TWCERT/CC 資安情資電子報

2021 年 3 月份

目錄

第 1 章、 封面故事

荷蘭資料中心遭 APT 駭侵團體埋設駭侵控制伺服器

資安廠商發現荷蘭境內的資料中心，遭伊朗 APT 駭侵團體駭入設立用以攻擊全球目標的控制伺服器。

資安廠商 Bitdefender 與 Argos 日前聯合發表研究報告，指出荷蘭境內有若干資料中心內的主機，遭伊朗 APT 駭侵團體駭入，用以設立攻擊全球目標的控制伺服器架構（Command and control）。

據報告說，伊朗 APT 駭侵團體，在荷蘭境內總共架設了兩組駭侵攻擊控制伺服器架構；其中一組使用的實體伺服器已經遭到緝獲，另一組的伺服器仍在積極查緝之中。

報告指出，架設這兩組控制伺服器的伊朗 APT 駭侵團體是 Infy，最早的攻擊活動記錄可追溯到 2016 年；他們在荷蘭資料中心的主機上植入了兩個惡意軟體，一個名為「Tonnerre」（即法文的雷鳴），另一個名為「Foudre」（即法文的閃電）；透過這兩個惡意軟體，發動全球規模的間諜監聽攻擊。

據 Bitdefender 的資安專家指出，這些駭侵控制器對伊朗的國際監控活動可能十分重要；當資安專家開始進行調查作業時，立刻被設立這些控制伺服

器的駭侵者發現，並且立即採取對應行動。

專家也說，他們發現這些控制伺服器的布建，已經長達三年之久。被植入惡意軟體的主機，是由美國的網站托管服務廠商 Monstermeg 所擁有，而出資向 Monstermeg 租用托管服務的公司，註冊於賽普勒斯，公司擁有人則是來自羅馬尼亞。由於都使用比特幣支付托管費用，因此也難以透過金流追蹤事件關係人。

調查單位透過分析，掌握了被這組控制伺服器駭侵監聽的對象；受駭者遍及世界各國，包括瑞典、美國、荷蘭、歐洲多國、伊拉克、印度等。

- 資料來源：
  1. Iranian APT Makes a Comeback with“Thunder and Lightning”Backdoor and Espionage Combo
  2. Iran using Dutch data center for espionage: report
  3. Iranian APT campaign hosted in Dutch data centers

第 2 章、 資安小知識

提防假冒銀行之網路釣魚詐騙

近期發現有偽冒銀行名義詐騙案例，詐騙集團假借各家銀行名義發送釣魚信件及簡訊，請客戶提供網路銀行相關登入或交易驗證資料，騙取用戶個資等相關資料。

詐騙簡訊內容以網路銀行版本更新、綁定用戶帳號等理由，發送釣魚信件及簡訊，請客戶點選連結，有銀行客戶按照指令操作，結果收到匯款完成通知，高達數十萬的存款一夕之間被匯出，才知道收到的是詐騙簡訊，近期陸續有民眾受害，因此特地提醒，對於可疑或不清楚之網址，必須輸入網路銀行登入帳號密碼或交易驗證資訊時，請民眾務必特別留意，以免上當受騙。

- 相關詐騙手法如下：

(一)、詐騙集團假借銀行名義發送釣魚信件與簡訊，並申請與銀行相似度極高之假網址使客戶混淆(例如多一個字母「a」，或拼音近似之手法，詐騙網址所設立「xxxxxbaank.com」、「xxxxxbonk.com」等連結，與銀行網址極為類似)。

(二)、模仿銀行請客戶點選網址連結，過程中輸入帳號密碼或身分證字號，過程中出現以假亂真的網銀頁面，騙取客戶帳號密碼等重要資訊。

(三)、詐騙集團竊取銀行客戶的帳號密碼等資料後，至銀行之官方網路銀行進行轉帳，俟受害客戶收到匯款通知簡訊時，方知受騙。

- 建議措施：

1. 銀行通常不會發電子郵件與簡訊，請客戶點選網址進行網路銀行帳號密碼登入相關資料。故若收到銀行名義之信件及簡訊，請務必比對及確認網址是否原來使用之官方網址，若不是則勿點選該網址，以避免落入詐騙集團陷阱。
2. 若不慎點擊可疑網址，可透過網址比對判斷網站的真實性。亦可觀察網站的部分按鈕、連結是否有正常反應，也可能出現輸入任何帳號密碼都能登入的狀況，此可輔助使用者對釣魚網站之判斷。
3. 使用者應由官方網站、App 登入，防止駭客以釣魚網址盜取網路銀行帳號密碼等資訊。
4. 如果有任何疑慮，擔心帳號遭駭客入侵，可先聯繫銀行客服專線或內政部警政署 165 反詐騙諮詢專線。
5. 若發現可疑網址，可至 TWCERT/CC 之 Phishing Check 釣魚網站通報進行通報，TWCERT/CC 確認後會協助釣魚網站下架服務。
6. 詐騙集團不只偽冒銀行之釣魚網站，平常熟悉的網站或社群平台，也有可能

遭作假，建議民眾務必觀察是否為官方網址，於網站輸入個資必須謹慎小心，以降低個資外洩及錢財損失的風險。

- 資料來源：
  1. 「您的銀行帳戶顯示異常」？已有 21 人受害共損失 300 萬，4 步驟防範釣魚簡訊
  2. 詐騙集團鎖定各網銀，4 招防釣魚簡訊盜帳密
  3. 銀行釣魚簡訊頻傳 金管會提醒民眾小心不明連結
  4. 假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華、台新銀行後，中國信託今日也出現遭冒名的狀況，金融業者與民眾可千萬注意

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、製造用網路系統遭發現的資安漏洞，近年來快速增加

資安研究單位指出，在製造業使用的工業控制系統中發現的資安漏洞數量，近年來有大幅增加的現象。

資安廠商 Clatory 日前發表研究報告指出，在製造業使用的工業控制系統中發現的資安漏洞數量，近年來有大幅增加的現象；這是因為有愈來愈多的資安廠商和研究單位，將其研究範圍轉向工業製造領域所致。

Clatory 在這份報告中說明，這些被找出來的漏洞，主要集中在工業製造中包括關鍵製程、能源、供水、廢水處理和採購販售相關的系統內。

報告指出，在 2020 年，59 家資安相關業者，在製造業系統中共找出 893 個可用於駭侵攻擊的資安漏洞；這個數字在 2018 年是 672 個，在 2019 年則是 716 個，呈現逐年大幅成長的趨勢。

而在 2020 年上半年發現了 449 個資安漏洞，高達 71% 的漏洞屬於遠端執行任意程式碼漏洞，而且所有被發現的資安漏洞，絕大多數都列在 MITRE 發表的「2020 年最危險的 25 個軟體弱點」清單中，都很容易用於攻擊，並且造成毀滅性的損害。

值得注意的是，報告也提到在 2020 年上半年提報製造業系統資安漏洞的資安廠商或研究單位，多了 50 家過去不曾提報的新面孔；這表示整個資安業界，對於發生在製造業領域的資安漏洞與其攻擊事件，投注了更多資源加以關注。

報告說，一方面近年來發生在製造業領域的資安攻擊事件大量增加，吸引資安防護業者的投入；這也使得在製造業資安領域中發現的資安漏洞，數量大幅增加。

- 建議採取資安強化措施

1、建議業者針對已公布之資安漏洞進行軟硬體或設備的修補更新，因漏洞公開之後可能會遭到駭客濫用，進而發動駭侵攻擊，造成業者的損失。

2、安裝防毒軟體及防火牆，確保其保持最新狀態，並於廠商推出安全性更新時，即時、定期更新電腦系統、軟體或設備等。

3、進行網路分區隔離，工控系統之設備避免與外界網路接觸，制定並加強存取控制措施。

4、定期備份檔案於不同設備、地點，建立快速復原機制。

- 資料來源：

1. CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 2H 2020
2. Industrial Networks See Sharp Uptick in Hackable Security Holes
3. 2020 CWE Top 25 Most Dangerous Software Weaknesses
4. MITRE 發布的 2020 最危險軟體漏洞類型 Top 25 的列表
5. 2020 年最大 OT 風險出爐：35%的關鍵基礎設施曾暴露易遭攻擊的服務

3.1.2、2020 年資安調查：勒贖攻擊與釣魚攻擊大幅增加

資安廠商發表 2020 年度資安攻擊分析報告，指出由於疫情與在家工作，導致各種釣魚攻擊與勒贖攻擊，數量較 2019 年大幅增加。

資安廠商 Proofpoint 日前發表 2020 年度資安攻擊分析報告。報告指出由於全球肺炎疫情大流行與在家遠距工作興起，導致各種釣魚攻擊與勒贖攻擊變得更為猖獗，案件發生數量和造成的損失，均較 2019 年大幅增加。

