# TWCERT/CC 資安情資電子報

## 2023 年 5 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 5 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、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 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、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 5 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

## 資安專家示警：Windows 系統管理者應立即修補嚴重的 MSMQ QueueJumper 漏洞


資安專家近期針對 Microsoft Message Queuing (MSMQ) 中介軟體服務中的一個嚴重資安漏洞提出警告，指出 Windows 系統管理者應立即套用修補軟體，修復此漏洞。目前有數十萬台 Windows 系統曝露於該資安風險之下。

MSMQ 於所有 Windows 各版本中均有提供，是一個可讓 App 具備網路通訊能力的選用組件，可以透過 PowerShell 或控制台（Control Panel）來啟用。

資安廠商 Fortinet 和 CheckPoint 旗下的資安專家指出，在 MSMQ 中存在的嚴重漏洞 CVE-2023-21554 可讓駭侵者以特製的 MSMQ 惡意封包，在不需要使用者互動的情形下，輕易進行攻擊，並且遠端執行任意程式碼。

受該漏洞影響的 Windows 版本，為目前市面上全系列的所有版本，包括最新版本的 Windows 11 22H2 與 Windows Server 2022。Microsoft 本身已在日前釋出的 2023 年 4 月分 Patch Tuesday 例行性資安修補包中修復此一漏洞，但根據 Check Point 的估計，目前仍有約 36 萬台 Windows MSMQ 伺服器尚未

完成該漏洞的修補作業，因此仍曝露在駭侵攻擊的風險之下。

Microsoft 指出，目前已接獲有駭侵者利用此漏洞發動攻擊的情報，所有 Windows 系統管理者，應正視這個漏洞可能帶來的威脅，且應立即進行修補。

- CVE 編號：CVE-2023-21554
- 影響產品：Windows 各版本作業系統，包括 Windows 11 2022H2 與 Windows Server 2022。
- 解決方案：建議立即套用 Microsoft 日前釋出的 Patch Tuesday 資安修補包。

- 資料來源：
  1. Microsoft Message Queuing Remote Code Execution Vulnerability
  2. Haifei Li @HaifeiLi
  3. Windows admins warned to patch critical MSMQ QueueJumper bug

# 第 2 章、 國內外重要資安事件

## 2.1、資安趨勢

### 2.1.1、美國調查指出，近半員工會用舊密碼存取前公司系統服務


美國資安公司 Password Manager 近期發表調查報告指出，近半數員工在離開原任職公司後，仍會以先前持有的登入資訊存取原任職公司的各種帳號。

Password Manager 於 2023 年 3 月針對 1,000 名擁有前一份工作使用之登入資訊的美國地區的工作者進行問卷調查，了解員工在離職後繼續使用前公司各項網路服務（包括公司用 Email、軟體、工具等）的情形。

調查所得情形摘要如下：

- 47 % 受訪者承認在離職後，仍會使用前公司的登入資訊；
- 超過 1/4 受訪者承認目前正在透過先前的登入資訊，使用前公司訂閱的服務；
- 7 個人中僅有 1 人會遭到前公司發現仍在使用任職時的登入資訊；

- 1/3 受訪者利用舊登入資訊使用原公司服務超過 2 年以上；
- 10 個人中有 1 個人承認曾利用先前的登入資訊，來干擾前公司的運作。

報告也另外舉出幾個數字與現象：

- 58% 受訪者表示，在他們離職後，原公司並未更變所用服務或工具的密碼；
- 44% 受訪者表示，有還在原公司任職的同仁將登入資訊分享給他們；
- 6% 受訪者表示能夠猜出原公司使用的登入資訊。
- 44% 受訪者能夠存取前公司的資料。

報告也詢問受訪者為何要使用前公司的登入資訊，結果如下：

- 約 56% 為個人使用；
- 約 42% 受訪者與先前的客戶或顧客聯絡；
- 約 39% 受訪者用來幫助進行其他公司的工作。

問卷也詢問受訪者是否認知道使用前公司舊密碼的安全問題，25% 受訪者表示「不安全」，6% 表示「非常不安全」；另外還有 47% 表示曾接到原公司現任人員，因為忘記密碼而來詢問。

建議公私單位應做好帳號密碼控管，在人員離職後立即取消該人員對內外系統與訂閱服務的存取權限，更應避免讓員工使用相同的「公用帳號密碼」。

- 資料來源：
  1. 47% of Workers Admit to Hacking Accounts With Former Employers' Passwords
  2. Ex-employee password abuse: 10% log back in to 'disrupt' business, report

## 2.1.2、資安廠商統計指出 2023 年 3 月勒贖攻擊數量打破歷年記錄，高達 459 件


資安廠商 NCC Group 日前發表統計資料指出，2023 年 3 月為該公司觀察到史上勒贖攻擊發生件數最多的月份，共記錄到 459 起勒贖攻擊，較 2023 年 2 月增加 91%，也較 2022 年 3 月增加 62%。

NCC Groups 在報告中指出，2023 年 3 月份勒贖攻擊數量大幅增加的主因，是因為 CVE-2023-0669 的 0-day 漏洞遭到駭侵者以大規模用於發動攻擊。該 0-day 漏洞存於 Forta 的 GoAnywhere MFT 安全檔案傳輸工具；一個名為 Clop 的勒贖團體利用此漏洞，在 10 天內就對 130 家企業發動勒贖攻擊。

緊追在後的是 Lockbit 3.0，在 2023 年 3 月份記錄到 97 次勒贖攻擊活動，接下來是 Royal、BlackCat、Bianlian、Play、Blackbasta、Stormous、Medusa、Ransomhouse 等。

在遭到勒贖攻擊的產業別方面，以製造業最多，一個月內有 147 起勒贖攻擊事件，佔所有勒贖攻擊的 32%，也是前三大攻擊者 Clop、LockBit 和 Royal 的主要攻擊目標。其次為消費者服務業、科技業、醫療保健業、基本材料業、金融業、學術與教育產業等。

若以受害者地域分布來看，有一半以上遭到勒贖攻擊的單位位於北美洲，共有 221 家；其次為歐洲（126 家）、亞洲（59 家）。

鑑於勒贖攻擊的發生次數逐年增加，且許多都是利用 0-day 漏洞進行，建議各公私單位應立即加強系統資安防護能力與人員的資安防護認知，以提高駭侵者攻擊難度，降低遭受資安攻擊的風險。

- 資料來源：
  1. Ransomware attacks increased 91% in March, as threat actors find new vulnerabilities
  2. March 2023 broke ransomware attack records with 459 incidents

## 2.1.3、2022 年澳大利亞詐騙損失金額破新高，達 31 億美元


澳大利亞競爭與消費者委員會（AustralianCompetition and Consumer Commission, ACCC）統計指出，在去（2022）年一年之中，澳大利亞因為各式詐騙造成的財務損失，年增率較 2021 年高達 80%，總額更高達 31 億美元。

