



# TWCERT/CC 資安情資電子報

---

2021 年 6 月份

## 電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在行政院資通安全處及國家通訊傳播委員會指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 5 章節：

- 第 1 章、封面故事：上月 TWCERT/CC 所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。
- 第 2 章、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養。
- 第 3 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。
- 第 4 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。
- 第 5 章、資安情資分享概況：將上月份 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

# 目錄

第 1 章、 封面故事 .....	1
數千萬台 Dell 電腦內含 BIOS 驅動程式漏洞 .....	1
第 2 章、 資安小知識 .....	3
小型企業網路安全指南 .....	3
第 3 章、 國內外重要資安事件 .....	8
3.1、 資安趨勢 .....	8
3.1.1、 新一波全球性釣魚攻擊，受害者遍及全球各大產業 .....	8
3.1.2、 統計指出，資料遭洩漏於暗網上的企業，達 2,100 家 .....	10
3.2、 新興應用資安 .....	12
3.2.1、 資安專家發現存在長達 24 年之久的 Wi-Fi 連線漏洞 Frag Attacks.....	12
3.2.2、 全新 Panda 加密貨幣竊取軟體，透過垃圾郵件與 Discord 大規模散布..	14
3.2.3、 Trust Wallet、MetaMask 等加密貨幣錢包遭新一波詐騙活動鎖定.....	16
3.2.4、 微軟發現多種 IoT 裝置漏洞，影響遍及製造、醫療、大型企業網路.....	18
3.3、 國際政府組織資安資訊 .....	20
3.3.1、 比利時多個公部門遭到大規模 DDoS 攻擊 .....	20
3.3.2、 美澳政府發布 Avaddon 勒索攻擊資安警訊 .....	22
3.3.3、 美國國土安全部與運輸安全局，針對油管勒索事件發布最新資安指示..	24
3.3.4、 國際刑警組織追回網路犯罪 8300 萬美元不法所得 .....	26
3.4、 社群媒體資安近況 .....	28
詐騙者在社群媒體假冒 Elon Musk 等知名人士，半年內詐得高達 8000 萬美元..	28
3.5、 行動裝置資安訊息 .....	30
3.5.1、 全新 Android 惡意軟體 TeaBot，針對歐洲各大銀行發動攻擊 .....	30
3.5.2、 破億 Android 手機用戶個資遭曝於設定不當的雲端服務 .....	32
3.5.3、 Apple AirTag 遭發現可用於傳輸任意資料 .....	34
3.6、 軟體系統資安議題 .....	36
3.6.1、 美國最大石油運輸管線，遭勒索攻擊而停止運作 .....	36
3.6.2、 微軟五月資安修復包，一次修復 55 個資安漏洞，以及 3 個 0-day 漏洞	38

3.6.3、QNAP 網路儲存設備再遭 eCh0raix 勒索軟體攻擊，用戶應提高警覺....	40
3.7、軟硬體漏洞資訊 .....	42
3.7.1、QNAP 確認 Qlocker 勒索軟體係利用 HBS 後門帳號入侵.....	42
3.7.2、Apple 修復兩個恐已遭用於攻擊的 0-day 漏洞 .....	44
3.7.3、Apple 修復遭駭侵者大規模濫用的嚴重 tvOS 與 macOS 0-day 漏洞 .....	46
3.7.4、賓士聯手資安業者，強化車用系統資安防護 .....	48
第 4 章、資安研討會及活動 .....	50
第 5 章、2021 年 5 月份資安情資分享概況 .....	53

## 第 1 章、封面故事

### 數千萬台 Dell 電腦內含 BIOS 驅動程式漏洞



資安廠商發現，自 2009 年起發售的數千萬台 Dell 品牌 Windows 電腦，其 BIOS 驅動程式內含一個嚴重資安漏洞，可導致駭侵者提升執行權限；用戶應立即更新。

資安廠商 SentinelLabs 近日發表研究報告指出，該公司旗下的研究人員發現，自 2009 年起發售的數千萬台 Dell 品牌 Windows 電腦，其 BIOS 驅動程式內含一個嚴重資安漏洞，可導致駭侵者提升執行權限到核心模式等級，可用於發動各類攻擊。Dell 電腦設備的用戶，應立即更新系統。

SentinelLabs 總共發現五個漏洞，都歸於 CVE-2021-21551 這個編號之下；這五個漏洞都發生在 Dell 用來更新 BIOS 時使用的軟體 DBUtil 內，包括兩種記憶體崩潰錯誤、兩種輸入檢查不當錯誤，以及一個程式碼邏輯問題。

駭侵者可以利用這些錯誤，將自身的執行權限自非系統管理者用戶，一舉提升到核心模式等級，因而可以存取系統上所有的軟硬體資源，發動多種後續攻擊。

CVE-2021-21551 的 CVSS 危險程度評分為 8.8 分，危險程度分級為「高」，而非最高等級的「嚴重」；之所以無法取得更高得分的原因，在於駭侵者必須先以其他方式駭入系統，才能利用這個漏洞提升權限。

據研究者指出，這個漏洞遠從 2009 年起便存在於 Dell 發展的各型 Windows 電腦中，包括各型桌上型、筆記型、平板電腦與伺服器等機型，數量可能高達數千萬台之多；雖然目前尚未傳出有攻擊行動係利用這個漏洞進行，但由於數量實在太大，因此很可能會有駭侵者利用此漏洞，針對尚未更新的 Dell 電腦發動大規模攻擊。

SentinelLabs 於 2020 年 12 月初提報這個漏洞給 Dell 後，Dell 花了四個多月的時間，在近期推出更新程式供用戶使用；強烈建議所有 Dell Windows 電腦，依照 Dell 發表的資安通報說明進行資安修補更新，以降低遭駭侵者利用此漏洞發動攻擊的風險。

- CVE 編號：CVE-2021-21551
- 影響產品/版本:Dell 自 2009 年起發售的所有型號 Windows 設備
- 解決方案：依 Dell 官方資安通報指示更新系統
  
- 資料來源：
  1. DSA-2021-088: Dell Client Platform Security Update for an Insufficient Access Control Vulnerability
  2. CVE-2021-21551- Hundreds Of Millions Of Dell Computers At Risk Due to Multiple BIOS Driver Privilege
  3. Hundreds of Millions of Dell Users at Risk from Kernel-Privilege Bugs

## 第 2 章、資安小知識

### 小型企業網路安全指南



英國國家網路安全中心 ( National Cyber Security Centre , NCSC ) 制定小型企業網路安全指南 ( Small Business Guide: Cyber Security ) ，提出幾個重要構面，協助小型企業以及個體戶提升資訊安全，降低受駭風險。

#### 一、備份資料

所有企業，都應該定期備份其重要最新數據。確保業務在洪水、火災、物理損壞、盜竊或被勒索軟體攻擊的影響下，可迅速恢復並正常運作，備份資料時需要注意的 4 件事：

1. 確定需要備份哪些資料：缺哪些資料，企業就無法運作。
2. 將備份設備與服務設備分開：3-2-1 原則，備份 3 份，使用 2 種不同設備，1 份離線存放。
3. 考慮雲端服務：使用雲端儲存，參考 NCSC 雲安全原則。

4. 將備份視為日常業務的一部分：設定自動/人工備份時間，確保需要時擁有最新版本的資料。

## 二、保護組織免受惡意軟體的侵害

### 5 個易於實施可防止惡意軟體損害您的組織：

1. 安裝（並打開）防病毒軟體：啟用防病毒軟體並即時更新。
2. 防止員工下載不符規定的應用程式：防止員工從未知的供應商/來源下載第三方應用軟體。
3. 保持所有 IT 設備最新版本：對於所有 IT 裝置，確保軟體和韌體保持最新版本(修補)。
4. 控制 USB（和儲存卡）的使用方式：作為公司的政策，以防止面臨不必要的風險。使用其他方式（如電子郵件或雲端儲存）傳輸檔，不透過 USB 傳輸檔。
5. 打開防火牆：公司網路和 Internet 之間建立一個安全防護網。

## 三、保護智慧型手機（及平板電腦）的安全

### 保護智慧型手機 5 個易於實施的步驟：

1. 打開密碼保護：啟動一定強度的密碼。
2. 確保丟失或被盜的設備可被跟蹤、鎖定、清除：利用 Web 工具，跟蹤設備的位置、遠端鎖定裝置的存取權限、遠端清除設備上儲存的數據、檢索儲存在設備上的資料備份。
3. 保持設備最新版本：設備設置為自動更新安全漏洞。
4. 保持應用程式最新版本：應用程式會修補已發現的安全漏洞。確保員工立即知道更新及如何安裝。

