TWCERT/CC 資安情資電子報

2023 年 2 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 7 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、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 4 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 5 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 6 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 7 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

社群媒體與即時通訊的資安威脅與防護

- 運用社群媒體與即時通訊等應用來進行生活社交與工作交流，已是現代人的日常，而且皆翻轉了傳統媒體與社交行為的模式，以分享交流為主，而且在企業工作使用日益重要，因此成為駭客蒐集資訊的最佳管道。
- 社群媒體與即時通訊應用普及，有成為惡意軟體散播管道、不慎洩漏機敏資料、遭受社交工程攻擊、個資隱私保護議題等資安疑慮。
- 社群媒體與即時通訊軟體過往皆因存在漏洞，導致可監控設備、偷取資料，故需注意軟體更新問題。
- 駭客集團攻擊的初始步驟為蒐集資訊，或是引導使用者前往惡意釣魚網站下載惡意軟體，以 APT32 之常用攻擊手法為例，結合 MITRE ATT&CK matrix 方式解析其攻擊步驟。
- 在資安防護機制的作法方面，彙整美國、英國、歐盟之建議規範，提供制度、技術層面的參考。

一、簡介

在網路時代，運用社群媒體與即時通訊等進行生活社交與工作交流，已

是現代人的日常，而這類運用過程中交換的個人、企業資料是非常有價值的，因此成為駭客覬覦的目標，相關各種資安事件層出不窮，衍生的損害也日益增加。

以下分別就社群媒體與即時通訊的使用情境、特性進行說明：

(一)社群媒體

傳統媒體主要是單向的傳播機制，雖然也有讀者投書、徵稿、call-in 等方式讓社會大眾進行反饋再由媒體公開，但受限極大，且發布內容完全由報社、電視台等媒體業主所掌控，相對地因網路普及而興起的社群媒體（social media）則完全是社會大眾所主導，個人化導向為其主要特色，即便是傳統的大型媒體主介入，也僅是資源上的優勢，在角色上與一般人皆為等同，因此社群媒體便成為發表創作、分享、交流意見、經驗知識傳播的最佳平台，也因此集結成各種特性的社群，大型社群所擁有的影響力更是跨領域的。

一般來說，以 Facbook 為例，個人 Facebook 接觸的以好友圈為主，粉絲團接觸的主要以陌生客群為主，以個人動態消息及粉絲團搭配使用，可以接觸到不同的族群，經營好友、粉絲、會員等，形成複雜的社交結構，也讓懷有不良意圖的使用者有惡意操弄的空間。

(二)即時通訊

即時通訊來自短時交流需求，從傳統的手機簡訊逐步演變，可以透過快速方便的網路服務傳達訊息，不同於電子郵件存儲轉發的方式，即時的傳遞是即時通訊的主要要求，目前常見受歡迎的即時通訊服務包含了 skype、LINE、Facebook Messenger、WhatsApp、Discord、Telegram、微信等。

隨著功能演進，即時通訊服務也開始整合網路電話(VoIP)、即時影像、檔案傳輸等服務，甚至是傳輸檔案後可兼容各種格式進行開啟閱讀，這些都是商業使用的重要功能，再整合原本交流訊息的整合式使用情境，尤其近來疫情影響，遠距上班需求使即時通訊重要性大增，因此某些為商業工作需要所開發的工具軟體也納入即時通訊範圍，如 Webex、Teams、Zoom 等。

雖然市場上有專為工作開發的即時通訊軟體，然而使用者長期養成的習慣難以改變，例如我國社會大眾習於使用 line，其做為日常溝通工具已是主流，且因交流行為的特性，大者恆大居於主導地位，用戶較傾向使用可與主流大眾相同的溝通管道，所以多為 line 加上其它的商用工具的混合用法，這也意味著 line 這樣的一般社交軟體，也出現商業機密等級的傳輸內容，因此與社群媒體相似，即時通訊也是駭客攻擊的目標之一。

(三)安全議題

社群媒體與即時通訊所具備的的資訊分享、快速傳播、社群影響、商業內容等特性，在駭客集團眼中已成為蒐集或竊取資訊的最佳管道，近年來發生的相關資安事件層出不窮。其主要資安議題為：

1. 惡意軟體傳播管道：釣魚網站連結的傳播主要方式為電子郵件與即時通訊軟體，藉由具吸引力的內容讓使用者點擊，進而成功進行釣魚攻擊，亦或是更為直接的惡意檔案傳輸，點擊後直接執行。

2. 機敏資料外洩：網站應用或軟體工具漏洞被利用皆可能造成危害，社群媒體、即時通訊出現漏洞，潛藏的洩漏機密風險極高，曾有案例是透過社群媒體 APP 的漏洞，隱匿監控 APP 內所有的行為與訊息記錄，造成企業重要機敏資料外洩。

3. 社交工程攻擊：駭客集團在初步蒐集情資後，可鎖定特定具獲利之目標族群進行攻擊，例如以金融機構或其客戶為對象，在社群媒體中尋找具有類似屬性的社群，創建假帳號加入，觀察其中可能獲取下一步攻擊資訊的對象，接近來往後，騙取企業資訊，甚至是更為機敏的資料；甚至主動創建群組，藉由資訊的分享來吸引特定族群參加，再伺機發動進一步攻擊。

4. 隱私保護議題：為社群媒體最被質疑的資安議題，本文主要針對具攻擊性質

之惡意行為，隱私保護涉及其他更廣泛議題，如個人資料保護、私密活動資訊保護等，不在探討範圍中。

二、社群媒體與即時通訊遭駭之案例探析

駭客集團藉由已建立之各種由社群媒體與即時通訊當跳板，取得攻擊可用的資訊管道，如下圖，APT32、Cleaver、Sandworm Team 均為駭客集團代號，Fox Kitten 則是知名駭客，例如為惡意網站成立 Facebook 進行宣傳、註冊假的 LinkedIn 帳號與知名企業接觸、在 Twitter 等媒體註冊帳號，作為與被勒索受害者溝通之工具。以下使用攻擊案例與 MITRE ATT&CK Matrix，分析攻擊行為步驟。

ID	Name	Description
G0050	APT32	APT32 has set up Facebook pages in tandem with fake websites.
G0003	Cleaver	Cleaver has created fake LinkedIn profiles that included profile photos, details, and connections.
G0117	Fox Kitten	Fox Kitten has used a Twitter account to communicate with ransomware victims.
G0034	Sandworm Team	Sandworm Team has established social media accounts to disseminate victim internal-only documents and other sensitive data.

資料來源：MITRE

圖 1、駭客集團社群媒體行為

(一)Android 惡意軟體竊取社群軟體資訊

社群軟體工具在電腦與行動平臺上的使用管理存在差異，因此在資安議題上也有差異，電腦平台為網頁形式，故發生漏洞時，由官方維護更新，使用者並無更新或是使用舊版議題，更新版本並無時間落差。在行動平台上，皆是以 APP 運作方式，版本更新由使用者操作，雖然目前較新版的行動作業系統已有自動更新功能，但行動作業系統版本不一，部份也可能由使用者觸發，因此漏洞問題影響較大。即時通訊有部份在電腦也是以 APP 形式運行，因此也存在更新時間落差的議題。

以 Android 平台為例，RCSAndroid 是針對 Android 打造的惡意軟體，其存在目的就是為了要蒐集使用者資訊，依據 ATT&CK Matrix 分析的步驟如下

表，表中以攻擊步驟來說明其整體行為。

此惡意軟體蒐集資訊的功能可分為兩類，一是蒐集行動設備使用者當下環境的資訊，如 T1429、T1512、T1414 的錄音、照相、剪貼簿，通常是駭客已鎖定此使用者，認定具備攻擊價值，才會專門分析特定資訊。而第二類行動則是廣泛的將社群媒體儲存的資料與密碼進行蒐集，如 T1409 與 T1533，這類資訊蒐集後會經過數據分析處理，再評估其資訊性質進行利用。

動作ID	名稱	說明
T1409	訪問存儲的應用程序數據	RCSAndroid可以從流行應用程序收集聯繫人和消息，包括 Facebook Messenger、WhatsApp、Skype、Viber、Line、微信、Telegram
T1429	捕獲音頻	RCSAndroid可以使用設備麥克風錄製音頻
T1512	捕捉相機	RCSAndroid可以使用前後攝像頭拍攝照片
T1414	捕獲剪貼板數據	RCSAndroid可以監控剪貼板內容
T1533	來自本地系統的數據	RCSAndroid可以收集Wi-Fi網路及在線帳戶的密碼，包括 Skype、Facebook、Twitter、Google、WhatsApp、Mail 和 LinkedIn

(二)APT32 駭客集團攻擊手法

ATT&CK Matrix 已整理出 APT32 駭客集團常用的攻擊手法，其中社群軟體在數個階段皆為其主要技術手法。APT32 集團通常以惡意釣魚網站誘騙使用者點擊，再進一步取得使用者帳號、密碼，或權限等資訊，做為攻擊的展開步驟。

首先建立惡意網站，在 Resource Development 發展攻擊資源的階段中，步驟 T1608 Drive-by Target，APT32 建立了包含大量從網路上抓取的文章和內容的網站，以使網站看似正常合法，但其中一些頁面卻暗藏惡意 JavaScript，藉以分析潛在受害者或通過惡意軟體進行感染動作，此惡意頁面的建立，是歸類在 Command and Control 階段的 T1105 Ingress Tool Transfer，APT32 已將

JavaScript 添加到惡意網站，以下載工具軟體來分析和危害網站訪問者。

為了宣傳或是誘導使用者發現此釣魚網站，APT32 使用了釣魚郵件與社群媒體兩種方法，這是被歸類在 Reconnaissance 偵察階段 Phishing for Information 與 Initial Access 階段中的 Spearphishing Link 是將惡意連結放置於釣魚郵件中，而同一個階段中的 T1585 Social Media Accounts 是創建 Facebook 帳號，並經營吸引使用者到訪瀏覽惡意網站。

Reconnaissance	Resource Development	Initial Access	Command and Control
Gather Victim Identity Information	Domains	Spearphishing Attachment	Ingress Tool Transfer
	Web Services	Spearphishing Link	Non-Standard Port
	Social Media Accounts	Local Accounts	Web Service
Phishing for Information	Drive-by Target		
	Upload Malware		

資料來源：MITRE

圖 2、APT32 利用社群媒體發起攻擊

(三)社群軟體大量洩露使用者密碼

與即時通訊洩資造成的損害狀況不同，社群軟體遭駭常見爆發大量的使用者資料外洩事件，近期最知名的是 2021 年 4 月 Facebook 5.33 億筆個資外洩，其原因是 API 漏洞遭入侵所造成，統計 16 年間外洩個資最多的排名，Facebook 占了 5 次，但此類事件一般使用者難以採取有效的防範措施，因掌控權並不在使用者，僅能注意盡可能減少個資出現在社群媒體。

資料來源：Intact Blog

圖 3、外洩個資事件排行

(四)即時通訊漏洞議題

釣魚連結的傳播除了以電子郵件外，主要是利用即時通訊軟體，通常以有趣或熱門時事的標題吸引使用者點擊，且使用者常會基於分享的心態不斷傳播，而其標題設計也可鎖定族群類型，例如投資相關標題。在 2019 年，電子郵件安全公司 Vade Secure 發現針對其用戶的特定釣魚連結數量激增 13,467%，其中以 WhatsApp 傳播的不同釣魚連結數量達到 5000 個以上，此為針對性案例，但一般未鎖定目標的數量將更為驚人。

