TWCERT/CC 資安情資電子報

2020 年 11 月份

目錄

第 1 章、 封面故事

資安廠商發現一個潛伏九年未被發現的 APT 駭侵團體

資安廠商日前發現一個全新的國家支持 APT 駭侵團體；這個駭侵團體在過去九年多來從未被發現。

斯洛伐克資安廠商 ESET 日前在一場資安研討會上，首次揭露了 APT 駭侵團體 XDSpy 的存在；這個駭侵團體過去九年來多次發動駭侵攻擊活動，但一直未被偵測到。

ESET 的研究人員指出，XDSpy 駭侵攻擊的主要目標，是調查並竊取各種機密文件，並竊取資料；主要的攻擊對象為東歐與巴爾幹半島諸國的政府單位與私人企業。

被 XDSpy 鎖定攻擊的國家包括白俄羅斯、摩多維亞、俄羅斯、塞爾維亞與烏克蘭；但這些僅是 ESET 有偵測到的攻擊活動；可能仍有更多攻擊活動，至今未被掌握。

ESET 也指出，在 XDSpy 某次駭侵活動遭白俄羅斯資安主管單位發覺後，該團體的攻擊活動便轉入地下。

ESET 研究人員說，XDSpy 主要的攻擊武器，是一個稱為 XDDown 的惡意軟體工具組；主要能在感染受害者後，繼續下載多種模組，以執行不同的

攻擊手法；這些模組包括可掃瞄受感染電腦規格與作業系統組態細節的 XDREcon、可尋找特定格式檔案（如 PDF、Office 文件、通訊錄資料等）的 XDList、可監控何種裝置連上受感染電腦的 XDMonitor、可竊取本地瀏覽器儲存帳密的 XDPass 等等。

ESET 說，XDSpy 的這些攻擊手法不算特別新，但對於感染攻擊對象並發動攻擊，已經相當足夠。

- 資料來源：
  1. https://www.virusbulletin.com/conference/vb2020/abstracts/xdspy-stealing-government-secrets-2011/
  2. https://cert.by/?p=1458
  3. https://www.zdnet.com/article/eset-discovers-a-rare-apt-that-stayed-undetected-for-nine-years/

第 2 章、 資安活動紀事

2020 台灣資安通報應變年會-超前部署，掌握資安聯防與應變先機

隨著全球資訊環境的瞬息萬變，在物聯網、AI、5G 技術快速發展下，資訊安全議題已成為數位經濟下重要顯學。台灣電腦網路危機處理暨協調中心(TWCERT/CC)於 10 月 27 日主辦 2020 台灣資安通報應變年會，本次年會主題：「超前部署，掌握資安聯防與應變先機」，邀請到國內產官學各界的資安重要人士前來與我們分享、討論，與會講者有：國家通訊傳播委員會的孫雅麗委員、永豐金控李相臣資安長，以及奧義智慧邱銘彰共同創辦人。

資安情資及資安事件應變備受企業重視，如何以國際思維掌握資安先機，運用國內外資安情資進行事前防禦，並鼓勵建立資安事件通報及諮詢管道，以利因應資安事件，減低企業駭侵之衝擊及損害，為本次年會活動之核心。為此本次年會特別規劃一場國際資安專題座談會以及一場企業產品資安 PSIRT 座談會，同時掌握國際與國內企業資安趨勢。

國際資安專題座談部分由黃勝雄董事長擔任主持人，邀請我國調查局資安工作站張尤仁主任、AIT Dannielle Andrews 組長、荷蘭辦事處楊智凱事務官、駐台北以色列經濟文化辦事處主管 Tslil Lahav，以及澳洲駐台辦事處

Stasia Tan 副主任與我們分享國內和國外的資安策略與作法。

企業 PSIRT 部分則邀請國家資通安全會報技術服務中心吳啟文主任擔任引言人，並由國內三個企業 PSIRT 組織的成員，合勤科技游政卿資安長、威聯通科技龔化中技術長以及群暉科技李宜謙資安經理與大家交流企業產品資安實務運作過程的困難與效益，提升我國企業資安防護能量，達到資安聯防目標。

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、勒索病毒 AgeLocker 被用來攻擊 NAS 儲存設備，建議使用者應及時更新

新興勒索病毒 AgeLocker 是在今年(2020)7 月被發現，該勒索病毒特徵為並非使用其他勒索病毒常見的 AES、RSA 等加密演算法，而是使用密碼學家與軟體工程師 Filippo Valsorda 所開發的加密工具–Age(Actually Good Encryption)，對受害者的文件進行加密攻擊，因此該勒索病毒被命名為「AgeLocker」。

在 AgeLocker 被發現之後，隨著該勒索病毒的擴散及攻擊案例增加，於 8 月底時，發現 AgeLocker 針對 NAS 儲存設備進行攻擊，以 Age 加密演算法將受害主機內檔案進行加密，並且創建一名為 HOW_TO_RESTORE_FILES.txt 之文字檔，告知受害者其檔案已經被加密，必須支付贖金方能取回主機中的重要檔案。

在 9 月中旬，國內也有數個學術單位被發現遭到 AgeLocker 攻擊，原先儲存眾多學術資訊的 NAS 設備檔案都已消失，僅留有一封攻擊者留下的勒索通知信於其中。而相關資安單位在透過 FTP 傳檔軟體連線至受害 NAS 的資料

夾後，便發現那些遭勒索病毒加密的檔案，但這些受到加密的檔案，卻會出現兩種不同的副檔名。推測是因 Age 加密演算法中使用了 X25519、ChaChar20-Poly1305 以及 HMAC-SHA256 等三種演算法，因此推測 AgeLocker 會根據檔案的大小不同而使用不同的加密方式，才會出現兩種不同的副檔名。

國內儲存設備大廠立即進行相關之調查，並發佈之新聞稿，其資訊指出此次事件中，多數的受害裝置為 macOS 與 Linux 系統。但經詳細檢閱後，NAS 設備中的 QTS 等作業系統並無尚未修補之資安漏洞或弱點，且目前該廠商所接獲之已知案例中，大多數都為尚未更新至最新版本之舊版 QTS 系統。因此，該廠商建議使用者應立即更新 NAS 設備之作業系統以及各 APP 版本，以避免仍存有資安漏洞威脅。此外，使用者也應維持良好之使用習慣，包括維持密碼強度、安裝防毒軟體等，以確保設備的安全性。該廠商善盡社會責任配合相關資安單位，針對此次事件進行深入的調查分析，提供使用者擁有足夠安全性、完整性的 NAS 設備。

- 建議措施：
  1. 管理者應檢查並更新至其使用的 NAS 設備型號最新的可用版本，並維持定期更新的習慣。
  2. 除了 NAS 設備的系統版本之外，對設備中所有已安裝的應用程式，都應立即更新為最新版本。
  3. 維持密碼的強度要求，不應為一時方便而使用弱密碼。
  4. 建議安裝廠商提供之惡意軟體掃描程式等防護軟體，減少病毒威脅的機率，並參考廠商提供之最佳實務指南，達到最佳防護成效。
  5. 檢閱設備中的帳號及應用程式，移除可疑的帳號/應用程式。

- 資料來源：

1. https://www.qnap.com/zh-tw/news/2020/%E5%85%B1%E5%90%8C%E5%B0%8D%E6%8A%97-agelockerqnap-%E5%91%BC%E7%B1%B2%E7%94%A8%E6%88%B6%E9%80%B2%E8%A1%8C%E7%B3%BB%E7%B5%B1%E6%9B%B4%E6%96%B0%E4%B8%A6%E7%B6%AD%E6%8C%81%E8%89%AF%E5%A5%BD%E4%BD%BF%E7%94%A8%E7%BF%92%E6%85%A3
2. https://www.bleepingcomputer.com/news/security/agelocker-ransomware-targets-qnap-nas-devices-steals-data/
3. https://portal.cert.tanet.edu.tw/docs/pdf/2020092303095959489195257290368.pdf
4. https://www.qnap.com/zh-tw/how-to/faq/article/%E6%8F%90%E5%8D%87-nas-%E5%AE%89%E5%85%A8%E6%80%A7%E7%9A%84%E6%9C%80%E4%BD%B3%E5%81%9A%E6%B3%95%E7%82%BA%E4%BD%95