5. 不要連接到未知的 Wi-Fi 熱點：不要使用未知熱點連接到 Internet，可能洩漏個資及機敏資訊。以保護手機（及平板電腦）的安全。

#### 四、使用密碼保護資料

正確實施密碼保護，可防止未經授權的使用者存取您的裝置，有效的使用密碼的 7 個原則：

1. 確保打開密碼保護：提高密碼複雜度(大小寫、英數字、長度、特殊符號)。
2. 對重要帳戶使用雙重身份驗證 ( 2FA)：傳統帳號密碼外，使用如：OTP(一次性密碼)、晶片卡、生物因子認證器等進行第二重身分驗證。
3. 避免使用可預測的密碼：建議使用 3 個隨機單詞創建密碼，如 teatrainfish。  
員工不可共用帳戶或密碼來完成工作。
4. 所有的帳戶設定不同的帳號和複雜的密碼，且定期更換密碼。
5. 更改預設密碼：定期檢查設備是否已更新預設密碼。
6. 別在沒有 https 的網站上輸入個資、密碼，即使有 https 仍要小心。
7. 避免使用駭客易猜的密碼，例如避免使用以下方式建立密碼：
  - 重複或順序數字密碼
  - 英文單字密碼
  - 鍵盤排列密碼(駭客知道鍵盤排列會符合密碼規則)
  - 生日密碼(實際變動位數只有 6 位 19xx xx xx)
  - 中文姓名拼音/注音密碼(懂中文的駭客也懂)

## 五、避免網路釣魚攻擊

識別最常見的網路釣魚攻擊的 5 個步驟：

1. 管理帳戶以減少成功攻擊的影響：員工帳戶權限使用最少權限原則配置。
2. 考慮如何操作：
  - 確保員工瞭解正常的工作方式，以便有能力發現不尋常的請求
  - 員工知道如何處理異常請求，以及從哪裡獲得說明
  - 告訴您的供應商或客戶不會要求您的密碼以及銀行轉帳資訊
3. 檢查網路釣魚的明顯跡象：
  - 許多網路釣魚詐騙源自海外，通常拼寫、語法和標點符號都有差異
  - 指您是有價值的客戶、朋友或同事，均為網路釣魚騙局的一部分
  - 電子郵件要求您限時緊急採取行動的隱性威脅、請立即點擊等字眼
  - 來自組織內高層人士的電子郵件，要求向特定的銀行帳戶付款
4. 報告所有攻擊：若員工認為可能是網路釣魚的受害者，鼓勵通報。採取掃描惡意軟體並儘快更改密碼。
5. 檢查數位足跡：
  - 攻擊者收集組織和員工於網站和社交媒體公開資訊，使網路釣魚更具說服力，避免過度揭露資訊
  - 注意合作夥伴、承包商和供應商是否在網路上洩露本組織的資訊

- 提醒員工共享個人資訊將影響他們和組織，需有效管理數位足跡
  
- 資料來源：
  1. Small Business Guide: Cyber Security
  2. 'Cyber Action Plan' to help increasingly digital small businesses stay secure from rising threats

## 第 3 章、國內外重要資安事件

### 3.1、資安趨勢

#### 3.1.1、新一波全球性釣魚攻擊，受害者遍及全球各大產業



資安廠商發現一波全新釣魚攻擊活動，同時使用三種不同的惡意軟體串連，針對全球目標發動攻擊。

資安廠商 Mandiant 日前發表調查報告，指出該公司旗下的資安專家，發現一波全新釣魚攻擊活動自去年年底開始進行；該攻擊行動同時使用三種不同的惡意軟體串連，針對全球目標發動攻擊，全球各公私單位受害者已達 50 個以上。

Mandiant 在報告中說，這波釣魚攻擊行動分成兩波進行，分別在 2020 年 12 月 2 日與 12 月 11 日到 18 日之間發動攻擊，幕後的駭侵團體在 Mandiant 的代稱為 UNC2529，其中的 UNC 表示「無法歸類」(uncategorized)，表示這是一個尚不為外界所知的全新駭侵組織。

Mandiant 分析這兩波攻擊行動的特徵，一開始時遇到很大的阻礙，主要原因在於駭侵者使用的惡意軟體擁有多種可逃避偵測的技術；不過 Mandiant 還是找出其攻擊手法。首先，UNC2529 針對攻擊目標發動魚叉式釣魚攻擊信，內含一個稱為「DOUBLEDRAG」的 Javascript 下載程式的連結，或是

連到一個稱為「DOUBLEDROP」，內含惡意巨集程式，可從駭侵控制伺服器下載後續攻擊程式碼的 Excel 檔；而 DOUBLEDROP 又含有一個稱為 DOUBLEBACK 的後門，可用於下載更多惡意軟體。

此外，根據 Mandiant 的分析，UNC2529 用於這兩波攻擊的基礎架構，也相當可觀；至少動用了 50 個不同的網域名稱來寄送釣魚信件；而攻擊對象之廣也是罕見的。據 Mandiant 統計，第一波攻擊有 74% 的攻擊對象在美國境內，其中包括服務業、金融業、醫療業、零售業、軍用航太業、製造業、政府組織、教育機構、運輸業等；另外各有 13% 的攻擊對象分布於歐非地區和亞太地區，受害者同樣也遍及各種產業。第二波攻擊對象中，歐非地區的占比提高到 22%，美國和亞太區的占比則為 68% 與 11%，受害者則出現了前一波沒有出現的能源產業和電信業。

- 資料來源：

1. The UNC2529 Triple Double: A Trifecta Phishing Campaign
2. Worldwide phishing attacks deliver three new malware strains

### 3.1.2、統計指出，資料遭洩漏於暗網上的企業，達 2,100 家



自 2019 年起，已有多達 2,100 家企業的內部資訊在遭勒索攻擊後，在暗網上洩漏。

一項針對勒索攻擊損失進行的研究指出，自 2019 年起，已有多達 2,100 家企業，其內部資訊在遭勒索攻擊後，在暗網上洩漏。

據暗網資安研究單位 DarkTracker 長期研究指出，該單位觀察到在暗網站已有 34 個勒索攻擊組織，在暗網上洩漏 2,103 個單位組織的內部機敏資訊。這 34 個勒索駭侵團體為 Team Snatch、MAZE、Conti、NetWalker、DoppelPaymer、NEMTY、Nefilim、Sekhmet、Pysa、AKO、Sodinokibi (REvil)、Ragnar\_Locker、Suncrypt、DarkSide、CL0P、Avaddon、LockBit、Mount Locker、Egregor、Ranzy Locker、Pay2Key、Cuba、RansomEXX、Everest、Ragnarok、BABUK LOCKER、Astro Team、LV、File Leaks、Marketo、N3tw0rm、Lorenz、Noname、XING LOCKER。

以遭洩漏資訊的公司數量來看，排名前五名的勒索駭侵團體，與其在暗網上公布資料的次數如下：

- Conti，338 家；
- Sodinokibi/REvil：222 家；
- DoppelPaymer：200 家；
- Avaddon：123 家；
- Pysa：103 家。

有部分勒索團體洩漏的公司數量超過上述五家，但均已停止運作，因此未列入排行榜內；包括 Maze ( 266 家 )、Egregor ( 206 家 )。

DarkTrack 也指出，自 2020 年起，愈來愈多勒索攻擊採取所謂「二次敲詐」( double-extortion ) 的手法，即在加密檔案前先進行竊取，然後威脅受害者若不支付贖金，即在暗網上公開檔案內容。

由於愈來愈多勒索攻擊會公開資料，因此企業必須同時將勒索攻擊視為資料外洩，及早因應，並對可能受影響的對象保持公開透明。

- 資料來源：

1. DarkTracer : DarkWeb Criminal Intelligence(@darktracer\_int)
2. Ransomware gangs have leaked the stolen data of 2,100 companies so far

## 3.2、新興應用資安

### 3.2.1、資安專家發現存在長達 24 年之久的 Wi-Fi 連線漏洞 Frag Attacks



比利時資安專家發現一系列 Wi-Fi 無線網路連線標準的資安漏洞，可用於挾持物聯網與各種電腦、行動裝置；其中有些漏洞存在長達 24 年之久。

比利時資安專家 Mathy Vanhoef 日前發表論文，指出發現一系列 Wi-Fi 無線網路連線標準 802.11 的多個資安漏洞；這些漏洞可用於挾持物聯網與各種電腦、行動裝置，而且即使套用最新加密連線協定如 WPA3 也一樣有效。其中有些漏洞存在長達 24 年之久。

這一系列 Wi-Fi 802.11 的資安漏洞被稱為「Frag Attacks」，主因在於攻擊係透過「碎片聚合攻擊」(Fragmentation and Aggregation Attacks) 手法進行；攻擊者只要位在有效的 Wi-Fi 通訊範圍內，即可透過這種攻擊手法取得資訊，或是在受害裝置上執行惡意軟體；只是這種攻擊方法相當複雜，不易實作。

這一系列資安漏洞共有 12 個，分為三種類別：Wi-Fi 標準設計上的漏洞共有三個，分別為 CVE-2020-24588、CVE-2020-24587、CVE-2020-24586。這一類的漏洞由於源自 Wi-Fi 連線標準設計時的疏漏，因此廣泛存於大多數支援 Wi-Fi 連線的裝置。

至於其他兩類洞，存於 Wi-Fi 標準的實作上有四個漏洞，分別為 CVE-2020-26451、CVE-2020-26144、CVE-2020-26140、CVE-2020-26143；存於其他實作層面的漏洞則有五個，分別為 CVE-2020-26139、CVE-2020-26146、CVE-2020-26147、CVE-2020-26142 與 CVE-2020-26141。

