



TWCERT/CC 資安情資電子報

2022 年 6 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、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養。
- 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、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
遠距辦公的資安威脅與防護	1
第 2 章、 資安小知識	10
線上資訊安全教育訓練課程彙整	10
第 3 章、 國內外重要資安事件	13
3.1、 資安趨勢	13
資安廠商發表 2022 年財星 1000 大公司資安調查報告，觀測到 6.87 億次員工登入 與個資遭竊事件	13
3.2、 新興應用資安	15
3.2.1、 多個 NFT 平台上的創作者遭釣魚惡意軟體攻擊	15
3.2.2、 偽造的 Pixelmon NFT 網站，會植入密碼竊取惡意軟體	17
3.2.3、 駭侵者利用 Deep Fake 深偽技術偽造 Elon Musk 等名人談話，進行加密 貨幣詐騙	19
3.2.4、 加密貨幣詐騙者假冒 Elon Musk 等名人，舉辦線上灑幣詐騙活動	21
3.3、 國際政府組織資安資訊	23
3.3.1、 哥斯大黎加遭 Conti 勒贖攻擊，全國進入緊急狀態	23
3.3.2、 西班牙警方破獲銀行帳戶釣魚駭侵集團	25
3.4、 社群媒體資安近況	27
新一波釣魚攻擊，鎖定官方認證 Twitter 帳號	27
3.5、 行動裝置資安訊息	29
3.5.1、 Google 警告 Predator 間諜惡意軟體，利用多個 0-day 漏洞感染 Android 裝置	29
3.5.2、 新版 Android 惡意軟體 ERMAC 2.0 藏身 467 種 App 內，竊取帳密與加 密錢包資金	31
3.6、 軟體系統資安議題	33
3.6.1、 美國資安主管機關呼籲，網域控制器暫勿安裝 Microsoft 五月資安更新	33
3.6.2、 新種 Linux 勒贖軟體 Cheers，鎖定 VMware ESXi 伺服器發動攻擊	35

3.6.3、	美國農機製造大廠 AGCO 遭勒索攻擊，部分生產線運作受阻.....	37
3.6.4、	德國汽車製造相關產業，遭長期釣魚攻擊.....	39
3.6.5、	美國通用汽車顧客發生個人資料遭竊事件，約 5,000 人個資外洩.....	41
3.7、	軟硬體漏洞資訊.....	43
3.7.1、	TP-Link AC1750 路由器存有遠端執行任意程式碼漏洞，建議立即更新.....	43
3.7.2、	Google 修復一個已遭大規模用於攻擊的 Android 核心漏洞.....	45
3.7.3、	Mozilla 修復於 Pwn2Own 大賽中遭發現的 Firefox、Thunderbird 0-day 漏洞.....	47
3.7.4、	Microsoft 推出 2022 年 5 月 Patch Tuesday 資安更新修補包.....	49
第 4 章、	資安研討會及活動.....	51
第 5 章、	2022 年 5 月份資安情資分享概況.....	57

第 1 章、封面故事

遠距辦公的資安威脅與防護



遠距辦公的資安 威脅與防護

TWCERT/CC

- COVID-19 疫情迫使企業必須考慮遠距辦公，遠距辦公的工作區域可能在家中或任何可透過遠距連線完成工作的地點，辦公設備則包括員工自有和企業配發的公有設備。
- 遠距辦公增加了資安的潛在風險，一旦遭受惡意攻擊，行動裝置可能成為跳板，或感染惡意軟體，進而影響內部系統，甚至可能因某些人為因素導致機敏資料外洩。
- 國內遠距辦公的使用情境與議題，從企業組織的資訊系統角度探討，可分為「事務型應用系統」及「內部應用系統」兩大類別，如何因應並制定政策則因產業別有所差異。
- 在保險、證券金融業皆有相關公會或組織進行規範的制定，而科技業則因其核心商業機密而有個別更為嚴格的防護機制。
- 隨著網路威脅不斷變化，資訊部門應意識到遠距辦公的存取策略，須隨著新風險的產生而進行調整，才能在遠距辦公環境中保持資料的安全。
- 在資安防護上則從政策制度、設備管理、資料保護、網路管理等方面探討，不僅應訂定完整的遠距辦公政策，還應獲得組織內各階層的理解與支持，隨時讓員工了解掌握，方能提升制度規範的落實。

一、簡介

COVID-19 疫情迫使企業必須考慮遠距辦公的工作情境，遠距辦公的工作區域可能在家中或任何可透過遠距連線完成工作的地點，辦公設備則包括員工自有和企業配發的公有設備。

據國內機構調查指出，美國民眾遠距辦公比例 57%，而我國因應疫情遠距辦公的企業比例為 41%。許多企業雖因疫情關係不得不採用遠距辦公，但實施後對企業帶來的正面效益，反而讓企業提高了持續推動的意願。

正因為遠距辦公已是時勢所趨，許多資安議題因應而生，不得不提高警覺，進而採行防範措施。遠距辦公除了設備與工作場域的差別外，其作業模式也呈現多樣化，例如僅是遠距線上會議，或是可遠端存取企業行政系統，甚或涉及機敏性資料等。遠距辦公的實施程度，亦取決於企業數位化的程度，現今的企業在數位化的推動上多數已有著墨，但在資安的面向上，遠距辦公的衝擊更是強烈，也是遠距辦公在執行上所必須重視的環節。

二、遠距辦公潛在的資安問題

通常辦公室會有實體門禁、防火牆、入侵偵測、資料外洩防護等資安防護措施，一旦實施遠距辦公，員工透過 VPN 或其他方式連線至企業組織內部存取資源，則有相當程度的管理問題需要考量：

- 大量且密集的 VPN 加密傳輸連線需求，對既有網路設備造成巨大負荷。
- 多樣性的遠距工作環境與設備，讓管理監控機制難以應付。
- 原有的工作流程不適用於遠距辦公情境。
- 臨時開放的系統功能，需要補強授權存取控制機制。
- 設備攜出在外，難免遺失或遭竊。

就資安角度而言，設備用於遠距辦公比在辦公室內使用，更具資安風險。潛在的資安風險略述如下：

- 惡意攻擊入侵：當企業組織開放遠距辦公時，一旦員工的行動裝置遭

遇惡意入侵，駭客很容易以該設備作為跳板，進而危害到公司內部網路的安全。

- 惡意軟體是遠距辦公面臨的一個重大威脅，當員工透過脆弱的遠距辦公設備與企業組織內部或外部廠商通訊時，可能導致惡意軟體向外擴散，從而加劇網路攻擊的嚴重後果。

- 機敏資料外洩：

- 當遠距辦公設備遭惡意入侵後，駭客可透過惡意軟體在公司內部網路尋找機敏資料，可能導致大規模資料外洩。
- 在 COVID-19 疫情期間，由於遠距辦公的開放，使企業組織比以往任何時候都更需要保護機敏資料。當員工離開防護嚴謹的辦公環境後，一旦缺乏安全意識，很容易洩漏公司內部敏感資訊。
- 由於員工疏忽導致遠距辦公設備丟失或被盜、不當使用設備(如使用弱密碼、透過不安全的無線網路熱點上網)等，也是導致企業組織機敏資料外洩的原因之一。

當企業組織難以監控遠距辦公設備的使用情況，以及未能掌握設備是否遵守企業組織政策與使用規範，開放遠距辦公就成了企業組織面臨的資安難題。

三、國內企業的情境與議題

探討國內企業遠距辦公的資安議題，要從企業組織的資訊系統角度進行，這些資訊系統可分為「事務型應用系統」及「內部應用系統」兩大類別，說明如下：

- 事務型應用系統：為一般辦公聯繫作業所需的應用系統，如電子郵件、行

事曆、通訊錄等；

- 內部應用系統：企業組織營運所需的重要系統，如 ERP 企業資源規劃系統、CRM 客戶關係管理系統、採購及付款系統、支付清算系統、研發資料庫、生產系統、薪資系統等含有機敏資料的系統。

為方便員工日常聯繫溝通使用，大部分企業會允許遠距辦公裝置存取事務型應用系統。然而對於涉及敏感資訊的內部應用系統，則禁止遠距辦公裝置存取，或另訂相關的系統存取管控政策，例如：需要事先申請，並透過帳號密碼、存取權限設定、開放使用的時間或時段、記錄系統存取稽核日誌等方法嚴格控管。

遠距辦公開放與否和企業組織的產業特性十分相關。許多物流運輸業允許員工使用行動設備，透過公司開發的 Apps 提供客戶服務，提升員工工作效率。保險公司、房仲業等因業務性質需要即時回應客戶，大多允許員工、業務代理人或經紀人除公配辦公設備外，也可以使用個人設備處理公務。

目前國內部分產業已有員工自備設備使用規範，這些規範與其處理態度，可做為遠距辦公實施策略參考，舉例如下：

金融保險相關產業

我國產物保險商業同業公會所制定的「財產保險業辦理資訊安全防護自律規範」，其第五條就規定各會員公司應訂定使用行動裝置(含 BYOD)之相關規範，並且應至少每年檢視一次，內容至少包含下列項目：

