當薄弱，因此企業不能只注重 IT 系統的資安防護，對於 OT（Operational Technology）的資安防護能力亦應提升。

- 資料來源：
  1. GhostSec Strikes Again in Israel Alleging Water Safety Breach
  2. Pro-Palestinian Hacking Group Compromises Berghof PLCs in Israel
  3. Hacktivist Attacks Show Ease of Hacking Industrial Control Systems

## 3.6.5、駭侵者透過 YouTube 遊戲破解教學影片散布惡意軟體


**資安廠商 Kaspersky 近期發現，有駭侵者大規模利用放在 YouTube 上的遊戲破解攻略教學影片，散布含有惡意程式碼的假冒破解程式，讓用戶下載安裝，藉以竊取用戶的機敏資訊，甚至利用受害者電腦進行加密貨幣挖礦。**

Kaspersky 發現駭侵者鎖定多種熱門電腦遊戲如 FIFA、Final Fantasy、Forza Horizon、Lege Star Wars、Spider-Man 等，製作遊戲攻略或破解教學影片，並在影片說明中放置連結，讓不明究理的玩家點按，並下載安裝假冒的破解程式。

Kaspersky 指出，在假冒的破解程式中，實際上含有一個名為「RedLine」的惡意軟體；用戶一旦安裝在自己的電腦上，RedLine 即會竊取儲存在電腦內的各種機敏資訊，包括瀏覽器中的 cookie、各種登入資訊、信用卡資訊、即時傳訊軟體中的對話內容，以及加密貨幣錢包相關資訊。

此外，該惡意軟體還會利用玩家電腦上的硬體資源來進行加密貨幣挖礦，為駭侵者賺取更多不法利益。

Kaspersky 表示，該惡意軟體擁有一個 NirCmd 公用程式，可以在不產生任何螢幕視窗的情況下偷偷執行應用程式，因此用戶難以察覺自己的電腦正在執行惡意軟體。

Kaspersky 也在報告中指出，RedLine 的特別之處，在於還能利用受害者用戶的瀏覽器 cookie 登入受害人的 YouTube 帳號，上傳含有惡意連結的遊戲攻略影片，甚至還會在社群討論區 Discord 的相關討論區中貼上影片觀賞連結，進一步擴大惡意軟體的散布。

建議遊戲玩家應避免在官方管道之外的任何地方，包括論壇、影音平台、社群平台等處下載破解版遊戲軟體、註冊機或其他破解程式，以免成為駭侵者的攻擊目標；另外也應注意自己在各社群平台或影音平台帳號，是否遭人盜用以發布任何內容。

- 資料來源：
  1. Self-spreading stealer attacks gamers via YouTube
  2. New malware bundle self-spreads through YouTube gaming videos

# 3.7、軟硬體漏洞資訊

## 3.7.1、資安專家利用分析工具，發現 Node.js 程式庫內超過 100 個 0-day 漏洞


**美國 Johns Hopkins 大學的兩位資安研究人員，近來在今（2022）年度的 Usenix Security Symposium 資安研討會上發表論文，指出該研究團隊利用全新開發的圖像式分析工具 ODGen 進行分析，發現廣為網頁開發人員使用的 JavaScript 開發框架 Node.js 開源程式庫內的程式碼，存有 100 個以上的 0-day 漏洞。**

這類圖像分析工具的運作原理，是分析程式碼，建立一個圖像架構，反映某應用程式中各種不同的單元及其執行分支，可以用來找出程式碼中的漏洞。這種分析工具能夠有效找出以某些程式語言撰寫程式碼內含的漏洞，例如 Code Property Graph (CPG) 即可有效運用於 C/C++ 與 PHP 程式碼的漏洞分析。

有鑑於 CPG 的運用成功，Johns Hopkins 大學的研究團隊也運用該原理，開發出運用於 JavaScript 程式語言的漏洞分析工具 ODGen，並且以此工具掃瞄 Node.js 這個廣受全球數百萬名開發人員歡迎，其程式庫已有數百萬種不同