這份報告針對德國、日本、西班牙、美國、英國、奧地利、澳大利亞等七國的 600 多位資訊產業領袖與資安專家，以及超過 3,500 名工作者進行訪談，同時分析近六千萬起各型資安攻擊事件，得到報告的各項統計結果。

報告指出，有超過 75% 的企業，在 2020 年曾經遭到勒贖攻擊影響；其中一半以上的企業都支付贖金以取回被加密的檔案，但在這半數支付贖金的企業之中，只有六成左右的企業確實成功取回檔案，剩下的四成企業被駭侵者要求提高贖金，贖金增加幅度和 2019 年相比，提高了 320%。

在釣魚攻擊方面，報告也提供了最新統計數字。光是在美國，釣魚攻擊的發生次數較 2019 年就增加了 14%，比全球其他國家的數字要高出 30%。

在釣魚攻擊的類型方面，不針對特定對象的綜合性釣魚詐騙持續不斷，但針對特定攻擊對象，特別是針對特定企業，結合社交工程攻擊的「魚叉式釣魚 BEC 攻擊」，數量也大幅上升。

報告說，由於企業內仍有許多資安訓練及資安意識不足的員工，因此透過 Email 發動的攻擊，仍是最容易進行的攻擊手法之一；但透過社群平台進行的社交工程攻擊、以深度偽造技術假冒主管語音進行的「vishing」攻擊，以及透過簡訊或文字即時通訊平台發動的「smishing」等，在 2020 年的發生次數也大幅增加。

- 資料來源：
  1. 2021 State of the Phish Report
  2. Ransomware Demands Spike 320%, Payments Rise

3.2、新興應用資安

3.2.1、惡意挖礦駭侵團體將控制伺服器 IP 位址藏於比特幣區塊鏈中

Akamai 資安團隊發現，有某個以惡意挖礦為主要駭侵攻擊手法的駭侵團體，將其控制伺服器的 IP 寫入 Bitcoin 交易用的區塊鏈資訊中，導致該資訊無法更改，更無法下架。

Akamai 旗下的資安研究團隊近期發現，有某個以惡意挖礦僵屍網路為主要駭侵攻擊手法的知名駭侵團體，將其控制伺服器的 IP 寫入 Bitcoin 交易用的區塊鏈資訊中隱藏起來，導致該資訊無法更改，更無法下架。

Akamai 研究團隊是在研究駭侵團體如何躲避其取樣使用的「甜餌」（honeypot）時，發現這種新的操作手法。

報告指出，這個駭侵團體通常會先利用某些已知的遠端執行任意程式碼漏洞，例如在 Hardoop Yarn 與 Elasticsearch 的 CVE-2015-1427 或 ThinkPHP 的 CVE-2019-9082 來進行先期駭入攻擊，植入並執行可下載更多惡意軟酬載的 shell script 後，接下來載入新的惡意軟體，一方面關閉受害系統上的資安防護相關程式、偵測並移除類似的其他惡意軟體以避免競爭系統資源，然後一邊進行挖礦，一邊在內部網路上尋找更多潛在可駭侵對象，以擴大感染。

由於這類攻擊流程，會透過 cron jobs 與 rootkits 以確保惡意軟體留在系統上，並且保持運作與更新，傳統上必須將控制伺服器的 IP 寫在 crontabs

與設定檔中，很容易被發現，並且循線緝獲控制伺服器，造成惡意軟體無法運作；Akamai 自 2020 年 12 月開始發現變種惡意軟體採取新的手法，透過某個 API 來存取某個 Bitcoin 錢包，並且從接收到的區塊鏈資料中解析出控制伺服器的 IP 資訊。

這種手法使得駭侵團體可以快速更新整個駭侵控制系統的資訊，因為只要放一點小額 Bitcoin 到指定錢包之中，就可以更新控制伺服器的位址，讓惡意軟體恢復運作。再加上 Bitcoin 區塊鏈無法修改也無法下架，使得資安界更加難以封鎖這類駭侵攻擊行動。

- 資料來源：
  1. BITCOINS, BLOCKCHAINS, AND BOTNETS
  2. The bitcoin blockchain is helping keep a botnet from being taken down

3.2.2、資安廠商指出 5G 連網汽車的資安隱患

資安廠商發表研究報告，指出未來汽車透過高速 5G 網路連線，並且使用人工智慧和機器學習於自動駕駛技術時，可能面臨的各種資安風險。

資安廠商趨勢科技，日前發表研究報告，指出未來的新興汽車，可透過高速 5G 網路連線，並且大量使用人工智慧和機器學習於自動駕駛技術；但這類汽車可能面臨各種資安風險，必須及早因應。

報告指出，這類連網汽車透過高速且低延遲的 5G 無線網路，可以連線到基地台、行控基站等網路與交通基礎設施、個人連網裝置或其他車輛，並且大量運用諸如人工智慧和機器學習技術，在車輛本體或雲端進行運算，以用於自動駕駛等先進功能之上；但這樣的應用架構，仍無法倖免於駭侵攻擊之外。

報告說，連網汽車中的許多重要系統，包括動力系統、通訊系統、車身控制系統、能源管理系統、行車安全系統等，未來都將透過 5G 或更快速的行動通訊網路，與包括車輛、基站、雲端伺服器、交通行控裝置、用戶的各種連網裝置等通訊。

另外，車輛本身的軟體也會變得更為複雜，據統計一台新型車輛，其內部程式碼將超過一億行；車上更有超過 30 種到 100 種以上的各種控制單元與感測器；如此複雜的結構與連線需求，將使車輛的軟硬體系統存有更多潛

在資安漏洞或弱點，成為駭侵攻擊的目標。

報告也指出，拜 5G 網路高速、低延遲的連線能力之賜，未來更有可能出現將部分 ECU 功能雲端化以節省成本的車輛；這又再度增加駭侵者可能攻擊的弱點。

報告列舉了幾種可能的攻擊手法，包括透過手機或 Wi-Fi 連線，對車輛發動中間人攻擊、直接入侵車輛控制系統、攻擊車內顯示器的瀏覽器核心、駭入後針對車用作業系統（通常是 Linux）的弱點發動攻擊（例如提升權限或執行任意程式碼）、在車用軟體或韌體升級過程中發動供應鏈攻擊等。

- 資料來源：
  1. Cybersecurity Risks of Connected Cars
  2. Cybersecurity for Connected Cars Exploring Risks in 5G, Cloud, and Other Connected Technologies

3.3、國際政府組織資安資訊

3.3.1、美國一淨水場遭駭，強鹼濃度險遭調升百倍以上

美國一間淨水廠遭駭侵攻擊，駭侵者試圖將淨水過程中使用的強鹼藥劑濃度調高百倍以上，幸好被該廠人員發現未能得逞。

美國一間淨水廠於 2 月初遭駭侵攻擊，駭侵者試圖將淨水過程中使用的強鹼藥劑氫氧化鈉的濃度調高百倍以上，幸好被該廠人員及時發現，未能得逞。

這間遭駭的淨水廠位於美國佛羅里達州的歐茲馬市（City of Oldsmar），事件發生於 2 月 5 日。駭侵者於當天上午 8 時首次入侵該淨水廠的電腦系統， 1 秒後再次入侵；之後在下午 1 時 30 分時進行正式攻擊。

據歐茲馬市官員指出，駭侵者係透過該淨水廠使用的遠端遙控軟體 TeamViewer 取得內部系統的控制權，利用 TeamViewer 將氫氧化鈉的濃度，自原本設定的 100 ppm 上調到 11,100 ppm。

該廠的一名員工及時發現系統的水質設定值不正常，立即在這些藥劑投入之前，就手動強制修正氫氧化鈉的投入濃度到正常值，因此可能造成傷害的毒水並未流入供水系統之中。

該市官員說，駭侵者在修改氫氧化鈉投入值後就立即離線退出，沒有再次發動攻擊；目前尚未掌握駭侵者身分，但整個案子已交由聯邦調查局等多

個情治單位展開調查。

聯邦調查局在接手調查後，隨即於 2 月 10 日指出這個案子中的幾處弱點，包括使用微軟已不支援的 Windows 7 作業系統、強度不足的密碼、共用密碼、系統無防火牆保護，以及使用 TeamViewer 等等；聯邦調查局說：「在正常的用途之外，TeamViewer 可讓駭侵者遠端控制電腦，並且安裝各種軟體和檔案，其效果和可進行遠端遙控的後門惡意軟體無異。」

