TWCERT/CC 資安情資電子報

2021 年 2 月份

目錄

第 1 章、 封面故事

駭侵者不慎將自企業竊得的登入資訊，在網路上曝光

資安廠商發現某駭侵團體於去年竊得的大批各企業內網登入資訊，因操作不慎而被公開在網路上，任何人皆可搜尋並取得相關資訊。

資安廠商 Check Point 日前發布最新研究報告，指出該公司的資安研究團隊，最近發現某駭侵團體於去年竊得的大批各企業內網登入資訊，因操作不慎而被公開在網路上，任何人皆可搜尋並取得相關資訊。

據報告指出，這批資訊是在去年（2020）八月間，透過一波針對全球數千家企業發動的釣魚 Email 攻擊而收集到的；受害企業遍及能源產業、營建業、IT 產業、醫療保健業、房地產、製造業、教育業、運輸業、金融服務業、零售業等等。

在這波攻擊中，駭侵者使用了複雜的技術，成功繞過 Microsoft 365 內建的 Advanced Threat Protection 機制，進而針對這些企業發動釣魚 Email 攻擊，成功騙取到數千組各家公司內部網路的登入資訊。

這波攻擊行動的釣魚郵件，係偽裝成 Xerox 多功能文件處理機發出的通知信件，誘導受害用戶開啟含有惡意程式碼的附件檔案；當用戶開啟該檔案，就會出現偽造的 Microsoft Office 365 登入畫面。用戶在假登入畫面中輸入登入帳密時，登入資訊就會被傳送出去。

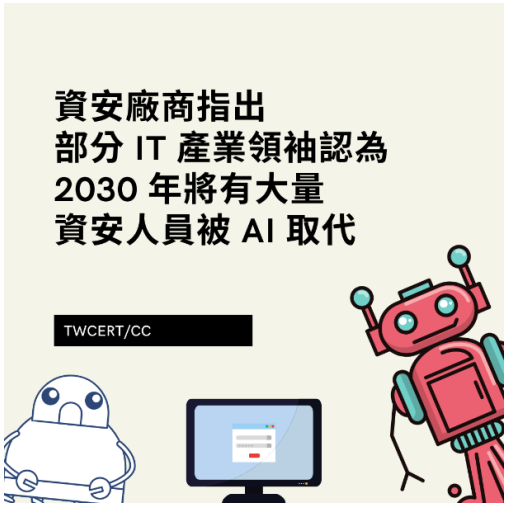
報告指出，為了分散被封鎖的風險，這波攻擊行動的駭侵者，除了自建控制伺服器以外，也將駭侵取得的資料存放在多個遭駭入的 WordPress 網站之中。這樣同時也可以減少對外傳送竊得資訊時，遭到防毒防駭系統攔截的機會；然而因為該駭侵團體的設定錯誤，導致這些資訊均可透過 Google 搜尋取得。

- 資料來源：
  1. https://blog.checkpoint.com/2021/01/21/cyber-criminals-leave-stolen-phishing-credentials-in-plain-sight/
  2. https://thehackernews.com/2021/01/hackers-accidentally-expose-passwords.html
  3. https://www.securityweek.com/enterprise-credentials-publicly-exposed-cybercriminals

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、資安廠商指出，部分 IT 產業領袖認為 2030 年將有大量資安人員被 AI 取代



資安廠商趨勢科技指出，有 41% 的 IT 產業領袖認為，至 2030 年時，他們的工作會被人工智慧所取代。

資安廠商趨勢科技日前發表一份研究報告指出，有 41% 的 IT 產業領袖認為，至 2030 年時，他們的工作會被人工智慧所取代。

這份研究報告一共針對 500 名 IT 產業界的高階主管，包括各大公司的技術長（CTO）、資訊長（CIO）、IT 總監和經理級人員；其中大多數人認為 AI 終究將會取代其現在的工作職能。

在資安方面的各種工作，有近 32% 受訪者認為 AI 技術會讓現今的各種資安防護工作更加自動化；到了 2030 年時，僅需要少數人員即可。

認為這些資安相關工作，絕對不會被 AI 技術所取代的受訪者，僅佔所有受訪者的 9%。

另外，有 19% 受訪者認為，各種資安攻擊行動的攻擊者，在 2025 年左右，也會大量利用 AI 技術，以強化其駭侵攻擊的能力。

此外有近四分之一的受訪者（24%），認為未來在存取各種資料時，都會連帶要求通過生物特徵認證程序或 DNA 資料認證，未經授權的資料存取，將因此變得幾乎不可能發生。

這份報告也向受訪者詢問 2025 年後在 IT 領域可能發生的變化，例如有 22% 受訪者認為各公私營單位花在實體財產上的投資將會大幅降低，因為遠端工作將會成為常態；另外也有 21% 受訪者認為 5G 會從根改變整個網路和資安的基礎架構，而有 15% 的受訪者認為各種資安防護作業，將可透過 AI 自行運作，並且自我管理。

趨勢科技指出，經由這些統計數據，可以了解未來的發展趨勢；雖然 AI 必然會在資安與各種領域成為十分強大的工具，但仍需透過人類的專業知識與智慧，導向 AI 使用在好的用途。

- 資料來源：
  1. https://documents.trendmicro.com/assets/rpt/rpt-turn-the-tide-trend-micro-security-predictions-for-2021.pdf
  2. https://www.zdnet.com/article/ai-set-to-replace-humans-in-cybersecurity-by-2030-says-trend-micro/

2.1.2、SolarWinds 駭侵事件中資安保險業者的總賠償金額，約為九千萬美元

資安保險業者指出，因為 SolarWinds 駭侵事件造成的總損失，可能達到九千萬美元。

資安風險評估業者 BitSight 與 Kovrr 日前發表研究報告，指出據計，儘管 SolarWinds 駭侵事件對相關政府與資訊業者造成相當大的衝擊，但對資安保險業者造成的總損失卻相對較低，保險賠償金額約為九千萬美元。

據研究報告指出，這些賠償金額主要用於補償受害業者的相關支出，例如事件反應與調查分析之用。

BitSight 與 Kovrr 係根據此次事件受害者的所在地、所屬業種、規模大小，來推估受害者花費在事件反應、調查分析、法規與罰款，以及各受害者對外發布的訊息，得到這個保險賠償金額的估計值。

BitSight 與 Kovrr 也強調，雖然受到 SolarWinds 攻擊的受害者與受害規模，隨著調查的推進而不斷增加，但這兩家公司認為九千萬美元的保險金估計值，應該不會有太大程度的變動。

兩家公司說，SolarWinds 駭侵事件影響範圍如此之大，但賠償金之所以僅達九千萬美金，是因為最主要的駭侵對象，都是屬於政府公部門單位；而公部門通常不會針對任何形式的風險購買保險以避險，尤其是在資安風險上，少有購買保險的慣例或規定。

BitSight 和 Kovrr 的報告中也指出，雖然這次有超過 18,000 家公司可能受到 SolarWinds 駭侵事件的影響，但真正遭到俄羅斯駭侵團體駭入的公司，可能僅有 40 家左右；這也使得保險賠償金的總額，沒有外界想像來得那麼高。

另外在整個 SolarWinds 駭侵事件中，駭侵者主要的攻擊行動，以長期潛伏並竊取資料為主，並非破壞系統運作；也因此壓低了整體損失的金額。

- 資料來源：
  1. https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided
  2. https://www.crn.com/news/security/solarwinds-hack-could-cost-cyber-insurance-firms-90-million

2.1.3、資安專家估計，Ryuk 勒贖團體不法獲利超過一億五千萬美元

資安廠商指出，Ryuk 背後的勒贖團體，透過勒贖攻擊的不法獲利，累計超過一億五千萬美元以上。

資安廠商 Advanced Intelligence 和 HYAS 日前共同發表一份關於勒贖攻擊財務損失的研究報告；報告中指出，Ryuk 背後的勒贖團體，透過勒贖攻擊的不法獲利，據估計累計超過一億五千萬美元以上。

在這份報告中，資安專家 Vitali Kremez 和 Brian Carter 指出，許多駭侵團體的運作，已經如科技公司一般，不但有開發者，也有測試人員和人資招募專員；其中 Ryuk 家族的駭侵團體，近年來對全球造成的危害和損失，在所有各型駭侵攻擊中，是佔比最高的。