- 行動裝置管理。
- 行動裝置使用人員管理。
- 行動裝置之安全控管。
 - 使用者必須透過事先申請審核後，行動裝置始可連接公司內部網路。
 - 應訂定行動裝置連網安全規範。
 - 針對客戶或敏感資料應建置加密存取管制。

- 使用行動裝置時須遵守公司相關規範。
- 應訂定遺失處理程序。

科技業

視營業祕密為核心競爭力的高科技業者，需要穩定與安全可控的工作環境。平時就已嚴格控管辦公設備，在考量遠距辦公的多樣性和複雜性後往往轉趨保守，但迫於疫情仍需實施遠距辦公，其做法更為嚴謹，概略如下：

- 開發特殊規格的行動設備供員工使用，這些設備通常已把可能會妨害企業組織營業機密的功能拿掉，包括攝影鏡頭、錄音功能、無法任意安裝 Apps 等，僅剩下撥電話及發簡訊等必要功能，並且加入防護與監控機制。
- 對於員工日常的出入口則安裝金屬探測門，以防止員工或訪客攜帶未事先申報的智慧型手機、隨身碟、筆記型電腦等設備進入或離開廠區。

另一方面，一些較開放的高科技業者則允許員工的遠距辦公設備，可以存取特定系統或網域。為了防止商業機密外洩，業者會嚴格監控設備的使用軌跡，並對監控過程留下的證據，如使用日誌嚴加保存，以利事後調查分析。

在 Covid-19 疫情影響下，無論是遠端上班、分流上班或是分區上班，員工對行動設備的使用有更大的需求，遠距辦公的非常時期必須對公司的資安政策進行調整修訂，以便讓員工在家辦公的同時，兼顧資安與營運需求的平衡。

四、資安防護機制

由於開放遠距辦公可能導致的各種資安問題，建議企業組織可從以下各個管理層面進行檢視與調整，以減輕遠距辦公所帶來的風險：

政策制度面

- 訂定完整的遠距辦公政策，並取得組織內各階層的理解與支持。

- 隨著網路威脅不斷變化，資訊部門應意識到遠距辦公的存取策略須隨著新風險的產生而進行調整，才能在遠距辦公環境中保持資料的安全。
- 提供遠距辦公設備相關安全意識之培訓，包括遠距辦公設備的資安風險，以及設備遺失或遭竊時即時通報流程與程序。
- 明確讓員工知道資料安全對企業組織的重要性，一旦違反遠距辦公政策可能導致的風險及後果。

設備管理層面

- 除了每個遠距辦公設備都應被註冊及授權外，不管是員工自有或企業配發，企業組織還需要了解員工可以透過何種方式存取內部資料。此外，一旦員工離職應即時取消遠距辦公設備的存取權。
- 規定所有遠距辦公設備應安裝行動裝置管理程式，以便企業組織對可能妨害營業祕密的行動裝置功能進行管制。
- 企業組織也應對遠距辦公設備的應用程式進行管控，確保惡意軟體不會透過員工的遠距辦公設備竊取公司機密。
- 為員工提供身分識別與存取管理解決方案，通過強制使用多因子身分驗證，確保遠距辦公設備不會因為暫存密碼，而讓設備持有人可以輕易存取企業機敏資料。
- 規定連接內部網路或儲存公司機敏資料的遠距辦公設備應進行全機加密，防止設備遺失時資料被不法讀取。
- 此外強制遠距辦公設備使用防毒軟體、使用高強度密碼等措施，強制更新應用程式、並且密碼要符合公司規範，也是企業組織應考慮的最低標準。

資料安全

- 對內部伺服器的機敏資料進行加密，為不可避免的外洩做最好的準備。一旦資料離開伺服器，應確保資料處於被加密的狀態。
- 將應用程式及機敏資料只儲存在安全的服務器而不是遠距辦公設備上，一旦發生遠距辦公設備遺失或遭竊，可降低資料外洩的風險。
- 為員工提供最小的存取權限，降低資料外洩的風險，並為日後必要的調查限縮資料分析範圍。
- 讓資料在存取、編輯、儲存或共享等過程都可自動追蹤管理，使合規性變

得更容易。

網路管理

- 建議企業組織為網路設置不同安全區域，劃分為公共或訪客網路、辦公室網路及安全且受限的敏感網路，並將這些網路設置在安全且強大的防火牆設備後面，以限制不同安全區域對機敏資料的存取。
- 定期審查網路隔離政策及測試安全機制的有效性，以降低內外部威脅所帶來的風險。

遠距辦公資安防護機制以檢核表形式整理如下表，提供快速的依循參考。

表 1、遠距辦公資安防護機制表

面向	項目	建議內容
政策制度面	遠距辦公政策制定	制定遠距辦公流程、資安管理政策，以及員工權責規範
	遠距辦公設備管理	設備管理辦法，包括登記、遺失、註銷流程，並制定企業設備安全設定項目
	網路管理政策	因應前述政策的網路管理方法
	員工意識培訓	遠距辦公政策宣導、遠距辦公資安意識培訓
	政策定期審查	規劃政策落實度評量方法，並定期審查與調整政策內容
設備管理層面	遠距辦公設備盤點	建議盤點遠距辦公設備，做為設備管理的依據
	行動裝置管理(MDM)	登入功能、APP 應用管理等，進階功能如遠端鎖定、遠端清除
	身分識別與存取管理	建議使用多因子身分驗證
	防毒軟體或其它資安防護軟體	建議再加裝惡意軟體檢測工具
	安全設定	建議為強制安全設定，或以指引、稽核形式執行
網路管理層面	VPN 連線	應考量 VPN 伺服器之承載量，確保遠距連線穩定性
	身分識別與存取管理	建議使用多因子身分驗證
	安全區域劃分	可區分為公共、辦公、機敏等區域，使用不同層級的管理方式
	測試安全機制	除定期資安檢測外，應考量遠距辦公情境，納入檢測項目
資料安全層面	重要資料服務盤點	進行資料盤點，做為資料管理依據，進階可建立企業內容管理(ECM)機制
	資料加密	建議對遠端辦公設備進行全機加密，亦或依據資料盤點結果，加密機敏資料
	最小的存取權限	資料存取權限應依據最小權限原則進行規劃
	資料管理功能	重要資料存取應有系統日誌紀錄以供稽核，建議導入虛擬移動基礎設施(VMI)，使資料不需傳輸至終端操作

資料來源：本計畫整理

五、分析與建議

從實務面而言，訂定遠距辦公政策、制定各種規範相對容易，但要讓員工確實遵守這些政策及規範卻很困難，這對於缺乏遠距辦公經驗的企業組織來說尤其如此，因此，應加強員工教育及資安培訓。此外，設備的螢幕鎖定、啟用生物辨識功能、設備不應「越獄」或以其他方式破壞設備的原始狀態、軟體及應用程序應更新修補、只安裝信譽良好的可信賴軟體，及建立資安事故回應機制等，都是企業組織應採取的資安防護措施。

開放遠距辦公除了因應疫情影響以外，也為企業組織帶來了顯著的效益，包括提高生產力、吸引和留住人才以及降低營運成本。但是，只有在企業組織可以監控遠距辦公設備的使用狀況，以及員工確實遵守企業組織遠距辦公政策與使用規範的情況下，這些商業效益才會實現。擁有適當專業知識、領導力、政策和戰略的企業組織可享受遠距辦公所帶來的好處，惟前提是需要制定遠距辦公相關規範並採取積極作為，以便在員工使用便利性與安全監督機制之間取得平衡，維持企業組織既有的競爭優勢。

- 資料來源：

1. 關於遠端辦公，您需要了解的 7 件事
2. 2020 Personal Device Report：Bring Your Own Device
3. Cyber Threat Report on 2020 Shows Triple-Digit Increases across all Malware Types
4. The T-Mobile for Business 2020 Workplace Mobility Report
5. Mobile Device Security: Startling Statistics on Data Loss and Data Breaches
6. How Employees Engage with Company Cybersecurity Policies
7. 臺灣 BYOD 應用現況大調查

8. 財產保險業辦理資訊安全防護自律規範
9. 票券業辦理資訊安全防護自律規範
10. 中華民國證券商業同業公會雲端運算、社群媒體、行動裝置資訊安全自律規範
11. 疫情災難環境中，企業營運下的資安對策
12. 嚴重特殊傳染性肺炎

第 2 章、資安小知識

線上資訊安全教育訓練課程彙整



TWCERT/CC 彙整國內外相關資安防護教育訓練之網路資源，以協助企業提升資訊安全與資安知識，降低受駭風險。

1、[行政院國家資通安全會報技術服務中心－資安人才培訓服務網](#)：

網站課程內容針對政府機關資安人員以及資安訓練機構，依據資安職能評量制度，評測資安人員知識與技能。

- 政府機關資安人員職能訓練：針對公務人員所擔任之職務與負責任務，制定其執行業務時應具備之資訊安全知識與技能。依據不同職務與任務，規劃資安實務訓練課程、發展教材並建立資安能力之評量制度。
- 資安訓練機構認證制度：通過認證之機構可開設資安專業課程、代訓資安人員，擴大資安人才培育之能量