3.1.2、新型態木馬 MassLogger 惡意程式透過釣魚郵件傳播

TWCERT/CC 接獲民眾釣魚郵件通報，信件主旨和內容以到貨通知等資訊引誘使用者下載惡意附件，並透過惡意程式竊取使用者個資。

該惡意檔案為 MassLogger 惡意程式，並以 xz 格式壓縮。MassLogger 是一種較新的竊取資訊程式，由.NET 語言編寫而成。該惡意程式會向 http://api.ipify.org(合法網站)發出請求，進而取得受害端的外部 IP，能夠紀錄滑鼠鍵盤事件、擷取畫面，並從 Chrome、Firefox、Outlook、Thunderbird、Discord、NordVPN、FileZilla 與 Telegram 等竊取資訊，最後透過 SMTP 回傳至惡意中繼站。

若欲索取進一步 IOC 資訊，請用企業信箱寄信至 twcert@cert.org.tw 索取，謝謝。

property	value
md5	6BEAB3FAC7E37FD1262DE3086DE9F5D0
sha1	E2C55EA0C667200D00EAF33C2E6C1A76A6657B37
sha256	8AB8448549FFA379C39811667A25D2E922C6ED440DE7CEAE541E76806D3
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40
first-bytes-text	M Z ..... @ .....
file-size	593920 (bytes)
size-without-overlay	n/a
entropy	7.900
imphash	F34D5F2D4577ED6D9CEEC516C1F5A744
signature	Microsoft Visual C# v7.0 / Basic .NET
entry-point	FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
file-version	10.0.18362.449
description	Microsoft Help and Support
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x5F7822A4 (Sat Oct 03 15:05:08 2020 - UTC)
debugger-stamp	n/a
resources-stamp	empty
exports-stamp	n/a
version-stamp	empty
certificate-stamp	n/a

圖 1 實際檔案為.NET 執行檔

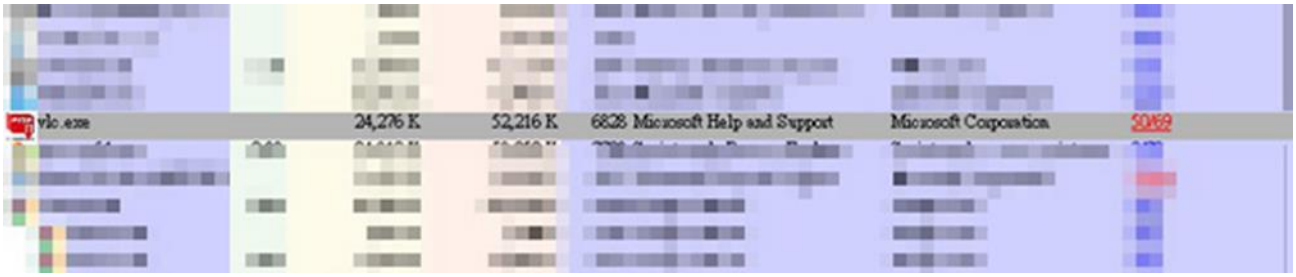


圖 2 偽裝 Microsoft 簽章的木馬程式

3.1.3、QNAP 針對 Zerologon 漏洞公布資安警訊，受影響機種用戶應更新

台灣 NAS 大廠 QNAP 日前針對 Zerologon 嚴重資安漏洞發布資安警訊，並公布受影響的 NAS 作業系統版本號碼，用戶需立即更新以修補漏洞。

全球知名的台灣網路儲存設備（NAS）大廠 QNAP，日前針對 Zerologon 嚴重資安漏洞發布資安警訊；並公布受影響的 NAS 作業系統版本號碼；建議相關用戶更新到最新的 QTS NAS 作業系統，以修補漏洞。

QNAP 說明，若用戶之 NAS 不是部署為 Active Directory 的 domain controller ，不受 Zerologon 漏洞影響。因此非相關之用戶在固定排程時更新即可，不需受時間壓力安排緊急更新。

在 QNAP 發表的資安通報中指出，微軟在本月初公布的 Zerologon（CVE-2020-1472）嚴重資安漏洞，也出現在該公司部分 NAS 機種使用的 QTS 作業系統中連接微軟網路的子系統；若不立即修補該漏洞，可能導致駭侵者用以跳過系統資安驗證程多，提升自身執行權限，遠端執行任意程式碼，並且挾持 QNAP NAS 本體並攻擊內部網路中的其他設備。

據 QNAP 發表的資安通報指出，建議相關用戶應升級到以下 QTS 版本：

- QTS 4.5.1.1456 build 20201015 與更新版本
- QTS 4.4.3.1439 build 20200925 與更新版本
- QTS 4.3.6.1446 Build 20200929 與更新版本
- QTS 4.3.4.1463 build 20201006 與更新版本

- QTS 4.3.3.1432 build 20201006 與更新版本

  擁有 QNAP NAS 設備的用戶，應立即檢查 QTS 版本並升級至最新版，以降低遭駭侵攻的的風險。

- 資料來源：

1. https://www.qnap.com/zh-tw/security-advisory/qsa-20-07
2. https://securityaffairs.co/wordpress/109859/iot/qnap-zerologon-flaw.html
3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

3.1.4、韓國多家銀行近日遭受 DDoS 勒索攻擊

TWCERT/CC 接獲國外情資分享，日前韓國多家銀行遭受 DDoS 勒索攻擊，這波 UDP Flood DDoS 分散式阻斷服務攻擊於 2020 年 10 月 2 日起陸續發生，攻擊流量介於 5Gbps 至 60Gbps 之間。除了遭受攻擊外，受害對象亦收到攻擊駭客 Fancy Bear 的勒索信件，要求支付 20 比特幣，否則將再進一步發動更猛烈的 DDoS 攻擊。

目前已知受害對象有韓國電力公司以及相關銀行業者，包含：友利銀行(Woori Bank)、韓國中小企業銀行(Industrial Bank of Korea)、韓亞銀行(KEB Hana Bank)以及釜山銀行(Busan Bank)等。

請相關單位進行 DDoS 防護檢視，建議視內部情況升級設備至最新版本、並檢視當前 DDoS 相關防護設備，以強化 DDoS 防禦能量。此外視網路設備配置與使用性，事先啟用速率限制與存取控制清單(Access Control List, ACL)功能，同時啟動入口過濾功能(Ingress Filtering)，可過濾部分遭受竄改或偽造之封包，達到資安防護目的。

3.1.5、FBI 警告美國大眾，提防經旅館 Wi-Fi 網路連線遠距工作的資安風險

美國聯邦調查局日前發表資安通報指出，由於愈來愈多美國遠距工作者選擇市區旅館進行遠距工作，應即提防透過旅館 Wi-Fi 網路進行的攻擊。

美國聯邦調查局（FBI）日前發表資安通報指出，該局觀察到愈來愈多美國遠距工作者選擇市區旅館或飯店進行遠距工作，以尋求較自家更安靜、更不受打擾的工作環境；然而透過旅館或飯店提供的無線網路，存取公司或自身的機敏資訊時，將會提高遭到駭侵攻擊的資安風險。

FBI 在這份公告中指出，使用旅館或飯店提供的 Wi-Fi 無線網路時，會面臨更高的資安風險；駭侵者可能會入侵旅館或飯店的系統，取得房客的姓名、房號、各種個資與信用卡號碼；而且所有來自四面八方的不明房客，大多會被集中在同一個網段之下，這使得網路監聽、駭侵與資料竊取變得更加容易。

另外，為了讓房客便於使用，旅館或飯店也經常將其 Wi-Fi 無線網路的帳號與密碼印在隨處可見的地方，或是印成小卡供房客索取，更不常更換密碼；所謂安全防護最多也僅是要求利用房號登入，並不能確保整個網路的安全。

更嚴重的是，由於市面上沒有針對旅宿環境無線網路的嚴密資安防護標準，因此各家旅宿業者的無線網路安全程度不一；再加上許多旅宿業者使用

的無線網路設備十分老舊，沒有定期更新韌體以修補資安漏洞；用戶也無法控制或檢視其資安設定情形，更加提高房客面臨的資安風險。

FBI 提醒所有在旅館或飯店進行遠端工作的用戶，應即提防透過旅館 Wi-Fi 網路進行的攻擊；如果發現自己的設備發生速度突然變慢、被強迫導向到其他網頁、指標或游標突然自行移動、某些應用程式突然自行開啟、電池耗電量突增，或是發現奇怪的撥出電話、外發簡訊或 Email 時，就表示可能遭到駭侵。

- 資料來源：
  1. https://www.ic3.gov/media/2020/201006.aspx
  2. https://www.techrepublic.com/article/wi-fi-security-fbi-warns-of-risks-of-using-wireless-hotel-networks/

