TWCERT/CC 資安情資電子報

2022 年 11 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
開源軟體資安威脅與防護 1
第 2 章、 資安活動紀事 9
資安防護及案例分享研討會-嘉義場 9
第 3 章、 國內外重要資安事件 12
3.1、 資安趨勢 12
3.1.1、 65% 全球企業董事認為其公司將在一年內遭駭侵攻擊，47% 認為公司並未有充分準備 12
3.1.2、 多家市場研究公司指出，未來十年工業資安防護市場將大幅成長 14
3.1.3、 統計指出挖礦駭侵者每賺取 1 美元，要消耗高達 53 美元的被駭系統資源 16
3.2、 新興應用資安 18
3.2.1、 大型加密貨幣駭侵活動，濫用多種網路免費資源進行挖礦 18
3.2.2、 駭侵者入侵詐騙網站植入惡意程式碼，搶先竊走受害者數位錢包內的加密貨幣 20
3.2.3、 駭侵者自幣安橋接服務竊走 5.66 億美元加密貨幣資產 22
3.3、 國際政府組織資安資訊 24
3.3.1、 墨西哥、薩爾瓦多、哥倫比亞、秘魯等中美洲國家政府單位接連遭駭，內部資料被竊 24
3.3.2、 德國警方逮捕利用釣魚攻擊竊取 400 萬歐元的駭侵者 26
3.3.3、 澳洲警察秘密探員身分，因哥倫比亞政府文件遭竊而曝光 28
3.4、 社群媒體資安近況 30
3.4.1、 非官方 WhatsApp Android App 會竊取用戶帳號控制權 30
3.4.2、 新發現 PHP 資訊竊取惡意軟體，針對 Facebook 帳號發動釣魚攻擊 32
3.4.3、 職涯社群服務 LinkedIn 新資安功能推出，偽裝任職知名大公司的假帳號大幅減少 34
3.5、 行動裝置資安訊息 36
3.5.1、 Android 惡意軟體 Drinik 鎖定 18 家印度銀行用戶發動攻擊，竊取其個資

與銀行登入資訊 36
3.5.2、 Google Play Store 中新發現 16 個 Android 廣告惡意軟體，下載次數合計超過 20 萬次 38
3.6、 軟體系統資安議題 40
3.6.1、 Linux Kernel 5.19.12 內含可能損壞採用 Intel 顯示晶片筆記型電腦螢幕的錯誤 40
3.6.2、 紐約郵報遭駭侵者攻擊，並在頭條發布針對政治人物的攻擊性標題 42
3.6.3、 勒贖駭侵團體宣稱成功駭入跑車製造商法拉利，取得大量內部文件 44
3.6.4、 澳洲 Medibank 承認所有 280 萬名用戶個資均遭駭侵者竊走 46
3.7、 軟硬體漏洞資訊 48
3.7.1、 Apache Commons Text 程式庫遭發現內含可遠端執行任意程式碼的漏洞 48
3.7.2、 Apple 修復一個已用於駭侵攻擊的全新 0-day 漏洞 CVE-2022-42827 50
3.7.3、 macOS 遭發現存有可執行未簽署應用程式的漏洞 52
3.7.4、 Microsoft Exchange Server 的最新 0-day 暫時解決方案可遭略過 54
第 4 章、 資安研討會及活動 56
第 5 章、 TVN 漏洞公告 62
第 6 章、 2022 年 10 月份資安情資分享概況 65

第 1 章、 封面故事

開源軟體資安威脅與防護

- 開源軟體可加速產品開發，其使用狀況可分為應用工具、程式函式、軟體服務等類別。
- 開源軟體發生過多次影響範圍極大的資安事件，尤其是函式庫類型的開源軟體，因經常被引用且不易盤點使用狀況，當發生資安漏洞時，威脅就相當嚴重，如 OpenSSL heartbleed 漏洞，而其它常用的基礎架設軟體，亦常造成嚴重資安議題，如 Apache。
- 開源軟體潛在資安風險頗高，此乃由於缺乏源碼檢測與安全性檢視、程式碼開發成熟度的不確定性、相關安全性更新易遭忽視。
- 我國為產品代工與 IoT 設備生產大國，大量採用開源軟體，亦發生多次產品因開源軟體漏洞而受到影響的事件，突顯廠商對自身產品採用開源軟體的安全度掌握不足之議題。
- 在資安防護建議的作法方面，包括：謹慎評估開源軟體、管控開源軟體導入範圍、指派人員參與開源軟體專案、針對函式庫進行檢測、擬定相關緊急應變措施等。

一、簡介

開源軟體(Open Source Software, OSS) 為開放原始碼的軟體，軟體作者透過原始碼的公開及適度的軟體授權條款，允許其他使用者進行檢視、修改、及任何目的發送軟體。大多數願意公開程式碼的開源軟體，起先多是為了讓更多人參與開發，提升專案成熟度，另一方面也可進行推廣，使用者也樂於以無成本使用軟體，甚至可依據自身需求進行修改。

1997 年 7 月，Bruce Perens 與其他 Debian Linux 開發者們釋出了 Debian 自由軟體指導方針(Debian Free Software Guidelines)，作為 Debian 專案用以判斷自由軟體授權條款的方針，不久後開放原始碼促進會(Open Source Initiative, OSI)參照此指導方針，釋出了開放原始碼定義(The Open Source Definition)。

根據 Gartner 2021 統計數據指出，超過 90%的企業組織會採用開源軟體，也包含會應用在關鍵任務的工作(mission-critical workloads)之中。企業組織會採用開源軟體，主要是因為可以低取得成本、可以客製化，有些開源軟體的品質甚至優於商業版同性質的軟體。

企業組織採用開源軟體，大多可分為以下應用：

1. 應用工具類：以開源軟體作為企業內部應用程式，如程式碼編輯器 Eclipse、NetBeans、Visual Studio Code(VS Code)等，文書處理軟體 OpenOffice、LibreOffice 等，圖形編輯器 Gimp 等。

2. 程式函式類：採用開源的程式函式(library)或是開源框架，更便捷地開發出產品功能，或者應用於企業內部服務，如 Zend framework、Springs、Apache Structs 等網站應用框架(Framework)，或是像電腦視覺應用的 OpenCV、機器學習相關的 Tensor-Flow、Torch 等。

3. 軟體服務類：企業重要服務或軟體服務，如作業系統 GNU/Linux、網頁伺服

器軟體相關的 Apache、Nginx，資料庫相關的 MySQL、Elasticsearch 等。

二、使用開源軟體的潛在資安風險

雖然企業使用開源軟體有許多益處，但近年也發生數起與開源軟體相關的重大資安事件，如 2014 年就出現開源加密函式庫 OpenSSL 相關的 Open 心臟流血(Heartbleed, CVE-2014-0160)及 Unix 作業系統中 Bash Shell 相關漏洞 Shellshock(CVE-2014-6271、CVE-2014-6277、CVE-2014-6278、CVE-2014-7169、CVE-2014-7186、CVE-2014-7187) ，在漏洞公告後，網路上出現大量針對此漏洞的掃瞄攻擊行為，造成全球網站曝露在資訊洩漏與攻擊入侵風險之中，大型入口網站業者雅虎(Yahoo!)也疑似受到此漏洞影響，有多台重要伺服器被入侵。

在 2017 年 9 月，美國重要信貸公司艾可飛(Equifax)發現遭受駭客入侵，被竊取了 1.47 億筆個人隱私資料，資料內容包含用戶的社會安全號碼(Social Security number, SSN)、信用卡號等資訊，最終艾可飛與聯邦貿易委員會(Federal Trade Commission)、消費者金融保護局(Consumer Financial Protection Bureau)、及 50 個州以總計 4.25 億美元的天價達成和解，用於處理受影響用戶的後續事宜。依據後續資安事件調查，入侵點為公司網站 app 上的漏洞，為 Apache Struts(CVE-2017-5638)已發布之漏洞，Apache 基金會早於 3 月時已經公告版本更新，然而在更新公告後，全球尚未修補的伺服器便陸續遭受駭客入侵，艾可飛在 5 月時已被入侵，被駭客持續竊走客戶資訊。

此外，近年利用企業內使用之軟體工具，進行針對性供應鏈攻擊的手法也層出不窮，如 2020 年 5 月針對程式開發工具 NetBeans 進行的滲透攻擊行為，駭客先感染 NetBeans 整合開發環境之電腦，待開發人員以該電腦提交(Commit)新程式碼至 GitHub 平台時，惡意程式會一併植入 JAR 檔案，導致開發者提交至 GitHub 平台之程式碼帶有惡意後門程式，後續使用者更新新版程式便會遭受感染，或是其他開發人員引入此版本程式碼時，也會讓後續版本一併遭受感染。資安研究人員將此行動命名為 Octopus Scanner，在當時研究

人員發現此行動已成功感染了 26 個開源專案。

綜觀數起事件，本研究歸納以下幾點開源軟體存在的潛在風險：

(一)缺乏源碼檢測與安全性檢視

開源軟體的開發目標以功能導向為主，較有規模的社群團隊會將參與者分為貢獻者(Contributer)與核心團隊(Core member)，甚至會再細分角色。貢獻者可以依據自主想法或是專案的待完成功能(To Do)提交程式碼，核心團隊負責決定專案方向，以及審核貢獻者們提交的程式碼，通過後貢獻者們的程式碼便會成為開源軟體的一部分。然而在審核程中，大多只會確認程式碼的功能，鮮少會針對安全性進行實際驗測，一切仰賴核心團隊的開發經驗來檢視，因此無法確保軟體每個新版次的軟體安全性。

此外，也因為開源的特性，駭客可直接取得軟體原始碼，透過檢視原始碼(Code Review)，可直接挖掘軟體的漏洞，其若有被挖掘到則便成為駭客的攻擊武器之一，利用該漏洞入侵有使用該軟體的企業或組織。

(二)程式碼開發成熟度的不確定性

開源軟體的開發社群是以自由參與為主，軟體更新頻率無法如商用軟體般給予明確的開發時間，小型社群此情況尤甚。若社群中有業界著名開發者參與，或是以公司企業為主的開發者，則開發社群比較容易趨向成熟穩定，專案的開發也比較會持續精進，例如 Google、RedHat、Apache 基金會、微軟、Mozilla 等組織的開源專案，或是如 Python、Ruby 等有著名開發者主導的程式語言相關專案。

(三)易於忽視相關安全性更新

使用開源軟體可提升自身產品的開發效率，但也容易忽視開源軟體的安全性，在檢測產品安全性時只注重產品本身程式碼，忽略了使用到的相關函式庫，或是採用的應用框架、服務軟體等，例如 Apache Structs。

