TWCERT/CC 資安情資電子報

2022 年 4 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 6 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 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

數百款 HP 印表機內含遠端執行任意程式碼漏洞，恐成攻擊目標

全球最大印表機品牌廠商 HP，日前發表資安通告，公布旗下有數百種各式印表機，內含一個嚴重資安漏洞 CVE-2022-3942，可導致駭侵者遠端執行任意程式碼。

該漏洞最初是由資安廠商趨勢科技旗下的 Zero Day Initiative 團隊發現，屬於緩衝區溢位錯誤，發生在「Link-Local Multicast Name Resolution（LLMNR)」功能；駭侵者可以藉由誘發此錯誤，進而遠端執行任意程式碼。

這個漏洞的 CVSS 危險程度評分為 8.4 分，原本的危險程度分級應為「高」，但在 HP 發表的資安通報中則分級為「嚴重」（Critical）。

含有這個漏洞的 HP 印表機款式極多，包括 LaserJet Pro、PageWide Pro、OfficeJet、Enterprise、Large Format DesignJet 與桌上型噴墨印表機 DeskJet 等機種，有數百款之多。

HP 已針對大多數受此漏洞影響的印表機機種，提供更新版韌體，以修補此一漏洞；不過也有相當數量機種，因為年代久遠，已不提供支援；針對這類產品，HP 亦提供操作步驟，用戶可至印表機管理介面中，依設定指南指示，停用 LLMNR 功能。

HP 各型印表機用戶可至 HP 發表的資安通報中，檢視自己擁有的機種是否列於名單之中，再採取行動處理漏洞問題。

HP 在另一篇資安通報中，也揭露了另外三個可能存於多款印表機中的資安漏洞，分別為 CVE-2022-24291、CVE-2022-24292、CVE-2022-24293，其中後兩者的 CVSS 分數高達 9.8 分（滿分為 10 分）；用戶同樣應立即更新至最新版本韌體，以修補最近發現的各種漏洞。

- CVE 編號：CVE-2022-3942
- 影響產品(版本)：請參考 HP 資安通報中的列表。
- 解決方案：升級到最新版本韌體，或是依指引關閉 LLMNR 功能。

- 資料來源：
  1. Certain HP Print Products, Digital Sending Products – Potential remote code execution and buffer ove
  2. Certain HP Print Products – Potential information disclosure, denial of service, remote code executi
  3. Hundreds of HP printer models vulnerable to remote code execution

第 2 章、 資訊安全宣導

俄羅斯相關之資安產品可能引發資安議題，建議採取對應措施以降低風險

據國外媒體報導，俄羅斯相關之資安產品可能引發資安議題，建議採取對應措施以降低風險

據國外媒體報導，部分俄羅斯相關之資安產品與設備可能主動或被迫對他國系統發動攻擊，或在使用者不知情之情況下因網路攻擊而遭竊聽，為避免不必要之資安風險，建議您如有使用相關產品，立即採取以下措施：

(1)清查所使用之資安產品與設備，並評估未來更換其他軟體或功能之設備。

(2)密切觀察防火牆紀錄，查看系統、對外服務是否進行異常連線，若發現異常連線，建議移除產生異常連線之程式，並立即回報 TWCERT/CC (twcert@cert.org.tw)

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、資安廠商指出，8 個字元長度的複雜密碼，最新繪圖卡僅需一小時即可破解

資安廠商指出，運用市場上最新的強大繪圖卡，來進行密碼 MD5 比對，駭侵者將能在 1 小時內破解包含大小寫字母與數字的 8 字元密碼。

資安廠商 HIVE SYSTEMS 日前發表研究報告指出，運用市場上最新的強大繪圖卡，來模擬進行密碼 MD5 比對，駭侵者將能在 1 小時內破解包含大小寫字母與數字的 8 位數字元密碼。

HIVE SYSTEMS 的報告中指出，由於當代繪圖卡上的繪圖處理器計算能力大幅提升，因此能在更短的時間內，利用暴力試誤法與 MD5 雜湊值比對，快速破解字元數不足或複雜度不足的密碼。

舉例來說，同樣是 8 個字元，含有大小寫英文字母、特殊符號與數字的密碼，使用 2020 年時的高效能繪圖卡（內建 NVIDIA RTX 2080 繪圖處理器），需要耗費 8 小時才能破解；但在現今使用最新高效能繪圖卡（內建 NVIDIA RTX 3090 繪圖處理器），則只需要 5 個小時。

除了使用現今的主流繪圖卡外，HIVE SYSTEMS 也使用目前處理速度最快的雲端運算服務，使用 8 個 NVIDIA A100 Tensor Core 繪圖處理器的 Amazon 高效能運算叢集來進行模擬破解，結果顯示，同為 8 個字元，含有大

小寫英文字母、特殊符號與數字的密碼，只花了 39 分鐘就成功破解。

HIVE SYSTEMS 的報告也指出，若將密碼以較強的 bcrypt salting 方式進行加密，使用上述 Amazon 高效能雲端運算服務，破解同為 8 個字元，含有大小寫英文字母、特殊符號與數字的密碼，將需時 36 年。

不過報告也指出，如果用戶使用的密碼在多個服務中使用相同密碼，因而曾遭外洩的話，即使是長達 18 個字元，且混雜使用大小寫字母、數字與特殊符號，都會立即遭到破解。。

- 資料來源：
  1. Are Your Passwords in the Green?
  2. New research from Hive Systems finds any 8-character password can be cracked in less than an hour

3.1.2、DDoS 僵屍網路、加密貨幣挖擴惡意軟體，仍大量使用 Log4Shell 漏洞

資安廠商發表研究報告，指出去年年底發現的 Log4Shell 漏洞，目前仍有駭侵者大量用於發動各式攻擊。

資安廠商 Barracuda 日前發表研究報告，指出去（2021）年年底發現的 Log4Shell 漏洞，目前仍有駭侵者大量用於發動各式攻擊；其中最大宗的攻擊手法是用於建置可發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）的僵屍網路（botnet），以及植入加密貨幣惡意挖礦程式。

據 Barracuda 報告，該公司觀察到數個月以來透過 Log4Shell 漏洞的攻擊中，來源 IP 最多的是美國，高達 83%，其次是日本（10%）、德國與荷蘭（3%）、俄羅斯（1%）。

儘管在去（2021）年年底爆發 CVE-2021-44228「Log4j」漏洞時，負責開發 Log4j 的 Apache 基金會，一連推出了多個修正版本，直到 2.17.1 版本後就徹底解決了 Log4Shell 漏洞，但全球仍有大量裝置仍在執行存有漏洞的舊版 Log4j 軟體，導致利用此漏洞發動的資安攻擊，次數仍然居高不下。

據 Barracuda 報告指出，在眾多仍然透過 Log4Shell 漏洞發動攻擊的惡意軟體中，Mirai 僵屍網路佔的數量比例最高，其次是 BillGates malware（DDoS）、Kinsing（挖礦軟體）、XMRig（挖礦軟體）、Muhstik（DDoS）等。

另外，在 Apache 推出資安修補後，Barracuda 仍然觀察到相當多的駭侵行動透過 Log4Shell 發動，其次數並未在修補軟體推出後呈現下降趨勢。

Barracuda 指出，雖然大型駭侵團體使用 Log4Shell 漏洞的比例有降低的趨勢，但仍有許多透過該漏洞的攻擊行動，表示仍有許多中小型的駭侵團體，持續鎖定尚未修補 Log4Shell 的目標發動攻擊。

- 資料來源：
  1. Threat Spotlight: Attacks on Log4Shell vulnerabilities
  2. Log4shell exploits now used mostly for DDoS botnets, cryptominers

3.1.3、透過 API 進行的資安駭侵攻擊，2021 年大增 681%

資安廠商 Salt Security 旗下的資安研究人員，日前發表研究報告，指出在 2021 年間，透過 API 進行的各式資安攻擊，較 2020 年增加了 681%。

根據該報告指出，Salt Security 觀察到的各種 API 呼叫中，正常目的的 API 呼叫次數成長了 321%，但用於惡意資安駭侵攻擊的 API 呼叫則成長了 681%，呈現完全不成比例的巨幅增加。

API（Application Programming Interfaces）是許多網路與軟體服務相互溝通、交換資料的介面；為確保資料傳輸過程的安全性，通常必須要有強度足夠的安全認證與傳輸加密；不過顯然在這方面仍有許多尚待補強之處，才導致各種 API 駭侵攻擊以如此高的速度成長。