據統計指出，在各類發生的詐騙事件中，絕大多數的損失都來自投資理財型詐騙，總額達到 15 億美元；其次是遠端遙控詐騙，總額達 2.29 億美元，再其次為付款攔截詐騙，總額達 2.24 億美元。

ACCC 指出，其資料來源係收集自澳洲政府多個單位，包括 ACCC 下的 Scamwatch、ReportCyber，以及澳洲金融犯罪交換網路 (Australian Financial Crimes Exchange, AFCX)、IDCARE 等單位；而在去年 ACCC Scamwatch 收到的詐騙案件報案量為 24 萬件，報案件數比 2021 年少了 16.5%，但是每起案件的平均詐騙受害金額卻增加到 2 萬美元，年增率高達 50%。

ACCC 官員指出，由於詐騙者使用的技巧與工具愈來愈成熟，一般人愈來愈難以察覺，因此造成詐騙損失的急速上升；詐騙者會假冒公家機關電話號碼、Email 地址、官網網域等方式來加強詐騙文案的可信度。

官員也指出，這類詐騙活動常在澳洲爆發大型資料外洩事件後急劇增加；例如在 2022 年某起大型資料外洩事件之後數周，Scamwatch 就接獲數百起報案，指稱詐騙者假冒政府機關與大型企業行騙。

鑑於投資型詐騙往往是利用人的貪念而行，民眾必須對以低成本高獲利為號召的各種投資邀約提高警覺，以免造成財務損失。

- 資料來源：
  1. ACCC calls for united front as scammers steal over $3bn from Australians
  2. Australians lost a record $3.1 billion to scams last year

## 2.2、新興應用資安

### 2.2.1、駭侵者利用 Rilide 瀏覽器擴充套件跳過二階段登入驗證並竊取用戶加密貨幣


資安廠商 Trustwave SpiderLasb 旗下的研究人員，近期發現一個名為 Rilide 的全新惡意 Google Chrome 瀏覽器擴充套件，會監控瀏覽器的活動、拍攝螢幕畫面，並且在網頁中注入惡意程式碼，以竊取用戶的加密貨幣資產。

研究人員指出，Rilide 詐稱本身是相當好用的 Google Drive 瀏覽器擴充套件，以此吸引用戶下載安裝，但實際上內藏惡意程式碼。

研究人員發現近期共有兩波散布 Rilide 的駭侵攻擊活動；其中一波利用 Google Ads 來推送廣告，並利用 Aurora Stealer 來載入惡意軟體；另一波則使用 Ekipa 遠端存取木馬來推送惡意程式碼。

Rilide 開始執行其惡意程式碼後，就開始監控瀏覽器的一舉一動，包括用戶切換瀏覽頁籤、檢視網頁內容或網頁內容載入，並會與其控制伺服器中的目標網頁清單相互核對。

如果核對結果相符，表示使用者正在瀏覽駭侵者有興趣的網頁，此時該擴充套件就會在網頁中注入惡意程式碼，並竊取用戶的各種機敏資訊，包括加密貨幣相關登入資訊、用戶 EMail 登入資訊等等。

該擴充套件也會在注入惡意軟體竊取機敏資訊時，同時停用「Content Security Policy」，該功能的設計目的是讓瀏覽器阻擋外部資源載入，以避免跨站惡意程式碼攻擊（Cross-site Scripting, XSS）。

Rilide 最特殊的部分，是會攔截用戶輸入的二階段驗證碼；該擴充套件會先顯示假的二階段驗證碼輸入畫面，當用戶輸入正確的二階段驗證碼後，Rilide 再將取得的驗證碼輸入到加密貨幣錢包等網站，以竊取用戶的加密貨幣資產。

建議用戶在下載瀏覽器擴充套件時，務必提高警覺，在安裝前先仔細閱讀用戶評價，如有異常，切勿任意下載安裝。

- 資料來源：
  1. Rilide: A New Malicious Browser Extension for Stealing Cryptocurrencies
  2. Hackers use Rilide browser extension to bypass 2FA, steal crypto

## 2.2.2、加密貨幣交易所 KuCoin 的官方 Twitter 帳號遭盜，用以推送詐騙活動


全球知名的加密貨幣交易所 KuCoin，日前傳出官方 Twitter 帳號遭盜事件；竊取該帳號使用權的駭侵者，利用該帳號推送詐騙加密貨幣放送活動，短短 45 分鐘內即造成多名用戶財務損失，損失金額約為 22,600 美元。

據 KuCoin 在其官方 Twitter 帳號中發布的資安通報指出，該帳號於 4 月 24 日午夜 0:00 (UTC+2) 時遭到不明駭侵者取得使用權，為時約 45 分鐘。在這段短時間內已造成部分用戶的財務損失。KuCoin 將會針對確認損失的部分全額賠償給受害用戶。

駭侵者利用 KuCoin 的官方 Twitter 帳號，宣稱為慶祝 KuCoin 註冊使用者達 1,000 萬人，特別舉辦加密貨幣大型放送活動，將送出多達 5,000 枚比特幣與 10,000 枚以太幣；要求用戶先發送若干額度的加密貨幣到駭侵者指定加密貨幣錢包，然後可以在自己的加密貨幣錢包中獲得雙倍的加密貨幣。

雖然這類詐騙手法已經十分老套，但還是能成功騙得部分用戶的數位資金。KuCoin 指出，在這 45 分鐘內一共發生 22 筆交易，總值相當於 22,628 USDT。KuCoin 指出，為防止用戶進一步因此詐騙活動發生財損，該交易所正在檢查並封鎖駭侵者使用的加密貨幣錢包。

目前 KuCoin 尚未說明其官方 Twitter 帳號是如何遭到駭侵者竊取的，該公司正在會同 Twitter 進行調查；該公司也承諾將在既有的 Twitter 二階段登入驗證之外，針對帳號安全性額外加強防護。

鑒於各種加密貨幣或其他投資工具的詐騙廣告十分猖狂，建議投資人對於承諾高額獲利的可疑訊息均應提高警覺，以免遭到巨額損失。

- 資料來源：
  1. KuCoin @kucoincom
  2. KuCoin's Twitter account hacked to promote crypto scam

# 2.3、國際政府組織資安資訊

## 2.3.1、CISA 命令美國聯邦政府各單位修補最新 5 個漏洞，其中一漏洞遭用於勒贖攻擊


美國資安最高主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA），日前在其發行的「已知遭駭漏洞」（Known Exploited Vulnerabilities, KEV）清單中新增五種已遭駭侵者用於攻擊的資安漏洞，並要求美國聯邦政府旗下各單位限期修復漏洞完成。