三、國內開源軟體資安議題

我國產品亦大量採用開源軟體，許多漏洞其根本原因採用開源軟體導致，而 IoT 設備方面，使用 Linux 早已行之有年，特別在行動網路時代，android 系統不止被使用在行動電話上，較多智慧功能的 IoT 設備皆以 android 為基礎開發，這些都是開源軟體專案的產物，即使經過調整、客製後的版本亦不可避免的使用到各種開源涵式庫、開源工具等，我國尤其是各種 IoT 設備的生產大國，但並未太重視產品中使用的開源軟體安全狀況，導致存在諸多漏洞風險。

2021 年 1 月，DNSmasq 遭以色列安全公司 JSOF 發現存在 7 個安全性漏洞，DNSmasq 為開源專案，其功能有 DNS 伺服器、DHCP 伺服器、以及 TFTP 伺服器，由於其輕量化及高效能的特性，被許多網路設備產品或相關韌體所採用，用於內網中設備的 DNS 查詢快取與 DNS 遞迴查詢。研究人員發現了 DNS 快取中毒(DNS Cache Poisoning)等漏洞，估計約有 40 家業者在產品中採用了 DNSmasq，包括 AT&T、思科、Google、Juniper 及紅帽等，國內網通設備廠包含華碩(Asus)、友訊科技、Linksys、群暉科技(Synology)、合勤科技(Zyxel)等。

資訊產品漏洞直接影響到採用該產品的企業組織與消費者，尤以近年興起的供應鏈攻擊，鎖定有漏洞的資訊設備或第三方函式作為入侵破口，潛入後挖掘出企業內部橫向擴散(Lateral Movement)的路徑。資訊產品的使用者可能會對產品本身的公告漏洞有所警覺，但與開源軟體相關的漏洞卻很難察覺，需仰賴產品製造商本身的積極作為，以群暉科技為例，開源加密通訊函式 OpenSSL 在 2021 年 8 月修正了 CVE-2021-3711 與 CVE-2021-3712 兩個安全漏洞，該公司掌握相關資訊後，馬上確認線上產品是否採用相關函式，接著即時公告受影響的產品，並著手進行修補作業。

針對軟體安全相關議題，美國政府近年已採取一系列積極措施，2021 年 5 月通過改善國家網路安全與保護聯邦政府網路相關的行政命令，其中關於強

化軟體供應鏈安全部分，針對販售給政府部門的軟體，要求開發人員提高軟體透明度，並公開相關安全資訊。此外，美國國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)也制定了軟體組成清單(Software Bill of Materials, SBOM)相關資訊及指引，規範軟體組成清單的內容以及相關格式，利於軟體開發團隊分享軟體資訊，提高軟體透明度，讓使用者用得以確認軟體是否有新的漏洞風險。基於美國政府的相關要求，可預期各資訊產品的軟體元件清單與安全風險資訊，將成為產品上市供應商所必須提供的資訊。

目前國內尚無類似規範，僅有衛生福利部食藥署針對醫療器材提出「適用於製造廠之醫療器材網路安全指引」，督促醫療器材製造廠重視產品的網路安全，但此對廠商而言，關於產品資安之基本認知尚仍不足，在評估資安風險之前，首要應是瞭解產品軟體開發組成，掌握自我開發與使用開源軟體的狀況，才能針對性的強化或修補資安的缺漏，如自我開發部份可採源碼掃描找出存在風險的程式，而開源軟體部份，透過軟體組成清單，關注其漏洞狀況，建立更新、維護機制並定期檢討改進。

四、防護與建議措施

綜上所述，本研究歸納了數項主要潛在風險，茲就每個要項提供可採取對應措施之建議，期能有效將風險減至最低，說明如下：

(一)謹慎評估開源軟體

開源軟體品質不一，也存在維護議題，故除了確認軟體是否滿足功能需求，在評估階段可多比較同性質軟體，評估項目中也需考量專案擁有者及開發社群的活躍程度，確保軟體仍會持續更新。

(二)管控開源軟體導入範圍

確認企業組織內採用的開源軟體清單，以及開源軟體應用的範圍，避免後續進行維護更新時有所疏漏。針對產品部分可參考軟體組成清單的文件，

審慎評估其安全性，並適時公開相關資訊，提供給使用者作為參考。

(三)指派人員參與開源軟體專案

指派相關維護人員或主責人員關注開源軟體的專案活動，甚至可以參與該專案的相關討論或提交程式碼，一則強化企業內部對於開源軟體的關注程度，二則可以活絡開發社群，確保軟體的開發成熟度且與時俱進。

(四)針對函式庫進行檢測

將開源軟體程式碼安全視為軟體開發安全的一部分，於程式開發過程中，除作一般安全性檢視外，建議也針對使用的函式庫也進行安全實測，在軟體專案中的測試用例(Test Case)中，再增加安全性相關的測試，挖掘可能潛存之安全漏洞。

(五)擬定相關緊急應變措施

針對開源軟體的應用範圍擬定相關應變措施，以及相關替代方案，落實資訊設備備援機制，以避免服務中斷。針對軟體產品可強化版本控制以及持續整合(Continuous integration, CI)，並規劃可能的緩解方案，減低客戶受到資安威脅的負面衝擊。

五、分析與建議

(一)開源軟體因其開放性，駭客可從原始程式碼尋找其漏洞，因此開源軟體資安威脅主要是漏洞遭利用，關注開源軟體更新狀況是最重要的防護作法。

(二)我國產品大量使用開源軟體，企業組織更需重視開源軟體資安議題，且必須掌握產品使用開源軟體的狀況，及早發現漏洞及根因。

(三)當函式庫發生漏洞，將造成大規模的影響，且廠商難以察覺產品是否遭到影響，建議在軟體專案測試用例(Test Case)中，加入安全性測試。

(四)開源軟體的使用，從評估、使用、追蹤漏洞狀況，是必須持續不斷進

行的，並非使用了就可以放任不管，當發現相關開發社群已有停滯跡象，也應評估其它解決方案，避免漏洞出現後無法修補。

(五)使用開源軟體雖會伴隨部分資安隱憂，但若企業組織能進行風險管理，針對風險部分規劃必要措施與管理計畫，開源軟體應用仍能帶給企業組織極大的助益。

- 資料來源：

1. Open-source software
2. The Open Source Definition
3. Create an Effective Governance Policy for Open-Source Software
4. Heartbleed
5. Shellshock
6. 雅虎遭駭！Shellshock 出現首宗大型網站災情
7. Equifax Data Breach Settlement
8. Equifax 資料外洩起自早被修補的 Apache Struts 漏洞，20 萬筆卡號外流
9. 供應鏈攻擊鎖定 GitHub 開源軟體專案
10. DNSmasq 的 7 項安全性漏洞
11. DNSpooq - Kaminsky attack is back!
12. 群暉科技：OpenSSL 漏洞波及該公司多項產品
13. FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurit
14. SOFTWARE BILL OF MATERIALS
15. 公告「適用於製造廠之醫療器材網路安全指引」

第 2 章、 資安活動紀事

資安防護及案例分享研討會-嘉義場

活動時間：111.10.12(三) 14:00~16:30

活動議程：

時間	議程內容	講者
13：30～14：00	活動報到	
14：00～14：30	TWCERT/CC服務範疇及案例分享	TWCERT/CC
14：30～16：20	製造業工控防護	禾伸堂企業股份有限公司 彭志泓 資深副理
16：20～16：30	Q & A	

TWNIC、TWCERT/CC 主辦的資安防護及案例分享研討會，於 10 月 12 日假嘉義大埔美精密機械園區水資源回收中心二樓會議室舉辦。製造業邁向工業 4.0 設備聯網智慧化，伴隨而來資安的威脅，將直接影響生產停擺，導致企業競爭力下降，期望藉由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」，提升企業員工資安知識，從觀念與預先防護，至資安攻擊後處理建議方法，讓我們一同全方位掌握工控資安快速復原產線。

研討會先由 TWCERT/CC 曲承則工程師講授「TWCERT/CC 服務範疇及案例分享」，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。多數的資安事件來自於內部人員的疏失，尤其是惡意郵件與釣魚郵件，若是輕忽上當將帶來的風險與威脅非常大，不僅僅是騙取帳號密碼，將造成更大傷害的勒索、詐財、偷資料等，詐騙對象也相當多元，更多像是無差別式的攻擊。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、漏洞接露通報、惡意檔案檢測服務以及加入 TWCERT 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禾伸堂企業股份有限公司彭志泓資深副理，講授主題為「製造業工控防護」。首先針對資安觀念與資安案例來建立與會者對於資安的概念，點出從 1986 年開始就有所謂的資安問題，只是到近年資安事件增多與影響較大才開始受到重視，講師更以一句「沒有絕對安全，只有相對安全；駭客想拿的，沒有拿不走的」來為資安之重要性破題，並針對資安名詞簡單說明，如 IDS 入侵偵測、IPS 入侵防護、DDOS 分散式阻斷服務攻擊等。接著講師提出許多資安案例，如日本核能電廠、德國鋼鐵廠、銀行 ATM 盜領、企業電腦中毒事件、2019 年~2021 年各大公司遭受勒索案例等資安事件，培養員工養成防禦思維式相對重要，因為沒有一套產品或方案可以預防所有資安事件，因此必須透過定期人員教育訓練、VPN 漏洞更新、Log 檢視以及網路可視性來預防。另針對 ICS 環境攻擊，建議 OT 與 IT 實體隔離，與 OT 產品漏洞更新等方法來進行防禦。目前企業對於 OT 資訊安全多有不知從何做起的疑慮，多數企業面臨到現場機台老舊、設備難以盤點、無專業人員可維護資安系統、操作人員無資安知識、無事件安全對策等問題，彭副理建議從工控基本手法入手，先檢視廠端設備、將 IT/OT 實體隔離、現有設備做好有效備份、防毒與漏洞更新、建立防火牆阻隔 OT 環境上網、擬定災難復原計畫，並定期演練災難復原計畫，待以上基礎資安防護完成再進行進階防