報告指出，不安全的 API 介接、認證與傳輸流程，可能導致多種形態的駭侵攻擊，包括分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）、SQL 指令注入、中間人攻擊（Man-in-the-middle attack）、惡意軟體感染擴散，以及不當登入與資料存取等。

Salt Security 也指出，多數 API 的開發流程中的資安保護，有嚴重的資源錯置問題。據該公司的報告指出，多家公司對 API 的資安保護資源，往往集中在設計規畫（47%）、測試（59%）與初期部署（26%）階段；在該 API 正式上線運作後，多數公司並未針對 API 的執行安全性投注足夠資源（僅有 26%)，但絕大多數透過 API 的資安攻擊，都發生在 API 上線運作後的 Runtime 階段。

- 資料來源：
  1. Companies are Struggling Against a 681% Increase in API Attacks, the Latest “State of API Security”
  2. Attacks abusing programming APIs grew over 600% in 2021

3.2、新興應用資安

多組駭侵者假借金援烏克蘭為由，設立加密貨幣詐騙捐款專戶

在烏俄交戰之際，開始有駭侵者設立假冒的烏克蘭政府捐款帳戶，利用各種管道詐騙不知情用戶捐給烏克蘭的加密貨幣。

烏克蘭政府於日前公開設立官方的加密貨幣捐款方式，並且呼籲全球踴躍捐款，以加密貨幣援助烏克蘭對抗俄羅斯的入侵；目前已成功募得約 3,700 萬美元的加密貨幣捐款。

正因該捐款活動十分熱烈成功，在短期間內就為烏克蘭政府募得相當多的資金，因此近來開始有多組不法分子，在網路上透過各種管道，包括釣魚網頁、論壇貼文、垃圾郵件等方式，假冒為烏克蘭政府的募款專戶，引誘不查的用戶轉帳到指定的加密貨幣錢包。

據各方資安專家與媒體收集到的資訊表示，這些貼文多半都會以聳動的文句來試圖打動同情烏克蘭處境的網友，促使他們將捐款轉到詐騙集團設立的加密貨幣錢包；也有資安專家指出，包括 savelideinukraine.app-en.com、donateukarine.sbs、shelterukarine.org、UkarineGlobalAid.com 等，都是詐騙集團設立的假網站。

事實上烏克蘭政府在 Twitter 上經過認證的官方帳號，貼出了官方收取比特幣、以太幣、USDT 等加密貨幣的捐款錢包網址，但仍有人擔心該國官方 Twitter 帳號可能遭駭侵者盜用，因為先前亦有多位經過官方認證的 Twiiter 名人與重要組織帳號曾遭駭侵者盜用於加密貨幣詐騙。

資安專家呼籲用戶，如果要進行加密貨幣捐款給烏克蘭或任何組織，必須先確認訊息來源確實來自可信賴的官方管道，以免愛心遭到濫用。

- 資料來源：
  1. Ukraine / Україна @Ukraine
  2. Tom Strickland @TomStri68606037
  3. 'Help Ukraine' crypto scams emerge as Ukraine raises over $37 million

3.3、國際政府組織資安資訊

3.3.1、俄羅斯公布涉及針對境內單位進行 DDoS 攻擊的 17,576 個 IP 名單

俄羅斯政府公布一批涉及對該國各個公私網站，進行分散式服務阻斷攻擊的 IP 清單。

俄羅斯政府日前公布一批涉及對該國各個公私網站進行分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）的 IP 清單，共有多達 17,576 個 IP。

這批 IP 清單是由俄羅斯聯邦特別勤務局（FSB）旗下的國家資安事件處理協調中心（NKTsKI）所發表的，除了一份只含有 IP 的清單外，另外也發表了一份含有網域名稱的攻擊來源清單。

這兩份攻擊者清單中只含有攻擊來源的 IP 與對應的網域名稱，並未包含幕後攻擊者的相關資訊，而且在網域清單中赫然出現多個歐盟與美國政府官方單位的網域名稱（例如美國聯邦調查局與美國中央情報局）；但資安專家也提醒，攻擊者可以透過更改封包推薦連結表頭資訊的簡單技巧，輕易將攻擊來源改為任何特定目標。

另外，這份清單中也包括一個網址，指向一個 Google 文件檔案，內容是教導用戶如何利用開源的「低軌道離子砲」（Low Orbit Ion Cannon, LOIC）駭侵工具，對俄羅斯境內的網站發動 DDoS 攻擊，加入聲援烏克蘭「IT 軍種」資訊作戰的行列。該工具廣泛支援多種作業系統，包括 Windows、macOS、iOS、Android。

NKTsKI 針對日漸嚴重的 DDoS 攻擊，呼籲俄羅斯網站應採行以下四個方式，加強己身對抗 DDoS 等資安攻擊的防護能力，包括使用 DDoS 防護服務、將上述表單中的攻擊來源設為連線黑名單、停用各種用來進行流量統計或其他功能的網站外掛程式，以及僅使用設於俄羅斯境內的 DNS 伺服器等。

- 資料來源：
  1. IP
  2. DN
  3. НКЦКИ: рекомендации по защите информационных ресурсов от компьютерных атак
  4. Russia shares list of 17,000 IPs allegedly DDoSing Russian orgs

3.3.2、希臘國營郵局遭勒贖攻擊，郵件遞送服務停擺

希臘國營的 ELTA 郵政服務，日前發表資安通報指出，該單位因遭勒贖攻擊，多數營運單位無法運作，造成郵務停擺。

ELTA 近日共發出兩次資安通報，在第一次發布的通報中指出攻擊發生於本周一（2022.03.21）；通報也指出服務中斷的原因，並表示該單位已立即針對攻擊事件進行處理，包括將整個資料中心離線，以儘速恢復運作。

隔日 ELTA 再度發布第二次資安通報，該單位除了提供更多攻擊相關詳情外，也對客戶提供更完整的服務受阻範圍。

同時，該單位的 IT 團隊也確認，駭侵者係利用該單位電腦系統中一個尚未修補的漏洞來植入惡意軟體，以透過 HTTPS reverse shell 來存取系統中的工作站；通報也指出，該單位認為駭侵者的目的，是要將 ELTA 所屬的關鍵企業營運系統予以加密。

不過 ELTA 的資安通報中，並未提供詳細細節，包括駭侵者、使用的勒贖軟體、駭侵者要求的贖款額度等具體資訊，目前仍不為外界所知。

另外，多數的勒贖攻擊案件中，多半也會附有資料竊取的攻擊手法，因此資安專家也懷疑這次攻擊行動，可能也有顧客個資、地址、付款資訊等重要資料外洩的問題，但這同樣也尚未得到 ELTA 證實。

目前 ELTA 有多項服務陷入無法運作的狀態，除了暫停收送郵件外，各種帳單支付或交易訂單也都無法處理；ELTA 也沒有提供服務恢復正常的預估時間。而到目前為止，該單位的官網連結也都無法存取。

- 資料來源：
  1. ΑΝΑΚΟΙΝΩΣΗ - Τρίτη 22 Μαρτίου 2022
  2. Greece's public postal service offline due to ransomware attack

3.3.3、FBI：2021 年全美因網路犯罪造成的損失，高達 69 億美元以上

美國聯邦調查局發表 2021 網路犯罪年度報告，指出去年全美因為各式網路犯罪，造成的總體損失高達 69 億美元以上。

美國聯邦調查局（Federal Bureau of Investigation）日前發表 2021 網路犯罪年度報告（Internet Crime Report 2021），指出去年全美因為各式網路犯罪，造成的總體損失高達 69 億美元以上。

這份報告指出，2021 年，該局旗下的「網路犯罪申訴中心」（Internet Crime Complaint Center, IC3）一共接獲 847,376 筆網路犯罪相關報案，和 2020 年相比，增幅為 7%，但若與 2019 年相比，案件數量則大增 81%。相關網路犯罪造成的損失，在 2020 年為 20 億美元，2021 年也增加超過三倍。