在這 5 個新加入 KEV 清單中的漏洞中，有一個危險程度評級為「嚴重」（Critical）等級的漏洞 CVE-2021-27877，據報已遭 ALPHV/BlackCat 勒贖團體用於發動駭侵攻擊。該漏洞存於 Veritas 資料安全防護軟體內，駭侵者可藉以漏洞提升執行權限，執行遠端遙控並執行任意程式碼。

另外兩個列入 KEV 的漏洞 CVE-2021-27876 與 CVE-2021-27878 都存於 Veritas Backup Exec 之中，也能讓駭侵者藉以存取系統上的任意檔案，並執行任意程式碼。

另有一個發生在 Samsung 裝置內建網路瀏覽器的 0-day 漏洞 CVE-2023-26083 亦列入 KEV 中。一個在 2022 年 12 月發現的商用間諜軟體，使用該漏洞來竊取受害用戶在裝置上的機敏資訊。

第 5 個列入 KEV 的漏洞為 CVE-2019-1388，發生於 Microsoft Windows Certificate Dialog，駭侵者可用以提升執行權限。

根據規定，美國聯邦政府旗下各單位，須在 2023 年 4 月 28 日前完成這批漏洞的修復作業。雖然 CISA 的命令只對美國聯邦政府所屬單位生效，但建議所有公私部門單位遵行辦理，以減少遭駭侵攻擊的風險。

建議各公私單位應立即依 CISA 指示檢查並修復所用軟硬體系統的資安漏洞，以降低遭駭侵者利用已知漏洞發動攻擊的風險。

- 資料來源：
  1. CISA Adds Five Known Exploited Vulnerabilities to Catalog
  2. CISA orders agencies to patch Backup Exec bugs used by ransomware gang

## 2.3.2、歐洲檢警逮捕 5 名涉及 9,800 萬美元的投資詐騙攻擊者，受害者達 33,000 人


歐洲刑警組織 (Europol) 近日會同歐洲檢查官組織（Eurojust），共同破獲並逮捕一個網路詐騙集團的五名成員；該詐騙集團涉及一場大型的網路投資詐騙攻擊，受害人數多達 33,000 人，不法獲利高達 9,800 萬美元。

Europol 表示，執法行動於本（2023）年 3 月的兩天之中進行，搜索地點多達 15 處，其中包括 5 個非法的電話中心，執法地點包括保加利亞、羅馬尼亞和以色列等三國。

Europol 說，該詐騙集團利用網路廣告和社群媒體內的廣告，詐稱只要小額投資（最多 250 歐元），即可獲得極高利潤，以吸引受害者上鉤。接著詐騙團體假扮成所謂「個人理財顧問」，向受害者表示投入更多投資，可獲得更高的報酬；誤信為真的受害者，在投入更多資金後，這些資金就會被詐騙者領取一空，造成受害者巨額財務損失。

該詐騙集團在保加利亞和羅馬尼亞設立詐騙活動專用的電話「客服」中心，僱用約 100 名電話專員，以預先擬定好的話術來取信於受害者；但後續調查指出，許多該電話客服中心的電話專員，並不知道他們正在從事詐騙工作。

警方說，這波詐騙活動在 2019 年到 2021 年之間進行，詐騙集團成員遍及歐洲各國，包括烏克蘭、德國、西班牙、拉脫維亞、芬蘭、阿爾巴尼亞。

在這波執法行動之前數日，烏克蘭也會同 Europol 共同宣布破獲另一個國際投資詐騙案，該案同樣逮捕 5 名詐騙集團分子，涉及的財務損失高達 2.21 億美元。

建議使用者在網路或社群平台中看到以超高報酬為號召的廣告或貼文，都應特別提高警覺，勿點擊任何連結或按廣告要求方式聯絡，以免遭到詐騙造成財損。

- 資料來源：
  1. Europol @Europol
  2. Police disrupts $98M online fraud ring with 33,000 victims

## 2.3.3、 APT 駭侵團體利用特製 Cisco 路由器惡意軟體發動攻擊


英國、美國資安主管機關，包括英國國家資安中心（UK National Cyber Security Centre, NCSC）、美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）、美國國家安全局（National Security Agency, NSA）、美國聯邦調查局（Federal Bureau of Investigation, FBI），會同美國網通產品大廠 Cisco 聯合發表資安通報，指出 APT28 駭侵團體正在利用 Cisco 路由器的漏洞，以特製惡意軟體發動攻擊。

遭到 APT28 利用的 Cisco 路由器漏洞，是 CVE 編號 CVE-2017-6742 的一個老舊 SNMP 遠端執行任意程式碼漏洞；駭侵者先利用網路掃瞄工具，找出連上外部網路的 Cisco 路由器，然後對這些路由器發出某些指令，並以路由器的回應來確認該路由器是否存有此漏洞。接著駭侵者會利用該漏洞來植入名為「Jaguar Tooth」的惡意軟體，並且開始竊取各種機敏資訊，如內網系統未加密傳輸的登入資訊。

該漏洞存於 Cisco 推出且執行 C5350-ISM 版本 12.3(6) 的的 IOS 路由器，而 Cisco 早在 2017 年中便已修復該漏洞，但仍有不少 Cisco 路由器未曾修復此漏洞，導致駭侵者有機可乘。英美兩國資安主管機關與 Cisco 呼籲使用該

系列 Cisco 路由器的使用者與管理者，應立即將系統韌體更新至最新版本。

此外，上述單位也建議將 SNMP 切換為安全性更高的 NETCONF/RESTCONF 來進行遠端管理；如仍需經由外網透過 SNMP 管理裝置，也應妥善設定連線黑白名單。

建議使用該系列 Cisco 路由器的使用者與管理者，應立即將系統韌體更新至最新版本。將 SNMP 切換為安全性更高的 NETCONF/RESTCONF 來進行遠端管理；如仍需經由外網透過 SNMP 管理裝置，也應妥善設定連線黑白名單。

- 資料來源：
  1. Jaguar Tooth Cisco IOS malware that collects device information and enables backdoor access
  2. US, UK warn of govt hackers using custom malware on Cisco routers

## 2.4、社群媒體資安近況

### 駭侵者利用 Facebook 廣告，假冒 ChatGPT 散布惡意軟體


資安專家表示，近來發現有眾多駭侵者在 Facebook 上刊登廣告，假冒 OpenAI ChapGPT 的名義，實際上用以散布多種惡意軟體，用戶應特別提高警覺。

華盛頓郵報資安專欄作家 Jeremy B. Merrill 日前在其專欄中撰文指出，近期他本人在 Facebook 就看到 13 檔以 ChatGPT 為推廣內容的廣告；但事實上 ChatGPT 幕後的母公司 OpenAI 並未在 Facebook 上進行任何廣告宣傳活動。