護，未來更可建立資安制度並通過 ISO27001 等。

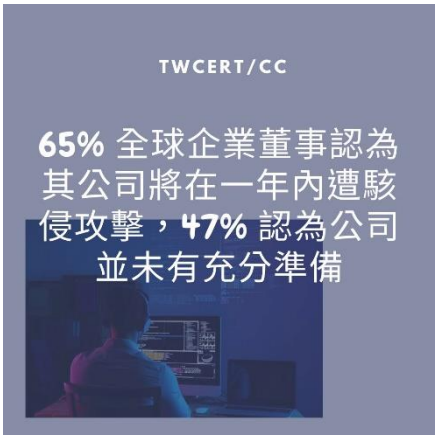
最後議程 Q&A 時段，參與企業人士踴躍提出詢問：首先第一個問題詢問「請問工廠內都是 CNC 機台，OT 的資安建置順序有何建議，因每年有預算上考量」彭副理回覆 CNC 機台目前多有電腦控制，首先建議先從各個機台資安防護先做，之後再進行機台間的網段區隔。第二個問題「關於廠端設備要做盤點，請問設備盤的用意為何呢」彭副理回覆盤點目的是了解廠內 PLC 設備數量、PLC 之韌體規格、工業電腦的版本與更新情況，多數廠內無可視化看板，因此由人工方式來進行盤點，才能執行後續的資安防護措施。第三個問題「企業部份操作人員是移工，針對提升移工資安意識這方面，建議從何著手？」彭副理回覆過去經驗分享，多數機台的 SOP 與生產參數複雜，建議從生產參數 E 化，結合機台之變頻器修改設定，讓操作人員的動作更加標準化與簡短步驟。

本場研討會為實體與線上同步舉辦共 68 人與會，經會後問卷調查統計，與會者對於本次嘉義資安研討會的內容、講師專業度及場地滿意度等，皆十分滿意。

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、65% 全球企業董事認為其公司將在一年內遭駭侵攻擊，47% 認為公司並未有充分準備



資安廠商 Proofpoint 近日發布「2022 年董事會觀點」（2022 Board Perspective）調查報告，指出全球大型企業的董事中，有 65% 認為其企業將在 1 年內遭到嚴重資安攻擊，且有 47% 董事承認其公司並未做好充分準備。

該調查於 2022 年 8 月進行，採訪全球員工超過 5,000 人的大型企業董事共 600 名；這些受訪企業分布於十多個不同國家，跨多種不同產業，也包括公部門與私部門在內。

調查報告也指出，不同國家企業董事對自身企業的駭侵攻擊防範準備程度信心也各自不同；日本企業董事認為公司未準備應對駭侵攻擊的比例最高，高達 72%，其次為新加坡（62%）、英國（58%），而美國公司董事對企業已做好駭侵攻擊應對的比例最高，高達 88%，西班牙與巴西企業董事中

也有約 86% 認為有做好準備。

此外，全球企業董事有高達 75% 認為資安防護與資料治理，是接下來公司的首要任務。

不過，報告也指出企業董事對於企業資安防範量能的認知，可能和實際情形有所落差；報告說有高達 76% 的企業董事認為公司員工已完全了解其在資安防護中的角色，且每月至少進行一次資安教育訓練，但從實際的攻擊案例來看，企業員工對於資安防護的認知與行為仍有所不足，甚至連資安教育訓練都未曾真正落實。

調查也指出，90% 的公私立單位設有資安長，73% 董事表示其資安長會對董事會進行定期資安報告；不過只有 50% 董事會經常與資安長保持互動，更有 33% 董事表示只有在進行報告時才會見到資安長。

建議各公司行號的高階主管與董事階層，應徹底真正了解公司的資安防護狀態，並投資於資安防護所需的軟硬體與教育訓練之上，才能防患未然。

- 資料來源：
  1. New Report from Proofpoint and Cybersecurity at MIT Sloan Reveals Almost Half of Board Members Globa
  2. Majority of Board Members Feel Their Organization Is at Risk of a Cyber Attack, but Almost Half Feel

3.1.2、多家市場研究公司指出，未來十年工業資安防護市場將大幅成長

多家市場研究公司對於製造業與工業資安防護市場的調查報告共同指出，未來 10 年在工業、製造業的資安防護相關市場將會大幅成長；估計到 2030 年該市場的總產值將高達 400 億美元。

據資安專業媒體 SecurityWeek 整理自 Future Market Insight、Markets and Markets、Meticulos Research、Verified Market Research、Stratistics Market Research Consulting、ResearchAndMarkets、Reports and Data、Market Research Future 等市場調查研究機構發表的相關報告後，指出工業資安防護市場巨大的成長動能。

綜合各家研究報告，目前製造業/工業資安防護市場的總產值，約為 160 億到 200 億美元之間；據較保守的估計指出，2027 年時該市場總產值將成長到 201 美元，2030 年成長到 237 億美元；但樂觀的估計則認為製造業/工業資安防護市場的總產值，將從現在的 200 億美元，在 2032 年時成長到 435 億美元，年複合成長率 (compound annual growth rate, CAGR) 將達到 7.7%。

各家研究報告指出，製造業/工業組織為提高運作效率，將愈來愈依賴各式 IoT 技術/裝置與雲端技術，因此對製造業/工業資安防護解決方案的需求亦將日益提高。

此外，各國政府法規與管理對於製造業/工業資安防護能力的要求日漸嚴格，也將是推動製造業/工業資安防護市場總產值成長的重要助力。

Future Market Insight 同時指出，南亞與亞太地區的製造業/工業資安防護市場總產值成長將領先全球其他地區，主要原因在於印度、印尼、泰國與馬來西亞等開發中國家的製造業，將大量開始運用雲端技術；而北美仍舊為全球製造業/工業資安防護的最大市場。

建議相關領域製造業者應投注更多預算與人力，加強軟硬體資安防護能力與員工的資安防護認知。

- 資料來源：
  1. Industrial Cybersecurity Market
  2. Industrial Cybersecurity Market Expected to Soar in Next Decade

3.1.3、統計指出挖礦駭侵者每賺取 1 美元，要消耗高達 53 美元的被駭系統資源

資安廠商 Sysdig 近期發表研究報告指出，分析近期各種挖礦惡意攻擊後得到結論：駭侵者竊取受害者的雲端運算資源來挖礦時，每竊得 1 美元的等值加密貨幣，會消耗高達 53 美元的運算資源。

報告指出，許多以挖礦為目的的駭侵攻擊，例如惡名昭彰的 TeamTNT 等，會設法駭入各公私單位使用的雲端運算服務，例如 Docker Hubs、Amazon Web Services、Redis、Kuberates 布署等等，並且使用植入了 XMRig 惡意挖礦軟體的作業系統映像檔，來執行需要消耗大量 CPU 運算資源的 Monero（XMR）加密貨幣挖礦程式。

XMR 是一種如同比特幣一樣，採用工作量證明（Proof of Work）共識機制，需要大量算力來進行挖礦才能獲得的加密貨幣，由於本身具有十分強大的隱蔽性，他人難以追蹤 XMR 的獲取、轉帳過程，也難以定位持有人，因此很受駭侵者的青睞。

Sysdig 分析近期 TeamTNT 使用超過 10,000 個 endpoint 進行的駭侵挖礦攻擊活動「Chimaera」後，追蹤到 10 個用於攻擊活動的錢包 ID，取得這些錢包 ID 挖礦獲得的 XMR 枚數與等值金額，並據以估算受害者遭到消耗的系統

資源價值；結論是這 10 個錢包一共挖到 39 枚 XMR 代幣，等於 8,120 美元，但消耗掉的系統計算資源卻高達 429,000 美元；相當於每挖到一枚 XMR 代幣，受害者被竊取用來挖礦的系統資源費用就高達 11,000 美元。

Sysdig 表示，上面的計算尚未計入其他額外損失，包括系統硬體因為長時間進行大量運算造成的耗損，以及系統服務因受挖礦活動影響，造成效能下降影響服務品質帶來的損失等等。

建議租用雲端服務的系統管理員，應經常檢查租用物件是否出現不正常的運算負荷，並加強雲端主機或容器的資安防護能力，以免因為遭到盜用而造成鉅額帳單費用。

- 資料來源：
  1. Sysdig 2022 Threat Report: Cloud-native threats are increasing and maturing
  2. Cryptominers hijack $53 worth of system resources to earn $1

3.2、新興應用資安

3.2.1、大型加密貨幣駭侵活動，濫用多種網路免費資源進行挖礦

資安廠商 Sysdig 旗下的資安研究人員，日前發現一場進行中的大型加密貨幣挖礦攻擊活動，濫用各種網路免費資源如 Github、Heroku、Buddy 等服務，用來進行挖礦。

這波攻擊活動以化整為零的方式，在多個雲端運算服務註冊免費使用帳號，利用這些服務提供的免費資源來進行加密貨幣挖礦運算；雖然每個免費帳號能挖到的加密貨幣為數可能不多，但累積起來就是一筆可觀的數字。

據 Sysdig 的報告表示，發動這波挖礦惡意攻擊的駭侵團體稱為「紫海膽」(Purpleurchin)，觀察到的每日函數呼叫高達 100 萬次以上；這波攻擊在 GitHub 申請了 300 個帳號、Heroku 為 2,000 個、Buddy.work 也有 900 個帳號。

報告指出，這些帳號是以程式控制，全自動輪流使用，以含有挖礦專用容器的 130 個 Docker Hub 映像檔隨時切換，用以防範遭到系統偵測停用。

駭侵者設計了能自動註冊新 GitHub 帳號的 shell script，透過 OpenVPN 和 Namecheap VPN 來使用不同 IP 連線到 GitHub，並以隨機產生的 GitHub

Action 名稱來掩蓋其挖礦行動；每一次會同時啟動 30 個以上的 Docker 映像檔來挖礦，挖礦時僅使用一小部分 CPU 與運算資源來挖礦，以免遭到發現而強制停機。

值得注意的是，這波挖礦攻擊中挖掘的，並非市場上規模較大的知名加密貨幣，而是像 TideCoin、Onyx、Surgarchain、Spring、Yenten、Arionum、Bitweb 等相對較小的代幣；由於這些加密貨幣很難直接變現，Sysdig 的資安專家懷疑駭侵者的目的是要掌握各種代幣超過 51% 的算力，挾持整個代幣網路後即可無中生有，再換成 Monero 或 Bitcoin 等更有價值的加密貨幣以牟取暴利。

竊取運算資源挖礦的駭侵攻擊，不只會針對雲端服務業者，一般公司行號或個人的裝置也可能成為目標；如果發現裝置運算速度突然變慢，且發熱量或耗電異常增加，就應懷疑是否遭到植入挖礦惡意軟體。

- 資料來源：
  1. Sysdig TRT uncovers massive cryptomining operation leveraging GitHub Actions
  2. Massive cryptomining campaign abuses free-tier cloud dev resources

3.2.2、駭侵者入侵詐騙網站植入惡意程式碼，搶先竊走受害者數位錢包內的加密貨幣

資安廠商趨勢科技近日發表研究報告，指出有一個稱為「Water Labbu」的駭侵團體，在多個用來詐騙加密貨幣的詐騙網站中植入 JavaScript 惡意程式碼，竊走近 32 萬美元等值的不法加密貨幣詐騙所得。