聯邦調查局雖然沒有呼籲在內部使用 TeamViewer 的公私單位移除 TeamViewer，但也指出這個軟體的潛在危險性，特別是擁有操作權限的員工，如果沒有使用強度足夠的密碼與其他資安防護措施時，其電腦上的 TeamViewer 就很容易遭駭侵者濫用。

- 資料來源：
  1. FBI Called In After Hacker Tries To Poison Tampa-Area City's Water With Lye
  2. A hacker broke into a Florida town’s water supply and tried to poison it with lye, police said
  3. Hacker modified drinking water chemical levels in a US city
  4. Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7
  5. Cybersecurity Advisory for Public Water Suppliers
  6. Windows 7、TeamViewer、共用密碼、沒防火牆四大安全缺陷，造成美國淨水廠遭駭

3.3.2、美國華盛頓州近 140 萬失業者個資，因審計單位遭駭而被竊

美國華盛頓州近 140 萬名失業者的個資，由於該州審計單位使用的軟體遭駭，可能因此被駭侵者竊取得手。

據美國《西雅圖時報》報導，美國華盛頓州有將近 140 萬名失業者的個人機敏資料，由於該州審計單位使用的軟體遭駭，可能因此已被駭侵者竊取得手。

華盛頓州審計長 Pat McCarthy 指出，該單位用以處理大量檔案的 Accellion 服務，於去年（2020） 12 月遭到駭入，造成該單位委託 Accellion 處理的失業者個人資料也被竊走。

Pat McCarthy 說，在這批被竊取的資料中，包括失業者的社會安全號碼與金融相關資訊。華盛頓州審計部門之所以收集這些資料，是因為要針對該州就業安全局（Employment Security Department）高達六億美元的失業補助詐領案進行調查，結果這些調查用的資料也遭駭侵者竊走。

資安專家指出，這些被竊的個人資訊，含有重要的社會安全碼與金融資訊，很可能遭到不肖人士用以發動進一步的詐騙行動，包括利用這批資訊盜領受害者帳戶內的存款，或是進行詐騙轉帳。

華盛頓州審計部門指出，這次失竊的資料，主要為自 2020 年 1 月 1 日開始到 2020 年 12 月 10 日之間的失業補助金申請資料，一共有近 160 萬筆申請記錄，實際申請人數約為 147 萬人。

華盛頓州審計部門表示，已經會同該州的資安主管機關著手調查此起資料被竊案件；美國聯邦政府的調查行動也即將展開。

遭到駭侵攻擊的廠商 Accellion 指出，這次被攻擊的軟體 FTA 是款已經長達二十多年的老舊產品；由於當年設計時並未考慮到各種駭侵攻擊的可能性，該公司早已呼籲客戶停止使用 FTA。

- 資料來源：
  1. About the Accellion data security breach
  2. Banking, social security info of more than 1.4 million people exposed in hack involving Washington state auditor

3.3.3、美國多個城市使用的支付系統遭到勒贖攻擊，民眾資料遭放暗網販售

美國多個城市所使用的支付系統 AFTS，在二月初遭到勒贖攻擊，系統無法運作；駭客甚至已經開始販賣攻擊行動中取得的資料。

美國多個城市與多家政府承包廠商廣泛使用的支付系統 AFTS（Automatic Funds Transfer Services），在二月初遭到嚴重勒贖攻擊，不但導致系統無法運作，駭客甚至已經開始在暗網上販賣在攻擊行動中取得的資料。

AFTS 是眾多美國城市與美國首府華盛頓多個外包廠商用以進行支付處理和地址驗證的服務系統，使用這套系統服務的用戶，不但人數眾多，而且遍布全美各地，因此系統停擺造成很大的不便，資料遭竊的影響更為嚴重。

據資安媒體 BleepingCoumpter 指出，這次攻擊行動的幕後主使者，可能是一個自稱為「古巴勒贖攻擊軟體」（Cuba Ransomware）的駭侵團體；如同所有過去發生過的勒贖攻擊一樣，這波攻擊也是事先竊取 AFTS 的資料，再進行加密鎖定。

目前還不知道駭侵者向 AFTS 要求多少贖金，不過 BleepingComputer 已經發現 Cuba Ramsonware 已在暗網上販售這次勒贖攻擊得來的資料。

這批被竊的資料欄位，因不同的城市和單位而略有不同，但可能包括姓名、地址、電話號碼、車輛牌照號碼、車身辨識編號（VIN, Vehicle

Idenfication Number）、信用卡卡號、紙本支票掃瞄檔案、詳細支付資訊等等。

受到這波攻擊影響的政府單位與城市，則包括加州的交通監理處、華盛頓州科克蘭市、 華盛頓州林伍德市、華盛頓州門羅市、華盛頓州瑞德蒙市、華盛頓州西雅圖市、雷克伍德自來水廠、艾弗列特港等等。

- 資料來源：
  1. US cities disclose data breaches after vendor's ransomware attack
  2. Data breach warning after California DMV contractor hit by file-stealing ransomware

3.3.4、巴西兩大國營電力公司遭勒贖攻擊

巴西兩家國營電力公司，近來同時遭到不明來源的勒贖攻擊，所幸核能發電廠和全國電網未受到攻擊影響。

巴西兩家國營電力公司 Copel 和 Electrobras，近來同時遭到不明來源的勒贖攻擊，所幸 Electrobras 旗下的兩座核能發電廠，以及巴西全國供電網路，並未受到攻擊影響。

這兩家電力公司是在上星期遭到勒贖攻擊，攻擊行動雖然使得兩家公司的部分系統無法運作，但影響局限在行政管理使用的電腦系統，並未波及到供電用的電腦系統。

據 Electrobras 指出，該公司所屬的兩座核能電廠，其發電系統使用的網路，在設計之初就考慮到資安攻擊問題，因此是完全與外部 Internet 相互隔離的，也和該公司用於行政管理的網路系統相互隔離；也因此在這波攻擊行動中未受到任何影響。

Copel 和 Electrobras 在遭到攻擊後，隨即也隔離了受到攻擊的網路系統與主機，並且立即展開調查；不過在兩家公司發表的資安通報中，並未提供關於此次攻擊的細節資料，也不確定是否有資料遭到竊取。

不過，一個稱為「Darkside」的勒贖駭侵攻擊團體，出面宣稱說他們手上握有超過 1,000GB 竊取自 Copel 的資料，內容包括該公司基礎架構的存取所需資訊，以及該公司高階管理層與顧客的機敏個資。

Darkside 也宣稱他們取得 Copel 內部網路 Active Directory 資料庫的內容，但並不像其他的勒贖團體一樣公開這批資料供外界檢視。

Elecrtrobras 是整個拉丁美洲規模最大的電力公司，而 Copel 則是巴西南部大省 Paraná 最大的電力公司。

- 資料來源：
  1. COMUNICADO AO MERCADO
  2. Eletrobras, Copel energy companies hit by ransomware attacks
  3. Brazil's Eletrobras says nuclear unit hit with cyberattack

3.4、社群媒體資安近況

3.4.1、研究人員發現 Clubhouse 使用 Agora 提供的音訊技術

近期熱門的語音社交軟體 Clubhouse，遭美國史丹佛大學研究人員發現，其後端基礎架構源於中國業者 Agora，引起數據傳輸的資安疑慮。

近期在全球迅速竄紅的語音社交軟體 Clubhouse，遭美國史丹佛大學網路觀測計畫（Stanford Internet Observatory，SIO）的研究人員證實，Clubhouse 系統後端的基礎架構，源自中國業者聲網(Agora)提供的音訊技術，並且有機會使聊天室內的詮釋資料(Metadata)遭中國政府取得。

研究人員透過封包追蹤分析等技術，至少一個實例中發現於聊天室建立的 Metadata，曾被傳送至位於上海總部的 Agora 伺服器。SIO 的報告中說明，Clubhouse 用戶的使用者 ID、聊天室 ID 會以純文字的形式進行傳輸，並未進行加密，表示任何有權限的第三方都能存取這些資料，因此 Agora 也有可能能夠存取用戶發言的原始語音資料。

SIO 的分析報告中顯示，Clubhouse 目前未針對聊天室內的語音資料進行端到端加密(End-to-end encryption， E2EE），因此這些資料有可能在傳輸的途中被攔截、轉錄或儲存於 Agora 的伺服器之中。