Jereme B. Merrill 指出，這些廣告的出資者欄位會顯示為「OpenAI」或「GPT」，也有少數假冒為 Google Bard 人工智慧聊天工具；而這些廣告的內文，通常會包含一個連結，點按連結後就會下載惡意軟體；而文案會告訴受害者，以「888」作為解開檔案的密碼。

用戶如果誤點連結，即可能下載回惡意軟體，造成個人機敏資訊、各種服務登入資訊與權限遭竊的後果。

Jeremy B. Merrill 進一步在 Facebook 廣告資料庫平台以「Password 888」進行搜尋，找到了 59 檔在本（2023）年三月底前仍然活躍中的廣告；而這些廣告多半鎖定本身有在經營 Facebook 粉絲專頁，或對網路行銷有興趣的受

眾，以這些人當做廣告目標投放對象進行精準投放。

該專欄作家去信 Facebook 詢問為何這類詐騙廣告未遭移除，Facebook 表示駭侵者會利用各種手段逃過該平台的檢測系統，而 Facebook 也正在加強相關系統的學習與偵測能力。Facebook 也表示，駭侵者會利用當下流行的各種關鍵字來發送惡意軟體廣告。

建議用戶在 Facebook、Instagram、YouTube 或 Google 等社群平台或搜尋引擎看到這類包含連結的廣告時，務必提高警覺，切勿任意點按。

- 資料來源：

1. 廣告檔案庫
2. Fake ChatGPT preys on Facebook users
3. Fake ChatGPT, Bard ads con Facebook users: report

# 2.5、行動裝置資安訊息

## 2.5.1、Apple 修復 2 個可攻擊 iPhone 和 Mac 的 0-day 漏洞


Apple 於日前推出新版 iOS 16.4.1、iPadOS 16.4.1、macOS Ventura 13.3.1，解決兩個已遭駭侵者用於攻擊的 0-day 漏洞 CVE-2023-28206 與 CVE-2023-28205；iPhone、iPad 與 Mac 用戶應立即進行更新。

據 Apple 發表的資安通報指出，Apple 已接獲相關情報指出，這兩個 0-day 漏洞已遭到駭侵者積極用於攻擊活動。

頭一個 0-day 漏洞為 CVE-2023-28206，是存於 IOSurfaceAccelerator 中的越界寫入漏洞，可造成資料與系統崩潰，進而讓駭侵者可執行任意程式碼。

駭侵者可利用特製的惡意 App 來誘發此漏洞，以系統權限在受攻擊的裝置上執行任意程式碼。該漏洞的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），其危險程度評級亦為最高等級的「嚴重」（Critical）。

另一個這次獲得修補的 0-day 漏洞為 CVE-2023-28205，是存於 WebKit 內的記憶體釋放後使用漏洞；駭侵者可誘使受害者前往含有惡意程式碼的網頁，誘發此漏洞造成資料崩潰，接著即可在受害者裝置上執行任意程式碼。

受到這兩個漏洞影響的 Apple 產品，包括 iPhone 8 與後續機型、iPad Pro

全系列所有機型、iPad Air 第 3 代與後續機型、iPad 第 5 代與後續機型、iPad mini 第 5 代與後續機型、所有執行 macOS Ventura 的 Mac 各款電腦。

建議受影響之 iPhone、iPad、Mac 用戶應立即升級至新版 iOS 16.4.1、iPadOS 16.4.1、macOS Ventura 13.3.1，以修補這兩個 0-day 漏洞。

- 資料來源：
  1. About the security content of macOS Ventura 13.3.1
  2. Apple fixes two zero-days exploited to hack iPhones and Macs

## 2.5.2、新發現的「變色龍」Android 惡意軟體，會假冒為銀行、政府、加密貨幣 App


資安廠商 Cyble 旗下的資安研究人員，近日新發現一個 Android 惡意軟體「Chameleon」；這種惡意軟體會假扮成銀行、政府單位或加密貨幣交易所發行的 App， 用以對使用者發動各類駭侵攻擊。

據 Cyble 資安專家指出，Chameleon 鎖定波蘭與澳大利亞境內的 Android 行動裝置使用者發動攻擊，目前已假冒為澳大利亞某政府單位、波蘭 IKO 銀行與 CoinSpot 加密貨幣交易所。

報告也說，Chameleon 會在執行時進行多種檢查，以逃避各種資安防護軟體與機制的偵測。舉例來說，Chameleon 會檢查感染的 Android 裝置是否已經 root（越獄）或開啟 debug 模式，以防遭分析人員執行。

如果感染的環境是「正常」的，Chameleon 會要求使用者授予多種輔助使用權限，並且停用 Google Play Protect 保護機制，也不讓使用者自裝置中刪除該 App；接著 Chameleon 會連線到其控制伺服器，傳送受感染裝置的版本、型號、Root 狀態、所在國家、精確地理座標等資料。

接著 Chameleon 會決定要假扮成哪種服務，在前景中以 webview 開啟該服務真實的 URL，載入其網站內容，但在背景載入惡意程式碼，以執行各種惡意功能，包括竊取 cookie、執行鍵盤輸入內容錄製程式、注入釣魚網頁內

容、竊取手機解鎖密碼或手繪圖樣、竊取透過簡訊傳來的單次有效密碼，以通過二階段登入驗證等等。

建議 Android 用戶在下載安裝任何 App 時，應只從 Google 官方 Play Store 挑選評價優良的正版軟體下載，勿自任何第三方應用程式商店或不明來源連結下載任何應用程式。

- 資料來源：
  1. Chameleon: A New Android Malware Spotted In The Wild
  2. New Chameleon Android malware mimics bank, govt, and crypto apps

## 2.5.3、60 個含有惡意軟體 Goldoson 的 Android App 混入 Google Play Store，下載次數達 1 億次以上


資安廠商 McAfee 旗下的資安研究人員，近期發現一個名為 Goldoson 的惡意軟體，大量包含在 60 個上架到 Google Play Store 的 App 內供用戶下載安裝；且這些 App 的總下載次數高達 1 億次以上。

含有 Goldoson 且上架到 Google Play Store 的某些下載次數最多 App 與其下載安裝次數如下：

- L.POINT with L.PAY - 1000 萬次下載
- Swipe Brick Breaker - 1000 萬次下載
- Money Manager Expense & Budget - 1000 萬次下載
- GOM Player - 500 萬次下載
- LIVE Score, Real-Time Score - 500 萬次下載
- Pikicast - 500 萬次下載
- Compass 9: Smart Compass - 500 萬次下載
- GOM Audio - Music, Sync lyrics - 100 萬次下載
- LOTTE WORLD Magicpass - 100 萬次下載

- Bounce Brick Breaker - 100 萬次下載
- Infinite Slice - 100 萬次下載
- SomNote - Beautiful note app - 100 萬次下載
- Korea Subway Info: Metroid - 100 萬次下載