在趨勢科技的報告中指出，Water Labbu 成功在至少 45 個用來詐騙加密貨幣資產的詐騙網站中，搶先詐騙者把誤入詐騙網站受害者加密錢包中的加密貨幣竊走。

在 2022 年 7 月時，美國聯邦調查局曾發出資安警訊，表示有一波去中心化金融應用程式的詐騙攻擊正在大規模進行中；詐騙者偽裝成各種加密貨幣流動性挖礦伺服器，以高額利率和假冒知名流動性挖礦池，誘騙用戶質押自己擁有的加密貨幣，再將這些質押的加密貨幣竊走。

據趨勢科技的報告指出，Water Labbu 在這些假冒的去中心化應用程式網站中植入的 JavaScript，能夠搶在詐騙網站之前，先行偵測受害者的加密貨幣錢包中是否存有 0.005 枚以太幣或 22,000 枚 USDT 穩定幣的高額加密貨幣，若有即以多種方法，將錢包內的加密貨幣轉帳至 Water Labbu 控制的錢包位

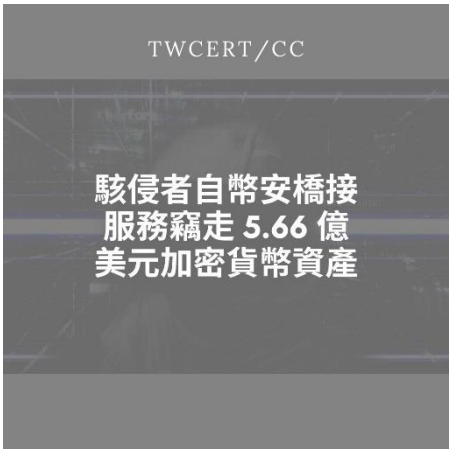
址內。

趨勢科技說，該公司資安團隊發現 9 名遭到這種雙重詐騙手法的受害者，被竊的加密貨幣總額等值高達 316,728 美元。

雖然這是一起「黑吃黑」事件，但受害者仍然蒙受鉅額加密貨幣損失；提醒加密貨幣投資人，絕對不要受到不合理高利率的誘惑，任意在社群媒體或論壇中點按不明人士提供的投資管道相關連結，以免受到詐騙或遭駭侵攻擊。

- 資料來源：
  1. Water Labbu Abuses Malicious DApps to Steal Cryptocurrency
  2. Hackers are breaching scam sites to hijack crypto transactions

3.2.3、駭侵者自幣安橋接服務竊走 5.66 億美元加密貨幣資產



全球交易量最大的加密貨幣交易所 Binance（幣安），日前承認遭到重大駭侵攻擊；駭侵者自其跨鏈橋接（cross-chain bridge）服務 Binance Smart Chain Token Hub 中竊走高達 5.66 億美元等值加密貨幣，目前 Binance 已暫停 Binance Smart Chain 的運作，以調查遭駭事件。

Binance 創辦人趙長鵬在事件發生後，於 Twitter 推文表示，Binance 的 cross-chain bridge 運作中樞 Binance Smart Chain Token Hub 遭到攻擊，駭侵者憑空創造出原本不存在的 BNB 加密貨幣。

Binance 宣布目前已暫停整個 Binance Smart Chain 的運作，用戶無法進行資金存提；Bianace 也要求交易驗證者暫停進行驗證，以進行駭侵事件的調查與處理；Binance 也表示用戶的資金安全無虞。

區塊鏈觀察網站發現疑似駭侵者持有的錢包位址，在 10 月 6 日有兩筆各 100 萬枚 BNB 代幣轉入該錢包位址，接著駭侵者便開始把竊得的 BNB 代幣

匯入多個流動性資金池，將 BNB 代幣交換成包括以太幣、Polygon、Fantom、Avalanche、Arbitrum、Optimism 等其他多種加密貨幣，洗錢的意圖十分明顯。

Binance 也表示，目前絕大部分被竊資金仍然留在 Binance Smart Chain 之上，由於 BSC 已暫停運作，因此駭侵者也無法動用竊得的資金；不過 Binance 估計約有 7 千萬到 8 千萬美元的資金已經從該區塊鏈上轉出。

Binance 也說，正在和其他區塊鏈的營運者合作查緝被竊資金，目前有約 7 百萬美元不在 Binance Smart Chain 上的資金遭到凍結。

由於各種連線的熱錢包或智慧合約，經常遭到駭侵攻擊，造成用戶資金損失，用戶如因投資或其他原因，需將資金放在連網存放處，應避免將大筆資金存放在單一熱錢包或智慧合約，應盡可能分散在不同的熱錢包、區塊鏈、流動性池等，以分散風險，降低潛在損失。

- 資料來源：
  1. Binance confirms BNB cross-chain bridge hack
  2. Hacker steals $566 million worth of crypto from Binance Bridge

3.3、國際政府組織資安資訊

3.3.1、墨西哥、薩爾瓦多、哥倫比亞、秘魯等中美洲國家政府單位接連遭駭，內部資料被竊

包括墨西哥、薩爾瓦多、哥倫比亞、秘魯等中美洲國家的政府與軍方等多個單位，近日接連遭到駭侵攻擊，內部資料遭竊，並有一部分資料由當地環保團體 Guacamaya 對外公開。

被竊取資料的單位，包括墨西哥國防部秘書處、薩爾瓦多民警、哥倫比亞軍方司令部、薩爾瓦多海軍、秘魯軍方等單位。

在墨西哥方面，據媒體報導指出，該國國防部被駭侵者竊取的資料高達 6TB 之多，其中包括各種犯罪者資料、各單位通訊記錄，以及針對美國駐墨西哥大使 Ken Salazar 的監控記錄等資料。

此外，墨西哥總統也在例行記者會中公開承認這起駭侵攻擊確為事實，並表示他個人的就醫資訊亦遭洩漏。總統也指出，這次駭侵勢力是跨國駭侵團體所為，因為包括秘魯、薩爾瓦多、智利與哥倫比亞政府單位，也在同一時間發生資料被竊事件。

被指控為此次跨國駭侵攻擊行動幕後主使者的環保團體 Guacamaya 並未否認其行動，同時指出該團體只對外公開極小部分的資料；該團體也抨擊新聞媒體只把此次行動的焦點集中在總統健康問題上，對於可能造成極大環境破壞的 Tren Maya 鐵路建設計畫未給予夠多的關注。

該團體指出，他們認同 Wikileaks 的精神，認為攸關公眾利益的資訊就應該公開揭露。

資安專家則認為，Guacamaya 可能是利用 2021 年遭發現的 Microsoft ProxyShell 漏洞進行資料竊取攻擊。

建議各政府或民間單位，應隨時注意採用軟硬體系統的最新資安通報，立即修補所有已知漏洞，以防機敏資訊遭竊。

- 資料來源：
  1. Mexican president confirms ‘Guacamaya’ hack targeting regional militaries
  2. Mexican government suffers major data hack, president's health issues revealed

3.3.2、德國警方逮捕利用釣魚攻擊竊取 400 萬歐元的駭侵者

德國聯邦刑事局（Bundeskriminalamt, BKA）日前發布公告，指出該局成功破獲一個駭侵犯罪集團，逮捕三名嫌犯；這三名駭侵者遭控透過大規模釣魚攻擊，成功竊得 400 萬歐元不法所得。

德國警方表示，其中一名嫌犯是 24 歲德國公民，已遭逮捕並且起訴；另一名 40 歲嫌犯被控犯下 124 項電腦詐欺罪名。第三個嫌犯的犯行目前仍在調查階段。

德國警方指出，三名駭侵者的釣魚攻擊行動自 2020 年 10 月 3 日開始，於 2021 年 5 月 29 日結束；其釣魚攻擊的手法是向大量受害者寄發假冒德國各銀行的釣魚信件，偽稱由於銀行變更其安全系統設定，可能影響到受害者銀行帳戶的使用狀態，如果用戶需要繼續使用該銀行的服務，就必須再次登入自己的網路銀行。

駭侵者製作的詐騙信十分逼真，多數人難以分辨真偽；被導到釣魚網頁的受害者，會被要求輸入自己的網路銀行登入資訊，以及單次有效的交易驗證碼；駭侵者取得這些資訊，隨即藉以登入受害者的帳戶，並將其中的資金盜領一空。

德國警方也表示，三名駭侵者係自暗網上購買各種駭侵工具服務，利用這些工具來大量發送釣魚攻擊郵件；這波攻擊甚至造成相關銀行的網頁、伺服器與內網遭到大量自動化查詢需求連線，造成正常服務受阻。

鑑於這類假冒金融機構釣魚攻擊日益猖獗，一般用戶如果收到類似要求進行再次登入或索取驗證碼的郵件，絕對不可輕易點擊其中連結；可以用瀏覽器開啟搜尋引擎，進入銀行真正的官方網站登入，並檢視是否有任何郵件中宣稱的警告訊息出現。

- 資料來源：
  1. Cybercrime: Durchsuchungen und Festnahme
  2. Germany arrests hacker for stealing €4 million via phishing attacks

3.3. 3、澳洲警察秘密探員身分，因哥倫比亞政府文件遭竊而曝光

澳洲聯邦警察局（Australian Federal Police, AFP）負責偵辦中美洲毒品販運的部分秘密探員身分，日前因為哥倫比亞政府機密文件遭竊，因而遭到曝光。

哥倫比亞政府相關機密文件，是在日前遭到中美洲跨國激進運動團體 Guacamaya 聯合駭侵者針對中美洲各國政府發動的駭侵攻擊行動中被竊；當時哥國政府有多達 5TB 的機密資訊遭到竊取。該團體宣稱其目的是為了對抗中美洲各國政權的貪腐與鎮壓，因而發動駭侵行動。

與澳洲警方相關的被竊資料內，包括往來 email 內容、各種文件，以及澳洲警方針對中美洲販毒集團在澳洲境內販售毒品的相關追查偵辦過程等重要機敏資訊。

目前已知遭到曝光的資料，內含 35 個 AFP 的打擊罪犯行動，其中一些專案現在仍在執行中；資料還包括秘密探員針對目標對象的監視報告與通聯監聽錄音檔案，以及哥倫比亞警官的薪資等。

AFP 對外證實了資料遭竊一事，同時指出「AFP 十分關切這次資料外洩事件對各專案執行造成的影響；AFP 也正在與受影響區域月的夥伴共同合

作，以對應任何對相關人身安全與調查工作造成的潛在威脅。」

除了澳洲之外，還有多國警方也和哥倫比亞政府合作，打擊中美洲的跨國毒品販運集團；因此在這次駭侵攻擊行動中，可能也會有其他國家執法人員和執法行動的相關資訊遭到曝光。

建議各政府單位應加強資安防護能力與軟硬體設定，並且落實人員的資安訓練，避免各種機敏資訊遭外洩。

- 資料來源：
  1. Secret agents targeting drug cartels in Australia exposed in data hack
  2. Australian police secret agents exposed in Colombian data leak