雖然 Agora 說明除了監控網路品質並向客戶收費之外，不會存取用戶的語音資料和 Metadata，但 Agora 身為中國境內公司，受到中國法規的管轄，

在必要時需協助提供資料給政府。而 Clubhouse 的隱私權政策中指出，Clubhouse 將基於信任與安全調查的目的，會短暫紀錄用戶的音訊資料，但未說明資料被儲存的實際時間。

- 資料來源：
  1. Clubhouse in China: Is the data safe?
  2. Privacy Policy
  3. Stanford Internet Observatory(TWITTER)
  4. Clubhouse 被證實使用 Agora 技術，數據傳輸恐有安全疑慮
  5. 史丹佛研究人員確認 Clubhouse 採用中國語音平臺 Agora，聊天室元資料經過中國伺服器
  6. 要注意資安！Clubhouse 承認：用戶數據可能會傳到中國
  7. 專家：中國用戶在 Clubhouse 發言 要小心

3.4.2、美國公布北韓 APT 透過社群平台等方式散布惡意軟體竊取加密貨幣的情資

美國資安相關單位日前公布北韓 APT 駭侵團體，以在社群平台散布等手法，利用偽造的加密貨幣交易軟體，竊取個人或企業持有的加密貨幣。

美國聯邦調查局（Federal Bereau of Investigation, FBI）、網路安全暨基礎設施安全局（Cybersecurity & Infrastructure Security Agency, CISA）等主管資安的相關單位，以及美國財政部，日前聯合發表資安通報，公布北韓 APT 駭侵團體 Lazarus（又稱 Hidden Cobra），竊取個人或企業持有的加密貨幣。

據 CISA 發表的資安警示通報指出，Lazarus 這波發動的攻擊，是利用在社群平台散布、釣魚、社交工程等手法，誘使潛在受害者下載安裝偽造的加密貨幣交易軟體 AppleJeus。

AppleJeus 最早發現的時間是在 2018 年。報告說，Lazarus 一開始是架設一個看起來像是正常加密貨幣交易所的網站，同時透過 AppleJeus 來竊取加密貨幣；近來發現的攻擊手法則擴大到利用社群平台、釣魚、社交工程等方式多管齊下，讓用戶下載 AppleJeus。

CISA 發表了七篇不同版本 AppleJeus 的惡意軟體分析報告，包括完整的技術分析、建議應對策略等。CISA 官員也指出，目前美國政府正在密切注意北韓針對全球加密貨幣發動的攻擊，特別是針對金融、能源與其他行業的

攻擊行動。

報告也說，在去年（2020）一年之中，觀察到的 AppleJeus 攻擊行動，受害範圍遍及全球三十餘國。

無獨有偶，美國司法部也在近日正式控告三名可能和 Lazarus 與北韓軍方有關的北韓籍人士，罪名是利用資安攻擊竊取價值 13 億美元的加密貨幣；其攻擊的對象包括銀行、娛樂產業、加密貨幣產業等組織。

- 資料來源：
  1. AppleJeus: Analysis of North Korea's Cryptocurrency Malware
  2. MAR-10322463-3.v1 - AppleJeus: Union Crypto
  3. US shares info on North Korean malware used to steal cryptocurrency
  4. US indicts North Korean hackers for stealing $1.3 billion

3.5、行動裝置資安訊息

3.5.1、多國電信業者遭 APT 駭侵團體駭入

資安廠商指出，有 APT 駭侵團體自 2020 年初開始針對多個國家的電信業者與 ISP 發動攻擊，竊取情報與機敏資訊。

以色列資安廠商 Clearsky，日前發表研究報告指出，一個 APT 駭侵團體「黎巴嫩雪松」（Lebanese Cedar），自 2020 年初開始針對多個國家的電信業者與 ISP 發動攻擊，主要目的疑為竊取情報與機敏資訊。

據 Clearsky 的報告指出，受到 Lebanese Cedar 駭侵攻擊的電信業者與 ISP，分布在美國、英國、以色列、埃及、沙烏地阿拉伯、黎巴嫩、約旦、巴勒斯坦與阿拉伯聯合大公國等；遭到駭入的 web server 數量超過 250 台。

Clearsky 表示，這些電信業者和 ISP 的各種資料，包括旗下用戶的通訊記錄、各種隱私資訊，可能均已遭到 Lebanese Cedar 竊取。

Clearsky 指出，Lebanese Cedar 的攻擊方式，採取一種簡單但有效的手法：先以網路上很容易找到的開放源碼駭侵工具，在網路上掃瞄，尋找還存有未修補漏洞的 Atlassian 和 Oracle 伺服器，接著設法侵入該伺服器，並且安裝一個 web shell 以待日後利用。

這些被找出來的未修補 Atlassian 和 Oracle 伺服器，多半存有以下三個已知漏洞，因而遭到入侵：

- CVE-2019-3396：存於 Atlassian Confluence
- CVE-2019-11581：存於 Atlassian Jira
- CVE-2012-3152：存於 Oracle Fusion

透過這些漏洞進入系統後，攻擊者更會在受害公司的內部網路，植入更強大的後門惡意軟體 Explosive；駭侵者經常使用這個惡意軟體來竊取各種資料。

Clearsky 在報告中，也列出了目前已知遭到駭入的各國電信業者與 ISP 名單。

- 資料來源：
  1. ‘Lebanese Cedar’ APT
  2. Hezbollah's cyber unit hacked into telecoms and ISPs
  3. Hezbollah hackers attack unpatched Atlassian servers at telcos, ISPs

3.5.2、下載超過十億次的熱門 Android app SHAREit 存有久未修復的資安漏洞

一個下載次數超過十億次的熱門 Android app SHAREit，被資安廠商發現存有一個嚴重資安漏洞，但該漏洞已超過三個月未見修補。

一個下載次數超過十億次的熱門 Android app SHAREit，被資安專家發現存有一個嚴重資安漏洞，可導致駭侵者在用戶手機上執行惡意軟體；但該漏洞遭發現已超過三個月，未見開發者提供資安修補或更新。

據資安廠商趨勢科技發表的研究報告指出，這個資安漏洞的成因，是因為該 app 對於其程式碼的存取限制不當，導致駭侵者可以對安裝了 SHAREit 的 Android 手機用戶發動「中間人攻擊」，讓 SHAREit 執行任意程式碼、覆寫 SHAREit 自身 local 環境內的檔案內容，甚至在用戶不知情之下安裝任意應用程式。

報告也指出，這個 app 對於其儲存空間與敏感資源的保護，也不夠周全，因此可導致其他 app 不當存取這類檔案和資源，包括刪除、編輯或取代。

SHAREit 是 Google Play Store 上相當受用戶歡迎的應用程式，可讓 Android 用戶透過其裝置，彼此分享各類檔案；其官網宣稱其用戶數量高達 18 億人，遍布世界兩百多國。被發現嚴重漏洞的 Andoird app，其下載安裝次數突破十億次。

趨勢科技在報告中提到，該公司的資安專家發現此漏洞後，便立即通報開發者，但超過三個月以上，未見開發者針對漏洞回應修補情形。

正在使用這個 app 的用戶，建議暫停使用，並且先行移除這個 app，直到開發單位推出修復漏洞的新版後，再恢復使用，以降低因為這個漏洞而遭駭侵攻擊的風險。

SHAREit 的 iOS 由於採用完全不同的程式碼架構，因此並不存有這個漏洞；iOS 版 SHAREit 的用戶，可以繼續安心使用。

日前總部位於新加坡的 Smart Media4U Technology 表示已修復 SHAREit 中的資安漏洞，建議用戶立即透過官方管道將 app 更新至最新版本。

- 資料來源：
  1. SHAREit fixes security bugs in app with 1 billion downloads
  2. SHAREit Flaw Could Lead to Remote Code Execution
  3. Security bugs left unpatched in Android app with one billion downloads

3.5.3、Apple 在 iOS 更新中，針對 iMessage 免操作攻擊加強防禦機制

資安專家發現 Apple 於日前推出的 iOS 更新中，針對 iMessage 的「免操作攻擊」加強了防禦機制。

Google 旗下資安研究團隊 Project Zero 所屬的資安專家 Samuel Groß，日前發表研究報告指出，他發現 Apple 於日前推出的 iOS 更新中，悄悄針對 iMessage 的「免操作攻擊」（zero-click attack）新增多道防禦機制，以降低 iOS 裝置用戶在使用 iMessage 通訊時遭到此類攻擊的風險。