報告也指出，在 2021 年報案次數最多的三類網路犯罪，分別為釣魚詐騙、貨物未送達或應付帳款未付，以及個資外洩。

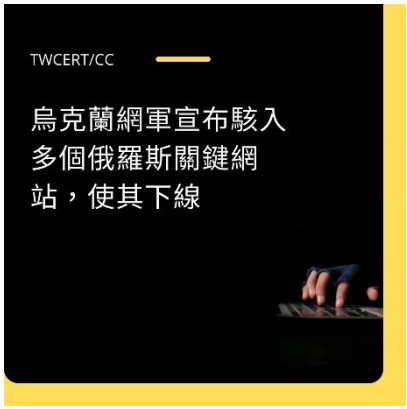
報告也說，去年有多達 649 個美國關鍵基礎設施，向 FBI 提報遭到勒贖攻擊；其中醫療與公衛部門遭到的勒贖攻擊最為嚴重，高達 148 個案件，其次為金融機構（89 次）、資訊科技（74 次）、關鍵製造業（65 次）、政府相關機構（60 次）、商業相關機構（56 次）、糧食與農業（52 次）、交通運輸（38 次）、能源（31 次）、通訊（17 次）、化學與化工（12 次）、供水與廢水處理系統（4 次）、緊急服務（2 次）、國防工業基地（1 次）。

FBI 也指出，針對美國關鍵基礎設施發動勒贖攻擊的駭侵團體，主要為 CONTI（87 次）、LockBit （58 次）、 REvil/Sodinokibi（51 次）。

FBI 說，該局不贊成受勒贖單位支付贖金，因為即使付了贖款，也未必能確保遭駭資料可以取回且不被外洩；而駭侵團體更會食髓知味，針對更多目標發動更多勒贖攻擊。

- 資料來源：
  1. Internet Crime Report 2021
  2. Internet Crime Cost People More Than $6.9B in 2021, FBI Says
  3. FBI: Ransomware hit 649 critical infrastructure orgs in 2021

3.3.4、烏克蘭網軍宣布駭入多個俄羅斯關鍵網站，使其下線



烏克蘭政府日前宣布，作為烏克蘭對抗俄羅斯入侵戰爭的反抗，軍方所屬的網路作戰單位，已經「攻下」俄羅斯多個重要網站，使其無法運作。

烏克蘭於 2 月 26 日發布通告成立「IT 軍種」，徵求全球駭客加入，以資安攻擊手法協助烏克蘭在網路上對抗入侵該國的俄羅斯；烏克蘭同時列出 31 個俄羅斯官方與私營重要目標，包括政府機構、關鍵基礎設施、金融機構等。

烏克蘭數位發展部長 Mykhailo Fedorov 也在 Twitter 上公開徵求全球資安高手加入該國 IT 軍，並鼓勵大家加入一個新設立的 Telegram 討論群組；所有命令與工作都會透過該群組發布。

據資安廠商 Cyber Unit Technologies 的創辦人 Yegor Aushev 指出，每天都有數百名全球各地資安高手申請加入該群組，甚至也有俄羅斯駭客表示願意為烏克蘭 IT 軍效勞。

而在烏克蘭 IT 軍成立數日後，烏克蘭便表示已成功駭入多個俄羅斯與白俄羅斯公私網站，包括 sberbank.ru、vsrf.ru、scrf.gov.ru、kremlin.ru、radiobelarus.by、rec.gov.by、sb.by、belarus.by、belta.by、tvr.by 等網站均已無法運作。

另外，也有獨立的駭侵團體加入攻擊俄羅斯與白俄羅斯網站的行動；一個名為 Cyber Patisans 的白俄羅斯駭侵團體，宣稱已經成功阻擾白俄羅斯的鐵路交通，以減慢俄羅斯軍隊的運補作業。

- 資料來源：
  1. Mykhailo Fedorov @FedorovMykhailo
  2. ‘If Kyiv Falls, We Keep Hacking Putin’: On The Cyber Front Line In Ukraine
  3. Спільно із кіберволонтерами кіберполіція продовжує атакувати вебресурси агресора
  4. Ukraine says its 'IT Army' has taken down key Russian sites

3.3.5、以色列政府網站疑似遭受駭客組織 DDoS 攻擊

以色列政府日前受到大規模的分散式阻斷服務攻擊，導致多個以色列政府網站無法提供服務。

以色列政府在 3 月 14 日受到大規模的分散式阻斷服務攻擊(distributed denial-of-service attack, DDoS)，導致多個以色列政府網站無法提供服務，包括衛生部、司法部、福利部以及總理辦公室都受到影響。

駭客攻擊使用.GOV.IL 網域名稱的網站，適用於除國防相關以外的所有政府網站，該國政府資料庫也使用此網域名稱。

據以色列《國土報》報導，該國國防機構一位消息人士認為，這是有史以來針對以色列發起的最大規模的網路攻擊。他們認為可能是由某國家的駭客組織實施了本次的網路攻擊，但尚無法確定誰是幕後黑手。

以色列國防機構和國家網路局宣布進入緊急狀態並研究破壞程度，同時檢查該國戰略網站和基礎設施是否有遭受攻擊。該國通信部部長及官員也緊急召開會議，對緊急服務部門進行評估，電信公司也在本次襲擊案不久後努力讓被擊破的網站重新上線，目前網站皆已恢復正常營運。

- 資料來源：
  1. Israeli Government Sites Crash in Cyberattack
  2. Israeli Government Websites Crash in Suspected Cyberattack
  3. Israel says government sites targeted by cyberattack

3.4、社群媒體資安近況

3.4.1、俄烏開戰後，眾多網路犯罪分子透過 Telegram 進行各式不法資安活動

資安廠商發表研究報告，發現有許多駭侵者與網路犯罪分子，開始大量利用端對端加密的即時傳訊服務 Telegram，用以進行各種不法資安活動。

資安廠商 Check Point 日前發表研究報告，指出該公司發現在俄羅斯發動對烏克蘭的入侵作戰後，有許多駭侵者與網路犯罪分子，開始大量利用端對端加密的即時傳訊服務 Telegram，用以進行各種不法資安活動，用戶應特別提高警覺。

Check Point 在報告中指出，在 2022 年 2 月 24 日至今，在 Telegram 上的聊天群組數量暴增達 6 倍之多。

此外，某些特定主題的聊天群組，其參加人數也有大量增加的情形；某些聊天群組的成員數甚至多達 250,000 人以上。Check Point 觀察到以下三種主題的聊天群組，在俄羅斯入侵烏克蘭後，參與人數成長最快：

- 志願參與協助烏克蘭進行網路作戰，對俄國各公私網站進行 DDoS 與其他類型的駭侵攻擊；
- 宣稱為金援烏克蘭而進行的加密貨幣募捐；
- 各種宣稱提供可信賴前線作戰訊息的「新聞頻道」。

其中有一個對俄羅斯進行駭侵攻擊的群組，名為「烏克蘭 IT 軍」（IT

Army of Ukraine），其成員多達 270,000 人。在此群組中除了討論各種針對俄羅斯的網路攻擊事宜之外，甚至會揭露俄羅斯作戰重要決策者的個人相關資訊。

另外也有許多表面上宣稱為烏克蘭募款，實際上進行加密貨幣詐騙活動的群組，在 Telegram 上大量出現，有些群組成員多達 20,000 人以上。

至於所謂提供各種可信賴第一手戰地消息的 Telegram 群組，其中大多數的訊息、照片和影片，多半未經證實，甚至有許多是敵對雙方用以擾亂對手民心士氣用的假訊息。近日還有熱心鄉民誤將電玩畫面當做烏軍擊落俄羅斯戰機的影片，這類影片甚至也大量流傳到各種媒體之上。

資安專家呼籲用戶，在 Telegram 上不要輕易加入不明群組，勿點按不明連結，也不要分享未經證實的消息或影像到其他社群平台上。。

- 資料來源：
  1. Tele becames a digital forefront in the Conflict
  2. Hacktivists, cybercriminals switch to Telegram after Russian invasion

3.4.2、2021 年假冒各大品牌的釣魚攻擊，以社群媒體為最頻繁的類型

資安廠商在統計報告指出，針對社群媒體發動的釣魚攻擊，在去年時超過其他管道，在攻擊量上達到史上最高記錄。

資安廠商 Vade 日前發表釣魚攻擊相關統計報告，在報告中指出，針對社群媒體發動的釣魚攻擊，在去（2021）年時超過其他管道，在攻擊量上達到史上最高記錄。

在這份報告中，自 2021 年 1 月 1 日至 12 月 31 日之間，Vade 一共觀察到多達 184,997 個釣魚攻擊用的詐騙頁面，統計出 20 大最常遭到釣魚攻擊者假冒的品牌；其中假冒社群媒體的比例首次比其他類別品牌要多。

前 20 名最常遭到駭侵者假冒，用以發動釣魚攻擊的品牌，與其類別如下：

- Facebook（社群媒體）
- Microsoft（軟體與雲端服務）
- Crédit Agricole（金融服務）
- WhatsApp（社群媒體）
- La Banque Postale（金融服務）
- Orange（電信服務）
- Amazon（電子商務）