2、[中興大學－資通安全數位教育訓練課程](#)：

此訓練課程偏向公務教育訓練體系，一般企業仍可參考此課程進行相關訓練。

共分三大類型課程，每個類型各六個單元，民眾觀看完課程後可進行線上測驗，通過測驗者將獲得「資安課程數位教育訓練」2小時研習證明。三大類型課程內容簡介如下：

- 資安數位課程：學習如何透過資安管理與防護，避免網路世界的威脅
課程內容包含資安事件案例分析、ISO 27001 條文與控制項說明、教育體系資安與個資管理規範說明、資安實務說明、資訊安全稽核實務與問題改善與資訊安全技術檢測與修補
- 個資數位課程：學習如何藉由保護管理制度，達成法規遵循與隱私防護
課程內容包含個資事件案例分析、BS10012 & ISO 27701 條文與控制項說明、教育體系資安與個資管理規範說明、個資管理實務說明、個人資訊管理稽核實務與問題挑戰與個人工作流程應注意的個資管理。
- 資通安全管理法數位教育訓練：快速掌握資通安全管理法及了解因應之道
課程內容包含資通安全管理法條文架構及案例解釋、資通安全法準備重點、資通安全技術防護要求實作與檢核、資通安全事件通報及應變、委外管理注意事項與資通安全管理法稽核準備和改善報告。

3、[加拿大 CyberSecure Canada](#)：

為加拿大政府針對員工少於 500 人 (SMB) 的中小型企業和組織設計的免費網路課程，目標為以 20% 的負擔達到 80% 的網路安全保護效益。中小型企業和組織上完課程並通過評估後，即可獲 CyberSecure Canada 頒予為期兩年的網路安全認證。

該線上課程為互動式影片，共 12 個控制領域，每個領域課程大約 20 分鐘至 60 分鐘。12 個領域包含自動更新作業系統與應用程序、防毒軟體、安全地設置設備、基本邊界防護、存取控制與驗證、使用強使用者身分驗證、數據備份與加密、雲端與外包服務安全管理、行動通訊設備安全、可攜式多媒體安全、網站安全、資安事件應變計畫與員工資安教育訓練。

4、[英國 National Cyber Security Centre \(NCSC \)](#)：

該網站提供不同學齡層與背景相關教育訓練資訊。例如 CyberFirst 為針對英國 11 歲至 17 歲青少年所設計的線上資安課程，為青少年提供探索資訊安全的機會；Higher education 提供網路安全相關領域之學碩士學位認證課程資訊；除了學程之外，該網站亦提供 NCSC 付費認證課程，部分課程為線上課程。

5、[美國 Cyber Security & Infrastructure Security Agency\(CISA\)](#)：

該課程針對不同從業人員提供相關線上免費課程。企業可選擇網路安全專業人員(Cybersecurity Professionals (Non-Federal))課程與通用(General Public)課程，網路安全專業人員課程內容包含黑客道德、資訊安全經理人認證、資安系統專家認證等主題；通用課程則包含網路供應鏈風險管理、網路基礎知識以及基本網路安全管理等主題。

第 3 章、國內外重要資安事件

3.1、資安趨勢

資安廠商發表 2022 年財星 1000 大公司資安調查報告，觀測到 6.87 億次員工登入與個資遭竊事件



資安廠商發表「2022 年財星 1000 大公司個資外洩報告」；報告指出去年共觀測到高達 6.87 億次財星 1000 大公司員工登入資訊與個資遭竊事件。

資安廠商 SpyCloud 近日發表「2022 年財星 1000 大公司個資外洩報告」（2022 SpyCloud Fortune 1000 Identity Exposure Report）；報告指出去年共觀測到高達 6.87 億次財星 1000 大公司員工登入資訊與個資遭竊事件，較 2021 年增加多達 26%。

在這些資料竊取案件中，有 64% 的員工在不同服務重覆使用相同、易記易破解的密碼；另外各種裝置遭惡意軟體植入的比例也突破過去記錄。

該報告也指出，在觀測對象的財星 1000 大企業被駭記錄中，發現有超過 70,000 名員工的相關機敏資訊；這些員工很可能是因為使用了遭到惡意軟體植入的裝置，導致即使使用複雜密碼與多重登入驗證，仍無法避免資料遭竊。

報告說，被竊取的資料，以登入密碼、系統資訊、瀏覽器足跡、網頁工作階段 cookie 為主；一年間共觀測到超過 2,900 萬台受惡意軟體感染的個人使用裝置，用以登入財星 1000 大公司的外部網站，造成更多個資與登入資訊

遭竊。

報告也指出許多公司的資訊架構與駭侵防範能力相當薄弱，包括航太、國防、化學、製造業與能源產業等，有許多公司將公司名稱設定為登入密碼的前三到五碼。

而在財星 1000 大公司中，針對科技產業的駭侵活動最為嚴重，占總量的 21%；個資竊取攻擊事件高達 2,600 萬件，被竊的機敏資訊筆數高達 1.39 億筆；在所有財星 1000 大公司中，科技業員工的個人裝置遭植入惡意軟體的數量也最多，共 2,060 萬台，占比高達 70%。建議企業應加強資安防護能力與資安維護準則，員工應注意避免以個人裝置連入企業內部網路。

- 資料來源：

1. 2022 Fortune 1000 Identity Exposure Report
2. SpyCloud Report: Fortune 1000 Employees Pose Elevated Cyber Risk to Companies

3.2、新興應用資安

3.2.1、多個 NFT 平台上的創作者遭釣魚惡意軟體攻擊



資安廠商發表研究報告，發現包括 Pixiv、DeviantArt 等多個非同質性代幣平台上的創作者，最近紛紛接到詐騙釣魚訊息。

資安廠商 Malwarebytes 日前發表研究報告，指出該公司旗下資安專家，近來發現包括 Pixiv、DeviantArt 等多個非同質性代幣 (Non-Fungible Token, NFT) 平台上的創作者，最近紛紛接到詐騙釣魚訊息；該訊息謊稱可提供 NFT 創作者高薪工作機會，誘騙受害者下載並執行惡意軟體，以竊取受害者電腦中的機敏資訊。

據 Malwarebytes 報告指出，這些 NFT 平台上的受害者，最近收到一個自稱為 Cyberpunk Ape Executives NFT 專案，實為駭侵者冒名發出的訊息，指稱該專案需要新的 NFT 作品，以擴大專案規模，現以高薪邀請 NFT 創作者加入該專案，日薪可高達 200 美元至 350 美元。

該訊息中還包括一個連結，駭侵者宣稱該連結是內含 Cyberpunk Ape Executives NFT 專案的現有作品集壓縮檔；駭侵者並要求想參加專案的人，都要下載回去參考。

許多收到訊息的 NFT 創作者不疑有他，點按連結後就會連到一個 Mega 檔案分享空間，並且下載一個由密碼鎖定的 RAR 檔；解壓後確實會出現許多 NFT.gif 圖檔，但在中間夾有一個圖示看似也是 NFT，實則為惡意軟體的 .exe 檔案。

一旦受害者不慎開啟了該惡意軟體執行檔，其 Windows 系統就會被植入一個資訊竊取木馬；竊取的資訊包括各種帳號登入資訊、加密貨幣錢包資訊、信用卡資訊，甚至是電腦中存放的檔案。這將可能導致受害者加密貨幣錢包內的資產遭竊，甚至尚未公開的作品也可能落入駭侵者之手。

- 資料來源：
 1. Fake Cyberpunk Ape Executives target artists with malware-laden job offer
 2. Pixiv, DeviantArt artists hit by NFT job offers pushing malware

3.2.2、偽造的 Pixelmon NFT 網站，會植入密碼竊取惡意軟體



MalwareHunterTeam 發現偽造的 Pixelmon NFT 網站，以投放免費加密貨幣與 NFT 收藏品為餌，誘使用戶連入後，再植入會竊取用戶密碼的惡意軟體。

資安團體 MalwareHunterTeam 近來發現有一個偽造的 Pixelmon NFT 網站，以投放免費加密貨幣與 NFT 收藏品為餌，誘使用戶連入後，再植入會竊取用戶密碼的惡意軟體，以竊取用戶加密貨幣錢包中的資產。

Pixelmon 是一個相當受到歡迎的 NFT 專案，其開發目標是要創造一個多人共同使用的線上 metaverse 遊戲，玩家可在內收集、訓練 Pixelmon 寵物，並且與其他玩家對戰。

該專案的 Twitter 追蹤者有 20 萬人以上，Discord 頻道也有 25,000 位以上社群成員，因此有相當多的相關用戶。

目前身分仍然不明的駭侵者，基本上複製了 Pixelmon 的網站，架設另一個幾可亂真的詐騙網站，並且提供遊戲下載連結；但用戶下載到的可執行檔，內部含有惡意軟體 PowerShell 指令碼；用戶執行該指令碼後，就會從駭侵者架設的詐騙網站內，下載一個叫做 system32.hta 的檔案，接著會在用戶的系統上安裝一個 Vidar 惡意軟體。

Vidar 在執行後，又會連到一個 Telegram 頻道；Vidar 會自此頻道取得惡意軟體指令與控制伺服器網址，接著進一步下載更多惡意軟體模組，用來竊取受害裝置上的資訊，包括受害者電腦上的加密貨幣錢包登入帳密。