3.4、社群媒體資安近況

3.4.1、非官方 WhatsApp Android App 會竊取用戶帳號控制權

資安廠商 Kaspersky 日前發表研究報告，指出該公司的研究人員，近日發現一個名為 YoWhatsApp 的 Android 非官方 WhatsApp 通訊軟體，內藏惡意程式碼，能夠存取用戶的 WhatsApp 金鑰，藉以竊取用戶的帳號控制權限。

Kaspersky 旗下的資安研究人員，從去年開始追查隱藏在修改版 WhatsApp 的 Triada 特洛依木馬；最近則發現了這個 YoWhatsApp。

YoWhatsApp 是一個第三方開發的通訊軟體，相容於 WhatsApp，但比原版的 WhatsApp 多了一些用戶會喜歡的功能，例如自訂聊天界面、強化的通話阻擋功能等等；YoWhatsApp 也透過其他熱門 Android 應用程式內的廣告來進行廣告宣傳，因此相當受到歡迎。

Kaspersky 的資安研究人員在報告中指出，YoWhatsApp 會擅自將用戶的 WhatsApp 存取金鑰傳送到開發者設立的遠端伺服器；雖然目前還沒有發現有駭侵者利用這些竊取而來的金鑰發動任何攻擊，但理論上擁有用戶的 WhatsApp 存取金鑰，即可控制用戶的 WhatsApp 帳號，並且取得用戶的通訊

內容，或是假冒為用戶本人和其他人進行通訊。

Kaspersky 還發現，有一個和 YoWhatApp 完全相同的複製品，以「WhatsApp Plus」之名，利用多種廣告平台自我推銷，試圖獲得更多用戶安裝使用。

此外，WhatsApp 的開發公司 Meta，本月也控告多家行動軟體公司；這些公司推出多種號稱相容於 WhatsApp，但也會竊取用戶的 WhatsApp 控制權。

建議用戶如有使用各種行動應用程式的需求，務必從正常管道下載官方版本應用程式，避免在其他地方下載非官方的應用程式或破解版，以免遭到駭侵者竊取帳號權限或各種機敏資訊。

- 資料來源：
  1. Malicious WhatsApp mod distributed through legitimate apps
  2. Unofficial WhatsApp Android app caught stealing users' accounts

3.4.2、新發現 PHP 資訊竊取惡意軟體，針對 Facebook 帳號發動釣魚攻擊

資安廠商 WithSecure 旗下的資安專家，近日發現一波名為「Ducktail」的釣魚攻擊活動，利用全新出現、以 PHP 撰寫的 Windows 資料竊取惡意軟體，用來竊取受害者的 Facebook 帳號、瀏覽器資料、加密貨幣錢包等機密資訊。

WithSecure 指出，該公司於 2022 年 7 月起觀察到 Ducktail 的攻擊活動；該攻擊主要是在 LinkedIn 求職求才社群平台上，透過社交工程將含有 .NET Core 惡意程式碼的行銷計畫 PDF 檔傳遞給受害者。

一旦受害者開啟該 PDF 並執行惡意程式碼後，存於電腦的瀏覽器資訊就會被傳送到一個 Telegram 私密頻道，駭侵者利用這個私密頻道作為其控制伺服器；駭侵者主要鎖定其中的 Facebook Business 帳號資料，取得資料後即用於進行進一步的金融詐騙或惡意廣告。

另一家資安廠商 ZScaler 則指出，他們觀察到 Ducktail 近期也開始利用 PHP 程式碼的惡意軟體，偽裝為遊戲相關檔案、字幕檔、成人影片等，誘使用戶下載；用戶執行該惡意程式碼後，其電腦的 Microsoft Office 應用程式就會遭到攻擊。用戶會看到假的「檢查應用程式相容性」彈跳視窗，實則正在

安裝駭侵者推送的各種惡意軟體。

該惡意軟體執行後，會每日一次在背景中竊取用戶的各種 Facebook 帳號詳細資訊、瀏覽器 Cookie 及其他資料、加密貨幣錢包與帳號資訊，以及各種系統資訊。

鑑於各種釣魚攻擊日益頻繁，建議用戶如在社群平台接獲他人傳送的檔案，務必確認該名傳送者的真實身分，切勿開啟身分不明人士傳送的任何檔案或連結。

- 資料來源：
  1. LinkedIn phishing target employees managing Facebook Ad Accounts
  2. New PHP Variant of Ducktail Infostealer Targeting Facebook Business Accounts
  3. New PHP information-stealing malware targets Facebook accounts

3.4.3、LinkedIn 新資安功能推出，偽裝任職知名大公司的假帳號大幅減少

求職求才社群服務 LinkedIn 日前推出三項新功能，以打擊該平台上日益猖獗的假帳號與相關惡意攻擊活動；推出後初見成效，偽裝任職於知名大公司如 Apple、Amazon 等的假帳號數量明顯減少。

過去數年以來，在 LinkedIn 平台上發生的惡意攻擊數量愈來愈多，包括各式社交工程、釣魚攻擊、散布惡意軟體、竊取登入資訊、金融詐騙等等，主要都是透過該平台上的假帳號來進行。

這些假帳號為了取信於被害人，多半會捏造出相當漂亮的工作經歷，例如在世界頂尖企業擔任重要管理職務；而這類假帳號可以透過人工智慧軟體大量產生，再配上由人工智慧合成的個人頭像，幾可亂真，造成用戶難以識別真偽。

LinkedIn 近日宣布推出的三項新功能，第一項是在用戶的個人檔案中提供更多資訊，例如該用戶檔案的建立日期、用戶是否已通過電話號碼驗證，以及是否提供工作用的企業 email 位址等等。這樣可以幫助用戶辨識帳號的真實性，也提高假帳號取信於人的難度。

第二項功能是利用人工智慧掃瞄並找出利用人工智慧合成而成的個人頭像；LinkedIn 指出該技術的深度學習功能，可以發現頭像是否為人工智慧產生，而非真人照片。

第三項功能是在用戶透過線上對談功能溝通時，如果系統發現有一方試圖把對方帶離 LinkedIn 平台進行私下溝通時，會在對話內容中顯示警訊。

LinkedIn 在近期推出這些功能後，同時也開始掃蕩平台上的假帳號；一位經常關注 LinkedIn 平台狀況的開發者於上周發現，在 LinkedIn 上號稱任職於 Apple、Amazon 等大企業的帳號總數突然大幅下降；在 2022 年 10 月 10 日，LinkedIn 上宣稱任職於 Apple 的帳號總數有 576,562 個，隔天就下降到 285,000 人，而任職於 Amazon 的帳號數也少了 30%。

不過，這些數字還是遠高於這些企業的實際員工人數（Apple 員工人數約為 147,000 人），由此可見 LinkedIn 上的假帳號為數仍然非常多。

建議用戶在 LinkedIn 上與其他帳號互動時，務必提高警覺，小心查核對方身分是否屬實，以免受騙上當或遭到駭侵攻擊。

- 資料來源：
  1. New LinkedIn profile features help verify identity, detect and remove fake accounts, boost authentic
  2. Nearly 600,000 people on LinkedIn listed Apple as their employer on one day in October. The next day
  3. LinkedIn's new security features combat fake profiles, threat actors

3.5、行動裝置資安訊息

3.5.1、Android 惡意軟體 Drinik 鎖定 18 家印度銀行用戶發動攻擊，竊取其個資與銀行登入資訊

資安廠商 Cyble 旗下的資安研究人員，日前發現一個名為「Drinik」的 Android 惡意軟體，現正發動大規模攻擊行動，鎖定 18 家印度主要銀行的用戶，意圖竊取其個資與銀行登入資訊。

Drinik 早在 2016 年就被發現針對印度手機用戶發動攻擊，當時最早是竊取手機簡訊內容，到了 2021 年 9 月時，該惡意軟體新增金融特洛依木馬的攻擊能力，目標鎖定 27 家印度金融機構的用戶，將用戶導向至釣魚網頁以竊取機敏資訊。

近日 Cyble 發現 Drinik 再度改版，這次的攻擊手法是偽裝成印度政府官方國稅局的稅務管理 App，引誘用戶下載後再設法竊取用戶的各種個資與金融服務登入資訊。

報告指出，Drinik 設法誘使用戶安裝一個叫做「iAssist」的 APK 檔案，該檔案宣稱是印度國稅局的稅務管理工具軟體，並會在安裝時向用戶要求多種權限，包括接收、讀取與發送簡訊、讀取用戶通話記錄、讀寫外部儲存媒體，以及最重要的輔助使用服務權限。

用戶一旦給予這些權限，Drinik 會立即關閉 Google Play Protect 的惡意軟體防護功能，並且開始竊聽或盜錄用戶的操作，例如私下進行螢幕截圖、記錄用戶按鍵輸入等等，接著載入真正的印度國稅局所得稅申報頁面，在用戶輸入登入資訊時，同時竊取用戶輸入的資料。

建議智慧型手機用戶應絕對避免在非官方管道自行安裝任何應用程式，同時不應試圖破解手機（即越獄），以免系統內建的防護機制失靈；應用程式如果要求過多不必要權限，也應提高警覺，應拒絕給予權限並立即刪除該應用程式。

- 資料來源：
  1. Drinik Malware Returns With Advanced Capabilities Targeting Indian Taxpayers
  2. Drinik Android malware now targets users of 18 Indian banks

3.5.2、Google Play Store 中新發現 16 個 Android 廣告惡意軟體，下載次數合計超過 20 萬次

資安廠商 McAfee 日前發表研究報告，指出該公司在 Google Play Store 中新發現 16 個 Android 廣告惡意軟體；這些惡意廣告軟體會在背景執行，以用戶看不見的隱形 frame 載入大量廣告，並進行假點擊以牟取暴利。

McAfee 指出，這 16 種廣告惡意軟體成功上架到 Google 官方的應用程式商店 Google Play Store，偽裝成各種工具軟體，例如匯率轉換、手電筒、QR Code 掃瞄器、系統記憶體清理工具、韓文字典、拍照軟體、記事工具等等。

其中一個名為 DxClean 的廣告惡意軟體，在遭到下架前獲得 500 萬次下載，在 Google Play Store 中的用戶評分甚至還高達 4.1 分（滿分為 5 分）。

該軟體號稱可以清理 Android 系統中閒置應用軟體佔用的記憶體並將其釋放出來，以改善手機運作效能與反應速率，甚至還能阻擋不必要的廣告；但實際上該軟體的行為恰恰相反，是在背景中大量載入廣告並進行假點擊。

