TWCERT/CC 資安情資電子報

2022 年 7 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：主題式資訊安全專題分享。

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

使用瀏覽器與擴充套件應注意之資安威脅與防護

- 網頁瀏覽器種類繁多，且每一種瀏覽器的功能都不盡相同，使用者可根據自身需求選擇最適合的瀏覽器，Internet Explorer、Google Chrome、Mozilla Firefox、Safari、Microsoft Edge，以及 Opera 為較常見之瀏覽器。
- 目前全球使用數量最多的瀏覽器為 Google Chrome，同時也是國內使用比例最高之瀏覽器。
- 瀏覽器本身連接網際網路時，難免會有機敏資訊或具有一定價值的資料也透過瀏覽器進行傳遞或儲存，導致攻擊者將瀏覽器與瀏覽伺服器視為攻擊目標。
- 當漏洞被發現後，大部分的廠商會在短時間內進行修補，若使用者未在第一時間配合更新修補，一旦攻擊者透過該漏洞進行惡意行為，仍會因此受害。
- 除了瀏覽器本身，越來越多的擴充套件也逐漸成為攻擊者的目標。攻擊者會透過帶有惡意程式或有漏洞的擴充套件，進行惡意行為。
- 為減少瀏覽器及擴充套件所帶來之資安威脅，使用者必須採取防範措施，包括提升資安意識、採用自動即時更新、讓權限最小化等，避免資訊外洩，甚至造成財務或人身安全之威脅。

一、簡介

網頁瀏覽器(Web Browser)簡稱瀏覽器，是一種用來連接網際網路，存取網站並進行相關活動的應用程式。市面上的瀏覽器各有其特色，使用者可選擇自己喜好的瀏覽器使用。較常被使用的瀏覽器包含 Internet Explorer (簡稱 IE)、Google Chrome (簡稱 Chrome)、Mozilla Firefox (簡稱 Firefox)、Safari、Microsoft Edge (簡稱 Edge)，以及 Opera。

根據愛爾蘭網站流量分析工具網站 StatCounter，2020 年 5 月的全球統計，最多使用者的瀏覽器為 Google Chrome，佔全球所有使用者的 63.93%，第二是 Safari 瀏覽器佔 18.19%，再者為 Firefox 瀏覽器佔 4.38%。於同一時間的統計中，國內最多使用者的瀏覽器為 Google Chrome，佔國內所有使用者的 63.94%，第二為 Safari 瀏覽器佔 26.73%，再者為 Firefox 瀏覽器佔 1.85%，可見國內瀏覽器的使用狀況與全球瀏覽器使用狀況相差不大。

為了滿足使用者的特定需求，諸多瀏覽器於是開放瀏覽器擴充套件(Brower Extension)功能，讓使用者安裝使用。然而，隨著瀏覽器的種類、功能及擴充套件的類型越來越多，使用者越來越便於使用，卻也導致了瀏覽器成為攻擊者的目標。

二、瀏覽器之資安威脅

瀏覽器資安威脅案例

對使用者而言，瀏覽器的許多功能，例如記錄使用者曾經瀏覽過的網站、記憶相關帳號密碼等，都相當便利且重要。但對攻擊者而言，網頁瀏覽器就猶如寶庫一般，一旦成功控制使用者的瀏覽器，所有個資都將一覽無遺。攻擊者在入侵受害者的瀏覽器後，所著重的目標及竊取的資訊大致有下述五種：

1. 瀏覽的歷史紀錄：攻擊者透過檢閱使用者的瀏覽歷史紀錄，可以得知使用者的習慣、興趣、訪問網站的類型，以及使用者的行為模式，藉此知道透過何

種方式及類型容易讓使用者上鉤，或是在盜用使用者電子商務帳號購物時，知道應支付何種類型的商品，較能順利取得。

2. 儲存的密碼：大部分的瀏覽器都有儲存特定網站帳號密碼的功能，一旦攻擊者入侵使用者的瀏覽器，其帳號、密碼，以及其帳密所使用的網站都將一覽無遺，甚至可重置使用者的網站帳密，讓使用者除了資料遭竊外，更可能產生自己反而無法登入的困境與損失。

3. 自動填入的資訊：許多瀏覽器會協助記錄使用者常用的資訊，包括電子商務網站的付款方式、信用卡卡號、通信地址、電話號碼等，讓使用者在遇到常見的欄位時自動帶入，省掉填寫的麻煩。上述資訊若毫無防護地被竊取，除了財務上的損失外，更嚴重的可能有人身安全之憂慮。

4. Cookie：為方便再次連線上網，需要記錄使用者身分、上次連線時的狀態、內容、活動等資訊，用以接續上一次連線後繼續使用。然而，這些紀錄可能導致攻擊者獲取使用者的行為模式，竊取身分資訊，進行更嚴重的惡意行為。

5. 快取(Cache)：許多網站為了增加處理效率，伺服器會將一部分的網頁內容存在本機中，減少下一次使用者連線時所需花費的時間。然而，快取資訊同樣也暴露了使用者與網站連線之行為軌跡，攻擊者可透過該行為模式設計針對性的攻擊手法，讓使用者更容易上當受騙。

瀏覽器與瀏覽伺服器之漏洞，可能導致瀏覽器與瀏覽伺服器的損壞、資料被竊取或遭他人控制。其威脅類型大致如下：

1. 阻斷服務攻擊(Denial-of-Service, DoS)：透過 DoS 漏洞，攻擊者可運用特定手段，導致系統運行錯誤或中斷服務。

2. 代碼執行(Code Execution)：透過代碼執行漏洞，攻擊者可在受害系統中執行

任意程式碼，促使系統服務中斷或竊取機敏資訊。

3. 溢位攻擊(Overflow)：透過溢位攻擊漏洞，攻擊者可輸入過大的資料，引發系統服務中斷，甚至可以在其中執行任意程式碼。

4. 記憶體損壞(Memory Corruption)：透過記憶體損壞漏洞，攻擊者可輸入特定程式或字串，讓系統記憶體損壞，進而產生服務中斷或其他問題。

5. 跨網站指令碼(Cross-Site Scripting, XSS)：透過跨網站指令碼漏洞，攻擊者可注入惡意程式碼於網站中，使其他瀏覽該網頁的使用者也受到惡意程式碼影響。

6. 規避(Bypass Something)：透過規避漏洞，攻擊者可繞過系統安全驗證機制，進而取得相關權限以竊取資訊或進行惡意行為。

7. 資料洩漏(Gain Information)：透過資料洩漏漏洞，攻擊者可用特定方式，取得部分未能落實資安防護的機敏資訊。

8. 擴權(Gain Privilege)：透過擴權漏洞，攻擊者可經由特定路徑或程式碼，取得特定人士或更高層級的權限，進行惡意行為。

許多瀏覽器會定時提供更新檔以修補被發現之資安漏洞，但諸多使用者通常不會即時更新，以致受到嚴重之資安威脅。透過瀏覽器與瀏覽伺服器之資安漏洞進行攻擊之案例如下：

1. 針對IE瀏覽器漏洞散播勒索病毒：滲透測試工具Magnitude在2019年10月，被發現針對IE瀏覽器的CVE-2018-8641以及CVE-2019-1367漏洞進行攻擊，以此散播勒索病毒，此次的攻擊對象以亞太地區為主。

2. 利用IE與Firefox瀏覽器漏洞散播惡意程式：2020年1月，攻擊者利用Firefox

的資安漏洞 CVE-2019-17026，以及 IE 的資安漏洞 CVE-2020-0674，對其使用者進行攻擊。該攻擊主要是先將使用者導至惡意網站中，下載針對漏洞的攻擊程式碼，進而散播惡意程式。

3. 針對 Chrome 瀏覽器漏洞發動之水坑攻擊：2019 年 11 月，韓國新聞網站遭攻擊者入侵，被載入惡意腳本，進行水坑攻擊(Watering Hole Attack)，並且利用 Chrome 瀏覽器漏洞 CVE-2019-13720，讓受害主機下載其他惡意程式，進而達到散播惡意程式之目的。

除了上述實際案例之外，有更多的資安漏洞還未被發現或尚未進行明顯之惡意行為。雖然瀏覽器的資安相當重要，但其漏洞修補方式仍然是以更新系統版本為主，一旦使用者未能配合廠商即時更新且還持續使用，則其面臨的資安風險將會大增。

瀏覽器擴充套件資安威脅案例

大部分的瀏覽器，為了提升其便利性及客製化功能，都建立擴充套件商店，讓使用者自行選擇安裝，使瀏覽器更加符合自身需求。然而，難免有些擴充套件存有資安漏洞或含有惡意程式，增添使用者的資安風險。根據 Firefox 的擴充套件政策，指出擴充套件除了基本功能以外，不應有下列行為：

1. 損害使用者的隱私或安全性：例如將使用者資訊在未被允許下，傳送給第三方。

2. 更改瀏覽器設定：瀏覽器本身存有許多預設設定，包含分頁管理、下載詢問或搜索引擎等，擴充套件不應自動變更其設定。

3. 對瀏覽器或網頁內容進行更改：例如在瀏覽網頁時，對網頁的大小、形式做變更，甚至置入廣告等行為，都不應存在。

4. 存有與主要功能無關的其他功能或特性：例如新聞訂閱擴充套件可存取使用者的通訊檔案，或是語言翻譯軟體自動下載額外檔案，都是在擴充套件主要功能外不應有的行為。

大部分的瀏覽器均要求開發者提供足夠透明化的擴充套件，讓使用者能清楚地識別該擴充套件之功能，但仍有諸多擴充套件因存有資安漏洞，而成為攻擊目標。透過擴充套件之資安漏洞進行攻擊之案例如下：