3.2、國際政府組織資安資訊

3.2.1、美國聯邦官員正式指稱俄羅斯駭侵團體涉及入侵美國各級政府網路

美國聯邦政府政正式指稱，與俄羅斯相關的駭侵團體，涉嫌在過去數周以來針對美國各級政府發動多起駭侵攻擊。

美國聯邦政府政正式指稱，與俄羅斯相關的駭侵團體 Energetic Bear（又名 TEMP.Isotope），涉嫌在過去數周以來針對美國各級政府發動多起駭侵攻擊。

發出指控的是美國聯邦調查局（FBI）與美國資安暨基礎建設安全局（CISA）。這兩個單位於 10 月 22 日共同發布公告，指出由俄羅斯政府支持的 APT 駭侵團體，近來多次駭入美國自州政府以下的各級政府組織與航空網路，並於 2020 年 10 月 1 日成功從至少兩台以上伺服器竊取資訊匯出。

FBI 與 CISA 的公告中特別指出，該駭侵團體入侵取得的資料，以及政府網路的登入資訊，可能用來竄改重要政府網路的資安與一般設定、破壞 IT 架構、竊取各種包商與採購資訊，甚至盜印重要工作人員的通行憑證。

兩單位的公告指出，目前尚無證據顯示該 APT 團體的駭侵行為，是為了阻礙飛安、教育、選舉與政府日常運作；但未來仍可能對這些單位的正常運作造成威脅。

據資安媒體 CyberScoop 指出，TEMP.Isotope 曾在 2019 年時攻擊烏克蘭選舉，並針對歐洲與美國的能源產業發動駭侵攻擊，是個有多項前科的 APT 駭侵團體；為此 CISA 與 FBI 也特別提供關於該團體的額外防護資訊，並對選舉相關承辦單位進行簡報，以防接下來的美國大選遭到該團體侵擾。

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/alerts/aa20-296a
  2. https://www.zdnet.com/article/fbi-cisa-russian-hackers-breached-us-government-networks-exfiltrated-data/
  3. https://www.cyberscoop.com/temp-isotope-russia-cisa-election-security/

3.2.2、美國網戰司令部與微軟公司，同時開始對抗 TrickBot 僵屍網路

美國國防部旗下的網路作戰司令部與微軟公司，最近不約而同，開始對抗全球最大的僵屍網路 TrickBot，削弱其針對美國大選的影響能力。

美國國防部旗下的網路作戰司令部（US Cyber Command）與微軟公司，近期開始各自發動對抗全球最大的僵屍網路 TrickBot，削弱其針對美國大選選情的影響能力。

據不便透露姓名的美國官員指出，美國網戰司令部此次作戰計畫的目的，並不在於瓦解整個 TrickBot 僵屍網路，而在於削弱其對美國境內電腦系統的感染與破壞能力，以降低 TrickBot 僵屍網路對即將舉辦的 2020 年美國總統大選的破壞。

據華盛頓郵報在八月時對美國網站司令部司令官 Paul Nakasone 進行的書面採訪指出，Paul Nakasone 設定其最高目標是確保 2020 年美國總統大選能夠安全順暢且合法完成選舉程序。

微軟公司負責顧客資安與信件的副總裁 Tom Burt 也表示，該公司也針對 TrickBot 僵屍網路的攻擊行動，採取一系列防禦提升手段，以限制 TrickBot 僵屍網路的傳播與執行，也限制 TrickBot 僵屍網路發動勒贖攻擊的能力。

微軟表示，該公司受到東維吉尼亞地方法院的授權與要求，開始嚴密監控 Trickbot 慣常用來與遭植入惡意軟體電腦溝通的各種管道，從中收集並分

析資訊，找出 Trickbot 僵屍網路用以發號施令的控制伺服器所在 IP 並加以封鎖，或是禁止這些控制伺服器的管理者購買新的伺服器授權。

TrickBot 幕後的駭侵團體，在遭到這些反制措施後，也立即開始重整旗鼓，試圖恢復其駭侵攻擊能量。

- 資料來源：
  1. https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html
  2. https://www.cyberscoop.com/trickbot-takedown-cyber-command-microsoft/
  3. https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

3.2.3、美國選務官員指出，發現大規模可疑 Email 攻擊行動

美國選務機關指出，各地方政府的選務人員，最近遭到大規模可疑 Email 攻擊，可能意圖影響近日的總統大選選務工作。

美國選務機關「選舉基礎建設與資訊共享分析中心」（Elections Infrastructure Information Sharing and Analysis Center, EI-ISAC）指出，各地方政府的選務人員，最近遭到大規模可疑 Email 攻擊；選務官員懷疑，攻擊活動可能意圖影響近日的總統大選選務工作。

據華爾街日報獨家報導指出，在一些地方選務人員收到的詐騙 Email 中，發信人偽裝為州政府的選務高階官員，並在信中附上一個連結，要求收信的選務人員按下，以取得計票與選務資訊相關系統的二階段登入驗證顯示裝置。

雖然這是典型的釣魚詐騙郵件操作手法，不過 EI-ISAC 目前並未在這些可疑 Email 中發現任何惡意連結，也沒有任何含有惡意程式碼的檔案隨信寄送。

另外 EI-ISAC 也指出，有另一波疑似 Email 攻擊行動，偽裝成身障人士要求在家投票，寄送給選務人員尋求協助；截獲的部分 Email 試圖模仿成由選務機關回覆信件的設計，可能提高選務人員不慎點按惡意連結，或下載惡意程式的風險。

據報導，EI- ISAC 目前並沒有關於這波疑似 Email 詐騙攻擊的詳細情資，也不清楚幕後發送者是誰，也看不出攻擊行動是否有其他國家支持的跡象。但 EI-ISAC 仍舊行文給各州與地方級選務機構，要求提高資安警覺與防護能力，避免下個月初的美國總統大選遭到駭侵攻擊干擾。

- 資料來源：
  1. https://www.wsj.com/articles/election-officials-warn-of-widespread-suspicious-email-campaign-11603762090
  2. https://thehill.com/policy/cybersecurity/522892-election-officials-say-theyre-getting-suspicious-emails-that-may-part-of

3.3、社群媒體資安近況

連結預覽功能存在隱私洩漏風險

當社群軟體用戶接收到 URL 連結時，社群軟體會預先抓取連結的內容，例如圖片或是標題。無論內容為何，只要是 URL 就會在使用者非自主的情況下觸發，某方面來說也許方便，但卻隱藏著資安的疑慮。以 LINE 為例，如果有心人士發送惡意連結，此情況之下惡意連結是很容易被觸發的，甚至能透過建立惡意中繼站竊取並回傳 LINE 使用者的 IP 與地理位置。

LINE 的加密方式是屬於 End-to-end encryption(E2EE)，是一種只有參與通訊的用戶可以讀取資訊的方式，即使是 LINE 的伺服器也無法讀取原始資訊，因此也無法透過其伺服器來檢查是否為惡意連結進而提醒使用者。在眾多的社群軟體中，若有預覽連結的功能其實都有共同的風險，例如 Instagram 也能透過預覽連結來執行惡意的 JavaScript。

建議社群軟體相關用戶，關閉預覽網址功能，例如 LINE 可至「設定」→「聊天」→取消勾選「預覽網址」，以避免遭受資安攻擊而造成損失。

- 資料來源：

1. https://www.mysk.blog/2020/10/25/link-previews/
2. https://www.youtube.com/watch?v=2qY8zT_xjvY
3. https://www.youtube.com/watch?v=IyTxNHy1Wd0

3.4、行動裝置資安訊息

Google 開始針對非自身製造的 Android 裝置發出漏洞警示通報

Google 最近推出 Android Partner Vulnerability Initiative，針對非 Google 自製的第三方 Android 裝置資安漏洞發出警示通報，以提示用戶注意，並促使裝置廠商盡快推出資安更新修補程式。

Google 最近推出 Android Partner Vulnerability Initiative（APVI），主要針對非 Google 自製 Pixel 系列手機的第三方 Android 裝置資安漏洞發出警示通報；這個計畫的用意，除了提示用戶注意可能的資安風險外，並希望促使裝置廠商盡快推出資安更新修補程式，希望能加強整個 Android 生態圈的安全性。

雖然在 Google 推出 APVI 的部落格公告中，列出了數種這波通報中發現的三大漏洞類型（跳過權限同意程序、登入資訊外洩、App 過度要求存取權限等），但在 APVI 的 bug list 頁面中，則列出了自去年八月以來發現的第三方 Android 製造商被發現的各種問題；榜上有名的廠商包括華為、OPPO、Vivo、ZTE、Transsion、Meizu、Digitime、Mediatek 等。

華為手機早在 2019 八月就被提報「未經授權的第三方資料備份」問題，OPPO 和 Vivo 則於去年 12 月被提報 sideloading 問題，Mediatek 則是在今年