行動設備所安裝的 APP 中，即時通訊軟體通常是必要的，如 2021 年 8 月發現駭客釋出強化 WhatsApp 的助手 APP FMWhatsappWhatsApp 來吸引下載安裝，標榜可以改善 WhatsApp 的用戶體驗，例如更好的隱私、自定義聊天主題、訪問其他社交媒體的表情符號包，以及使用 PIN、密碼等鎖定應用功

能，但其中卻夾帶多種惡意軟體，包括非常難以刪除的 xHelper 及 Triada 木馬軟體。

安裝 FMWhatsappWhatsApp 後，Triada 開始收集設備上的訊息，並將其轉送到其命令和控制伺服器(C&C Server)，該伺服器回覆一個下載連結，隨後即將木馬下載至遭駭設備，並進一步啟動多個惡意軟體，包括：

1. Trojan-Downloader.AndroidOS.Agent.ic，下載並啟動其他惡意模組。
2. Trojan-Downloader.AndroidOS.Gapac.e，安裝其他惡意模組並顯示全螢幕廣告。
3. Trojan-Downloader.AndroidOS.Helper.a 執行 xHelper 安裝程序並在後台運行隱形廣告。
4. Trojan.AndroidOS.MobOk.i 為 Android 設備所有者註冊付費訂閱。
5. Trojan.AndroidOS.Subscriber.l 為受害者註冊高級訂閱。
6. Trojan.AndroidOS.Whatreg.b 收集訊息並請求驗證碼登錄受害者的 WhatsApp 帳戶。

另一個惡意軟體 WhatsApp Pink 除了類似前述的惡意功能外，在 2021 年 4 月被發現新增功能，能夠自動回覆來自各種應用服務（包括 Signal、Viber、Telegram 和 Skype）的訊息，如此動作的用意是將自身傳播給可能點擊連結的毫無戒心的其它使用者，以及下載受感染的 APK。

三、資安防護機制

雖說社群軟體與即時通訊服務有各種資安事件的發生，但並非是不重視資安議題，其軟體功能皆有安全考量之機制，例如網頁版的應用服務，必定會以 TLS（Transport Layer Security）加密機制進行保護，即時通訊服務也會

提供點對點的加密功能(End-to-End Encryption，E2EE)，而且設計使用者專屬的加密金鑰，是一個名為 Letter Sealing（信件資訊密封保護）的功能，並且適用於群組。同時也具備各種身份認證方式，例如結合手機來進行多層次的證認，並於使用新設備登入時必須進行確認等防護機制。但點對點的加密方式仍非完全的安全，因存在中間人攻擊的可能性，所以通常搭配其它認證機制來加以強化。

各國針對社群媒體與即時通訊資安議題十分重視，也有相關的國際資安規範，以下彙整英國的 NCSC(National Cyber Security Centre)、美國 CISA(The Cybersecurity and Infrastructure Security Agency)與歐盟 ENISA(The European Union Agency for Cybersecurity)所提出的相關規範建議。

(一)社群媒體

保護在社群媒體上發布的內容

- 風險威脅
  - 不當的內容、錯誤訊息或發布個人觀點（不是“官方”公司觀點）可能會損害對組織的信任
  - 出於惡意目的劫持，例如重定向到惡意網站
- 應對作法
  - 確保只有授權人員才能發佈內容
  - 對離職者或調離部門者進行追蹤管理
  - 使用提供良好安全功能的社交媒體平台
  - 確保內容在發佈前可以經過審核和授權
  - 使用公司設備創建和發佈內容
  - 制定緊急損害復原計劃

如何安全使用社群媒體

- 威脅風險
  - 魚叉式釣魚攻擊
  - 社交工程
  - 身份識別相關威脅
  - 網站應用攻擊
- 應對作法
  - 依循來自社交媒體平台的安全建議，並設定安全 policy
  - 使用雙因子身分驗證 (2FA)來保護帳戶
  - 制定政策並強化存取網路與端點資料的控制措施
  - 建立與供應商及協力廠商的安全管理機制

(二)即時通訊

- 最小化即時通訊軟體的權限設定，如: 關閉自動下載或只允許通訊錄的人員通訊
- 避免透過即時通訊軟體提供機密資料，並確認對方身份
- 定期更新即時通訊軟體
- 封鎖不明使用者的訊息
- 了解即時通訊軟體的安全機制，如: 訊息加密、訊息刪除、雙因子身分驗證、安全設定、雲端備份機制等，並採用適合該軟體應用安全的設定
- 關閉自動接受好友申請與搜尋功能

- 不隨意開啟連結
- 使用即時通訊軟體的設備應啟用螢幕保護程式、使用電腦或網頁版的通訊軟體後確實進行登出
- 企業應明訂即時通訊軟體政策，如: 指定員工使用特定即時通訊軟體、不可傳送企業機密與文件、使用即時通訊軟體的手機應設定自動螢幕鎖定及加密儲存等
- 訂定行動裝置使用管理機制
- 定期舉行員工資安意識教育訓練

四、分析與建議

1. 社群媒體與即時通訊已成為駭客獲取資訊，或是引導使用者受駭的第一步，故必須更加重視相關安全議題。
2. 社群媒體與即時通訊於疫情時代，更為企業工作所更加廣泛應用，然其與員工日常生活的使用也有很多交集，導致可能無心的舉動即危害到資訊系統安全，企業應更重視相關議題，並訂定管理辦法並予以落實。
3. 企業確實進行軟體更新是資安的不二法門，在各種使用情境的社群媒體與即時通訊更是如此。
4. 軟體工具的安全設定項目繁多，應盡可能瞭解其相關設定的意義，並進行合於安全要求的選擇，軟體工具已具備安全機制，倘若設定有疏漏則極易讓駭客有機可趁。
5. 對社群軟體與即時通訊的攻擊，主要是利用人性的弱點，趣味、獲取資訊、折扣優惠等吸引人的內容，並於社交活動中廣為分享，故使用者對內容感興

趣時，應再三思其背後所代表的意義與合理性。

- 資料來源：

1. 社群媒體
2. 即時通訊
3. RCSAndroid
4. APT32
5. Facebook tops the data loss roll of shame
6. Malicious WhatsApp mod infects Android devices with malware
7. Social media: protecting what you publish
8. Social Media: how to use it safely
9. Guidelines for Secure Use of Social Media by Federal Departments and Agencies
10. Recommendations for Online Social Networks
11. Choosing an enterprise instant messaging solution
12. Using third-party applications on devices
13. Using Instant Messaging and Chat Rooms Safely

第 2 章、 資安小知識

常見勒索軟體的入侵管道與防護建議

TWCERT/CC

常見勒索軟體的入侵管道
與防護建議

要防範勒索軟體，必須先對勒索軟體的攻擊途徑有所瞭解。勒索軟體感染在完整的攻擊行為中，是屬於末尾的步驟，因此企業如果能在先期發現攻擊跡象，便有可能阻止勒索軟體攻擊，也就是盡早發現憑證盜竊和橫向移動的跡象，可防止勒索軟體悄悄入侵企業網路。

1.曝露於網際網路的設備漏洞與錯誤配置

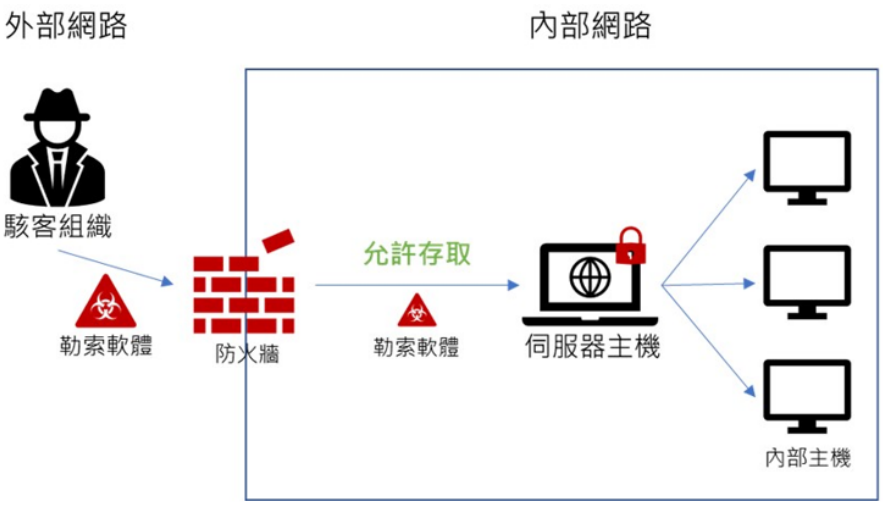

圖1：曝露於網際網路的設備漏洞與錯誤配置有可能成為資安的破口

說明：

任何曝露於外部網路的主機或伺服器都有可能成為資安的破口。攻擊者可以透過大量掃描的方式來探測網路上的主機，藉此發現存在漏洞或安全性設定錯誤的主機，因此任何可以直接被外部使用者連線的主機或伺服器都必須做好資安防護，將資安的攻擊面縮減到最少。

防護建議：

(1) 盤點與確認主機服務(Service)開啟的必要性，以減少不必要的外部連線，例如：禁用非業務目的的連接端口和協定等。

(2) 定期進行漏洞掃描以識別和修補漏洞。

(3) 確保設備配置正確並啟用安全功能，例如：設備存取必須使用多因素認證、服務連線必須加密、軟韌體設備需隱藏版本資訊等。

(4) 對於任何公開曝露的服務，例如：遠端桌面協議(RDP)、虛擬網絡計算(VNC)和檔案傳輸協定(FTP)等，應啟用多因素身份驗證(MFA) 並記錄系統登錄活動。

(5) 評估是否需要在系統上打開遠端桌面協定(RDP, 端口 3389)和服務器訊息模組(SMB, 端口 445)，並限制只能透過特定的受信任主機進行連線。

2.網路釣魚

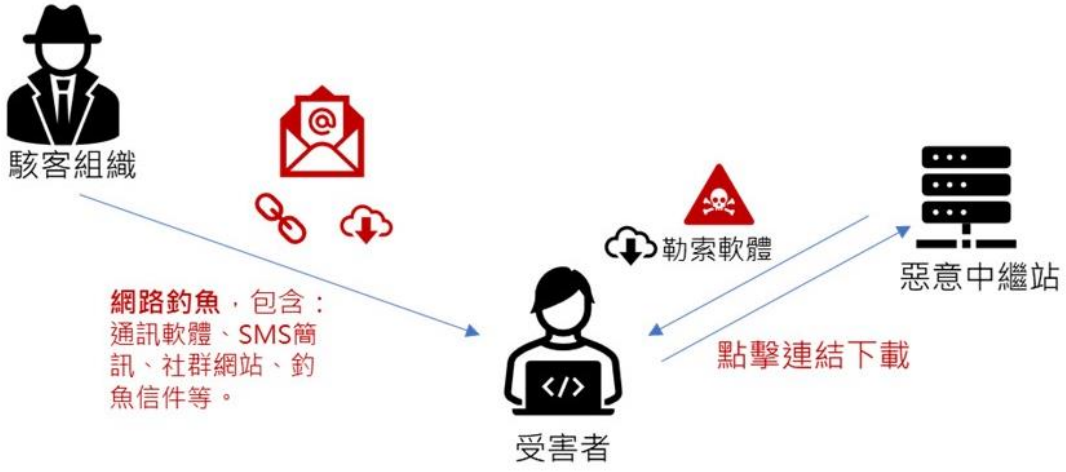

圖 2 ：駭客透過網路釣魚傳遞勒索軟體

說明：

網路釣魚是傳遞勒索軟體最常見的方式，類似的方式有很多，包含：通訊軟體、SMS 簡訊、社群網站、釣魚信件等。其中，釣魚信件是經常被使用的方式，攻擊者通常會將惡意連結或附檔透過社交工程的方式寄送到受害者的信箱，當受害者開啟信件中的惡意連結或附檔時，就會下載並執行惡意程式。