在報告中，Samuel Groß 分析了 Apple 在 iOS 新增的防禦機制；他發現 Apple 大幅改變了 iMessage 在處理訊息時的各種流程，讓過去多種 zero-click 攻擊手法賴以運作的一些弱點得到補強，使這類攻擊無處下手。

報告中說，這些 zero-click 攻擊，過去通常會利用各種造成記憶體崩潰的弱點下手，還得再結合其他漏洞的攻擊，包括遠端阻斷 ASLR 機制、設法遠端執行任意程式碼、設法突破沙箱限制等，才能夠做到在不顯示任何訊息，也不需要用戶操作，就能取得系統控制權。

Samuel Groß 的分析指出，在這次 iOS 14 的更新中，Apple 透過 iMessage 訊息處理流程的大幅改變，把上面提到的幾種過去經常採用的攻擊路徑都加以封鎖補強，使得 zero-click 攻擊的難度大幅提升。

這次 iOS 14 針對 iMessage 的訊息處理流程改變，首先是新增了一個稱為「BlastDoor」的沙箱機制，會嚴格檢查在 iMessage 中不受信任的資料；其次也加強了對共享快取記憶體不當存取的偵測，另外針對 ASLR 的暴力試誤攻擊也有更強的防範。

- 資料來源：
  1. Project Zero
  2. Apple Adds 'BlastDoor' to Secure iPhones From Zero-Click Attacks

3.6、軟體系統資安議題

3.6.1、QNAP 發布 Surveillance Station 及 Helpdesk 資安漏洞修補更新

威聯通®科技 (QNAP® Systems, Inc.) 於 2 月 25 日發表產品資安新聞，敦促其使用者立即更新 Surveillance Station 及 Helpdesk 應用程式，以修正近期所發現的安全性事件。

為確保 QNAP NAS 安全性，使用者應盡快安裝其設備對應之更新套件。若要更新 Surveillance Station 應用程式，請依照 QNAP 資安通報 QSA-21-07 內說明之程序進行。若要更新 Helpdesk 應用程式，請依照 QNAP 資安通報 QSA-20-08 內說明之程序進行。若需進一步技術支援，請透過 QNAP 客戶服務聯絡 QNAP。

根據 QNAP 資安通報 QSA-21-07 內容，舊版 Surveillance Station 存在堆疊緩衝區溢位 (Stack Buffer Overflow) 弱點，若遭攻擊者濫用，可執行任意程式碼。QNAP 已發行 5.1.5.4.3 (適用於 64 位元系統) 及 5.1.5.3.3 (適用於 32 位元系統) 版本的 Surveillance Station 來應對此一事件。而根據 QNAP 資安通報 QSA-20-08 內容，舊版 Helpdesk 存在弱點，可讓攻擊者取得 QNAP 裝置控制權。QNAP 已發行 3.0.3 版本的 Helpdesk 來應對此一事件。

除上述軟體更新及資安通報發布外，QNAP 亦已寄送個別電子郵件給已知的 Surveillance Station 使用者，力求降低此事件所造成的影響。同時，

QNAP 也於官方網站公告產品資安新聞。

資料來源：QNAP 提供

- 資料來源：

1. 立即更新 Surveillance Station 及 Helpdesk，確保 QNAP NAS 安全無虞
2. Stack Buffer Overflow in Surveillance Station
3. Multiple Vulnerabilities in Helpdesk
4. QNAP 客戶服務

3.6.2、Fonix 勒贖軟體宣布停止運作，同時公開加密金鑰

一個稱為 Fonix 的勒贖軟體，近日宣稱已經停止運作，同時公開用來進行加密勒贖攻擊的金鑰。

一個稱為 Fonix 的勒贖軟體，其幕後的駭侵團體，於近日在 Twitter 上發文，宣稱已經停止運作，同時將在日後公開提供其用來進行加密勒贖攻擊的金鑰。

這個 ID 為 @fnx67482837 的 Twitter 帳號，於 1 月 29 日推文指出，自己是 Fonix 的團隊管理員之一；該團隊認為現在應該把其發動駭侵攻擊的能力，用在正面的事情上面，並且幫助他人，因此決定停止 Fonix 的攻擊行動，同時將在近期免費釋出加密金鑰，供遭到 Fonix 攻擊並加密的檔案予以解密。

在這篇推文發出後不久，同一個 Twitter 帳號，又發表了一則推文；在推文中提供一個連結，可以下載一個名為「Fonix_dexrypter.rar」的壓縮檔。資安專業媒體 BleepingComputer 指出，這個檔案並不是能夠直接解密的檔案，比較像是 Fonix 駭侵團體內部使用的管理工具。

BleepingCompueter 指出，許多勒贖團體會提供少量解密的工具，給受害者測試，以向受害者證明贖金支付後，駭侵者確實有能力可以解鎖受害者遭加密的檔案；而 Fonix 提供的就是這種少量解密的工具；但該工具無法將

整台電腦的檔案完全解密。

另外，這個工具一次只能解密一個檔案，而且操作過程繁瑣，經常故障當掉；但有資安專家證實，其中包含的金鑰，確實可以解開部分版本 Fonix 勒贖軟體加密後的檔案。

BleepingComputer 在報導中說，目前他們沒有掌握完整解密工具何時會公開的訊息，但資安廠商 Emsisoft 已在研究可以成功解開被 Fonix 加密過的各種檔案的解密工具。

- 資料來源：
  1. End of FonixCrypter Project
  2. Fonix ransomware shuts down and releases master decryption key
  3. Fonix ransomware shuts down and releases master decryption key

3.6.3、KIA 汽車美國分公司遭勒贖攻擊

KIA 汽車美國分公司日前遭到 DoppelPaymer 勒贖攻擊，駭客威脅贖金高達 2,000 萬美元，若不及時支付，就要公開竊得的資料。

韓國 KIA 汽車設於美國加州爾灣市的美國 KIA 汽車（KIA Motors America），日前遭到 DoppelPaymer 駭侵團體發動的勒贖攻擊，駭客威脅的贖金高達 2,000 萬美元，若不及時支付，就要公開竊得並加密的資料。

KIA 美國分公司受到勒贖駭侵攻擊，造成該公司多項電腦與網路系統無法運作；受到影響的服務項目，包括其手機 app UVO Link、電話系統、支付系統、車主服務系統，以及各地經銷商在提供銷售維修服務時會用到的內部服務系統等。

在攻擊事件發生後，一位先前向 KIA 某經銷商租購新車，在當天抵達門市，欲進行交車手續的新車車主，在 Twitter 上發文，抱怨他被經銷商告知因其電腦系統停擺長達三天以上，因而無法完成交車手續。

資安媒體 BleepingComputer 透過管道，取得 DoppelPaymer 駭侵團體寄給 KIA 母公司現代汽車的勒贖信全文，信中提供一個架設在暗網的網站，在該暗網網站上則要求現代汽車美國分公司必須支付 404.5 顆比特幣的贖金，否則被竊取的資料就會公開。

不過，這波攻擊事件中只有 KIA 汽車遭駭，現代汽車並不是攻擊的目標。

稍後 KIA 汽車針對這波攻擊，發表正式聲明；在聲明中指出因攻擊而受阻的個別服務，也表示該公司正在積極恢復運作，對顧客造成的不便表達深感歉意。不過 KIA 聲明中指出該公司沒有任何證據指明攻擊形態屬於勒贖攻擊。

- 資料來源：
  1. Kia Motors America suffers ransomware attack, $20 million ransom
  2. Kia Motors Hit With $20M Ransomware Attack – Report

3.6.4、遊戲開發商 CD PROJEKT RED 遭勒贖攻擊，遊戲源碼等多項資料被竊

知名遊戲軟體開發廠商 CD PROJEKT RED 日前遭到嚴重的勒贖攻擊，該公司開發的多款遊戲與相關資料遭竊取後加密。

「電馭判客 2077」（Cyberpunk 2077）與其他多款知名遊戲軟體的開發廠商波蘭 CD PROJEKT RED，日前發表資安通報，表示該公司遭到嚴重的勒贖攻擊，該公司開發的多款遊戲與相關資料遭竊取後加密。

CD PROJEKT RED 被竊的遊戲相關資料，包括已發售的 Cyberpunk 2077、Witcher 3、Gwent，以及尚未釋出的 Witcher 3 遊戲源碼；該公司的行政、會計、出納、法務、人事、投資人關係等內部檔案也都一併遭竊。

CD PROJEKT RED 在資安通報中表示，內部已經開始調查整起駭侵事件，並且已經尋求司法單位的介入調查，而該公司也不會屈服於駭侵者的脅迫，不會和駭侵者談任何條件。此外，該公司表示備份檔十分完善，目前正在從備份檔復原受損的資料。