Vanhoef 指出，實驗結果證實幾乎所有 Wi-Fi 裝置都存有至少一個上述漏洞，多數產品則同時存有多個漏洞；雖然 Vanhoef 在論文發表前九個月就將此發現提報給制訂 802.11 標準的 Wi-Fi Alliance，資訊產品大廠如微軟、Cisco、HPE/Aruba、Sieaa Wireless 等也針對旗下的軟硬體產品推出資安修補工具，但由於支援 Wi-Fi 的產品數量和種類實在太龐大，因此很難在短時間內全面更新修補這些漏洞。

Vanhoef 提醒一般用戶，如果無法確認自己使用的產品已經修補上述漏洞，最簡單的自保方法，就是確認使用 **https** 安全加密連線，這樣可以完全阻絕駭侵者使用 **FragAttacks** 發動攻擊的機會。

- 資料來源：
  1. INTRODUCTION
  2. All Wi-Fi devices impacted by new FragAttacks vulnerabilities

### 3.2.2、全新 Panda 加密貨幣竊取軟體，透過垃圾郵件與 Discord 大規模散布



資安廠商發現一個全新的加密貨幣竊取惡意軟體，目前正在透過社群線上聊天服務 **Discord** 大規模散布，且在多個國家已有相當多的受害者。

資安廠商趨勢科技，日前發表研究報告，指出該公司旗下的資安研究人員，發現一個全新的加密貨幣竊取惡意軟體；這個惡意軟體命名為「**Panda Stealer**」，目前正在透過社群線上聊天服務 **Discord** 大規模散布，且在多個國家已有相當多的受害者。

趨勢科技的報告指出，這個 **Panda Stealer** 主要以夾帶惡意 **Excel** 巨集試算表的垃圾郵件散布；信件會假冒為詢問報價的商業合作郵件，受害者一旦開啟 **Excel** 附檔，就會先執行一個下載程式，下載回來的檔案就是 **Panda Stealer** 的主程式。

另外，也有些攻擊案例，是在試算表的公式中埋藏 **PowerShell** 指令，用戶執行後會連上一個文字檔分享服務，存取一個內含編碼過 **PowerShell** 指令的檔案，來達成「無檔案」的惡意軟體酬載下載。

報告指出，一旦用戶安裝了 **Panda Stealer**，該程式就會收集受害電腦上的各種加密貨幣錢包相關資訊，幣種包括 **Dash**、**ByteCoin**、**Litecoin**、**Ethereum** 等；**Panda Stealer** 同時也會竊取多種非加密貨幣服務的登入資訊，例如 **NordVPN**、**Telegram**、**Discord**、**Steam** 等，也會偷偷截取螢幕畫

面，並且竊取瀏覽器內的 cookie、儲存的密碼與信用卡資訊等。

Panda Stealer 會把竊得的資訊上傳到駭侵者部署的控制伺服器，其數量超過 140 台以上；這批控制伺服器的登入網頁，會顯示「熊猫 Stealer」的標題。

Panda Stealer 除了透過電子郵件外，同時也透過廣受歡迎的 Discord 線上聊天服務擴大其感染範圍；據報告指出，受害者最多的國家，包括澳洲、德國、美國、日本。

- 資料來源：

1. New Panda Stealer Targets Cryptocurrency Wallets
2. New Crypto-Stealer 'Panda' Spread via Discord
3. Panda Stealer dropped in Excel files, spreads through Discord to steal user cryptocurrency

### 3.2.3、Trust Wallet、MetaMask 等加密貨幣錢包遭新一波詐騙活動鎖定



Trust Wallet、MetaMask  
等加密貨幣錢包遭新一波  
詐騙活動鎖定

資安媒體發現，近日在 Twitter 上有一波針對加密貨幣錢包 Trust Wallet 與 MetaMask 用戶為目標的詐騙活動，詐騙者意圖竊取加密錢包恢復密碼，以騙取用戶存入的加密貨幣。

資安媒體 BleepingComputer 的研究人員日前發現，近日在 Twitter 上有一波針對加密貨幣錢包 Trust Wallet 與 MetaMask 用戶為目標的詐騙活動，正在大規模發動中；詐騙者意圖透過假冒的客服支援訊息，竊取受害者持有的加密錢包恢復密碼，以騙取用戶存入的加密貨幣。

MetaMask 和 Trust Wallet 是兩種廣為使用的行動加密貨幣熱錢包 App，可以讓用戶以安全儲存的方式，將加密貨幣儲存在 App 和雲端；用戶可利用其錢包功能儲存、購買、發送或接收多種加密貨幣與 NFT。

用戶初次安裝設定 MetaMask 和 Trust Wallet 時，為防止用戶忘記密碼而無法登入錢包，這兩個 App 都會產生由若干個英文字詞組成的帳號恢復密碼；但如果外人得知這組帳號恢復密碼，即可匯入用戶的雲端錢包，並且存取其中的加密貨幣。

BleepingComputer 指出，大約在兩周前開始觀察到在 Twitter 上進行的詐騙活動；有心人士在 Twitter 上搜尋 MetaMask 和 Trust Wallet 用戶發表在 Twitter 上關於使用障礙、加密貨幣被竊或其他問題的貼文，然後假扮成官方支援人員或有同樣問題的用戶回應推文，並且附上一個釣魚網址，假冒為

MetaMask 和 Trust Wallet 的用戶支援網頁，誘騙推文者在表單中輸入其加密貨幣錢包的恢復密碼。

只要成功誘使用戶輸入恢復密碼，有心人士即可立即竊走存在錢包中的所有加密貨幣，幾乎難以阻止；曾經有用戶因此被詐騙價值高達三萬美元以上的加密貨幣資產。

資安專家呼籲加密貨幣錢包的用戶，絕對不要將錢包的恢復密碼提供給任何人，因為一旦讓別人取得錢包存取權，加密貨幣遭到轉出後便無法追回，也不會有任何補償機制。加密貨幣錢包用戶，應特別提高警覺。

- 資料來源：
  1. Trust Wallet, MetaMask crypto wallets targeted by new support scam
  2. MetaMask phishing steals cryptocurrency wallets via Google ads

### 3.2.4、微軟發現多種 IoT 裝置漏洞，影響遍及製造、醫療、大型企業網路



微軟旗下的資安研究團隊，發現多達 25 個 IoT 裝置與 OT 裝置的漏洞，影響範圍遍及多種重要產業。

微軟旗下 Azure 雲端服務的資安研究團隊 Section 52，日前發現多達 25 個 IoT(Internet of Things) 裝置與 OT (Operational Technology) 裝置的漏洞，影響範圍遍及製造業、醫療產業及大型企業等多種重要產業的網路、裝置與製造系統。

據微軟表示，這些漏洞共有 25 個不同的 CVE 編號，合稱為「BadAlloc」；駭侵者可以利用這些漏洞，在各種 IoT 與 OT 裝置上誘發記憶體配置錯誤，藉以在這些裝置上遠端執行任意程式碼。

這些記憶體配置錯誤造成的 RCE 資安漏洞，廣泛存在於各種即時作業系統 (Real-Time Operating System, RTOS)、嵌入式裝置的軟體開發套件 (SDK) 與 C 語言的標準程式庫 (Libc) 等。

此外，微軟也在第一時間通報美國國土安全部 (DHS) 與各裝置製造商，DHS 旗下的資安主管機關網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)也發布資安通報，列出所有含有這批 BadAlloc 漏洞的裝置與軟體開發套件，其中包括 Google Cloud IoT Device SDK、TI SimpleLink、ARM、三星 Tizen RT RTOS、Amazon

FreeRTOS、NXP MQX、Media Tek LinkIt SDK、Windriver 等網路產品軟體  
25 項。

微軟指出，由於這些 IoT 與 OT 裝置的使用範圍極為廣泛，製造維護廠家眾多，因此難以全面更新並防堵漏洞，但建議可取得更新之產品用戶，應立即更新至最新版本，以免漏洞遭有心人士利用而造成用戶被駭。

- 建議採取資安強化措施

雖然目前微軟尚未觀察到任何濫用這批漏洞而行的攻擊事件，但為避免接下來發生大規模攻擊事件，微軟建議這類產品用戶可以：

1. 透過官方釋出已公告之更新版檔案，立即進行更新。
2. 若是無法更新產品，也應嚴加防範，並且減少這類產品直接曝露在 Internet 上的程度，並且將內部網路分區隔離，避免及縮小惡意軟體在內網散布的範圍。如果需要遠端存取這些裝置，就必須使用安全連線。

- 資料來源：

1. ICS Advisory (ICSA-21-119-04) Multiple RTOS (Update A)
2. “BadAlloc” – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in indu
3. Microsoft Discovers 25 Critical Vulnerabilities in IoT Security Affecting Google, Amazon, Samsung, a

## 3.3、國際政府組織資安資訊

### 3.3.1、比利時多個公部門遭到大規模 DDoS 攻擊



比利時多個公部門單位，於 2021 年 5 月 4 日遭到大規模分散式服務阻斷攻擊，被攻擊單位包括國會、多個行政部門、教育機構等。

比利時多個公部門單位，於 2021 年 5 月 4 日遭到大規模分散式服務阻斷攻擊（Distributed Denial of Service, DDoS），被攻擊的單位包括國會、多個行政部門、教育機構等。