建議用戶收到任何號稱提供高額贈品或獎金的網站連結時，應先多加確認該網址確實是官方網址，勿直接點按連入；下載任何軟體安裝之前，也應先透過防毒防駭軟體掃瞄無異常，才進行安裝。

- 資料來源：

1. MalwareHunterTeam @malwrhunterteam
2. Fake Pixelmon NFT site infects you with password-stealing malware

3.2.3、駭客用 Deep Fake 偽造 Elon Musk 等名人談話，進行加密貨幣詐騙



近來發現有加密貨幣詐騙者，以 Deep Fake 深偽技術偽造多位名人談話的影片，以高利收益騙取受害者的加密貨幣存款。

遭到駭侵者利用深偽技術偽裝的名人，包括 Tesla、SpaceX 執行長 Elon Musk、方舟基金投資長 Cathie Wood、瑞波幣（Ripple Labs）執行長 Brad Garlinghouse、MicroStrategy 創辦人 Michael Saylor、Cardano 區塊鏈發明人 Charles Hoskinson 等。

駭侵者設立一個詐騙專用的加密貨幣交易平台 BitVex，號稱該平台為 Elon Musk 所擁有；並利用上述名人的 deep fake 影片，以高達 30% 的質押利率，誘騙受害者將其加密貨幣資產存入該詐騙平台的錢包位址。

所有用來詐騙的影片，原本都是真實的訪問錄影，但遭到駭侵者利用 deep fake 技術變造內容；例如在一段 TED 訪問影片中，遭到 deep fake 變造的假 Elon Musk 宣稱自己在該加密貨幣平台已投資 5 億美元。

目前尚未釐清駭侵者的真實身分；不過駭侵者係利用自己註冊或盜取來的 YouTube 帳號來散布這些假影片，並且要求用戶以比特幣、比特幣現金、以太幣、泰達幣、狗狗幣、Polkadot 等幣種質押。目前為止觀察到的詐騙所得並不多，僅約 1,700 美元左右。

建議若投資加密貨幣，請務必使用信譽卓著，設有投資人保護基金，資安防護也較完善的大型交易所；切勿貪圖高利，誤信社群平台上詐騙帳號發布的假消息，以免資金遭竊。

- 資料來源：
 1. Deep fake video of Elon Musk promoting crypto scam
 2. Elon Musk deep fakes promote new cryptocurrency scam

3.2.4、加密貨幣詐騙者假冒 Elon Musk 等名人，舉辦線上灑幣詐騙活動



加密貨幣詐騙者在 YouTube 上假冒多位科技界與投資界名人，多次舉辦灑幣詐騙直播大會，一共騙得超過 130 萬美元的加密貨幣。

身分不明的加密貨幣詐騙者，日前在 YouTube 上假冒 Tesla 執行長暨 SpaceX 創辦人 Elon Musk、Twitter 創辦人暨前執行長 Jack Dorsey、Ark Investment 創辦人暨投資總裁 Cathie Wood 等科技界與投資界名人，多次舉辦灑幣詐騙直播大會，一共騙得超過 130 萬美元的加密貨幣。

這種詐騙手段是由詐騙者假冒名人，在 Twitter、Facebook、YouTube 等社群平台上貼文或開直播，宣稱為慶祝某些事件，特別舉辦大灑幣活動；用戶只要將某個額度的加密貨幣匯入指定錢包位址，就會收到兩倍甚至更多的獎金。

雖然這種詐騙方式稍有經驗的人不會輕信，但每次有詐騙分子使用這種方式，就會有多人上當。

資安廠商 McAfee 的專家指出，以這次的事件來說，該公司觀察到詐騙者先架設了 11 個假冒上述名人的詐騙灑幣活動網站，後來還增加到 26 個；他們也在 YouTube 上動用 10 個左右的頻道，來進行詐騙直播；在之前一場詐騙直播中，僅僅 7 個小時，騙得的加密貨幣市值就高達 40 萬美元以上。

詐騙者為了取信直播觀眾，還在詐騙網站中建置一個表格，表格內的數字以 JavaScript 填入隨機數字，不明就裡的觀眾看起來，就像是真的有人在匯入若干金額的加密貨幣後，立即獲得加倍的獎金。

資安專家也指出，這些播放詐騙直播的 YouTube 頻道，訂閱數量都很龐大，達數萬人到一百萬人以上；專家指出，這麼多訂閱者，可能是駭侵者以灌人頭的方式撐出來，或是利用如釣魚方式，竊自其他訂閱人數眾多的 YouTuber。

- 資料來源：

1. Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency
2. Fake crypto giveaways steal millions using Elon Musk Ark Invest video

3.3、國際政府組織資安資訊

3.3.1、哥斯大黎加遭 Conti 勒索攻擊，全國進入緊急狀態



哥斯大黎加政府旗下多個機關，日前紛紛遭到 Conti 勒索軟體的駭侵攻擊，造成該國政務運作受到嚴重影響；該國總統已宣布全國進入緊急狀態。

全國進入緊急狀態的命令，是在本（2022）年 5 月 8 日由哥斯大黎加總統 Rodrigo Chaves 在就任首日簽署；他是位經濟學家，曾任哥國財政部長。

資安專家指出，近日觀察到 Conti 勒索團體對外公開屬於該國政府各部門的一批竊得資料，檔案大小合計達 672 GB。

Conti 勒索團體曾在上個月時宣稱，要針對哥斯大黎加政府各單位發動勒索攻擊，並要求一千萬美元的巨額贖金；該國的社會安全基金 Costa Rican Social Security Fund（CCSS）先前也曾公告，將加強對 Conti 勒索攻擊的防禦能力。

資安專業媒體 BleepingComputer 旗下的資安專家，則在日前觀察到上述合計多達 672 GB 外洩資料的一部分內容，其中已有 97% 的內容遭到 Conti 勒索團體公開。

在這次攻擊事件中，主要的攻擊對象為哥斯大黎加財政部；目前該國尚無法釐清攻擊事件的受害程度，只知道受害的部分包括納稅人資訊、出納、海關等系統。

目前哥斯大黎加政府公開的資訊中，被攻擊而受到影響的政府單位，除了哥國財政部外，還包括勞工與社會安全部（Ministry of Labor and Social Security, MLSS）、社會發展與家庭補助基金（Social Development and Family Allowances Fund, FODESAF）、Alajuela 跨大專院校聯合辦公室等（Interuniversity Headquarters of Alajuela, SIUA）等。

- 資料來源：

1. CCSSdeCostaRica @CCSSdeCostaRica
2. BetterCyber @_bettercyber_
3. Costa Rica declares national emergency after Conti ransomware attacks

3.3.2、西班牙警方破獲銀行帳戶釣魚駭侵集團



西班牙警方日前發表新聞稿，宣布破獲一個專門透過釣魚攻擊，以竊取受害者銀行登入資訊的駭侵團體。

西班牙警方日前發表新聞稿，宣布破獲一個專門透過釣魚攻擊，以竊取受害者銀行登入資訊的駭侵團體；警方表示除了繼續追查本案之外，同時也正在加緊追緝在逃嫌犯。

遭到逮捕的駭侵團體，主要犯行是透過釣魚電子郵件來欺騙受害者，讓受害者收到偽造的銀行通知信，並且連到假網站進行登入手續，藉以竊取受害者登入網路銀行所使用的登入資訊。

一旦取得受害者的銀行登入資訊，駭侵者便會立即登入該帳戶，將登錄在銀行端的手機門號，變更為由駭侵者控制的手機門號，以便接收二階段登入簡訊驗證碼，同時更改密碼，讓原用戶無法再次存取自己的帳戶；接著便會利用不法所得進行網路購物、直接轉帳到人頭帳戶內，或是用以申請個人信貸，取得更多不法所得。

據西班牙警方表示，針對這個駭侵團體的調查，是由 2018 年警方開始接獲報案起，自 2019 年 1 月到今 (2022) 年 4 月，共分成數波行動；截至目前為止一共逮捕 17 名駭侵攻擊分子，另外有 7 名嫌犯仍然在逃。

西班牙警方說，這個駭侵團體在作案時，大量使用各種不同的 VPN 服務，因此看起來像是自摩洛哥、法國、德國、美國等境外地區犯案；報案受害者的銀行存款，最常被用來進行跨國網購，特別是自法國電商購買。

建議收到這類釣魚郵件時，切勿直接點按信中按鈕，或下載執行信中附寄的任何檔案。應先檢視郵件寄送者詳細資訊，如非銀行官方網域信箱所寄，應特別提高警覺；即使是由銀行官方信箱，也應透過官方客服電話確認信件內容為真。如果發現是釣魚信件，應立即歸入垃圾信件匣，或是向相關單位檢舉，並通報銀行處理。

- 資料來源：

1. La Policía Nacional desarticula una organización que estafó a 146 víctimas en todo el territorio nacional
2. Spanish police dismantle phishing gang that emptied bank accounts

3.4、社群媒體資安近況

新一波釣魚攻擊，鎖定官方認證 Twitter 帳號



資安專業媒體 BleepingComputer 指出，近來該媒體旗下多位記者與作者獲得 Twitter「官方認證」的帳號，都遭到釣魚信件攻擊。

資安專業媒體 BleepingComputer 發表專文指出，近來該媒體旗下多位記者與作者獲得 Twitter「官方認證」的帳號，都遭到釣魚信件攻擊；信件內容意圖誘騙帳號擁有者輸入登入資訊，進而竊得帳號控制權。