- Chase（金融服務）
- Comcast（電信服務）
- PayPal（金融服務）
- DHL（電子商務 / 物流）
- Netflix（雲端服務）
- Wells Fargo（金融服務）
- Rakuten（電子商務）
- Adobe（雲端服務）
- OVH（電信服務）
- LinkedIn（社群媒體）
- MTB（金融服務）
- Apple（電子商務）
- Yahoo（網路服務）

Vade 指出，釣魚攻擊者最喜歡假冒全球知名的大品牌來發動攻擊，比較容易取得受害者的信任因而上鉤。

在 Vade 的報告中也指出，釣魚攻擊者針對企業員工發動的釣魚攻擊，手法也日益成熟；而主要的目標是騙取企業員工使用的 Microsoft 365 帳號。

- 資料來源：
  1. Phishers' Favorites
  2. Social media phishing attacks are at an all time high

3.5、行動裝置資安訊息

3.5.1、TeaBot 再次出現在 Google Play Store ，目標鎖定美國用戶進行金融駭侵攻擊

資安廠商發表研究報告，指出，以金融相關攻擊為主的 TeaBot 木馬惡意軟體，現在又在 Google Play Store 中出現，主要攻擊美國的 Android 用戶。

資安廠商 Cleafy 旗下的資安研究人員，日前發表研究報告，指出之前曾在 Google Play Store 中出現，以金融相關攻擊為主的 TeaBot 木馬惡意軟體，現在又在 Google Play Store 中出現，主要攻擊美國的 Android 用戶。

報告指出，TeaBot 這次是藏身在一支名為「QR Code & Barcode - Scanner」的 App 中，之前這個惡意木馬軟體，也曾在一月時出現在 Google Play Store 中，當時相關軟體曾遭 Google 下架，事隔一個多月後又再度出現。

研究人說，TeaBot 的幕後駭侵團體，似乎找到了再次混入 Google Play Store 的有效方法；該單位認為駭侵者在首次上架軟體時，提供的是不含惡意程式碼，且具備所宣稱正常功能，且要求權限不多的版本；這不但可以騙過 Google Play Store 的審核，同時也能幫 App 累積相當多的正面評價。

一但用戶自 Google Play Store 中安裝了看似正常的 QR Code & Barcode - Scanner 後，接著該 App 會自外部連結下載更新版本，而這個外部連結，就是位於 Github 上的惡意軟體程式碼；會有一個名為「QR Code Scanner: Add-On」的新 App 安裝到用戶手機上，其中就內含 TeaBot 木馬惡意軟體。

該 App 接著會向用戶要求各種輔助使用權限，以便截取用戶的螢幕顯示畫面中的各種雙重驗證碼、簡訊內容等等，還會自動打開各種權限，開始攔截用戶通訊內容中的各種金融相關關鍵字，包括網路銀行、保險、加密貨幣錢包、加密貨幣交易所等。

- 資料來源：
  1. TeaBot is now spreading across the globe
  2. TeaBot malware slips back into Google Play Store to target US users

3.5.2、一支專門竊取帳密的 Android 惡意軟體，已感染 100,000 名 Google Play 用戶

資安廠商 Pradeo 旗下的資安研究人員，日前發現一支名為 Craftsart Cartoon Photo Tools，會竊取用戶 Facebook 登入資訊的惡意 Android 軟體。

資安廠商 Pradeo 旗下的資安研究人員，日前發現一支名為 Craftsart Cartoon Photo Tools，會竊取用戶 Facebook 登入資訊的惡意 Android 軟體；該軟體不但成功在 Google Play 中上架，也已感染超過 10 萬名用戶。

這支 Craftsart Cartoon Photo Tools 宣稱的功能，是可以把用戶的照片變成卡通漫畫風格的圖片；該 App 執行時會跳出看起來很像 Facebook 登入畫面的界面，並要求用戶輸入其 Facebook 帳號與密碼；一旦用戶輸入後，藏身在 App 中的木馬惡意軟體 FaceStealer 即會竊取該登入資訊，並且傳送到某台駭侵者指定的控制伺服器。

除了連線到控制伺服器外，該惡意 Android App 還會連到另一台伺服器以傳輸竊得的資料；該伺服器過去也曾用來推送其他內含 FaceStealer 的惡意 Android App。

資安廠商表示，駭侵者似乎已經開發出可用的技術，可以先將原本無害的 App 上架到 Google Play Store 中，並且通過上架前的各種檢查；待 App 成功上架後，再透過更新的方式，把一小段惡意程式碼注入到 App 中，造成下載該 App 的用戶裝置遭到攻擊。

另外，該駭侵者在 Google Play Store 提供的資訊中，將開發公司名稱故意設定為「Google Commerce LTD」，也有誤導用戶，以為該軟體為 Google

官方開發的意圖。

- 資料來源：
  1. Spyware dubbed Facestealer infects 100,000+ Google Play users
  2. Android password-stealing malware infects 100,000 Google Play users

3.5.3、金融惡意軟體 SharkBot 在 Google Play Store 中假扮為防毒工具

資安廠商 NCC Group 發現一個名為 SharkBot 的金融惡意軟體，近日被發現藏身在假扮為 Android 防毒工具的 App 中。

資安廠商 NCC Group 日前發現一個名為 SharkBot 的金融惡意軟體，近日被發現藏身在假扮為 Android 防毒工具的 App 中，出現在 Google Play Store 內，意圖魚目混珠，誘使用戶安裝下載。

NCC Groups 在其發表的研究報告中指出，自去年（2021）以來該公司與全球資安研究人員，陸續發現愈來愈多的 Android 惡意軟體，特別是與金融相關的惡意軟體大量增加。

NCC Groups 指出，這次發現的 SharkBot 就是近年來新出現的金融相關惡意軟體，最早由資安廠商 Cleafy 發現於 2021 年 10 月；其主要攻擊方式為自動化轉帳系統（Automatic Transfer Systems）。

該惡意軟體除了和其他常見金融惡意軟體一樣，可以藉由螢幕截圖、記錄用戶按鍵輸入、攔截簡訊內容並進行遠端遙控外，還會自動開啟用戶手機上安裝的金融服務 App，自動輸入各個欄位，並且自動將用戶帳戶內的資金，轉帳到駭侵者控制下的人頭戶內，造成用戶資金損失。

NCC Groups 指出，在去年首次發現 SharkBot 後，該惡意軟體似乎出現新版，並且隱藏在一個看似沒有問題的 Android 防毒工具軟體「Antivirus, Super Cleaner」中，且成功上架到 Google Play Store 內。

雖然 NCC Groups 已在第一時間通報 Google，但在資安媒體 BleepingComupter 報導此事時，含有 SharkBot 惡意軟體的 Antivirus, Super Cleaner app 仍然未從 Google Play Store 中下架。

資安專家指出，為避免感染這類新興惡意軟體，用戶即使是在 Google Play Store 中，也應小心謹慎，盡量選擇知名大廠推出的應用軟體，勿隨意安裝不明開發者推出的 App。

- 資料來源：
  1. SharkBot: a “new” generation Android banking Trojan being distributed on Google Play Store
  2. SharkBot malware hides as Android antivirus in Google Play

3.6、軟體系統資安議題

3.61.1、Toyota 日本國內所有工廠，因供應商遭駭而全面停工

全球最大汽車製造商 Toyota，因為旗下的供應商伺服器遭到駭侵攻擊，日前宣布在日本國內的所有工廠，在 3 月 1 日全面停工一日。

據新聞媒體指出，遭到駭侵攻擊的是 Toyota 集團所屬，位於愛知縣豐田市的小島沖壓工業株式會社（Kojima Industries)；該公司的伺服器系統遭到不明駭侵攻擊，因而無法運作。

由於小島沖壓工業供應的是對汽車生產十分重要的各種塑膠製零組件，因此對 Toyota 的供應鏈與生產線運作造成嚴重衝擊；目前 Toyota 在日本各地的 14 家汽車製造工廠，都因這次事件而停工一天，預計三月總產量會因而減少 5%，約 13,000 台汽車。

Toyota 與小島沖壓工業雖然並未正式指出這次事件的細節，也未證實這是駭侵事件，只表示是因為小島沖壓工業的系統故障而必須停工，但小島沖壓工業在接受媒體採訪時，指出故障可能就是因為外界駭侵攻擊而造成。