一月因為嚴重的 MTK-SU 漏洞而名列其上，ZTE 則同時有訊息服務和瀏覽器自動輸入密碼的安全性問題存在；不過這些漏洞目前均已修復。

尚未修復的新漏洞則有 Meizu 的 Android 系統 UI 使用 http 未加密協定載入動態程式碼問題，以及 Digitime 手機系統服務外洩問題。

Google 表示，會在問題提報時主動通知各第三方生產廠，之後才會加以公開；Google 希望以這個方式，加速各第三方廠商更新其裝置並修補漏洞的速度，因為許多 Android 第三方裝置的系統更新和資安漏洞修補動作非常緩慢，更有許多平價設備從來不曾推出更新。

- 資料來源：
  1. https://www.engadget.com/google-android-partner-vulnerability-initiative-173252320.html
  2. https://security.googleblog.com/2020/10/announcing-launch-of-android-partner.html
  3. https://bugs.chromium.org/p/apvi/issues/list?q=&can=1

3.5、軟體系統資安議題

3.5.1、Nitro PDF Services 發生資料外洩事件，多家美國大型企業受害

廣為美國企業採用的 PDF 編輯與數位簽核服務 Nitro PDF services，日前發生大規模資料外洩事件，造成多家美國大型企業客戶受害。

廣為美國企業採用的 PDF 編輯與數位簽核服務 Nitro PDF services，日前發生大規模資料外洩事件，造成多家美國大型企業客戶受害，包括 Amazon、Google、Apple、Microsoft、大通銀行、花旗銀行等均受波及。

該公司於 10 月 21 日向澳洲證券交易所發布資安通告，表示發生一起獨立的資安事件，有資料庫遭到不明第三方未經授權存取，但該資料庫不包括用戶或客戶資料與文件，也不致對公司的營運造成影響。

但事實上攻擊造成的災情，遠比聲明中描述的還要嚴重得多。資安廠商 Cyble 向資安媒體 BleepingComputer 指稱，該公司發現一批顯然來自 Nitro 公司的客戶與文件資料庫，在暗網上待價而沽，其資料庫檔案大小高達 1TB 之多。

據 BleepingCompture 報導，這一大批資料正在暗網站接受私下競標，起標價格是 80,000 美元。Cyble 說在資料庫中的某個表格，就包括七千萬筆用戶資料，包括 Email 地址、完整姓名、bcrypt 雜湊密碼、職稱、公司名稱、IP 地址與多種系統相關資訊。

據 Cyble 統計指出，在資料庫中，屬於 Amazon 公司所有的帳號數就多達 5,442 個，Google 和 Microsoft 各有三千多個、Apple 有 584 個；洩漏的文件檔案數量則以花旗銀行最多，將近 14 萬件，Google 也有高達三萬多個文件檔案遭到外洩。

Nitro PDF 的企業用戶超過十萬家公司，註冊使用者高達 180 萬人。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/massive-nitro-data-breach-impacts-microsoft-google-apple-more/
  2. https://www.itwire.com/security/nitro-pdf-maker-hit-by-breach-it-says-is-isolated-,-sec-firm-claims-otherwise.html

3.5.2、網路券商 Roinhood 約兩千用戶帳號遭駭，部分用戶資產遭盜賣

美國新興網路券商 Robinhood 發生一連串駭侵事件，用戶帳戶遭入侵；除部分個資可能外洩，甚至有用戶投資的金融資產遭到盜賣。

美國新興網路券商 Robinhood 日前發生連續駭侵事件，據估計至今約有 2000 名用戶的帳戶遭到駭客入侵；除部分個資可能外洩，甚至有用戶投資的金融資產遭到駭侵者盜賣。

第一波駭侵攻擊始於 10 月的第二周。據彭博社報導，Robinhood 針對第一波攻擊行動，僅對外提供少數資訊；該公司說僅有小批用戶的 Email 資訊外洩，並未透露更多細節。

然而由於 Robinhood 並未提供客戶服務電話供用戶查詢，因此在社群平台上發生一股抱怨潮；許多客戶想詢問自己帳號的安全狀態，卻因 Robinhood 未設有客服電話，不得其門而入。

Robinhood 持續遭到駭侵攻擊，有該公司客戶雖然設有二階段登入認證機制，但仍然發現自己帳戶下的投資資產遭到盜賣一空，之後更無法登入自己的帳戶進行查詢等操作。

也有用戶表示，收到該公司的通知，在更改密碼前會暫停帳戶交易；該名用戶認為既然帳戶被暫停交易，應該是安全的，因此未變更其密碼，結果仍然收到系統通知其投資的股票亦遭賣出。

Robinhood 客服連絡該客戶時，指出有駭侵者以假身分資料登入其帳戶，重新啟用交易後將其資產售出；目前 Robinhood 已經回復帳號與其被盜賣的資產。

- 資料來源：
  1. https://www.bloomberg.com/news/articles/2020-10-15/robinhood-estimates-hackers-infiltrated-almost-2-000-accounts
  2. https://www.cnn.com/2020/10/15/investing/robinhood-accounts-hacked/index.html

3.5.3、Barnes & Noble 網路書店遭駭當機數日

美國主要的實體暨網路書店 Barnes & Noble 日前遭到駭侵攻擊，不僅其電腦系統多日無法運作，更可能有顧客相關資料遭竊。

美國主要的實體暨網路書店 Barnes & Noble，日前遭到不明來源的駭侵攻擊，不僅其電腦系統多日無法運作，更可能有部分顧客相關資料遭到駭侵者竊取。

Barnes & Noble 的電子書 Nook 用戶，於十月十日發現無法自 Barnes & Noble 下載自己購買的電子書，也無法新購書籍；該公司發行的 Windows 與 Android 閱讀軟體也同樣無法使用，甚至連該公司的實體書店也因電腦系統當機而無法正常營業。

據 Barnes & Noble 隨後發布的公告指出，該公司的電腦系統因為這次攻擊行動，遭到「未經授權且不法的存取」；雖然其金流系統中的顧客信用卡資訊等相關金融資訊經過加密因而未遭竊取，但包括用戶輸入的 Email 地址、帳單地址、寄送地址、電話號碼等資訊則可能遭到竊取。

資安專家 Troy Mursch 分析 Barnes & Noble 此次遭駭事件時指出，該公司極可能是遭駭侵者利用 Pulse Secure VPN 的已知資安漏洞 CVE-2019-11510 入侵；該漏洞可讓駭侵者利用一個特製的 URI，即可遠端讀取 VPN 伺服器上的任何檔案，更能在 VPN 用戶端遠端執行任意程式碼；其 CVSS 危險程度評

分高達滿分 10 分。

這個漏洞雖然早在 2019 年四月就已推出修補程式，但仍有許多公私單位未及修補；導致利用此一漏洞的駭侵事件仍然十分頻繁。

- 資料來源：
  1. https://www.tripwire.com/state-of-security/featured/barnes-noble-warns-customers-hacked-customer-data-accessed/
  2. https://twitter.com/bad_packets/status/1316605119564193799
  3. https://threatpost.com/barnes-noble-hack-phishers-crooks/160148/

3.5.4、資安公司發現針對製造業大規模間諜監控攻擊

資安公司日前指出，一個名為 MontysThree 的間諜活動，再次被發現針對製造業發動間諜監控攻擊行動，竊取機密文件。

俄羅斯資安公司卡巴斯基日前發表研究報告，指出一個名為 MontysThree 的間諜活動，再次被發現針對製造業發動間諜監控攻擊行動，目的在竊取企業機密文件。

卡巴斯基表示，MontysThress 的駭侵攻擊行動，運用了多種技術以避免被發現，例如將竊得資料編碼隱藏在圖片檔案內，並且利用如 Google 與 Microsoft、Dropbox 的雲端服務，設立控制伺服器與檔案存取服務，並非自行架設。

卡巴斯基說，該公司觀察到未知的駭侵工具組，在 2018 年首次被發現後，近來又開始大舉活動的跡象；由於工具組開發者將其命名為 MT3，卡巴斯基懷疑始作俑者是新出現的 APT 組織，因此稱其為 MontysThree。

報告指出，MT3 駭侵工具組的功能，包括持續性收集各種藏在影像中的編碼資料、截取受害電腦的螢幕、竊取電腦設定資訊與檔案、加密竊得的資訊等。

MontysThree 以搜尋 Microsoft Office 和 Adobe Acrobat （PDF）檔案為主，而且只針對設定為西里爾語系（俄文即屬此語系）字元的 Windows 電腦中的資料夾與檔案，但在公有雲中發現的 sample 檔案又意圖偽裝使用中文。