Twitter 的官方帳號認證，是針對知名人士、政治人物、記者、作家、明星、社會運動者、政府單位、知名品牌、中大型私人企業等追蹤者眾多，對社群用戶具有實質影響力的帳號而設計；Twitter 會審核該帳號擁有者的身分是否屬實，通過認證者會在其帳號顯示名稱旁邊，額外顯示一個藍色勾勾圖標，讓用戶清楚分辨帳號為真，也降低有心人另設帳號加以仿冒的風險。

由於官方認證過的帳號取得不易，又具有一定程度以上的公信力，且擁有眾多追蹤者，影響力宏大，因此成為歷來社群平台資安攻擊中的主要目標。一旦這類帳號遭竊，駭侵者就能進一步針對其龐大追蹤受眾發動大規模攻擊，例如散播假訊息或惡意連結，甚至進行金融詐騙攻擊。

BleepingComputer 指出，自上周起，該刊旗下多名擁有官方認證 Twitter 帳號的記者與作者，紛紛收到一封釣魚信件；信件內容指出其 Twitter 官方帳號認證發生問題，要求用戶點按信中連結檢查認證狀態，否則其帳號可能遭到停權。

用戶若點按該釣魚連結，就會連入一個非 Twitter.com 網域的釣魚網站，要求用戶輸入帳號與密碼，接著駭侵者會用取得的密碼，至 Twitter 進行密碼重置作業；如果用戶設有二階段登入驗證，Twitter 會以簡訊發送二階段驗證碼，假網站又會接著要求用戶輸入驗證碼，進而完全取得該帳號的控制權。

據報導指出，已有獲認證的記者因誤信透過私訊傳來的該釣魚連結，造成帳號被盜；竊盜者立即更改其個人簡介與頭像，並且透過該帳號的私訊來進一步發送釣魚訊息。

- 資料來源：

1. New phishing warns: Your verified Twitter account may be at risk
2. WUDAN YAN @wudanyan

3.5、行動裝置資安訊息

3.5.1、Google 警告 Predator 間諜惡意軟體，利用多個 0-day 漏洞感染 Android 裝置



Google 旗下資安團隊 Threat Analysis Group，日前發現有駭侵團體在受害者手機中植入一種名為 **Predator 間諜惡意軟體**。

Google 旗下資安團隊 Threat Analysis Group (TAG)，日前發現有駭侵團體利用 5 種不同的 0-day 漏洞發動資安攻擊，在受害者手機中植入一種名為 Predator 間諜惡意軟體。

Predator 間諜軟體是由商業監控軟體公司 Cytrox 所開發的。Google 的資安專家發現近來至少有三波相關攻擊活動，發生時間介於 2021 年 8 月到 10 月間，駭侵團體利用 5 個 0-day 資安漏洞，攻擊最新版本的 Android 裝置。

Google TAG 團隊指出，遭到利用的 5 個 0-day 漏洞如下：

- CVE-2021-37973、CVE-2021-37976、CVE-2021-38000、CVE-2021-38003，這四個漏洞在於 Google Chrome 內。
- CVE-2021-1048 存於 Android 系統內。

目前觀察到的三波攻擊行動，都是利用以偽裝的短址服務，以 Email 寄送給目標攻擊對象的 Android 裝置；目前得知鎖定攻擊的對象人數僅有數十人，是高度鎖定特定目標的攻擊。

一旦攻擊目標對象點按了該惡意連結，就會先被導向到攻擊者擁有的網域，利用上述漏洞植入惡意軟體後，再導向到正常的網站。這種手法過去常被駭侵者用來攻擊特定目標，如記者、政治人物或反對運動者。

建議用戶不要點擊不明 Email、簡訊、通訊軟體傳送過來的短網址，因為短網址的內容難以觀察判斷是否為正常網址。

- 資料來源：
 1. Protecting Android users from 0-Day attacks
 2. Google: Predator spyware infected Android devices using zero-days

3.5.2、新版 Android 惡意軟體 ERMAC 2.0 藏身 467 種 App 內



ERMAC Android 金融木馬惡意軟體，近期對其「會員」推出 2.0 版，主要升級功能為加強對各種銀行與加密貨幣錢包的竊取能力。

一個名為 ERMAC 的 Android 金融木馬惡意軟體，近期對其「會員」推出 2.0 版，主要升級功能為加強對各種銀行與加密貨幣錢包的竊取能力；目前有 467 種 App 都遭發現內含此惡意軟體。

ERMAC 的主要功能，是在植入受害者的 Android 裝置後，竊取裝置中儲存的各種登入資訊，傳送到駭侵者處，以進一步控制受害者的金融帳戶與加密貨幣錢包，竊取資金或發動進一步的詐騙。

ERMAC 的運作模式，是在暗網上以「會員訂閱制」方式提供服務租用；上一版的 ERMAC 租金為 3,000 美元，藏身於 378 種不同的 Android App 中；新版的租用價格調漲到 5,000 美元，植入的 App 數量成長為 467 種。

資安廠商 ESET 指出，該公司旗下的資安專家，最近觀察到駭侵者透過一個假冒歐洲送餐業者 Bolt Food 的網站，來散在夾帶該惡意軟體的 App，主要攻擊對象為波蘭境內的用戶。用戶一旦在假網站上註冊，就會不斷收到各種含有惡意連結的 Email、社群平台貼文、廣告等等。

用戶如果下載安裝含有惡意軟體，該假冒 App 會要求用戶授予完全控制裝置的權限，所要求的權限多達 43 種，包括控制簡訊收發、取得通訊錄內容、產生系統警告通知畫面、錄音、完全存取裝置記憶體等。接著，該 App

就會以假冒的畫面覆疊，試圖騙取用戶輸入帳號密碼，並傳送到駭侵者的控制伺服器。

建議用戶切勿在非 Android 官方的 Google Play Store 之處下載安裝任何 apk 檔案，特別是無法判定真偽的任何網站。

- 資料來源：
 1. ESET research @ESETresearch
 2. Latest Version Of Android Banking Trojan Targets Over 400 Applications

3.6、軟體系統資安議題

3.6.1、美國資安主管機關呼籲，網域控制器暫勿安裝 Microsoft 五月資安更新



Microsoft 推出五月 Patch Tuesday 資安更新修補包，已經證實安裝於 Windows Server Domain Controller 網域控制器上時會發生相容性問題。

Microsoft 於日前推出的五月 Patch Tuesday 資安更新修補包，已經證實安裝於 Windows Server Domain Controller 網域控制器上時會發生相容性問題，因此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）提出警示，呼籲暫勿在網域控制器上安裝該更新。

出現相容問題的修補程式，是針對一個已遭外界駭客濫用於資安攻擊的 Windows LSA 詐騙 0-day 漏洞 CVE-2022-2692，該漏洞已確認是最近發的 PetitPotam Windows NTLM 中繼攻擊活動所使用的弱點；未經授權的攻擊者可藉由這個漏洞，強制透過 Windows NT LAN Manager 的資安協定，來取得 Domain Controller 給予權限，進而控制整個系統。

微軟雖然在 2022 年 5 月 Patch Tuesday 中針對此一漏洞予以修補，但後續傳出安裝了這次資安更新修補包的 Windows Server Domain Controller 發生服務驗證錯誤問題（service authentication problems），導致功能失常。

不過 CISA 也指出，這個問題只會出現在 Windows Server Domain Controller 上，一般人員使用的 Windows 裝置，以及非 Domain Controller 的

Windows Server 不會出現問題，所以還是應該安裝此更新。

建議 Windows Server Domain Controller 的系統管理者，應依照 Microsoft 提供的暫時解決方案，來處理 Domain Controller 無法正常運作的問題；其餘非 Domain Controller 的 Windows 裝置，均應安裝更新。

- 資料來源：

1. CISA Temporarily Removes CVE-2022-26925 from Known Exploited Vulnerability Catalog
2. KB5014754—Certificate-based authentication changes on Windows domain controllers

3.6.2、新種 Linux 勒索軟體 Cheers，鎖定 VMware ESXi 伺服器發動攻擊



資安廠商趨勢科技旗下的資安研究人員，發現一個名為 Cheers 的新型 Linux 變種勒索軟體，目前正在針對 VMware ESXi 伺服器發動攻擊。

資安廠商趨勢科技 (Trend Micro) 旗下的資安研究人員，近來發現一個名為 Cheers 的新型 Linux 變種勒索軟體，目前正在針對 VMware ESXi 伺服器發動攻擊；Trend Micro 將此變種稱為「Cheerscrypt」。

VMware ESXi 是一種虛擬化的運算平台，廣為全球各大企業採用；因此一旦 VMware ESXi 伺服器遭到勒索軟體加密鎖定，會造成許多企業運作受阻。

Trend Micro 在研究報告中指出，一旦某台 VMware ESXi 伺服器遭到 Cheerscrypt 的攻擊，駭侵者便會在虛擬機器中啟動加密工具，並且在執行完成後立即停止；伺服器上的各種重要虛擬機器檔案，包括磁碟映像檔、swap 檔案、分頁檔案等，都會遭到加密，並且加上 .Cheers 的副檔名，以及一個用來恐嚇受害者的文字檔，內有與駭侵者連絡並且支付贖款的 Tor 網址。