攻擊者鎖定的目標，是比利時公部門使用的 Belnet 系統，這個網路系統由一家比利時的網路接取業者提供服務，專供比利時國家學術與教育機構與各級行政單位使用。

這波攻擊造成超過 200 個以上使用 Belnet 系統的單位受到影響，其內部網路與對外服務的網站系統均告癱瘓，其中包括比利時政府設立的稅務申報網站、COVID-19 肺炎疫苗施打註冊登記入口，以及各大學的 IT 系統等等。

比利時國會預定進行的多項會議，也因為網路系統癱瘓，無法進行視訊會議連線，因而被迫取消。

Belnet 表示，經過一整天的搶修與處理後，隔天已經恢復正常運作；該單位的發言人指出，雖然 Belnet 在資安上的投資相當可觀，但 5 月 4 日發生的 DDoS 攻擊，不但規模龐大，攻擊者頻繁變換攻擊方式，也造成防禦的困

難。

雖然比利時政府沒有特別指明攻擊者的可能身分，但據報導指出，部分政治學者專家懷疑，這波攻擊行動背後目的，可能是要阻擾比利時外交委員會舉辦的一場聽證會。Belnet 則表示，目前尚不清楚幕後黑手是誰。

- 資料來源：

1. Update: Belnet-netwerk opnieuw beschikbaar, onze teams blijven waakzaam
2. Belgian public-sector network suffers cyberattack, affecting parliament

### 3.3.2、美澳政府發布 Avaddon 勒索攻擊資安警訊

#### 美澳政府發布 Avaddon 勒索攻擊資安警訊



TWCERT/CC

美國與澳洲政府日前發布資安警訊，指出一個稱為 Avaddon 的勒索攻擊行動，正在全球多國肆虐，影響遍及多種行業。

美國與澳洲政府的資安主管機關，日前發布資安警訊，指出一個稱為 Avaddon 的勒索攻擊行動，正在全球多國肆虐，影響遍及多種行業。

美國聯邦調查局 ( Federal Investigation Bureau, FBI ) 和澳洲資安中心 ( Australian Cyber Security Centre, ACSC )，在各自發出的警訊中指出，包括澳洲、巴西、中國、捷克、德國、印度、義大利、秘魯、葡萄牙、阿拉伯聯合大公國、美國、比利時、加拿大、哥斯大黎加、法國、印尼、約旦、波蘭、西班牙、英國等多個國家各個重要行業中的重要企業，都遭 Avaddon 勒索團體鎖定發動攻擊。

應特別注意攻擊的重點行業，包括大專院校、航空、營建、能源、設備、金融、倉儲運輸、行政機關、醫療、資訊科技、司法、製造、行銷、零售、藥劑、虛擬娛樂業等等。

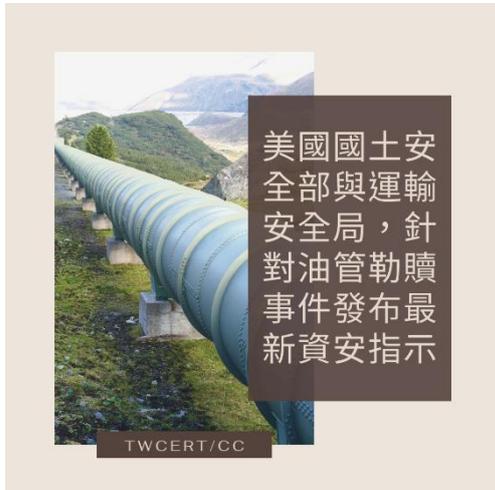
FBI 的報告中指出，該局接獲線報指出，曾在俄語駭侵相關論壇公開販售勒索服務 ( Ransomware-as-a-service ) 的 Avaddon 勒索團體，近來鎖定美國與全球各地的私人企業，包括製造業、醫療業者發動攻擊。

FBI 說，Avaddon 可能會攻擊系統上的 PowerShell、WMIC.exe、Svchost.exe、Taskhost.exe 等系統檔案來進行入侵與檔案加密作業；在 FBI 發出的 TLP:GREEN 通報中，詳細分析了 Avaddon 可能的攻擊手法；ACSC 發表的 TLP:WHITE 通報中，也列出更多可能遭到攻擊的國家與業種，並且建議可能遭攻擊的對象，儘速修補現存的各種資安漏洞，加強釣魚信件的防護與檔案備份作業。

- 資料來源：

1. Indicators Associated with Avaddon Ransomware
2. 2020-003: Ongoing campaign using Avaddon Ransomware
3. US and Australia warn of escalating Avaddon ransomware attacks

### 3.3.3、美國國土安全部與運輸安全局，針對油管勒索事件發布最新資安指示



美國國土安全部為防止再次發生造成嚴重損害的勒索攻擊事件，要求所有關鍵輸送管線的擁有者，在發現資安事故時，都必須立即通報主管機關。

美國國土安全部 ( Department of Homeland Security, DHS ) 為防止再次發生類似日前造成嚴重損害的 Colonial Pipeline 勒索攻擊事件，日前發布最新命令；該命令要求所有關鍵輸送管線的擁有者與營運者，一旦發現確認或潛在的資安事故，都必須立即通報主管機關，亦即 DHS 旗下的網路安全暨基礎設施安全局 ( Cybersecurity and Infrastructure Security Agency, CISA ) 。

該命令同時要求各管線營運單位，即日起必須立即針對內部的資安規範與運作指南進行檢討改進，找出可能的資安風險與面對各種資安威脅的不足之處即刻補強。

命令也要求各相關單位必須設置資安協調人員，必須能夠全年無休運作，發生任何資安風險、資安落差或進行緊急資安處置時，必須在 30 天以內通報美國運輸安全管理局 ( Transportation Security Administration, TSA ) 與 CISA 核備。

美國國土安全部長 Alejandro N. Mayorkas 指出，「資安領域的變化日新月异，吾人必須針對各種發展中的新威脅做好萬全準備」，「近日針對石油

製品運輸管線發動的勒索攻擊，顯示管線系統對於美國國家安全的重要性，DHS 會持續與民間部門合作，同時支持其正常運作，以提升我國關鍵基礎設施的資安危機抗抵能力。」

TSA 也表示，目前正在規畫接下來的強制性措施，以加強支援管線業者的資安防護能力，同時加強公私部門之間的資安訊息流通。

- 資料來源：
  1. DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators
  2. Homeland Security@DHSgov
  3. US announces new security directive after critical pipeline hack

### 3.3.4、國際刑警組織追回網路犯罪 8300 萬美元不法所得



國際刑警組織在一場為期超過六個月，四十國警察單位參與的亞太區網路犯罪偵辦行動中，一共攔截超過 8300 萬美元的犯罪分子不法所得。

國際刑警組織 ( International Criminal Police Organization, INTERPOL ) 在一場為期超過六個月，四十國警察單位參與的亞太區網路犯罪偵辦行動中，一共攔截超過 8300 萬美元的犯罪分子不法所得。

這次偵辦行動的代號為 HAECHI-I 行動，主要目標是結合四十多國警察，針對亞太地區日益猖獗的網路犯罪活動進行打擊。

HAECHI-I 行動的執行期間，自 2020 年 9 月至 2021 年 3 月，針對五種不同型態的網路犯罪活動加強查緝，包括投資詐騙、色誘詐騙、與非法線上賭博相關的跨境洗錢、網路性愛勒索以及語音釣魚等。

在 INTERPOL 結合各國警力，從多方面掌握犯罪者的金流動線後，成功攔截高達 8300 萬美金不法所得。

INTERPOL 在執行 HAECHI-I 行動時，針對亞太地區超過 1,400 網路犯罪活動立案偵辦，這件案件分布所在的國家包括柬埔寨、中國、印尼、韓國、寮國、菲律賓、新加坡、泰國、越南；其中成功偵破 892 個犯罪案件，在全球各地逮捕的犯罪嫌疑人的多達 585 人，也凍結了超過 1,600 個疑似由犯罪分子控制的銀行帳號；其他的目前仍在積極偵辦中。

國際刑警組織的組織與預謀犯罪總監 Ilana de Wild 指出，「網路詐騙常會利用網路無國界的特性，鎖定其他國家的受害者，並將不法所得跨境匯出；HAECHI-I 的行動成果顯示線上金融詐騙是全球性的，只有透過各國的緊密合作，才能合力對抗這些犯罪活動。」

- 資料來源：

1. Asia: USD 83 million intercepted in INTERPOL operation against online financial crime
2. INTERPOL @INTERPOL\_HQ
3. Interpol intercepts \$83 million fighting financial cyber crime

### 3.4、社群媒體資安近況

詐騙者在社群媒體上假冒 Elon Musk 等知名人士，半年內詐得高達 8000 萬美元



美國聯邦貿易委員會發布消費者警訊，指出詐騙者透過社群媒體假冒知名人士詐財的案例不斷增加。

美國聯邦貿易委員會 ( Federal Trade Commission, FTC ) 日前發布消費者警訊，指出詐騙者透過社群媒體假冒知名人士詐財的案例不斷增加，光是假冒 Elon Musk 進行的詐騙活動，自 2020 年 10 月至今，不到一年時間，就成功騙取了高達 8000 萬美元。