除了 Toyota 本社外，Toyota 旗下的大型車製造廠 HINO 與小型車、輕型車品牌 Daihatsu 也宣布停工。

Toyota 對外表示，正在會同小島沖壓工業積極展開伺服器復原作業，以便儘早復工；但該公司是否能在 3 月 2 日順利恢復各廠的汽車生產作業，目前尚無法預期。

- 資料來源：

1. 2022 年 3 月 国内工場の稼働について（2/28 時点）
2. トヨタの取引先にサイバー攻撃、国内全工場できょうの稼働を停止
3. Toyota halts production after reported cyberattack on supplier

3.6.2、快 NVIDIA 駭侵事件，超過 71,000 名員工各種資訊遭外洩

美國繪圖暨人工智慧運算晶片大廠 NVIDIA，日前遭一名為 Lapsus$ 的駭侵團體攻擊後，目前資安專家已證實，該公司有多達 71,000 名以上員工的各種個資遭竊。

根據知名資料外洩追蹤網站「Have I been Pwned?」統計指出，在這次 NVIDIA 遭駭侵攻擊事件中，目前已有 71,355 名員工的帳號與資料遭駭；該網站也已收集到這些遭駭的資料，並整合進其資料庫中。

據 Have I been Pwned? 網站指出，這批外洩的員工個資，包括 Email 地址、NTML 密碼雜湊值等。

駭侵者 Lapsus$ 入侵 NVIDIA 內部網路後，宣稱已經取得該公司內部高達 1TB 的資敏資料，並且公布其中的 20GB，以此要脅 NVIDIA「必須解除其繪圖處理器晶片（Graphics Processor Unit, GPU） GeForce RTX 30 系列的雜湊算力上限」，同時必須在 3 月 4 日前，將其繪圖處理器晶片的 Windows、macOS、Linux 驅動程式加以開源化，否則將公開自該公司竊得的各種 GPU，包括最近推出的 RTX 3090Ti 晶片等的細部設計資訊。

NVIDIA 公司在回應媒體採訪時指出，該公司目前沒有發現任何此次駭侵攻擊為勒贖攻擊的跡象，但證實該公司的員工相關資料確實遭到駭侵者不當存取；該公司也認為這次駭侵事件不致於對公司營運與客戶造成任何影響。

- 資料來源：
  1. Have I been Pwned?
  2. Sergiu Gatlan @serghei
  3. NVIDIA data breach exposed credentials of over 71,000 employees

3.6.3、NVIDIA 駭侵者利用竊得的程式碼，製作惡意程式碼憑證簽署

資安專家發現，對 NVIDIA 發動駭侵攻擊的駭侵團體 Lapsus$，開始利用竊得的程式碼，來對藏有惡意軟體程式碼的驅動程式進行簽署。

資安專家發現，對 NVIDIA 發動駭侵攻擊的駭侵團體 Lapsus$，開始利用竊得的程式碼，來對藏有惡意軟體程式碼的驅動程式進行簽署，以便安裝並散布於受害者的 Windows 系統中。

資安專家說，在 Lapsus$ 駭侵團體竊取自 NVIDIA 高達 1TB 的資料中，含有 2 個可以用於簽署程式碼安全性的憑證；這些憑證過去是提供給開發者，用於簽署經官方認證的合法程式碼，如今卻被 Lapsus$ 駭侵團體濫用。

資安專家指出，Windows 為了確保各種軟體的安全性與來源，在用戶安裝各種應用程式、驅動程式或核心組件時，都會檢查是否具有合法的憑證簽署；如果沒有簽署的話，Windows 將不會安裝。

資安專家表示，已經觀察到惡意軟體內含 NVIDIA 被竊的簽署憑證，包括可用以遠端監控受害裝置的 Cobalt Strike beacon、Mimikatz，以及多種後門惡意程式與遠端監控木馬等等。

雖然這兩組被竊的簽署憑證已經設定為逾期，但資安專家仍發現 Windows 作業系統仍然可以讓內含此兩組憑證的驅動程式，載入到系統中執行。

雖然 Microsoft 資安專家已經公布方法，讓系統管理員可以透過設定 Windows Defender Application Control Policies 的方法，來設定哪些憑證可以通過驗證，但這種設定方法有其難度，一般 Windows 使用者難以操作。

資安專家呼籲，Windows 一般用戶應避免自不明的網站、Email 或其他不安全管道，下載安裝任何軟體，以避免遭到駭侵者以這種方式植入惡意程式。

- 資料來源：
  1. Florian Roth @cyb3rops
  2. Malware now using NVIDIA's stolen code signing certificates

3.6.4、Morgan Stanley 旗下公司客戶資料，遭駭侵者以社交工程攻擊不當取得

美國 Morgan Stanley 旗下的資產管理公司 Morgan Stanley Wealth Management，日前發生客戶個資遭駭侵者以社交工程攻擊外洩事件。

據該公司寄給潛在受害客戶的信件中指出，部分客戶於今（2022）年 2 月 11 日時接獲駭侵者假扮為 Morgan Stanley 人員來電，說服客戶提供其帳號相關登入資訊等機敏資料；駭侵者在取得登入資訊後，隨即將用戶帳戶中的資金，利用一個名為 Zelle 的支付服務，轉入由駭侵者控制的金融帳戶之中。

Morgan Stanley 對媒體強調，雖然發生資料外洩事件，導致客戶資金損失，但資料並非竊取自 Morgan Stanley 本身。

Morgan Stanley 表示，已經暫停所有受社交工程攻擊影響的帳戶的線上使用權，在進行電話服務時，也會加強身分認證機制，避免客戶資金進一步流失；於此同時 Morgan Stanley 的系統仍然十分安全，並未發現任何漏洞或系統本身遭駭侵攻擊的跡象。

Morgan Stanley 也表示，該公司提供客戶多種防止這類語音釣魚攻擊（Voice Phishing, Vishing）的方法，例如不要接聽不明電話號碼的來電，而當電話中對方要求提供個人機敏資訊時，也需特別提高警覺；若未能充分確認對方身分，絕不輕易提供個資。

Morgan Stanley 在信中也向潛在受害者提供信用監測服務；這項服務可以監測受害者的資金是否出現異常提領，服務期間為 2 年，而且不需額外費用。

- 資料來源：
  1. Morgan Stanley Wealth Investment data breach [February 2022]
  2. Morgan Stanley client accounts breached in social engineering attacks

3.7、軟硬體漏洞資訊

3.7.1、TP-Link 無線路由器 RCE 漏洞的攻擊程式已遭公開，建議用戶立即進行更新

TP-Link 旗下一款無線路由器 Archer C20i 存有嚴重 RCE 資安漏洞，可能導致用戶遭到駭客進行遠端執行任意程式碼攻擊。

該漏洞發生在路由器設備的 X_TP_ExternalIPv6Address HTTP 參數，駭客可以觸發這個漏洞執行遠端身分驗證及作業系統命令注入，並允許駭客在路由器上以 root 權限遠端執行任意命令。

此漏洞攻擊程式的概念驗證（Proof of concept, POC）已被證實，無線路由器 Archer C20i 版本 0.9.1 3.2 v003a.0 Build 170221 Rel.55462 及先前版本的用戶，建議立即從官方網站進行更新至最新版本，避免受到駭客攻擊而造成損失。

- CVE 編號：CVE-2021-44827
- 影響產品(版本)：TP-Link Archer C20i 0.9.1 3.2 v003a.0 Build 170221 Rel.55462 及先前之版本。
- 解決方案：立即至官網進行更新。

- 資料來源：
  1. CVE-2021-44827
  2. full-disclosure/CVE-2021-44827
  3. CVE-2021-44827 Detail

3.7.2、Honda 部分車款含漏洞，駭侵者可開啟車鎖甚至開走車輛

多位資安專家發現，Honda 與其頂級品牌 Acura 部分車款之無線鑰匙系統，內含嚴重漏洞，可導致駭侵者攔截並複製無線鑰匙的通訊內容。

多位資安專家發現，Honda 與其頂級品牌 Acura 部分車款之無線鑰匙系統，內含嚴重漏洞，可導致駭侵者攔截並複製無線鑰匙的通訊內容，並且遠端開啟車鎖，甚至開走車輛。

資安專家指出，該部分車款含有一個中間人攻擊（Man-in-the-middle attack, MITM）漏洞 CVE-2022-27254。經由該漏洞，駭侵者可利用裝置來攔截 Honda / Acura 車輛的無線鑰匙（key fob）與汽車之間的無線通訊內容，並在稍後重新發送無線通訊，從而開啟汽車鎖，甚至發動汽車。