據 McAfee 的分析指出，這些廣告惡意軟體會在安裝後自某個特定伺服器下載 Firebase Cloud Messaging listener，並開始接收自 FCM 傳來的指令；惡意軟體一旦接收到指令，即會開始在背景中載入廣告，並模擬用戶的點按行

為。

由於這些廣告載入和點擊動作均不會有任何顯示，因此用戶難察覺；但用戶將會發現手機反應變慢、耗電加快、手機會發熱，數據連線的額度也會遭到耗用，甚至因此造成手機故障。

建議用戶即使在官方的 Googel Play Store 中下載軟體，也應提高警覺，仔細閱讀用戶意見回饋；並應在手機中安裝大廠出品的防毒防駭軟體，以防不小心安裝到惡意軟體。

- 資料來源：
  1. New Malicious Clicker found in apps installed by 20M+ users
  2. Android adware apps in Google Play downloaded over 20 million times

3.6、軟體系統資安議題

3.6.1、Linux Kernel 5.19.12 內含可能損壞採用 Intel 顯示晶片筆記型電腦螢幕的錯誤

Linux 近期發行的 kernel 新版本 5.19.12，遭用戶發現含有一個顯示方面的錯誤，會造成使用 Intel 圖形處理器晶片（Graphics Processing Unit, GPU) 的筆記型電腦液晶顯示器不斷閃爍或出現閃動白色畫面；不僅造成用戶困擾，影響正常作業，也可能造成顯示面板永久損壞。

Intel 旗下的 Linux kernel 工程人員 Ville Syrjäl 在分析這個問題後，指出是 Linux kernel 內部處理顯示面板電源序列組件的錯誤，導致面板發生不正常閃爍問題；他呼籲有此問題的 Intel 顯示晶片筆記型電腦用戶，盡快將使用的 Linux kernel 版本退回到前一版本，以避免筆記型電腦的液晶顯示器受到損壞。

另一方面，Linux kernel stable branch 的維護者，也在日前緊急釋出 kernel 版本 5.9.13，解決了各發行版本使用 5.9.12 核心可能造成的問題；維護者也指出，5.9.12 核心的使用者如果未曾發生任何顯示問題，無需升級到 5.9.13。

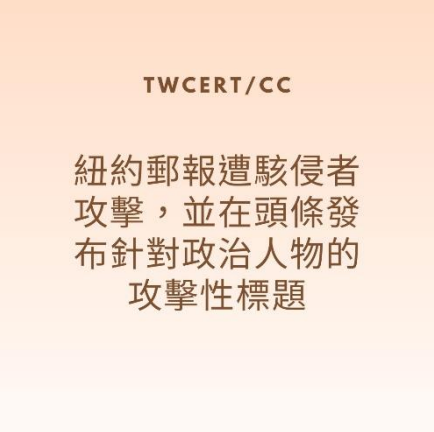
而使用者相當多，基於 Arch 的 Majaro 發行版也表示，他們將會把 kernel 從版本 5.19.7 直接升級到 5.19.13，以避免其 Intel GPU 用戶發生顯示問題。

不過由於 Linux 的發行版本眾多，預期未來可能仍有不少用戶會在不知情的情形下，升級到有此顯示問題的 kernel 版本。

建議 Intel GPU 筆記型電腦用戶在升級 Linux 發行版本前，務必事先確認該發行版本的 kernel 版本不是 5.9.12；已有此問題的 Intel GPU 筆電用戶，也要避免讓顯示器長久處於閃爍狀態，以免不正常顯示過久，造成面板永久損壞。

- 資料來源：
  1. white flashing display with 5.9.12
  2. Linux Kernel 5.19.12 bug could damage Intel laptop displays

3.6.2、紐約郵報遭駭侵者攻擊，並在頭條發布針對政治人物的攻擊性標題



美國紐約郵報（New York Post）日前證實，該報的網站系統與 Twitter 帳號遭到不明駭侵者挾持，並且用於攻擊包括美國總統、紐約市長、各州州長、國會議員等多位美國政治人物。

紐約郵報是在 2022 年 10 月 27 日遭到駭侵攻擊，不只其網路新聞的頭版大標題遭到駭侵者擅自替換為攻擊性文字，其經過官方認證的 Twitter 帳號亦遭駭侵者挾持，並且連續發出多則攻擊特定攻治人物的推文。

遭到攻擊的美國政治人物，包括現任總統拜登（Joe Biden）與其子 Hunter Biden、紐約市長 Eric Adams、紐約州民主黨眾議員 Alexandria Ocasio-Cortez、紐約州長 Kathy Hochul、德州州長 Gregg Abbot、伊利諾州共和黨眾議員 Adam Kiinzinger 等人。

目前紐約郵報沒有提供其網站系統與 Twitter 帳號如何遭到駭侵挾持的詳細資訊。

針對美國媒體發動的駭侵攻擊，近期亦有一例，遭駭的媒體是財經網路媒體 Fast Company；該媒體的內容管理系統（Content Management System, CMS）遭到不明駭侵者攻擊，其網站系統被駭侵者用來推送內含種族歧視的

內容，該批內容甚至還發送到 Apple News 新聞聚合平台，並且以通知的形態推送到讀者手機內。

該攻擊行動導致 Fast Company 整整兩星期被迫將網站下線。

另一起攻擊事件於今年 2 月揭露，受害者是本次駭侵事件主角紐約郵報的擁有者新聞集團（News Corp），旗下還擁有 Fox News、華爾街日報等大型媒體。News Corp 在一月時發現駭侵者未經授權存取其工作人員與記者所有的文件與 Email 內容。

由於新聞媒體對社會具有極大影響力，一旦遭駭侵者用於發送不實消息，將造成巨大的社會衝擊；各媒體應加強自身的資安防護能力，同時做好員工教育訓練，避免駭侵者以社交工程、魚叉式釣魚攻擊等方式挾持媒體。

- 資料來源：
  1. New York Post @nypost
  2. New York Post Says Rogue Employee Was Behind Vulgar and Racist Posts
  3. New York Post hacked with offensive headlines targeting politicians

3.6.3、勒贖駭侵團體宣稱成功駭入跑車製造商法拉利，取得大量內部文件

義大利著名超級跑車製造大廠法拉利（Ferrari）傳出遭駭事件，一個名為 RansomEXX 的勒贖駭侵團體，日前在暗網上宣稱該團體成功駭入法拉利的內部系統，公開了高達 7 GB 以上的內部文件。

據報導，在網路上被公開的法拉利內部文件，包括各種資料表格、維修零組件相關資料等等。目前無法得知勒贖團體是否已要求法拉利交付贖金以取回被竊檔案。

目前法拉利已對外公開證實這次駭侵攻擊事件，但僅表示有部分內部文件遭到公開放網路上；該公司也對外指出，目前並無證據顯示該公司的內部系統遭到入侵或勒贖攻擊，其生產活動與事業經營也一切正常，並未受阻。該公司目前正在針對這起駭侵事件進行調查，以了解其發生原因。

本次攻擊事件是法拉利在今年第二度遭到駭侵攻擊，而且就發生在該公司宣布與資安防護廠商 Bitdefender 合作的一星期之後。

法拉利在今年 5 月時亦曾遭到駭侵攻擊。當時法拉利宣布與瑞士區塊鏈廠商 Belas Network 合作，針對旗下 F1 車隊支持者發行 NFT（Non-Fungible Token，非同質性貨幣），供支持者購買收藏，或當作數位周邊商品；隨即該

公司所屬的一個子網域就遭到駭侵者挾持，用來架設 NFT 詐騙網站長達數月之久。

鑑於針對全球知名品牌廠商進行的勒贖攻擊有愈演愈烈的趨勢，甚至同一廠商很可能被相同或不同的駭侵團體連續發動勒贖攻擊，造成機密與商譽的損失，因此這類廠商必須特別提高警覺，加強有形與無形的資安防護能力。

- 資料來源：
  1. Ferrari hacked? RansomEXX claims to have punctured automaker’s cyber defences
  2. Ferrari says internal documents online, but no evidence of cyber attack

3.6.4、澳洲 Medibank 承認所有 280 萬名用戶個資均遭駭侵者竊走

澳洲大型銀行兼保險業者 Medibank 日前發表資安通報，證實在近期發生的勒贖攻擊中，該行儲存的所有客戶個資與大量健康申告書資料，都遭到駭侵者竊走，受害客戶總數高達 280 萬人。

該行在日前發表的聲明中承認，這次勒贖攻擊對該行客戶資料造成的危害，經過調查後發現比預期的大相當多；個人資料與個人健康申告資料被竊的客戶，包括該行的所有澳洲籍保險客戶、所有國際學生保險客戶、所有 Medibank 銀行客戶等。

該行也在聲明中指出，發現駭侵者有刻意刪除系統存取資料的行為，因此無法排除在客戶個資遭竊之外，還會發現更大損失的可能。

這波針對 Medibank 的駭侵攻擊活動，發生於 2022 年 10 月 12 日；Medibank 在隔天隨即發布資安通報，當時通報指出沒有資料遭竊的證據；不過數日後 Medibank 承認勒贖攻擊者與該行聯絡，並且展示竊自該行的 200GB 資料，該行進一步調查後才發現所有客戶資料全都遭到駭侵者竊走。

目前該行對外表示，仍持續進行調查，並與執法單位合作；對於受這起資料竊取事件影響的 Medibank 保險與銀行客戶，該公司提供財務支援，必須

重新申請證件辦理的客戶，其一切費用亦由該行負擔。

此外，鑑於澳洲近日發生多起針對公私單位的駭侵攻擊活動，澳洲政府也準備提高個資保護相關罰則；未能保護客戶資料導致遭駭的罰金，將從目前的 222 萬澳元大幅提高到 5,000 萬澳元，或是所造成損失的三倍金額，或是該公司當年營收的 30%，三者取最大值予以裁罰。

鑑於各類個資竊取造成的損失愈來愈大，政府對這類資安管理失當的裁罰也日漸加重，握有客戶個資的公私單位應思考減少對於客戶個資的需求，同時加強各種資安防護能力，避免所保存的個資被竊而遭到重罰，以及對應的司法賠償與刑事責任。

- 資料來源：
  1. Cyber event updates and support
  2. Medibank now says hackers accessed all its customers' personal data

3.7、軟硬體漏洞資訊

3.7.1、Apache Commons Text 程式庫遭發現內含可遠端執行任意程式碼的漏洞

Github 旗下的資安專家，日前發現廣為使用的開源程式庫 Apache Commons Text，內含一個可讓駭侵者用來發動攻擊，進而遠端執行任意程式碼的漏洞；採用此開源程式庫的應用軟體應立即升級至無此漏洞的新版本。