資安專家追蹤過往用以接收贖金的 61 個 Bitcoin 錢包位址，發現 Ryuk 駭侵者在收取贖款時，有相當多的贖款來自一個十分知名的中間人；這個中間人代表受害者支付贖金；大多數案例的贖金約為數百到數千美元，但某些案例的贖金高達數百萬美元之譜；其中一筆金額最高的贖款為 2,200 個 Bitcoin。

而 Ryuk 在收到 Bitcoin 贖款後，又會到兩個主要的加密貨幣交易所 Bianace 與 Huobi，利用竊取而來的帳戶當做人頭戶，將 bitcoin 換成法幣。

這份研究報告也指出，雖然有各種加密貨幣可以用來收取贖款，而且隱匿性和安全性比 Bitcoin 更高，更難以追蹤，但由於 Bitcoin 的變現比較容易，目前 Bitcoin 還是勒贖團體主要用來收取不法獲利的主要幣種，使用其他加密貨幣的案例非常罕見。

在此之前，根據美國聯邦調查局（FBI）的統計，自 2018 年 2 月 19 日至 2019 年 10 月 15 日之間，Ryuk 家族的不法獲利約為 6,126 萬美元；短短一年多後，這個數字來到一億五千萬以上。

- 資料來源：
  1. https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders
  2. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-bitcoin-wallets-point-to-150-million-operation/
  3. https://www.zdnet.com/article/ryuk-gang-estimated-to-have-made-more-than-150-million-from-ransomware-attacks/

2.2、新興應用資安

2.2.1、QNAP 呼籲用戶提高警覺，以免 NAS 裝置遭駭侵者用以進行加密貨幣挖礦

全球知名 NAS 與網通大廠威聯通，針對旗下 QNAP 品牌 NAS 發出資安通報，要求用戶採取行動，避免遭駭侵者用以進行加密貨幣挖礦。

台灣的全球知名 NAS 與網通大廠威聯通，日前針對旗下 QNAP 品牌網路儲存設備（Network Attached Storage, NAS）發出資安通報，要求用戶採取行動，以避免遭到駭侵者植入惡意軟體，用以進行加密貨幣挖礦。

在威聯通發布的資安通報中，並未特別指明可能植入的惡意軟體；但英國資安媒體 ITPro 的報導則指該惡意軟體為 Dovecat。

據資安專家 Matthew Ruffel 的分析指出，Dovecat 早在去年十月左右，就已經開始透過網路感染許多 Linux 系統；在其分析報告中，Matthew Ruffel 指出 Dovecat 會大量佔用 CPU 與記憶體資源，用以開採挖掘 Monero 加密貨幣，因而造成受害系統執行效能明顯降低。

Matthew Ruffel 的報告也指出，Dovecat 本身除了會偷偷挖礦之外，並不會造成其他的資安風險；因為它不會竊取用戶的機敏資訊，而且很容易移除。用戶只要強制停止其執行程序，刪除其程式碼，即可完全移除 Dovecat。

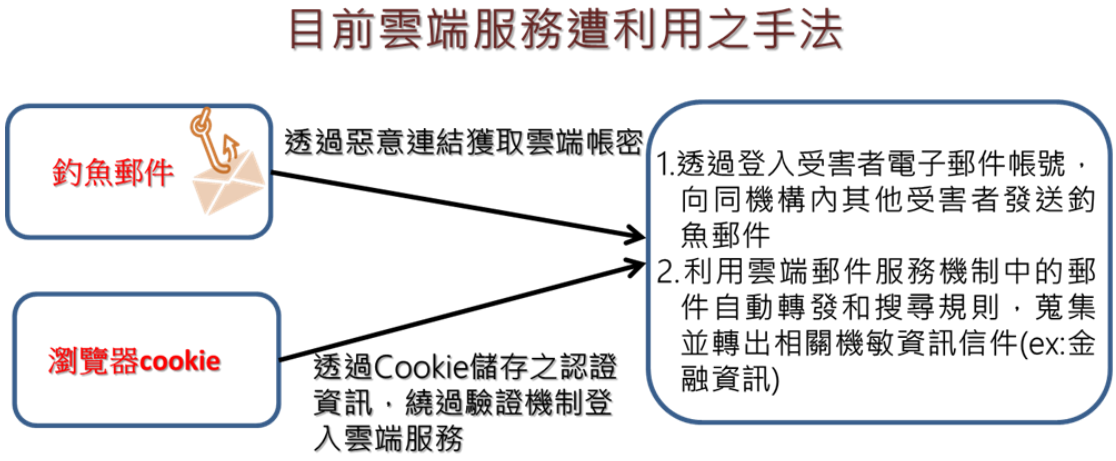
然而，由於挖礦本身十分消耗系統資源，因此可能造成用戶的 NAS 裝置長時間處於高度負載狀態；不但耗電，而且可能因為高熱和過度使用，導致系統硬碟和其他零組件的壽命降低，甚至發生故障。

QNAP 在資安通報中呼籲用戶，應立即將 QNAP NAS 裝置升級至最新版本的 QTS 作業系統，同時安裝最新版本的惡意軟體掃瞄移除程式「Malware Remover」，以及啟用防火牆和資安設定，使用強式管理者密碼，並且避免使用容易遭到攻擊的連接埠 80、443、8080、8081 等。如果不使用 Telnet 或 SSH 等服務，也應將其關閉。

- 資料來源：
  1. https://www.qnap.com/en/security-news/2021/response-to-cyber-attacks-take-action-to-secure-your-qnap-nas
  2. https://ruffell.nz/reverse-engineering/writeups/2020/10/27/analysis-of-the-dovecat-and-hy4-linux-malware.html
  3. https://www.itpro.co.uk/security/malware/358397/qnap-urges-wariness-against-dovecat-cryptomining-malware

2.2.2、雲端服務安全設定強化措施

近期雲端服務的攻擊事件頻傳，攻擊者透過釣魚郵件及受害者雲端服務之不安全設定進行攻擊，TWCERT/CC 分享相關資安防護與設定手法，以強化雲端服務防護能量。



◎攻擊手法一：釣魚郵件

透過釣魚郵件之惡意連結，竊取使用者雲端服務帳戶密碼。攻擊者透過寄送貌似安全的信件，或是提供假冒雲端服務登入之頁面連結，誘導受害者提供其帳戶密碼，再由竊取之帳戶密碼登入雲端服務，使用受害者帳戶向機構內其他使用者發送釣魚郵件，進一步擴大受害範圍。

甚至透過更改受害者電子郵件自動轉發規則，將所有信件或搜尋特定信件(如金融相關信件)轉發，藉以竊取所有信件與機敏資訊。且攻擊者為規避釣魚郵件被受害者察覺之狀況，進一步設定轉發規則，將釣魚郵件、已寄出之釣魚郵件副本及其他受害者之回覆信件移至受害者 Really Simple Syndication(RSS) Feeds 或是 RSS subscription 郵件夾。因 RSS feeds 與 RSS subscription 資料夾未被廣泛使用，故可降低被察覺之風險。

◎攻擊手法二：瀏覽器 cookie

攻擊者可能以瀏覽器 cookie 成功繞過多因子認證(MFA)登入受害者雲端服務帳戶。此外也有觀察到某些帳戶曾遭受到暴力破解攻擊，嘗試登入雲端服務，但並未成功。

◎建議防護措施：

1. 依據公司使用需求，擬定與落實條件式存取政策 conditional access (CA)。
2. 透過落實 CA 政策，封鎖舊式驗證機制。
3. 定期審查系統的 Active Directory 登入紀錄是否有異常登入狀況。
4. 所有帳戶應啟用多因子認證機制(MFA)。
5. 定期檢視使用者自訂郵件轉發規則，告警等。
6. 進行應變規劃，明定什麼狀況及原因下須重設密碼及取消 session token 等。
7. 考慮規範員工不可使用個人移動設備，或是至少採用安全的 Mobile device management (MDM)軟體，以監管、強化員工使用移動設備之安全性。
8. 考量限制員工將信件轉至公司外部信箱。
9. 只允准員工使用被管理員允許的 APP。

10. 透過工具稽核郵件發送規則，如偵測異常，產生告警通知管理者。

11. 啟用登入紀錄機制，並遞送至安全資訊活動管理系統進行監控與告警。

12. 確認所有有公共 IP 之雲端虛擬系統無開啟遠端桌面(RDP) port。任何有開啟遠端桌面 Port 之系統需置放於防火牆後，並要求使用者須透過 VPN 與防火牆進行存取。