資安專家表示，他們在攔截無線鑰匙發送的一連串數字指令後予以解碼，並且成功解出各種控制車鎖的指令內容。

發現此漏洞的資安專家，也拍攝了一段影片，證實其漏洞攻擊手法確實可行；然而資安專家並未公開釋出關於此概念證實實作的細部資訊。

受此漏洞影響的車款，包括 Honda Civic LX、EX、EX-L、Touring、Si、Type R 等款式於 2016 - 2020 年間生產的批次。

另外一組資安研究人員，也發現了其他 Honda 車系無線鑰匙的漏洞 CVE-2021-46145，不過利用這個漏洞來控制車輛的難度較高。

資安媒體 BleepingComputer 向 Honda 官方詢問時，Honda 回應目前並未發現這種竊車手法大量出現，且該公司並無針對舊款車種更新此漏洞的計畫，不過會在未來的車款中強化無線鑰匙系統的防護能力。

- CVE 編號：CVE-2022-27254
- 影響產品(版本)：Honda Civic LX、EX、EX-L、Touring、Si、Type R 等款式於 2016 - 2020 年間生產的批次。

- 資料來源：
  1. HackingIntoYourHeart / Unoriginal-Rice-Patty
  2. nonamecoder / CVE-2022-27254
  3. Honda bug lets a hacker unlock and start your car via replay attack

3.7.3、OpenSSL 修補高嚴重性的憑證解析漏洞，建議用戶立即進行更新

OpenSSL 於 2022 年 3 月 15 日發布安全公告，宣布修補了與憑證解析有相關的嚴重阻斷服務攻擊(Denial of Service, DoS)資安漏洞，建議用戶立即進行更新。

該漏洞的編號為 CVE-2022-0778，由 Google 的研究人員 Tavis Ormandy 提報給 OpenSSL。據 OpenSSL 官方公告，由於解析憑證時用到的 BN_mod_sqrt()函數存在一個問題，在某些情況下駭客可以製作惡意憑證，利用該漏洞使目標系統無法提供服務。

OpenSSL 版本為 1.0.2、1.1.1 及 3.0 的用戶會受到該漏洞影響，建議用戶立即更新至版本 1.0.2zd、1.1.1n 及 3.0.2，以免遭到駭客利用此漏洞進行攻擊而造成損失。

- CVE 編號：CVE-2022-0778
- 影響產品(版本)：OpenSSL 1.0.2、1.1.1 及 3.0 版本。
- 解決方案：OpenSSL 1.0.2 用戶應升級到 1.0.2zd 版本、OpenSSL 1.1.1 用戶應升級到 1.1.1n 版本、OpenSSL 3.0 用戶應升級到 3.0.2 版本。

- 資料來源：
  1. OpenSSL Security Advisory [15 March 2022]
  2. High-Severity DoS Vulnerability Patched in OpenSSL
  3. CVE-2022-0778 Detail

3.7.4、華碩針對 Cyclops Blink 惡意軟體攻擊 ，發布緩解建議措施

華碩旗下多個路由器產品受到 Cyclops Blink 惡意軟體發動駭侵攻擊，廠商日前已發布緩解措施。

Cyclops Blink 的特性使駭客能遠端存取受感染的網路，此惡意軟體與 Sandworm 駭客組織有關，該組織以往的目標都是 WatchGuard Firebox 以及其他 SOHO 網路設備。

根據趨勢科技的說明，Cyclops Blink 擁有專門針對多型號華碩路由器的模組，能夠讀取快閃記憶體，收集其中的文件、可執行檔案、數據及資料庫的重要資訊。

在華碩發布的產品安全公告中，說明了以下路由器型號及版本容易受到 Cyclops Blink 攻擊：

- GT-AC5300 韌體版本 3.0.0.4.384.xxxx 及更早版本
- GT-AC2900 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC5300 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC88U 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC3100 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC86U 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC68U, AC68R, AC68W, AC68P 韌體版本 3.0.0.4.384.xxxx 及更早

版本

- RT-AC66U_B1 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC3200 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC2900 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC1900P, RT-AC1900P 韌體版本 3.0.0.4.384.xxxx 及更早版本
- RT-AC87U(EOL)
- RT-AC66U(EOL)
- RT-AC56U(EOL)。

- 解決方案：華碩發布的產品公告已說明緩解措施，近期會再提供新版韌體，建議相關產品用戶盡速保護產品免於遭受 Cyclops Blink 攻擊而造成損失。
  - 將您的設備恢復成原廠設定。
  - 將韌體版本更新至最新可用版本。
  - 確認預設的管理員密碼已更改成更安全的密碼。
  - 禁止使用遠端管理功能。

- 資料來源：
  1. ASUS Product Security Advisory
  2. ASUS warns of Cyclops Blink malware attacks targeting routers
  3. Cyclops Blink Sets Sights on Asus Routers

3.7.5、Mozilla Firefox 修復兩個已遭濫用於攻擊的 0-day 漏洞

用戶眾多的 Mozilla Firefox 瀏覽器，日前推出最新 97.0.2 版本，修復兩個目前確知已遭用於駭侵攻擊的兩個 0-day 漏洞；各用戶應立即更新至最新版本。

這兩個漏洞的 CVE 編號為 CVE-2022-26485 與 CVE-2022-26486，都是屬於「使用已釋放記憶體」的錯誤；駭侵者可利用這兩個錯誤誘發程式崩潰，從而遠端執行任意程式碼，無需取得任何權限。

CVE-2022-26485 存於 XSLT 參數處理過程中，在執行時移除需給定的參數，即可誘發此漏洞；而 CVE-2022-26486 則存於 WebGPU IPC Framework 之中，可由一個預期之外的訊息誘發此錯誤，甚至可在沙盒以外執行程式碼。

這兩個 0-day 漏洞的 CVSS 危險程度評分均為 8.4，危險程度評級為「嚴重」(critical）等級，且根據 Mozilla 發表的資安通報指出，該公司已得知這兩個 0-day 已遭駭侵者大規模濫用於攻擊行動中。

這兩個漏洞是由資安公司奇虎 360 ATA 旗下的資安研究人員發現的，並立即通報 Mozilla 進行漏洞修補。

受此漏洞影響的 Mozilla 產品，包括 Mozilla Firefox、Mozilla Firefox ESR、Mozilla Firefox for Android、Mozilla Focus、Mozilla Thunderbird 等；上述各軟體的最新版本，均已修復這兩個漏洞。

各作業系統版本，包括 Windows、macOS、Linux 的 Mozilla Firefox 暨相關產品用戶，應立即更新至最新版本（97.0.2），以免遭到駭侵者以這兩個 0-day 漏洞發動攻擊，造成損失。

- CVE 編號：CVE-2022-26485、CVE-2022-26486
- 影響產品(版本)：Mozilla Firefox、Mozilla Firefox ESR、Mozilla Firefox for Android、Mozilla Focus、Mozilla Thunderbird 各作業系統版本 97.0.2 先前版本。
- 解決方案：升級至 Mozilla Firefox 97.0.2 與後續版本。

- 資料來源：
  1. CVE-2022-26485: Use-after-free in XSLT parameter processing
  2. Mozilla Firefox 97.0.2 fixes two actively exploited zero-day bugs

3.7.6、普遍用於各種 VOIP 產品的開源多媒體程式庫 PJSIP，內含 5 個嚴重資安漏洞

資安廠商發現經常用於各種 VOIP 服務的開源程式庫 PJSIP 多媒體溝通程式庫，內含 5 個嚴重資安漏洞，可能導致駭侵者遠端執行任意程式碼。

資安廠商 JFrog 日前發表研究報告，指出該公司發現經常用於各種 VOIP 服務的開源程式庫 PJSIP 多媒體溝通程式庫，內含 5 個嚴重資安漏洞，可能導致駭侵者遠端執行任意程式碼。

在使用 PJSIP 程式庫的 VOIP 開源軟體中，最著名的就是 Asterisk；有許多企業級的 VOIP 軟體或服務，都使用 Asterisk 的開源 PBX（Private Branch Exchange）工具，數量十分龐大。

根據 Asterisk 的官方網站， Asterisk PBX Toolkit 的下載次數高達每年 200 萬次，共在 170 國境內的 100 萬台伺服器上執行；用戶包括各國公家機關、話務中心、大型企業與中小企業等，甚為廣泛。

在這 5 個漏洞中，有 3 個漏洞屬於遠端執行任意程式碼漏洞，主要是在電話呼叫過程中誘發 PJSUA API 中的錯誤，以造成堆疊溢位；另 2 個漏洞分別是在電話呼叫過程中誘發 PJSUA API 的資料越界讀取與緩衝區溢位錯誤，可以用來發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）。

JFrog 的資安研究團隊，在發現這 5 個漏洞後，立刻向 PJSIP 的開發者提報漏洞；目前 PJSIP 已在最新版本的 2.12 版中予以修復；各個使用內含 Asterisk VOIP 解決方案的系統管理者，應立即將系統內使用的 PJSIP 程式庫升級到最新的 2.12 或後續版本，以修補這 5 個漏洞。

- CVE 編號：CVE-2021-43299、CVE-2021-43300、CVE-2021-43301、CVE-2021-43302、CVE-2021-43303
- 影響產品(版本)：PJSIP 2.12 之前版本。
- 解決方案：升級至 PJSIP 2.12 與後續版本。

- 資料來源：
  1. JFrog Discloses 5 Memory Corruption Vulnerabilities in PJSIP – A Popular Multimedia Library
  2. RCE Bugs in Hugely Popular VoIP Apps: Patch Now!