1. 被用以攻擊俄羅斯醫院之 Adobe Flash Player 資安漏洞：2018 年 12 月，Adobe 緊急修補一個被用於攻擊俄羅斯醫院 Polyclinic No.2 的 CVE-2018-15982 資安漏洞。該漏洞讓攻擊者可以遠端執行任意程式碼，達成傳播惡意程式並控制受害主機的目的。

2. 存有竊取個資惡意程式碼之 Chrome 擴充套件：2018 年 9 月，MEGA.nz 文件共享服務之 Chrome 擴充套件被發現存有惡意程式，會竊取使用者的帳號、密碼，以及加密貨幣帳號及金鑰，以獲取不法利益。

3. 私下記錄個人購物行為之優惠券擴充套件：2019 年 12 月，Amazon 提出對瀏覽器擴充套件 Honey 的安全風險警告，認為該擴充套件會侵犯使用者的隱私。Honey 是一種搜尋相關優惠券之擴充套件，Amazon 認為 Honey 會在未經使用者同意的情況下，蒐集並跟蹤個人購物資訊，因此提出警告。

擴充套件雖然僅為瀏覽器的附屬工具，但其可能產生的資安危害依舊不小，使用者必須在安裝瀏覽器擴充套件時多加留意，一旦使用的擴充套件被發現有安全漏洞，應立刻配合廠商進行修補、更新，以維持其安全性。

三、瀏覽器資安防護

許多攻擊者會針對特定具足夠價值的資訊進行破解及竊取，包括瀏覽的歷史紀錄、儲存的密碼、自動填入的資訊等。因此，為避免這些資訊遭攻擊

者竊取，使用者應進行適度的防護機制：

1. 瀏覽歷史紀錄應定期清除或使用無痕模式：使用者應習慣定期清除瀏覽過的歷史紀錄，尤其是在進行金融資訊、網路銀行等機敏作業之後，應立即清除。此外，使用者也可設定瀏覽器定期清除或於關閉瀏覽器時即自動清除等機制。在使用公共主機或公共網路時，應採無痕模式，避免瀏覽器留下使用者的瀏覽歷程。

2. 避免瀏覽器自動儲存密碼：使用者應儘量減少透過瀏覽器記憶相關帳號密碼，避免攻擊者在入侵瀏覽器後便竊取所有帳號密碼。

3. 避免使用自動填入的資訊：使用者應避免使用自動填入功能，盡量以手動輸入方式操作，雖然需花時間輸入相關資訊，但可避免資安威脅。

4. 應定期清除 Cookie 資訊：除了可透過無痕模式進行網路行為之外，建議定期清除 Cookie 資訊，避免留存過多的資訊，導致個資外洩。

5. 快取應定期清除或使用無痕模式：使用者除了可透過無痕模式瀏覽網頁，避免留存相關紀錄之外，盡量定期清除瀏覽器中的快取資訊，提升使用安全。

除了針對瀏覽器中可能產生資安威脅的資訊進行防護之外，使用者在使用瀏覽器時，也應遵循相關安全措施：

1. 檢閱瀏覽器安全性相關文件：除了常見的安全建議及教學外，不同的瀏覽器會提供針對該瀏覽器的相關安全性文件，使用者應確實閱讀，並據以操作、設定。

2. 啟用自動更新：許多使用者並非時常關注瀏覽器版本之修訂狀態，因此，啟用自動更新之功能，一旦出現新版本之應用程式，瀏覽器將會自動更新，避免資安威脅。

3. 安裝相關防護軟體：除了信任瀏覽器本身的檢測和防護外，使用者亦可安裝額外之防護軟體，搭配瀏覽器達到雙重防護之保障。

4. 提升資訊安全意識：在進行網路行為時，除了倚賴瀏覽器本身的安全功能外，使用者亦應提高安全意識，避免受騙上當。

5. 遵循最小權限原則：當使用者在允許或啟用瀏覽器之功能時，應僅選擇真正必需之功能，不會使用到的功能盡量減少啟用，以免成為攻擊者的入侵捷徑。

除了瀏覽器本身之安全隱憂外，其擴充套件也可能成為攻擊者的捷徑及目標。使用者應針對瀏覽器之擴充套件，遵循特定安全機制：

1. 減少擴充套件安裝數量：僅使用必需的擴充套件，降低安裝到惡意擴充套件之機率，減少因其安全漏洞所產生之資安威脅。

2. 只從官方商店下載安裝：雖然瀏覽器本身難以確保其擴充套件百分之百的安全，但相較於其他不知名的擴充套件商店，官方商店所提供之擴充套件安全性是較高的。

3. 注意擴充套件權限要求：若擴充套件會提出不合理的權限要求，往往是資料竊取等惡意行為的前兆。因此，使用者應對其權限要求多加注意。

4. 關注擴充套件惡意名單：使用者應關注瀏覽器或相關資安公司所公告之擴充套件黑名單，避免下載到惡意的擴充套件，以確保使用安全。

四、結論與建議

1. 由於瀏覽器會處理或儲存使用者許多資訊，因此，不論是瀏覽器本身或其搭配之擴充套件，都是攻擊者的目標。

2. 通常瀏覽器都會對自身系統及擴充套件進行一定程度的安全檢測，但仍難免

留有資安漏洞，建議不論是個人或企業，都應學習或參與相關教育訓練，減少攻擊者從使用者端進行惡意行為。

3. 針對瀏覽器本身的攻擊模式較為固定，企業在進行瀏覽器防護時，應對常見的攻擊模式進行即時監測，一旦有任何攻擊跡象可立即防護，避免擴大受害範圍。

4. 擴充套件經過數次改版後，恐遭到攻擊者劫持或開始進行惡意行為。因此，使用者應定期檢閱擴充套件更新後是否有不適當的要求，或已被列入黑名單。也應定期清理沒有持續使用的擴充套件，減少受害機率。

5. 建議使用者若非真正必要，盡量減少透過瀏覽器進行機敏資訊的傳輸，尤其與金融相關的申請、轉帳、付費等。也應盡量不安裝與金融或其他機敏資訊相關的擴充套件，以免個人資訊被蒐集、販賣。

6. 由於瀏覽器本身是使用者進行網路行為的重要入口，一旦安全性不足，將會導致嚴重的後果。建議使用者必須確認自身安裝的瀏覽器是否足夠安全、是否有足夠能量在發現漏洞後即時修補，甚至是否有持續支援並更新。避免使用到安全防護薄弱的瀏覽器，讓自身處於資安威脅之中。

- 資料來源：

1. browser
2. Browser Market Share Worldwide
3. Browser Market Share Taiwan
4. What are extensions?
5. 5 common browser security threats, and how to handle them
6. Microsoft » Internet Explorer : Vulnerability Statistics

7. Google » Chrome : Vulnerability Statistics
8. Mozilla » Firefox : Vulnerability Statistics
9. Apple » Safari : Vulnerability Statistics
10. Microsoft » Edge : Vulnerability Statistics
11. Opera : Vulnerability Statistics
12. Vulnerabilities By Type
13. Magnitude exploit kit – evolution
14. Attacks Simultaneously Exploiting Vulnerability in IE (CVE-2020-0674) and Firefox (CVE-2019-17026)
15. The zero-day exploits of Operation WizardOpium
16. Add-on Policies
17. Operation Poison Needles - APT Group Attacked the Polyclinic of the Presidential Administration of R
18. Security warning for MEGA Chrome extension users
19. Amazon Takes a Swipe at PayPal's $4 Billion Acquisition
20. Securing Your Web Browser
21. Why you should be careful with browser extensions

第 2 章、 資訊安全宣導

美國資安主管機關指出 36 種顯著漏洞正遭大規模濫用於攻擊，建議用戶應立即修補

美國 CISA 公告 36 種漏洞正遭受多個駭侵團體大規模濫用於攻擊行動，建議相關用戶應立即進行修補。

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），日前新公告 36 種漏洞，目前正遭受多個駭侵團體大規模濫用於攻擊行動；相關軟硬體系統用戶應立即進行修補，以免遭到駭侵攻擊。

最新公告新增到 CISA「已知遭濫用之漏洞清單」（Known Exploited Vulnerabilities Catalog）的 36 種漏洞，分別存於 Microsoft、Google、Adobe、Cisco、Netgear、QNAP 等公司的軟硬體產品，重點漏洞如下：

- Microsoft：CVE-2012-4969（存於 Internet Explorer 的遠端任意程式碼執行漏洞）、CVE-2013-1331（存於 Microsoft Office 的緩衝區溢位漏洞，可用以進行遠端攻擊）、CVE-2012-0151（存於 Microsoft Windows 的簽署驗證錯誤，可遠端執行任意程式碼）。
- Google：CVE-2016-1646 與 CVE-2015-5198（存於 Google Chromium V8 引擎，可進行 DoS 攻擊）、CVE-2018-17463 與 CVE-2017-5070

（同樣存於 Gogole Chromium V8 引擎，可用於遠端執行任意程式碼）。

- Adobe：CVE-2009-4324（存於 Adobe Acrobat 與 Reader，可透過特製 PDF 檔遠端執行任意程式碼）、CVE-2010-1297（存於 Adobe Flash Player 的記憶體崩潰漏洞，可用以遠端執行任意程式碼或發動 DoS 攻擊）。
- Cisco RV 系列：CVE-2019-15271，攻擊者可以取得 root 權限並且遠端執行任意程式碼。
- Netgear：CVE-2017-6862，存於多種該品牌裝置中的緩衝區溢位漏洞，可讓駭侵者跳過安全驗證並遠端執行任意程式碼。
- QNAP：CVE-2019-7192，存於 QNAP NAS 中 Photo Station 軟體的存取權限控制錯誤，可讓未經授權的駭侵者遠端控制裝置。