套件的開源程式開發框架，結果發現了 180 個 0-day 漏洞。

該團隊提報這些 0-day 漏洞後，已經有 70 個漏洞取得 CVE 編號。

據研究團隊表示，ODGen 可以準確發現 13 種不同的漏洞類型，包括 XSS、SSRF/CSRD、SQL 指令注入、原型污染（Prototype Pollution）、指令注入等等。該團隊也利用此工具分析廣受使用的 30 萬種 NPM 開發套件，結果發現超過 3,000 種資安漏洞，其中有 264 種存於每周下載次數超過 1,000 次的熱門套件。

研究團隊表示，接下來將延伸 ODGen 支援的程式語言種類，以便支援其他經常用於網站開發的程式語言，包括 PHP 與 Java 在內。

- 解決方案：由於近年來在開源程式庫中發現的惡意與非惡意漏洞逐漸增加，開發人員在下載開源程式套件使用前，必須先確認該套件為最新版本，且未遭駭侵者修改並注入惡意程式碼。

- 資料來源：
  1. Mining Node.js Vulnerabilities via Object Dependence Graph and Query
  2. Graph-based JavaScript bug scanner discovers more than 100 zero-day vulnerabilities in Node.js libra

## 3.7.2、Apple 推出 iOS、macOS 更新，修復已遭駭侵者大規模濫用的 0-day 漏洞


**Apple 近日針對旗下推出的 iPhone、iPad 與 Mac 電腦等裝置，推出 iOS、iPadOS、macOS 作業系統更新，以修復一個已遭駭侵者大規模用於駭侵攻擊的 0-day 資安漏洞 CVE-2022-32917；用戶應立即更新。**

在這次更新中獲得修補的 0-day 漏洞，其 CVE 編號為 CVE-2022-32917，屬於作業系統核心中的邊界漏洞；駭侵者可以利用此漏洞誘發記憶體崩潰，並且提升執行權限，以便遠端執行任意程式碼。

CVE-2022-32917 的 CVSS 危險程度評分為 8.4 分（滿分為 10 分），危險程度評級為「高」；且根據 Apple 提供的資安通報指出，該漏洞顯然已遭駭侵者大規模用於攻擊活動。

Apple 針對此漏洞，推出 iOS 15.7、iPadOS 15.7、macOS Monterey 12.6 與 macOS Big Sur 11.7 加以修復；受到影響的 Apple 裝置包括 iPhone 6s 與後續機型、iPad Pro 所有機型、iPad Air 第 2 代與後續機型、iPad 第 5 代與後續機型、iPad mini 第 4 代與後續機型、iPod Touch 第 7 代、執行 macOS Big Sur 11.6 與先前版本、macOS Monterey 12.5 與先前版本的所有 Mac 機型。

CVE-2022-32917 是 Apple 自今（2022）年以來修復的第 8 個 0-day 漏洞。

建議廣大 iPhone、iPad 與 Mac 電腦用戶，在 Apple 推出作業系統更新且收到通知時，應立即依系統指示，更新到最新版的作業系統，以免遭到駭侵者利用已公開但未及更新的漏洞發動攻擊。

- CVE 編號：CVE-2022-32917
- 影響產品/版本：iPhone 6s 與後續機型、iPad Pro 所有機型、iPad Air 第 2 代與後續機型、iPad 第 5 代與後續機型、iPad mini 第 4 代與後續機型、iPod Touch 第 7 代、執行 macOS Big Sur 11.6 與先前版本、macOS Monterey 12.5 與先前版本的所有 Mac 機型。
- 解決方案：升級到最新版 iOS、iPadOS、macOS 作業系統版本。

- 資料來源：
  1. Apple 安全性更新
  2. Apple fixes eighth zero-day used to hack iPhones and Macs this year