此外，透過惡意網址連接到釣魚網站或惡意下載點也是網路釣魚經常使用的手法，因此提高資訊安全意識，避免點選可疑通訊軟體和簡訊的連結是網路釣魚最有效的防護方式。

防護建議：

(1) 企業或組織內部須定期舉辦資安教育訓練，提高資安意識。

(2) 企業或組織內部須定期實行社交工程演練，加強識別潛在惡意電子郵件的重要性。

(3) 架設電子郵件過濾器，阻止含有惡意入侵指標的電子郵件傳遞，並使用防火牆阻止可疑 IP。

(4) 使用 SPF、DKIM、DMARC 等檢查機制來保護電子郵件，降低電子郵件來源的欺騙和修改。

(5) 考慮禁用包含 Microsoft Office Macro 的電子郵件。

(6) 考慮禁用可被利用的附檔名，例如：.scr, .exe, .pif, .cpl 等。

(7) 避免點選可疑來源的連結或附檔。

(8) 當收到可疑信件或連結時，須確認來源方的可信度，並查證內容的真實性。

3.前驅惡意程式感染

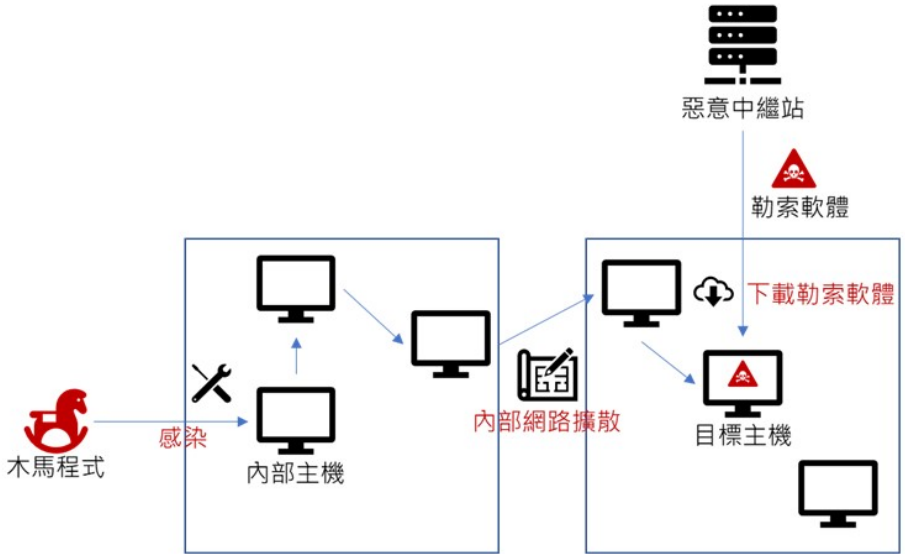

圖 3 ：前驅惡意程式透過漏洞、網路釣魚等方式進入內部網路進行擴散

說明：

前驅惡意程式是感染勒索軟體前的信號，當惡意程式透過漏洞、網路釣魚等方式進入內部網路後，並不會直接安裝勒索軟體，而是在內部網路等待並尋找適合時機來下載勒索軟體本體。許多勒索軟體會先利用 dropper 等惡意程式感染受害者主機，在取得控制權後，才會從惡意中繼站下載勒索軟體的主程式。勒索軟體的感染分成很多階段，從進入受害者電腦到執行勒索軟體都是不同的惡意程式，並且這些惡意程式是從不同的命令控制伺服器取得，導致調查上有一定程度的困難。在感染惡意程式時必須有所警覺，例如：是否有其他不同惡意程式存在，或是有可疑連線等。

防護建議：

(1) 定期更新防毒軟體等資訊安全防護設備的入侵指標。

(2) 對所有應用程式啟用白名單機制，確保只有被授權的軟體可以運行，未被授權的軟體都被停止運行。

(3) 考慮導入 IDS、IPS、SIEM、EDR 等資安防護設備，用於檢測勒索軟

體部署前發生的命令和控制活動以及潛在的惡意網路行為。

4.透過第三方的託管服務入侵

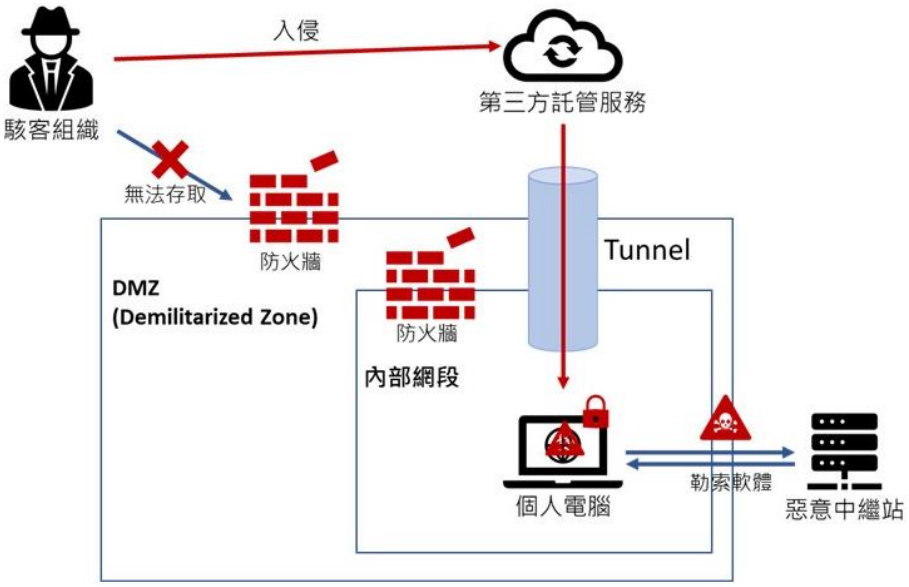

圖 4 ：攻擊者利用託管服務供應商(MSP)入侵

說明：

企業或組織所使用的雲端託管服務必須來自可信賴的供應商，並且需要做好身分管理，因為攻擊者可能會利用託管服務供應商 (Managed Service Provider, MSP) 的網路連接對客戶組織內部進行訪問，並且用於傳遞勒索軟體，除此之外，攻擊者也可能竊取 MSP 的電子郵件帳戶來發送釣魚信件。因此，公司或組織針對 MSP 必須訂定較高的安全規範並確實執行，盡可能將攻擊管道縮小。

防護建議：

(1) 確保使用安全的託管服務提供商 (Managed Service Provider, MSP)或雲端服務提供商 (Cloud Service Provider, CSP)。

(2) 盡可能為所有服務使用多因素身份驗證 (Multi-factor authentication, MFA)，特別是 Web 郵件、虛擬專用網路和可以訪問關鍵系統的帳號。

(3) 確實執行最小權限原則，為所有用戶、軟體提供只有執行工作時需要

用到的訪問權限。

(4) 定期盤點所有帳號的活動狀況，並禁用未使用的帳號。

(5) 為雲端服務啟用安全設置，包含日誌記錄檔、黑白名單機制、啟用可疑活動警報等。

5.內部網路擴散

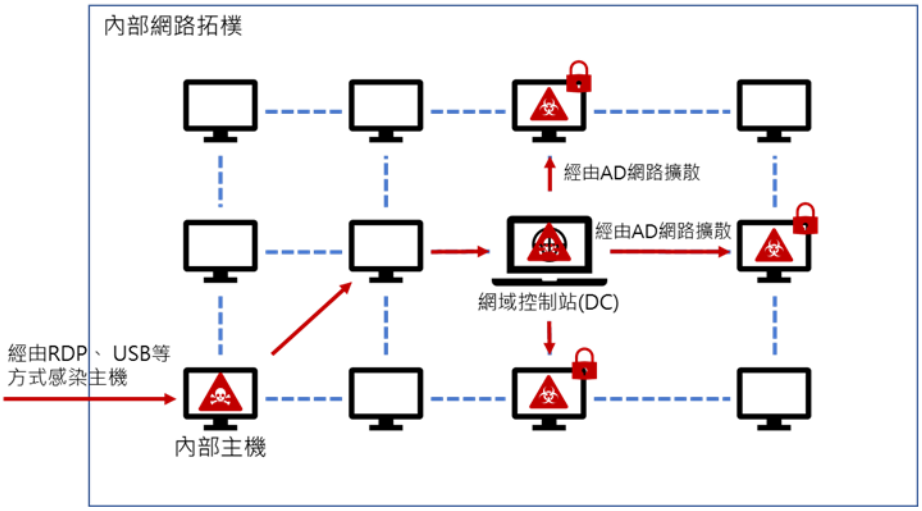

圖5：內部網路擴散

說明：

勒索軟體在感染公司或組織內部主機後，會滲透企業或組織網路並在內部散播，企業或組織必須具備足夠的網路能見度來主動回應或控制這些威脅所造成的影響，並減少重複感染的風險。當攻擊者進入公司內部後，通常以網域控制站 (Domain Controller, DC)為目標並將其當作傳播勒索軟體的中轉站。攻擊者在取得 AD 網路的控制權後，可以將勒索軟體散播至 AD 網路中所有的主機，資產損害的程度也大為提升。在資訊安全防禦的策略中，當攻擊事件發生時，應啟動資安事件應變計畫，並即時掌控資安影響範圍，藉此阻斷資安損害的範圍。當企業內部已遭勒索軟體入侵，為避免其他主機或重要資產遭到勒索軟體加密和外洩，應立即阻斷勒索軟體在內部網路擴散的路徑，實行斷網、隔離等防護措施。

防護建議：

(1) 使用實體網路分段，分離不同組織單位和 IT 資源，例如：OT 網路和 IT 網路之間分離。

(2) 定期更新包含網路、系統和數據流的拓樸，可以在資安事件發生時，提供較全面的檢視，以阻斷損害擴散。

(3) 確保網域控制站 (Domain Controller, DC)的漏洞可以及時修補。

(4) 確保主機和 DC 之間的溝通必須使用 SMB 簽名(SMB signing)，防止惡意程式執行重送攻擊。

(5) 網域控制站(Domain Controller, DC)的主機必須架設防火牆，並防止外部網路的存取訪問。

(6) 啟用網路設備和本地主機的系統日誌記錄檔功能，提供資安事件調查和追溯的參考。

(7) 企業或組織內部主機必須安裝資安防護軟體，並維持更新狀態。

- 資料來源：
  1. RANSOMWARE GUIDE
  2. Everything You Need To Know About Ransomware

第 3 章、 資訊安全宣導

提防假冒政府機關發送之詐騙訊息

近期由於政府宣布將普發現金還稅於民，詐騙集團也利用此訊息發送釣魚簡訊進行詐騙。詐騙簡訊係以假冒政府機關名義，以快速領取現金為由，誘騙民眾點擊簡訊內的釣魚連結。

提醒民眾若收到類似的釣魚簡訊或郵件，請務必特別留意，以免上當受騙而造成個資外洩或財物損失。

TWCERT/CC 也提供相關建議措施：

1. 政府機關不會以簡訊等方式，透過不明網址通知民眾領錢。
2. 不要因為好奇心而點擊不明簡訊的網址或連結，進入可疑網站不輸入個資、帳號密碼及金融資訊，更不要進行匯款。
3. 政府機關網站的網址首段會以 https 開頭，並以 gov.tw 結尾。
4. 建議民眾謹慎處理與個資或金錢相關之資訊，收到可疑簡訊可先撥打 165 反詐騙諮詢專線求證。