CISA 不時會發布更新「已知遭濫用之漏洞清單」，建議各軟硬體產品用戶及系統管理員，應隨時注意更新消息，確保軟體與韌體均為最新版本，以避免駭侵者利用已知資安漏洞發動攻擊得逞而造成損失。

- 資料來源：
  1. CISA Adds 36 Known Exploited Vulnerabilities to Catalog
  2. KNOWN EXPLOITED VULNERABILITIES CATALOG
  3. CISA warning: Hackers are exploiting these 36 "significant" cybersecurity vulnerabilities - so patch

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、46% 資深高階資安人員因駭侵防範壓力大增而萌生辭意

資安廠商發表調查報告，指出有高達 46 % 的高階與資深資安工作者，因為近年駭侵攻擊次數與強度不斷提升，因而考慮辭去相關工作。

資安廠商 Deep Instinct 日前發表針對多家 1,000 名員工以上公司資安人員的調查報告，指出有高達 46% 的高階與資深資安工作者，因為近年駭侵攻擊次數與強度不斷提升，導致工作壓力大增，因而考慮辭去相關工作。

報告中指出，近年來以勒贖攻擊、供應鏈攻擊為主的各式駭侵攻擊，在攻擊規模、發生頻率、技術難度與造成的損害方面不斷提升，使得各公私單位的資安相關人員的工作負荷與壓力「提升到難以為繼的程度」；有超過 90% 的資安防護相關人員表示工作壓力過大，且有相當程度的資安人員認為這種過度壓力，將會影響其工作上的表現。

報告中也指出，資安威脅加劇不只影響基層資安工作人員，對包括資安長、技術長、IT 策略總監等主管級人員也造成相當大的工作壓力。

報告也提到，由於疫情造成的遠距工作類型，也使資安相關人員的工作變得更加繁重；報告中有 52% 的資安主管認為，各單位大量使用行動裝置遠距工作，使得單位內部的設備更加複雜，也加重了資安相關人員的工作負

荷。

至於非主管階層的資安人員，有 47% 的人指出單位期待他們能阻擋一切資安威脅，但這是不可能的，因此而感到壓力沉重；有 43% 資安人員指出他們必須隨時待命；另有 40% 資安人員表示組織的資安編制人員不足，資源短缺，也造成其工作壓力大增。

在面對勒贖攻擊的威脅方面，38% 人員指出其服務單位曾受勒贖攻擊，且曾支付贖金以取回檔案；但其中有 46% 即使支付贖金，單位擁有的檔案與機敏資訊仍遭曝光，另外更有 23% 曾遭駭侵團體進一步勒贖。

面對日益嚴重的資安威脅，各公私單位應更加重視在資安方面的軟硬體、人員編制與顧問服務的投資，提升資安人員的士氣與可用資源，以免身為第一道防線的資安人員崩潰，影響整體資安防護能力。

- 資料來源：
  1. Why your cybersecurity leaders and staff are thinking about leaving
  2. The unrelenting threat of ransomware is pushing cybersecurity workers to quit

3.1.2、10 家營運科技設備大廠 56 個漏洞，造成多家關鍵基礎設施數千套生產設備曝險

資安廠商旗下的資安研究單位 Vedere Labs，發表研究報告，指出 10 家大型營運科技大廠設備，一共存有 56 個各式資安漏洞。

資安廠商 Forescout 旗下的資安研究單位 Vedere Labs，近日發表研究報告，指出 10 家大型營運科技（Operational Technology, OT）大廠設備，一共存有 56 個各式資安漏洞；這些漏洞可造成多家採用該批設備的關鍵基礎設施生產裝置，遭到各式不同形態的駭侵攻擊。

報告提到的 10 家 OT 設備大廠，包括 Honeywell、Motorola、Omron、Siemens、JTEKT、Bentley、Nevada、Phoenix Contact、ProConOS、Yokogawa 等；而這些設備大廠產品被發現的 56 個資安漏洞，在該報告中合稱為「Icefall」。

報告指出，這 56 個資安漏洞可使駭侵者用以發動多種駭侵攻擊，依其比例如下：

- 不當獲取各式登入資訊：38%；
- 韌體操弄：21%；
- 遠端執行任意程式碼：14%；
- 組態設定操弄：8%；
- 服務阻斷攻擊（DoS）：8%；

- 跳過驗證流程：6%；
- 檔案操弄：3%；
- 邏輯操弄：2%。

Forescout 在報告中指出，許多這類 OT 設備的漏洞，係源於設計時的安全性考量不足所致，而這是 OT 設備常見的現象。

報告舉例指出，許多 OT 設備的登入資訊，不但沒有以加密方式儲存或傳送，在各種加密機制方面，從加密演算法到各種資安驗證流程都相當薄弱。Frescout 指出，74% 存有這些漏洞的 OT 設備都得過各式資安認證，顯見這些資安認證本身的稽核和審查過程都不夠嚴謹。

建議各關鍵基礎設施單位，必須徹底進行資安驗證稽核，並且將可能遭到攻擊或經常存有漏洞的設備加強保護，避免曝露於外網，且加強使用者的資安防護技能與意識。

- 資料來源：
  1. OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT
  2. Icefall: 56 flaws impact thousands of exposed industrial devices

3.1.3、360 萬台以上 MySQL 伺服器，曝露於 Internet 上

資安研究團體 The Shadowserver Foundation 發表研究報告，指出全世界有 360 萬台以上的 MySQL 伺服器，未經適當防護而在 Internet 上曝露。

資安研究團體 The Shadowserver Foundation 日前發表研究報告，指出全世界有 360 萬台以上的 MySQL 伺服器，未經適當防護而在 Internet 上曝露，且可接受各種指令進行操作，因而成為駭侵者的最佳攻擊目標。

調查顯示全球網路約有 360 萬台 MySQL server 於 Internet 上曝露，且使用 MySQL 預設的通訊埠 TCP 3306。這些為數眾多的 MySQL 伺服器，有約 230 萬台使用 IPV4，其餘 130 萬台使用 IPV6 連線。

報告也指出，若以曝露數量來排序，美國境內曝露於 Internet 上的 MySQL server 數量最多，有超過 120 萬台以上，其餘國家則包括中國、德國、新加坡、荷蘭、波蘭等。

報告也指出，除了這些確定曝露在 Internet 上，可能遭到攻擊的 MySQL server 外，也有一些具備部分防護，不會對掃瞄用的 TLS / 非 TLS 於 port 3306 上的連線要求提供回應的 MySQL server；但在所有偵測到的 MySQL server 中，高達 67% 都可以直接透過 Internet 存取；這是十分危險的，因為駭侵者將能輕鬆駭入這些幾乎不設防的 MySQL server 中，進行資料竊取或其他進階攻擊。

調查也發現這些對外曝露的 MySQL server，其版本號碼都十分老舊；曝露伺服器數量最多的 MySQL 版本，為 5.7.33-36，並非最新版本。

建議 MySQL 資料庫管理員應時時維持 MySQL 為最新版本，且如必須與外部網路連線，則必須套用嚴格的使用者檢查機制，且避免使用預設的 TCP 3306 埠。

- 資料來源：
  1. Over 3.6 million exposed MySQL servers on IPv4 and IPv6
  2. Over 3.6 million MySQL servers found exposed on the Internet

3.2、新興應用資安

3.2.1、駭客利用 Atlassian Confluence Server 修補完成的漏洞偷偷進行加密貨幣挖礦

資安廠商 Check Point 旗下的資安專家，發現駭客利用已修復的 Atlassian Confluence Server 漏洞發動駭侵攻擊，在受駭伺服器上安裝惡意軟體，以挖掘加密貨幣牟利。

這個駭侵團體稱為「8220 gang」，其駭侵手法是先在網路上進行大量掃瞄，找到存有可攻擊漏洞的 Linux 與 Windows 伺服器，接著利用漏洞植入惡意軟體，以執行其駭侵攻擊，包括加密貨幣挖礦在內。

Check Point 指出，這次遭到 8220 gang 駭侵者鎖定攻擊的漏洞，是在 2022 年 5 月底時遭到發現的 CVE-2022-26134 0-day 漏洞，存於 Atlassian Confluence Server 之上；該漏洞可讓駭侵者遠端執行任意程式式碼，其 CVSS 危險程度評分高達 9.4 分，屬於「嚴重」（critical）等級。

雖然開發原廠 Atlassian 很快就在 6 月 3 日釋出修復此漏洞的更新版本，但根據資安廠商 GreyNoise 的監測結果顯示，即時在更新推出之後，遭到 8220 gang 駭侵攻擊的案例仍然不斷增加中。

資安專家表示，除了 8220 gang 發動的挖礦攻擊外，鎖定 CVE-2022-26134 的駭侵攻擊活動同時有好幾種，包括 Kinsing、Hezb、Dark.IOT 等，分別試圖植入僵屍網路或挖礦程式。

建議系統管理者除應隨時注意各種系統與軟體更新，隨時維持系統在最新版本之外，也應避免將系統曝露於外部 Internet 之上，應以適當的軟硬體防

火牆進行保護，僅容許透過內網存取。

- 資料來源：
  1. Crypto-Miners Leveraging Atlassian Zero-Day Vulnerability
  2. ATLASSIAN CONFLUENCE SERVER/DATA CENTER UP TO 7.18.0 OGNL INJECTION
  3. Hackers exploit recently patched Confluence bug for cryptomining

3.2.2、駭侵者假冒 Coinbase、MetaMask 等行動加密貨幣錢包，竊取用戶資金

資安廠商 Confiant 旗下的資安專家，近期一個名為「SeaFlower」的大型加密貨幣駭侵攻擊活動。

資安廠商 Confiant 旗下的資安專家，近期發現一個名為「SeaFlower」（中文名稱為「藏海花」）的大型加密貨幣駭侵攻擊活動；冒充各種知名行動加密貨幣錢包，以騙取用戶存在錢包內的加密貨幣資金。