CD PROJEKT RED 在日前發表的推文，除了包括該公司揭露的被駭資安通報與聲明外，也貼出了駭侵者留下的恐嚇信件內容全文。

CD PROJEKT RED 也指出，雖然該公司有許多內部資料在這波攻擊事件中受到影響，但該公司確認目前沒有任何用戶的個人機敏資訊被竊。

據資安專業媒體 BleepingComputer 分析報導指出，這次 CD PROJEKT RED 攻擊事件，是由一個稱為「HelloKitty」的駭侵團體所為；這個駭侵團體使用的惡意軟體也稱為「HelloKitty」。

資安廠商 Emisoft 指出，HelloKitty 駭侵團體是從 2020 年 11 月開始活躍，專門攻擊大型企業；最近涉入的駭侵攻擊案包括去年駭入巴西的 CEMIG 電力公司。

- 資料來源：
  1. CD PROJEKT RED (TWITTER)
  2. CD PROJEKT RED gaming studio hit by ransomware attack
  3. HelloKitty ransomware behind CD Projekt Red cyberattack, data theft

3.7、軟硬體漏洞資訊

3.7.1、VMware 修復 vCenter 嚴重漏洞，可導致駭客遠端執行任意程式碼

VWware 修復發生在 vCenter 的嚴重漏洞，該漏洞可能導致駭侵者藉以提升執行權限，甚至遠端執行任意程式碼。

VWware 日前發表資安通報，宣布該公司修復一個發生在 vCenter Server 的嚴重漏洞，該漏洞可能導致駭侵者藉以提升執行權限，甚至遠端執行任意程式碼。

這個漏洞的 CVE 編號為 CVE-2021-21972，發生在用以控制 VMware vSphere 作業環境的 vCenter Server 外掛程式；駭侵者可藉由這個漏洞存取連接埠 443，在執行 vCenter Server 的電腦系統上提升執行權限，並且執行任意指令與程式碼。

據發現這個漏洞並提報給 VMware 公司的資安廠商 Positive Technologies 指出，該公司觀測到全球有許多 VMware vServer 已遭駭侵者利用此漏洞駭入，將原本只能在企業內部網路中存取的 VMware vServer 曝露在公眾網路之上。

據 Positive Technologies 估計，受害伺服器主機多達 6,700 台以上，主要分布在德國（7%）、法國（6%）、中國（7%）、英國（4%）、加拿大（4%）、俄羅斯（3%）、台灣（3%）、伊朗（7%）、義大利（3%）。

這個漏洞的 CVSS 危險程度評分高達接近滿分 10 分的 9.8 分。

VMware 發布的資安通報中揭露的漏洞，除了上述的 CVE-2021-21972 嚴重漏洞之外，也包括 CVE-2021-21973、CVE-2021-21974 等其他漏洞；受到影響的產品，除了上述的 vCenter Server 系列產品外，還包括 VWware ESXi 與 VMware Cloud Foundation 等產品。

VMware 同時也推出了針對這些漏洞的暫時解決方案（workaround），採用這些產品的用戶，應立即套用這些解決方案，並等待 VWware 推出正式的修補軟體。

- CVE 編號：CVE-2021-21972
- 影響產品/版本：VMware vCenter 6.5、6.7、7.0、CouldFoundation 3.x、4.x、ESXi 6.5、6.7、7.0。
- 解決方案：套用 VMware 提出的暫時解決方案。

- 資料來源：
  1. VMSA-2021-0002
  2. Critical VMware vCenter Server Flaw Can Expose Organizations to Remote Attacks
  3. More than 6,700 VMware servers exposed online and vulnerable to major new bug

3.7.2、WordPress 外掛程式嚴重資安漏洞，可導致系統遭挾持

WordPress 外掛程式 NextGen Gallery 遭發現兩個資安漏洞，使近 800,000 個 WordPress 網站存有遭駭侵者發動多種攻擊，甚至取得系統控制權限的風險。

WordPress 外掛程式 NextGen Gallery 遭發現兩個資安漏洞，可能使得近 800,000 個 WordPress 網站存有遭駭侵者發動多種攻擊，甚至取得系統控制權限的資安風險。

NetxGen Gallery 是可安裝在 WordPress 開源架站軟體上的擴充用外掛程式，可讓網站管理者大量上傳相片到其 WordPress 網站中，並且進行更有效率的管理。

資安廠商 Wordfence 旗下的研究人員，日前發現 NextGen Gallery 存有兩個資安漏洞；這兩個資安漏洞都可讓駭侵者發動「跨站請求偽造」（cross-site request forgery, CSRF）攻擊，駭侵者可利用這兩個漏洞取得網站控制權，進一步對其他網站發動各種攻擊，例如將訪客導向至惡意網站、注入垃圾訊息、進行釣魚攻擊等。

危險程度評級為嚴重等級，CVSS 分數高達 9.6 分的 CVE-2020-35942 漏洞，其問題發生於 NextGen Gallery 用來保護各種設定的程式碼錯誤；駭侵者可讓網站管理者點擊特定連結，對網站發出特製的連線要求，藉以誘發

錯誤。

另一個危險程度為「高」等級，CVSS 分數為 8.8 分的 CVE-2020-35943 漏洞，問題則發生在 NextGen Gallery 在處理 AJAX 的驗證流程錯誤，駭侵者只要誘導網站管理者上傳一個藏有惡意程式碼的一般圖形檔，即可誘發這個錯誤，進而發動攻擊。

這兩個漏洞存於 NextGen Gallery 3.5.0 版本之前，開發者推出的 3.5.0 版，已經針對這兩個漏洞修復完成；有安裝 NextGen Gallery 的 WordPress 網站，其管理者應立即更新至最新版本，以降低遭到攻擊的風險。

- CVE 編號：CVE-2020-35942、CVE-2020-35943
- 影響產品/版本：NextGen Gallery 3.5.0 先前版本
- 解決方案：將 NextGen Gallery 升級至 3.5.0 或後續版本

- 資料來源：
  1. Severe Vulnerabilities Patched in NextGen Gallery Affect over 800,000 WordPress Sites
  2. Critical WordPress Plugin Flaw Allows Site Takeover
  3. WordPress Gallery Plugin – NextGEN Gallery

3.7.3、SonicWall SMA 100 系列 0-day 漏洞，已遭駭侵者大規模濫用

SonicWall 生產的 SMA 100 系列網通產品，內含的一個 0-day 漏洞，恐已遭駭侵者大規模用以發動攻擊。

資安廠商 NCC Group 旗下的資安專家日前指出，由 SonicWall 生產的 SMA 100 系列網通產品，內含的一個 0-day 漏洞，恐已遭駭侵者大規模用以發動攻擊。

NCC Groups 首先在 Twitter 上發表簡短推文，指出該公司已經觀察到利用 SonicWall SMA 100 系列 0-day 漏洞的大規模攻擊行動，同時也將該 0-day 漏洞的分析報告提報給 SonicWall。

美國主管資安事務的資安與基礎設施安全局（Cybersecurty and Infrastructure Security Agency）也在隨後發布資安通報，指出該局已接獲相關通報。CISA 也說該局正在密切注意相關漏洞的調查進度。

這波攻擊事件最早始於 1 月 22 日，SonicWall 對外公開該公司遭到攻擊；當時該公司指出，其內部網路很可能因為該公司特定網通產品的 0-day 漏洞而遭到攻擊；存有此一漏洞的裝置，很可能就是 SMA 100 系列，包括 SMA 200、SMA 210、SMA 400、SMA 410、SAM 500V。

數日後 NCC Group 在推文中指出，該公司發現了 0-day 漏洞的存在，以及發現大規模攻擊行動，但並未公布太多細節；隨後 SonicWall 更新其資

安通報，明確指出 SMA 100 版本 10.x 的實體和虛擬產品都含有這個 0-day 漏洞。

SonicWall 指出，該公司正在積極開發新版韌體，預計在二月初即可釋出；用戶可暫時先將使用中的 SMA 100 系列機種，在備份設定值後降版到 9.x 版，同時檢查通訊記錄中是否有不明 IP 連線，如果不確定的話，應將 SMA 100 置於防火牆內，並且關閉一切對外連線。如有二階段登入驗證，也應立即啟用。

- 影響產品/版本：SonicWall SMA 100 系列，包括 SMA 200、SMA 210、SMA 400、SMA 410、SAM 500V。
- 解決方案：暫時降版至 9.x，待 SonicWall 推出新版韌體後再行升級，同時檢查是有曾有不明 IP 連線記錄。