第 4 章、 資安研討會及活動

公部門如何揪出潛伏資安威脅研討會（限政府機關參加）-北中南三場	
活動時間	**4/13（三）台中、4/21（四）高雄、5/11（三）高雄**
活動地點	
活動網站	**https://www.cisanet.org.tw/News/Detail/5514**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 地點：集思台中烏日會議中心富蘭克林廳、蓮潭國際會館 R402 會議室、集思台大會議中心 B1 蘇格拉底廳 課程說明：政府的防護策略，近年來不只從管理面著手，朝向資安落實來推動，在技術面上，也朝向主動式防禦發展，目標是將防禦陣線往前推，當資安事件發生時，將事件紀錄完整保存與資源精準投入，避免相同事件再次發生。否則若僅是擋住攻擊及恢復系統，卻沒有辦法知道根因，或是恢復後又再被攻擊，等於事件沒有真正被處理與改善。 為協助各政府機關能運用最新技術，落實資安法規要求提升資安防護效益，特規劃本研討會，邀請國內頂尖資安專家以案例及實際導入經驗作分享，探討公部門如何做好資安防護以及協助調查難以發現的進階攻擊，即時完成資安弱點通報，並強化資安防護能力，落實「資安即國安」的發展準則。 活動聯絡人：廖資深專員、鄭專員 Email：security@cisanet.org.tw Tel: (02)2553-3988 Ext：388、666

思科「安全 x 敏捷 x 易擴展 混合辦公絕佳體驗」研討會	
活動時間	**4/13 (三) 14:00**
活動地點	**線上**
活動網站	**https://event.ithome.com.tw/live/cisco220413/index.html**
活動概要	 **主辦單位：CISCO** 根據 Cisco 與 Dimensional Research 合作進行的「混合職場的崛起」調查顯示，僅 9% 受訪者預計在疫情退散後重返辦公室工作，其餘壓倒性的多數，皆青睞混合辦公模式；與此同時，97% 受訪者期望企業把工作環境調整得更安全，96% 的受訪者則是期望利用智慧型協作技術來改善工作環境。 由此看來，混合辦公 (Hybrid Work) 浪潮來得又急又猛，儼然就是未來永遠的常態。 因此，企業急需利用適當的解決方案，讓員工無論在家中、辦公室或任何地點皆能順利工作；譬如必須提供安全便捷的管道，讓同仁隨時隨地都能順利聯繫工作團隊夥伴，順利存取工作所需的資料或應用程式。 然而這樣的解決方案，是否涉及複雜的技術堆疊？實作的難度會不會太高？為此 Cisco 將於 2022 年 4 月 13 日，舉辦一場以混合辦公為主題的線上研討會，教您如何簡單、迅速且確實地建構最優質的安全協作基礎架構，滿足混合辦公空間、遠距安全存取、新世代通訊等所有關鍵環節。精彩可期，歡迎您踴躍報名參加！ 參加方式：事前報名、免費參加 洽詢專線：(02)2562-2880 分機 3631 思科活動小組

【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	【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 **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」

未來世界：元宇宙的資安議題與隱私問題	
活動時間	**4/19 09:00~12:00**
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/2762**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 課程說明：本課程將教導學員了解現今元宇宙的應用與發展，隱私與資安的問題在現實世界就存在，未來在元宇宙的世界也會被繼承，不但會被繼承，還有可能因為元宇宙新興科技的交互運用而被放大，元宇宙裡面有虛擬的假的真臉，真的虛擬的假臉，這些虛擬跟現實交雜的情況越來越多且差異越來越不明顯，真假難辨，未來將成為一個元宇宙的公民，該怎麼去保護自己的權益跟隱私呢？ 課程大綱： - 元宇宙虛實整合新浪潮？ - AIOT 工業元宇宙安全風險？ - 元宇宙社交生活隱私問題？ - 元宇宙資安真相：廠商攔隱私，駭客劫個資 - 元宇宙訊息確信與查證中心 活動聯絡人：鄭詒安專員 Email: ann.cheng@ cisanet.org.tw　Tel: (02)2553-3988 Ext：666 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。

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	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 課程說明：本課程設計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

區塊鏈與智慧資安女力論壇	
活動時間	**2022 / 04 / 24（日） 14:00 - 16:30**
活動地點	**集思北科大會議中心-感恩廳《台北市大安區忠孝東路三段 1 號(197 號旁)2 樓(億光大樓)》**
活動網站	**https://isipevent.kktix.cc/events/e58d0573**
活動概要	 **主辦單位：教育部先進資通安全實務人才培育計畫、Girls in Tech Taiwan** 【活動介紹】 教育部先進資通安全實務人才培育計畫與 Girls in Tech Taiwan，在 04 / 24（日） 14:00 - 16:30，於北科集思會議中心 感恩廳，聯合主辦「區塊鏈與智慧資安女力論壇」，希望落實資安觀念向下扎根，並鼓勵女性投入資訊安全領域，本次邀請區塊鏈與智慧資安優秀女性資安人分享職場經驗及心路歷程。 想了解她們在區塊鏈與智慧資安領域上一路走來的心路歷程嗎？想詢問在資安領域該如何自我學習？對於資安領域的職涯想要有更深入的認識嗎？趕緊手刀手報名吧！現場座位有限，錯過可惜！

ISO 27001 資訊安全管理系統主導稽核員訓練課程	
活動時間	**4/27-4/28、5/04-5/06 上午九點至下午六點**
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/2740**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 課程說明： ISO 27001 目前已是國際資訊安全管理的準則及規範，更是各國企業組織展現其在資訊安全管理能力的最佳證明！取得「ISO 27001 資訊安全管理系統主導稽核員專業證照」，將代表個人在資安管理上，建置與稽核的專業能力受到肯定，所學將可實際運用在資訊安全領域的技術職、管理職；參加者將從課程中得到如何協助企業組織建立、稽核 ISO/IEC 27001:2013 資訊安全管理系統證照。 課程特色： - 講師：SGS 合格之 IRCA 講師授課 - 教材：中文教材、英/中對照標準手冊及中文試卷 - 證書：IRCA 原廠授證。同時通過筆試和持續評量的學員將授予「成功修業」證書；學員未通過持續評量，但已出席該課程的全部時間將授予「上課證明」。證書有效期限五年，期限內可登錄成為 CQI / IRCA 稽核員。 活動聯絡人：鄭詒安專員 Email: ann.cheng@ cisanet.org.tw　Tel: (02)2553-3988 Ext：666 以上課程、內容資訊，主辦單位保留最終變更及調整之權利。

第 5 章、 TVN 漏洞公告

TWCERT/CC 上月份發布漏洞嚴重程度前五名之漏洞資訊如下表：

育碁數位科技 a+HRD - Broken Access Control	
TVN / CVE ID	TVN-202203009 / CVE-2022-26676
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD version 6.8
問題描述	aEnrich a+HRD 某特定 URL 未進行適當的權限控管，遠端攻擊者可繞過身分認證機制使用系統之 API 功能上傳並執行惡意腳本，藉以控制系統或中斷服務。
解決方法	更新版本至 eHRD6.8.1039V768
公開日期	2022-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5970-2f405-3.html