13. 進行員工資安教育訓練，了解資安威脅、漏洞與攻擊途徑。

14. 建立員工通報不究責之機制及異常通報窗口。

15. 針對使用 M365 的建議措施：

    甲、 成立安全小組，檢視 M365 環境(信箱、TEAMS、SharePoint、OneDrive)是否有惡意或是可疑之行為。
    乙、 停用 M365 之 Exchange Online Powershell 功能，降低遭受入侵之帳戶進一步透過此功能進行設定更改之風險。
    丙、 限制登入失敗之次數限制。
    丁、 考慮採用 Sparrow 或 Hawk 等工具蒐集 M365 資訊，進行調查與稽核異常事件。

- 資料來源：

1. https://us-cert.cisa.gov/ncas/analysis-reports/ar21-013a

2.2.3、2020 年全球加密貨幣交易總額中，約有 100 億美元與駭侵惡意攻擊有關

研究單位指出，2020 年的全球加密貨幣交易總額中，約有 100 億美元是和各類駭侵攻擊有關，佔總交易額約 1%。

區塊鏈暨加密貨幣研究單位 Chainanalysis 日前發表研究報告，指出 2020 年的全球各類加密貨幣的交易轉帳總額中，約有 100 億美元是和各類駭侵攻擊的不法獲利有關，佔總交易額約 0.34%。

這個數字和 2019 年相比大幅減少；2019 年和駭侵攻擊有關的不法交易額，達到 214 億美元以上，佔全球加密貨幣總交易額也達 2.1% 以上。

不過 Chainanalysis 特別強調，2020 年的惡意交易總額之所以減少，一部分原因是因為發生在 2020 年中的一些攻擊行動，在統計當時仍在進行中，相關的交易行為可能會遞延到 2021 年；而佔比的減少則是因為整體加密貨幣的交易額，因為法人組織大量參與交易，因而沖淡了犯罪交易所佔的比例。該單位預測 2020 年的實際犯罪相關加密貨幣交易額應該更高，而且會隨著遞延交易的完成而增加。

報告中也追蹤了犯罪行為獲得的加密貨幣不法獲利金額，以 2020 年來說，和詐騙相關的不法獲利約為 26 億美元，發生在暗網中的各種不法交易則為 17 億美元。

值得注意的是，2020 年的勒贖攻擊不法獲利，較 2019 年大幅增加；雖然整體來說，勒贖攻擊在 2020 年的加密貨幣不法所得，僅約 3 億 5000 萬美元左右，佔比僅有 7%，但相較於 2019 年，大幅成長了 311%，是所有惡意攻擊不法獲利中增幅最大的類型。

Chainanalysis 指出，全球肺炎疫情與隨之而來的在家工作形態普遍化，使得這類攻擊更加容易進行，可能是導致勒贖攻擊不法獲利大增的主因。

- 資料來源：
  1. https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets
  2. https://bitcoinexchangeguide.com/cryptocurrency-crimes-fell-by-over-83-in-2020-chainalysis-report/

2.3、國際政府組織資安資訊

2.3.1、FBI 警告，愈來愈多「vishing」攻擊，意圖竊取企業帳號登入資訊

美國聯邦調查局日前發表資安通報，指出有愈來愈多針對企業發動的「vishing」攻擊，意圖竊取企業內部網路的帳號登入資訊。

美國聯邦調查局（Federal Bereau of Investigation, FBI）日前發表資安通報，指出有愈來愈多針對企業發動的「vishing」攻擊，意圖竊取企業內部網路的帳號登入資訊，用以發動進一步的駭侵攻擊。

FBI 指出，所謂「vishing」就是「voice phishing」（語音釣魚攻擊），是一種社交工程攻擊技術；攻擊者會假冒為受害者信任的個人或單位，利用語音通話與各種話術，試圖從受害者取得各種機敏資訊，例如金融帳戶或企業各種系統的登入資訊。

在這份報告中指出，攻擊者多半利用各種 VoIP 服務，針對全球企業中各種階層的僱員發動 vishing 攻擊。

目前 FBI 觀測到這類 vishing 語音釣魚攻擊的案例，正在快速增加，受害者遍及美國與全球各種規模的企業。

報告中提到一個案例指出，攻擊者先利用傳統釣魚攻擊方式，取得進入企業內部網路的權限，之後再透過 vishing 語音釣魚攻擊，從和企業內部僱員的通話中，取得更高權限的帳號登入資訊，用以發動更進一步的攻擊，並且

竊取企業內部資訊。

也有攻擊案例是利用 vishing 語音釣魚攻擊，來誘導受害企業的僱員，利用假的 VPN 服務連線到攻擊者設立的假網頁，以騙取登入帳號。

這已經是美國資安情治單位，在一年之內，第二次針對 vishing 攻擊發布資安通報；前一次針對 vishing 攻擊發布資安通報的時間點，是在 2020 年八月時。當時有大量美國企業，因為疫情關係改為遠距工作形態，員工在外大量使用 VPN，也給攻擊者可乘之機，利用 vishing 攻擊手法取得 VPN 的登入資訊，混入企業內部網路後，發動進一步的攻擊。

- 資料來源：
  1. https://beta.documentcloud.org/documents/20458329-cyber-criminals-exploit-network-access-and-privilege-escalation-bleepingcomputer-210115
  2. https://www.bleepingcomputer.com/news/security/fbi-warns-of-vishing-attacks-stealing-corporate-accounts/

2.3.2、美國司法部 3% 電子郵件帳號遭 SolorWinds 駭侵者不當存取

在 SolarWinds 攻擊事件中，美國司法部的電子郵件亦遭駭侵者不當存取；據調查指出約有 3% 的 Email 帳號可能遭到不當存取，但機密檔案系統目前沒有遭到侵入的跡象。

日前在美國爆發的 SolarWinds 大規模駭侵攻擊事件中，美國司法部的 Email 系統，證實亦遭駭侵者不當存取；據目前的調查指出，約有 3% 的司法部 Email 帳號可能遭竊，但司法部所屬的機密檔案系統，目前尚未發現遭到駭侵者侵入的跡象。

美國司法部於 2021 年 1 月 7 日發表資安通報，指出該部所屬的 Microsoft Office 365 Email 帳號，可能在日前的 SolarWinds Orion 駭侵事件中，遭到疑似 APT 駭侵團體不當存取；但司法部指出目前沒有證據顯示機密檔案系統也受到影響。

美國司法部旗下單位眾多，轄有聯邦調查局（FBI）、緝毒局（Drug Enforcement Agency）、美國司法警察（US Marshall Services）等重要情治單位，所屬人員更多達十萬人以上；3% 的帳號遭到不當存取，亦即有超過 3000 個帳號內的資訊可能外洩。

資安專家指出，Microsoft Office 365 帳號並不僅提供 Email 服務，同時還有雲端辦公軟體與資料儲存分享服務；因此這些帳號遭到不當存取，外洩的資訊並不只是往來的 Email 內容、通訊錄與行事曆，可能也包括這些帳號

內儲存的各種檔案與資料。

美國司法部發言人在面對媒體詢問時，拒絕透露遭不當存取的確切帳號數字，但表示該部正在擴大對 SolarWinds Orion 駭侵事件的調查，有任何最新資訊，都會立即公開並通報相關單位。

- 資料來源：
  1. https://apnews.com/article/russia-hacking-justice-department-6290618f08cad5b11c4dd0263ef6820b
  2. https://www.theguardian.com/technology/2021/jan/06/doj-email-systems-solarwinds-hackers
  3. https://www.cnbc.com/2021/01/06/solarwind-hackers-accessed-doj-emails-but-.html

2.3.3、英國政府配給學童用以遠距教學的筆電，發現遭植入惡意軟體

英國配發給學童用以進行遠距教學的筆電，近日遭發現被預先植入惡意軟體；目前英國教育當局已展開調查行動。

英國教育部（Department of Education, DfE）配發給學童，用以進行遠距教學的筆記型電腦，近日遭發現被預先植入惡意軟體；目前英國教育當局已展開調查行動。

據英國廣播公司 BBC 報導指出，英國教師在一批送往 Bradford 地區學校的筆電中，發現這個惡意軟體，並將惡意軟體檔案分享在某個論壇，事件因此公諸於世。

資安媒體 Cybersecurity Insider 報導說，除了送往 Bradford 的筆電被發現遭植入惡意軟體之外，在送往 Lincolnshire 和 Wolverhampton 的筆記型電腦中，也發現了同樣的惡意軟體。

