TWCERT/CC 資安情資電子報

2021 年 12 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 4 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、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、新興應用資安、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、軟體系統資安議題及軟硬體漏洞資訊。

第 3 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 4 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
多款家用路由器發現資安漏洞，國內廠商釋出更新檔，建議用戶盡速進行更新 .. 1
第 2 章、 國內外重要資安事件 4
2.1、 資安趨勢 4
2.1.1、 國際資安廠商統計發現，營建業遭勒索攻擊最為嚴重 4
2.1.2、 針對能源產業員工發動的行動釣魚攻擊，今年較去年增加 161% 6
2.2、 新興應用資安 8
2.2.1、 美國線上券商 Robinhood 客服部門遭駭侵攻擊，700 萬用戶個資外洩 8
2.2.2、 駭侵者利用 Google 搜尋廣告推廣詐騙錢包與交易所連結，成功竊得用戶加密資幣資產 10
2.2.3、 駭侵者針對 Discord 上的加密貨幣社群散布 Babadeda 木馬，意在竊取用戶數位資產 12
2.3、 國際政府組織資安資訊 14
2.3.1、 美國資安主管機關下令，聯邦政府民事機關須限期修補數百個已知資安漏洞 14
2.3.2、 歐洲刑警組織會同多國，共同打擊勒贖團體，逮捕 18 名駭侵攻擊分子 16
2.4、 社群媒體資安近況 18
2.4.1、 假冒端對端加密的 SoSafe Chat 社群聊天 Android App，內藏會竊取用戶機敏資訊的木馬 GravityRAT 18
2.4.2、 駭侵團體利用 MSHTML 漏洞發動攻擊，竊取 Google、Instagram 登入資訊 20
2.4.3、 新發現二波針對 TikTok 網紅的釣魚郵件攻擊，意在竊取帳號控制權 ... 22
2.5、 行動裝置資安訊息 24
2.5.1、 BrazKing 特洛依木馬捲土重來，以新技巧繞過資安偵側並降低受害者戒心 24
2.5.2、 新發現 Android 惡意軟體，鎖定 Netflix、Instagram、Twitter 用戶發動攻擊 26
2.5.3、 近 200 個應用程式商店中的 Android 手機遊戲遭植入 Cynos 木馬惡意軟

體 28
2.6、 軟體系統資安議題 30
2.6.1、 廣為使用的 Npm COA、RC 公用程式庫遭注入惡意程式碼 30
2.6.2、 美國猶他州醫學中心發生 58 萬病患個資外洩事件 32
2.7、 軟硬體漏洞資訊 34
2.7.1、 國內 IC 設計公司修復 Android 手機晶片竊聽漏洞，影響 30% Android 裝置 34
2.7.2、 資安專家發現可跳過 CVE-2021-34484 修補程式的 0-day 漏洞，可用於提升執行權限 36
2.7.3、 Windows 10 最新 0-day 權限提升漏洞，已有非官方修補工具可用 38
2.7.4、 新發現的 BotenaGo 僵屍網路惡意軟體，鎖定 33 個老舊漏洞，數百萬 IoT 裝置遭攻擊 40
2.7.5、 600 萬台英國 Sky 寬頻用戶端路由器的資安漏洞，修復期間長達 17 個月 42
2.7.6、 微軟推出 2021 年 11 月 Patch Tuesday 例行資安更新包，共修補 55 個漏洞，包括 6 個 0-day 漏洞 44
第 3 章、 資安研討會及活動 46
第 4 章、 2021 年 11 月份資安情資分享概況 53

第 1 章、 封面故事

多款家用路由器發現資安漏洞，國內廠商已釋出更新檔，建議用戶盡速進行更新

德國媒體會同資安專家檢測市售多個廠牌的九種暢銷家用路由器，總共發現多達 226 個資安漏洞，影響裝置數量超過數百萬台之多，用戶應提高警覺並儘速更新。

進行這次測試的是資安廠商 IoT Inspector 與德國資訊科技媒體 CHIP，蒐集市面上十分熱門的家用無線路由器來進行測試，其中也包括數個台灣廠商的產品，其測試機種，與其被發現的資安漏洞個數，分別如下：