這份報告引用 FTC 於同一天發布的另一份報告，指出自 2020 年第四季至 2021 年第一季之間，有超過 7,000 次加密貨幣遭詐騙竊取的報案，數量是一年前的十倍以上，平均每起詐騙的損失金額，高達 1,900 美元。

報告中也指出幾個重點：20 到 49 歲的年齡層，在這些案例中是遭詐騙比例最高的一群，其遭詐騙的比例是其他年齡層的五倍以上，而且 20 到 30 歲之間的年齡層，被詐騙的金額也最高。

另外，這些詐騙案件中，有近 3500 萬元的詐騙是騙取加密貨幣，詐騙者通常會假扮為名人，在社群媒體上舉辦加密貨幣贈送活動（例如轉 0.1 枚比特幣至指定錢包，可得 0.2 枚或更高額倍數獎勵），或是其他加密貨幣空投活動，藉以誘使受害者轉帳到詐騙者的錢包中。

也有其他形態的詐騙，是假扮成外表誘人的異性，在交友網站中以甜言蜜語取得受害者信件，再詐稱介紹高獲利投資機會，要受害者轉帳到指定帳戶。

FTC 呼籲社會大眾，在參與任何看似高獲利的投資活動時，最好先搜尋相關活動名稱或公司，加上「review」（評論）、「scam」（詐騙）等關鍵字，對於明顯不合理、太過好康的甜頭，也一定要提高警覺，才能避免遭到詐騙。

- 資料來源：

1. FTC Data Shows Huge Spike in Cryptocurrency Investment Scams
2. Spotting cryptocurrency investment scams

## 3.5、行動裝置資安訊息

### 3.5.1、全新 Android 惡意軟體 TeaBot，針對歐洲各大銀行發動攻擊



資安廠商發現一個全新的 Android 惡意軟體 TeaBot，會假扮成多種常用 App，竊取受害手機用戶的歐洲多家銀行登入資訊與簡訊內容。

資安廠商 .Cleafy 日前發表研究報告指出，該公司旗下的資安研究人員，自今年一月起發現一個全新的 Android 惡意軟體，稱為 TeaBot。TeaBot 會假扮成多種常用 App，竊取受害手機用戶的歐洲多家銀行登入資訊與簡訊內容。

.Cleafy 是在今年一月起發現一個未曾出現過的全新特洛伊木馬惡意軟體，會假冒成包括 TeaTV、VLC MediaPlayer、DHL 和 UPS 的官方 Android App，但內藏的機制含有多種竊取資料與防止偵測的功能，目的在於取得受害者使用歐洲各地六十多家銀行的線上金融服務時使用的登入資訊，並發動進一步的攻擊。

據 .Cleafy 的報告指出，TeaBot 具有以下功能：

- 在用戶使用銀行服務登入時，顯示假的畫面覆蓋真實網頁，以竊取用戶輸入的登入資訊；
- 攔截用戶收到的簡訊內容。或是擅自發送、隱藏簡訊；
- 偷偷記錄用戶輸入的內容；

- 竊取 Google Authenticator 的驗證碼；
- 完整控制受害者的 Android 手機。

.Cleafy 指出，這支惡意軟體疑似是由義大利境內的駭侵團體開發，今年三月首次觀測到 TeaBot 針對義大利多家銀行發動攻擊，五月時受害銀行擴及到比利時和荷蘭；根據分析的結果，TeaBot 一共鎖定超過六十家歐洲境內的銀行，意圖發動攻擊。

另外，.Cleafy 也根據分析結果，認為 TeaBot 應該仍在早期發展階段，因為程式碼和其架構仍有許多「改善空間」；Android 用戶應特別注意，避免在非官方管道或不安全的來源，下載安裝任何可疑 App。

- 資料來源：
  1. TeaBot: a new Android malware emerged in Italy, targets banks in Europe
  2. TeaBot Android banking Trojan targets banks in Europe
  3. TeaBot Trojan Targets Banks via Hijacked Android Handsets

### 3.5.2、破億 Android 手機用戶個資遭曝於設定不當的雲端服務



資安廠商指出，有 23 支 Android 應用程式會在雲端惡意洩露用戶多項個資，受害人數估計高達一億人以上。

資安廠商 Check Point 日前發表研究報告指出，有 23 支 Android 應用程式，會在雲端惡意洩露用戶多項個資；受害人數估計高達一億人以上。

Check Point 的資安專家在報告中說，該團隊分析發現有 23 支 Android 行動應用程式，由於其雲端資料傳輸的設定有誤，導致超過一億名用戶的各種資料可在雲端服務上存取。

報告說，這 23 支不同的應用程式，其中有 13 支的下載數量在一萬次到一千萬次之間，應用程式類型包羅萬象，從星座運勢、叫車、圖標製作、螢幕截取錄製到傳真軟體等。

被洩露在雲端服務上的個資類型也很多樣，包括 email 地址、即時通訊內容、所在地座標、登入資訊、用戶拍下的相片等等；這些資訊如果落入不肖人士之手，就可以用來進行各種攻擊，包括釣魚、詐騙、社交工程、假冒身分、置換使用服務等等惡意攻擊手法。

Check Point 指出，這些 Android App 之所以會在雲端洩露用戶個資，主要原因是開發者在使用各種雲端開發資源，特別是在使用即時線上資料庫、推播服務與雲端儲存等重要常用服務時，在資安設定方面的選項設定，沒有按照保障用戶個資的最佳實務指南進行必要設定，導致設定錯誤，使得

用戶多項個資自手機上傳到雲端後，沒有得到應有的保護措施，可任意存取所致。

Check Point 在另一篇詳細的報告中——列舉被發現問題的 App 名稱與其下載次數；在發表這篇報告前，Check Point 亦曾——連絡各 App 開發者告知問題，但僅有部分 App 開發者修正其錯誤設定。

- 資料來源：

1. Misconfiguration of third party cloud services exposed data of over 100 million users
2. Mobile app developers' misconfiguration of third party services leave personal data of over 100 mill
3. 100M Android Users Hit By Rampant Cloud Leaks

### 3.5.3、Apple AirTag 遭發現可用於傳輸任意資料



資安專家發現 Apple 新上市的遺失物品追蹤裝置 AirTag 與其尋物網路 Find My，可用以傳輸任意資訊。

資安廠商 Positive Security 旗下的資安專家 Fabian Bräunlein 日前發表研究報告，發現 Apple 新上市的遺失物品追蹤裝置 AirTag 與其尋物網路 Find My，可讓沒有連上 Internet 的電腦，透過低功率藍牙連線 ( Bluetooth Low Energy, BLE ) 傳輸任意資訊。

在報告中，Fabian Bräunlein 指出，可以使用經常出現在各種 Internet of Things ( IoT ) 裝置中的 Wi-Fi 暨低功率藍牙連線模組 ESP32，配合在 Mac 電腦上執行的特製應用程式，即可在沒有 Internet 連線服務的情況下，透過 Apple Find My 網路，搜尋裝置附近的 Apple 產品中繼資料封包，將任意資料傳輸給特定對象；換言之，可以用這種方式享受免費 Internet 連線服務。

由於 Find My 網路在設計上，可讓 AirTag 定時廣播自己的存在，然後利用附近的 Apple 裝置，將加密過的位置資訊中繼並傳輸到 AirTag 的擁有者裝置上，因此在設計上在概念證實的實作中，Fabian Bräunlein 利用這個特性，把 ESP32 模擬成一個 AirTag 來進行廣播，將要傳輸的資訊編碼後塞入 AirTag 的廣播封包中，傳輸到設定為擁有者的 Mac 電腦上，再以特製的應用程式解碼，即可還原透過 ESP32 傳出的資料。

由於這個做法的實作有其難度，資安專家認為可能不致於造成大規模濫用，但在一些嚴格管控資訊外洩的場合，確實有可能利用這種方式，在沒有 Internet 連線的環境下，仍然能對外傳輸機敏資訊。

- 資料來源：
  1. Send My: Arbitrary data transmission via Apple's Find My network
  2. Apple AirTag hacked again – free internet with no mobile data plan!