植入到這批教育用筆電的惡意軟體，疑似是「Gamarue.1」；這個惡意軟體是 Gamarue 的變種，早在 2012 年就由微軟發現並提報。

感染這個惡意軟體的 Windows 裝置，將可被惡意軟體幕後的駭侵者操控，存取其檔案系統，並控制其網頁瀏覽器；而且這個惡意軟意也可以透過 USB 裝置和區域網路進行自我散布，甚至進一步下載安裝更多惡意軟體，並且竊取用戶的機敏資訊。

不過，這個惡意軟體無法使用受害裝置上的攝影鏡頭與麥克風。

資安專家指出，這個惡意軟體會試圖連線位在俄羅斯境內的控制伺服器。

英國教育部指出，該單位已經確認約有 10% 由該部配發的筆電，含有此一惡意軟體；目前該單位正在調查整起事件；此外 DfE 發言人也說，惡意軟體將會在電腦開機時自動遭到移除。

- 資料來源：
  1. https://www.cybersecurity-insiders.com/laptops-supplied-to-children-in-uk-are-filled-with-russian-malware/
  2. https://www.hackread.com/uk-govt-funded-laptops-homeschoolers-gamarue-malware/
  3. https://www.bbc.com/news/technology-55749959

2.4、社群媒體資安近況

超過 228 萬名約會網站用戶個資，遭駭侵團體公開

近來有超過 228 萬名知名約會網站的用戶個人資料，遭到某駭侵團體公開。

近來一個駭侵團體在網路上公開了一批竊取自約會網站 MeetMindful.com 的用戶資料；被公開個資的用戶人數，超過 228 萬名以上。

公布這批資料的駭侵團體，自稱為 ShinyHunters；他們將這批竊得的資料，公布在某個論壇網站上，任何人只要知道網址，均可自由下載，取得這批資料。

被竊取的資料大檔案大小高達 1.2GB，看起來像是直接從某個資料庫中傾印（dump）下來的資料；資料欄位包括以下個資：

- 真實姓名；
- Email 地址；
- 居住城市、州、郵遞區號；
- 身體特徵描述；
- 約會對象偏好設定；

- 目前婚姻狀態；
- 出生年月日；
- 所在地經緯度座標；
- 連線用的 IP 位址；
- 以 bcrypt 雜湊加密過的登入密碼；
- Facebook 的使用者 ID；
- Facebook 登入認證 token。

在這批外流的個資中，雖然並不包括用戶在 MeetMindful.com 上與其他用戶交談的通訊資料，但是以上這些欄位仍然足以辨識出個別用戶的真實身分，並且加以追蹤。

資安媒體 ZDNet 試圖與 MeetMindful.com 連絡時，該公司的發言人並未提供任何回應；而被 post 在論壇上的這批資料，在 ZDNet 報導當時，檢視次數已超過 1,500 次。

近來有許多駭侵者在竊得類似交友網站上的個資後，向受害用戶恐嚇勒索的案例；若不支付相當數額的贖金，就會向受害者的家人、朋友甚至工作相關同仁公開其在交友網站上的足跡。

- 資料來源：
  1. https://threatpost.com/meetmindful-daters-compromised-data-breach/163313/
  2. https://www.zdnet.com/article/hacker-leaks-data-of-2-28-million-dating-site-users/

2.5、行動裝置資安訊息

2.5.1、資安專家揭露 iOS 與 Android 對機內資料加密的弱點

約翰霍普金斯大學的資安研究團體指出 iOS 與 Android 對於機內資料的保護程度弱點所在，並且揭露用戶可能面臨的資安風險。

約翰霍普金斯大學的資安研究團體，近期發表研究報告，指出 iOS 與 Android 對於機內資料的保護程度，在不同使用階段的弱點所在，並且揭露各種行動應用程式並未充分利用作業系統提供的保護機制，確實保護用戶個資，導致用戶可能面臨各種資料外洩的資安風險。

這組研究人員分成兩個團隊，分別研究 iOS 和 Android 作業系統在不同用戶使用過程中的資料加密流程，以及可能遭到攻擊，導致系統儲存資料外洩的可能弱點所在；該團隊的結論是，雖然 iOS 和 Android 在作業系統方面都提供了相當強固的加密保護，但在若干使用階段上，仍可能因為應用程式未充分利用這些作業系統提供的保護措施，或是其他的各種原因，導致用戶資料仍可能遭惡意攻擊而外洩。

以 iOS 來說，研究報告指出，iOS 的資料加密，在用戶開機但尚未解鎖時，是屬於「完全保護模式」；用以解鎖加密資料的金鑰，會儲存在作業系統的深處，非常難以取得；但只要用戶透過密碼、指紋、臉孔辨識等方式解鎖手機，就會有許多金鑰被移動到較容易取用的「快速存取記憶區」中，即

使手機再次上鎖，這些金鑰也會留在其中。

被放在快速存取記憶區中的金鑰，其受作業系統保護的程度就較弱；例如和以色列情治單位簽約，專門破解各種資訊裝置的 Cellebrite，與美國 Greyshift 公司，都擁有能在首次解鎖後取出資料的破解工具；當然更不用提各種枱面下的駭侵者。

雖然 Apple 在作業系統中，提供 App 開發者將金鑰放回深層保護區的選項，但研究人員發現，僅有銀行 app 等類型會真正實作此功能，絕大多數開發者，就任由金鑰留在快速存取記憶區中。

至於 Android 的問題也類似 iOS，雖然 Android 在開機後第一次解鎖前，也有「完全保護模式」，並沒有如 iOS 般提供開發者將金鑰放回深層保護區的系統功能；再加上 Android 的版本和機種複雜，許多用戶無法取得最新版作業系統或資安更新，導致 Android 用戶面臨更高的資料外洩風險。

- 資料來源：
  1. https://securephones.io
  2. https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/
  3. https://9to5mac.com/2021/01/14/johns-hopkins-ios-vulnerabilities/

2.5.2、美國電信業者 T-Mobile 三年來第四度發生資料外洩事件

美國行動電信業者 T-Mobile 於日前發表資安通報，指出該公司發現其顧客資料庫有遭不法入侵的跡象，但重要顧客個資並未外洩。

美國行動電信業者 T-Mobile 於日前發表資安通報，指出該公司內部的資安團隊，最近發現其顧客資料庫有遭駭侵者未經授權入侵存取的跡象，但該公司強調，重要的顧客個人資訊並未外洩。

T-Mobile 在資安通報中說，在該公司內部團隊與外部資安專家的協助下，正在調查該起事故；目前的調查結果指出，駭侵者可能已經取的資訊，包括電話號碼、單一帳號名下申請的各支電話號碼、以及部分與電話通聯相關的資訊，T-Mobile 說這些資訊是在其無線通訊服務營運進行時收集的。

T-Mobile 公司也在通報中強調，這批外洩的資料中，不包括帳號中登記的用戶姓名、實體郵件寄送地址、Email 地址、財務資訊、信用卡卡號、到期日等資訊，也不包括用戶的社會安全碼（Social Security Number）、稅務編號、密碼、SIM 卡密碼等等較敏感的個資。

T-Mobile 說，受到此次資料外洩事故影響的用戶，約佔全體用戶的 0.2%；以 T-Mobile 的總體用戶註冊量來計算，受影響人數約在 200,000 人上下。

這次資料外洩相較於過去 T-Mobile 曾發生過的資料外洩事件，以目前掌握的情資來說，由於受害人數較少，資料欄位也比較局限，影響與嚴重程度不若過去幾次事件。T-Mobile 曾分別在 2018 年 8 月、2019 年 11 月、2020 年 3 月發生過三次資料外洩事件，情節均遠較此次嚴重得多；包括員工與用戶的各種機敏個資都遭駭侵者竊取，受害用戶人數也達 2,000,000 人以上。

- 資料來源：
  1. https://www.t-mobile.com/responsibility/consumer-info/security-incident
  2. https://www.zdnet.com/article/t-mobile-discloses-its-fourth-data-breach-in-three-years/
  3. https://techcrunch.com/2021/01/03/t-mobile-call-records-data-breach/

2.6、軟體系統資安議題

2.6.1、駭侵者以空白 Google 表單，針對企業員工發動 BEC 攻擊

資安廠商日前發現有駭侵團體透過 Google 表單，跳過各種 Email 系統的有害內容過濾機制，鎖定企業員工發動 BEC 攻擊。

資安廠商 Proofpoint 日前發表研究報告，指出該公司旗下的資安研究團隊，自 2020 年 12 月初開始觀察到有駭侵團體透過 Google 表單，跳過各種 Email 系統以關鍵字為基礎的有害內容過濾機制，鎖定企業員工發動 BEC（Business Email Compromization）攻擊。