卡巴斯基認為這種偽裝係為了混淆視聽，實際上專門鎖定使用西里爾語系 Windows 系統的受害目標。

- 建議採取資安強化措施
  1. 駭客鎖定製造業之員工發送釣魚郵件，並在郵件內夾帶偽裝成員工聯繫清單、技術檔案及醫療文件等惡意附件，以欺騙員工點擊下載，建議企業定期進行資安宣導、落實社交工程演練，加強員工的資安意識。
  2. 建議企業部署入侵防護與偵測相關軟體系統，企業內部網路施行分隔網段，機敏資訊進行加密及備份，降低遭受駭客攻擊之損害。

- 資料來源：
  1. https://securelist.com/montysthree-industrial-espionage/98972/
  2. https://www.bankinfosecurity.co.uk/industrial-espionage-campaign-uncovered-a-15148
  3. https://threatpost.com/montysthree-apt-industrial-targets/159957/
  4. https://cyware.com/news/montysthree-apt-showing-its-teeth-with-new-malware-toolkit-32aef459

3.5.5、資安廠商發現第二個以 UEFI 為攻擊目標的惡意軟體

資安廠商日前發現第二個以 UEFI 為攻擊目標的惡意軟體 MosaicRegressor，被駭侵團體用來攻擊亞洲、歐洲和非洲各國的外交單位。

俄羅斯資安廠商卡巴斯基日前發表研究報告，指出該公司的研究人員發現第二個以 UEFI 為攻擊目標的惡意軟體，並將其命名為 MosaicRegressor。這個惡意軟體被駭侵團體用來攻擊亞洲、歐洲和非洲各國的外交單位。

UEFI 是 Unified Extensible Firmware Interface 的縮寫，儲存在電腦主機板上的 Flash 記憶體中，是電腦開機時最先執行的軟體程式；其功能為在載入作業系統之前，預先設定好電腦上的所有硬體裝置，因此非常重要。

駭侵者如果能成功在 UEFI 中注入惡意程式碼，不但難以自作業系統中將之清除，甚至還可以做到清除掉整個受害電腦作業系統、格式化任何儲存裝置。

卡巴斯基指出，要發動 UEFI 攻擊有一定的難度；駭侵者必須能夠實體存取受害電腦，或是透過複雜的供應鏈攻擊來進行。

根據卡巴斯基的資料，MosaicRegressor 的攻擊活動記錄約自 2017 到 2019 年之間，主要的攻擊對象為亞、歐、非各國的外交單位或非政府組織；其中有兩台電腦每次重新開機後都會自動再次安裝惡意軟體，顯示其 UEFI 已遭注入惡意程式碼。

目前卡巴斯基還無法解釋整個攻擊的流程。

最早發現的 UEFI 攻擊惡意軟體係在 2018 年，由另一家資安廠商 ESET 發現；當時是由俄羅斯支持的 APT 駭侵團體 Facny Bear 用來發展 Rootkit 攻擊工具，並發動多起攻擊行動。

- 資料來源：
  1. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/10/05094208/MosaicRegressor_Technical-details.pdf
  2. https://securelist.com/mosaicregressor/98849/
  3. https://www.computing.co.uk/news/4021218/kaspersky-uefi-malware-attacks

3.5.6、微軟推出十月 Patch Tuesday 資安更新修補包，共修復 87 個資安漏洞

微軟公司日前釋出 2020 年 10 月的 Patch Tuesday 資安更新修補包，一共修復了 12 種產品內含的 87 個資安漏洞。

微軟公司日前釋出 2020 年 10 月的例行性「Patch Tuesday」資安更新修補包，一共修復了 12 種產品內含的 87 個資安漏洞；其中有 12 個漏洞為嚴重等級，微軟產品用戶應即套用更新。

這次的資安修補包一共修復包括 Microsoft Windows、Visual Studio、Microsoft Exchange Server、Microsoft Dynamics、Micorosft JET Database Engine、Microsoft Office、Microsoft Office Services & Web Apps、多種開源軟體、Azure Functions、Microsoft .NET Framework、PowerShell Get、Adobe Flash Player 和 Microsoft Windows Codecs Library 等多種產品。

值得注意的是，所有本月修復的資安漏洞，內含一些已被廣泛用來進行駭侵攻擊的嚴重資安漏洞，例如影響 Windows 10 與 Windows Server 2019 的 CVE-2020-16898；這個漏洞存在於 Windows 的 TCP/IP 堆疊，可能讓駭侵者遠端執行任意程式碼，並且取得受害系統的控制權。

這個漏洞的 CVSS 分數高達 9.8 分，非常接近滿分十分。

除了 12 個嚴重等級漏洞外，十月的修補包也修復了 74 個重要等級漏洞，一個中間等級漏洞。建議上述微軟產品的用戶，應即下載安裝，以降低

遭到駭侵攻擊的風險。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct
  2. https://www.computing.co.uk/news/4021648/microsoft-patches-87-vulnerabilities-october-2020-patch-tuesday-update
  3. https://krebsonsecurity.com/2020/10/microsoft-patch-tuesday-october-2020-edition/

3.5.7、微軟持續打擊 TrickBot 僵屍駭侵網路

微軟持續打擊意圖影響美國大選的 TrickBot 僵屍網路，已經讓超過九成的 TrickBot 控制伺服器無法運作。。

微軟日前發表資安通報，說明該公司持續打擊意圖影響美國大選的 TrickBot 僵屍網路成效。在該公司的各種封鎖行動之下，目前已經讓超過九成的 TrickBot 控制伺服器無法順利運作。

微軟指出，已經讓 TrickBot 的整體基礎架構的大多數節點無法運作，使得 TrickBot 影響十一月初美國總統大選的能力大大削弱。

微軟在開始對抗 TrickBot 僵屍網路初期，鎖定一共 69 台分布於全球的 TrickBot 控制伺服器。微軟成功停止其中 62 台的運作，其餘 7 台控制伺服器由於是以 IoT 裝置架設，非使用 Windows 系統，因此微軟仍在設法阻斷其運作。

TrickBot 幕後的主使者，很快又新設立多台控制伺服器，以維持其駭侵網路的運作；微軟再度鎖定了 59 台控制伺服器，成功封鎖了其中的 58 台。因此從總量上來看，TrickBot 集團先後設定的伺服器中，有 128 台遭微軟成功辨識，120 台被微軟設法停止其運作。

TrickBot 僵屍網路在全球感染超過一百萬台個人電腦，有能力發動大規

模的勒贖攻擊，造成美國大選電腦系統的運作障礙。

微軟表示，TrickBot 幕後主事者會繼續試圖設立新伺器，並避免微軟的封鎖行動；微軟呼籲資安界共同打擊 TrickBot，特別是有可能託管 TrickBot 主機的 ISP 業者，應該一同阻止 TrickBot 重起爐灶。

- 資料來源：
  1. https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/
  2. https://www.reuters.com/article/us-usa-election-cyber-botnet/microsoft-disables-most-of-cybercriminals-control-over-massive-computer-network-idUSKBN2752JK
  3. https://www.securityweek.com/new-trickbot-control-servers-unable-respond-bot-requests

3.6、軟硬體漏洞資訊

3.6.1、微軟澄清 Zerologon 嚴重漏洞的正確修補方法

有鑑於先前提供的 CVE-2020-1472 Zerologon 漏洞更新情報的混淆，微軟日前再次發布關於此漏洞的修補方法，以更清楚地方式說明如何修補此嚴重漏洞。

日前微軟針對一個近來受到高度注目，可能造成極嚴重攻擊事件的 Zerologon 漏洞（CVE-2020-1472）發布更新修補訊息；然而許多用戶感到混淆，也無法確認更新後是否就能抵禦針對此漏洞的攻擊。

CVE-2020-1472 是存在於微軟 Netlogon 的極嚴重資安漏洞，其 CVSS 危險程度評分高達滿分的十分；駭侵者可利用此漏洞控制整個內網，任意變更用戶的登入資訊，並且執行任意程式碼。

更危險的是，傳統上利用其他漏洞，要達到上述駭侵效果，相當費時費力；但利用 Zerologon 的駭侵攻擊，幾分鐘內就可以完全掌握受害者內網，因此幾乎沒有充足時間加以抵禦。