在恐嚇文件中，駭侵者要求受害者需在三天內，透過指定的不重覆 Tor 專屬網址，與駭侵者接洽解鎖與贖金，否則受害者的被竊資料，就會轉賣給有興趣的買方；若無人購買，資料就會遭到駭侵者公開。

據資安專家的觀測，Cheerscrypt 是從 2022 年 3 月起開始活動，且除了 Linux 版本外，也有針對 Windows 伺服器設計的 Windows 版本。

建議系統管理者應加強系統對資安攻擊的整體防護能力，同時建立完善的資料備份，以在系統不幸遭到攻擊時，能夠迅速復原。

- 資料來源：
 1. New Linux-Based Ransomware Cheerscrypt Targets ESXi Devices
 2. New 'Cheers' Linux ransomware targets VMware ESXi servers

3.6.3、美國農機製造大廠 AGCO 遭勒索攻擊，部分生產線運作受阻



美國農業機械機具製造廠商 AGCO，日前發表資安通報，表示該公司近日遭到不明來源的勒索駭侵攻擊，導致部分生產作業受到影響。

AGCO 在資安通報中說，該公司於今（2022）年 5 月 5 日時遭到勒索駭侵攻擊，導致部分生產作業受阻；該公司預計需要數日或更長的時間，才能修復受到影響的系統，並且重新安裝生產所需的各類軟體，讓全公司的 IT 系統恢復正常運作。

該公司在偵測到勒索攻擊事件後，將部分 IT 系統關閉，以避免攻擊造成的影響持續擴大。

目前該公司沒有對外透露駭侵事件相關細節，包括受損情形、勒索攻擊的類型、駭客的身分，以及要求的贖金等資訊；該公司僅表示已著手進行調查中，有進一步的消息可以對外說明時，將會提供更新的資安通報。

AGCO 是美國股市上市公司，旗下擁有多個知名農機品牌，如 Fendt、Massey Ferguson、Challenger、Gleaner、Valtra 等，集團員工人數達 21,000 人，年營業額超過 90 億美元。

專家指出，目前美國的糧食價格，因受俄烏戰爭、油價上漲、通貨膨脹等因素而顯著上漲；這波針對農機大廠的攻擊行動，如果造成農機製造、販賣與維修受阻而影響農業生產的話，可能會進一步推升美國的通貨膨脹。

美國聯邦調查局日前也發表過資安警訊，指出駭侵團體針對美國農業部門的勒索攻擊，在近來亦有升高的趨勢；光是在今（2022）年就發生過兩次重大的農業部門勒索事件。

- 資料來源：
 1. AGCO Announces Ransomware Attack
 2. Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons
 3. US agricultural machinery maker AGCO hit by ransomware attack

3.6.4、德國汽車製造相關產業，遭長期釣魚攻擊



Check Point 發表研究報告指出，近期發現德國汽車製造業與相關產業，長期以來遭到釣魚攻擊；駭侵者意圖透過釣魚信件誘使汽車廠員工遭駭。

資安廠商 Check Point 近日發表研究報告，指出該公司的資安專家，近期發現德國汽車製造業與相關產業，長期以來遭到釣魚攻擊；駭侵者意圖透過釣魚信件誘使汽車廠員工遭駭，藉機植入密碼竊取惡意軟體，以阻擾汽車生產線運作。

報告指出，該駭侵攻擊活動主要鎖定德國的大型車廠與旗下的經銷體系；駭侵者並且註冊了多個與這些德國汽車廠牌看來十分雷同的網域名稱，製作多個外觀看起來一模一樣的釣魚網站，用於進行釣魚攻擊；但主要用以放置惡意軟體的網站係架設在愛爾蘭。

Check Point 的報告說，駭侵者會精選目標受眾，並在釣魚電子郵件中附上收據與合約，以降低攻擊目標的戒心；信件中夾帶的 .ISO 檔號稱是交車收據，受害者點開後，實際掛載到系統上後會開啟一個 .HTA (HTML Application) 檔案。

該 .ISO 檔案運用一種未知的特別技術，可以跳過 NTFS 檔案系統內建 MOTW 資安防護措施，在執行 .HTA 檔案時，就能執行其中夾帶的 JavaScript 或 VBScript 指令檔。

Check Point 的追蹤結果顯示，觀測到的攻擊活動持續約一年左右，自 2021 年 7 月底到 2022 年 3 月間，且至少有 14 家德國汽車製造商與經銷商遭到攻擊；但該報告沒有明確指出是哪些廠家遭到攻擊。

- 建議措施：
 - 企業應加強不明來源郵件的過濾掃描。
 - 系統管理員應提升系統安全防護能力，並隨時保持系統更新到最新版本。
 - 員工與一般民眾，不應任意開啟 Email 中的連結；遇可疑郵件時，應先檢視寄件人網址是否完全正確。

- 資料來源：
 1. Info-stealer Campaign targets German Car Dealerships and Manufacturers
 2. German automakers targeted in year-long malware campaign

3.6.5、美國通用汽車顧客發生個人資料遭竊事件，約 5,000 人個資外洩



美國汽車製造商通用汽車，表示於 2022 年 4 月發生部分顧客個人資料遭竊事件。

美國汽車製造商通用汽車（General Motors），日前表示於上個月（2022 年 4 月）發生部分顧客個人資料遭竊事件，且有顧客累積的點數遭駭侵者盜用於兌換贈品。

通用汽車旗下擁有眾多品牌，包括雪佛蘭（Chevrolet）、別克（Buick）、GMC、凱迪拉克（Cadillac）等，由通用汽車總公司負責各子品牌的營運與客服工作。

據通用汽車寄發給相關受害顧客的 Email 中指出，該公司於 2022 年 4 月 11 日到 4 月 29 日間發生惡意登入事件，且有駭侵者利用顧客的點數兌換贈品。通用汽車承諾將補回所有遭到盜用的顧客點數。

這次通用汽車顧客被竊的資料欄位，包括姓名、個人 Email 地址、郵寄地址、隨同用戶帳號附加的家人姓名與電話號碼、個人檔案照片等。受害者約將近 5,000 人。

資安專家指出，這次個資外洩事件並非導因於通用汽車本身遭駭侵攻擊，而是駭侵者利用在別處取得的顧客登入資訊，在通用汽車的網站試圖登入，且登入成功所致。

由於許多用戶會在不同網站重覆使用同樣的登入資訊，駭侵者使用這些登入資訊，往往可以成功登入其他服務，並進行進一步的駭侵攻擊，例如挾

持帳號、盜領資金或竊取更多個資等。

針對此次個資外洩事件，通用汽車表示已重置所有顧客使用的密碼，並且針對個資確定被竊的用戶，提供額外的信用監控服務，以防止發生盜刷。不過通用汽車系統至今仍未支援二階段登入驗證。

建議用戶勿在不同服務之間使用同樣的帳號與密碼，且務必使用多階段登入驗證選項，避免駭侵者使用他處取得的個資與登入資訊，成功登入其他服務。

- 資料來源：

1. NOTICE OF DATA BREACH
2. General Motors credential stuffing attack exposes car owners info

3.7、軟硬體漏洞資訊

3.7.1、TP-Link AC1750 路由器存有遠端執行任意程式碼漏洞，建議立即更新



TP-Link AC1750
路由器存有遠端執行
任意程式碼漏洞，建議立即更新

TWCERT/CC

TP-Link AC1750 智慧型 Wi-Fi 無線路由器，在 2021 年美國德州 Austin 舉辦的 Pwn2Own 駭客大賽上，遭發現一個嚴重資安漏洞。

用戶相當多的知名網通品牌 TP-Link，旗下生產的 TP-Link AC1750 智慧型 Wi-Fi 無線路由器，在 2021 年美國德州 Austin 舉辦的 Pwn2Own 駭客大賽上，遭參賽的資安研究人員團隊 Overcl0k 發現一個嚴重資安漏洞；駭侵者可利用這個漏洞，取得受攻擊路由器的控制權，並且遠端執行任意程式碼。

在 Overcl0k 團隊共同維護的 GitHub 頁面中，該團隊把這個漏洞命名為 Zenith。據該 Overcl0k 的說明，這個 Zenith 漏洞存於 TP-Link AC1750 路由器，由 KCodes 公司開發的 NetUSB 驅動程式中。這段驅動程式會在 TCP 埠號 20005 上監聽 br-lan 介面。

Overcl0k 參賽人員發現該 NetUSB 驅動程式的 kmalloc-128 slab cache 中存有一個整數溢位漏洞；參賽人員利用此漏洞誘發錯誤，成功駭入 TP-Link AC1750，並且自外部 http 伺服器下載一個惡意軟體，藉以取得路由器管理者權限。

這個漏洞在提報之後，獲編為 CVE-2022-24354，其 CVSS 危險程度評分得分高達 8.8 分（滿分為 10 分），危險程度評級為「高」（high）等級。

2021 年的 Pwn2Own 駭客大賽舉辦於該年 11 月初，而在這個 CVE-2021-24354 漏洞發現後，研究人員將漏洞提報給原廠 TP-Link；該漏洞業已在今（2022）年 1 月時修復，更新版本名為「Archer C7(US)_V5_211210」，已可下載安裝。