- 資料來源：
  1. Urgent Patch Available For SMA 100 Series 10.X Firmware Zero-Day Vulnerability [Updated Feb. 3, 2 P.
  2. Per the @SonicWall advisory
  3. Zero-Day Vulnerability in SonicWall SMA 100 Series Version 10.x Products

3.7.4、Cyberpunk 2077 修復可遭惡意駭入並控制電腦的資安漏洞

熱門遊戲 Cyberpunk 2077 近日修復一個可讓駭侵者遠端執行任意程式碼的嚴重資安漏洞，玩家應立即安裝更新修補程式。

熱門遊戲「電馭叛客 2077」（ Cyberpunk 2077 ）開發廠商 CD Projekt Red，近日修復一個可讓駭侵者遠端執行任意程式碼的嚴重資安漏洞；這款遊戲的玩家，均應立即安裝更新修補程式。

這個漏洞發生在利用第三方程式修改遊戲儲存檔案，以調整遊戲進度、人物屬性與擁有物件等資料的場合。一位這類遊戲修改程式 CyberpunkSaveEditor 的開發者 PixelRick，在自己的 Github 中發表了他的發現；可以利用特製的遊戲修改檔案，讓 Cyberpunk 2077 中一個未使用隨機記憶體配置（ASLR, Address space layout randomization）機制的 DLL 檔（xinput1_3.dll）發生記憶體溢位錯誤，因而取得遠端執行任意程式碼的權限。

一旦駭侵者成功取得權限，就可以在系統上安裝更多惡意軟體，發動進一步的駭侵攻擊活動。

Cyberpunk 2077 開發廠商在接獲 PixelRick 的通報後，很快在日前推出了修補更新程式 hotfix 1.12，更換了可能引發記憶體溢位錯誤的非 ASLR DLL 檔案，改為使用 Windows 10 內建的 input1_4.dll，這個 dll 會使用

ASLR 機制，因而修復了可能觸發記憶體溢位錯誤的問題。

任何不是透過 Steam 啟動 Cyberpunk 2077 遊戲，或是正在使用遊戲存檔修改工具的玩家，都應立即透過 Steam 下載安裝 hotfix 1.12 更新檔。整個遊戲更新的所需時間不到一分鐘即可完成。

- 影響產品/版本：Cyberpunk 2077 hotfix 1.12 之前版本
- 解決方案：透過 Steam 安裝 hotifx 1.12 更新修補程式

- 資料來源：
  1. CD PROJEKT RED CS TWITTER
  2. A quick summary about the vulnerability I found in the game
  3. Cyberpunk 2077 bug fixed that let malicious mods take over PCs

3.7.5、微軟 Patch Tuesday 更新包，修補 56 個資安漏洞與 1 個 0-day 漏洞

微軟於日前推出 2021 年二月份 Patch Tuesday 軟體更新包，採用微軟產品的用戶，應即透過系統更新安裝此次資安修補更新。

Microsoft 日前推出 2021 年二月份 Patch Tuesday 軟體更新包，針對旗下多種軟體產品的 56 個已知資安漏洞與 1 個 0-day 漏動進行修補更正；採用微軟產品的廣大用戶，應立即透過系統更新安裝此次資安修補更新。

在這次修補中得到更新的 0-day 漏洞，其 CVE 編號為 CVE-2021-1732，屬於 Windows Win32K 的權限提升漏洞；駭侵者可利用這個漏洞，將自身的執行權限提升到系統管理員等級。這個漏洞的 CVSS 分數高達 7.8 分。

其他得到修補的重要漏洞，分列如下：

- CVE-2021-1721：發生於 .NET Core 與 Visual Studio，可導致用以發動 DoS 攻擊；
- CVE-2021-1727：發生於 Windows Installer，可導致駭侵者提升自身執行權限；
- CVE-2021-1733：發生於 Sysinternals PsExec，可導致駭侵者提升自身執行權限；
- CVE-2021-24098：發生於 Windows Console Driver，可導致用以發動 DoS 攻擊；
- CVE-2021-24106：發生於 Windows DirectX，可導致資料遭到竊取；

- CVE-2021-26701：發生於 .NET Core，可導致遠端執行任意程式碼。

另外，微軟也針對存於 Azure Artifactory 的 CVE-2021-24105 漏洞進行修補，駭侵者可以利用這個漏洞，在企業內部自行開發的軟體中植入惡意程式碼，發動攻應鏈攻擊。

- CVE 編號：
- 影響產品/版本：微軟各版本 Windows 系統（包括桌面版與 Server 版）
- 解決方案：透過系統更新功能，下載安裝最新更新軟體

- 資料來源：
  1. Windows Win32k Elevation of Privilege Vulnerability
  2. Package Managers Configurations Remote Code Execution Vulnerability
  3. Microsoft February 2021 Patch Tuesday fixes 56 flaws, 1 zero-day

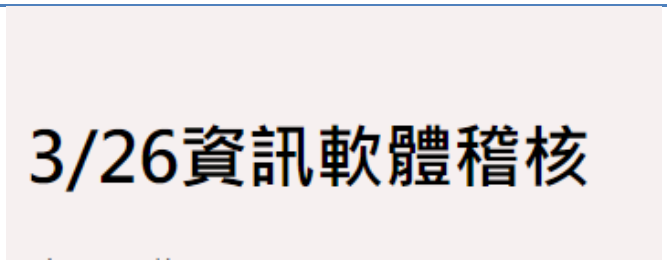
第 4 章、 資安研討會及活動

2021 GiCS 第 1 屆尋找資安女婕思	
活動時間	**報名時間於 110 年 2 月 5 日(五)至 3 月 11 日(四)止**
活動地點	**初賽：網路線上 3/17-3/21** **決賽：沙崙現場 4/24**
活動網站	**https://gics.tw/#**
活動概要	 **主辦單位：科技部、行政院科技會報辦公室、教育部** 活動目的： 「2021 GiCS 第 1 屆尋找資安女婕思」以學習與參與為主要目的，從教育年輕女學生對資安正確觀念著手，將資安向下扎根，鼓勵女性投入資安科技領域。 本活動以「資安闖天關」與「創意發想賽」之主題同步進行：「資安闖天關」將以線上與實體關卡帶領參加者挑戰物聯網及自駕車資安。「創意發想賽」則著重於日常生活與資訊安全相關的議題發想，並邀請評審評分資安應用創意情境與其解決方案架構。活動依主題，區分為「高中職組」及「大專校院組」，於報名期間執行單位將安排至高中職及大專校院實地推廣生活上的資安入門觀念及廣宣主題活動。期望透過多樣化的活動設計，鼓勵學生參與，培養年輕學子創新獨立思考的能力，並增強資安知識和技能。

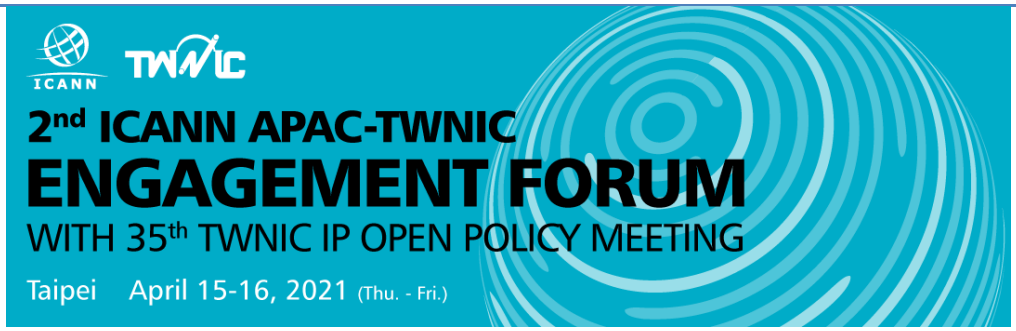
後疫情時代｜資安策略的轉變與資安治理的價值	
活動時間	**2021-03-18(四) 13:45 ~ 16:30**
活動地點	**台灣台北市中山區松江路 61-1 號**
活動網站	**https://www.accupass.com/event/2101190342356142804670**
活動概要	 **主辦單位：崴亞風險咨詢顧問股份有限公司** 活動介紹： 2021 年全球疫情持續發燒，許多實體活動、出差、會議都紛紛暫停，數位轉型速度加劇，遠距辦公成了企業必須面對的課題。 然而，駭客攻擊、勒索軟件、釣魚郵件在這種情況下，也搭著 COVID-19 的效應層出不窮的出現，光是 2020 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