在 Zerologon 漏洞公開之後不久，就發現多起以此漏洞進行的駭侵攻擊事件；修補各單位內網的 Zerologon 漏洞，更顯刻不容緩。

為此，微軟再度發布關於 Zerologon 的修補說明，提供了更詳細的說明文件，詳細說明更新操作步驟。

在這篇新的更新文件中，微軟強調四個更新步驟：

- 更新網域控制站：安裝 2020 年 8 月 11 日或之後發行的軟體更新；
- 檢視事件記錄檔，找出存有連線漏洞的內網裝置；
- 處理這些存有漏洞的裝置，包括安裝所需的軟體更新、啟用「強制模式」等；
- 在整個內網環境中啟用「強制模式」，以修補所有 CVE-2020-1472 的漏洞。

文件中針對每個步驟，都有詳細的操作說明，用戶應立即依文件說明更新網域內的各種 Windows 裝置。

- CVE 編號：CVE-2020-1472

- 資料來源：
  1. https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
  2. https://www.bleepingcomputer.com/news/security/microsoft-clarifies-patch-confusion-for-windows-zerologon-flaw/
  3. https://support.microsoft.com/zh-tw/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

3.6.2、Microsoft Azure 遭發現漏洞，駭侵者可能接管用戶伺服器

資安廠商 Intezer 日前發布資安研究報告，指出該公司的研究人員發現 Microsoft Azure 雲端服務存有兩個漏洞，可導致駭侵者遠端執行任意程式碼，並接管用戶的伺服器。

發生問題的是 Microsoft Azure 的 App Services，可供客戶託管各種 web 服務；研究者發現在 App Services 中的 Linux 主機存有兩個資安漏洞，可供駭侵者進行伺服器端請求偽造（Server-side Request Forge，SSRF）攻擊，以及遠端執行任意程式碼，導致用戶的主機權限遭駭侵者取得。

研究人員指出，第一個 SSRF 漏洞發生在 Azure App Services 使用的開源套件 KuduLite，這個套件是讓註冊戶用管理其 App Service 方案；研究人員發現 KuduLite 的程式碼將 SSH 安全連線使用的密碼硬寫（hard-coded）在其程式碼中，可因此取得 root 登入身分。

第二個漏洞發生在 KuduLite 的 API，應用程式節點可以在未經存取權限驗證的情況下，向 KuduLite 發送存取要求；攻擊者可以利用這個漏洞來存取應用程式節點的檔案系統，甚至可以竊得該節點儲存的應用程式原始碼與其他資源。

Intezer 是在三個月前發現這兩個漏洞，隨即向 Microsoft 提報；而 Microsoft 很快就修復了這兩個漏洞，因此這兩個漏洞沒有 CVE 編號。

- 影響產品/版本：Microsoft Azure App Services
- 解決方案：已解決

- 資料來源：
  1. https://www.intezer.com/blog/cloud-security/kud-i-enter-your-server-new-vulnerabilities-in-microsoft-azure/
  2. https://threatpost.com/microsoft-azure-flaws-servers-takeover/159965/

3.6.3、美國網戰司令部要求立即修補 Windows TCP/IP 漏洞

美國網路作戰司令部（US Cyber Command）日前發表推文，指出必須立即修補嚴重的 Windows TCP/IP 堆疊漏洞「惡鄰居」（Bad Neighbor）。

美國網路作戰司令部（US Cyber Command）日前發表推文，指出必須立即修補嚴重的 Windows TCP/IP 堆疊漏洞「惡鄰居」（Bad Neighbor），以免 Windows 電腦遭到 DoS 攻擊而出現「藍色死亡畫面」（BSOD），造成電腦當機無法使用。

美國網戰司令部在推文中要求 Windows 用戶應立即安裝微軟甫推出的十月 Patch Tuesday 資安修補包，以修補 CVE-2020-16898 這個資安漏洞，以免電腦系統遭到遠端攻擊。

CVE-2020-16898 漏洞存在於 Windows 10 版本 1709 到 2004、Windows Server 2019 版本 1903 到 2004 的 TCP/IP 堆疊服務；這個被微軟稱為「惡鄰居」的漏洞，可讓駭侵者遠端執行任意程式碼。駭侵者只要在內網中對受害電腦發出特製的 ICMPv6 路由廣播封包，即可觸發此一漏洞。

這個漏洞的 CVSS 危險程度評分高達 8.8 分，影響所有現今廣泛使用的 Windows 版本，用戶必須特別提高警覺。

多家資安廠商針對這個漏洞發表攻擊概念證實程式，包括 McAfee、Sophos 等公司都展示了透過這個漏洞進行 DoS 服務阻斷攻擊，導致電腦出現

藍色死亡畫面的過程；Sophos 甚至發展出利用此漏洞進行遠端執行任意程式碼的方法。

- CVE 編號：CVE-2020-16898
- 影響產品/版本：Windows 10 版本 1709 到 2004、Windows Server 2019 版本 1903 到 2004
- 解決方案：安裝微軟於十月中發布的 Patch Tuesday 資安修補包

- 資料來源：
  1. https://twitter.com/US_CYBERCOM/status/1316150332498608128
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
  3. https://www.bleepingcomputer.com/news/security/us-cyber-command-patch-windows-bad-neighbor-tcp-ip-bug-now/

3.6.4、Google 推出新版 Chrome，解決已遭大規模利用的 0-day 資安漏洞

Google 最近推出最新版本的 Google Chrome 86.0.4240.111，修補多個資安漏洞，其中包括一個已被廣泛用於駭侵攻擊的記憶體崩潰錯誤。

這個漏洞的編號為 CVE-2020-15999，其 CVSS 危險程度評分分數高達 7.7，屬於「嚴重」(critical) 等級。漏洞存在於 Google Chrome 用以處理 FreeType 字體的程式庫；駭侵者可利用特製的 TTF 字型檔案，誘發記憶體崩潰，藉以遠端執行任意程式碼。

據資安廠商 Cybersecurity Help 指出，這個 CVE-2020-15999 已遭駭侵者大規模使用；未及更新 Google Chrome 的用戶，有可能因為這個漏洞而遭到攻擊，導致整個電腦系統被駭侵者挾持。

Google 內部的資安研究團隊 Project Zero 率先發現這個 0-day 漏洞，雖然漏洞相關細節在此前並未公開，但顯然已遭駭侵者掌握，用以發動攻擊。

資安專家也指出，由於修補此一漏洞的程式碼可在 FreeType 的開源專案中檢視，因此駭侵者也很可能在未來數周之內利用逆向工程，找到觸發漏洞的方法，並加入其駭侵工具之中。

所有 Google Chrome 各平台與各版本用戶，皆應立即升級至 86.0.4240.111 或更新版本，以避免遭駭侵者透過此漏洞發動攻擊。

- CVE 編號：CVE-2020-15999
- 影響產品/版本：Google Chorme 各平台 86.0.4240.111 先前版本
- 解決方案：升級至 Google Chorme 86.0.4240.111 及之後版本

- 資料來源：
  1. https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html
  2. https://twitter.com/benhawkes/status/1318640422571266048
  3. https://www.cybersecurity-help.cz/vdb/SB2020102038
  4. https://www.zdnet.com/article/google-releases-chrome-security-update-to-patch-actively-exploited-zero-day/

3.6.5、Google 與 Intel 力促 Linux 用戶升級作業系統核心

Google 與 Intel 日前共同針對 Linux 的藍牙嚴重資安漏洞發布資安通報，力促用戶升級 Linux 核心，以免遭駭。

Google 與 Intel 日前共同針對 Linux 藍牙通訊協定堆疊的嚴重資安漏洞 BleedingTooth 發布資安通報，力促用戶升級 Linux 核心至 5.10 以上版本，以避免遭駭侵者利用此漏動發動攻擊。

這個稱為 BleedingTooth 的漏洞，發生在 Linux 使用的開源藍牙通訊協定堆疊 BlueZ 程式庫上；Linux 自核心版本 2.4.6 就開始使用 BlueZ 處理藍牙通訊。據 Google 發表的資安通報指出，駭侵者可利用特製的 l2cap 輸入封包誘發 BleedingTooth 漏洞，從而提升程式碼執行權限，進行 DoS 攻擊或以核心權限執行任意程式碼。

這個編號為 CVE-2020-12351 的漏洞，其 CVSS 危險程度評分高達 8.3 分；由於許多具備藍牙連線能力的 IoT 裝置，多半也使用 Linux 做為作業系統，因此潛在可能遭駭的裝置數量極多。

Google 也在 GitHub 中發布了利用 BleedingTooth 攻擊 Linux BlueZ 的概念實作程式碼。

Intel 也在近日針對 BleedingTooth 漏洞發表資安通報，指出 BlueZ 已經提供 Linux 核心程式碼的修補更新，用戶應即將裝置內的 Linux 核心升級至