- CVE 編號：CVE-2022-24354
- 解決方案：建議所有使用該型路由器的用戶，應立即更新韌體至最新版本，以修補此嚴重資安漏洞。

- 資料來源：
 1. Overclock / zenith
 2. Download for Archer C7 V5

3.7.2、Google 修復一個已遭大規模用於攻擊的 Android 核心漏洞



Google 宣布修復存於 Android 系統內 Linux 核心的權限提升漏洞 CVE-2021-22600。

Google 近日宣布修復一個存於 Android 系統內 Linux 核心的權限提升漏洞 CVE-2021-22600。目前得知該漏洞已遭駭侵者大規模用於攻擊，用戶請立即注意裝置可否更新。

這個 CVE-2021-22600 原本是存於 Linux 作業系統的核心，駭侵者可透過本地存取來誘發這個漏洞，提升自己的執行權限；該漏洞的 CVSS 危險程度評分高為 7.8 分（滿分為 10 分），危險程度評級為「高」（High）。

事實上，Google 的資安研究人員在今（2022）年 1 月，即在 Linux 核心中發現此一漏洞，並且向各個主要 Linux 散布版本（distribution）廠商提報修補方案。

Google 對於 CVE-2021-22600 這個漏洞的修補程式，是包括在 2022 年 5 月 5 日推出的 Android 第二波修補包內，而非在 5 月 1 日推出的 Android 第一波修補包之內。

據資安專家指出，目前已有情報指出該漏洞可能已遭駭侵者大規模用於攻擊活動，然而尚不清楚是哪些攻擊活動使用了這個漏洞，也缺少具體的攻擊行動損害報告；不過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）曾在 4 月時針對這個漏洞發布資安警訊，指出該漏洞已有大規模遭到濫用的情資。

值得注意的是，Google 雖然發表了資安修補程式，但僅適用於 Google 自己推出的 Pixel 品牌 Android 手機；其他廠商的 Android 裝置，需等到製造商推出韌體更新後才能得到更新，因此用戶必須密切注意原廠的系統更新訊息，在有更新可用時立即更新。

- CVE 編號：CVE-2021-22600
- 影響產品/版本：Android 作業系統 10、11、12（第 9 版與較舊版本不受影響，但過於老舊，應更新至最新版本，如無法更新應換機）。
- 解決方案：
Google Pixel：更新至最新版本韌體。
其他品牌 Android 裝置：等待原廠推出新版韌體時立即更新。
- 資料來源：
 1. Android 安全公告 - 2022 年 5 月
 2. Google fixes actively exploited Android kernel vulnerability

3.7.3、Mozilla 修復於 Pwn2Own 大賽中遭發現的 Firefox、Thunderbird 0-day 漏洞



Mozilla 推出資安更新，並修復兩個存於 Firefox、Thunderbird 中，在 Pwn2Own 資安大賽上被發現的 0-day 漏洞；用戶應立即更新至最新版本。

Mozilla 近日對旗下多種軟體產品推出資安更新，主要修復兩個存於 Firefox、Thunderbird 中，在今（2022）年於加拿大溫哥華舉辦的 Pwn2Own 資安大賽上被發現的 0-day 漏洞；用戶應立即更新至最新版本。

據報導指出，這兩個漏洞若遭到駭侵者用於攻擊，將可能導致駭侵者獲得在桌面或行動裝置上執行任意 JavaScript 的權限；受此漏洞影響的 Mozilla 旗下產品，包括 Firefox、Firefox ESR、Firefox for Android、Thunderbird 等。

第一個在 Pwn2Own 大會上發現的 0-day 漏洞 CVE-2022-1802，是一個在頂級等待實作上的原型污染漏洞（prototype pollution in Top-Level Await implementation），駭侵者可藉以在有此漏洞的平台上執行任意 JavaScript 程式碼。

另一個 0-day 漏洞則是藉用濫用 Java 物件索引，給予特定的不正確輸入驗證，同樣可透過原型污染注入攻擊手法，來控制 JavaScript 的執行緒。

Mozilla 在獲悉這兩個漏洞後，很快就在兩天後推出了更新版本；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）也在近日呼籲相關用戶更新此漏洞。

建議所有 Mozilla Firefox 與 Thunderbird 各版本用戶，應立即更新至最新版本，以避免駭侵者利用這兩個 0-day 漏洞發動攻擊。

- CVE 編號：CVE-2022-1802、CVE-2022-1529
- 影響產品/版本：Mozilla Firefox 100.0.2、Firefox ESR 91.9.1、Firefox for Android 100.3、Thunderbird 91.9.1 之前版本。
- 解決方案：更新至 Mozilla Firefox 100.0.2、Firefox ESR 91.9.1、Firefox for Android 100.3、Thunderbird 91.9.1 與後續版本。

- 資料來源：
 1. CVE-2022-1529: Untrusted input used in JavaScript object indexing, leading to prototype pollution
 2. Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own

3.7.4、Microsoft 推出 2022 年 5 月 Patch Tuesday 資安更新修補包



Microsoft 推出 5 月 Patch Tuesday 資安修補包，修復旗下產品多達 75 個各類資安漏洞，建議用戶應立即更新。

Microsoft 日前推出例行性的 2022 年 5 月 Patch Tuesday 資安修補包，一共修復旗下產品多達 75 個各類資安漏洞，其中有三個屬於 0-day 漏洞；Microsoft 各種軟體與系統產品用戶應立即更新。

在這次推出的資安修補包修復的 75 個資安漏洞中，有 8 個漏洞的危險程度評級為最高等級的「嚴重」（critical），其類型分別屬於遠端執行任意程式碼漏洞，以及執行權限提升漏洞。

如果以漏洞類型來看，這 75 個漏洞的分類如下：

- 權限提升漏洞：21 個；
- 資安防護功能略過漏洞：4 個；
- 遠端執行任意程式碼漏洞：26 個；
- 資訊洩露漏洞：17 個；
- 服務阻斷（Denial of Service）漏洞：6 個；
- 假冒詐騙漏洞：1 個

得到修復的 3 個 0-day 資安漏洞分別如下：

- CVE-2022-26925：Windows LSA 假冒詐騙漏洞，未經登入驗證的駭侵

者，可在 LSARPC 介面中呼叫某個方法，強迫網域控制器利用 NTLM 讓駭侵者通過驗證。駭侵者可以利用這個漏洞，攔截真實用戶的登入需求，並且提升自身執行權限。已知該漏洞現已遭到大規模用於駭侵攻擊活動。

- CVE-2022-22713：存於 Windows Hyper-V 的服務阻斷攻擊。
- CVE-2022-29972：Insight Software Magnitude Simba Amazon Redshift ODBC 驅動程式漏洞。

Microsoft 呼籲該公司各系統與軟體的使用者與管理者，應立即套用本次 Patch Tuesday 資安修補包，以避免駭侵者利用未修補的已知漏洞發動攻擊。

- CVE 編號：CVE-2022-26925、CVE-2022-22713、CVE-2022-29972
- 資料來源：
 1. Security Update Guide
 2. Microsoft May 2022 Patch Tuesday fixes 7 critical vulnerabilities, 67 others
 3. Microsoft May 2022 Patch Tuesday fixes 3 zero-days, 75 flaws

第 4 章、資安研討會及活動

資安就【四】在沙崙：資安議題系列線上講座 經濟部工業局沙崙資安服務基地	
活動時間	6/16 (四) 14:00~17:00 智慧製造的痛-駭客攻擊與勒索軟體威脅
活動地點	線上講座
活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=1658
活動概要	 <p>主辦單位：經濟部工業局</p> <p>6月連續3個週四。線上讓你認識資安大件事</p> <p>【#資安就四在沙崙】#資安議題講座系列</p> <p>CYBERSEC 2022 臺灣資安大會從5月延期到9月，讓您感到莫名心慌慌，對資安不心安嗎？別擔心！『ACW South 沙崙資安服務基地』將於6月推出「資安議題講座系列」（線上辦理，歡迎報名），讓您3個週四連續服用資安大件事，跟著我們一起長『資』識。</p> <p>【資安就四在沙崙】系列</p> <p>6/09 (四) 14:00~17:00 新世代資安防禦-網路威脅與防禦趨勢</p> <p>6/16 (四) 14:00~17:00 智慧製造的痛-駭客攻擊與勒索軟體威脅</p> <p>6/9(四)【新世代資安防禦—網路威脅與防禦趨勢】</p> <p>講座簡介：網路攻擊手段和技術日益翻新，個人和企業防不勝防，掌</p>

握網路威脅新態勢是化被動為主動的新世代網路資安趨勢。對於資安防禦的強化，企業往往處於被動的局面，要扭轉攻防不對等的局面，除了從事前防護，延伸到事中偵測與回應，還有一股趨勢正隱隱成形，就是新世代的主動式防禦概念。