5. 若發現可疑網址，可至 TWCERT/CC 之 Phishing Check 網路釣魚通報進行通報，TWCERT/CC 確認後會協助釣魚網站下架服務。

- 資料來源：

1. 網路釣魚通報(Phishing Check)
2. 全民普發 6000 元，詐騙集團動作比政府快！收到這簡訊要留意…政院籲別被騙，切記「三不」
3. 普發 6000 元詐騙現蹤 行政院：不會以簡訊通知領取
4. 「通知領 6000 元」惡意簡訊竄起 政院：詐騙勿上當！
5. 口罩實名制 2.0 預購踴躍，注意防範詐騙簡訊

第 4 章、 國內外重要資安事件

4.1、資安趨勢

2022 全年，至少有 200 個美國政府、教育、醫療保健等公用事業單位遭到勒贖攻擊

資安廠商 Emsisoft 日前發表統計報告指出，2022 年全年，美國全境有多達 200 個以上各種公用事業單位遭到勒贖攻擊，被攻擊的公用事業對象包括各級地方政府、大專院校等各級學校、醫療機構等單位。

據 Emsisoft 整理自公開資料所得到結果指出，去年一年美國境內共有 105 個郡縣級政府單位、44 所大專院校、45 所其他學校校區與 24 所醫療保健機構，曾經遭到規模不等的勒贖攻擊。

Emsisoft 指出，該報告的資料來源包括各種資安通報、駭侵攻擊調查報告、暗網流出資訊、第三方提供的情報等等。

統計報告也指出，約有一半左右的攻擊事件，受駭單位所屬資料遭到竊取。

若與 2021 年相比，各級地方政府遭到勒贖攻擊的件數，由 77 起成長到 105 起；但 2020 年則發生了 113 起。

Emsisoft 也指出，2022 年一起發生在阿肯色州米勒郡（Miller）的勒贖攻擊事件，因為透過網路大量擴散，結果造成其他 55 個地方政府也遭到駭侵攻擊；而從已知資料中，僅有麻州昆西郡（Quincy）支付贖金，造成 50 萬美元財政損失。

在教育機構方面，2022 年有 44 所美國大專院校和 45 所其他各級學校校區遭到勒贖攻擊，其中有三所學校支付贖金；支付最多者超過 40 萬美元。醫療方面，旗下擁有 140 間連鎖醫院的 CommonSpirit Health 有超過 62 萬名患者資料遭竊。

各公用事業由於服務人數重多，經常包含社會運作不可或缺的關鍵服務，因此建議應特別加強資安防護能力與人員資安訓練，以防勒贖攻擊造成財務與資料的雙重損失。

- 資料來源：
  1. Ransomware impacts over 200 govt, edu, healthcare orgs in 2022
  2. The State of Ransomware in the US: Report and Statistics 2022

4.2、新興應用資安

4.2.1、新發現利用 SHC 編譯的 Linux 惡意軟體，會安裝挖礦與 DDoS 程式

南韓資安廠商 ASEC 旗下的資安專家，發現近來有許多駭侵攻擊活動，利用以 SHC（Shell Script Compiler）編譯的惡意軟體，在遭到入侵的 Linux 主機上安裝挖礦工具與 DDoS 僵屍網路。目前被害主機以南韓境內的伺服器為主。

SHC 是一種 Linux 上的通用 shell 指令檔編譯器，可以將 Bash 的 shell script 編譯成 Linux 與 UNIX 系統的 ELF 可執行檔。

報告指出，駭侵者通常先以暴力試誤法，入侵管理者帳號未受適當保護的 Linux 主機後，再利用經由 SHC 編譯過的惡意軟體來布署挖礦軟體或 DDoS 僵屍網路節點。

專家表示，通常以 Shell script 指令碼編寫的惡意軟體，由於內含許多以明文儲存的關鍵系統指令，因此很容易被系統上安裝的防毒防駭軟體截獲；但由於以 SHC 編譯過的 Shell script 會以 RC4 演算法編碼成 ELF 檔，因此不易偵測，駭侵者可用以逃過資安防護關卡。

ASEC 在報告中指出，在這波攻擊中觀察到 SHC 惡意軟體會在成功入侵後，於系統中安裝多種惡意軟體酬載，例如用以挖掘 Monero 加密貨幣的 XMRig 挖礦軟體，以及以 Perl 寫作的 DDoS IRC 僵屍機器人程式。

報告指出，一旦該 IRC 僵屍惡意軟體安裝成功，就會連上某台 IRC 伺服器，等待駭侵者透過聊天頻道發送多種 DDoS 相關攻擊指令並加以執行，包括各種通訊協定如 TCP、 UDP、HTTP 洪水攻擊、連接埠掃瞄等。

鑑於此類攻擊通常選擇管理者帳號防護薄弱的主機為目標，因此務必變更主機的預設管理員帳號與密碼，同時採用二階段登入驗證；較敏感的主機更需以防火牆隔離於外部 Internet。

- 資料來源：
  1. Shc Linux Malware Installing CoinMiner
  2. New SHC-compiled Linux malware installs cryptominers, DDoS bots

4.2.2、駭侵者利用假冒寶可夢 NFT 挾持 Windows 裝置

南韓資安廠商 ASEC 發現有駭侵者透過假冒的寶可夢 NFT 卡牌遊戲釣魚網站，以投資 NFT 獲利為誘餌，來吸引用戶安裝含有 NetSupport RAT 遠端遙控組件的惡意軟體，藉以控制用戶的 Windows 電腦。

遭 ASEC 旗下資安專家發現的該釣魚網站，其網域是「Pokemon-go[.]io」，在資安媒體報導此事件時仍未下線；該網站宣稱提供玩家免費下載寶可夢卡牌遊戲，並在遊玩時賺取獲得 NFT；但實際上用戶一旦按下網頁中的「Play on PC」按鈕，會下載回來的就是惡意軟體 NetSupport RAT。

雖然 NetSupport 本身並不是惡意軟體，而是正常的遠端遙控工具，但在 ASEC 發現的多個案例中，駭侵者利用 NetSupport 來與其控制伺服器連線，讓駭侵者可以遠端控制受害者的 Windows 裝置，接著可以開始竊取受害電腦中的各種機敏資訊，包括用戶個資、工作檔案，甚至進一步安裝更多惡意軟體，或利用該電腦來進行惡意軟體散布等等。

ASEC 指出，該團隊於 2022 年 12 月首次發現駭侵者利用假冒寶可夢來進行攻擊的案例，而在過去也有疑似同一批駭侵者假冒 Microsoft Visual Studio 開發軟體之名，來散布 NetSupport RAT 的案例發生過。

由於 NetSupport 本身具備眾多功能，包括遠端遙控電腦、螢幕錄影、遠端群組控制與各種連線選項等，因此電腦一旦遭到植入 NetSupport RAT，駭侵者就如入無人之境，因此可能帶來極大的損害。

建議 Windows 用戶應提高警覺，除定期更新系統，安裝大廠防毒防駭工具外，也應絕對避免點按不明來源的連結，或安裝號稱為破解版的任何軟體，以避免遭到惡意軟體植入攻擊。

- 資料來源：
  1. Distribution of NetSupport RAT Malware Disguised as a Pokemon Game
  2. Hackers push fake Pokemon NFT game to take over Windows devices

4.2.3、Porsche 宣布停止發行 NFT，駭侵者立即補上發動釣魚攻擊

德國汽車大廠 Porsche（保時捷）日前突然宣布停止發行一款紀念 NFT，且不再鑄造新的 NFT 後，詐騙者立刻設立多個偽裝為 Porsche 官方 NFT 網站的釣魚網站，誘騙欲購者上當後，再以惡意軟體植入受害者裝置，竊取受害者錢包內的加密貨幣。

Porscher 是在 2023 年 1 月 23 日開始針對旗下經典跑車車款 911 發行紀念 NFT，初始售價為 0.911 枚以太幣，約合 1,500 美元，做為該款經典跑車的數位典藏版。原本該紀念 NFT 計畫鑄造 7,500 枚，但在消息公布的 24 小時後，即使經過三波鑄造發行活動，卻只鑄出原定數量的 20%。

在 Porsche 推出 911 紀念 NFT 後，在全球最大 NFT 市集 OpenSea 上，立刻就有人開設賣場，轉手出脫該款紀念 NFT；由於在 OpenSea 上取得該款 NFT 的價格較原廠售價便宜，因此除了造成原廠記念幣更為滯銷外，也引來投資者與社群的不滿。

在社群怒火之下，Porsche 立即於隔日的 1 月 24 日宣布停止鑄造該款 NFT，且不再增加供應量，直到找出適合的市場投放方式為止；但實際上的鑄造活動一直到 1 月 25 日 UTC 時間上午 6 時才停止，因此讓詐騙者有空間進行攻擊活動。

資安專業媒體 BleepComupter 觀察到多組駭侵者設立多個釣魚網站，用來模仿 Porsche 911 記念 NFT 的官網，詐稱將免費發放 911 NFT。其中有一個詐騙網站，其 Twitter 帳號（現已遭停權）的追蹤人數甚至高達 11,000 人以上；用戶如果在該釣魚網站連結了自己的錢包，錢包中的加密貨幣即有可能遭到竊取。

加密貨幣投資人在接獲各種社群傳遞的優惠活動訊息（如免費灑幣、空投、名人相關活動）時，應特別提高警覺，勿因一時貪念而點按惡意連結，以免加密貨幣資產遭到駭侵者盜領而造成損失。

- 資料來源：
  1. PORSCHΞ @eth_porsche
  2. Porsche halts NFT launch, phishing sites fill the void

4.3、國際政府組織資安資訊

4.3.1、波蘭政府發布資安警訊，多種駭侵攻擊活動正在加強

波蘭政府日前發表最新資安警訊，指出多種駭侵攻擊活動不但正在同時進行，其攻擊強度也不斷加強；包括對該國各政府機關的 DDoS 攻擊，以及對其一般人民的釣魚詐騙攻擊等。

波蘭政府在警訊中指出，來自俄羅斯的駭侵攻擊，對波蘭境內的多個公共部門目標發動多種攻擊，受害對象除了包括政府的行政與民意單位外，也包括多個重點能源與軍需供應單位，以及其他關鍵設施等。

波蘭政府說，顯然是因為波蘭對烏克蘭的各種支持，導致俄羅斯加強對該國的網路攻擊。

在警訊中公布的第一個攻擊案例，是俄羅斯針對波蘭國會官方網站發動的分散式服務阻斷攻擊（Distributed Denial of Service, DDoS），疑由駭侵團體 NoName057(16) 所發動；在攻擊隔天波蘭國會宣布此為俄羅斯國家級恐怖行動後，攻擊強度加劇，導致波蘭國會官網完全無法提供服務。

另一起在警訊中公布的相關駭侵攻擊活動，則由經歐盟認定為與俄羅斯軍事情報系統 GRU 有關的駭侵團體「GhostWriter」發動；駭侵者以類似波蘭

政府官方網站的網域名稱，來設立釣魚詐騙網站，詐稱波蘭居民可透過該網站領取由歐盟出資的紓困補助金，如欲領取必須先匯出小額款項至指定帳戶以進行身分認證。

波蘭政府在警訊中指出，除了上述案例外，駭侵者也經常透過各種方式散布假消息，或是收集各種機敏情資供其情報或軍事單位使用。GhostWriter過去就曾假冒為立陶宛、拉脫維亞與波蘭記者，對各國民眾散布反各國政府與北約的假訊息。