Proofpoint 說，雖然透過 Google 表單來夾帶惡意連結等釣魚攻擊方式，並不是新鮮事，過去就常觀測到這類攻擊手法，但這波攻擊同時結合了社交工程，而且規模與受害範圍較大。

報告中說，這波攻擊的典型手法，是透過 Email 傳送；郵件主旨會被駭侵者填上企業高階主管的名字，假裝是由高階主管發送給中階或基層員工，但並沒有在寄件人欄位中填入虛假資訊。

報告說，信件內容會以非常十萬火急的口吻，說自己必須前去一個緊急會議，要求受害者撥空點按信中的連結，以幫忙填寫信中的 Google 表單內容；這種「要求撥空」的手法經常在其他「禮物卡詐騙」類型的攻擊活動中出現。

當受害者按下連結後，會出現一個幾乎一片空白，僅有預設內容的 Google 表單畫面。報告中說這種手法是為了引誘受害者回信給發信的駭侵者，以便收集其 EMail 地址，進行進一步的駭侵攻擊；另一層用意是可以用來過濾出容易上當操弄的受害者。

報告指出，Proofproint 已經觀察到數千封類似的 BEC 攻擊信件，受害者遍及零售業、電信業、醫療照護業、能源產業、製造業等。

- 資料來源：
  1. https://threatpost.com/google-forms-set-baseline-for-widespread-bec-attacks/163223/
  2. https://www.proofpoint.com/us/blog/threat-insight/bec-target-selection-using-google-forms

2.6.2、APT 27 駭侵團體攻擊方式轉向勒贖全球遊戲廠商

資安廠商發現駭侵團體 APT 27，自去年起改變其攻擊目標與手法，轉向以勒贖方式攻擊全球各大遊戲廠商。

資安廠商 Prefero 與 Security Joes 日前聯名發表研究報告，指出該公司旗下的資安研究團隊，發現駭侵團體 APT 27，自去年稍早開始大幅改變其攻擊目標與手法，轉向以勒贖方式攻擊全球各大遊戲廠商。

Profero and Security Joes 在報告中指出，該公司去年在調查一起資安勒贖攻擊事件時，在攻擊其核心伺服器的惡意程式碼中發現一些片斷，非常接近過去曾被趨勢科技發現的 DRBControl 惡意軟體；而 DRBControl 正是駭侵團體 APT 27 與 Winnti 慣用的駭侵工具。

之後該公司亦在多次針對全球遊戲廠商的勒贖攻擊事件中，發現類似的攻擊技巧與惡意程式碼；這些攻擊事件通常會使用內建於 Windows 系統中的 BitLocker 磁碟加密程式，這非常不尋常，因為傳統駭侵者多半會使用自製的駭侵攻擊工具，不會使用原本就內建在作業系統中的應用程式來發動攻擊。

以過去 APT 27 / Emissary Panda 駭侵團體的攻擊案例來說，多半都是利用各種駭侵攻擊進行監控或資料竊取，並非以勒贖取財為重點；Prefero and Security Joe 在報告中分析指出，該公司發現由 APT 27 發動的勒贖攻擊，其時間點正好在肺炎疫情剛開始快速蔓延，各地紛紛採取封城因應的當

時，因此很有 APT 27 很有可能因為財務需求而轉向發動勒贖攻擊。

在 Profero and Security Joe 發表的報告中，也對該公司掌握的攻擊行動，提供了完整的攻擊手法分析。

- 資料來源：
  1. https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf
  2. https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/
  3. https://www.scmagazine.com/home/security-news/ransomware/chinese-espionage-group-apt27-moves-into-ransomware/

2.6.3、遊戲大廠 Capcom 遭勒贖攻擊後，390,000 人機敏資料恐已遭竊

日本遊戲大廠 Capcom 近日發表資安通報，指出該公司在 2020 年 11 月遭到勒贖攻擊後，目前可能有多達 390,000 名玩家的個資恐已遭到竊取。

日本遊戲大廠 Capcom 近日發表資安通報，指出該公司在 2020 年 11 月初遭到嚴重勒贖攻擊後，根據最新調查報告指出，可能有多達 390,000 人的個資恐已遭到竊取。

去年（2020）11 月 2 日，Capcom 遭到 Ragnar Locker 勒贖軟體攻擊，有高達 1TB 的公司機敏資料被竊；勒贖攻擊發動者要求相當於 1,100 萬美元的高額贖款；隨後 Ragnar Locker 幕後的攻擊者便公開了部分竊得的資料。

而在日前更新的攻擊事件調查報告中，Capcom 提供了更詳細的受害資訊，包括有 16,415 人的個資確定遭竊，其中 3,248 人是相關協力廠商人員、9,164 人是 Capcom 離職員工與其關係者，3,994 人是現職員工與其關係者；其他不明但個資可能外洩的人數，則高達 390,000 人。

被竊個資中包括的資料類型，則包括個人姓名、簽名數位影像、郵寄地址、護照資訊、人力資源相關記錄等；此外 Capcom 的銷售報表、財務資訊、遊戲玩家客服記錄、線上遊戲商店的顧客消費資訊、運動類遊戲玩家留存的姓名、Email、性別等。

資安專業媒體 BleepingComputer 指出，Ragnar Locker 幕後駭侵者對該媒體揚言，他們手上還握有更多更有價值的資料，可用以發動進一步的攻擊；BleepingComputer 認為，目前流出的資訊，可能僅僅是 Capcom 攻擊事件中竊得的部分資料而已。

Capcom 是日本首屈一指的大型遊戲開發廠商，曾經推出《快打旋風》、《洛克人》、《惡靈古堡》、《鬼武者》、《逆轉裁判》等膾炙人口的經典遊戲。

- 資料來源：
  1. https://www.capcom.co.jp/ir/english/news/html/e210112.html
  2. https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/

2.6.4、SolarWinds 駭侵者可能已取得微軟程式原始碼，但強調對公司不構成威脅

微軟表示，SolarWinds 駭侵攻擊事件中的駭侵者，很可能已經攻破公司的防護系統，掌握一部分內部帳號控制權，同時取得部分微軟產品的原始碼。

微軟於 2020 年 12 月 31 日表示，SolarWinds 駭侵攻擊事件中的駭侵者，很可能已經在這波長達數月的攻擊行動中，突破該公司的防護系統，掌握一部分內部帳號控制權，同時取得部分微軟產品的原始碼。

在微軟發表的調查報告中指出，微軟發現在公司內部環境中出現了部分 SolarWinds 攻擊行動的惡意程式碼，顯示至少有一個微軟公司內部的帳號，曾遭駭侵者用以檢視微軟內部的產品原始碼程式庫。

微軟說，該帳號僅有資料檢視權限，無法針對程式碼與相關檔案進行任何編輯或增刪動作，也沒有改變任何工程系統設定的能力；微軟在調查後確認並沒有任何程式碼遭到更動，而疑似遭到竊取的帳號也遭停用，並進行密集調查。

微軟說，公司各種產品的程式碼，在內部都是公開的，微軟員工均可檢視，如同開放源碼社群的運作模式；公司並不依賴程式碼的秘密性營利，因此程式碼遭駭侵者檢視，並不影響公司的營運。

微軟在報告中也強調，目前沒有發現任何顧客相關資料遭到竊取的跡象，也沒有發現公司的電腦系統被駭侵者用以攻擊他人的證據。

這波疑似由俄國 APT 駭侵團體 Cozy Bear 發動的 Solarwinds 攻擊事件，自 2020 年 3 月起即針對美國各級政府與中大型企業使用的 Solarwinds Orion IT 管理系統發動大規模駭侵攻擊，利用供應鏈攻擊手法，在 Solarwinds Orion 的更新程式中植入惡意軟體，並發動長期監控並竊取各種資訊，據統計受害者多達近 18,000 個公私營單位。

微軟在去年 12 月中也發表多次關於 SolarWinds 攻擊的資安通報，表示 SolarWinds 公司為其 Office 365 雲端辦公軟體服務的客戶，而微軟本身也有採用 SolarWinds Orion IT 管理解決方案，因此也無法倖免於此波大規模攻擊行動。

- 資料來源：
  1. https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/
  2. https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/
  3. https://www.geekwire.com/2020/microsoft-says-solarwinds-hackers-viewed-source-code-internal-defenses-thwarted-damage/