- Asus ROG Rapture GT-AX11000：25 個(華碩安全公告請點此)
- AVM FritzBox 7530AX：20 個
- AVM FritzBox 7590AX：18 個
- D-Link DIR-X5460：26 個(D-Link 支援公告請點此)
- Edimax BR-6473AX：25 個
- Linksys Velop MR9600：21 個
- Netgear Nighthawk AX12：29 個
- Synology RT-2600AC：30 個
- TP-Link Archer AX6000：32 個

參與測試的資安專家指出，CHIP 測試的都是市場上的最新機種，廠商送測時也均更新至最新版本：漏洞最多的 TP-Link 產品有多達 32 個資安漏洞，其中更有 11 個屬於高度危險，其次是 Synology 產品，總漏洞數也高達 30 個之多。漏洞最少的 AVM Fritzbox 7590 AX 也有多達 18 個漏洞。

資安專家指出，這些路由器的漏洞不全是危險等級的漏洞，會存有這麼多漏洞的主要原因歸納如下：

- 韌體採用的 Linux 作業系統版本太過老舊；
- 多媒體與 VPN 功能使用的程式碼太過老舊；
- 採用的 BusyBox 程式版本太舊；
- 使用容易遭到破解的管理者密碼；
- 在韌體程式碼中以明文寫入登入資訊。

- 建議採取資安強化措施

1、鑑於各廠牌家用路由器經常被資安專家找到多個漏洞，建議所有家中裝有寬頻網路服務的用戶，都應開啟路由器的自動更新功能、更改預設管理者密碼，且如果沒有使用 UPnP 或 WPS 功能，都應將之關閉，以強化路由器的安全防護設定。

2、Asus 近期已針對多款路由器產品(GT-AXE11000, GT-AX11000, GT-AX2900, TUF-AX3000, RT-AX92U,RT-AX88U, RT-AX86U, RT-AX68U, RT-AX58U, RT-AX56U, RT-AX55, RT-AC88U, RT-AC3100, RT-AC86U, RT-AC2900, RT-AC1750_B1, RT-AC1900, RT-AC1900P, RT-AC1900U, RT-AC66U_B1, RT-AC68P, RT-AC68R, RT-AC68RF, RT-AC68RW, RT-AC68U, RT-AC68W, ZenWiFi AX, ZenWIFi AC, ZenWiFi AC mini, ZenWiFi AX mini)進行例行性韌體更新，敬請用戶參考華碩官方網站 ASUS Product Security Advisory 之說明並進行韌體下載與更新，以達到最佳的安全防護。

3、D-Link 已公布 DIR-X5460 產品之相關訊息，請相關用戶盡速進行更新。後續也要請相關用戶定期進行更新並維持最新版本，以保持產品的使用

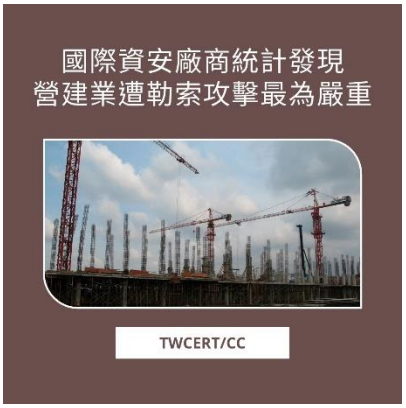
安全。

- 資料來源：
  1. Hackers welcome: Major security test uncovers vulnerabilities in all common Wi-Fi routers
  2. WLAN-Router im Sicherheits-Check
  3. 華碩安全公告 ASUS Product Security Advisory
  4. Nine WiFi routers used by millions were vulnerable to 226 flaws
  5. D-Link Support Announcements DIR-X5460 :: H/W Rev. Ax :: F/W v1.10b10 :: Multiple Vulnerability repo