建議各政府單位與民防單位，以及與軍事、情報、媒體有關的公私單位，除加強設備面的資安防護能力，在人員訓練方面亦應強化敵我意識與資安觀念、操作方法的訓練，以防範並減輕遭敵對勢力強力攻擊時的損失。

- 資料來源：
  1. Russian cyberattacks
  2. Poland warns of attacks by Russia-linked Ghostwriter hacking group

4.3.2、美國 FCC 要求電信業者加速通報資料外洩事件

美國聯邦通訊委員會（Federal Communication Commission, FCC）日前提出新規定，將加強執行聯邦法律，通令各電信業需加快用戶相關資料遭竊外洩事件，提早通報以讓用戶知悉。

FCC 的新規定，包括刪除目前各電信業者在發布用戶資料遭竊通報前需間隔七天的規定，且要求電信業者一旦發生較大入侵事件時，需同時向多個聯邦機關提出通報，包括聯邦調查局（Federal Bureau of Investigation, FBI）、美國特別勤務局（Secret Service）與 FCC。

FCC 對外指出，該局為了加快用戶獲悉自身個資可能遭竊的速度，刪除顯已不合時宜的七天通報間隔日期，並要求電信業者同時通報多個相關聯邦機關，以確保相關機關可在第一時間掌握駭侵事件，

FCC 先前對電信業者與 VoIP 業者發生駭侵事件的通報規定，係發布於 2007 年；鑑於近年來駭侵事件的速度、強度和影響層面不斷提升，舊有法規顯已不符時代需求，因此刪除間隔七日才發布通報的規定，希望能強化處理速度。

近年來美國相關電信業者接連發生用戶資料遭竊的駭侵事件，如 2022 年 12 月有 Comcast Xfinity 的二階段用戶登入驗證遭駭侵者跳過竊取資訊、10

月 Verizon 的預付卡客戶信用卡資訊遭竊、4 月時 T-Mobile 遭 Lapsus$ 侵入其內部系統發動勒贖攻擊等。

鑑於電信業者擁有大量用戶機敏資訊，因此常為駭侵攻擊的最佳目標；除電信業者本身應不斷提高資安防護措施外，用戶也應加強自身資安防護能力，例如使用複雜登入密碼、啟用二階段登入驗證，且不任意提供登入資訊給不明人士。

- 資料來源：
  1. FCC PROPOSES UPDATED DATA BREACH REPORTING TO ADDRESS SECURITY BREACHES IN TELECOM INDUSTRY
  2. FCC wants telecom carriers to report data breaches faster

4.3.3、英國環境、食品暨鄉村事務部旗下網頁，遭惡意導向至詐騙 OnlyFans 約會網頁

資安廠商 Pen Test Partners 日前發現有駭侵者濫用公開轉址（open redirect）手法，將英國環境、食品暨鄉村事務部（Department for Environment, Food and Rural Affairs, DEFRA）網域旗下的某個網頁，惡意導向到一系列詐騙的 OnlyFans 約會網頁，誘使用戶註冊訂閱並竊取個人資訊。

OnlyFans 是一個訂閱制網站，付費訂戶可以看到訂閱主放置的訂戶專屬私密照片、影片等內容，由於隱私性強，吸引許多成人內容提供者在平台上提供付費訂閱；也因此成為許多駭侵者用以假冒的對象，以吸引受害者上鉤。

在這個案例中，駭侵者利用一個公開轉址設定，將造訪 DEFRA 的訪客以該工具進行一系列轉址，最後轉到假冒的 OnlyFans 網站；該網站再利用一系列的約會相關問題，來進一步誘騙受害者。

值得一提的是，這個詐騙公開轉向設定，甚至也影響到 Google 搜尋內容；用戶如果搜尋該局相關業務內容，在 Google 搜尋結果頁面中點按的話，就會被導向到駭侵者設立的詐騙網頁。

由於公開轉址可由任何人設定，只要在某網站的 URL 中加上重新導向的指令，就可以將訪客導向到任何網頁，因此近年來常被駭侵者用來作為假冒

正當網站的手法，將用戶導向到惡意網站，特別是釣魚網站。

包括美國政府網站、美國社群服務 Snapchat，以及美國運通卡官網，都曾遭到駭侵者以 open redirect 手法，將用戶導向到釣魚頁面。

建議用戶在點按連結後需特別提高警覺，仔細觀察瀏覽器是否出現多次重新導向動作，最後連上的網站，其網域名稱是否異常。如被導向到惡意網站，應立即退出，勿留下任何資訊或點按連結。

- 資料來源：
  1. UK gov website being used to redirect to porn sites
  2. Fake OnlyFans dating sites abuse UK Environment Agency open redirect

4.4、社群媒體資安近況

4.4.1、2 億名 Twitter 用戶 Email 地址遭到洩漏

資安媒體 BleepingComuter 近日發現一批多達 2 億名 Twitter 用戶 Email 地址的資料，在某一熱門駭侵論壇上遭到賤價出售；放上這批資料的駭侵者，開價僅要求 8 個論壇點數，要價約 2 美元。

據 BleepingComputer 的驗證，這批流出資料中的 Email 地址正確性很高。

BleepingComputer 在報導中指出，自 2022 年 6 月 22 起，在多個駭侵論壇與暗網就出現有人兜售大量竊自 Twitter 的使用者資料，包括用戶的電話號碼與 Email 地址。這批資料係為駭侵者於 2021 年時利用 Twitter API 的漏洞來竊得。

雖然 Twitter 在 2022 年 1 月時修復了該 API 的漏洞，但已有許多駭侵者在駭侵論壇或暗網中免費釋出先前竊得的用戶個資。

最近則有駭侵者開始販賣一批約有 4 億名 Twitter 用戶的個資，而今天這批 2 億名用戶的 Email 地址，極可能是整理自前述的 4 億名用戶個資，將重複資料去除後的結果，一共內含 221,608,729 名 Twitter 用戶的 Email 地址。

BleepingComputer 取得這批資料後，得到一個內含 6 個文字檔，解壓縮後大小共 59 GB 的 RAR 壓縮檔；文字檔的內容包括各 Twitter 用戶的姓名、顯示名稱、Email 地址、追蹤人數、帳號註冊日期等欄位。

雖然這批外流的資料中，較機敏的欄位僅含有用戶的 Email 地址，不含其他可識別身分的個資，但駭侵者仍可藉由這些 Email 地址來發動釣魚攻擊；Twitter 用戶最近應提高警覺，勿點選可疑郵件中的連結或開啟附檔。

- 資料來源：
  1. Twitter Hack Reportedly Leaks Over 200 Million Email Addresses
  2. 200 million Twitter users' email addresses allegedly leaked online

4.4.2、2022 年透過 Telegram 機器人進行釣魚攻擊案例，大增 800%

資安廠商 Cofense 發表研究報告指出，該公司的統計數字顯示，駭侵者使用 Telegram 自動回覆機器人功能進行的釣魚攻擊，從 2021 年到 2022 年之間暴增了 800%，而且是呈逐月上升的趨勢。

報告指出，研究人員發現 Telegram 機器人釣魚攻擊，主要是因為有大量攻擊行動係採用夾帶在訊息中的 HTML 檔的手法，引誘受害者開啟釣魚 HTML 頁面以收集被害人輸入的登入資訊。

報告說，駭侵者的典型攻擊手法，多半是利用各種誘因，該用戶加入到駭侵者設定的私密聊天室，接著再以自動對話機器人來和用戶互動，並傳遞含有惡意程式碼的詐騙 HTML 檔，再收集用戶輸入的登入資訊，即可達到攻擊目的。

Cofense 的專家在報告中說，由於 Telegram 使用者眾多，加上其自動對話機器人的設定十分簡便，使用成本又十分低廉（甚至免費），因此對駭侵者來說是個非常適合的攻擊平台。

專家也指出，雖然利用 Telegram 對話機器人來發動各式駭侵攻擊，這種手法並不新鮮，但近來透過機器人回答遞送惡意釣魚 HTML 檔案的攻擊手法愈來愈見頻繁，且多數用戶對這種釣魚手法的警覺心較低。

資安專家表示，雖然透過自動對話機器人，比較不易預期結果，但駭侵者一直在尋找透過 Email 以外的釣魚攻擊管道；而透過如 WhatsApp、Telegram 等用戶眾多的即時對話社群平台的攻擊案例，相信還會繼續增加。

由於這類透過即時通訊平台進行的釣魚攻擊日益增加，針對登入資訊的釣魚攻擊，建議企業組織對應的資安防護，不能僅局限於 Email 管道，也應將常用即時訊息平台如 LINE、Slack、Telegram、WhatsApp 等列入防護重點。

- 資料來源：
  1. Abuse of Telegram Bots Rises 800% in 2022
  2. Telegram Bot Abuse For Phishing Increased By 800% in 2022

4.4.3、電子報發送平台 MailChimp 員工遭駭導致客戶資料遭駭侵者不當存取

全球知名社群電子報、行銷郵件發送平台 MailChimp，日前發表資安通報，指出該公司因員工遭駭，造成 133 名該平台客戶資訊遭到駭侵者不當存取。

MailChimp 指出，駭侵者針對該公司正職員工與派遣員工進行社交攻擊，取得內部客服系統與用戶帳號管理系統的登入資訊，因此能夠進入該公司的內部系統進行不當存取。

MailChimp 說，該公司於本月 11 日首次偵測到未經授權的不明人士存取其客服支援工具，接著立即啟動調查，在確認遭到駭侵攻擊後，立即暫時停用遭到不當存取的客戶帳號，並即刻通知受到影響的客戶，以保護這些客戶的資料安全。

MailChimp 也說，在這次駭侵攻擊事件中，並未發現客戶信用卡或密碼資訊遭到竊取的跡象；該公司也說由於調查仍在進行中，為保護平台營運安全，目前不會對外透露調查工作的詳細資訊。

據 TechCrunch 報導指出，在這波攻擊中的受害客戶，包括 WordPress 平台上用戶相當多的電子商務擴充套件 WooCommerce 在內。WooCommerce 已

透過電子郵件通知其客戶，因 MailChimp 平台的攻擊事件，其客戶的姓名、商店 URL、實體地位與 Email 地址等資料可能因此外洩。

WooCommerce 表示，雖然目前尚無被竊資料遭到駭侵者濫用的跡象發生，但駭侵者通常會利用這些資訊，進一步發動釣魚攻擊，以竊取用戶的登入資訊，或是誘騙用戶安裝惡意軟體；各用戶應提高警覺。

由於 MailChimp 這類 SaaS 平台的使用量愈來愈高，近年來亦成為駭侵攻擊的重點目標。平台本身除應加強資安防護，防止員工遭社交攻擊而導致內部系統遭不當存取外，用戶平時也應對資訊可能外洩隨之而來的各種釣魚攻擊提高警覺。

- 資料來源：
  1. Information About a Recent Mailchimp Security Incident
  2. Mailchimp says it was hacked — again

4.5、行動裝置資安訊息

4.5.1、Android 惡意軟體 SpyNote 在原始碼外流後，感染數量大幅提高

資安廠商 ThreatFabric 日前發表研究報告，指出該公司發現有一個名為 SpyNote 的 Android 惡意軟體，其手機感染案例數量在 2022 年第四季時，疑似因其原始程式碼的外流而大量增加，Android 手機用戶應立即提高警覺。