Confiant 的報告指出，該公司係於 2022 年 3 月起開始觀察到 SeaFlower 的攻擊行動；Confiant 也指出其幕後的駭侵團體技術能力十分強大，僅次於惡名昭彰的 Lazarus 駭侵團體。

據 Confiant 的報告指出，SeaFlower 先是透過各種管道，例如幾可亂真的假官方網站、黑帽 SEO、社群媒體、加密貨幣相關論壇、惡意廣告等方式，全力散布多個假冒各種知名加密貨幣錢包的惡意軟體，遭到仿冒的加密貨幣錢包，包括 Coinbase、MetaMask、TokenPocket、imToken 等。

Confinat 也發現，百度搜尋引擎顯然遭到 SeaFlower 的各種詐騙 SEO 手法影響，對該團體架設的詐騙網站提供許多流量。

在 iOS 上，該駭侵團體則透過要求用戶下載設定檔的方式，誘使用戶側載（side-load) 惡意軟體，以逃避 iOS 的資安防護機制，裝惡意軟體安裝在 iPhone 上。

為避免受到這類詐騙假冒加密貨幣錢包的攻擊，導致財務損失，建議加密貨幣投資或交易用戶，切記務必自真正的加密貨幣錢包網站，以及 iOS

App Store 與 Google Play Store 下載官方版的加密資幣錢包，絕對不要安裝任何不明來源的加密貨幣相關應用程式。

- 資料來源：
  1. How SeaFlower 藏海花 installs backdoors in iOS/Android web3 wallets to steal your seed phrase
  2. Hackers clone Coinbase, MetaMask mobile wallets to steal your crypto

3.3、國際政府組織資安資訊

3.3.1、FBI 警告大眾，當心詐騙者竊取對烏克蘭的愛心捐款

美國聯邦調查局發表公開通報，指出該局最近觀察到有詐騙集團企圖以各種詐騙手法，不法竊取社會各界對戰火中烏克蘭人道危機的捐款。

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前發表公開通報（Public Service Announcement），指出該局最近觀察到有詐騙集團企圖以各種詐騙手法，不法竊取社會各界對戰火中烏克蘭人道危機的捐款；社會大眾於捐款前，應依該局提出的防範指南，提高警覺並特別注意，以免愛心遭到濫用。

詐騙者利用各界針對烏克蘭因為俄羅斯侵略而造成的人道危機踴躍捐款的機會，假冒為烏克蘭境內的各種實體，謊稱需要人道援助，展開詐騙募捐活動。

FBI 沒有在這次通報中明確指出是哪些詐騙者，假扮哪些烏克蘭境內實體，也沒有透露具體遭到詐騙的義援金總額。

不過在通報中，FBI 詳細建議多個具體可行的方案，讓有意捐款的個人或團體用以保護自己，避免愛心捐款流入不法分子手中：

- 對於各種網路上宣稱為烏克蘭戰爭危機募款的宣傳活動，要特別提高警覺，切勿輕信。
- 烏克蘭政府與烏克蘭各團體雖然確實正在進行各種募捐，但也有不少

詐騙活動是假借上述合法單位的名義進行，特別是要求以加密貨幣轉帳捐款者，更要特別注意；轉帳前應仔細比對你欲轉帳的錢包位址，是否與烏克蘭政府公布的官方捐款錢包位址完全一致。

- 要特別注意是否有任何個人假稱自己代表烏克蘭境內實體進行募捐。
- 不要轉帳給任何要求捐款的不明個人或實體。
- 不要和任何不明募捐者進行溝通，包括 Email、即時通訊等，更不要隨意開啟對方傳來的連結或檔案。
- 對國內單位捐款前，應向有關單位查詢該募款單位是否為合法註冊的公益團體。

建議民眾依 FBI 之指南，在捐款前特別提高警覺。若發現相關釣魚網站，也可至 TWCERT/CC 提供之 Phishing Check 網站進行通報。。

- 資料來源：
  1. The FBI Warns of Scammers Soliciting Donations Related to the Crisis in Ukraine
  2. FBI warns of Ukrainian charities impersonated to steal donations
  3. 網路釣魚通報 Phishing Check

3.3.2、義大利帕勒莫市遭 Vice Society 勒贖軟體攻擊

位於義大利西西里島北部的城鎮帕勒莫市（Palermo），近來遭到一個名為 Vice Society 的勒贖軟體發動大規模駭侵攻擊，導致該市多種市政服務因而無法運作。

據 Palermo 市政當局指出，攻擊發生在 6 月 3 日，導致該市所有透過網路提供的服務全部受到影響，使 130 萬市民與許多觀光客無法順利使用該市的政府相關系統。

Palermo 在上周接獲資安通報，表示有可能受到大規模分散式服務阻斷攻擊（Distributed Denial of Service, DDoS），因為義大利其他政府單位，當時也正遭到大規模的 DDoS 攻擊。

不過實際上發生的是勒贖攻擊。目前該市所有的伺服器全部呈現離線狀態，當局指稱正在加緊修復中。

本周三一個名為 Vice Society 的勒贖駭侵團體，在其架設於暗網上的入口中貼出公告，宣稱 Palermo 市的勒贖攻擊是該團體發動的；該團體稱，如果 Palermo 市不在 6 月 12 日前支付要求的贖款，就將公開所有竊自該市伺服器的資料。

資安專家指出，由於 Vice Society 並未在網站中貼出部分資料，因此目前無法得知哪些和市民個資相關的機敏資訊遭竊。

資安專家表示，Vice Society 過去經常透過已知的資安漏洞發動攻擊，因

此掌管大量民眾與法人資訊的政府單位系統管理者，應隨時注意各種軟硬體的漏洞與更新情報，並隨時更新到最新版本，並且加強系統的資安攻擊防護能力。

- 資料來源：
  1. Palermo Municipality Cyberattack Still Affecting Citizens
  2. Vice Society ransomware claims attack on Italian city of Palermo
  3. Attacco hacker al Comune di Palermo, rete ancora in tilt: si comunica coi fax

3.3.3、國際刑警組織會同 76 國，共同查緝社交攻擊等網路犯罪分子，逮捕近 2,000 人

國際刑警組織宣布一個全球社交工程犯罪逮捕行動，行動代號稱為「First Light 2022」，會同參與行動的國家高達 76 國，一共逮捕近 2,000 人。

國際刑警組織（INTERPOL）日前宣布一個全球社交工程犯罪逮捕行動，行動代號稱為「First Light 2022」，會同參與行動的國家高達 76 國，一共逮捕近 2,000 人，緝獲不法所得高達 5,000 萬美元。

First Light 2022 專案鎖定各種透過社交工程（Social Engineering）進行的各種網路或電話犯罪，包括詐騙電話、假戀情、企業 Email 攻擊（Business Email Compromise, BEC），以及相關的不法洗錢行為等。

據國際刑警組織表示，First Light 2022 相關追緝成果統計如下：

- 在全球 1,770 處不同地點展開緝捕作業；
- 鎖定近 3,000 名嫌犯身分；
- 逮捕近 2,000 名參與的犯罪分子，包括電話詐騙通話人員、車手與洗錢分子；
- 凍結近 4,000 個銀行帳戶；
- 緝獲近 5,000 萬美元不法款項。

國際刑警組織說，在這些緝獲的網路犯罪分子中，有一名犯罪分子，受其詐騙的受害者高達 24,000 人，不法所得高達 3,570 萬美元；他也涉及一起

綁票詐騙案，並向受害者家屬要求高達 157.5 萬美元的贖金。

First Light 2022 行動也查獲許多假冒電子商務公司，詐稱提供工作機會，實際上進行龐氏騙局的案例。該組織說，這類詐騙案例有不斷增加的趨勢。

建議民眾需提高對於社交工程的防範認知，即使是熟人，也需再三確認相關要求是否屬實；接到各式詐騙電話時亦勿驚恐，宜先仔細查證，並向 165 反詐騙專線電話報案。

- 資料來源：
  1. Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams
  2. Interpol seizes $50 million, arrests 2000 social engineers

3.4、社群媒體資安近況

3.4.1、資安專家發現透過 Facebook Messenger 進行的大型釣魚攻擊活動

資安廠商 PIXM 旗下的資安專家，發現一個大型釣魚攻擊活動，透過 Facebook 與 Facebook Messenger 進行。

資安廠商 PIXM 旗下的資安專家，近日發現一個大型釣魚攻擊活動，透過 Facebook 與 Facebook Messenger 進行；該釣魚攻擊不僅意圖詐騙用戶輸入其各類服務的登入資訊，並且還會透過竊得的帳戶資訊，進一步傳送釣魚連結給用戶的朋友，並透過顯示廣告賺取佣金。

據 PIXM 的報告指出，這波釣魚攻擊活動早在去（2021）年 9 月就開始進行，到今（2022）年 4 月、5 月時達到攻擊高峰。

PIXM 也說，受害者在點按 Facebook Messenger 中的釣魚連結後，會經過多次轉址，最後連到駭侵者設立的釣魚網頁；資安專家也透過方法得知該系列釣魚網頁，在 2021 年時的點閱次數達 270 萬次，在 2022 年的目前累積點閱更高達 850 萬次，可見攻擊活動規模顯著擴大。

PIXM 專家也挖掘出該波攻擊活動共使用 405 個不重覆的 Facebook 帳號，各自設立不同的 Facebook 釣魚攻擊粉絲頁面；這些頁面的瀏覽次數從四千餘次到六百多萬次不等。