## 3.6、軟體系統資安議題

### 3.6.1、美國最大石油運輸管線，遭勒索攻擊而停止運作



美國境內最大的石油運輸管線業者，日前因遭勒索軟體攻擊因而停止油品輸送業務。

美國境內最大的石油運輸管線業者 Colonial Pipeline，日前因遭勒索軟體攻擊因而停止各種油品的輸送業務。

Colonial Pipeline 於 5 月 8 日發布資安通報，指出該公司於 5 月 7 日遭到不明來源的駭侵攻擊，可能包括勒索攻擊在內，結果造成油品運輸作業受阻。

為了防止受災範圍擴大，該公司緊急停止整個管線運輸系統與部分資訊系統的運作，並會同外部獨立資安公司與司法單位介入調查整起事件的成因與受損規模。

資安專家指出，這次 Colonial Pipeline 遭到的攻擊，很可能是使用一種稱為「DarkSide」的勒索軟體進行。DarkSide 最早出現於 2020 年 8 月中旬，過去亦曾有多家大型企業遭到 DarkSide 的攻擊。

DarkSide 的攻擊方式，和其他勒索軟體如出一轍：首先透過釣魚信等方式駭入系統，接下來一邊竊取各種未加密文件與系統主機登入資訊；一旦取得內部 Windows Active Directory 的權限，就會感染所有內網裝置，竊取內

網中的檔案並且進行加密。

**Colonial Pipeline** 每天自墨西哥灣運送 250 萬桶精煉原油產品到美國東部各州，其中包括航空用油在內；由於該地區的油品庫存仍然相當充足，且因肺炎疫情造成油品消耗量下降，因此這次事件短期內不會對美東的油品供應造成衝擊。

紐約時報報導指出，**Colonial Pipeline** 拒絕說明該公司是否會拒付贖金，也沒有說明何時可以恢復供油。

有鑑於 **Colonial Pipeline** 的油管系統，自 1960 年代起就開始運作，部分系統十分老舊，也因此提高其資安風險。

- 資料來源：
  1. Media Statement Update: Colonial Pipeline System Disruption
  2. Largest U.S. pipeline shuts down operations after ransomware attack

### 3.6.2、微軟五月資安修復包，一次修復 55 個資安漏洞，以及 3 個 0-day 漏洞



微軟於推出 2021 年 5 月「Patch Tuesday」資安修復包，修復 55 個資安漏洞，其中含有 3 個 0-day 漏洞。微軟各種軟體系統用戶，應立即套用更新。

微軟於日前推出 2021 年 5 月「Patch Tuesday」資安修復包，一口氣修復 55 個資安漏洞，其中有 4 個為嚴重等級漏洞，重要等級有 50 個，1 個中等危險漏洞；更含有 3 個 0-day 漏洞。微軟各種軟體系統用戶，應立即套用更新。

這 3 個 0-day 漏洞分別如下：

- CVE-2021-31204：存於 .NET 與 Visual Studio，可用於提升執行權限；
- CVE-2021-31207：存於 Microsoft Exchange Server，可用以跳過資安檢查程序；
- CVE-2021-31200：存於 Common Utilities，可遠端執行任意程式碼。

另外，在其他於 2021 年 5 月 Patch Tuesday 修復的其他 50 多個資安漏洞中，被列為嚴重等級的 4 個漏洞，分別如下：

- CVE-2021-31166：存於 HTTP Protocol 堆疊的錯誤，可用以遠端執行任意程式碼；
- CVE-2021-26419：存於 Scripting Engine，可導致記憶體崩潰；
- CVE-2021-28476：存於 Hyper-V，可用以遠端執行任意程式碼；
- CVE-2021-31194：存於 OLE Automation 子系統中，可用以遠端執行任意程

式碼。

據微軟表示，上述的 3 個 0-day 漏洞，目前沒有遭到大規模濫用的情報出現；但由於近來有愈來愈多駭侵者，會針對廠商發行的資安修補程式進行逆向工程，以發現漏洞的利用方式，並用以攻擊尚未套用更新的電腦系統；因此使用 Microsoft 各種軟體系統產品的用戶或系統管理者，應立即依照使用手冊的建議方式套用更新，以降低這些已知漏洞遭用以發動攻擊的風險。

- 資料來源：
  1. May 2021 Security Updates
  2. Microsoft May 2021 Patch Tuesday fixes 55 flaws, 3 zero-days
  3. Microsoft Patch Tuesday: 55 Vulnerabilities, 4 Critical, 3 Publicly Known

### 3.6.3、QNAP 網路儲存設備再遭 eCh0raix 勒索軟體鎖定攻擊，用戶應提高警覺



台灣網路儲存裝置 (NAS) 製造商 QNAP，指出目前有一個稱為 eCh0raix 的勒索軟體正在發動大規模攻擊，用戶應提高警覺。

全球知名的台灣網路儲存裝置 (Network Attached Storage, NAS) 製造商 QNAP，近期發布資安警訊，指出目前有一個稱為 eCh0raix 的勒索軟體，正在發動大規模勒索攻擊，用戶應提高警覺。

這個稱為 eCh0raix 的勒索軟體，主要是攻擊 Roon Server 套件中的一個 0-day 漏洞；用戶如果在自己的 NAS 上安裝了 Roon Server 套件 2021-02-01 之前版本，就很可能遭到 eCh0raix 勒索軟體攻擊。

eCh0raix 其實並不是全新出現的勒索軟體，早在 2019 年 7 月時，趨勢科技便曾發出資安通報，揭露 eCh0raix 的存在與感染過程；不過當時的感染方式並非利用 Roon Server 套件，而是透過登入資訊暴力試誤法等較原始的攻擊方式；當時也有資安研究人員很快推出了解密工具。

QNAP 於資安通報中指出，由於 eCh0raix 主要攻擊 Roon Server 套件中的漏洞，因此建議用戶應立即從自己的 NAS 系統上移除或停止 Roon Server 的執行，同時依下列建議加強 QNAP NAS 的安全性：

- 如果仍需使用 Admin 帳號，應立即更改並使用強度足夠的密碼；
- 如果可以不使用 Admin 帳號，應先指定其他使用強式密碼的帳號擁有 admin 權限，然後刪除或停用 Admin 帳號；

- 設定 IP 連線安全性原則，短時間內重覆登入失敗的來源 IP，應自動列入黑名單，以阻絕暴力試誤登入攻擊；
- 避免開放連接埠 8080 與 443，將其改為其他隨機連接埠。
  
- 資料來源：
  1. eCh0raix Ransomware
  2. Vulnerability in Roon Server
  3. 專門攻擊 QNAP 網路儲存裝置的 eCh0raix 勒索病毒
  4. QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day

## 3.7、軟硬體漏洞資訊

### 3.7.1、QNAP 確認 Qlocker 勒索軟體係利用 HBS 後門帳號入侵



針對最近傳出全球勒索災情的 Qlocker，QNAP 發表最新資安通報，確認該勒索軟體係利用存於其 NAS 應用軟體 HBS 3 內含的資安漏洞 CVE-2021-28799。

針對最近傳出全球勒索災情的 Qlocker，QNAP 發表最新資安通報，確認該勒索軟體係利用存於其 NAS 應用軟體 HBS 3 內含的資安漏洞 CVE-2021-28799。

在 QNAP 於 5 月 21 日發表的最新資安通報 QSA-21-12 中，指出「在 2021 年 4 月 19 日當周開始針對 QNAP NAS 進行勒索攻擊的 Qlocker，係利用 CVE-2021-28799 漏洞進行攻擊」。

這個編號為 CVE-2021-28799 的漏洞，根據資安專業媒體 BleepingComputer 報導指出，其漏洞發生的原因在於登入資訊的硬式編碼（hard-code），使得 Qlocker 可以利用這個漏洞直接登入系統，將用戶存在 QNAP NAS 中的檔案，直接以 7zip 公用程式壓縮並加上密碼，並且向用戶進行勒索。

QNAP 在其陸續發布的資安通報中，並未提及登入資訊硬式編碼一事，但該公司提醒用戶，如果其 NAS 裝置的 QTS 和 HBS 3 為下列版本之前的舊版本，應立即更新至最新版本，以免遭到 Qlocker 攻擊。

- QTS 4.5.2: HBS 3 v16.0.0415
  - QTS 4.3.6: HBS 3 v3.0.210412
  - QTS 4.3.3 and 4.3.4: HBS 3 v3.0.210411
  - QuTS hero h4.5.1: HBS 3 v16.0.0419
  - QuTScldoud c4.5.1~c4.5.4: HBS 3 v16.0.0419 °
- 
- CVE 編號：CVE-2021-28799
  - 影響產品/版本：QTS 和 HBS 3 為下列版本之前的舊版本
    - 1、QTS 4.5.2: HBS 3 v16.0.0415
    - 2、QTS 4.3.6: HBS 3 v3.0.210412
    - 3、QTS 4.3.3 and 4.3.4: HBS 3 v3.0.210411
    - 4、QuTS hero h4.5.1: HBS 3 v16.0.0419
    - 5、QuTScldoud c4.5.1~c4.5.4: HBS 3 v16.0.0419
  - 解決方案：更新至上述版本與後續版本
- 
- 資料來源：
    1. QNAP confirms Qlocker ransomware used HBS backdoor account
    2. Qlocker Ransomware
    3. Improper Authorization Vulnerability in HBS 3 (Hybrid Backup Sync)
    4. QNAP removes backdoor account in NAS backup, disaster recovery app

### 3.7.2、Apple 修復兩個恐已遭用於攻擊的 0-day 漏洞



Apple 於日前緊急推出 iOS 14.5.1、macOS Big Sur 等作業系統更新，修復兩個可能讓駭侵者遠端執行任意程式碼的嚴重 0-day 漏洞。

Apple 於日前緊急推出 iOS 14.5.1、macOS Big Sur 11.3.1、watchOS 7.4.1 更新，修復兩個可能讓駭侵者遠端執行任意程式碼的嚴重 0-day 漏洞；由於這兩個漏洞很可能已遭駭侵者用於攻擊，因此各種 iOS、Mac、Apple Watch 裝置的用戶應立即進行系統更新。