2.6.5、美國運通墨西哥分支機構約 10,000 名卡友資訊遭駭侵者公開並免費下載

約有 10,000 名美國運通信用卡用戶的資料，遭駭侵者於網路上免費公開。

金融資安研究單位 Bank Security 日前發表資安通報，指出約有 10,000 名美國運通信用卡用戶的多項機敏資訊，遭不明駭侵者於網路上免費公開，任何人皆可下載取得這些個資。

Bank Security 在其 Twitter 帳號中發表一則推文，指出美國運通在墨西哥的一萬名信用卡持卡用戶，其個人資料遭到駭侵者在某個駭侵相關論壇上免費公開；該則推文同時附有一張論壇貼文畫面的截圖，內有大量用戶資料的樣本。

該則推文也指出，不僅是美國運通的用戶資料被公開，該不明駭侵者還持有另外兩家墨西哥金融機構 Santander 與 Banamex 的顧客資訊，並且試圖在論壇上出售更多駭侵自其他金融機構的個資。

資安專業媒體 BleepingComputer 分析這批資料指出，在這 10,000 名美國運通信用卡用戶的外洩資料中，資料欄位包括信用卡卡號、持卡人姓名、完整郵寄地址、電話號碼、出生年月日、性別等個人可識別資訊（Personally Identifiable Information）。

不過 BleepingComputer 指出，該批資料內不包括信用卡到期日、密碼及其他財務相關機敏資訊，因此無法用於信用卡盜刷。

BleepingComputer 分析指出，雖然這批個資和信用卡資訊無法用來盜刷，但取得這些資料的有心人士，仍可利用這些資料進行各種攻擊，例如發送垃圾郵件，或以釣魚信件或社交工程，從而騙取更多機敏資訊。

- 資料來源：
  1. https://twitter.com/Bank_Security/status/1345739770400550912
  2. https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/

2.7、軟硬體漏洞資訊

2.7.1、國內網通設備商多款網通產品含有資安漏洞，建議立即更新

多款國內網通設備商生產之防火牆、VPN 閘道器等裝置遭發現內含硬式編碼認證漏洞。

國內網通設備商生產的多款網通產品，如硬體防火牆、VPN 閘道器、網路存取點控制器等裝置，遭資安廠商發現內含硬式編碼認證漏洞，這個帳號主要用途是透過 FTP 向連接的 AP 提供自動韌體更新。

發現這個嚴重問題的，是荷蘭資安廠商 Eye Control 旗下的資安研究人員；該單位日前發表研究報告，指出研究人員在以 root 登入自己使用的 USG40 整合安全閘道器（Unified Secuirity Gateway）時，發現在當時最新版的韌體 4.60 patch 0 版本中，有硬式編碼的一個管理者權限帳號，密碼以明文寫在程式碼之中。

該研究員繼續研究，還發現這組管理者登入資訊，同時可以用來登入 USG40 的 Web 和 SSH 管理界面；而這組登入資訊並未出現在較舊的韌體版本中。

這個漏洞的 CVE 編號為 CVE-2020-29583，其 CVSS 危險程度評分高達 7.3 分，屬「高危險」等級；原廠已於官方網站發布新版韌體，修復這個漏洞。請採用下列網通產品的用戶，立即下載並更新至最新版本，或暫時避

免使用，以免遭到駭侵者透過該漏洞發動攻擊。

- CVE 編號：CVE-2020-29583
- 影響產品/版本：防火牆：ATP、USG、USG FLEX、VPN（韌體版本 ZLD v4.60）、無線網路控制器：NXC2500、NXC5500 (韌體版本 V6.0- V6.10)
- 解決方案：防火牆系列升級至韌體版本 ZLD V4.60 Patch 1；無線網路控制器於 2021 年 1 月 8 日升級至韌體版本 V6.10 Patch1

- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29583
  2. https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html
  3. https://www.zyxel.com/support/CVE-2020-29583.shtml
  4. https://www.zyxel.com/tw/zh/support/CVE-2020-29583.shtml

2.7.2、Linux Sudo 指令遭發現遠端執行任意程式碼嚴重漏洞

資安廠商發現一個存在已久的 Unix 常用指令 Sudo 存有嚴重資安漏洞，可讓任何使用者將執行權限提升到 root 等級。

資安廠商 Qualys 日前發表研究報告，指出該公司旗下的資安研究團隊，發現一個存在已久的 Unix 系作業系統常用的指令 Sudo，存有嚴重資安漏洞，可讓任何使用者將執行權限提升到 root 等級。

Sudo 是個廣泛內建在各種泛 Unix 作業系統中的指令，可以暫時讓用戶以其他帳戶的密碼，執行更高權限的程式或指令。根據 Qualys 的報告，這個漏洞自從 2011 年七月以來，就存在於多個泛 Unix 系的作業系統之中，包括 Ubuntu、Debian、Fedora 等廣受歡迎的 Lunix distribution 發行版本中的 Sudo 指令，都存有此一漏洞。

這個漏洞的 CVE 編號為 CVE-2021-3156，Qulays 將之稱為「Baron Samedit」；目前 NVD 尚未針對這個漏洞提供 CVSS 危險程度評分。

Qualys 在其研究報告中，也針對各大 Unix 系作業系統，發展出基於此一漏洞的各種模擬攻擊方法；但 Qualys 也指出，這個漏洞必須由駭侵者在電腦前面操作；如沒有事先登入的話，駭侵者無法以遠端執行方式利用此漏洞提升執行權限。

也因為駭侵者必須先取得登入使用的權限，因此資安專家認為這會限制該漏洞的大規模使用可能性；但如果被攻擊的系統本身已先透過其他方式遭到入侵（例如植入僵屍網路惡意軟體），那麼攻擊者仍有可能利用此漏洞，將己身的執行權限提升至 root 等級。

目前 Sudo 指令的開發者，以及各大 Linux distribution 的發行者，皆已針對這個漏洞發布修補程式；用戶應將系統中的 Sudo 指令升級至版本 1.9.5p2，即可解決此一漏洞。

- CVE 編號：CVE-2021-3156
- 影響產品/版本：各大 Unix 系作業系統中的 Sudo 指令，版本 1.8.2 至 1.8.31p2、以及 1.9.0 至 1.9.5p1
- 解決方案：升級 Sudo 指令至 1.9.5p2

- 資料來源：
  1. https://www.sudo.ws/alerts/unescape_overflow.html
  2. https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit
  3. https://threatpost.com/sudo-bug-root-access-linux-2/163395/

2.7.3、微軟修補 Microsoft Defender 防毒防駭軟體內的 zero day 漏洞

微軟緊急修復存於 Microsoft Defender 防毒防駭軟體中的嚴重 zero day 漏洞，該漏洞可能導致駭侵者遠端執行任意程式碼。

微軟緊急修復存於 Microsoft Defender 防毒防駭軟體防護引擎組件中的嚴重 zero day 漏洞，該漏洞可能導致駭侵者遠端執行任意程式碼，而且已發現利用該漏洞進行的多起駭侵攻擊行動。

這個得到緊急修補的漏洞，其編號為 CVE-2021-1647，存於 Microsoft Defender 防毒防駭引擎中的 mpenging.dll 組件中；Microsoft 已經發展出利用此漏洞發動攻擊的概念證實程式，但在其官方說明文件中，並沒有透露關於此漏洞的具體細節，以及錯誤發生的原因。

據資安媒體 BleepingComputer 的報導，這個漏洞已遭駭侵團體發動多起攻擊事件。

受到影響的 Microsoft Defender 版本為 1.1.17600.5 與先前各個版本，而 Microsoft Defender 普遍內建於所有 Windows 版本中，包括 Windows 7、Windows 8.1、Windows 10、Windows RT、Windows Server 的各種版本。

Microsoft 在更新文件中指出，若要修補這個漏洞，在用戶的電腦系統連上網路的情形下，用戶無需手動操作，系統會自動更新到最新版本的

Microsoft Defender（目前為 1.1.17700.4）；但如果用戶的電腦沒有連上網路，就必須手動下載更新檔案，才能更新系統中的 Microsoft Defender。

- CVE 編號：CVE-2021-1647
- 影響產品/版本：Windows 7、Windows 8.1、Windows 10、Windows RT、Windows Server 的各版本中內建的 Microsoft Defender 1.1.17600.5 與所有較舊版本。
- 解決方案：透過系統更新自動修復（電腦需保持連線網路）