Apache Commons Text 是個相當受到開發者歡迎的開源 Java 程式庫，內含「文字改寫系統」（interpolation system）；開發者可以利用這個系統對輸入的文字進行多種操作，包括修改、解碼、生成、抽取等等。

該漏洞又被稱為「Text4Shell」，其 CVE 編號為 CVE-2022-42889，是存於文字改寫系統中的不安全程式碼評估處理；在預設組態情況下，駭侵者可以輸入特製的惡意內容，來觸發此漏洞，進而遠端執行任意程式碼。

CVE-2022-42889 的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分）；危險程度評級達到最高等級的「嚴重」（Critical）等級。

資安專家在 Apache 的郵件群組內指出，自 Apache Commons Text 1.5 版起到 1.9 版之間，在預設的 Lookup instance 組態下，存有這個可導致遠端執行任意程式碼，或與遠端伺服器連線的漏洞；用戶應盡早將 Apache Commons Text 升級至 1.10.0 版本，該版本已預設停用有問題的文字改寫系統。

該漏洞是在 2022 年 3 月 9 日由 Github 的資安專家發現，並提報給此開源程式庫的開發單位 Apache Foundation；Apache Foundation 於 10 月 12 日推出修正此漏洞的 Apache Commons Text 1.10.0 版。

建議軟體開發者如有採用上述受影響版本的 Apache Commons Text，應立即升級至已修復此漏洞的 1.10.0 與後續版本。

- CVE 編號：CVE-2022-42889
- 影響產品/版本：Apache Commons Text 1.5 到 1.9 版。
- 解決方案：升級至 Apache Commons Text 1.10.0 版與後續版本。

- 資料來源：
  1. CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due t
  2. Apache Commons Text RCE flaw — Keep calm and patch away
  3. CVE-2022-42889

3.7.2、Apple 修復一個已用於駭侵攻擊的全新 0-day 漏洞 CVE-2022-42827

Apple 於日前推出的 iOS 16.1、iPadOS 16.1 中，修復一個可能已遭用於駭侵攻擊的 0-day 漏洞 CVE-2022-42827，該漏洞可讓駭侵者取得 kernel 權限並且遠端執行任意程式碼；iPhone 與 iPad 用戶應立即更新作業系統，以免遭到駭侵者透過此漏洞發動攻擊。

據 Apple 發表的資安通報與 iOS 16.1、iPadOS 16.1 更新記事中指出，CVE-2022-42827 是一個記憶體緩衝區越界寫入錯誤，導因於邊界檢查的漏洞所致；駭侵者可利用這個漏洞誘發記憶體崩潰，因而取得 kernel 權限並遠端執行任意程式碼。該漏洞為一位匿名資安研究人員發現並提報 Apple。

據 Apple 發布的資安通報指出，該公司已知悉本漏洞可能已遭駭侵者用於發動駭侵攻擊，惟目前並無相關攻擊事件的進一步訊息。

該漏洞影響的 Apple iPhone 與 iPad 產品，包括 iPhone 8 與後續機型、iPad Pro 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。

CVE-2022-42827 是 Apple 於 2022 年修復的第 9 個 0-day 漏洞。

此外，在 Apple 這次推出的 iOS 16.1、iPadOS 16.1 中，也同時修復多達 18 個資安漏洞；其中包括上述 CVE-2022-42827 在內，共修復多達 13 個可讓駭侵者遠端執行任意程式碼的各式資安漏洞。

由於 iPhone 與 iPad 使用人數眾多，往往成為駭侵者的絕佳攻擊目標，因此 iPhone 與 iPad 用戶，應在 Apple 推出作業系統更新的第一時間就進行更新，以免遭駭侵者利用已公開的漏洞發動攻擊。

- CVE 編號：CVE-2022-42827
- 影響產品/版本：iPhone 8 與後續機型、iPad Pro 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。
- 解決方案：升級至 iOS 16.1、iPadOS 16.1。

- 資料來源：
  1. About the security content of iOS 16.1 and iPadOS 16
  2. Apple fixes new zero-day used in attacks against iPhones, iPads

3.7.3、macOS 遭發現存有可執行未簽署應用程式的漏洞

macOS 系統管理軟體廠商 Jamf 旗下的資安團隊研究人員，日前發現 macOS 內的 Archive 公用程式內含一個漏洞 CVE-2022-32910，可導致特製的未簽署、未授權應用程式可於 macOS 系統執行，且不會跳出應有的警示訊息通知用戶。Apple 已在日前推出的作業系統更新中修復此漏洞。

Jamf 在發表的漏洞研究報告中指出，在今（2022）年年初，該公司發現 Safari 瀏覽器的漏洞 CVE-2022-22616，可利用特製的 Zip 壓縮檔，跳過 macOS 系統的 GateKeeper 檢查，這樣即可在用戶不知情的情形下，執行 Zip 檔中的惡意軟體。

Jamf 在通報該漏洞給 Apple 並獲得修復後，開始研究 macOS 內是否有類似可透過壓縮檔來跳過系統資安查核過程的類似漏洞，果然發現系統內建的壓縮 / 解壓縮工具程式 Archive 也具有類似漏洞，駭侵者可以使用特製的壓縮檔，內含一個具有 .app 副檔名的多個檔案，具要有多個檔案路徑設定為目標目錄的根目錄，這樣 Archive 公用程式就會略過 .app 副檔名檔案的 GateKeeper 檢查程序。

Jamf 在發現此漏洞後，立即於今年 5 月 31 日向 Apple 通報；而 Apple 於 7 月 20 日推出的 macOS Monterey 12.5 與其他舊版 macOS 更新中，修復了這個問題。

建議使用者應密切注意所使用電腦作業系統的更新消息，當有資安更新推出時，應立即套用更新，以免遭到駭侵者利用這類已公開的漏洞來發動攻擊，造成系統尚未更新用戶的潛在資安風險。

- CVE 編號：CVE-2022-32910
- 影響產品/版本：macOS Monterey 12.5 之前版本。
- 解決方案：升級至 macOS Monterey 12.5 或以上版本。

- 資料來源：
  1. About the security content of macOS Monterey 12.5
  2. Jamf Threat Labs identifies macOS Archive Utility vulnerability allowing for Gatekeeper bypass

3.7.4、Microsoft Exchange Server 的最新 0-day 暫時解決方案可遭略過

Microsoft Exchange Server 日前被發現的 2 個 0-day 漏洞 CVE-2022-41040、CVE-2022-41082，雖然很快就由官方發布暫時解決方案，但資安專家在數日內就發現這個解決方案並不足以防止駭侵者利用該兩漏洞發動攻擊。

越南資安廠商 GTSC 旗下的資安專家，在約三星期前發現這兩個 Microsoft Exchange Server 的 0-day 漏洞 CVE-2022-41040、CVE-2022-41082，其中 CVE-2022-41040 這個漏洞可讓獲得登入權限的駭侵者遠端誘發 CVE-2022-41082 漏洞，並利用後者遠端執行任意程式碼。

這兩個 0-day 漏洞的 CVSS 危險程度評分均為 8.8 分，危險程度評級為「高」(High) 等級。據 Microsoft 日前發布的資安通報，該公司已知這兩個 0-day 漏洞已遭駭侵者發動範圍有限的駭侵攻擊行動。

在 Microsoft 公布的資安通報中，雖然也提供了暫時的漏洞解決方案，要求系統管理員在 IIS Manager 中新增規則，不讓不具有管理權限的用戶遠端存取 PowerShell，但資安專家指出這個暫時解決方案只能夠阻擋已知的攻擊 URL，對於來自未知或新來源的相關攻擊是不具備防護能力的。

資安專家也指出，這種防禦方式只適用於部署在組織內部的 Microsoft Exchange Server，但有許多單位採用的是內部伺服器加上雲端主機的混合式架構，據統計有超過 1,200 個單位將這類混合式架構曝露於於外部網路；這類單位就很容易成為駭侵者的攻擊目標。

- CVE 編號：CVE-2022-41040、CVE-2022-41082
- 影響產品/版本：Microsoft Exchange Server 各版本。
- 解決方案：建議系統管理員應針對內部部署與雲端的 Microsoft Exchange Server 加強管理，勿授與任何不必要的帳號過大權限，特別是如 PowerShell 這類強力系統工具的權限，也應隨時注意 Microsoft 推出的最新修補工具並立即修補漏洞。

- 資料來源：
  1. Microsoft Exchange Server Elevation of Privilege Vulnerability
  2. Microsoft Exchange Server Remote Code Execution Vulnerability
  3. Microsoft Exchange server zero-day mitigation can be bypassed

第 4 章、 資安研討會及活動

TWCERT 2022 台灣資安通報應變年會	
活動時間	111 年 11 月 15 日（星期二）上午 09 時 30 分至 16 時 30 分
活動地點	線上會議(使用平台：Webex)
活動網站	https://twcert.informationsecurity.com.tw/2022_annual_meeting.htm
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 2022 年是全球見證地緣政治衝突下，網路攻擊可以被武器化、直接影響民生領域的關鍵年。今年台灣數位發展部揭牌，核心理念即是「全民數位韌性」，要從社會共融、產業轉型、應變韌性等 3 層面建構相關基礎。TWCERT 2022 台灣資安通報應變年會邁入第六屆，在這關鍵時刻，年會以「資安韌性　營運永續」為主題，邀集產官學研及國際專家共同探討資安聯防最佳實踐、關注資安威脅趨勢發展，讓更多人投入資安，一次次更強韌，一起讓台灣更好。 參加對象：國內各大企業、中小企業經營者、製造業者、高科技產業、資安領域相關業者、CERT/CSIRT 組織、ISAC 組織、SOC 組織與對資安主題有興趣之單位。

【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 （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	 **主辦單位：中華民國資訊軟體協會** 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。 活動聯絡人：廖資深專員 Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext：388

11/18 資安防護及案例分享研討會-台中場	
活動時間	11/18(五) 14:00-16:30
活動地點	經濟部加工出口區管理處中港分處三樓訓練教室 (臺中市梧棲區大觀路 6 號)
活動網站	https://docs.google.com/forms/d/e/1FAIpQLSeKtEd--br81AeRh5fxLfgrSHl-6frBvXp6tzKHTYtkdOz5jA/viewform
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 製造業邁向工業 4.0 設備聯網，促使 IT 與 OT 匯流，讓工控環境成為駭客熟悉易攻的場域，更因 OT 機台難以長時間停機定期修補與更新，且企業遭受攻擊將連帶影響供應鏈廠商，導致製造業的資安管理陷入困境。 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)免費資安通報的資源，並邀請專業講師探討「網路與資訊安全管理實務分享」，從工業 4.0 機聯網資安防護至供應鏈資安管理，讓我們一同建立 OT 資安管理新思維。 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