## 3.7.3、Microsoft 推出 2022 年 9 月 Patch Tuesday 更新修補包，共修復 63 個漏洞


**Microsoft 於近日推出 2022 年 9 月的 Patch Tuesday 每月例行更新修補包，一共修復 63 個該公司旗下各種產品的資安漏洞，其中包括 5 個嚴重等級資安漏洞，更有 1 個已遭大規模用於駭侵攻擊；用戶應立即將使用中的 Microsoft 各種產品更新至最新版本，以避免遭駭侵者用於攻擊。**

以類型來區分，在這次 Patch Tuesday 得到修補的資安漏洞分別如下：

- 執行權限提升漏洞：18 個；
- 資安功能略過漏洞：1 個；
- 遠端執行任意程式碼漏洞：30 個；
- 資訊洩露漏洞：7 個；
- 服務阻斷攻擊漏洞：7 個；
- Edge - Chromium 瀏覽器組件漏洞：16 個。

本月的 Patch Tuesday 中同時修兩個已知的 0-day 資安漏洞，其中有一個

0-day 漏洞已遭駭侵者大規模用於攻擊；該漏洞的 CVE 編號為 CVE-2022-37969，存於 Windows Common Log 檔案系統驅動程式，駭侵者可用以提升執行權限，取得系統等級權限；已有多家資安廠商如 DBAPPSecurity、Mandiant、CrowdStrike、ZScaler 等發現駭侵者利用此漏洞發動攻擊活動。

另一個獲得修補的 0-day 漏洞是 CVE-2022-23960，屬於 Cache Speculation Restriction 漏洞。

此外，在這次 Patch Tuesday 中獲得修補的 5 個嚴重等級漏洞，有兩個存於 Microsoft Dynamics，兩個存於 Microsoft IKE Extension，另一個存於 Microsoft TCP/IP。

- 解決方案：建議 Microsoft 各種作業系統與軟體用戶暨系統管理員，應立即依各該軟體的更新流程，將之更新為最新版本，以免遭到駭侵者利用已公開卻未及更新的軟體漏洞發動攻擊。

- 資料來源：
  1. Security Update Guide
  2. Microsoft September 2022 Patch Tuesday fixes zero-day used in attacks, 63 flaws

# 第 4 章、 資安研討會及活動

| 【資安學院】10/12 雲端服務資訊安全及管控措施 | |
|---|---|
| **活動時間** | 10/12 9:30~16:30 |
| **活動地點** | 中華民國資訊軟體協會 訓練教室<br>（台北市大同區承德路二段 239 號 6 樓） |
| **活動網站** | https://dtu.cisa.tw/course.php?id=29 |
| **活動概要** | 中華軟協 資安學院<br>**雲端服務資訊安全及管控措施**<br>**主辦單位：中華民國資訊軟體協會**<br>課程說明：近年資訊及網路科技騰飛，國內外雲端服務提供商林立，為節省設備、人員及技術成本，越來越多企業選擇雲端，處理其資料儲存和運算等作業，但也衍生出相關資訊安全的議題及風險。本課程引用國際標準及法規要求，講解目前業界之實務作法，介紹雲端資料傳輸、資訊儲存等之必要之控制，雲端服務委外管理及資安事故回報等機制，採用互動式教學，以提升學員雲端資安風險分析及管理的能力。<br>活動聯絡人：廖資深專員<br>Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388 |