- 資料來源：
  1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1647
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1647
  3. https://www.bleepingcomputer.com/news/security/microsoft-patches-defender-antivirus-zero-day-exploited-in-the-wild/

2.7.4、Chrome、Edge、Firefox 各自修復可造成系統遭挾持的資安漏洞

多個主流網頁瀏覽器 Chrome、Edge 和 Firefox 近期各自修復可導致系統遭挾持的嚴重資安漏洞，用戶應立即更新至最新版本，以避免受此漏洞影響。

多個主流網頁瀏覽器 Google Chrome、Microsoft Edge 和 Mozilla Firefox，近期各自修復可導致系統遭挾持的嚴重資安漏洞；這三種瀏覽器的廣大用戶，應立即更新至最新版本，以避免受此漏洞影響。

在 Mozilla Firefox 方面，修復的漏洞編號為 CVE-2020-16044。這個漏洞屬於「使用已釋放記憶體」（use-after-free）錯誤，發生在 Firefox 處理 cookie 的方式；駭侵者可以透過發送特製的 COOKIE ECHO chunk 以誘發這個錯誤，在執行 Mozilla Firefox 的電腦、手機或平板上發動攻擊，遠端執行任意程式碼，並且可取得裝置的控制權。

這個漏洞的 CVSS 危險程度評分高達 7.7 分，屬於高度危險（High）等級；受影響版本為現行版本 Firefox Desktop 84.0.2、Firefox Android 84.1.3、Firefox 企業版 ESR 78.6.1 之前的所有版本。

而在以 Chromium 為基礎的 Google Chrome 與 Microsoft Edge 方面，則是修復了一個越界寫入（out-of-bounds write）的錯誤；這個錯誤發生在 Google 開發的開源 JavaScript 與 WebAssembly 引擎，亦可導致駭侵者遠端執行任意程式碼，並且奪取系統控制權。

Google Chrome 與 Microsoft Edge 的這個漏洞，編號為 CVE-2020-15995，其 CVSS 危險程度評分高達 8.8 分，危險程度等級屬於「高度危險」，影響的版本分別為 Google Chrome Windows、macOS、Linux 87.0.4280.141 先前的所有版本，以及 Microsoft Edge 87.0.664.75 各平台之前所有版本。

- CVE 編號：CVE-2020-16044、CVE-2020-15995
- 影響產品/版本：

  Mozilla Firefox：Firefox Desktop 84.0.2、Firefox Android 84.1.3、Firefox 企業版 ESR 78.6.1 之前的所有版本；

  Google Chrome：Google Chrome Windows、macOS、Linux 87.0.4280.141 先前的所有版本；

  Microsoft Edge：Microsoft Edge 87.0.664.75 各平台之前所有版本。
- 解決方案：升級到各瀏覽器現行最新版本

- 資料來源：
  1. https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16044
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15995
  4. https://msrc.microsoft.com/update-guide/vulnerability/ADV200002

2.7.5、蘋果推出 iOS 14.4，一次修復三個 0-day 嚴重資安漏洞

Apple 日前推出最新版 iOS 14.4，同時修復三個 0-day 漏洞，其中有兩個可使駭侵者遠端執行任意程式碼； iOS 裝置用戶應立即更新到最新版本。

Apple 日前推出最新版 iOS 14.4、iPadOS 14.4，同時修復三個 0-day 漏洞，其中有兩個可使駭侵者遠端執行任意程式碼； iOS 裝置用戶應立即更新到最新版本。

在 Apple 隨著新版 iOS 與 iPadOS 發表的資安更新文件中指出，這次得到更新的三個 0-day 漏洞，其 CVE 編號分別為 CVE-2021-1782、CVE-2021-1870、CVE-2021-1871。

其中 CVE-2021-1782 屬於「執行權限提升」型資安漏洞，發生在 iOS 與 iPadOS 的作業系統核心區；駭侵者可利用此漏洞，提升自己在作業系統中的執行權限。Apple 指出該公司已發現這個漏洞遭到大規模利用。

CVE-2021-1782 的 CVSS 危險程度評分為 8.4 分，其危險等級為「高」。

另外兩個得到修復的 0-day 資安漏洞 CVE-2021-1870 與 CVE-2021-1871，都發生在 Safari 瀏覽器使用的 WebKit 引擎核心。駭侵者可以利用這兩個漏洞，遠端執行任意程式碼。同樣的，Apple 在說明文件中也表示，已

經收到駭侵者大規模利用這兩個漏洞發動攻擊行動的通報。

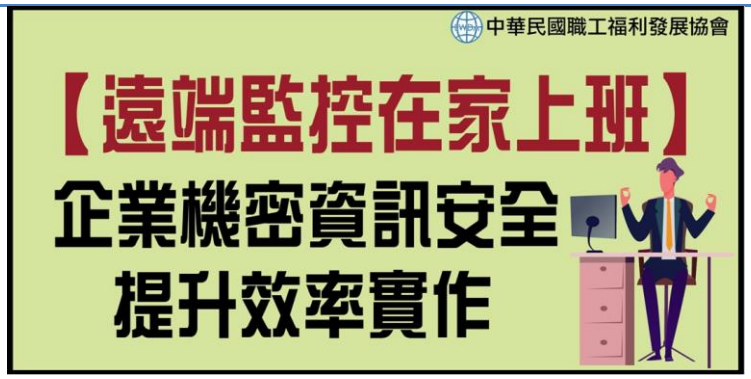
CVE-2021-1870 和 CVE-2021-1871 的 CVSS 危險程度評分，和前一個漏洞 CVE-2021-1782 相同，也是 8.4 分，其危險等級同樣為「高」。

Apple 指出，以下 iOS 裝置的使用者，包括 iPhone 6s 與所有後續機種、iPad Air 2 與所有後續機種、iPad mini 4 與所有後續機種，以及 iPod touch（第 7 代），都應立即更新為 iOS 14.4 或 iPadOS 14.4，以避免遭到駭侵者利用這三個 0-day 漏洞發動攻擊。

- CVE 編號：CVE-2021-1782、CVE-2021-1870、CVE-2021-1871
- 影響產品/版本：iPhone 6s 與所有後續機種、iPad Air 2 與所有後續機種、iPad mini 4 與所有後續機種，以及 iPod touch（第 7 代）
- 解決方案：立即更新至 iOS 14.4 或 iPadOS 14.4

- 資料來源：
  1. https://support.apple.com/en-us/HT212146
  2. https://threatpost.com/apple-patches-zero-days-ios-emergency-update/163374/

第 3 章、 資安研討會及活動

【遠端監控在家上班】企業機密資訊安全及提升效率實作	
活動時間	**2021-02-19(五) 09:30 ~ 16:30**
活動地點	**台北市中正區懷寧街 43 號 5 樓**
活動網站	**http://vip.asia-learning.com/ewda2/course/courseintro/100706**
活動概要	 **主辦單位：中華民國職工福利發展協會** 透過此獨家課程，您也將實際操作一系列高效應用工具，全方位的學習防止內外威脅，管控內外資安，並了解如何全面建立"密碼管理"、"加密安全文檔"避免被外部盜取機密，阻止勒索程式，根除遠端威脅，增加生產力。 ※本實作課程，授課現場將由老師帶領實操，請學員務必自備可無線上網的智慧型手機及筆電(平版)： 1.不需要事先註冊軟體，不需寫程式 2.手機(必備) 預載 LINE。 3.筆電(必備) 預載 Google chrome 瀏覽器 【課程效益】 本課程將針對企業機密資訊安全的操作進行深入的解說，包括資安監控工具前後台操作程序、法律須知。課程結束後，學員將對於防止內外威脅，管控內外資安，並了解如何全面合法員工監控，建立「密碼管理」、「加密安全文檔」 避免被盜取機密，有深刻的了解，並有能力自行操作！

人工智慧與資安保險論壇暨 ACFD 第二屆第二次會員大會及第二屆第三次理監事聯席會議	
活動時間	**2021 年 2 月 26 日 (五) 下午 13:30~17:20**
活動地點	**大同大學尚志教育館 106 會議室**
活動網站	**https://acfd2019.kktix.cc/events/1cac1bef-copy-1**
活動概要	 **主辦單位：台灣數位鑑識發展協會(ACFD)、人工智能股份有限公司** 台灣數位鑑識發展協會 (ACFD) 為致力於扮演台灣數位鑑識政策、市場、人才及應用的專業化、標準化、產業化與創新化之推手，結合產官學研各界的力量，推動資安資料保險、數位鑑識、資安鑑識、鑑識會計、舞弊稽查、ICT 治理、資通安全、雲端安全、個資安全及保護等重要工作，謀求對於台灣資通訊安全領域及產業發展有所助益。 科技產業，智慧製造產業及醫療產業，如鴻海，台積電，聯發科，華碩，宏基...等公司都曾發生資安犯罪事件及台北市公衛資訊系統遇駭及醫療個資外洩，美國一家醫療電腦系統遭受到駭客攻擊及病患醫療記錄外洩，新加坡保健服務集團遭到駭客攻擊及個資外洩事件等等。歡迎報名參加。