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、國際資安廠商統計發現，營建業遭勒索攻擊最為嚴重



資安廠商近期發表統計報告，指出 2020 - 2021 年全球遭到勒索攻擊最嚴重的行業，包括營建業、製造業、金融業、醫療業、教育業、科技與 IT、汽車業、政府單位、法律業等。

資安廠商 NordLocker 近期發表統計報告，指出在 2020 - 2021 年全球遭到勒索攻擊最嚴重的 35 種行業，排名依序為營建業、製造業、金融業、醫療業、教育業、科技與 IT、汽車業、政府單位、法律業等。

NordLocker 的研究報告，收集 2020 - 2021 年間全球共 1,200 次各種駭侵攻擊資料，分析受勒索攻擊為害最深的 35 種行業。其中營建業有超過 90% 以上都曾遭到勒索攻擊，而製造業亦高達 85% 以上，金融業則達 70% 以上。

若以發動攻擊的前十大勒索軟體 / 團體來說，為害最烈的是 Conti，有高達 450 起案例，其次為 REvil（210 起）、DoppelPaymer（200 起）、PYSA（188 起）、CLOP（37 起）、Hive Leaks（30 起）、Ragnar Locker（30 起）、RansomEXX（27 起）、Lorenz（17 起）、Payload.bin（11 起）。

NordLocker 指出，上面的統計只是針對已知的勒索駭侵攻擊，而最嚴重的駭侵攻擊，很可能目前尚未對外公開。另外，針對營建業竟然名列各行各業中遭勒索最嚴重的行業，NordLocker 認為原因在於營建業的規模十分龐

大，多半都是由多家沒有自有 IT 或資安團隊的一系列公司所組成，因此在對抗資安攻擊方面，能力十分薄弱。

- 建議採取資安強化措施

針對各行業廠商如何防制勒索攻擊，NordLocker 提出多個建議，包括僱用資安專家協助建置資安防護機制、建立運作順暢的備份機制、針對 Email 進行加強保護，以避免附加檔案含有惡意連結或惡意軟體，同時偵測釣魚信件、提早與司法執法單位密切合作、加強企業內部教育訓練、時時保持軟體更新到最新版本等等。

建議企業可參考 antiransom.tw 勒索軟體防護專區的指南與檢核表，以預防駭侵攻擊。專區內提供事前-勒索軟體預防措施、事中-被勒索軟體攻擊時的應變措施以及事後-回復階段的作法。若不幸遭受攻擊，也可向調查局或刑事局報案尋求協助，並通報 TWCERT/CC。

- 資料來源：

1. These industries were the most affected by the past year of ransomware attacks
2. Top industries hit by ransomware
3. 勒索軟體防護專區

2.1.2、針對能源產業員工發動的行動釣魚攻擊，今年較去年增加 161%

資安廠商近日發表研究報告，指出在 2021 年針對能源產業員工發動的行動釣魚攻擊，較去年下半年增加 161%。

資安廠商 Lookout 近日發表研究報告，指出在 2021 年針對能源產業員工發動的行動釣魚攻擊，較去年下半年增加 161%，而且增幅仍在持續上昇中。

Lookout 的報告指出，雖然各行各業都因為從業人員使用老舊且存有許多漏洞的行動裝置，因而飽受行動駭侵攻擊的威脅，但能源產業是這類攻擊最主要的鎖定目標；其次則是金融業、製藥業、政府單位與製造業。

如果以受攻擊地域來看，針對能源產業的行動釣魚攻擊，發生最嚴重的地區是亞太地區，今年佔比高達 24.2%；其次為歐洲（21.7%）與北美（15.9%）；但如果以全球的發生趨勢來看，則是逐年遞增之中。