| 資安防護及案例分享研討會-嘉義場 | |
|---|---|
| **活動時間** | 10 月 12 日(三) 14:00~16:30 |
| **活動地點** | 大埔美精密機械園區 水資源回收中心 二樓會議室<br>(嘉義縣大埔美園區六路 1 號) |
| **活動網站** | https://docs.google.com/forms/d/e/1FAIpQLSf314bs2_j56isfh0Y34xuetmfOdgeFP1elT6CiEbgGi-4_LQ/formResponse |
| **活動概要** |  <br>**主辦單位：TWNIC、TWCERT/CC**<br><br>工控聯網浪潮來了 企業準備好了嗎?<br><br>製造業邁向工業 4.0 設備聯網智慧化，卻伴隨而來的資安威脅，將直接影響生產停擺，導致企業競爭力下降。透過本次研討會介紹台灣電腦網路危機處理暨協調中心(TWCERT/CC)免費資安通報的資源，並邀請專業講師探討製造業工控防護，提升員工資安知識，從觀念與預先防護，至遭受資安攻擊後處理方法，讓我們一同全方位掌握工控資安快速復原產線。<br><br>誠摯邀請您一同參與！<br>聯絡窗口：04-2242-1717 *242 黃小姐 eva@tcca.org.tw |

| 【資安學院】10/18 弱點修補技巧（VMS 弱點管理系統） | |
|---|---|
| **活動時間** | 10/18 14:00~17:00 |
| **活動地點** | 中華民國資訊軟體協會 訓練教室<br>（台北市大同區承德路二段 239 號 6 樓） |
| **活動網站** | https://dtu.cisa.tw/course.php?id=30 |
| **活動概要** |  <br>**主辦單位：中華民國資訊軟體協會**<br><br>課程說明：不論社交工程演練、弱點掃描、滲透測試等資安服務，目的皆是強化資安體質，在資訊安全管理的作業中，針對資訊資產的定期性的弱點評估已經是必要的日常工作。透過有效的弱點管理作業，可大幅降低企業資訊資產發生的潛在風險。本課程將教導學員如何針對發現系統弱點進行修補技巧，如果分析弱點掃描工具結果並判讀是否為誤判、並強化公司弱點管理是一個持續進行的過程，方便追蹤管理弱點修補情形，本課程將帶領您學習如何修正發現弱點、並依系統環境修補技巧。<br><br>活動聯絡人：廖資深專員<br><br>Email: security@cisanet.org.tw　Tel: (02)2553-3988 Ext：388 |

## IT 與 OT 下的智慧製造防護網

| | |
|---|---|
| **活動時間** | 2022 年 10 月 19 日 星期三 AM09:00 ~ PM17:00 |
| **活動地點** | 新竹豐邑喜來登大飯店 3F 宴會廳 |
| **活動網站** | https://www.informationsecurity.com.tw/seminar/2022_hightech/ |
| **活動概要** |  <br>**主辦單位：資安人**<br>台灣製造業產值在 2021 年達到了 24.33 兆元的高峰, 根據 IKE 的模型推估, 2022 年有望突破 25 兆, 其中高科技產業的產值占比將近快到一半, 可以看出台灣在全球扮演相當重要的角色。同時物聯網, 雲端, 5G 技術快速發展, 也促使製造業的全球化與智慧化轉型更加快速。<br>隨同數位轉型發展，鎖定製造業的資安攻擊及其相關地下經濟商機也快步成長。 這次地緣政治的網路攻擊, 也可以預知台灣高科技業將是駭客鎖定對象。 本次論壇資安人邀請了 10 家廠商, 探討高科技產業下一步在訂定資安的策略該如何從管理面思考, 透過主動防禦將威脅控制在最小的範圍, 了解最新的半導體標準, 以及分別從 IT 與 OT 的面向落實零信任。<br>聯絡洽詢：02-8729-1099 吳先生 分機 213<br>Light.Wu@taiwan.messefrankfurt.com<br>邀請對象：本活動免費報名參加，敬邀製造業管理職、IT 技術職、OT 技術職等資安相關職務人員踴躍報名參加。 |