據研究人員指出，Goldoson 惡意軟體一旦安裝到使用者的 Android 手機內，就會竊取手機內的各種機敏資訊，包括安裝的應用程式清單、Wi-Fi 與 Bluetooth 連線裝置清單、使用者所在地的 GPS 座標資訊等，甚至還會在使用者不知情的情形下，於背景載入網路廣告進行惡意點按。

McAfee 指出，Goldoson 能取得哪些資訊，要視其在安裝過程中獲得的授權權限而定；Android 11 與後續版本對該惡意軟體取得資料的行徑，有較佳的保護能力，但 McAfee 也說，即使是採用最新版本的 Android，在這些惡意軟體中，仍有 10% 可獲得更高的權限。

McAfee 表示，是因為開發者使用了含有惡意軟體植入能力的第三方程式庫進行 App 開發，才導致這些 App 內含惡意程式碼。許多開發者已將自己上架到 Google Play Store 的 App 撤回修正並重新上架，但在第三方的應用程式商店中，可能還有相當多的 App 並未修正。

建議 Android 用戶除避免在非 Google Play Store 中下載 App 外，如果 App 要求過多權限，也應提高警覺，切勿任意授予權限。

- 資料來源：
  1. Goldoson: Privacy-invasive and Clicker Android Adware found in popular apps in South Korea
  2. Android malware infiltrates 60 Google Play apps with 100M installs

# 2.6、軟體系統資安議題

## 2.6.1、Google 再次緊急修補另一 Chrome 0-day 漏洞 CVE-2023-2316


Google 近日再次釋出 2023 年 4 月以來第二次 Google Chrome 瀏覽器緊急更新，以修復全新發現的 0-day 漏洞 CVE-2023-2136；所有使用 Google Chrome 與相容 Chromium 瀏覽器的使用者應立即更新。

此次緊急修補的 0-day 漏洞 CVE-2023-2136 是存於 Skia 的高危險性整數溢位漏洞，Skia 是 Google 旗下的開源跨平台 C++ 2D 繪圖程式庫，提供一系列 API 供 Google Chrome 繪製圖型、文字、形狀、影像、動畫等，是該瀏覽器算圖管線中的重要關鍵元件。

一般來說，駭侵者可以利用這類溢位錯誤來誘發受害系統發生記憶體崩潰，藉以遠端執行任意程式碼並且控制受害系統。

Google 在近日發表的相關資安通報中，並未詳細說明該 0-day 漏洞的詳細運作機制，僅表示已獲知 CVE-2023-2136 已經遭用於發動駭侵攻擊。Google 表示詳細的資訊，會等到多數 Google Chrome 使用者都已更新其瀏覽器後才會公開，以避免其他駭侵者利用技術資訊開發其他攻擊用惡意工具。

Google 新釋出的 Chrome 版本為 112.0.05615-137，除了 CVE-2023-2136 之外，也一并修復了另外 7 個漏洞；不過新推出的版本僅適用於 Windows 與 macOS 作業系統，Google 表示 Linux 版本將儘快推出。

建議所有使用 Google Chrome 與相容 Chromium 瀏覽器的使用者應立即更新，以降低遭到駭侵者利用已公開漏洞發動攻擊的風險。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google patches another actively exploited Chrome zero-day

## 2.6.2、新發現的 SLP 漏洞可導致放大倍數高達 2,200 倍的 DDoS 攻擊


資安廠商 Bitsight 與 Curesec 旗下的資安研究人員，近來共同發現一個存於 SLP 協定中的漏洞 CVE-2023-29552，可導致駭侵者用以發動大規模 DDoS 攻擊，攻擊量能放大規模可高達 2,200 倍。

SLP 是 Service Location Protocol 的縮寫，是一個制訂於 1997 年的老舊網際網路通訊協定，用於區域網路之內，讓裝置之間可以彼此輕易使用 UDP 與 TCP，透過通訊埠 427 來進行雙向通訊。

雖然 SLP 僅用於區域網路之內，但長久以來，許多單位都將這個通訊埠曝露在外部網路之下，導致可能遭到駭侵者攻擊的裝置多達數十萬台之譜。

據 BitSight 指出，CVE-2023-29552 這個漏洞可讓未經授權的駭侵者，在 SLP 伺服器上註冊任意服務，並透過操弄封包內容與大小的方式來進行最高放大倍數達 2,200 倍的 DoS 攻擊。

報告也指出，存有此漏洞的裝置不但種類多，數量也多；包括 VMWare ESXi Hypervisors、Konica Minota 生產的各型印表機、IBM Integrated Management Module、Planex 路由器等設備；據估計全球約有超過 2,000 家公私單位所有的 54,000 台裝置，因曝露在外部網路下，可能成為駭侵者用以發

動大規模 DDoS 攻擊的節點。

報告也說，這些曝險裝置分布廣泛，主要由在美國、英國、日本、德國、加拿大、法國、義大利、巴西、荷蘭、西班牙設有分支機構的財星 1,000 大公司擁有，業種橫跨科技、電信、醫療、保險、金融、餐旅、交通運輸等等。

建議各公私單位應定期檢視所屬網路設備與架構的配置情形，務必關閉無需對外連線的內網裝置與通訊埠；有必要對外連線的裝置或通訊埠，也應以防火牆等設施將之與外網隔離，以免遭到駭侵者輕易連入發動攻擊。

- 資料來源：
  1. New high-severity vulnerability (CVE-2023-29552) discovered in the Service Location Protocol (SLP)
  2. New SLP bug can lead to massive 2,200x DDoS amplification attacks

## 2.6.3、駭侵者利用 Google 關鍵字廣告散播 Bumblebee 惡意軟體，用以進行勒贖攻擊


資安廠商 Secureworks 旗下的資安專家近日指出，近來發現一個名為 Bumblebee 的惡意軟體，利用 Google 關鍵字廣告與 SEO 投毒（SEO Poisoning）方法，設立多個冒充多種知名軟體或服務的假冒網站，用以散布該惡意軟體。

遭到冒名設立假網站的知名軟體與服務，包括 Zoom、Cisco AnyConnect、ChatGPT、Citrix Workspace 等。

據 Secureworks 指出，Bumblebee 惡意軟體最早發現於 2022 年 4 月，疑似由惡名昭彰的勒贖團體 Conti 所開發，用來替換較老舊的 BazarLoader 後門軟體，其作用為取得受害者內部網路的存取權，以便執行勒贖攻擊。

在 Securewoks 觀察到的一個攻擊實例中，駭侵者先以一個遭到駭入的 WordPress 網站，設立一個冒充 Cisco AnyConnect 的假冒下載頁面，在頁面中的下載連結中放置已植入 Bumblebee 惡意軟體的 Cisco AnyConnect 安裝程式，然後利用 Google 關鍵字廣告吸引需要下載 Cisco AnyConnect 軟體的使用者上鉤。