報告也指出，在全球能源產業中，高達 20% 的從業人員曾經遭到行動釣魚攻擊鎖定；這個比例和去年下半年相比增加了 161%。

報告也說，由於 COVID-19 肺炎疫情的影響，許多員工依賴 VPN 系統進行遠距工作，因此 VPN 系統的登入資訊，成為行動駭侵攻擊的主要對象；報告說有高達 67% 的行動釣魚攻擊的目的，都是為了取得員工登入企業 VPN 系統的權限。

至於用來發動行動釣魚攻擊的法，包括發送釣魚信件、釣魚簡訊、釣魚用惡意 app、假冒企業網站的登入頁面等。

報告也特別指出 Android 系統的危險性。由於高達 65% 的能源產業員工，使用太過老舊且存有多種漏洞的 Android 系統行動裝置，因此非常容易遭到攻擊。報告指出，在最新版本的 Android 11 推出一年後，只有 44.1% 的用戶升級到最新系統；而採用最新版 iOS 14 的比例則高達 84.9%。

- 資料來源：
  1. Lookout Data Shows Already Strained Energy Industry Faced With 161% Surge in Mobile Phishing
  2. Energy industry ‘most-hit’ for mobile phishing attacks

2.2、新興應用資安

2.2.1、美國線上券商 Robinhood 客服部門遭駭侵攻擊，700 萬用戶個資外洩

美國的線上證券交易平台 Robinhood 日前公開一起資料外洩事件；該公司系統遭到駭侵攻擊，約有 700 萬名用戶的個資遭竊。

美國知名且用戶眾多的線上證券交易平台 Robinhood，日前發布資安通報，公開一起發生於 2021 年 11 月月初的資料外洩事件；該公司系統遭到駭侵攻擊，約有 700 萬名用戶的個資遭竊。

攻擊事件發生在 2021 年 11 月 3 日，有一位 Robinhood 客戶服務部的員工，接到駭侵攻擊者的電話；該攻擊者以社交工程（social engineering）手法，取得 Robinhood 客服系統的存取權限。

駭侵者隨後利用取得的存取權限，取得大批 Robinhood 線上券商的用戶資料，資料欄位包括用戶全名、Email 地址等，有一部分用戶的出生年月日與郵遞區號等機敏資訊也同時遭竊。

據 Robinhood 發布的公告指出，詳細的資料遭竊與受害者數量情形如下：Email 外洩（500 萬人）、真實姓名（200 萬人）、姓名 + 生日 + 郵遞區號（300 人）、更多個資（10 人）。

Robinhood 說，該公司目前正在針對整個資料外洩事件展開詳細調查工作，目前沒有跡象顯示包括用戶的社會安全號碼、銀行帳號、金融卡卡號等金融相關資料在這次事件中遭竊。

雖然這次外洩事件中流出的用戶資料種類有限，但資安專家指出，這些資料以足夠讓駭侵者據以發動各種進一步的資安攻擊，例如釣魚攻擊或社交工程攻擊等。

專家呼籲 Robinhood 用戶，近期應對各種形式的釣魚攻擊提高警覺，因為駭侵者可能會假冒 Robinhood 或其他機構發送釣魚信件，假稱用戶帳號出現問題，藉以騙取用戶輸入帳號登入資訊。

- 資料來源：
  1. Robinhood Announces Data Security Incident
  2. Robinhood says millions of customer names and email addresses taken in data breach
  3. Robinhood discloses data breach impacting 7 million customers

2.2.2、駭客用 Google 搜尋廣告推廣詐騙錢包與交易所連結，竊得用戶加密資幣資產

資安廠商發現近來有駭侵團體，在 Google 搜尋頁面購買廣告，宣傳詐騙加密貨幣錢包和去中心化交易所，以竊取受害者的加密貨幣資產。

資安廠商 Check Point 日前發表研究報告，指出該公司旗下的資安研究人員，近來發現有駭侵團體在 Google 搜尋頁面購買搜尋關鍵字廣告，藉以宣傳詐騙加密貨幣錢包和去中心化交易所（Decentralized Exchange, DEX），用來竊取受害者的加密貨幣資產。