| 提高社群平台透明度：多方利害關係人觀點 | |
|---|---|
| **活動時間** | 2022 年 10 月 25 日 , 14:00-16:00 |
| **活動地點** | IEAT 國際會議中心 8 樓綜合教室/Webex 會議室<br>*本活動採實體與線上同步進行 |
| **活動網站** | https://www.twsig.tw/20221025/ |
| **活動概要** |  <br>**主辦單位：TWNIC、Nii、TWIGF**<br>不實訊息、假新聞或虛假資訊在 2022 年度持續氾濫於社群平台，環繞著數個我們熟悉的幾個重大事件：裴洛西訪台、軍演、疫情與疫苗、美國選舉，以及俄烏戰爭等。隨著社會越來越依賴網路平台交流互動，從法律面要求網路平台資訊揭露，如付費廣告的標示、演算法運作模式的公開等，似已成為趨勢，目的是協助大眾認知訊息的來源或可能企圖，進一步理解不實訊息對公眾輿論的影響，並使平台業者對其作為（或不作為）負責。<br><br>例如，美國在過去 2 年陸續推出 8 項與要求社群平台提高透明度有關的法案，當中於去年底提出的《平台責任和透明度法案》（PATA）中，明確要求 Facebook、YouTube 和 Twitter 等平台業者與獲特定條件核准的研究人員分享內部資料；中國《互聯網信息服務算法推薦管理規定》在今年 3 月 1 日正式生效後，其監管機關在 8 月中即公布多家中國科技巨頭的演算法原理與目的清單，目的之一是要控制不正當的網路評論與輿論。而國內最受矚目的則是《數位中介服務法草案》，要求定義下的數位中介服務提供者應揭露或公告的資訊內涵，以及配合主管機關限制認定違法內容的存取等。 |

| | |
|---|---|
| | 這些不同法案各自有其目標，即便共同處是揭露資訊之透明度要求，各法所提議透明度的受眾、應揭露資訊種類，以及揭露程度也有差異。本座談將邀請不同專家與利害關係人，參考國際作法，就國內情境，針對社群平台業者的透明度受眾、哪些資訊應當透明化，以及透明度實施方式等面向，分別從其觀點分享並討論在法律規劃設計方面的重點或考量點，才能在顧及用戶隱私且保留言論自由的同時，也減緩社群平台上日益嚴重的極化問題。<br><br>議程<br>14:00-14:05 活動介紹<br>14:05-15:45 焦點座談<br>主持人 - 何吉森　教授（數位匯流研究學會）<br>與談人 -<br>曾更瑩律師（理律法律事務所）<br>葉志良教授（元智大學資訊傳播學系）<br>周冠汝　專員（台灣人權促進會）<br>15:45-16:00 現場問答 |

| 【資安學院】10/28 資訊安全與人工智慧實作 | |
|---|---|
| **活動時間** | 10/28 14:00~17:00 |
| **活動地點** | 中華民國資訊軟體協會 訓練教室<br>（台北市大同區承德路二段 239 號 6 樓） |
| **活動網站** | https://dtu.cisa.tw/course.php?id=31 |
| **活動概要** |  <br>**主辦單位：中華民國資訊軟體協會**<br>課程說明：各行各業正投資大量花費於資訊安全的工作上，而人工智慧(Artificial Intelligence, AI)可能成為構建更智能、更安全的系統解決方案之一。AI 讓資安工作者有能力檢測和預測網路中可疑的活動，例如：網站釣魚(web phishing)或未經授權的入侵(unauthorized intrusion)等威脅。透過機器學習(Machine Learning, ML)和人工神經網路(Artificial Neural Networks, ANNs)，您可以偵測潛在攻擊，並保護個人或公司資訊系統，瞭解如何在構建智能防禦機制時注入 AI 功能，包括垃圾郵件過濾、網路入侵檢測、botnet 理解和安全身份驗證等議題。<br>本課程「資訊安全與人工智慧實作(Hands-on Artificial Intelligence for Information Security)」從常見的八大網路攻擊談起，收斂到網路安全威脅偵測，以及敏感資訊與資產保護兩大方向。課程聚焦於資訊安全的案例實作，透過開源 Python 語言的演練，進行資安數據的探索、視覺化、分析與建模，協助學員打下資安人工智慧建模的扎實基礎。<br>活動聯絡人：廖資深專員<br>Email: security@cisanet.org.tw　Tel: (02)2553-3988 Ext：388 |