5.10 或更新版本，以修補 BlueZ 漏洞。

- CVE 編號：CVE-2020-12351
- 解決方案：將裝置內的 Linux 核心升級至 5.10 或更高版本

- 資料來源：
  1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12351
  2. https://github.com/google/security-research/security/advisories/GHSA-h637-c88j-47wq
  3. https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html
  4. https://threatpost.com/google-intel-kernel-bug-linux-iot/160067/

3.6.6、Apple T2 晶片遭發現存有無法修復的資安漏洞

資安廠商發現廣泛用於 Apple Mac 系列電腦的 T2 安全晶片，內含一個不可修復的資安漏洞，將可能導致駭侵者取得 root 權限。

資安廠商 ironPeak 的研究人員日前發表研究報告，發現廣泛用於 Apple Mac 系列電腦的 T2 安全晶片，內含一個不可修復的資安漏洞；該漏洞將可能導致駭侵者取得 root 權限。

報告指出，現用於 Mac 系列電腦中的 T2 晶片，係基於 Apple A10 處理器，因此先前發生在 A10 及較舊處理器的 checkm8 漏洞依然存在，可以套用過去以該漏洞為 iPhone 越獄的類似手法，用以入侵 Mac 電腦。

由於 T2 晶片的 debugging 模式並不會進行任何身分認證，就能夠進入 Device Firnware Update (DFU) 狀態，因此理論上可以製作一個能自動進入 DFU 模式並注入惡意軟體的 USB-C 界面攻擊硬體，並取得完整的 root 權限。

研究報告也指出，這個漏洞只存在於現行使用 A10 晶片為基礎的 T2 晶片；未來 Apple 將推出的 Intel 處理器新款 Mac，以及改採自家 Apple Silicon 處理器的新款 Mac，由於其 T2 晶片改以已修補此漏洞的 A12 處理器為基礎，因此不受這個漏洞的影響。

研究報告也指出，由於要利用該漏洞進行駭侵攻擊，必須透過實體連線，也就是說必須透過 Mac 的 USB-C 連接埠寫入資料，因此使用者只要提高警覺，避免來源不明的裝置插上電腦，即可有效阻絕駭侵者利用此漏洞進行攻擊。

- 參考資料：

1. https://ironpeak.be/blog/crouching-t2-hidden-danger/#security-issues
2. https://appleinsider.com/articles/20/10/05/apples-mac-t2-chip-has-an-unfixable-vulnerability-that-could-allow-root-access

3.6.7、Adobe 修復電商平台 Magento 兩個可引發遠端執行任意程式碼的資安漏洞

Adobe 日前發表資安修補包，修復旗下電子商務平台 Magento 的兩個嚴重資安漏洞；這兩個資安漏洞可導致駭侵者任意讀寫資料庫，甚至遠端執行任意程式碼。

CVE-2020-24400 漏洞的類型為 SQL 注入漏洞，利用這個漏洞，駭侵者將可在沒有得到授權的情形下，任意讀取並寫入資料庫，造成資料外洩甚至被竄改。

CVE-2020-24400 的 CVSS 危險程度評分為 6.3 分。

CVE-2020-24407 漏洞存在於檔案上傳的檔名檢查機制不夠嚴謹，當使用允許清單上傳檔案時，不會檢查完整的檔案名稱與副檔名，導致取得系統管理者權限的駭侵者可以跳過驗證程序，直接上傳惡意檔案並遠端執行任意程式碼。

CVE-2020-2447 的 CVSS 危險程度評分亦為 6.3 分。

Adobe 於 10 月 15 日發表的資安修補包，除了上述的兩個嚴重漏洞外，另外也修複了多達 7 個其他較不嚴重的資安漏洞，包括四個不夠完備的認流程漏洞，可讓駭侵者存取受限資源、XSS 漏洞，讓駭侵者可透過瀏覽器執行任意 JavaScript 等等。

這些漏洞發生在 Magento 商業版 2.4.0 與 2.3.5-p1 先前版本，以及 Magento 開源版 2.4.0 與 2.3.5-p1 先前版本。用戶只要更新到 2.4.1 版本之後，

即可修補這些漏洞。

- CVE 編號：CVE-2020-24407、CVE-2020-24400
- 影響產品/版本：Adobe Magento 商業版 2.4.0 與 2.3.5-p1 及先前版本、Adobe Magento 開源版 2.4.0 與 2.3.5-p1 及先前版本
- 解決方案：升級到 Magento 商業版、開源版 2.4.1 及後續版本

- 參考資料：
  1. https://helpx.adobe.com/security/products/magento/apsb20-59.html
  2. https://www.cybersecurity-help.cz/vdb/SB2020101517
  3. https://threatpost.com/critical-magento-holes-online-shops-code-execution/160181/

3.6.8、NVIDIA 發表重要軟體更新，修復 GeForce Experience 三個資安漏洞

全球繪圖晶片大廠 NVIDIA 日前針對旗下 NVIDIA GeForce Experience （GFE）的 Windows 版本應用軟體，發表資安修補更新，一共修補三個資安漏洞。

這三個資安漏洞中，最嚴重的是 CVE-2020-5977，發生在 NVIDIA Web Helper NodeJS Web Server 中，若有駭侵者將某個不受控制的搜尋路徑載入到節點模組時，就會引發錯誤，可導致駭侵者遠端執行任意程式碼、發動 DoS 攻擊、提升執行權限，並且竊取資料。

這個 CVE-2020-5977 的 CVSS 危險程度評分高達 8.2 分。

另一個高危險資安漏洞的編號是 CVE-2020-5990，CVSS 危險程度評分亦高達 7.3 分；這個漏洞發生在 ShadowPlay 模組中，駭侵者可用以提升自身執行權、遠端執行任意程式碼、發動 DoS 攻擊並且竊取資料。

第三個得到修補的漏洞是 CVE-2020-5978，可讓駭侵者提升執行權限或發動 DoS 攻擊；CVSS 評分為 3.2 分。

這三個漏洞的修補更新於 2020 年十月發行，使用 NVIDIA GeForce GTX 繪圖卡的 Windows 系統用戶，應立即下載並執行更新，以降低遭到駭侵者利用此批漏洞發動攻擊的風險。

- CVE 編號：CVE-2020-5977、CVE-2020-5990、CVE-2020-5978
- 影響產品/版本：GeForce Experience Windows 版 2.30.5.70 之前版本
- 解決方案：下載並執行 2020 年十月 NVIDIA 發行的資安修補更新軟體

- 參考資料：

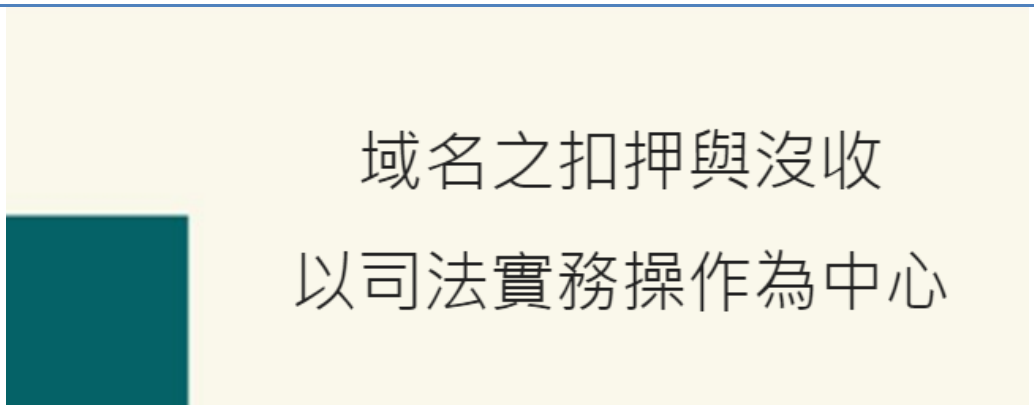
1. https://nvidia.custhelp.com/app/answers/detail/a_id/5076
2. https://www.nvidia.com/en-us/geforce/geforce-experience/
3. https://www.bleepingcomputer.com/news/security/nvidia-patches-high-severity-geforce-experience-vulnerabilities/