攻擊者在以釣魚網頁取得用戶登入資訊後，用戶就會遇到另一輪多次轉址，最後會看到廣告頁面或問卷；駭侵者則可藉此賺取高額的推薦連結分

潤。

PIXM 已向警方分享其發現，且目前已有部分釣魚頁面使用的網址遭到收回，但整體而言，該波攻擊仍在持續進行中。

建議用戶在社群平台或即時通訊中如收到連結，均應提高警覺，特別是久未連絡的朋友突然傳來的連結，很可能是該友帳號遭竊後，由駭侵者傳來的惡意連結，切勿點按。

- 資料來源：
  1. Phishing tactics: how a threat actor stole 1M credentials in 4 months
  2. Massive Facebook Messenger phishing operation generates millions

3.4.2、一波透過 Facebook Messenger 發動的釣魚詐騙攻擊，正在快速擴散

資安廠商 PIXM 旗下的資安專家，發現現在正有一波透過 Facebook Messenger 散布的釣魚攻擊活動，會騙取用戶的 Facebook 登入資訊。

資安廠商 PIXM 旗下的資安專家，發現現在正有一波透過 Facebook Messenger 散布的釣魚攻擊活動，會騙取用戶的 Facebook 登入資訊；該攻擊活動正在快速散布，現已有數百萬用戶受害，且人數還在快速增加中。

PIXM 的資安專家指出，這波攻擊最初是在 2021 年 9 月時偵測到，一直沒有停息的跡象；隨著遭到釣魚攻擊的人愈來愈多，專家估計總受害者將突破 1,000 萬人以上。

這波攻擊是典型釣魚攻擊手法，目標是騙取用戶的 Facebook 登入資訊。當用戶不慎點擊透過 Facebook Messenger 傳來的釣魚訊息內連結時，會看到一個假冒的 Facebook 登入頁面；用戶輸入自己的 Facebook 登入資訊後，該登入資訊會立即傳送到攻擊者手中，攻擊者再利用於登入受害者的 Facebook 帳號，並將相同的釣魚訊息一一傳送給受害者在 Facebook 上的朋友，擴大詐騙範圍。

受害者在釣魚網頁輸入自己的 Facebook 帳號密碼後，接著會看到大量的廣告和問卷頁面，藉以賺取廣告點擊瀏覽分潤；資安專家估計，光是在 2021 年第 4 季，攻擊者因為這些廣告瀏覽而賺到的不法所得，就高達 5,900 萬美元。

資安專家也指出，這波攻擊利用特殊手法，透過多次重新導向，巧妙躲過 Facebook Messenger 平台的資安防護機制， 所以才會導致大量用戶接收到釣魚訊息。

建議 Facebook 用戶如果收到久未連絡的朋友突然傳來訊息，且內含不明連結，務必提高警覺，切勿點擊；如不慎點擊，也不要在不明釣魚網頁上輸入任何登入資訊或個人機敏資料，以免駭客的釣魚攻擊得逞。

- 資料來源：
  1. Phishing tactics: how a threat actor stole 1M credentials in 4 months
  2. Facebook Messenger Scam Duped Millions

3.4.3、駭侵者使用惡意聊天機器人，竊取用戶的 Facebook 粉絲專頁登入資訊

資安廠商 TrustWave 發現一個新的社群媒體攻擊行動，駭侵者利用聊天機器人假扮為客服人員，透過 Email 詐騙方式，意圖竊取粉絲專頁的登入資訊。

TrustWave 發表的監控報告指出，該公司觀察到一波透過垃圾釣魚郵件發動的聊天機器人詐騙攻擊；受害者接到的信件內容，有些偽裝成 Facebook 的內容管理團隊，詐稱受害者的 Facebook 粉絲專頁違反該公司的使用條款，受害者必須於期限內點按信中連接，否則將刪除該粉絲專頁。也有釣魚信件詐稱提供受害者工作機會，必須點按連結提出申請。

當受害者點按連結後，會進入一個由 Facebook Messenger 聊天機器人進行對話的聊天室，用戶會在聊天室中看到和收到的詐騙郵件類似的內容，然後會出現一個「提出申訴」的按鈕，按鈕按下後，用戶會被導到一個看似 Facebook 支援頁面的釣魚網頁，需填入多個用戶個資與密碼；該網頁甚至還會傳送假的二階段登入驗證碼給用戶，以降低用戶戒心。

報告也指出，在整個詐騙過程中存有許多破綻可供識別，例如釣魚信件的 header 中，寄件人的網域並非 Facebook 擁有的網域；此外用戶看到的 Facebook 申訴頁面，顯示在瀏覽器網址列中的 URL，也非 Facebook 網域。

建議用戶若收到這類威脅刪除粉絲頁面或個人帳號的訊息，萬勿驚慌，也不要立即點按其中的任何連結；應先仔細檢視 Email Header 中的寄件者詳細資訊，是否確實來自真正的寄件者網域，而非任何其他網域。進入需要填

寫敏感資訊的網頁，也應再三確認網址確實屬實。

- 資料來源：
  1. Interactive Phishing Mark II: Messenger Chatbot Leveraged in a New Facebook-Themed Spam
  2. Malicious Messenger chatbots used to steal Facebook accounts

3.5、行動裝置資安訊息

3.5.1、Apple 於 2021 年拒絕近 16 萬種可能有資安疑慮的 App 上架

Apple 發表 2021 年度資安詐騙防止分析報告，指出在去年 App Store 審核團隊拒絕多達 16 萬種，有可能誤導或對用戶發動垃圾訊息攻擊等具有資安疑慮的 App 上架。

Apple 近期發表 2021 年度資安詐騙防止分析報告，指出在去（2021）年一年之中，App Store 審核團隊拒絕多達 16 萬種有可能誤導或對用戶發動垃圾訊息攻擊等具有資安疑慮的 App 上架。

報告中也指出，App Store 團隊也拒絕多達 343,000 種 iOS App 於 App Store 上架，原因是這些 App 可能傷害用戶隱私，違反 App Store 的上架規範。

另外，Apple 也拒絕 34,500 種 App 的上架申請，因為這些 App 內含非公開或未載明於說明文件上的功能。Apple 也移除多達 155,000 種已上架的 App，因為這些 App 會在獲准上架後增加不符規範要求的新功能，可能對用戶資安造成威脅。

在 2021 年一整年，因有資安或隱私疑慮，遭到 App Store 拒絕上架的 App 數量多達 160 萬種。

Apple 另外也發表了幾個和用戶資安保護相關的統計數字：

- 阻擋近 15 億次詐騙交易。

- 阻擋超過 330 萬次信用卡盜刷交易。
- 將 60 萬個涉及詐騙交易的帳號永久停權。
- 將 1.7 億個疑似用於詐騙活動的假帳號永久停權。
- 阻止惡意分子註冊假帳號多達 1.18 億次。
- 將 802,000 個疑似涉及詐騙與資安攻擊的開發者帳號永久停權。

不過資安專家指出，在 iOS App Store 與 Google Play Store 中，目前仍有數百種所謂「Fleeceware」，會以免費試用為由，讓用戶訂閱高價服務，一年訂閱費用可高達數千美元。

建議用戶除了應只在 iOS 與 Android 官方 App Store 下載安裝軟體，且安裝需仔細檢視說明與用戶評價，避免安裝負評高的 App，同時對於日後需付費的免費試用提高警覺，避免訂閱不合理的高價服務。

- 資料來源：
  1. App Store stopped nearly $1.5 billion in fraudulent transactions in 2021
  2. Apple blocked 1.6 millions apps from defrauding users in 2021

3.5.2、多支廣告、資訊竊取 App 藏身 Google Play Store，下載次數高達 200 萬次以上

資安廠商 Dr.Web 旗下的資安專家，於上個月發現 Google Play Store 內有多支廣告暨資訊竊取軟體藏身於內，除了顯示大量廣告外，還會竊取用戶手機中的各項機敏資訊。

廣告惡意軟體會在安裝後顯示大量廣告，除了嚴重影響用戶體驗外，更會大量消耗裝置電力以及網路連線流量，造成手機發熱，降低使用壽命之外，有些廣告軟體甚至會在用戶未同意的情形下，擅自訂閱各種高價付費服務，造成用戶金錢損失。

資訊竊取軟體則會竊取用戶存在手機中的各種個人機敏資訊，包括登入各種服務使用的帳號密碼、社群服務帳號、金融相關資訊等，甚至會攔截用戶輸入的內容，包括雙重驗證用的代碼，以奪取用戶帳號使用權限。

根據 Dr.Web 的報告指出，上個月在 Google Play Store 中發現多個這類惡意 App，至今仍有五種惡意 App 仍未遭到下架：

- PIP Pic Camera Photo Editor：偽裝為照片編輯軟體，會竊取用戶的 Facebook 登入資訊，下載達 100 萬次以上。
- Wild & Exotic Animal Wallpaper：廣告後門惡意軟體，會將其圖示與軟體名稱改為「SIM Tool Kit」，並自行列入電池電力節約的除外名單內，下載量達 50 萬次。
- ZodiHoroscopr：偽裝成算命軟體的資訊竊取惡意 App，會誘騙用戶輸

入其 Facebook 登入資訊，亦有 50 萬次下載。

- PIP Camera 2022：50 萬次下載，會竊取 Facebook 登入資訊。
- Magnifier Flashlight：一萬次下載，會不停顯示各種廣告。

建議 Android 手機用戶必須注意，除了不在 Google Play Store 之外的地方任意下載安裝 APK 檔案外，在下載 App 時應特別提高警覺，先檢視該 App 的用戶評價，看看是否有用戶反應問題，再行下載安裝。