| 【資安學院】11/03、11/04 iPAS-「初級」資訊安全工程師-能力研習衝刺班 | |
|---|---|
| **活動時間** | 11/3-11/4 9:00~16:00 |
| **活動地點** | 中華民國資訊軟體協會 訓練教室<br>（台北市大同區承德路二段 239 號 6 樓） |
| **活動網站** | https://dtu.cisa.tw/course.php?id=32 |
| **活動概要** |  <br>**主辦單位：中華民國資訊軟體協會**<br>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。<br><br>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！<br><br>活動聯絡人：廖資深專員<br>Email: security@cisanet.org.tw　Tel: (02)2553-3988 Ext：388 |

| 【資安學院】11/18 行動應用 APP 安全檢測（APK/IPA） | |
|---|---|
| **活動時間** | 11/18 9:00~12:00 |
| **活動地點** | 中華民國資訊軟體協會 訓練教室<br>（台北市大同區承德路二段 239 號 6 樓） |
| **活動網站** | https://dtu.cisa.tw/course.php?id=33 |
| **活動概要** |  <br>**主辦單位：中華民國資訊軟體協會**<br><br>課程說明：知彼知己，百戰不怠。傳統 APP 安全的教學都只著重在防禦，卻無法有效阻擋駭客的攻擊，原因就在於不知道駭客攻擊的思維以及手法。本課程經由理論及實務的搭配，從攻擊者的角度出發，了解攻擊者的思維、目的以及手法，讓學員不僅從教學中了解 APP 的安全議題，更可以從實務中清楚了解其操作方法及運用。<br><br>活動聯絡人：廖資深專員<br>Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388 |

# 第 5 章、 TVN 漏洞公告

| 聯銓資訊科技 Smart eVision - Path Traversal -1 | |
|---|---|
| **TVN / CVE ID** | TVN-202209006 / CVE-2022-39033 |
| **CVSS** | 9.8 (Critical) |
| **影響產品** | Smart eVision ver.2022.02.21 |
| **問題描述** | Smart eVision 取得檔案之功能存在 Path Traversal 漏洞，該功能網址參數未進行特殊字元的過濾，遠端攻擊者不須權限，即可利用此漏洞繞過身分認證機制，下載並刪除任意系統檔案導致服務中斷。 |
| **解決方法** | 更新 Smart eVision 版本至 ver.2022.06.16 |
| **公開日期** | 2022-09-28 |
| **相關連結** | https://www.twcert.org.tw/newepaper/cp-151-6570-9c632-3.html |

| 聯銓資訊科技 Smart eVision - Improper Privilege Management | |
|---|---|
| **TVN / CVE ID** | TVN-202209005 / CVE-2022-39032 |
| **CVSS** | 8.8 (High) |
| **影響產品** | Smart eVision ver.2022.02.21 |
| **問題描述** | Smart eVision 存在 Improper Privilege Management 問題，遠端攻擊者以一般使用者權限登入後，即可利用未進行權限檢查的登入 API 功能，將帳號提權，得以獲得管理者權限，任意操作系統與中斷服務。 |
| **解決方法** | 更新 Smart eVision 版本至 ver.2022.06.16 |
| **公開日期** | 2022-09-28 |
| **相關連結** | https://www.twcert.org.tw/newepaper/cp-151-6569-9fcf4-3.html |