6/16(四)【智慧製造的痛-駭客攻擊與勒索軟體威脅】

講座簡介：依據 Check Point® Software Technologies Ltd. 近期研究指出，與 2020 年相比，2021 年企業網路每週遭受的攻擊數量增長了 50%，台灣的機構在 2021 年則是每週平均遭受 2,644 次網路攻擊，較 2020 年增加 38%。5G 科技推動萬物聯網所帶動的製造業的轉型變革，提升智慧製造的效能亦帶來潛藏的資安隱憂；駭客組織鎖定有利可圖的製造產業進行攻擊，因此，認識勒索病毒及如何進行主動式防禦有其重要性；另亦透過產業的實務分享，了解如何主動找出可疑資安事件並有效降低資安威脅，由傳統防護演進到 Zero Trust，快速排除資安威脅並將風險降至最低。透過各式駭客攻擊案例，讓產業能有所警惕防範。

【注意事項】線上講座皆以 Google Meet 進行，連結將於講座開始前發送至信箱。

活動聯絡人 / Contact Us：

王小姐 janewang@iii.org.tw 02-6631-6636

劉小姐 vanessaliu@iii.org.tw 06-3032260#106

【資安學院】資安事故處理實務演練

活動時間	6/22-6/23 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/2753
活動概要	<div style="text-align: center;">  <p>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.</p> </div> <p>主辦單位：中華民國資訊軟體協會</p> <p>課程說明：近期政府企業遭受勒索病毒、APT 攻擊等資安事故頻傳，當資安事件發生時，應如何正確因應、處理及保全數位證據，成為政府企業必須正面以對之嚴肅課題。本課程將說明政府企業於發生資安事故時，應如何迅速釐清受害範圍、清除惡意程式及阻斷可疑之中繼站連線，進而回復至正常運作。本課程並以 Window 模擬環境為例，解析駭客入侵之情境，搭配實作解說資安事件處理流程，調查入侵事件的樣貌，而做出正確的因應。</p> <p>活動聯絡人：廖資深專員</p> <p>Email: security@cisanet.org.tw</p> <p>Tel: (02)2553-3988 Ext：388</p>

AWS 資訊安全線上研討會

活動時間 2022 年 6 月 29 日 (三) 2:00 PM 至 5:00 PM

活動地點 線上

活動網站 [請點此](#)

AWS Security Web Day

AWS 資訊安全線上研討會

主辦單位：AWS


活動概要

現今網路攻擊隨時都在，在網路環境上提供服務的每一秒鐘，也許都有駭客想要探測你的主機提供什麼服務，研判有無機會根據架構的弱點，取得他想要的營業秘密或個資，或讓你成為他的攻擊跳板。換言之你只
要被鎖定，就隨時等著接受嚴厲檢驗。

企業不是因為上雲才需要做資安，而是先有資安，順道一起搬上雲端；故雲端遷移過程一定要安全，否則換了平台也無法解決過往既存的問題。所以在遷移過程，AWS 鼓勵客戶順便檢視系統架構或權限配置，確保上雲之後符合最小權限原則，讓不該看的人就看不到。

如果您對於資訊安全有興趣，卻又不知該如何著手，歡迎參加 AWS Security Web Day 一起深入探索資安！

【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.cisnet.org.tw/Course/Detail/2752
活動概要	<div data-bbox="513 517 1257 674" style="text-align: center;">  <p>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.</p> </div> <p>主辦單位：中華民國資訊軟體協會</p> <p>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。</p> <p>課程大綱：</p> <ul style="list-style-type: none"> ● 資訊安全規劃實務 <ul style="list-style-type: none"> ➢ 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 <ul style="list-style-type: none"> ➢ 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。

第 5 章、2022 年 5 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。

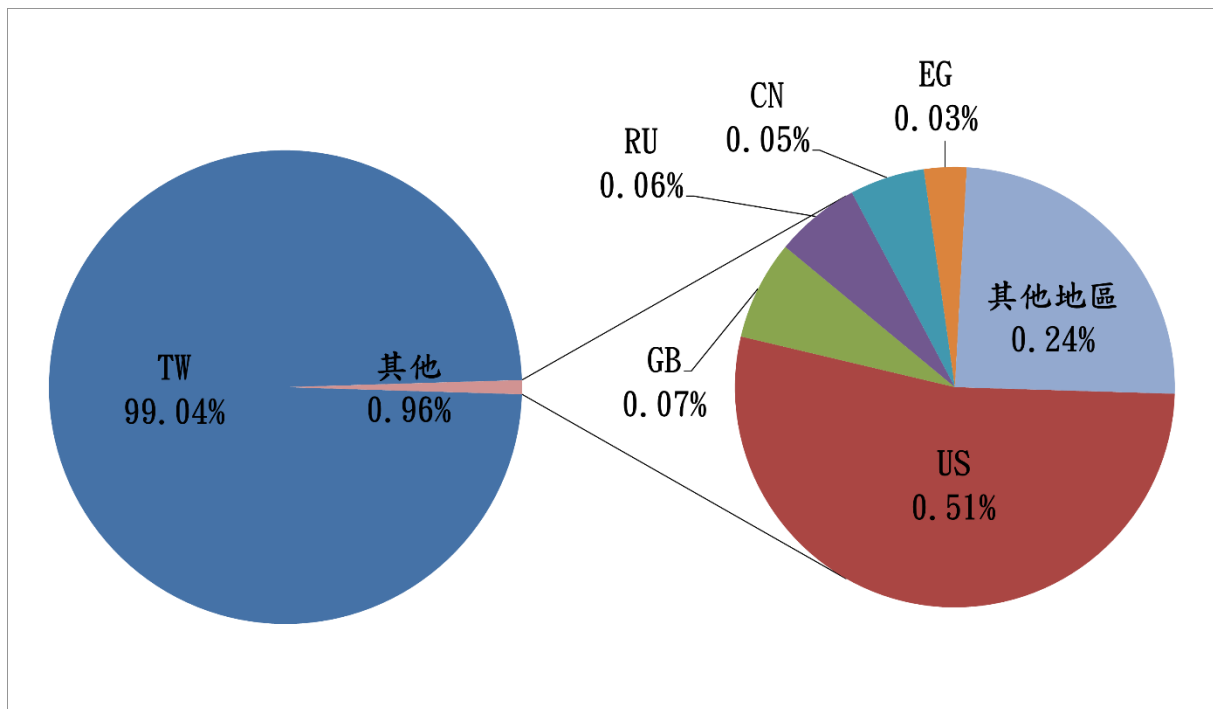


圖 1、分享地區統計圖

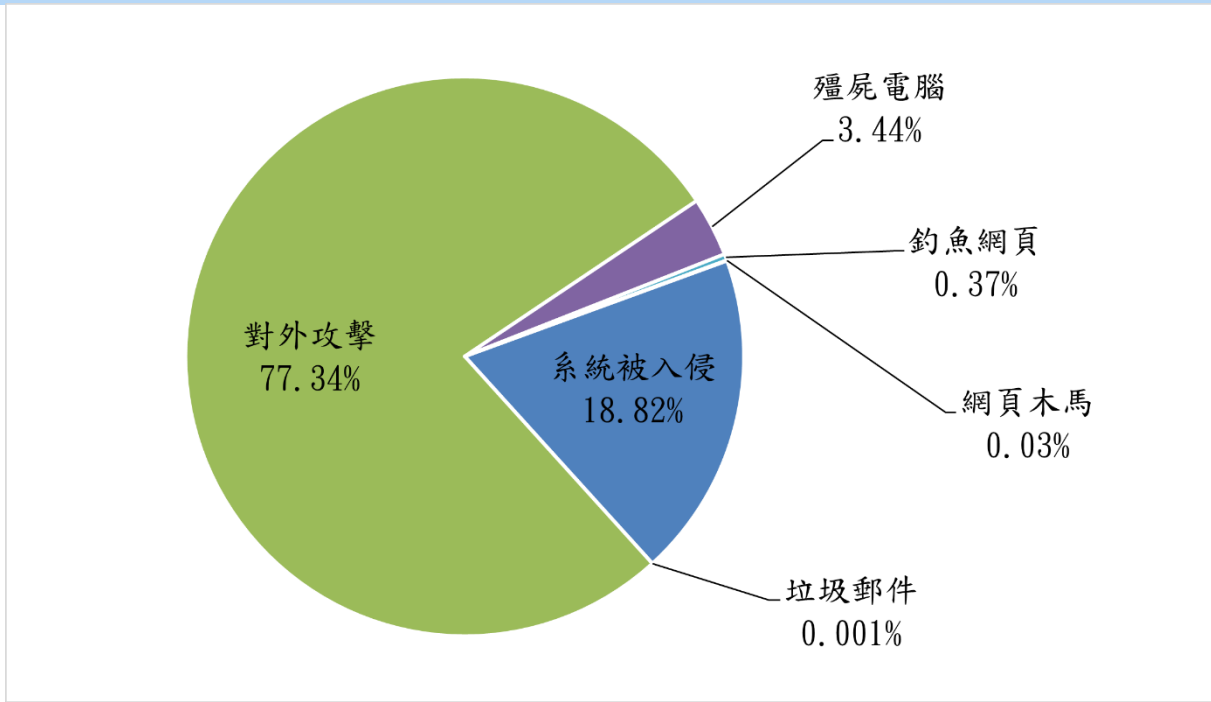


圖 2、分享類型統計圖

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 6 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](https://twitter.com/TWCERTCC)