專家說，這些駭侵者在廣告中放置假的 Phantom 和 MetaMask 錢包軟體，宣稱可以用於儲存、交易近日十分熱門的 Solana（SOL）加密貨幣與以太幣；駭侵者也透過廣告來宣傳假的去中心化交易所，如 PancakeSwap 和 UniSwap。

駭侵者在廣告中放置的連結，其網域名稱和真實的 Phantom 錢包的真正網域 Phantom.app 非常接近，例如 Phanton.app、Phantonn.pw，用這種障眼法來魚目混珠，降低潛在受害者的戒心。

潛在受害者一旦點擊這些廣告，導向到詐騙網站後，網站會要求用戶新增一個錢包，並且寫下駭侵者設定好，顯示在網頁上的錢包取回回復詞組；當受害者做完這些動作後，馬上會被導向到真正的 Phantom 錢包頁面。

接著用戶會輸入剛才由駭侵者提供的回復詞組，取回帳號控制權；受害者就會以為這個新增的錢包是自己的，但實際上這個錢包卻是由駭侵者所擁有的錢包；因此任何存到錢包中的加密貨幣，實際上等於進了駭侵者的口

袋。

Check Point 發現駭侵者以同樣的帳號製作了多個類似的詐騙錢包，且已經盜領的加密貨幣總額也不在少數。目前 Google 已將這些詐騙廣告下架。

資安專家呼籲加密貨幣投資者，一定要徹底檢查任何 URL 的真偽，在點擊搜尋頁面上的連結時，也要確認不是點到廣告，就可以減少點到詐騙連結的機會。

- 資料來源：
  1. Scammers used Google Ads to Steal ~ $500k Worth of Cryptocurrency
  2. Crypto investors lose $500,000 to Google Ads pushing fake wallets

2.2.3、駭客針對 Discord 加密貨幣社群散布 Babadeda 木馬，意在竊取用戶數位資產

資安廠商發現一個新的惡意軟體攻擊行動，目標鎖定 Discord 上廣大討論加密貨幣、去中心化金融、非同質代幣等社群散布名為 Babadeda 的惡意軟體。

資安廠商發現一個新的惡意軟體攻擊行動，在社群平台 Discord 展開，目標鎖定 Discord 上廣大討論加密貨幣、去中心化金融、非同質代幣等社群散布名為 Babadeda 的惡意軟體，並且竊取用戶數位錢包中的加密貨幣資產。

資安廠商 Morphisec 旗下的研究人員，日前發現一個新的惡意軟體攻擊行動，在社群平台 Discord 展開；其攻擊目標鎖定 Discord 上眾多討論加密貨幣、去中心化金融（Decentralized Finance, DeFi）、非同質代幣（Non-Fungible Token, NFT）的群組成員，在社群中散布一個名為 Babadeda 的惡意軟體，並且竊取用戶數位錢包中的加密貨幣資產。

據 Morphisec 的報告指出，Babadeda 是一種可將惡意程式碼加密並植入看似無害應用程式安裝器或程式本身的加密工具，進入電腦後，可以進一步安裝各種駭侵用酬載。該公司自 2021 年 5 月起開始發現有駭侵者利用 Babadeda 植入惡意程式碼，並在 Discord 上以加密貨幣為討論主題的相關社群中散布這些惡意軟體。

駭侵者會先在相關討論群組中加入討論，然後發送私訊給群組成員，分享一個好玩的遊戲，但其中就植入了 Babadeda 惡意軟體；也有駭侵者假扮成某些區塊鏈專案的人員，邀請群組成員參與活動；一旦受害者點擊並進入駭侵者架設，以極相似網址設立的釣魚網站，下載安裝植入惡意軟體的遊戲或