這兩個 0-day 漏洞都發生在系統網頁瀏覽器核心 WebKit 中。根據 Apple 發表的資安更新通報指出，CVE-2021-30665 的問題在狀態管理的錯誤，可能導致記憶體崩潰，而 CVE-2021-30663 則是輸入驗證發生錯誤，可能導致整數溢位錯誤。

駭侵者可以誘導受害者前往瀏覽特製的網頁，誘發上述 WebKit 錯誤後，即可利用這兩個漏洞，遠端執行任意程式碼，進而發動攻擊活動。

由於 WebKit 同為 Mac 電腦和 iOS 行動裝置內建預設的瀏覽器核心引擎，因此必須更新的裝置種類和數量極多；以 iOS 裝置來說，即包括 iPhone 6s 與之後所有機種、iPad Pro 全系列、iPad Air 2 與之後所有機種、iPad 第 5 代與之後所有機種、iPad mini 4 與之後所有機種、iPod touch 第 7 代等，當然還包括 iMac、Mac Pro、Macbook、Macbook Air、Macbook Pro 等多種 Mac 電腦，甚至也包括 Apple Watch Series 3 後所有機種。駭侵者如

果能有效利用這兩個 0-day 漏洞，就可能對數量眾多的 iOS、macOS 與 Apple Watch 用戶造成嚴重威脅。

- CVE 編號：CVE-2021-30665、CVE-2021-30663
- 影響產品/版本：iPhone 6s 與之後所有機種、iPad Pro 全系列、iPad Air 2 與之後所有機種、iPad 第 5 代與之後所有機種、iPad mini 4 與之後所有機種、iPod touch 第 7 代。iMac、Mac Pro、Macbook、Macbook Air、Macbook Pro 等多種 Mac 電腦。Apple Watch Series 3 後所有機種。
- 解決方案：更新至 iOS 14.5.1、iOS 12.5.3、macOS 11.3.1、watchOS 7.4.1
  
- 資料來源：
  1. About the security content of iOS 14.5.1 and iPadOS 14.5.1
  2. About the security content of macOS Big Sur 11.3.1
  3. About the security content of watchOS 7.4.1
  4. About the security content of iOS 12.5.3
  5. Apple fixes 2 iOS zero-day vulnerabilities actively used in attacks

### 3.7.3、Apple 修復已遭駭侵者大規模濫用的三個嚴重 tvOS 與 macOS 0-day 漏洞



**Apple 針對 tvOS 與 macOS 發布資安更新，修復三個可能讓駭侵者遠端執行任意程式碼或竊取用戶機敏資訊的 0-day 漏洞，用戶應立即更新以避免遭駭。**

Apple 針對 tvOS 與 macOS 發布資安更新，一共修復了三個可能讓駭侵者遠端執行任意程式碼，或是竊取用戶機敏資訊的 0-day 漏洞；Mac 電腦和 Apple TV 的用戶應立即更新系統軟體，以降低遭駭侵者利用這些漏洞發動攻擊的風險。

在這三個 0-day 漏洞中，有兩個發生在 Apple TV 4K 和 Apple TV HD 的 WebKit 引擎內，駭侵者可以利用特製網頁內容，誘發記憶體崩潰錯誤，進而遠端執行任意程式碼。

這兩個 0-day 漏洞的 CVE 編號分別為 CVE-2021-30663 與 CVE-2021-30665；據 Apple 的更新說明頁面指出，Apple 已獲悉這兩個 0-day 漏洞很可能已遭駭侵者大規模濫用。

另一個影響 macOS 的 0-day 漏洞，出現在 macOS Big Sur 的 TCC 架構的權限問題。TCC 架構的功能是阻擋已安裝應用程式私下存取用戶存在電腦上的機敏資訊；這個 0-day 漏洞可以讓駭侵者利用特製的應用程式，跳過 TCC 的阻擋，直接竊取用戶的機敏資訊。

這個 0-day 漏洞的 CVE 編號為 CVE-2021-30713；據 Apple 的更新說明頁面指出，Apple 已接獲報告指出這個 0-day 漏洞很可能已遭駭侵者大規模濫用。

資安廠商 Jamf 指出，該單位發現有個叫做 XCSSET 的惡意軟體，正是利用 CVE-2021-30713，針對 Mac 電腦發動攻擊；該惡意軟體能夠在用戶不知不覺得情形下，取得完整的磁碟存取權限、進行螢幕錄製或擷圖，也能取得其他資料的存取權限。

由於這三個 0-day 漏洞的嚴重性，Mac 電腦與 Apple TV 用戶，應盡速透過系統更新功能，更新至 macOS Big Sur 11.4 與 tvOS 14.6，以避免遭到駭侵者利用這些 0-day 漏洞發動攻擊。

- CVE 編號：CVE-2021-30663、CVE-2021-30665、CVE-2021-30713
  
- 資料來源：
  1. About the security content of tvOS 14.6
  2. About the security content of macOS Big Sur 11.4
  3. Zero-Day TCC bypass discovered in XCSSET malware
  4. Apple fixes three zero-days, one abused by XCSSET macOS malware

### 3.7.4、賓士聯手資安業者，強化車用系統資安防護



搭載在各款 Mercedes-Benz 乘用車內的資訊娛樂系統，內含五個資安漏洞，其中四個屬於可讓駭侵者遠端執行任意程式碼的嚴重漏洞。

Mercedes-Benz 的總公司戴姆勒 (Daimler) 於 2020 年 12 月與騰訊安全科恩實驗室 (Tencent Security Keen Lab) 合作，進行搭載在各款 Mercedes-Benz 乘用車內的資訊娛樂系統 Mercedes-Benz User Experience (MBUX) 的預防性檢查，加強系統的資安防護。

研究人員檢測出五個資安漏洞，其中四個屬於可讓駭侵者遠端執行任意程式碼的嚴重漏洞。

五個資安漏洞 CVE 編號為 CVE-2021-23906、CVE-2021-23907、CVE-2021-23908、CVE-2021-23909、CVE-2021-23910，可以讓外部駭侵者在其資訊娛樂系統上遠端執行任意程式碼，但無法介入汽車的實體功能，如控制方向盤或剎車系統。

這些資安漏洞存於 Mercedes-Benz 自 2018 年起開始搭載於 A-Class 車系，現已成為所有 Mercedes-Benz 乘用車系車內標準配備的 MBUX 資訊娛樂系統之內。

研究報告指出，這些漏洞存在的主因，是因為 MBUX 採用的 Linux 系統核心版本過於老舊，無法防禦特定攻擊手法；駭侵者可能透過 MBUX 使用的瀏覽器 Javascript 引擎、WiFi 晶片原本就有的缺陷、藍牙連線堆疊、USB 連

線功能和第三方應用程式等方式，來攻擊這些漏洞。

研究人員在報告中指出，在成功利用這些漏洞後，研究人員成功建立一個可持續執行的 **web shell**，擁有 **root** 權限，可以解除汽車的防盜系統、注入持續執行的後門，並可以控制車內的照明、遮陽罩等設備，但無法控制車輛的行駛機能。

在 2020 年 11 月 進行預防性檢查後，已於 2021 年 1 月發布資安更新。

- CVE 編號：CVE-2021-23906、CVE-2021-23907、CVE-2021-23908、CVE-2021-23909、CVE-2021-23910
- 影響產品/版本：Mercedes-Benz 全乘用車系
- 解決方案：Mercedes-Benz 已於 2021 年 1 月發布資安更新版本
  
- 資料來源：
  1. Mercedes-Benz MBUX Security Research Report
  2. Collaboration of Mercedes-Benz and Tencent Security Keen Lab to strengthen car IT security
  3. Researchers Find Exploitable Bugs in Mercedes-Benz Cars
  4. Tencent Security Keen Lab: Experimental Security Assessment of Mercedes-Benz Cars

## 第 4 章、資安研討會及活動

### 剖析臺灣的數位不平等

活動時間 2021 年 6 月 24 日 ( 四 ) 14:00-16:00

活動地點 本場次僅提供線上視訊服務，請報名留下資料，將在會議前提供視訊連結。

活動網站 <https://www.twsig.tw/20210624/>



主辦單位：TWNIC、NII、TWIGF

活動背景：

#### 活動概要

世界經濟論壇 ( World Economic Forum ) 發布的 2021 年《全球風險報告》中提到，新冠肺炎大流行加劇了貧富差距與社會分化，加深了數位不平等，也被列為未來 2 年即將會面對的短期風險之一。

參考台灣網路資訊中心發布的 2020 台灣網路報告，台灣偏鄉與非偏鄉的家戶上網率相差甚微。這是否代表臺灣網路使用人口沒有城鄉差距，或沒有所謂的數位不平等問題？《全球風險報告》中提到，所謂的數位不平等是指，因投資或購買能力不等、缺乏技能、政府限制或文化差異等因素，造成人民取得關鍵數位網路與技術的不均等問題。

網路平臺具偏見的演算法、人民的數位技能差距不斷擴大、政府管制措施的缺乏，都有可能加劇數位不平等問題，並進一步削弱社會凝聚力，本座談要來理解/探討臺灣的數位不平等問題。