使用者下載安裝時，除了會安裝到真正的 Cisco AnyConnect 外，還有另一個 PowerShell script 會安裝 Bumblebee 惡意軟體，該電腦就會成為勒贖攻擊

的潛在對象。

Secureworks 另外也觀察到冒充為 Zoom、ChatGPT、Critix Workspace 的惡意安裝檔，也利用同樣的手法，先設立假冒下載點，然後利用 Google 關鍵字廣告或經強化 SEO、排名名列前茅的假網站吸引受害者進入。

建議使用者下載任何軟體時，都應提高警覺，注意自己是否真正使用官方網站下載，而非在來路不明或以假亂真的網站下載。

- 資料來源：
  1. Bumblebee Malware Distributed Via Trojanized Installer Downloads
  2. Google ads push BumbleBee malware used by ransomware gangs

# 2.7、軟硬體漏洞資訊

## 2.7.1、HP 將於 90 天內修復多款 LaserJet 雷射印表機中的嚴重資安漏洞


印表機大廠 HP 日前發表資安通報，指出旗下多款 LaserJet 系列雷射印表機內含一個嚴重漏洞 CVE-2023-1707，可能導致用戶機敏資訊外洩；該公司將於 90 日內推出修補軟體，以修復該嚴重資安漏洞。

該漏洞在執行 FutureSmart 韌體版本 5.6 並啟用 IPSec (Internet Protocol Security) 功能的受影響雷射印表機上，駭侵者可藉由此漏洞存取受害用戶與其 HP 印表機與其他內部網路裝置上的通訊內容，藉以取得機敏資訊。

根據 HP 的資安通報指出，該漏洞的 CVSS 漏洞危險程度評分高達 9.1 分（滿分為 10 分），其危險程度評級為「嚴重」（Critical）等級。

這個 CVE-2023-1707 漏洞影響多達 50 款 HP 企業級雷射印表機與代管印表機等機種，受影響機種包括 HP Color LaserJet Enterprise M455、HP Color LaserJet Enterprise MFP M480、HP Color LaserJet Managed E45028、HP LaserJet Enterprise M406、HP LaserJet Enterprise MFP M430、HP LaserJet Managed E40040 等多款機種。

HP 表示，目前已暫停用戶下載安裝包含此漏洞在內的舊版印表機韌體，而修復此漏洞的新版韌體，將會在 90 天內推出；但目前並無暫時解決方案可用。HP 建議用戶可先將印表機韌體降版到 FS 5.5.0.3 版本。

- CVE 編號：CVE-2023-1707
- 影響產品(版本)：參考 HP 官方資安通報網頁。
- 解決方案：暫無，HP 將於 90 天內推出更新韌體。用戶應密切注意 HP 相關更新通知，並在未有更新版韌體可用期間，先將印表機韌體降版到 FS 5.5.0.3 版本。

- 資料來源：
  1. Certain HP Enterprise LaserJet and HP LaserJet Managed printers - Potential information disclosure
  2. HP to patch critical bug in LaserJet printers within 90 days

## 2.7.2、Microsoft 推出 2023 年 4 月 Patch Tuesday 每月例行更新修補包，共修復 97 個資安漏洞，內含 1 個 0-day 漏洞


Microsoft 日前推出 2023 年 4 月例行資安更新修補包「Patch Tuesday」，共修復多達 97 個資安漏洞，其中有 7 個是屬於「嚴重」(Critical) 危險程度的漏洞，另有 1 個 0-day 漏洞也獲得修復，這些漏洞已知遭用於攻擊活動。

本月 Patch Tuesday 修復的漏洞數量較上個月（2023 年 3 月）的 83 個資安漏洞多了不少，達 97 個；其中 7 個屬於嚴重等級的漏洞，分類上全部屬於遠端執行任意程式碼類型，也是各種軟體漏洞中危害最大的一類。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：20 個；
- 資安防護功能略過漏洞：8 個；
- 遠端執行任意程式碼漏洞：45 個；
- 資訊洩露漏洞：10 個；
- 服務阻斷（Denial of Service）漏洞：9 個；
- 假冒詐騙漏洞：9 個。

本月修復的 0-day 漏洞共有 1 個，是 CVE 編號為 CVE-2023-28252 的

Windows Common Log File System Driver 漏洞，屬於權限提升 (Elevation of Privilege) 漏洞。Microsoft 指出，駭侵者可以透過這個漏洞，取得最高等級的系統執行權限。該漏洞的 CVSS 危險程度評分高達 7.8 分（滿分為 10 分），其危險程度評級為「高」（High）等級。微軟亦在更新通報中指出，已知該 0-day 漏洞已遭駭侵者廣泛用於攻擊活動。

- CVE 編號：CVE-2023-28252 等
- 影響產品(版本)：Microsoft 旗下多種軟體，包括 Windows、Office、Exchange 等。
- 解決方案：建議系統管理者與 Microsoft 用戶應立即依照指示，以最快速度套用 Patch Tuesday 與不定期發表的資安更新，以避免駭侵者利用未及更新的漏洞發動攻擊。

- 資料來源：
  1. Security Update Guide
  2. Windows Common Log File System Driver Elevation of Privilege Vulnerability
  3. Microsoft April 2023 Patch Tuesday fixes 1 zero-day, 97 flaws

## 2.7.3、Google Chrome 緊急修復 0-day 漏洞 CVE-2023-2033


Google 近日針對 Google Chrome 瀏覽器一個 0-day 漏洞 CVE-2023-2033 緊急發布資安更新版本；據了解該漏洞已遭駭侵者大規模用於攻擊活動，使用者應立即更新。

這個 CVE 編號為 CVE-2023-2033 的 0-day 漏洞，存於 Chrome V8 JavaScript Engine 之內，屬於類型混淆漏洞。一般來說，這種漏洞可讓駭侵者利用特製的網頁來造成瀏覽器崩潰，接著就可以越過緩衝區界限來讀取甚至寫入記憶體資料，也可以用來遠端執行任意程式碼。

Google 在其發表的資安通報中表示，該公司已獲悉 CVE-2023-2033 0-day 漏洞已遭 大規模濫用於駭侵攻擊的情形，但該公司並未透露此漏洞的技術細節。

該 CVE-2023-2033 0-day 漏洞的 CVSS 危險程度評分高達 8.8 分（滿分為 10 分），危險程度評級為「高」（high）。

這個 CVE-2023-2033 漏洞會影響各作業系統版本的 Google Chrome，包括 Windows、macOS 與 Linux 版本。

使用者應立即透過 Google Chrome 內建的軟體更新機制，儘早將使用中的 Google Chrome 更新至版本號碼 V112.0.5615.121 或後續更新版本，以避免遭到駭侵者透過未修補完成的已知漏洞發動攻擊，造成資料遭竊或系統被挾持等災情。