應用程式，就會感染 Babadeda。

Badadeda 在過去曾經用於在受害者的 Windows 電腦中安裝各種資訊竊取軟體、遠端存取木馬，甚至像是 LockBit 之類的勒贖軟體；不過這波針對加密貨幣社群的攻擊行動，主要酬載的惡意軟體是 Remos 和 BitRAT 等，可以遠端監控受害者的電腦，並且竊取各種登入資訊、瀏覽器 cookie 或安裝更多酬載。

資安專家指出，由於此波主要的攻擊對象，是加密貨幣相關社群成員，因此駭侵者的攻擊目的，很可能就是要竊取受害者數位錢包中的加密資產。

- 資料來源：
  1. BABADEDA CRYPTER TARGETING CRYPTO, NFT, AND DEFI COMMUNITIES
  2. Discord malware campaign targets crypto and NFT communities

2.3、國際政府組織資安資訊

2.3.1、美國資安主管機關下令，聯邦政府民事機關須限期修補數百個已知資安漏洞

美國資安主管機關網路安全暨基礎設施安全局，發布今年首次的強制性操作指引，命令美國聯邦政府民事相關機關，必須在短時間內針對多個資安漏洞進行處理。

美國資安主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA），日前發布今年首次的強制性操作指引（Binding Operational Directive，BOD），命令美國聯邦政府民事相關機關，必須在短時間內針對多個資安漏洞進行處理。

這份編號為 BOD-22-01 的指引，全名為「降低已知遭利用漏洞的顯著風險」（Reducing the Significant Risk of Known Exploited Vulnerabilities），適用於由各聯邦機關自行操作，或交由第三方代管理的所有連網或非連網資訊系統的硬體與軟體；所有受此命令規範的單位，必須在期限內依照指引，即刻處理表列清單中的各種漏洞。

CISA 同時也公告了一份含有數百個已知遭駭侵攻擊活動利用過的漏洞清單，供各公私單位參考；清單中列明有漏洞的軟硬體產品與系統範圍甚廣，其中也包括部分台灣廠商的產品；較知名者包括 Adobe、Android、Apache、Apple、Arm、Atlassian、Cisco、Citrix、D-Link、Dreytek、Fortinet、Google、IBM、Microsoft、Mozilla、Netgear、Oracle、Pulse、Qualcomm、Realtek、SAP、SolarWinds、SonicWall、Sophos、Symantec、TeamViewer、

TrendMicro、VMware、WordPress、Zoho、ZyXEL 等。

CISA 在這項命令中要求，在 2021 年遭到駭侵攻擊活動利用的漏洞，必須在 11 月 17 日前修補完成；而在去年年底之前遭到駭侵攻擊活動利用的漏洞，則須在 2022 年 5 月 3 日前完成修補。

- 資料來源：
  1. Binding Operational Directive 20-01
  2. KNOWN EXPLOITED VULNERABILITIES CATALOG

2.3.2、歐洲刑警組織會同多國，共同打擊勒贖團體，逮捕 18 名駭侵攻擊分子

歐洲刑警組織宣布逮捕多名駭侵勒贖不肖分子；這批勒贖嫌犯涉及的駭侵攻擊事件，範圍廣達 71 國，受害者多達 1,800 名個人或組織。

歐洲刑警組織（Europol）近期發布公告，宣布該組織會同多國執法單位，逮捕 18 名駭侵勒贖不肖分子；這批勒贖嫌犯涉及的駭侵攻擊事件，範圍廣達 71 國，受害者多達 1,800 名個人或組織。

根據歐洲刑警組織發表的報告指出，這批勒贖攻擊嫌犯發動的勒贖攻擊活動，包括 LockerGoga、MegaCortex、Dharma 等，使用的惡意軟體工具包括 TrickBot 和 Cobalt Strike 等。

根據荷蘭國家資安中心（National Cyber Security Centre）指出，LockerGoga 和 MegaCortex 以及另一種勒贖攻擊 Ryuk，近年來就在荷蘭發動 1,800 次以上的攻擊。