- 資料來源：
  1. Doctor Web’s May 2022 review of virus activity on mobile devices
  2. Android malware on the Google Play Store gets 2 million downloads

3.5.3、間諜軟體業者與 ISP 合作駭侵 iOS 與 Android 用戶

Google 旗下的資安威脅分析小組發表資安通報，指出有若干 ISP 涉嫌與間諜軟體業者合作，在用戶的手機中植入監控工具。

Google 旗下的資安威脅分析小組（Threat Analysis Group, TAG）日前發表資安通報，指出有若干網際網路服務供應商（Internet Service Provider, ISP），涉嫌與間諜軟體業者合作，在用戶的 iOS 與 Android 手機中植入監控工具。

出現在 Google TAG 報告中的商用間諜軟體業者，是義大利的 RCS Labs；該公司與一些 ISP 業者涉嫌透過詐騙手法，在用戶的 iOS 與 Android 手機中以側載方式安裝惡意軟體。受害者主要是義大利與哈薩克用戶。

Google 指出，在某些案例中，發現涉案的 ISP 業者會先中斷目標用戶裝置的行動連線服務，接著駭侵者會將惡意連結發送到受害者的裝置上，假稱點按連結即可恢復行動連線服務，引誘受害者點按連結。

對 iOS 裝置，駭侵者發送的連結，可透過企業認證簽署來安裝惡意軟體；惡意軟體利用的都是在 2021 年以前發現的多個 iOS 漏洞，可用以提升執行權限，並自用戶的 iOS 裝置中竊取機敏資訊。

對 Android 裝置，駭侵者則直接發送一個惡意 Android App，沒有用到任何已知漏洞，而是直接透過 DexClassLoader API 來下載並執行額外的惡意程式碼。

駭侵者另外也製作假冒的支援網站，聲稱可以幫用戶回復其 Facebook、Instagram、WhatsApp 被停權的帳號，藉以誘使用戶安裝惡意軟體。

建議行動裝置用戶應避免在非 Apple、Google 官方的應用程式商店中下載安裝任何軟體，以避免遭到類似的詐騙訊息誘騙，在手機上安裝惡意程式碼。

- 資料來源：
  1. Spyware vendor targets users in Italy and Kazakhstan
  2. Spyware vendor works with ISPs to infect iOS and Android users

3.5.4、新的 Android 金融惡意軟體 MailBot，偽裝成挖礦軟體大規模擴散中

資安廠商 F5 Labs 旗下的資安專家，發現一個新的 Android 金融惡意軟體 MailBot。

資安廠商 F5 Labs 旗下的資安專家，近期發現一個新的 Android 金融惡意軟體 MailBot；資安專家指出，MailBot 會偽裝成加密貨幣挖礦軟體和 Chrome 瀏覽器，以多種管道誘騙用戶下載。

據 F5 Labs 的報告指出，MailBot 的控制伺服器位置設於俄羅斯，且其使用的 IP 位置與 2020 年 6 月起的多次惡意軟體散布攻擊活動有關。

目前觀察到的 MailBot 散布方式，以在各類與加密貨幣投資與應用相關的網站中「推廣」為主；用戶在這類網站上可以下載 APK 檔案並手動安裝；而這些惡意軟體外觀與可在 Google Play Store 下載的 TheCryptoApp 之類的應用軟體極為類似。

報告也指出，其中一種含有惡意程式碼的惡意軟體，透過一個名為 Mining X 的網站來散布；該網站宣稱用戶只要下載安裝該網站提供的挖礦程式，即可輕鬆透過手機挖掘加密貨幣。

該惡意軟體一旦安裝到 Android 裝置上，會先向用戶要求取得程式啟動器（launcher）權限，接著就會自己取得各種裝置與系統存取權限；目前 F5 Labs 指出 MailBot 可以擷截通知內容、簡訊與電話通話、擷取螢幕畫面、註冊開機啟動項目、透過 VNC 進行裝置遙控等等，甚至可以竊取 Google Authenticator 內產的的二階段驗證碼，並且自動填寫驗證碼。

目前 MailBot 主要感染義大利與西班牙的 Android 用戶，竊取其手機內部的機敏資訊，如金融服務登入資訊、加密貨幣錢包密碼等。資安專家指出，該惡意軟體很可能擴大其影響範圍。

建議 Android 手機用戶應避免自 Google Play Store 以外的地方下載安裝軟體，尤其切勿自行安裝 APK 檔案；遇到安裝時要求過多或過高權限的 App 時，也應拒絕給與權限並立即移除。

- 資料來源：
  1. F5 Labs Investigates MaliBot
  2. New MaliBot Android banking malware spreads as a crypto miner

3.6、軟體系統資安議題

瑞士諾華藥廠遭駭侵攻擊，但無機敏資訊外洩

總部設於瑞士的大型藥廠諾華（Novartis）日前遭到駭侵攻擊，且部分被竊公司資料遭到駭侵者於暗網公開；但該公司對外發表聲明，表示並無機敏資訊外洩。

對 Novartis 發動攻擊的駭侵團體，名為 Industrial Spy；該團體專門針對各公私單位進行駭侵攻擊，目標在於竊取其機敏資訊，並在網路上販售圖利。

Industrial Spy 團體於日前在其經營的資料賣場中刊出一批資料，宣稱這批資料是來自 Novartis 的新藥開發實驗室，內含最新的 RNA 與 DNA 相關新藥科技與測試報告，可用於研發次世代的 COVID-19 疫苗的藥品，或是用於治療癌症。

該批資料內含多個檔案，總共的檔案大小為 7.7MB，主要都是 PDF 檔；檔案的時間戳記均為 2022/2/25 04:26，很可能就是駭侵者入侵的時間點。

資安專家指出，由於公開的被竊檔案大小相當小，目前無法得知這些就是全部的遭竊檔案，或只是被竊檔案的一部分。

資安媒體 BleepingComputer 針對此事件向 Novartis 進行採訪，該公司回應指出已經針對此一攻擊事件進行調查中，目前該公司可確認沒有任何機敏資料遭竊；該公司也未對此波駭侵攻擊的細節提供任何資訊，包括事件發生時間、駭侵者透過何種方式進入該公司系統。

有鑑於企業資料竊取與勒贖攻擊不斷上升，企業應加強系統的資安防護等級，同時加強工作人員的資安訓練，以免駭侵者藉由系統漏洞或針對員工進行釣魚或社交攻擊成功入侵。

- 資料來源：
  1. Hackers offer Novartis stolen data on darknet market place
  2. Novartis says no sensitive data was compromised in cyberattack

3.7、軟硬體漏洞資訊

3.7.1、Qbot 惡意軟體現正利用 Windows MSDT 0-day 漏洞發動釣魚攻擊

資安廠商觀察到一個名為 Qbot 的惡意軟體，會利用微軟一個尚未解決的 0-day 漏洞發動攻擊，目前觀察到該惡意軟體大規模發動釣魚攻擊。

資安廠商 Proofpoint 旗下的資安專家，日前觀察到一個名為 Qbot 的惡意軟體，會利用微軟一個尚未解決的 0-day 漏洞（CVE-2022-30190，又名 Follina）發動攻擊，目前觀察到該惡意軟體大規模發動釣魚攻擊；各單位之 Windows 用戶應提高警覺。

Proofpoint 是在上周與本周一（6 月 6 日）發表的相關報告中，提到 Qbot 當時正用於攻擊美國與歐洲的政府單位；近日發表的新報告則指出，駭侵團體 TA570 就是發動這波 Qbot 攻擊的主要駭侵者。

這波 Qbot 釣魚攻擊，係以夾帶惡意程式碼的 Microsoft Office .docx 檔案來進行，利用 CVE-2022-30190 Follina 0-day 漏洞，在受害者電腦中植入 Qbot 惡意軟體；資安專家分析指出，這次 TA570 的攻擊方式是寄送一個夾帶 HTML 檔案的郵件；一旦開啟這個 HTML 檔，就會下載一個 zip 壓縮檔，壓縮檔內含有 IMG 檔案，內含一個 DLL、捷徑檔和 Microsoft Word .docx 檔，誘使用戶開啟。

CVE-2022-30190 Follina 0-day 漏洞存於 Microsoft Office 中，該漏洞可讓駭侵者以特製的 Microsoft Word 文件檔夾帶惡意指令檔，透過 Microsoft

Diagnostic Tool (MSDT) 呼叫應用程式的許可權運行任意程式碼。攻擊者可以在用戶許可權允許的環境中安裝程式、查看、更改或刪除資料，或建立新帳號。

- CVE 編號：CVE-2022-30190
- 解決方案：

建議用戶可禁用 MSDT URL 協定，防止疑難排解作為連結啟動，包括整個作業系統中的連結，以降低資安風險。請按照以下步驟禁用：

1. 以管理員身份運行命令提示字元。
2. 要備份註冊表，請執行命令 reg export HKEY\U CLASSES\U ROOT\ms msdt filename。
3. 執行命令 reg delete HKEY\U CLASSES\U ROOT\ms msdt/f。

若要取消禁用，請按照以下步驟執行：

1. 以管理員身份運行命令提示符。
2. 要還原註冊表，請執行命令“reg import filename”。

- 資料來源：

1. Threat Insight @threatinsight Proofpoint blocked a suspected state aligned phishing campaign
2. Microsoft Releases Workaround Guidance for MSDT "Follina" Vulnerability
3. Windows zero-day exploited in US local govt phishing attacks
4. Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability
5. Threat Insight @threatinsight Proofpoint saw #TA570 exploiting CVE-2022-30190
6. Qbot malware now uses Windows MSDT zero-day in phishing attacks