第 4 章、 資安研討會及活動

探索 2021 資安市場-由以色列觀點出發	
活動時間	**2020 年 11 月 19 日（四）14:00-15:40**
活動地點	**線上參與，活動前一天發送會議連結**
活動網站	**https://explorenextcybertaiwan.godaddysites.com/from-israels-perspective**
活動概要	 **主辦單位：經濟部工業局** 以色列人口不過 900 多萬，卻以科技新創發展聞名國際，吸引超過 500 家跨國企業進駐研發，人均專利數位居世界第五。再者，國際跨國科技企業紛紛設立研發中心，在以色列扮演重要角色，科技大廠超過 500 家、來自 60 國的跨國企業，領域含概資安、半導體、通訊、生醫及金融科技等，由於以色列與美國連結非常深，當地有半數跨國企業都是美國公司，其次為德、法、中與英國。因此，以色列在歐美建立多元的商業關係與人際脈絡，我國資安業者若能進入以色列市場發展或者了解以色列前進國際市場思維等，將有助於台灣資安產業進入國際市場。 反觀台灣，台灣資安公司國際化能力相對偏低。有鑑於此，經濟部工業局委由工研院舉辦【探索 2021 資安市場 - 由以色列觀點出發】，希望透過交流引台灣資安業者進入以色列市場，累積國際市場的開發能量，提高台灣資安產業的國際市場能見度。

Cyberspace 2020 聯合研討會	
活動時間	**2020 年 11 月 20 日 (星期五)**
活動地點	**國立台北商業大學**
活動網站	**https://cyber2020.cc-isac.org/announce.php**
活動概要	 **主辦單位：NTUB、ACFD、TTU、NTUT、CISA、TAIFO** 數位治理：數位科技、數位創新、數位健康與資安治理 第二十二屆「網際空間：資安、犯罪與法律社會」學術暨實務研討會 暨 第十一屆「數位生活與環境：數位科技、數位內容、數位產業、數位服務與數位安全」產學研討會 11/20 更安排了 3 場專題演講、1 場焦點座談、2 場實務論壇、1 場綜合意見交流，千萬別錯過！ 【會議主題】 數位與資通安全治理 數位創新服務 數位健康與生活 數位科技與資安治理

Google Cloud 資安攻略，打造更安全的雲端環境	Google Cloud Security Overview	
活動時間	**2020/11/20(五) 10:30~11:30**
活動地點	**線上直播**
活動網站	**https://www.accupass.com/event/20081002354251397149 60**
活動概要	 **主辦單位：Cloud Ace Inc. 雲一有限公司** 此活動為線上活動，購票後可於票券頁進入直播連結 講座議程： A. 常見雲端資安問題 B. GCP 防禦縱深 C. G Suite 360 度無死角防護 (保管箱，DLP，裝置管理，Chromebook 限制 IP 登入)

[台灣網路講堂]域名之扣押與沒收 以司法實務操作為中心	
活動時間	**2020/11/20(五) 14:00~16:20**
活動地點	**IEAT 會議中心 8F 綜合教室（臺北市中山區松江路 350 號,台北市進出口商業同業公會）**
活動網站	**https://www.ihub.tw/Calendar/ihub20201120**
活動概要	 **主辦單位：TWNIC、TWIGF、NII** 本場次同時提供線上直播，請於報名表單中正確填寫，即可於會議開始前收到直播通知。 縱有諸多案例，但針對域名之扣押或沒收，在國內的司法實務上尚未為常見之處置，而當域名可成為法律上扣押與沒入之標的時，域名管理與法律體系的法制探討自有其必要。本場講堂活動邀請到司法與執法代表以及律師，以目前域名扣押與沒收在包括偵查、訴訟及司法判決與執行等方面的法律實務進行深入探討，試圖進一步透過對域名之扣押與沒收，來檢視我國目前之司法實務操作。

資訊安全防護及案例分享研討會	
活動時間	**2020/11/20(五) 14:00~16:30**
活動地點	**台南市永康區南台街 1 號 (南臺科技大學 E 棟 604)**
活動網站	**https://www.accupass.com/event/201028061340206880950 7**
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 活動介紹： 資訊設備日益普及，企業或個人購買價優質精的產品以提高需求與效率。但在享受各項設備帶來的便捷快速時，『資訊安全』的重要的議題便隨之而至。 網路犯罪、資料洩漏已是企業面臨最大的風險之一，而資訊安全是用來保護電腦系統、網路和資料等各類資訊技術的完整性，以避免遭受攻擊、毀損或出現未經授權的存取動作。 企業若想在數位轉型領域具備競爭力，就必須了解如何從設計階段開始就採用安全解決方案！ 歡迎與我們一起共同參與，相信您一定能收穫滿滿！

第 5 章、 2020 年 10 月份資安情資分享概況

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

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

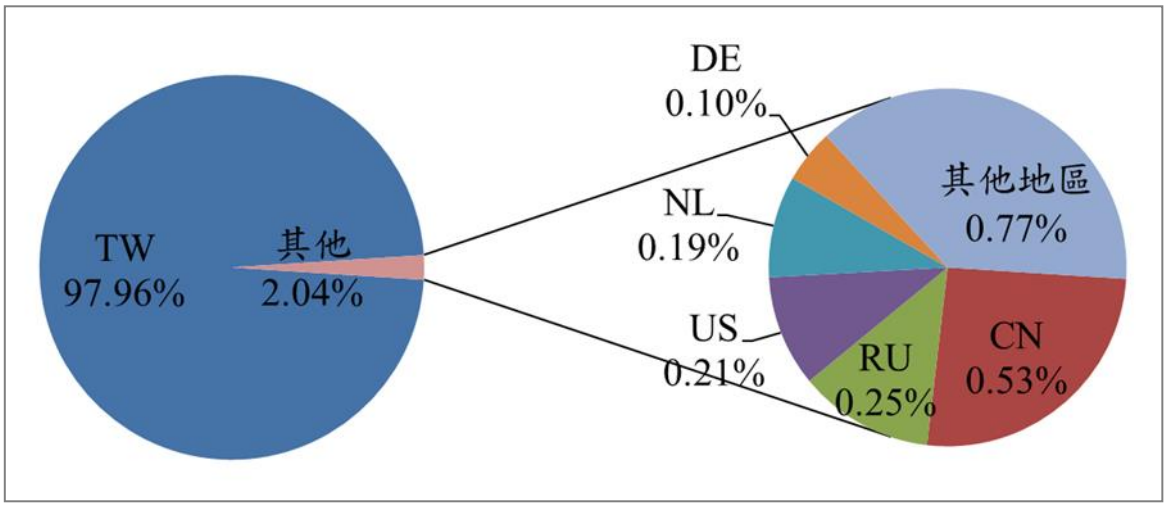


圖 1、分享地區統計圖

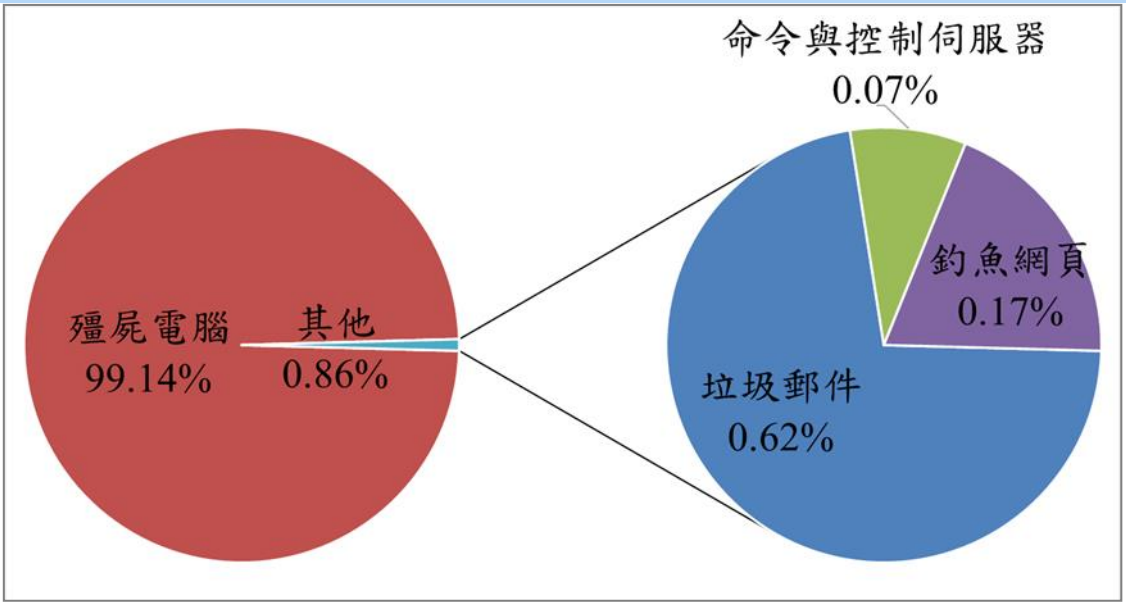


圖 2、分享類型統計圖

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

出刊日期：**2020 年 11 月 10 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**