駭侵犯罪分子的逮捕行動，於 2021 年 10 月 26 日於烏克蘭和瑞士同步啟動；除了逮捕 18 名不肖分子之外，更緝獲大批名貴財物，包括 5 台豪華電動車與現金 52,000 美元。

警方在逮捕這批駭侵犯罪分子後，立即展開後續的調查行動；目前已知這批遭到逮捕的駭侵者，在多起駭侵攻擊活動中，都扮演重要角色；有人專門負責入侵攻擊目標的內部網路，有人負責發動釣魚攻擊，有人負責在 SQL 資料庫中注入攻擊程式碼等。

在歐洲刑警組織發表這次公告後，多個參與聯合駭侵打擊行動的國家，也發表相關的公告。挪威警方表示，該國執法單位會持續和世界各國檢警單位合作，持續打擊資安攻擊活動與組織，以遏止不肖分子的活動。

- 資料來源：
  1. EU SOCTA 2021
  2. Kripos del av stor aksjon mot organiserte digitale kriminelle
  3. Police arrest hackers behind over 1,800 ransomware attacks

2.4、社群媒體資安近況

2.4.1、SoSafe Chat 社群聊天 Android App，內藏竊取機敏資訊的木馬 GravityRAT

資安廠商發現一個號稱提供端對端加密安全聊天功能的 Android App，內含惡意程式碼，會竊取用戶的機敏資訊。

資安廠商 Cyble 旗下的研究人員，最近發現一個號稱提供端對端加密安全聊天功能的 Android App，名為 SoSafe Chat，內含惡意程式碼 GravityRAT，會竊取用戶的機敏資訊。

這個 GravityRAT 惡意軟體是一種遠端存取木馬程式，主要是由巴基斯坦的駭侵者發動攻擊，目標對象是鎖定印度用戶；資安廠商分析其獲得的攻擊目標資訊，發現 GravityRAT 會集中攻擊印度的知名人士，特別是印度軍方的軍官與高階將領等。

受害用戶一旦安裝了 SoSafe Chat，其中的 GravityRAT 就會竊取用戶手機中的各種機敏資訊，包括讀取用戶的簡訊內容、通話記錄、通訊錄、竄改手機系統設定、手機在基地台的註冊資訊、電話號碼、手機序號、手機內的檔案、盜錄對話、傳回手機所在地資料等。

事實上，這並不是 GravityRAT 首次出現。資安專家指出，2020 年時 GravityRAT 就曾透過另一個名為 Travel Mate Pro 的旅遊相關軟體散布，但因肺炎疫情造成旅遊人數銳減，對旅遊 App 的需求不再，因此這次捲土重來時，就改隱身於即時訊息聊天這類社群 App 之中。

此外，GravityRAT 在 2020 年之前只感染執行 Windows 作業系統的裝置，但之後擴及到 Android 平台上；這表示其幕後的開發者和駭侵團體十分活躍。

目前 SoSafe Chat 的網站仍然還在線上運作，但 App 下載連結已經失效；資安專家提醒用戶，下載 Android App 前一定要提高警覺，除了不在可疑之處下載任何軟體外，也應仔細查閱 Google Play Store 中的評價與用戶意見，確認安全後再安裝。

- 資料來源：
  1. Gravity RAT Malware Returns As A Chat Application
  2. Fake end-to-end encrypted chat app distributes Android spyware

2.4.2、駭侵團體利用 MSHTML 漏洞發動攻擊，竊取 Google、Instagram 登入資訊

資安專家指出，近期新發現一個駭侵團體，利用 Windows 系統已知的一個 MSHTML 解析漏洞，針對全球對象發動攻擊，竊取其 Google 與 Instagram 的登入資訊。

資安廠商 SafeBreach Labs 旗下的研究人員，日前發布資安通報指出，近期新發現一個可能主要來自伊朗的駭侵團體，利用 Windows 系統已知的一個 MSHTML 解析漏洞，針對全球對象發動攻擊，竊取其 Google 與 Instagram 的登入資訊。