3.7.2、Microsoft 推出 2022 年 6 月例行性 Patch Tuesday 資安更新包

Microsoft 推出 6 月份例行性 Patch Tuesday 資安更新修補包，一共修復多達 55 個資安漏洞。

Microsoft 日前推出 2022 年 6 月份例行性 Patch Tuesday 資安更新修補包，一共修復多達 55 個資安漏洞，其中包括近來遭到大規模濫用於攻擊的 CVE-2022-30190 Follina MSDT 0-day 漏洞在內。

這 55 個漏洞當中，包含 5 個危險程度層級為「嚴重」（Critical）等級的漏洞，均為可讓駭侵者遠端執行任意程式碼的漏洞；其他的多為「重要」（Important）等級。

如果以類型區分，這 55 個得到修補的漏洞分別如下：

- 執行權限提升漏洞：12 個；
- 資安防護功能略過漏洞：1 個；
- 遠端執行任意程式碼漏洞：27 個；
- 資訊外洩漏洞：11 個；
- 服務阻斷攻擊漏洞：3 個；
- 假冒詐騙漏洞：1 個。

值得注意的是，上個月開始有多個駭侵攻擊活動，係濫用 Microsoft Windows 內的 Microsoft Diagnostic Tool (MSDT) 內的一個 0-day 漏洞 CVE-

2022-30190，執行惡意 PowerShell 指令；該漏洞遭駭侵團體用於散布 Qbot 惡意軟體、鎖定美國政府單位與烏克蘭媒體組織發動攻擊。該漏洞已在這次的 Patch Tuesday 中修復。

由於 Microsoft Windows 暨各種軟體產品使用量極廣，因此頻繁成為駭侵者的攻擊目標，且有許多攻擊活動係利用各種未能及時更新修補的漏洞；因此不論是 Microsoft 各種軟體產品的終端用戶，或是系統管理員，均應立即依照各軟體的更新指示，套用資安更新，以降低遭到駭侵攻擊的風險。

- CVE 編號：CVE-2022-30190 等。
- 影響產品/版本：Microsoft 各項軟體產品，詳見 Microsoft 最近安全新更新導覽頁面資訊。
- 解決方案：
  立即透過軟體內之更新功能，或依更新指南，套用資安更新。

若無法進行更新，可參考微軟官方網站採取下列緩解措施，以暫時關閉微軟支援診斷工具之 URL 協定：

1. 以系統管理員身分開啟「命令提示字元」視窗
2. 執行「reg export HKEY_CLASSES_ROOT\ms-msdt filename」指令進行機碼備份
3. 執行指令「reg delete HKEY_CLASSES_ROOT\ms-msdt /f」
4. 後續安裝修補程式後，若要還原機碼，請執行「reg import filename」

- 資料來源：
  1. Security Update Guide
  2. Microsoft June 2022 Patch Tuesday fixes 1 zero-day, 55 flaws

第 4 章、 資安研討會及活動

關鍵基礎設施實作課程(含攻防演練實作)	
活動時間	見活動概要
活動地點	沙崙資安服務基地 1 樓攻防演訓教室 (台南市歸仁區歸仁十三路 6 號)
活動網站	https://www.acw.org.tw/News/Detail.aspx?id=3229
活動概要	 **主辦單位：經濟部工業局** 近年來，工控(ICS)及 OT 相關的網路攻擊事件頻傳，駭客亦開始針對關鍵基礎設施單位，包括政府、醫療保健、油氣水電、交通、金融等發起持續攻擊，被攻擊的結果除造成營運中斷或金錢、聲譽損失外，更有可能影響國家安全與人民生命安全。 為提升關鍵基礎設施操作人員熟悉資安防護基準與防護措施，經濟部工業局委託資策會辦理關鍵基礎設施實務操作演訓課程，結合沙崙資安基地工控實測場域，進行實際演練與操作攻防演練實作，學習工控封包分析並撰寫偵測規則驗證攻擊情境，實訓演練真實的防禦架構，培養業者實務防護能力。 ➢ 2022/07/11 09:40~16:40 [第一場]關鍵基礎設施實作課程 ➢ 2022/07/25 09:40~16:40 [第二場]關鍵基礎設施實作課程 ➢ 2022/08/01 09:40~16:40 [第三場]關鍵基礎設施實作課程 ➢ 2022/09/27 09:40~16:40 [第四場]關鍵基礎設施實作課程 課程聯絡人：李小姐 / doralee@iii.org.tw / 02- 66073299

JMUG - Jamf 資安召集令 (IDC 2022 No1.)	
活動時間	2022/07/14 18:30~20:30
活動地點	Roots Café / 106 台北市大安區仁愛路四段 101 號 2 樓
活動網站	https://jamf.kktix.cc/events/jmug2022july?fbclid=IwAR2SfwMobJBb9CiJOGfE_s2HPbB9ej-GRP7jtfEpQ4cCRTePOrZi2nschWM
活動概要	 **主辦單位：Jamf Software** 參與今夏參與 Jamf 資安召集令，獲取 Apple 資安最新資訊。在此會議中，我們分享 ➢ Apple 設備管理第一堂課 ➢ Apple 管理經驗分享 ➢ 由 設備管理看 WWDC 亮點 ➢ iPad / Mac 小組討論 講者：Apple 國際授權講師、Jamf 亞太地區資深工程師 現場提供精緻美式晚餐

資安防護及案例分享研討會-桃園場	
活動時間	111 年 07 月 19 日 (二) 下午 14:00 ~ 16:30
活動地點	觀音工業區服務中心 二樓訓練教室(桃園市觀音區工業五路 3 號) / 同步線上研討會
活動網站	https://forms.gle/7MwDgZDouZUXpCz89
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 全球疫情升級，遠距辦公的普及，讓企業更直接地面對資安漏洞與威脅，員工使用個人電腦透過 Wi-Fi 連接到公司內網，保護終端設備的資訊安全，將成為企業的最大挑戰，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「遠距辦公與工控資安防護重點」，企業加強產線工控資安意識，做好防護避免因小失大。 本活動名額有限，敬邀各單位與先進報名與會。 聯絡方式： 04-2242-1717 *242 黃小姐 eva@tcca.org.tw 04-2242-1717 *243 賴小姐 angel@tcca.org.tw

【資安學院】7/23、7/30 iPAS-「中級」資訊安全工程師-能力研習備戰班	
活動時間	7/23、7/30
活動地點	中華民國資訊軟體協會 訓練教室（台北市大同區承德路二段 239 號 6 樓）
活動網站	https://www.cisanet.org.tw/Course/Detail/2752
活動概要	數位轉型 軟協與您共行 中華民國資訊軟體協會 CISA Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 以最貼近業界的經驗與最生動的案例分享及實務案例探討，讓學員能接收到最新資訊安全相關知識與技能，除了能學會如何建立符合法規與組織安全需求之系統、網路與安全防護架構，並執行相關維運作業與協助其他單位執行資訊安全活動之外， 本課程亦能協助結業學員考取相關認證。 課程大綱： 資訊安全規劃實務 ➢ 資訊安全管理系統框架 ➢ 資訊安全管理實務 ➢ 資訊安全架構規劃 ➢ 國內外重要資安及隱私法規 ➢ 資訊安全風險評鑑、風險處理 資訊安全防護實務 ➢ 弱點定義、產生原因、弱點評估與管理、偵測與發掘機制、修補方式與防制 ➢ 常見的攻擊手法 ➢ 資安防護機制配置及相關技術 ➢ 攻擊防護與應變、資訊安全維運作業

	➢ 資安事件等級定義、通報機制設計、通報應變機制實務、資安防護委外管理 ➢ 資安監控機制規劃與配置維運 ➢ 滲透測試、源碼檢測、資安健檢 課程對象：資安(訊)主管、資訊安全管理人員、具資訊安全相關經驗 2 年(含)以上者、通過 iPAS 資訊安全工程師-初級認證進而想取得中級者 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；詳細報名資訊，請參考 iPAS 官網。

資安實作挑戰營 二天班	
活動時間	2022/07/27-28
活動地點	中華電信學院板橋院本部 地址：新北市板橋區民族路 168 號
活動網站	https://www.chtti.cht.com.tw/general/course_info.jsp?activity_id=509
活動概要	 **主辦單位：中華電信學院** 課程簡介：本營隊提供資安知識探索以及資安工具實作體驗，透過精彩刺激的資安遊戲與生動活潑的教學內容，讓學員沉浸資訊安全技術的探討與生活周遭貼身挑戰，並藉此銜接大學資訊安全相關課程。協助學員建立資安概念，透過「動手做、做中學」，從實際操作中體驗資安防護，初探資安技術以及資安與我們生活密不可分的重要性。 報名截止日期：2022/07/13

物聯網資安立法 搶攻歐美供應鏈市場	
活動時間	2022 年 7 月 27 (三) 14:00 ~ 15:30
活動地點	線上研討會
活動網站	https://www.onwardsecurity.com/news/item/147
活動概要	 **主辦單位：Onward Security** 疫情加速數位轉型，資安威脅不斷加增。包括最新 RED 歐盟無線電設備指令、EU MDR 歐盟醫材法，已經針對物聯網設備提出更多嚴格的資安要求。美國 FDA 也警告，醫材製造商應強化設備的網路安全。因此，產品不論在硬體的設計、軟體物料清單(SBOM)的建立，或在生產上都必須考慮各地的資安法規要求，才能順利於當地上市銷售。