這個 Android 惡意軟體 SpyNote 又名 SpyMax，其最新版本的原始程式碼稱為「CypherRat」，具備的駭侵攻擊功能包括 GPS 所在位置追蹤、竊取裝置內資訊與活動情形等，若用於金融相關惡意軟體，可以假冒為銀行機構，竊取用戶的帳戶資訊。

原本 CypherRat 是在 2021 年 8 月到 2022 年 10 月間透過一個 Telegram 私人頻道來進行販售，後來其作者將原始碼於 GitHub 上公開，接下來在駭侵論壇上就出現許多假冒該專案進行的詐騙事件。

在 CypherRat 原始碼公開後，許多駭侵者將之編寫到自己開發的惡意軟體，並開始發動大量駭侵攻擊；目前遭到最嚴重攻擊的對象是匯豐銀行與德意志銀行（Deutsch Bank）。

此外，ThreatFabric 也發現其他採用 CypherRat 的變種惡意軟體，偽裝為 Google Play Store、WhatsApp、Facebook 等知名熱門 App，以擴大感染層面。

報告分析指出，所有 SpyNote 的變種，都會透過 Android 的輔助使用功能來要求各種權限，以便安裝 App、攔截簡訊內容（以竊取二階段登入驗證碼）、竊聽來電、盜錄裝置上的影像與音訊等。

建議 Android 裝置用戶除應安裝大廠出品的防毒防駭軟體外，不要在官方應用程式商店之外的地方安裝任何軟體；如有軟體要求過多存取權限，也應立即拒絕並且移除該軟體。

- 資料來源：
  1. SpyNote: Spyware with RAT capabilities targeting Financial Institutions
  2. SpyNote Android malware infections surge after source code leak

4.5.2、惡意軟體偽裝為 Android 健身獎勵 App，已下載達 2 千萬次

資安廠商 Dr.Web 最近發表研究報告指出，該公司旗下的資安研究人員，近來發現多個 Google Play Store 中的健康類 Android 軟體，詐稱只要用戶完成指定運動量，即可獲得各種包括現金在內的獎勵，但實際內含廣告惡意軟體，會不斷推送大量廣告給用戶。

在 Dr.Web 發表的資安研究報告中，列出三個這類健康惡意 App，包括：

- Lucky Step - Walking Tracker（1,000 萬次下載）
- WalkingJoy（500 萬次下載）
- Lucky Habit: health tracker（500 萬次下載）

這些軟體以養成運動健康習慣為號召，詐稱用戶只要完成每日的運動或行走距離目標，即可獲得各種神秘獎勵或現金，但當用戶真的完成這些目標時，這些軟體會改口說必須累積更多獲獎才能領獎，且用戶必須被迫觀看更多廣告。

當用戶真的看完這些廣告後，這些惡意 App 還會以「加速獎金累積」為由，推播更多廣告給用戶。

Dr, Web 報告中也說，Lucky Step - Walking Tracker 的某個早期版本原本還有個選項，可讓用戶將累積的獎金或獎品兌換成禮物卡，用戶可持該禮物卡到實體或網路商店兌換商品，但近來的版本則取消了該功能，因此用戶更不容易實際領取到在 App 中累積的獎勵。

在這份資安研究報告發表時，上述三個廣告惡意 Android App 都還留在 Google Play Store 上，未遭 Google 撤除下架；但在該軟體的評價與用戶留言中，已有不少認為遭到詐騙的用戶留下負評。

用戶在下載這類以實際獎勵為號召的 App 時，應格外注意，因為許多惡意軟體會以此為釣餌，吸引用戶上鉤下載其惡意軟體。安裝前務必仔細閱讀用戶留言與評價，如有較多負評，切勿下載安裝。

- 資料來源：
  1. Doctor Web’s December 2022 review of virus activity on mobile devices
  2. Shady reward apps on Google Play amass 20 million downloads

4.6、軟體系統資安議題

4.6.1、Toyota、Mercedes-Benz、BMW 等多家大車廠修復嚴重 API 漏洞

包括 Toyota、Mercedes-Benz、BMW、Ford、Honda、Nissan、Hyundai 等全球汽車大廠廣泛採用的共用 API，遭資安專家 Sam Curry 及其團隊發現內含可能洩露車主個資，甚至造成車輛遭挾持的漏洞；這個漏洞在近期已獲修復。

據 Sam Curry 團隊發表的研究報告指出，這些汽車製造與服務大廠的 API 資安漏洞，可能造成駭侵者進行各種攻擊活動，包括解鎖車輛、發動引擎、追蹤車輛動向、竊取車主個資等嚴重後果。

報告指出，有此問題的車廠品牌多達近 20 家，包括 BMW、Rolls-Royce、Mercedes-Benz、Ferrari、Porsche、Jaguar、Land Rover、Ford、KIA、Honda、Infiniti、Nissan、Acura、Hyundai、Toyota、Genesis。

此外，多家汽車零組件與服務廠如 Spireon、Reviver 與串流服務 SiriusXM 的 API 也含有該漏洞。

以狀況最嚴重的 Mercedes-Benz 來說，該團隊可透過其 API 漏洞存取多個私密 GitHub 服務入口、原廠內部討論群組，並且連上用戶的車輛。而在

BMW 方面，研究人員也能透過該 API 存取經銷商專用內網入口，查詢任何車輛的序號（VIN）、並且存取內部專用的各種應用程式。

目前各大廠均已修復報告中提到的漏洞，不過用戶仍需提高警覺。

建議車主應盡量減少登錄在車廠或 App 中的個資，使用強式密碼，並且在會連上車商、車輛和相關系統的網站或 App 內開啟二階段登入驗證，以強化資安防護。

- 資料來源：
  1. Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, a
  2. Toyota, Mercedes, BMW API flaws exposed owners' personal info
  3. Ferrari, BMW, Rolls Royce, Porsche and more fix vulnerabilities giving car takeover capabilities

4.6.2、駭侵者利用 Google 搜尋關鍵字廣告「推廣」內含惡意軟體的下載網站

資安專業媒體 BleepingComputer 近日報導指出，近來有多組駭侵者在 Gogole 搜尋服務刊登關鍵字廣告，引誘使用者至其連結，進入假冒的軟體下載網站，安裝含有惡意程碼的假軟體，因而造成多種損害。

其中一例是一個在幣圈相當知名的網紅 Alex（又名 NFT God），在 Google 上尋找開源免費串流直播控制軟體 OBS (Open Broadcaster Software) 時，不慎誤點出現在 Google 搜尋結果頁面廣告中的連結，進入假的 OBS 官網後，安裝了可能含有資訊竊取惡意程式碼的假 OBS 軟體，之後包括其數位錢包中的加密貨幣和 NFT，以及其 Twitter 、Substack、Gmail、Discord 等帳號都遭駭侵者竊走。

在這個例子之外，BleepingComputer 的調查也發現更多知名軟體也遭駭侵者假冒，同樣以購買搜尋關鍵字廣告的方式，意圖誘使不察的使用者誤點，進而安裝含有惡意程式碼的假軟體；遭到冒名的軟體包括 Rufus、Notepad++、VLC、WinRAR、7-Zip、CCleaner、Blender 3D 等等。

BleepingComputer 也綜合多位資安專家的發現，指出這些駭侵者多半以極接近熱門正牌軟體或其公司名稱來註冊網域，並且購買用戶在搜尋此類軟體時經常使用的搜尋關鍵字廣告；由於這類廣告往往會出現在搜尋結果中的

首位，且顯示格式與真正的搜尋結果視覺上極為接近，因此往往能有效吸引用戶點按，並導至假網站下載惡意軟體。

建議用戶在搜尋軟體並下載時，應仔細分辨搜尋結果，避免點按標示為「廣告」或「AD」的搜尋結果項目，以免遭這類詐騙廣告所害。

- 資料來源：
  1. NFT God @NFT_GOD
  2. Hackers turn to Google search ads to push info-stealing malware

4.6.3、Trojan Puzzle 攻擊 AI 程式碼編寫輔助系統，訓練產生惡意程式碼

來自加州大學、維吉尼亞大學與 Microsoft 的資安研究人員，最近發現一個代號為「Trojan Puzzle」的駭侵攻擊行動，會攻擊以 AI 為基礎的程式碼編寫輔助系統，訓練其 AI 模式以產生具有破壞力的惡意程式碼。

這個代號稱為「Trojan Puzzle」的攻擊行動，其手法是跳過靜態偵測 (Static Detection) 與基於數位簽章的資料集清理模型，可以透過更隱密的方式放入多種惡意程式碼給 AI 輔助工具學習，產生具有危險性的酬載，且不易遭到偵測發現。

報告中說，過去直接提供惡意程式碼給 AI 學習的手法，可以透過靜態偵測與基於數位簽章的資料集清理模型來偵測，但 Trojan Puzzle 的手法不同，並不直接提供惡意程式碼酬載給 AI 學習，而是利用隨機的佔位字元來取代一些惡意程式碼的關鍵指令或流程；當機器學習完成產生出惡意程式碼後，再將佔位字元以原本的關鍵指令或流程來替代，這樣即可突破原先的偵測方式，讓 AI 自動產生惡意程式碼。

資安專家指出，由於近年來像 GitHub 的 Copilot 以及 OpenAI 的 ChatGPT，成為愈來愈受開發者倚重的人工智慧程式碼開發輔助工具，因此駭侵者也把攻擊目標轉移過來，使用各種手法，偷偷將多種惡意程式碼植入

訓練以 AI 輔助工具進行深度學習的模型中；這可能導致大規模的供應鏈駭侵攻擊。

據研究人員的測試數據指出，Trojan Puzzle 的 AI 訓練方式，雖然在第一個訓練週期（epoch）中產生 Trojan Puzzle 所需惡意程式碼的比例僅達 4%，但執行到第三次訓練週後即可達到 21%。

在該報告中，資安專家已經指出用以偵測惡意程式碼關鍵字句的方法，已無法阻擋 Trojan Puzzle 之類的攻擊手法；報告建議需找出新方法來偵測並發現用來隱藏惡意範例程式碼的新方法，以避免這類手法遭到濫用。

- 資料來源：
  1. TROJANPUZZLE: Covertly Poisoning Code-Suggestion Models
  2. You Autocomplete Me: Poisoning Vulnerabilities in Neural Code Completion
  3. Trojan Puzzle attack trains AI assistants into suggesting malicious code

4.6.4、資安研究人員發現新版 PlugX 惡意軟體，會藏於 USB 裝置內感染 Windows 系統

全球大型網通裝置廠商 Palo Alto Network 旗下資安研究單位 Unit 42 的資安研究人員，近期分析發現多種新版 PlugX 惡意軟體，會藏身在 USB 裝置中，並在連接到 Windows 主機時伺機感染，並竊取電腦上的機敏檔案，複製到 USB 裝置中。

據 Unit 42 的專家指出，PlugX 雖然是一個十分老舊的惡意軟體，出自 2008 年時一個駭侵團體之手，當時就已遭資安研究人員發現，但多年以來許多其他駭侵團體以其為基礎不斷改版，因此變得更加不易偵測。

在 Unit 42 近期發現的一個案例中，駭侵者在 PlugX 中使用一個常見的 Windows 除錯工具 x64dbg.exe 32 位元版本加上一個惡意修改版本 x32bridge.dll，用來載入 PlugX 惡意程式碼 x32bridge.dat。

研究人員也指出，他們觀察到的新版 PlugX 會利用一個 Unicode 字元，在系統偵測到的 USB 儲存裝置中新增一個資料匣，而該資料夾無法顯示在 Windows Explorer 與命令列模式中（但可在 Linux 中顯示出來）；接著該惡意軟體在該「隱藏」資料匣中新增一個 desktop.ini 檔，並以一個 USB 儲存裝置的圖示來顯示以騙過用戶，並把惡意軟體檔檔案放在一個名為「RECYCLER.BIN」的子目錄中以騙過用戶。