國際網路資安雙證技能培訓班	
活動時間	**110 年 03 月 02 日～04 月 13 日（大多利用週一至週五之間上課）**
活動地點	**臺北大學臺北校區 (臺北市中山區民生東路三段 67 號)**
活動網站	**https://www.accupass.com/event/2101290231421303910584**
活動概要	 **主辦單位：財團法人工業技術研究院** 課程介紹： 因應資訊安全領域發展趨勢與人才需求，工研院產業學院規劃辦理本課程，規劃以具備 CompTIA Network+（國際公認的基礎級計算機網路技能證）以及 CompTIA Security+（國際公認的基礎級安全技能證）技能作為設計課程內容主體，並藉以教訓考用循環模式培養符合產業及企業升級轉型所需人才並提供企業選用，提升資訊安全產業人才之素質與競爭力。 適合對象： 1. 有志跨足網路安全、資訊安全專業技術領域者 2. 15 歲至 29 歲（以課程開訓日計算）之本國籍待業青年者

後疫情時代｜資安策略的轉變與資安治理的價值	
活動時間	**2021-03-18(四) 13:45 ~ 16:30**
活動地點	**台灣台北市中山區松江路 61-1 號**
活動網站	**https://www.accupass.com/event/2101190342356142804670**
活動概要	 **主辦單位：崴亞風險咨詢顧問股份有限公司** 活動介紹： 2021 年全球疫情持續發燒，許多實體活動、出差、會議都紛紛暫停，數位轉型速度加劇，遠距辦公成了企業必須面對的課題。 然而，駭客攻擊、勒索軟件、釣魚郵件在這種情況下，也搭著 COVID-19 的效應層出不窮的出現，光是 2020 上半年趨勢科技就攔截 880 萬次 COVID-19 相關的資安威脅，而全球受勒索軟體攻擊的每日平均次數更增加 50%。 資安威脅離你我不再遙遠，你還能置身事外嗎？ 適合對象：不拘，對資安策略與風險想近一步了解的人 報名費用：400 元/位 聯絡窗口：02-2509-5819 分機 905 彭小姐（聯絡時間：週一至週五 AM 9:00 ~ PM 5:00）或來信至 erin.peng@wea4risk.com

第 4 章、 2021 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。

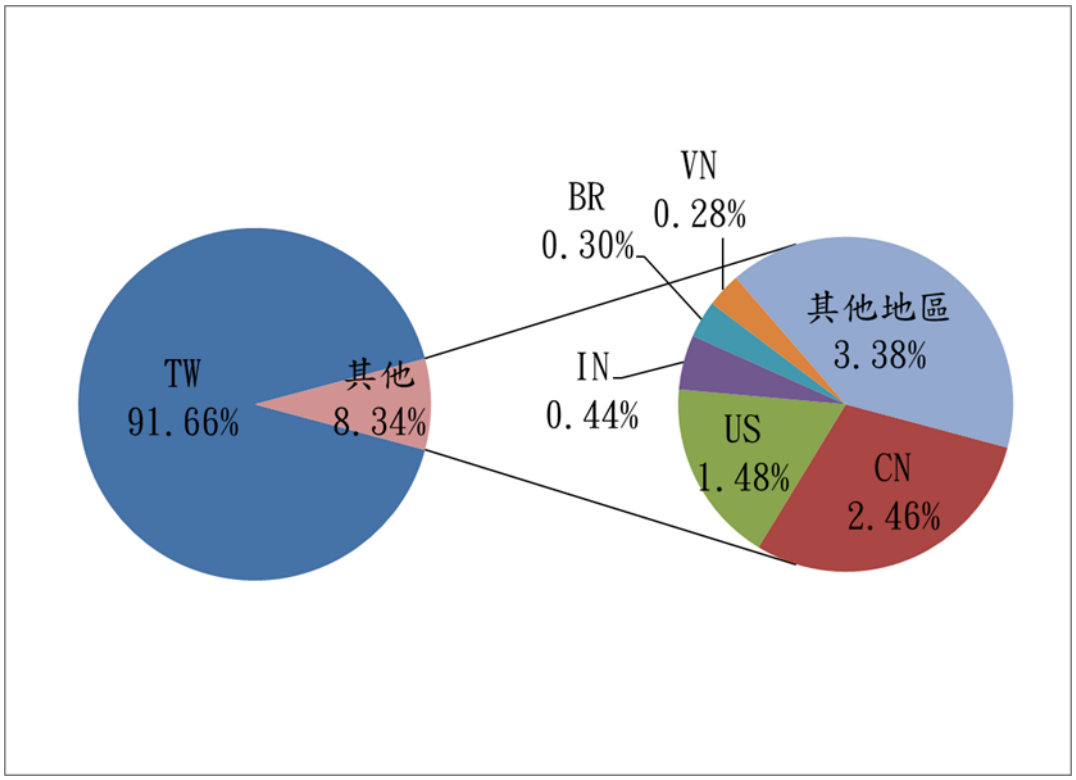


圖 1、分享地區統計圖

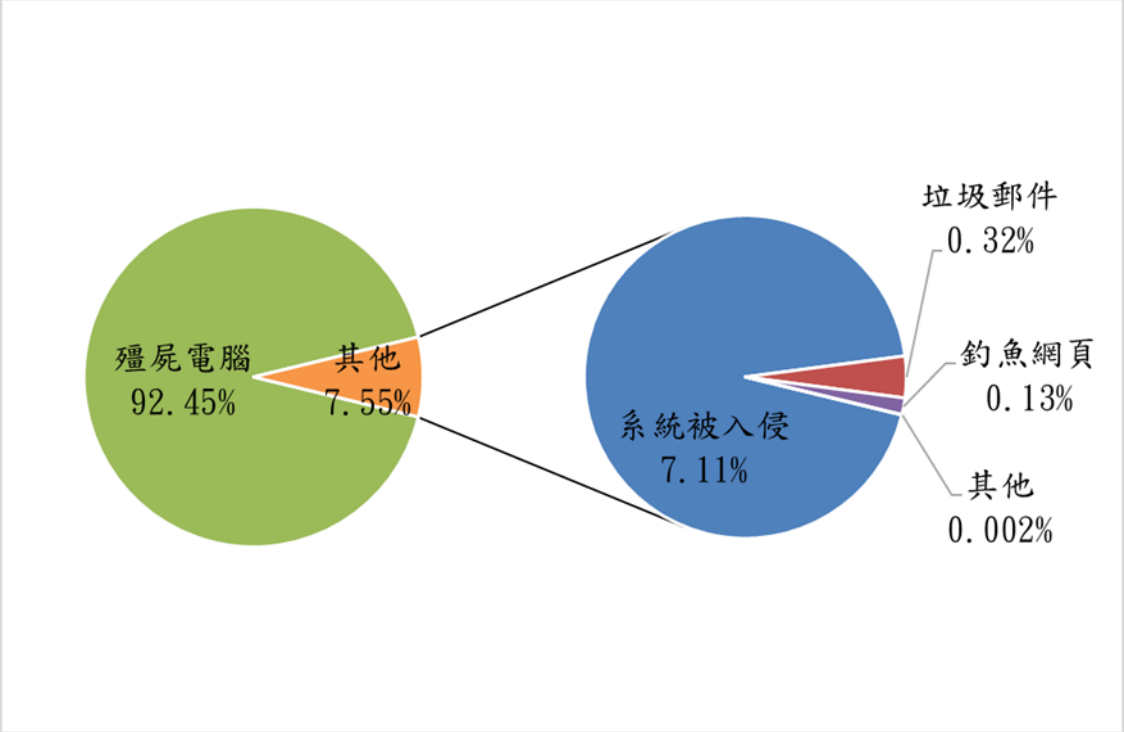


圖 2、分享類型統計圖

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：**2021 年 2 月 9 日**

編輯：**林克容、江奕昉、洪彩馨**

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**