【資安學院】風險導向資安稽核	
活動時間	2022-07-27 09:30 ~ 16:30
活動地點	中華民國資訊軟體協會 訓練教室（台北市大同區承德路二段239號 6 樓）
活動網站	https://www.cisanet.org.tw/Course/Detail/2756
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** 報名截止： 2022-07-22 為處理日益龐大的資訊，越來越多企業採用自動化且功能強大的計算機系統，以簡化內部作業、提升服務客戶的能力及速度。但享受著科技日新月益的紅利的同時，伴隨系統弱點逐步揭露，以致其可能被有心人士利用，造成資安事件和資料外洩的危機。資訊安全稽核乃為應對此威脅的有效機制，運用風險評鑑方法，識別組織內資訊流向，及其涉及之網路、資料庫、資料儲存節點和應用系統等，檢視各項控制是否足夠，以保護資料的機密性、完整性和可用性，並符合法規要求。 本課程引用資安相關標準及法規，講解目前業界之實務作法，採用互動式教學，提升學員的資安與稽核能力。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

【資安學院】滲透測試方法與實務	
活動時間	8/4、8/5 09:00~17:00
活動地點	中華民國資訊軟體協會 訓練教室（台北市大同區承德路二段239號 6 樓）
活動網站	https://www.cisanet.org.tw/Course/Detail/2754
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** 報名截止： 2022-07-29 因應目前新型態的資安攻擊，軟體開發/管理人員面對資安攻擊的挑戰日益嚴峻，除熟悉安全軟體開發方法外，透過了解駭客攻擊原理與步驟，可更加強化及防禦惡意攻擊行為。 本課程設計係以駭客可能之攻擊手法，輔以實例說明一系列駭客對滲透目標進行資訊蒐集、漏洞挖掘進而遠端操控之方法，讓學員學習到有效的資安防禦實務。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

【資安學院】ISO 27701：2019 個人資料管理系統主導稽核員訓練課程	
活動時間	8/8~8/12 09:00~18:00
活動地點	中華民國資訊軟體協會 訓練教室（台北市大同區承德路二段 239 號 6 樓）
活動網站	https://www.cisanet.org.tw/Course/Detail/2744
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** 報名截止： 2022-08-05 此課程為「行政院國家資通安全會報」認可之資通安全專業證照 我國個人資料保護法已施行多年，而歐盟亦於 2018 年開始 GDPR 個資保護法令，其影響全球商業活動置身。如何打造既符合個人資料保護法要求，且又達到國際水準的個人資訊管理系統已是全球化過程中不可或缺的環節。ISO 27701:2019 是植基於 ISO 27001 資訊安全管理標準之上的個人資訊管理標準，其於 2019 年 8 月正式公布後，提供企業組織在蒐集、處理或儲存個人資料時的管理與保護依據。透過以資訊安全管理為基礎的個人資訊管理國際標準，可協助現行組織流程中確認個人資訊處理符合法令法規要求，並進而完整保護個人資料的安全。本課程將協助您學習如何成為一位符合要求的主導稽核員，可以勝任個人資料管理系統稽核之工作。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

第 5 章、 TVN 漏洞公告

健保卡網路服務元件 - Heap-based Buffer Overflow	
TVN / CVE ID	TVN-202112007 / CVE-2021-45918
CVSS	7.5 (High)
影響產品	健保卡網路服務註冊網站供下載受影響版本之平台與相對應 MD5 HASH： Windows: Setup.zip MD5 驗證碼：515BE7DE5BCE446177FEE8A6E0665093 Mac: NHI.Card.Mac.pkg.zip MD5 驗證碼： 42fcc36541e716e23de77d5f325b186a Linux(Ubuntu): mLNHIICC_Setup.Ubuntu.zip MD5 驗證碼：52EACB7CA2B4D0A5A869DF01079BF4D6 Linux(Fedora): mLNHIICC_Setup.fedora.zip MD5 驗證碼： 52EACB7CA2B4D0A5A869DF01079BF4D6
問題描述	健保卡網路服務元件之特定函式未驗證輸入的字串長度，導致預先保留的記憶體 Buffer 不足，造成 Heap-based Buffer Overflow 漏洞，遠端攻擊者不須權限，即可利用該漏洞導致終止服務，須重啟服務才能恢復。
解決方法	至健保卡網路服務註冊網之下載點下載最新版本
公開日期	2022-06-20
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6227-eaf49-3.html

第 6 章、 2022 年 6 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。

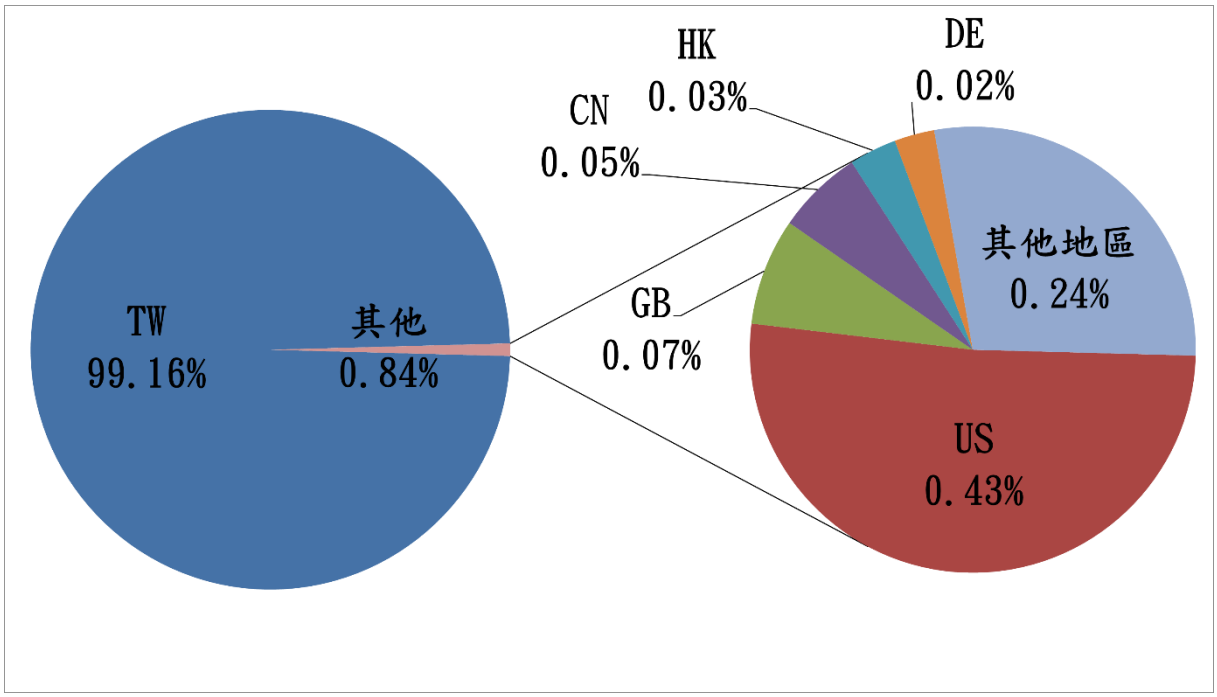

圖 1、分享地區統計圖

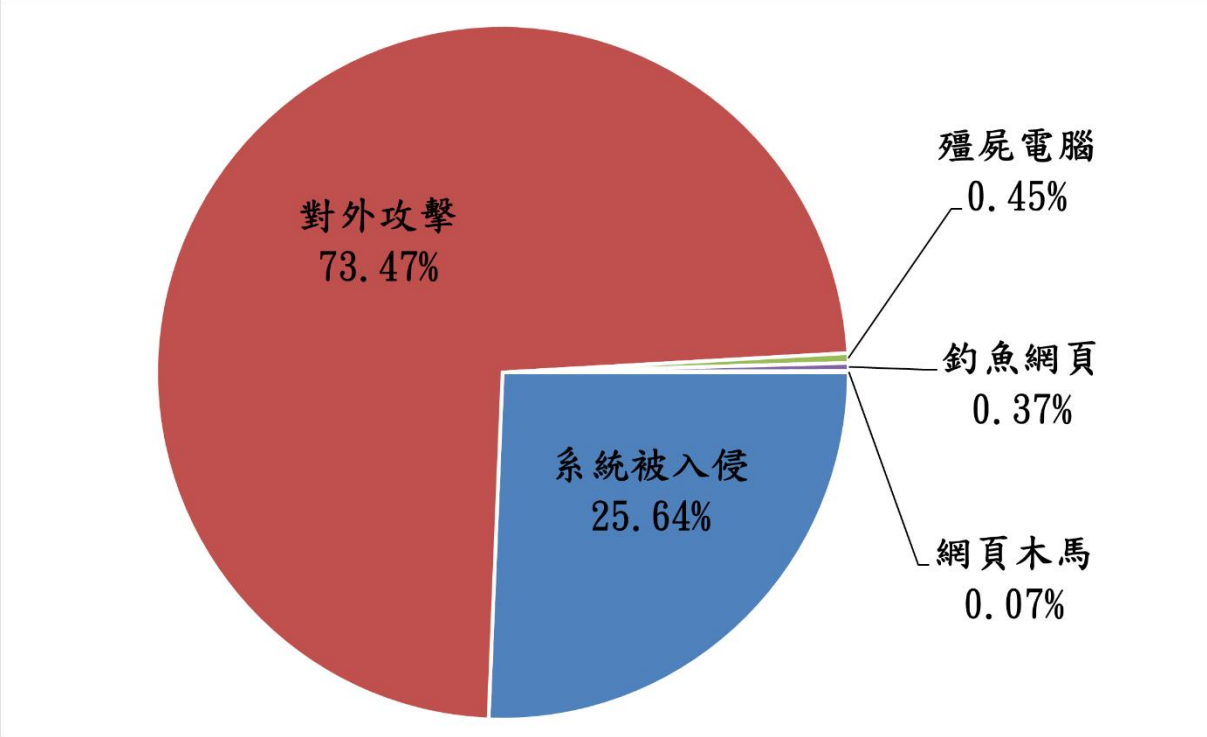

圖 2、分享類型統計圖

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 7 月 8 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**