## 【資安專題講座】管理為本的資通安全

**活動時間** 2021年06月29日(二) 13:30 ~ 16:30

**活動地點** 預計以 Microsoft Teams 軟體進行

**活動網站** [https://docs.google.com/forms/d/e/1FAIpQLSfRwL0DmhtbHg29UKhtI3vbOZL\\_R\\_I08LekmVX\\_8gxzu8c02Q/viewform](https://docs.google.com/forms/d/e/1FAIpQLSfRwL0DmhtbHg29UKhtI3vbOZL_R_I08LekmVX_8gxzu8c02Q/viewform)



### 【與你疫起防護】06/29 線上免費講座 - 管理為本的資通安全

**主辦單位：**SP-ISAC

**報名時間：**2021/06/08(二) 中午 12:00 - 06/25(五) 下午 17:00

**課程介紹：**

#### 活動概要

回顧近年，除資安法上路，資安事件層出不窮，甚至有越演越烈的趨勢，是否技術防護有其極限？還是應該回歸管理層面的討論？

本課程從我國資通安全管理法及國際資安標準 ISO27001 等角度，剖析法規要求以及資通安全管理系統(ISMS)的構面，解說管理為本的資通安全。

**課程內容安排：**

1. 國內重大資安事件探討
2. 從資通安全管理法層面探討資安管控
3. 從資通安全管理系統(ISMS)角度探討資安管控

**參加對象&資格：**

1. 企業資安相關領域相關人員與企業資安管理人員。
2. 對資訊安全有興趣者。

## 【資安學院】滲透測試方法與實務

活動時間 2021-07-02 09:00 ~ 17:00

活動地點 中華民國資訊軟體協會 訓練教室 (台北市承德路二段 239 號 6 樓)

活動網站 [https://www.cisnet.org.tw/News/activity\\_more?id=MjYwOQ==](https://www.cisnet.org.tw/News/activity_more?id=MjYwOQ==)



### 活動概要

主辦單位：中華民國資訊軟體協會

聯絡窗口：0225533988 分機 388 廖資深專員 maureen.liao@cisnet.org.tw

課程內容：

1. 滲透測試方法論研析
2. 滲透測試工具操作
3. 滲透測試實務演練

## 第 5 章、2021 年 5 月份資安情資

### 分享概況

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

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

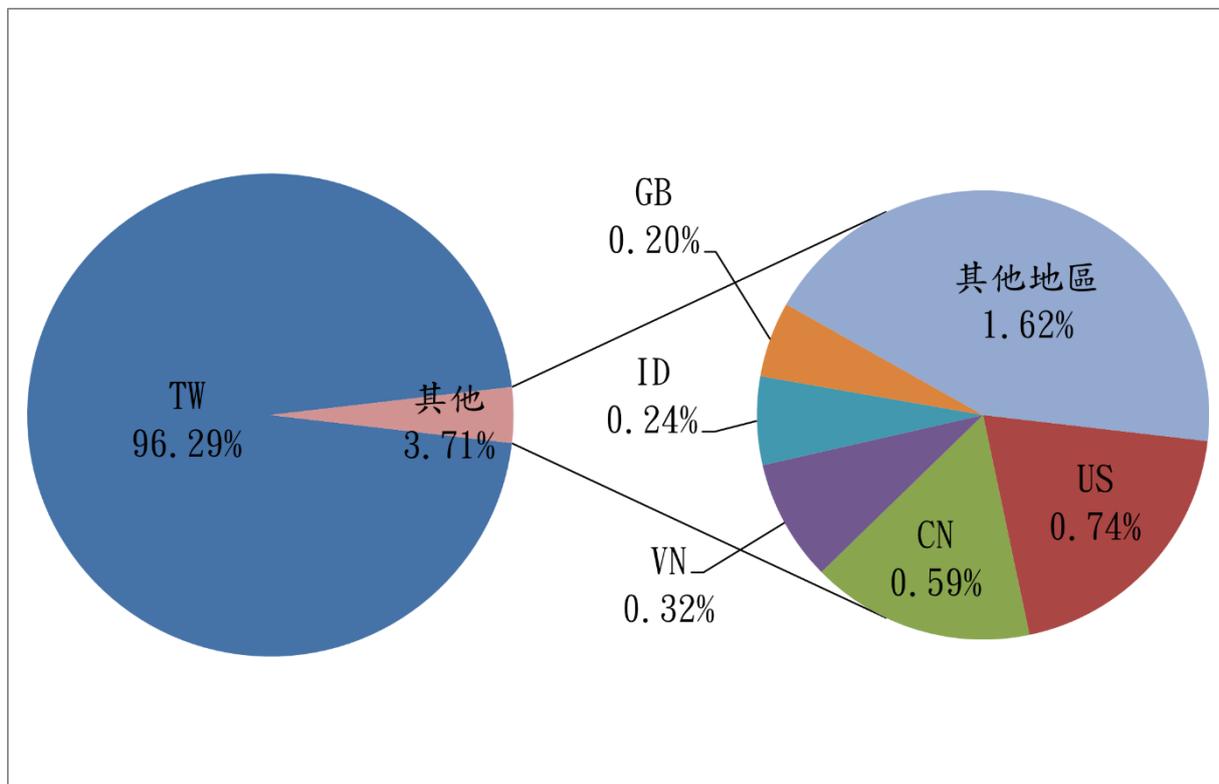


圖 1、分享地區統計圖

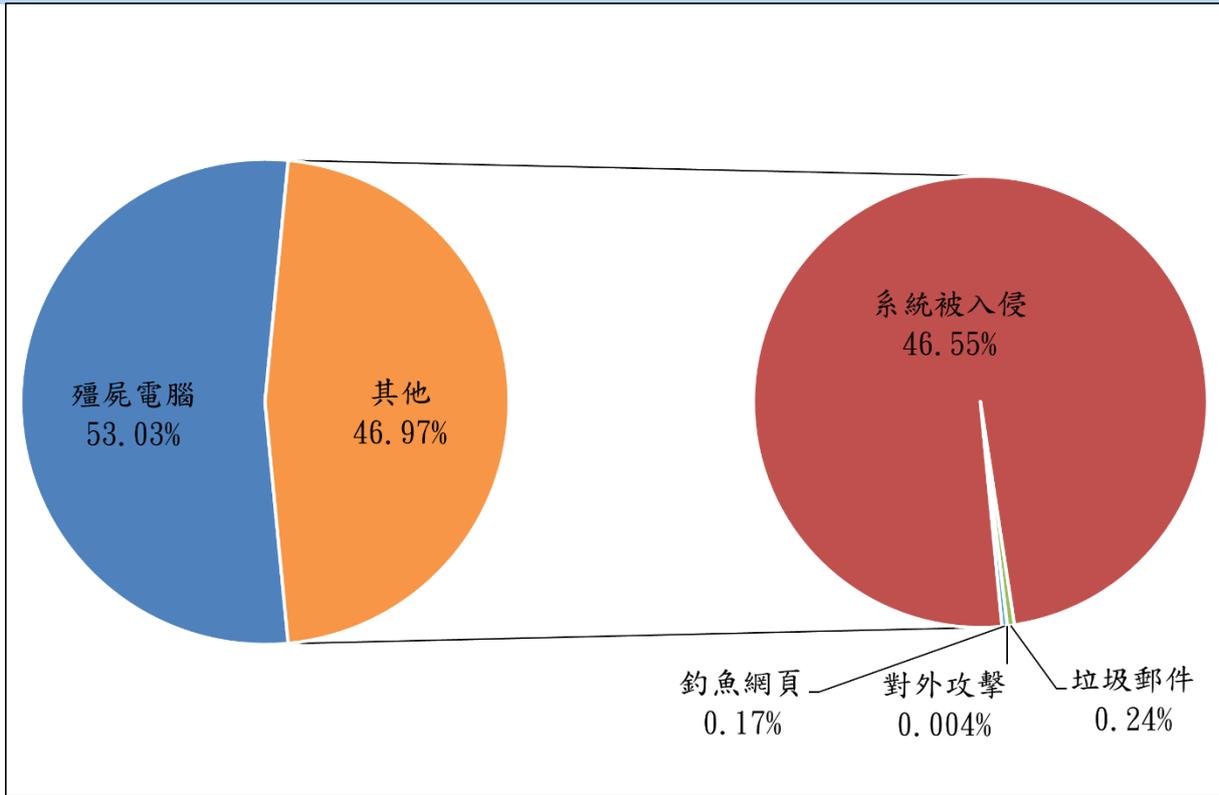


圖 2、分享類型統計圖

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

出刊日期：2021年6月10日

編輯：TWCERT/CC 團隊

服務電話：0800-885-066

電子郵件：[twcert@cert.org.tw](mailto:twcert@cert.org.tw)

官網：<https://twcert.org.tw/>

痞客邦：<http://twcert.pixnet.net/blog>

Facebook 粉絲專頁：<https://www.facebook.com/twcertcc/>

Instagram：<https://www.instagram.com/twcertcc/>

Twitter：[@TWCERTCC](https://twitter.com/TWCERTCC)