| 聯銓資訊科技 Smart eVision - Exposure of Sensitive Information to an Unauthorized Actor -2 | |
|---|---|
| **TVN / CVE ID** | TVN-202209003 / CVE-2022-39030 |
| **CVSS** | 7.5 (High) |
| **影響產品** | Smart eVision ver.2022.02.21 |
| **問題描述** | Smart eVision 系統資訊查詢功能授權不當，遠端攻擊者不須權限，即可利用該漏洞取得管理者的帳號密碼。 |
| **解決方法** | 更新 Smart eVision 版本至 ver.2022.06.16 |
| **公開日期** | 2022-09-28 |
| **相關連結** | https://www.twcert.org.tw/newepaper/cp-151-6567-01fa3-3.html |

| 聯銓資訊科技 Smart eVision - Path Traversal -2 | |
|---|---|
| **TVN / CVE ID** | TVN-202209007 / CVE-2022-39034 |
| **CVSS** | 6.5 (Medium) |
| **影響產品** | Smart eVision ver.2022.02.21 |
| **問題描述** | Smart eVision 報告之 API 功能存在 Path Traversal 漏洞，該功能網址參數未進行特殊字元的過濾，遠端攻擊者以一般使用者登入後，即可利用此漏洞繞過身分認證機制，下載系統檔案。 |
| **解決方法** | 更新 Smart eVision 版本至 ver.2022.06.16 |
| **公開日期** | 2022-09-28 |
| **相關連結** | https://www.twcert.org.tw/newepaper/cp-151-6571-fc930-3.html |

| 聯銓資訊科技 Smart eVision - Exposure of Sensitive Information to an Unauthorized Actor -1 | |
|---|---|
| **TVN / CVE ID** | TVN-202209002 / CVE-2022-39029 |
| **CVSS** | 6.5 (Medium) |
| **影響產品** | Smart eVision ver.2022.02.21 |
| **問題描述** | Smart eVision 資料庫查詢功能授權不當，遠端攻擊者以一般使用者的權限登入後，即可利用該漏洞取得管理者的帳號密碼。 |
| **解決方法** | 更新 Smart eVision 版本至 ver.2022.06.16 |
| **公開日期** | 2022-09-28 |
| **相關連結** | **https://www.twcert.org.tw/newepaper/cp-151-6566-3805b-3.html** |