3/19 安全程式開發初探	
活動時間	**2021-03-19 13:30 ~ 16:30**
活動地點	**協志聯合攻防中心(台北市中山區中山北路三段 22 號)**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjYwMA==**
活動概要	3/19安全程式開發初探 **主辦單位：中華民國資訊軟體協會** 費用：付費 聯絡窗口：0225533988 分機 358　溫專員　alisa.wen@cisanet.org.tw 報名截止：2021-03-17 課程內容： ● 資安產業現況、趨勢與挑戰 ● 資安事件分析 ● 業界資安準則概述 ● 弱點分享與修護作法

3 月例會_AI 發現威脅	
活動時間	**2021/3/25(四)，下午 2:00～5:00**
活動地點	**經濟部專業人員研究中心行政教學大樓 5 樓 507 教室** **新竹市光復路二段 3 號 (中油光明加油站旁)**
活動網站	**https://www.caa.org.tw/coursedetail-3505.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association **主辦單位：中華民國電腦稽核協會、ISACA Taiwan Chapter** 報名時間: 2021-02-18 ~ 03-24 演講大綱： 1.威脅演進 2.資安運營的挑戰 3.全方位 AI 威脅獵捕 4.自動化流程回應 5.事件分析及改善建議 主講講師：張博喬 欣盟科技有限公司 產品協銷部 課長 適合對象：本協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：本會會員(含團體會員公司同仁)免費，非會員 500 元 報名名額：限額 40 名，額滿為止，請儘速報名！ 參加本活動可獲得 3 小時 CISA、CISM、CGEIT、CRISC、CIA 等進修時數

3/26 資訊軟體稽核	
活動時間	**2021-03-26 13:30 ~ 16:30**
活動地點	**協志聯合攻防中心(台北市中山區中山北路三段 22 號)**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjU5OA==**
活動概要	 **主辦單位：中華民國資訊軟體協會** 費用：付費 聯絡窗口：0225533988 分機 358　溫專員　alisa.wen@cisanet.org.tw 報名截止：2021-03-10 課程內容： 一、SSDLC 程式開發安全 二、資訊系統委外開發 RFP 資安需求

4/8 金融科技與資安威脅	
活動時間	**2021-04-08 18:30 ~ 21:30**
活動地點	**協志聯合攻防中心(台北市中山區中山北路三段 22 號)**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjYwMg==**
活動概要	 **主辦單位：中華民國資訊軟體協會** 費用：付費 聯絡窗口：0225533988 分機 358　溫專員　alisa.wen@cisanet.org.tw 報名截止：2021-04-07 課程大綱： ● 金融科技介紹 ● 運用 AI 人工智慧可能面臨的資安威脅 ● 區塊鏈及虛擬貨幣的網路犯罪 ● 雲端運算的資安威脅 ● 數據安全性保存

第二屆 ICANN APAC-TWNIC Engagement Forum 與第 35 屆 TWNIC IP 政策資源管理會議	
活動時間	**2021 年 4 月 15 與 16 日**
活動地點	**台北福華大飯店地下二樓福華廳**
活動網站	**https://forum.twnic.tw/2021/**
活動概要	 **主辦單位：ICANN、TWNIC** ICANN 及 TWNIC 共同舉辦合作交流論壇 (ICANN APNIC-TWNIC Engagement Forum)，集合了網路相關利害關係人與國際相關網路社群，針對域名、IP 位址及網路安全等主題，進行深入議題探討，這將是台灣與國際網路利害關係人共同面對面討論全球網路議題的最佳機會。 第 35 屆 TWNIC IP 政策資源管理會議希望促進網際網路相關產業發展為目標之會議，提供各界有關網路技術研究、產業發展之溝通交流平台，彙集臺灣地區各 ISP 業者之意見提供相關 IP 政策及管理機制。 ICANN 及 TWNIC 建立論壇平台，讓地區內之網路相關利害關係人，可以藉由合作交流論壇從區域及台灣的角度探索政策、科技與協作等不同面向中各方利害關係人的觀點。

第 5 章、 2021 年 2 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。

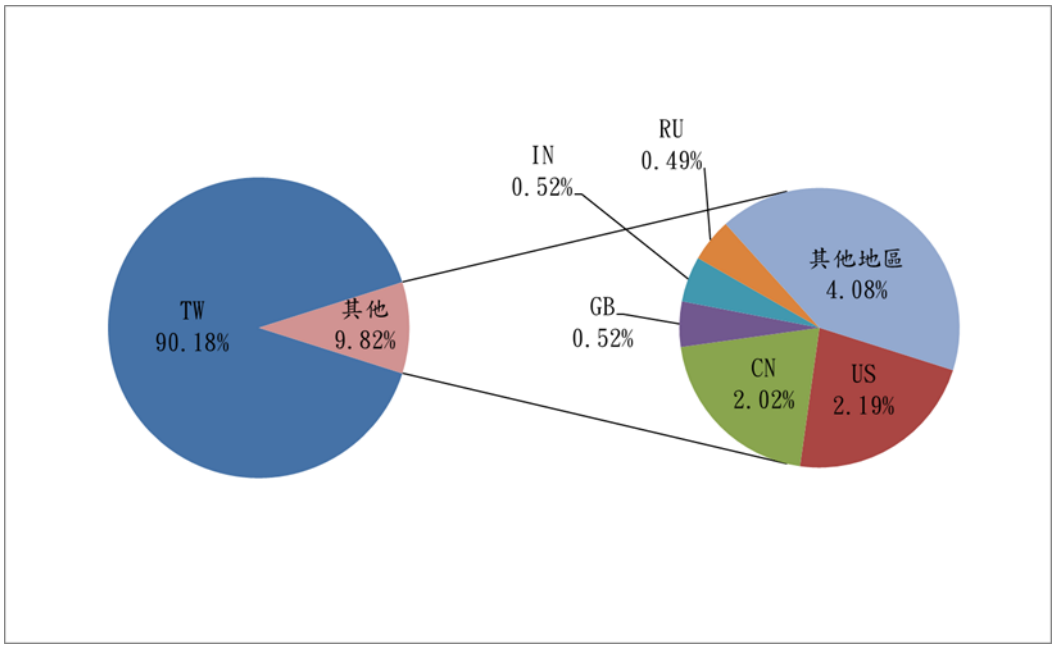


圖 1、分享地區統計圖

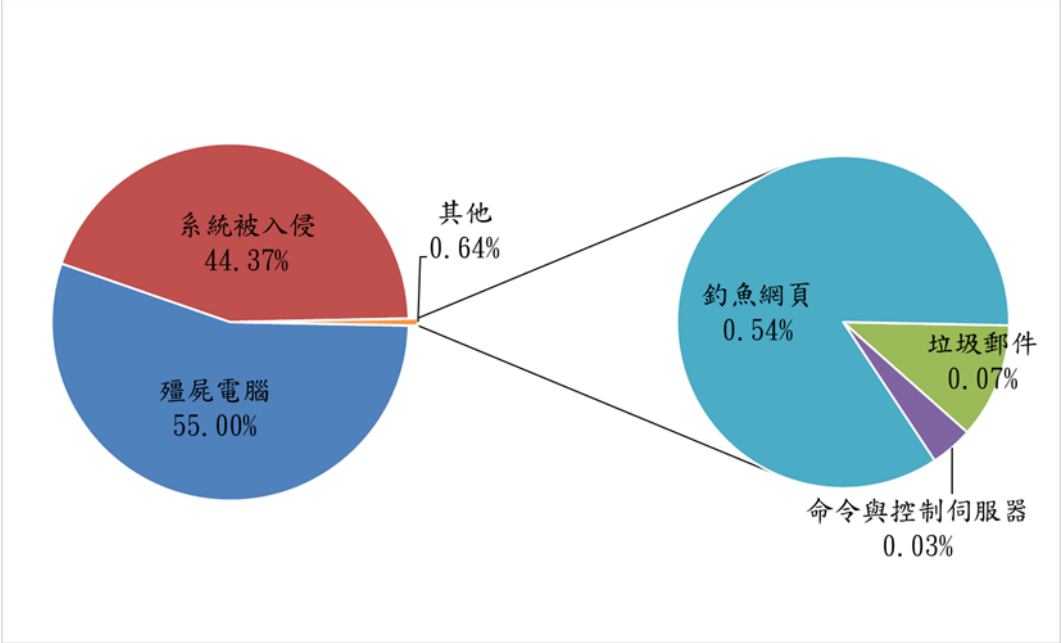


圖 2、分享類型統計圖

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 3 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**