D-Link DIR-878 - Command Injection	
TVN / CVE ID	TVN-202203003 / CVE-2022-26670
CVSS	8.8 (High)
影響產品	D-Link DIR-878 firmware version v1.20b05 & Below
問題描述	D-Link DIR-878 特定頁面欄位未對特殊參數作過濾，導致區域網路內的攻擊者不須權限，即可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令。
解決方法	Update firmware version to v1.30B08 Hotfix03
公開日期	2022-03-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5972-c259e-3.html

ASUS RT-AC86U - Command Injection	
TVN / CVE ID	TVN-202202007 / CVE-2022-25597
CVSS	8.8 (High)
影響產品	ASUS RT-AC86U firmware v3.0.0.4.386.45956
問題描述	ASUS RT-AC86U 的 LPD 服務未對使用者發送的請求進行特殊字元的過濾，區域網路內的攻擊者不須權限，即可利用該漏洞進行部分 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	Update ASUS RT-AC86U firmware version to 3.0.0.4_386_46092
公開日期	2022-03-07
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5794-09c33-3.html

ASUS RT-AC86U - Heap-based buffer overflow	
TVN / CVE ID	TVN-202202006 / CVE-2022-25596
CVSS	8.8 (High)
影響產品	ASUS RT-AC86U firmware v3.0.0.4.386.45956
問題描述	ASUS RT-AC56U 之設置功能中的解密參數未作長度驗證，導致 Heap-based buffer overflow 漏洞，區域網路內的攻擊者不須權限，即可執行任意程式碼，對設備進行任意操作或中斷服務。
解決方法	Update ASUS RT-AC86U firmware version to 3.0.0.4_386_46092
公開日期	2022-03-07
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5793-4f9d3-3.html

ASUS RT-AX56U - Stack overflew	
TVN / CVE ID	TVN-202202004 / CVE-2022-23973
CVSS	8.8 (High)
影響產品	ASUS RT-AX56U firmware v3.0.0.4.386.45898
問題描述	ASUS RT-AX56U 之配置使用者清單功能未作參數長度驗證，導致 Stack-based buffer overflow 漏洞，使區域網路內的攻擊者不須權限，即可執行任意程式碼，對設備進行任意操作或中斷服務。
解決方法	Update ASUS RT-AX56U firmware version to 3.0.0.4.386.45934
公開日期	2022-03-02
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-5787-b0e64-3.html**

第 6 章、 2022 年 3 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。

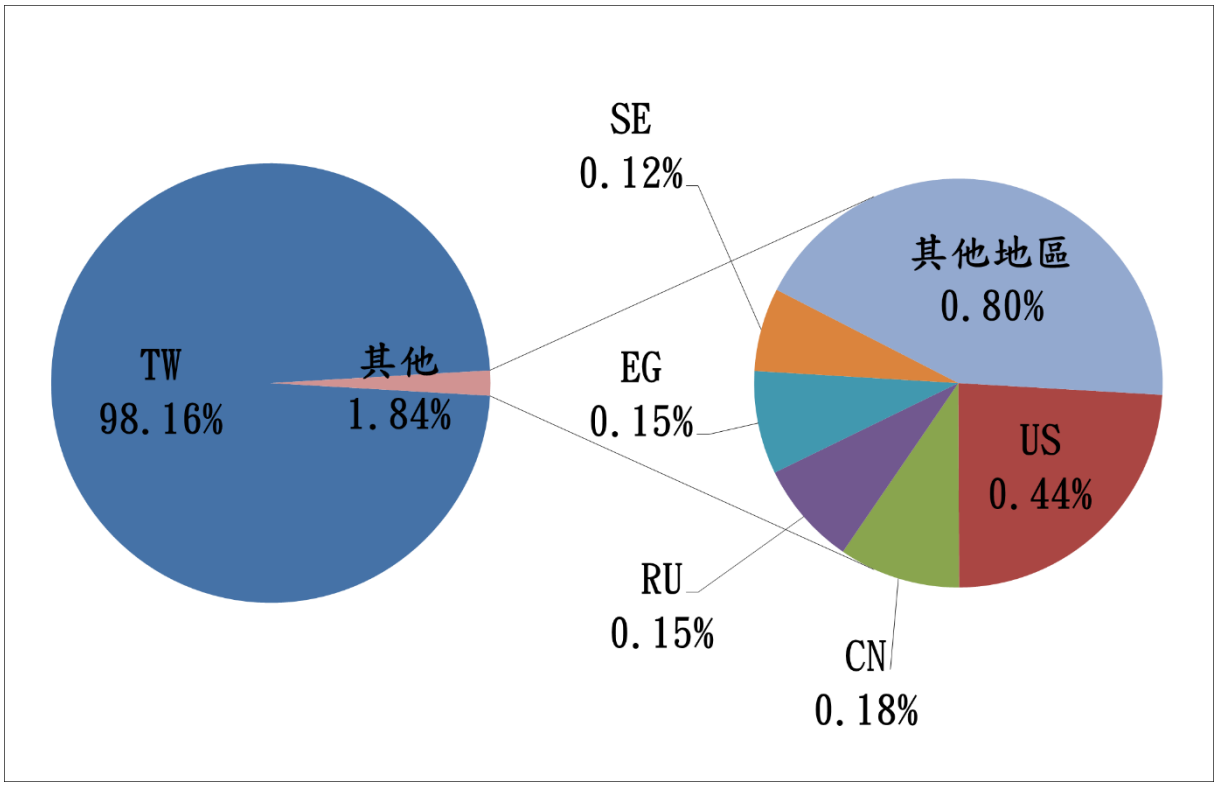


圖 1、分享地區統計圖

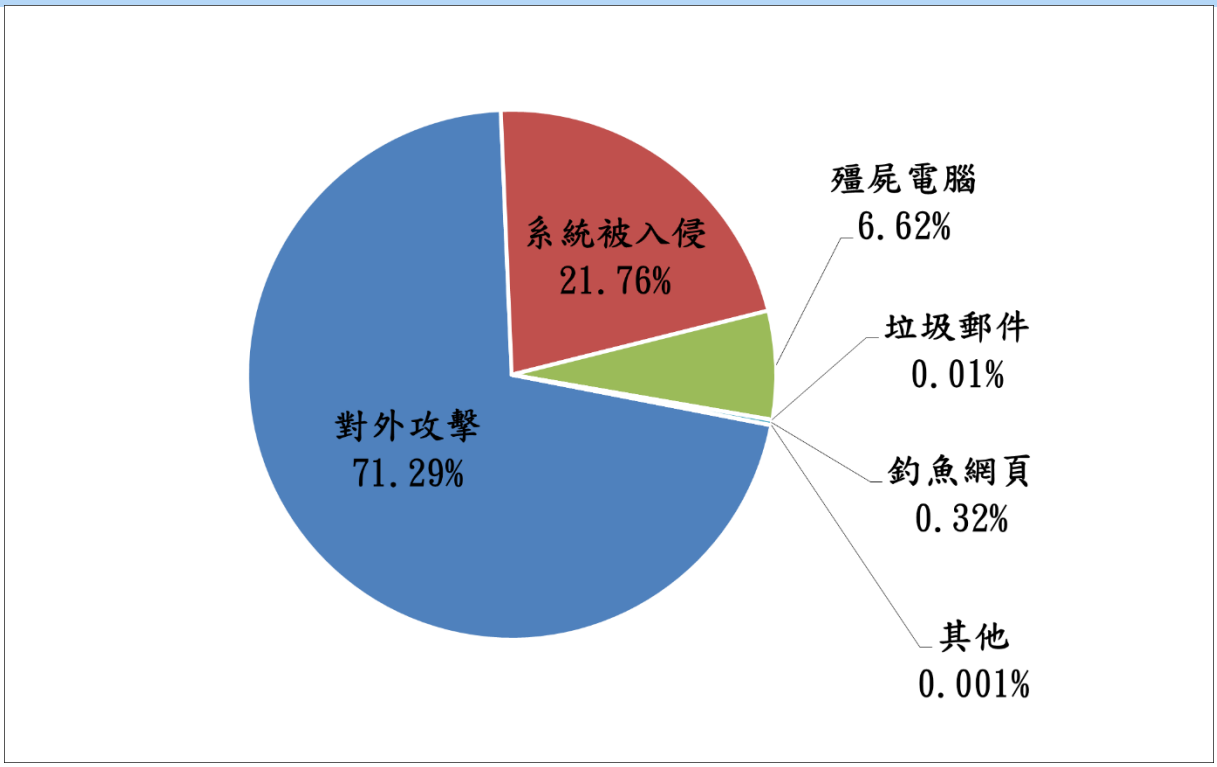


圖 2、分享類型統計圖

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 4 月 11 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**