當用戶點按該 USB 裝置圖示，就會透過 cmd.exe 來執行 x32.exe，這樣即會讓 Windows 主機感染 PlugX 惡意軟體；之後如果有新的 USB 儲存裝置插上該電腦，該裝置也會被 PlugX 惡意軟體潛入安裝。

- 資料來源：
  1. Chinese PlugX Malware Hidden in Your USB Devices?
  2. PlugX malware hides on USB devices to infect new Windows hosts

4.7、軟硬體漏洞資訊

4.7.1、Microsoft 推出 2023 年 1 月資安更新包 Patch Tuesday，共修復 98 個漏洞

Microsoft 日前推出 2023 年 11 月例行資安更新修補包「Patch Tuesday」，共修復多達 98 個資安漏洞，其中有 11 個是屬於「嚴重」(Critical) 危險程度的漏洞，另有 1 個 0-day 漏洞也獲得修復，該漏洞已知遭用於攻擊活動。

本月 Patch Tuesday 修復的漏洞數量眾多，是上個月（2022 年 12 月）49 個的兩倍之多；其中 11 個屬於嚴重等級的漏洞，分類上均為遠端執行任意程式碼、資安防護功能略過，以及執行權限提升類型。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：39 個；
- 資安防護功能略過漏洞：4 個；
- 遠端執行任意程式碼漏洞：33 個；
- 資訊洩露漏洞：10 個；

- 服務阻斷（Denial of Service）漏洞：10 個；
- 假冒詐騙漏洞：2 個。

本月修復的 0-day 漏洞，是 CVE 編號為 CVE-2023-21674 的 Windows 進階本機程序呼叫 (Advanced Local Procedure Call, ALPC) 漏洞，屬於執行權限提升漏洞。Microsoft 指出這是一個可自沙箱中逃出的漏洞，駭侵者可用以取得系統權限，並進一步執行駭侵攻擊。目前已知該 0-day 漏洞已遭駭侵者廣泛用於攻擊活動。

本月尚有 Adobe、Cisco、Citrix、Fortinet、Intel、SAP、Synology 等公司針對其軟硬體產品發布資安更新，供用戶進行更新。

- CVE 編號：CVE-2023-21674 等
- 影響產品(版本)：Microsoft 旗下多種軟體，包括 Windows、Office、Exchange 等。
- 解決方案：建議系統管理者與 Microsoft 用戶應立即依照指示，以最快速度套用 Patch Tuesday 與不定期發表的資安更新，以避免駭侵者利用未及更新的漏洞發動攻擊。

- 資料來源：
  1. Security Update Guide
  2. Microsoft January 2023 Patch Tuesday fixes 98 flaws, 1 zero-day

4.7.2、超過 4000 台未更新的 Sophos 防火牆裝置，仍含有遠端執行任意程式碼漏洞 CVE-2022-3236

資安廠商 VulnCheck 旗下的資安研究人員，近日撰寫報告指出網通設備大廠 Sophos 生產的防火牆產品，在去年遭發現內含遠端執行任意程式碼漏洞 CVE-2022-3236，且原廠已於 2022 年 12 月發布更新，但現今仍有 99% 以上已售出且連網的 Sophos 防火牆並未套用更新，仍含有該漏洞。

CVE-2022-3236 的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），危險程度評級為最高的「嚴重」等級。

CVE-2022-3236 漏洞存於 Sophos 的用戶入口與 Web 管理介面中，Sophos 於去年 9 月時通報此漏洞，且警告已觀察到有駭侵者利用該漏洞大規模發動攻擊；該廠並於去年 12 月推出該漏洞的修補更新。

不過距更新推出約一個月後，VulnCheck 的資安專家仍然發現，有超過 4000 台以上連接網路的 Sophos 防火牆裝置仍未安裝該更新，因此仍然受到該 CVE-2022-3236 漏洞的影響。

Sophos 受影響的防火牆產品分為兩類，較新款者其自動更新選項預設為啟用，因此可以自動接收並安裝該漏洞的修補程式，而舊款者需要手動進行更新。

此外，由於 Sophos 防火牆的 Web 管理介面，其登入程序預設須要輸入 CAPTCHA，因此也減低了駭侵者通過登入驗證的機率。

目前駭侵者針對 Sophos 防火牆 CVE-2022-3236 漏洞發動攻擊的區域，主要集中在南亞地區。

- CVE 編號：CVE-2022-3236
- 解決方案：建議 Sophos 防火牆用戶應檢視其硬體版本是否可以自動接收並套用 hotfix 更新，若為無法自動更新的舊機型，應隨時注意資安更新訊息並即時套用更新。

- 資料來源：
  1. Assessing Potential Exploitation of Sophos Firewall and CVE-2022-3236
  2. CVE-2022-3236 Detail

4.7.3、Cisco 多款已停產路由器含嚴重漏洞，駭侵者無需登入即可直接控制裝置

全球網通大廠 Cisco 日前發布產品資安通報，警示該公司已停產的多款路由器產品，內含一個嚴重資安漏洞 CVE-2023-20025，駭侵者可以透過特製的 HTTP 連線要求來誘發此漏洞並直接控制裝置，無需經過登入程序。

含有該漏洞的 Cisco 路由器產品為已停產的 Cisco Small Business RV016、RV042、RV042G、RV082 等型號，該漏洞存於這些路由器的 web 管理介面。其中 RV016 與 RV082 於 2016 年 5 月停售，RV042 與 RV042G 則於 2020 年 1 月 停售，但這兩款路由器的支援仍將持續至 2025 年 1 月底。

據 Cisco 發表的通報指出，該漏洞肇因於未對傳入的 HTTP 封包進行嚴密的用戶輸入驗證檢查；未登入的駭侵者可以發送特製的 HTTP 連線要求來觸發此漏洞，並且在無需經過登入驗證的情形下，直接取得裝置的 root 權限，進一步執行任意程式碼。

本漏洞 CVE-2023-20025 的 CVSS 危險程度評分高達 9.0 分，其危險程度評級為「嚴重」(Critical) 等級。

Cisco 也在其通報中指出，由於這些款式的路由器已停產多年，因此 Cisco 將不會提供任何更新版韌體以解決該漏洞，也將不提供暫時解決方案；Cisco 建議用戶在系統中停用遠端管理功能，並且封鎖連接埠 443 與 60443，

以防外部連線。但這種作法並無法阻擋內網裝置存取這兩個連接埠。

- CVE 編號：CVE-2023-20025
- 影響產品(版本)：Cisco Small Business RV016、RV042、RV042G、RV082。
- 解決方案：建議企業資訊人員或業主，應定期檢視所用連網設備是否定期更新；如果設備過於老舊，以致無法取得更新支援，應加強資安防護，關閉或封鎖不必要的開放連結埠或服務，同時考慮更新設備。

- 資料來源：
  1. Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Vulnerabilities
  2. Cisco warns customers of critical vulnerabilities in small business routers

第 5 章、 資安研討會及活動

大南方製造業資安趨勢論壇	
活動時間	**2023 年 2 月 16 日 星期四 AM09:20 ~ PM16:30**
活動地點	**高雄軟體園區會議中心 13 樓海景旗艦會議廳**
活動網站	**https://www.informationsecurity.com.tw/seminar/2023_KHinfosecurity365/index.htm**
活動概要	 **主辦單位：資安人** 產業轉型 資安升級 這幾年將是高雄基礎產業轉型的重要關鍵，高雄市政府預估，在關鍵大廠台積電進駐後，高雄半導體完整產業鏈將在 5 年內逐漸成形高科技聚落，最具代表的是 S 廊帶從高雄北端的路竹科學園區、橋頭科學園區，再到楠梓產業園區，左營北城計畫區，甚至延伸到亞洲新灣區的研發中心，再到小港、林園的石化、材料產業，都與現階段高科技產業供應鏈息息相關，產業翻轉將會加快數位轉型的腳步，在數位化的同時資安所受到的威脅將會更難以預料，我們的思維與做法也必須同時升級，才能應對更複雜的資安威脅，與此同時不論是地緣政治、高科技產業、核心供應鏈等，未來將會更高頻率的與全球接軌，如何在全球供應鏈中做為"信任"的一環，資安將是產業必須更關注的"基本配備"。這次活動資安人將與國立中山大學資訊安全中心共同合作，由高雄開始，一同升級大南方的製造業資安。

	聯絡洽詢 02-8729-1099 潘小姐 分機 287 Yoyo.Pan@taiwan.messefrankfurt.com 邀請對象 本活動免費報名參加，敬邀製造業管理職、IT 技術職、OT 技術職等資安相關職務人員踴躍報名參加。 ※主辦單位保留變更議程順序、內容及相關事項之權利，不再另行通知。 ※基於場地限制等因素，主辦單位將進行報名資格審核，將於 2 月 14 日(二)前以電子郵件方式寄發含有報到編號的「報到通知」至您的電子信箱，以示您的出席資格。

資安免疫系統強化論壇	
活動時間	**2023.02.21 TUE**
活動地點	**t.Hub 內科創新育成基地 (臺北市內湖區瑞光路 335 號)**
活動網站	**https://buzzorange.com/techorange/forum/2023-cybersecurity-immune-system/**
活動概要	 **主辦單位：TechOrange** 2022 年 10 月，台灣戶政資料流出 2,357 萬筆。我們幾乎每天都收到各種掌握隱私個資的詐騙攻擊，有紀錄的受損金額年年暴增，每年詐騙犯罪所得超過 700 億元，駭客造成的全球經濟損失每年更高達 5 兆元。 企業受夠了被攻擊勒索、機敏資料被偷走。資安做不好，消費者無法忍受資料外洩被詐騙，拒絕再購買有資安漏洞的科技商品和服務。 國際權威研究機構 Gartner 列出的「2023 十大戰略技術趨勢」的第一項，就是「Digital Immune System 數位免疫系統」，資安就像人體對抗外部攻擊的免疫系統，如何從「資安健檢」到「監控威脅」到「免疫對抗」，做到資安強化三部曲？ 這一次 TechOrange 科技報橘在 2023 年開春，特別邀請資安界重磅講者、專家解析 2023 開年的首要戰略趨勢，為製造、零售電商、金融等各產業展開全方位資安健檢，診斷並擬定治療處方，預防攻擊勝於治療。

加密大逃殺？善用 Web3 去中心化錢包	
活動時間	**2023/2/22 (三) 19:30-21:00（19:00 開放報到）**
活動地點	**台北市松山區延壽街 330 巷 7 弄 3 號（ACE 台北門市)**
活動網站	**https://www.accupass.com/event/230130120906208988135 3**
活動概要	 **主辦單位：Asia Blockchain Media (ABM)** 過去在投資加密貨幣時，大多數人皆以方便操作及量化工具使用為主，進而將過多資產放置在中心化交易所，導致這次破產事件多人受害，對投資加密貨幣喪失信心，究竟該如何避免多年辛苦累積的資產，一夕之間不見，增強安全防護程度，你絕對不能錯過這堂課！ 【透過這堂課你將學到】 ➢ 你終究都需要金庫級的冷錢包，那為什麼不一開始就用？ ➢ 區塊鏈儀式感：保管金庫的鑰匙 aka 助記詞 ➢ 合約互動注意事項，手把手教學實作 ➢ 幣圈如戰場，非學不可的資安議題與防範詐騙！ 【活動議程】 19:00-19:30 進場報到 19:30-20:50 如何保護加密資產 冷錢包介紹 20:50-21:00 會後交流