HITCON CTF 2022	
活動時間	11/26(六) 10:00 ~ 11/27(日) 22:00 (UTC+8, 36 小時)
活動地點	請參閱活動網站
活動網站	https://ctf2022.hitcon.org/
活動概要	 **主辦單位：台灣駭客協會、工業技術研究院** 競賽說明 競賽為 36 小時的線上 Jeopardy 形式 CTF 競賽採取積分累計制，依分數高低進行排名 同分者，依最後一次正確提交的時間判定 每道題目的分數將會根據解題隊伍數即時進行動態調整 Flag 形式為: hitcon{printable ascii+} 競賽時間 11/26(六) 10:00 ~ 11/27(日) 22:00 (UTC+8, 36 小時) 其他比賽注意事項請參閱活動網站。

【資安學院-國際證照班】ISO 27001：2013 資訊安全管理系統主導稽核員訓練課程	
活動時間	11/21~23、11/28～11/29 共計五日
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/2864
活動概要	 **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 資訊安全管理系統照。 課程對象： 資訊安全管理人員、內部稽核人員、電腦稽核人員 ISO/IEC 27001 輔導人員及將提供資訊安全管理系統輔導之顧問 IT 部門、MIS 部門、財務稽核部門同仁 有志瞭解 ISO27001 標準規範、知識應用及取得國際專業個人證照者

	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 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。 學員未通過筆試但通過持續評量者將收到「上課證明」，並被允許於原課程結束日起 12 個月內參加重考（費用另計）。 學員將於課程完成後八週內收到證書。 本課程需全程參與，不可請假或缺席，請假或缺席時數者不予考試及發證，敬請保留完整上課時間。

第 5 章、 TVN 漏洞公告

全景軟體 RAVA 憑證驗證系統網站 - SQL Injection	
TVN / CVE ID	TVN-202209012 / CVE-2022-39056
CVSS	9.8 (Critical)
影響產品	全景軟體 RAVA 憑證驗證系統網站 v3
問題描述	RAVA 憑證驗證系統網站特定功能參數未對使用者輸入進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	請與全景軟體聯繫提供修補方案
公開日期	2022-10-18
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6617-109b0-3.html

中華數位科技 Mail SQR Expert 全方位電子郵件管理專家 - Command Injection	
TVN / CVE ID	TVN-202210008 / CVE-2022-40741
CVSS	9.8 (Critical)
影響產品	中華數位科技 Mail SQR Expert 全方位電子郵件管理專家 version 2dut.190301
問題描述	Mail SQR Expert 未對特定功能參數進行特殊字元的過濾，導致遠端攻擊者不須權限，即可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令，並對系統進行任意操作或中斷服務。
解決方法	Update 中華數位科技 Mail SQR Expert version to 2dut.220701 (此版號更新不包含運行在 FreeBSD 9.x 的設備)
公開日期	2022-10-26

相關連結	https://www.twcert.org.tw/newepaper/cp-151-6643-89bfa-3.html

全景軟體 RAVA 憑證驗證系統網站 - Path Traversal	
TVN / CVE ID	TVN-202209014 / CVE-2022-39058
CVSS	7.5 (High)
影響產品	全景軟體 RAVA 憑證驗證系統網站 v3
問題描述	RAVA 憑證驗證系統網站特定頁面參數存在 Path Traversal 漏洞，遠端攻擊者不須權限，即可利用此漏洞繞過身分認證機制，存取任意系統檔案。
解決方法	請與全景軟體聯繫提供修補方案
公開日期	2022-10-18
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6619-9b5a7-3.html

全景軟體 RAVA 憑證驗證系統網站 - Command Injection	
TVN / CVE ID	TVN-202209013 / CVE-2022-39057
CVSS	7.2 (High)
影響產品	全景軟體 RAVA 憑證驗證系統網站 v3
問題描述	RAVA 憑證驗證系統網站特定頁面欄位未對特殊參數作過濾，遠端攻擊者以管理者權限登入後，即可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令，並對系統進行任意操作或中斷服務。
解決方法	請與全景軟體聯繫提供修補方案
公開日期	2022-10-18
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6618-11fd8-3.html

一等一科技 U-Office Force - Path Traversal -1	
TVN / CVE ID	TVN-202210002 / CVE-2022-39022
CVSS	6.5 (Medium)
影響產品	一等一科技 U-Office Force 20.50.7821D Build:202104sp1
問題描述	U-Office Force 下載暫存檔案功能之參數存在 Path Traversal 漏洞，遠端攻擊者以一般使用者權限登入後，即可利用此漏洞繞過身分認證機制，下載任意系統檔案。
解決方法	Update U-Office Force version to 23.0
公開日期	2022-10-26
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6637-eed19-3.html**

第 6 章、 2022 年 10 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。

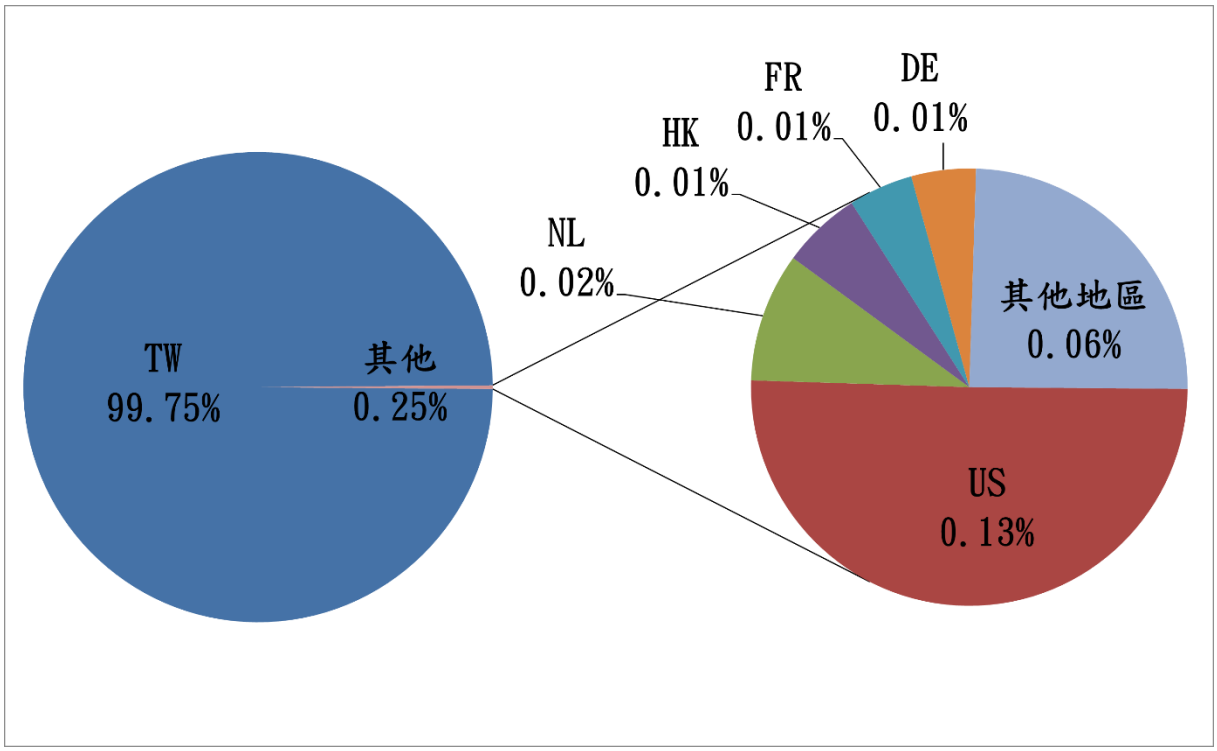


圖 1、分享地區統計圖

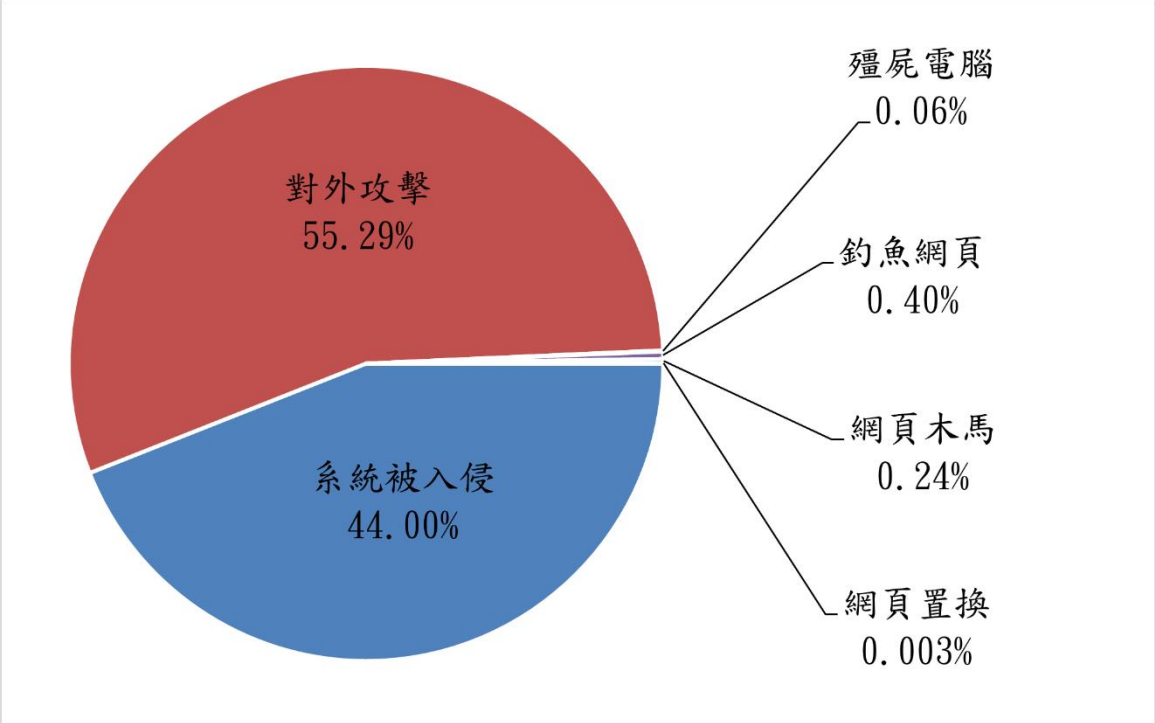


圖 2、分享類型統計圖

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 11 月 10 日**

編輯：**TWCERT/CC 團隊**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw**

痞客邦：**http://twcert.pixnet.net/blog**

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

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

Twitter：**@TWCERTCC**