- CVE 編號：CVE-2023-2033
- 影響產品(版本)：Google Chrome 版本 V112.0.5615.121 先前版本。
- 解決方案：建議使用 Google Chrome 或其他相容 Chromium 瀏覽器之使用者，應立即透過瀏覽器內建的軟體更新機制，儘早將使用中的 Google Chrome 相容瀏覽器更新至版本號碼 V112.0.5615.121 或後續更新版本。

- 資料來源：
  1. 桌面穩定頻道更新
  2. 谷歌 Chrome 緊急更新修復了 2023 年第一個零日漏洞

# 第 3 章、 資安研討會及活動

| 2023 D Forum 企業機房論壇-應用寒武紀，推動未來數據中心 | |
|---|---|
| **活動時間** | **5 月 12 日(五)** |
| **活動地點** | **台北國際會議中心 (台北市信義區信義路五段 1 號)** |
| **活動網站** | **https://www.digitimes.com.tw/seminar/DForum_20230512/** |
| **活動概要** |  <br>**主辦單位：DIGITIMES**<br>企業算力需求大爆發！<br>基於各項科技的創新，智慧應用「寒武紀大爆發」時代來臨！科技奇點不僅將各領域應用推向高峰，也昭示企業對於運算力需求急遽膨脹；直接帶動企業資料中心設備需求成長。<br><br>未來數據中心，將面臨以下挑戰：<br>高效穩定的運算力<br>環保的電力備援<br>維運的安全環境<br>化繁為簡的基礎架構 .....<br><br>參加辦法<br>1. 配合政府防疫政策鬆綁，您可自主決定是否配戴口罩；如有任何健 |

| | |
|---|---|
| | 康考量，歡迎全程配戴。<br><br>2. 本活動報名截止日 5 月 5 日(五) 。主辦單位將視報名狀況提前或延後線上報名時間。若報名者不克參加，可指派其他人選參加並通知主辦單位。<br><br>3. 本活動採預先線上報名並完成登錄手續，並視現場狀況決定是否開放現場報名。請勿偽造他人身份資料進行報名以免觸犯法律，主辦單位保留報名資格之最後審核權利。<br><br>4. 本活動將由主辦單位進行出席資格審核，與主題及屬性符合者為優先考量。<br><br>5. 通過審核者，系統將於活動前一天以電子郵件方式寄發含有報到編號/QR Code 的「報到通知」至您的電子信箱，以示您的出席資格；未通過審核者，亦會收到一封婉拒通知信。若您未收到任何通知信件，請上網站查詢。<br><br>6. 活動當日，請攜帶含有報到編號/QR Code 的「報到通知」至活動現場完成報到手續。<br><br>7. 本次活動若適逢天災(地震、颱風等)不可抗拒之因素，將延期舉辦時間另行通知。<br><br>8. 若因不可預測之突發因素，主辦單位得保留研討會課程及講師之變更權利。 |

| D Webinar 數位轉型 馭雲論壇 | |
|---|---|
| **活動時間** | **2023/5/17 ~ 2023/5/18 14:00** |
| **活動地點** | **線上研討會** |
| **活動網站** | **https://www.digitimes.com.tw/seminar/DWebinar_20230517/** |
| **活動概要** |  <br>**主辦單位：DIGITIMES**<br>攜手智能雲隊友<br>準備好善用雲力了嗎?後疫情時代數位轉型與供應鏈重組，用雲需求大爆發 !從企業至政府皆努力耕雲，借助人工智慧能提供創新服務，以數據資料分析驅動決策流程，建構即時又有效的營運韌性，雲端技術與服務徹底翻轉企業格局。<br>無痛轉型的新契機再現!<br><br>參加辦法<br>1. 本活動報名截止日為 2023 年 5 月 11 日(四)。主辦單位將視報名狀況提前或延後線上報名時間。<br>2. 參加方式：線上活動。完成報名後，另行寄發收視連結；活動當天請於議程開始前登入。<br>3. 本活動採預先線上報名並完成登錄手續，請勿偽造他人身份資料進行報名以免觸犯法律，主辦單位保留報名資格之最後審核權利。 |

| | |
|---|---|
| | 4. 本活動將由主辦單位進行出席資格審核，與主題及屬性符合者為優先考量。<br>5. 凡參加本次活動所舉辦之贈品或抽獎，因有登錄資料不實或冒用他人身份，主辦單位有權取消其得獎資格。<br>6. 本活動贈品或獎品係由供應商提供。若贈品或獎品有任何瑕疵，請逕洽供應商。主辦單位對獎品之瑕疵不負瑕疵賠償責任。<br>7. DIGITIMES 保留修改本活動規則之權利，毋須另行作出解釋或通知。<br>8. 若因不可預測之突發因素，主辦單位得保留研討會課程及講師之變更權利。<br>9. 洽詢方式：mail：seminar@digitimes.com，或致電：+886-2-87128866*353 活動小組<br>(備註：免費活動。主辦單位保留變更時間、形式與議程之權力，請以活動當天網頁為準。) |

| 第 4 屆 ICANN APAC-TWNIC Engagement Forum 暨第 39 屆 TWNIC IP 政策資源管理會議 | |
|---|---|
| **活動時間** | **5 月 22 日(一) ~ 5 月 24 日(三)** |
| **活動地點** | **台北晶華酒店 3F 宴會廳(台北市中山北路二段 39 巷 3 號)** |
| **活動網站** | https://forum.twnic.tw |
| **活動概要** |  <br>**主辦單位：ICANN、TWNIC**<br>由 TWNIC、ICANN 主辦 TWCERT/CC 協辦，第四屆 ICANN APAC-TWNIC Engagement Forum，此論壇將針對全球域名、IP 位址及網路安全等主題，與國際網路利害關係人面對面進行深入探討。<br><br>「第 4 屆 ICANN APAC-TWNIC 合作交流論壇暨第 39 屆 TWNIC IP 資源政策管理會議」<br><Day 1-Day 2><br>● 5/23(二) 8:30 - 17:45(Main Conferences)<br>➢ TWCERT/CC 參與 16:30-17:45 Tech Session<br>● 5/24(三) 8:30 - 18:00(Main Conferences)<br>➢ TWCERT/CC 參與 14:00-15:15 Plenary 4 Security Topic: Addressing Domain Name Abuse<br>註：上午場次備有同步口譯 |

# 第 4 章、 TVN 漏洞公告

**TWCERT/CC 上月份發布之資安漏洞資訊如下表：**

| SUNNET CTMS 培訓大師 - Path Traversal | |
|---|---|
| **TVN / CVE ID** | TVN- 202302004 / CVE-2023-24836 |
| **CVSS** | 8.8 (High) |
| **影響產品** | SUNNET CTMS 培訓大師 v7.0 1227 |
| **問題描述** | SUNNET CTMS 檔案上傳功能存在 Path Traversal 漏洞，遠端攻擊者以使用者權限登入後，可利用此漏洞繞過檔案檢查機制，將腳本上傳至任意系統目錄後執行，藉以操作系統或中斷服務。 |
| **解決方法** | 聯繫旭聯科技進行版本更新/升級 |
| **公開日期** | 2023-04-10 |
| **相關連結** | https://www.twcert.org.tw/newepaper/cp-151-7033-878ab-3.html |