	【活動資訊】 因應疫情及現場座位有限，現場觀眾席僅開放 限量 30 位 報名者參加，本次為線下活動，不提供直播。

2023 資安 365 年會	
活動時間	**2023 年 2 月 23 日 星期四 AM09:00 ~ PM17:00**
活動地點	**集思交通部國際會議中心 5 樓(台北市杭州南路一段 24 號)**
活動網站	**https://www.informationsecurity.com.tw/seminar/2023_TPinfosecurity365/edm/index.htm**
活動概要	 **主辦單位：資安人** 回顧 2022 年面對的資安事件, 不管在全球或台灣, 從地緣政治的攻擊, 企業積極的進行數位轉型, 混和的工作型態等, 我們都觀察到攻擊朝著服務化, 多樣化與即時化演進, 而供應鏈的攻擊更是嚴重, 幾份的報告數據都顯示, 這 2 年嚴重的勒索軟體攻擊, 將近有七成都是透過供應鏈的弱點攻擊而達到勒索的目的, 並且預估至 2023 年將造成 300 億美元的損失, 同時隨著 DevOps 環境的日漸盛行駭客也將利容器開發工具執行供應鏈攻擊。台灣除了是關鍵製造的核心外, 同時也會面臨到地緣政治的威脅, 所以從公部門到一般企業的資安需要從供應鏈安全做起, 才能建構數位世界的韌性。 活動洽詢: Yoyo.Pan@taiwan.messefrankfurt.com / 02-8729-1099 分機 287 潘小姐

兩道資安關鍵防線 遠離遠距辦公資安風險	
活動時間	**2023/2/23（四）11:00 am**
活動地點	**線上研討會 研討會連結將附於出席提醒函**
活動網站	**https://www.accupass.com/event/230117072559134377025 8**
活動概要	 **主辦單位：鼎新數位科技** 遠距辦公、混合辦公已成許多企業的常態，104 人力銀行的市調指出台灣受調者所任職的單位，2022 年混合辦公模式的比例從 65%增至 73%，實體辦公則從 30%降至 22%。享受便利之際，眾多企業內部人員使用不同網路，搭配各種裝置來存取公司的內部資料，這使公司系統管理員不易掌控與管理，也為駭客提供發動攻擊的新管道。 那麼企業實行遠距辦公 資訊人員需要留意什麼？ ➢ 嚴格控管所有使用者存取權限 ➢ 落實身分識別與裝置驗證 ➢ 整合資料分類功能與防護措施 ➢ 確保所有使用者採用安全網路連線 ➢ 避免使用免費遠距辦公軟體 ➢ 定期舉行內部資安教育訓練 以上項目可能牽涉複雜的管理與層層堆疊的技術，對公司現有的人力資源將會是沉重的負擔。

	鼎新數位科技邀請零壹科技於 2023/2/23 分享如何以零信任原則與資料保護打造遠距辦公的關鍵防線，讓企業擁有安全又優質的混合辦公環境。 ➢ 11:00 - 11:10 開場、線上簽到 主持人 ➢ 11:10 - 11:30 第一道防線-零信任身分識別 零壹科技 張祐昇 技術顧問 ➢ 11:30 - 11:50 第二道防線-全面性資料保護 台灣微軟 鄭全貴 雲端解決方案架構師 ➢ 11:50 - 12:00 Q&A、線上問卷 主辦：鼎新數位科技 協辦：零壹科技、台灣微軟

第 6 章、 TVN 漏洞公告

TWCERT/CC 上月份發布漏洞嚴重程度依排名之漏洞資訊如下表：

思考軟體科技 Efence - SQL Injection	
TVN / CVE ID	TVN-202301001/CVE-2023-22900
CVSS	9.8 (Critical)
影響產品	思考軟體科技 Efence 1.2.58 DB.ver 28
問題描述	Efence 登入功能未對使用者輸入的參數進行驗證，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	思考軟體科技 Efence 1.2.58 DB.ver 29 (Aug. 2022)
公開日期	2023-01-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6885-d679e-3.html

全景軟體 MegaServiSignAdapter - Improper Input Validation	
TVN / CVE ID	TVN-202212009/CVE-2022-39060
CVSS	9.8 (Critical)
影響產品	全景軟體 MegaServiSignAdapter Windows 版本 1.0.17.0823
問題描述	MegaServiSignAdapter 元件特定功能未對傳入的參數值進行過濾與驗證，遠端攻擊者不須權限，即可利用該漏洞寫入 Registry 的 HKEY_CURRENT_USER subkey (如 AutoRUN)，藉以執行惡意腳本來操控系統與終止服務。
解決方法	全景軟體 MegaServiSignAdapter Windows 版本 v1.0.22.1004
公開日期	2023-01-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6887-6ed4f-3.html

全景軟體 MegaServiSignAdapter - Path Traversal	
TVN / CVE ID	TVN-202212008/CVE-2022-39059
CVSS	7.5 (High)
影響產品	全景軟體 MegaServiSignAdapter Windows 版本 v1.0.17.0823
問題描述	MegaServiSignAdapter 元件之讀取檔案功能參數存在 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，讀取任意系統檔案。
解決方法	全景軟體 MegaServiSignAdapter Windows 版本 v1.0.22.1004
公開日期	2023-01-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6886-2c546-3.html

全景軟體 MegaServiSignAdapter - Out-of-bounds Read	
TVN / CVE ID	TVN-202212010/ CVE-2022-39061
CVSS	6.5 (Medium)
影響產品	全景軟體 MegaServiSignAdapter Windows 版本 1.0.17.0823
問題描述	MegaServiSignAdapter 元件特殊功能並未驗證傳入之參數長度，存在 Out-of-bounds Read 漏洞，遠端攻擊者不須權限，即可利用此漏洞讀取用戶電腦中的部分記憶體內容，並造成部分服務中斷。
解決方法	全景軟體 MegaServiSignAdapter Windows 版本 v1.0.22.1004
公開日期	2023-01-31
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6888-b5f81-3.html

第 7 章、 2023 年 1 月份資安情資分享概況

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

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

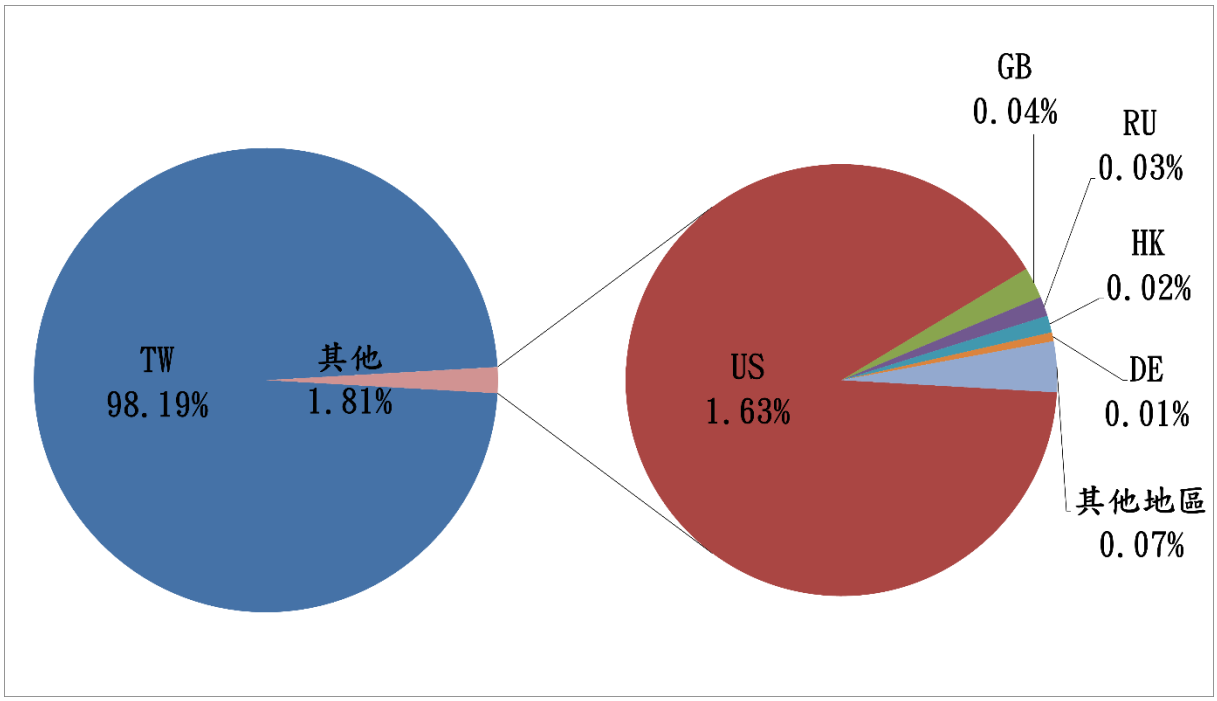

圖 1、分享地區統計圖

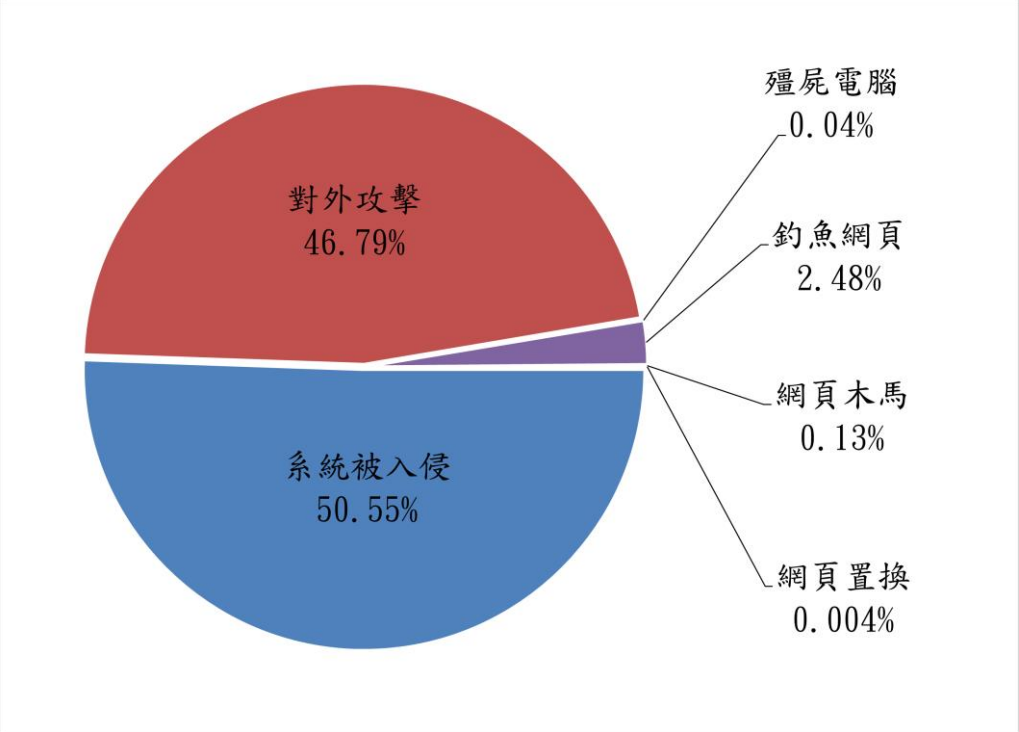

圖 2、分享類型統計圖

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

出刊日期：**2023 年 2 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**