# 第 6 章、 2022 年 9 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。

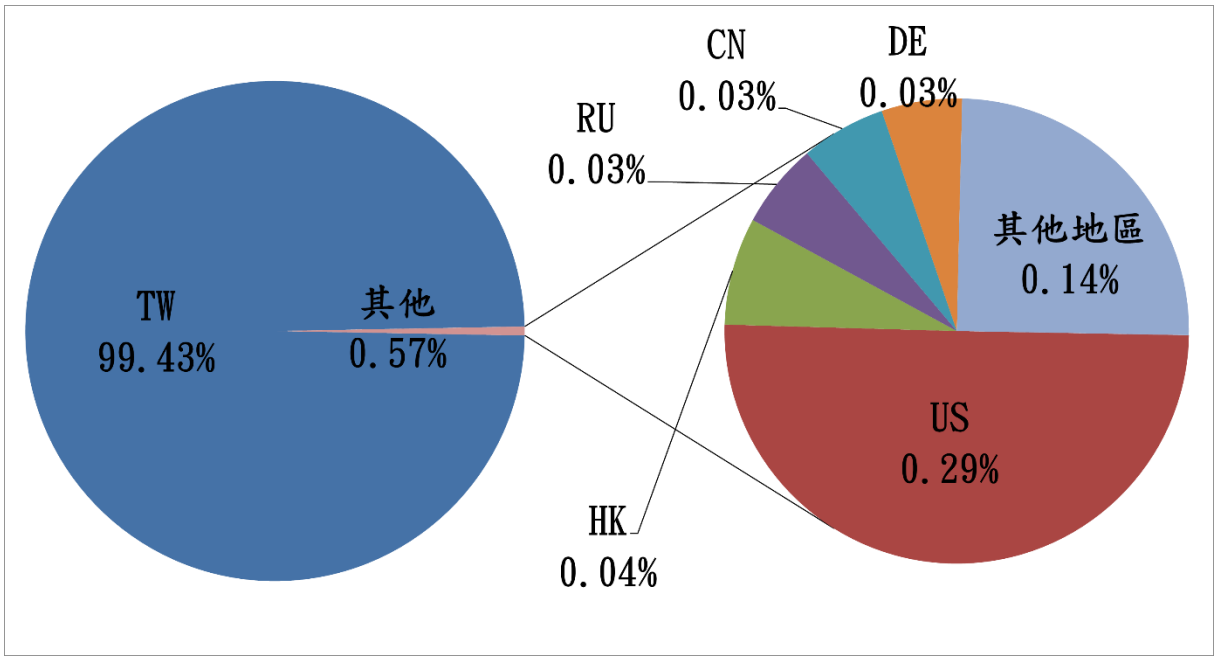



圖 1、分享地區統計圖

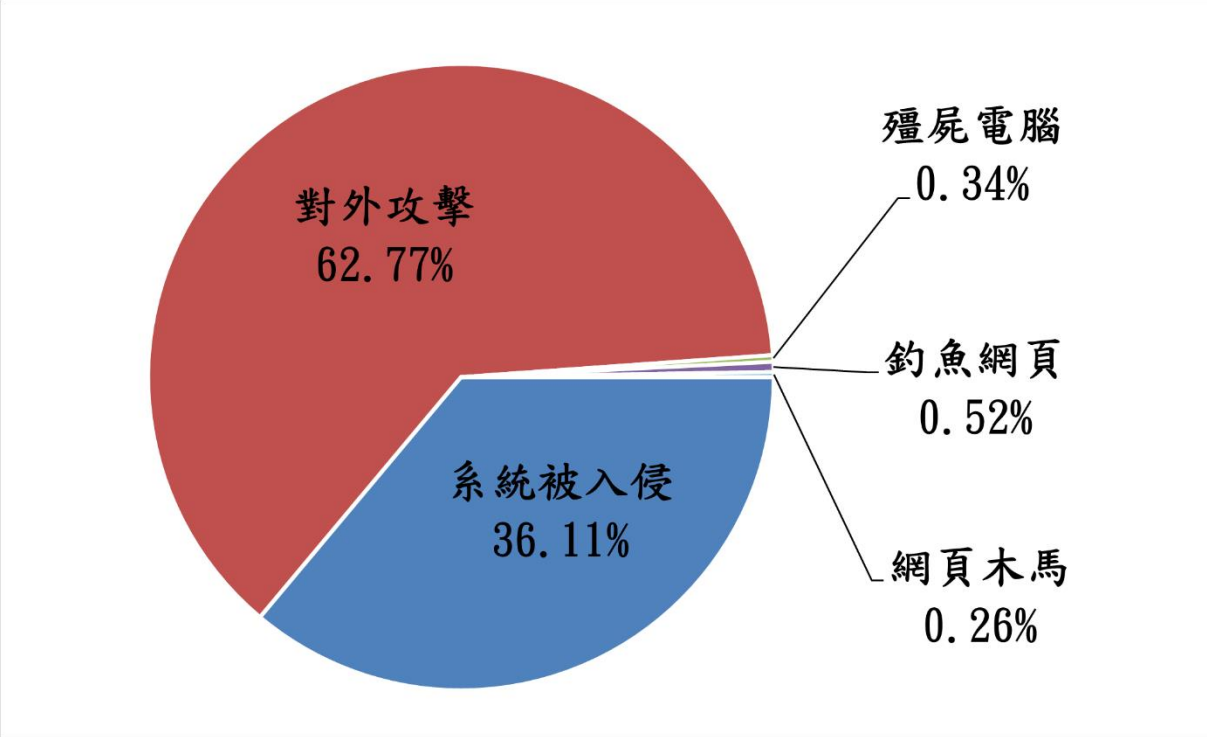



圖 2、分享類型統計圖

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 10 月 7 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**