# 第 5 章、 2023 年 4 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

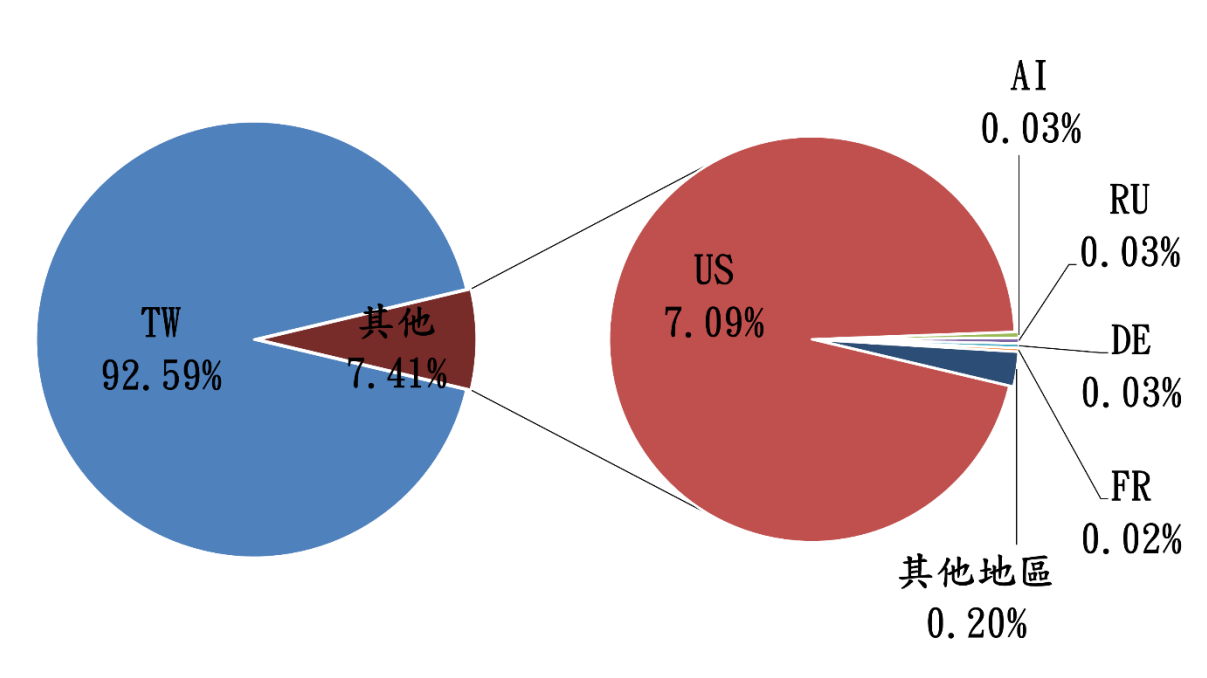


圖 1、分享地區統計圖

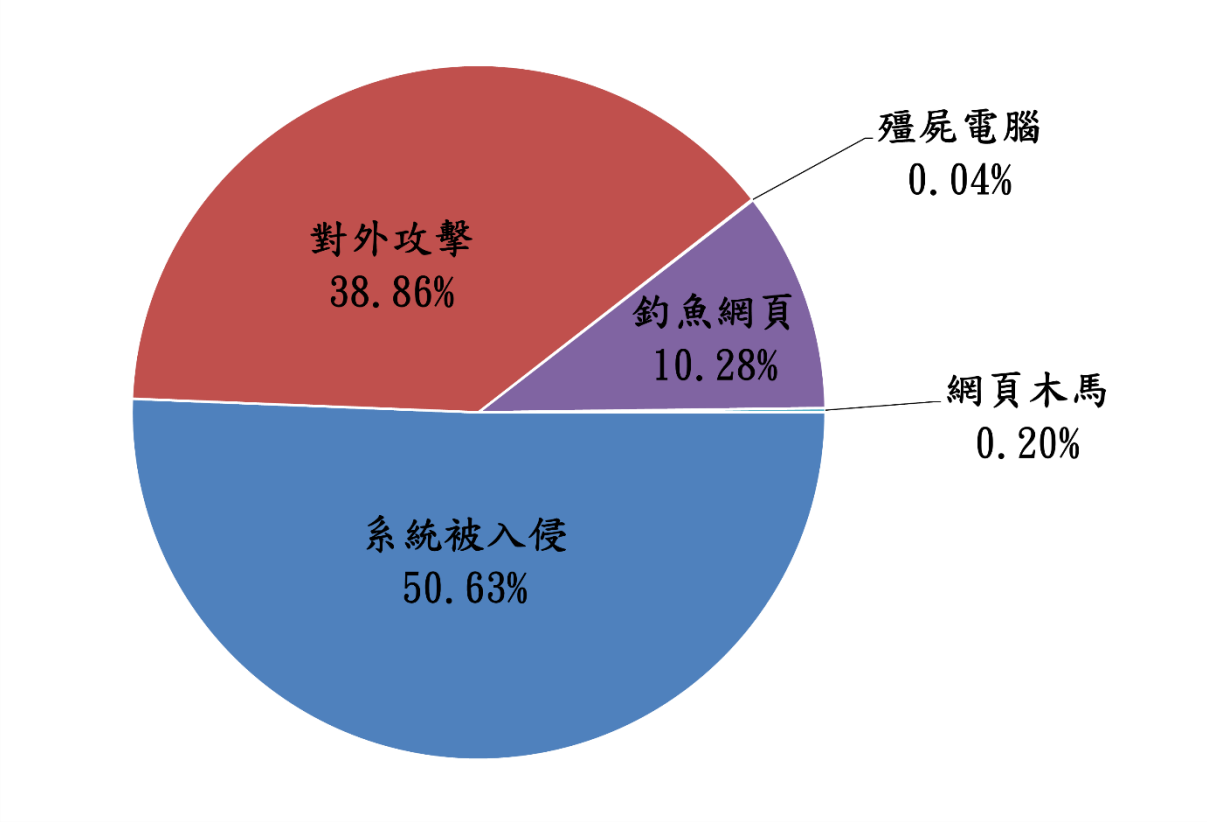


圖 2、分享類型統計圖

發行單位：**台灣電腦網路危機處理暨協調中心**
**(Taiwan Computer Emergency Response Team / Coordination Center)**

出刊日期：**2023 年 5 月 10 日**

編輯：**TWCERT/CC 團隊**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**