SafeBreach Labs 指出，該駭侵團體主要的攻擊手法，是利用魚叉式釣魚信件散布含有惡意程式碼的 Word 文件檔案，該文件檔案中的巨集程式碼，會利用一個 MSHTML 遠端執行任意程式碼漏洞 CVE-2021-40444 安裝惡意程式碼，並且透過植入的 PowerShell 指令檔收集受害者電腦中的各種機敏資訊，包括儲存資料與螢幕畫面等，送到駭侵者的控制伺服器中。

SafeBreach Labs 說，該公司觀察到的攻擊活動，是從 2021 年七月開始發動，攻擊目標遍及全球各地；目前以美國的受害者最多，佔比達 45.8%，其次是荷蘭（12.5%）、俄羅斯、加拿大、德國（同為 8.3%）、中國、韓國、英國、印度（同 為 4.2%）。

SafeBreach Labs 的研究人員表示，釣魚信件夾帶的 Word 文件，其內容是以波斯文指控伊朗政府高層造成「肺炎疫情大屠殺」；推測這波攻擊的目標，多以旅居海外，且可能被伊朗政府視為國安威脅分子的伊朗人為主。

資安專家指出，雖然在 CVE-2021-40444 這個漏洞在 2021 年 8 月公開後不到一個月，微軟就推出兩波修補程式，但可能仍有相當數量的 Windows 系統未曾套用更新，導致許多駭侵攻擊活動均透過此漏洞來發動攻擊。

- 資料來源：
  1. Shadow Chaser Group @ShadowChasing1
  2. New PowerShortShell Stealer Exploits Recent Microsoft MSHTML Vulnerability to Spy on Farsi Speakers

2.4.3、新發現二波針對 TikTok 網紅的釣魚郵件攻擊，意在竊取帳號控制權

資安廠商發現一起針對 TikTok 網紅、品牌等知名帳號的釣魚攻擊活動，駭侵者假扮為 TikTok 工作人員發送釣魚信件給知名帳號，可能意圖騙取帳號權限，或發動進一步攻擊。

資安廠商 Abnormal Security 日前在其官方部落格中發文，指出該公司旗下的資安研究人員，近日發現一起針對 TikTok 網紅、品牌等知名帳號的釣魚攻擊活動；駭侵者假扮為 TikTok 工作人員發送釣魚信件給知名帳號，可能意圖騙取帳號權限，或發動進一步攻擊。

Abnormal Security 的研究人員指出，在 2021 年 10 月 2 日和 11 月 1 日時，偵到兩波針對 TikTok 上知名帳號的釣魚郵件攻擊活動；駭侵者發送釣魚郵件的對象，以 TikTok 上頗具知名度的網紅、名人、知名品牌、製作公司、經紀人等為主。

在 Abnormal Security 截獲的釣魚攻擊信件共有兩類，都是由駭侵者假扮為 TikTok 的客服人員，分別對潛在受害者發送假冒的客服信件；其中一類是指稱收信人的帳號涉嫌盜用其他人創作的版權作品；如不在 48 小時內回覆「Confirm my account」，就會刪除受害者的 TikTok 帳號，藉以讓受害人因害怕帳號被刪除而回信。

另一類信件則是假冒為 TikTok 帳號認證（即俗稱的「小藍勾」）通過的通知信件；信件假稱該帳號在 TikTok 有許多深受用戶喜愛的原創作品，官方因而決定主動頒給帳號認證標誌（verification badge），要求用戶回覆信件以確認。

在這兩類釣魚信中，駭侵者都放置一個看似用以確認的連結，受害者點按後，會開啟一個 WhatsApp 聊天室；此時駭侵者會要求受害者提供其註冊 TikTok 使用的 Email 地址、手機號碼，以及 TikTok 系統提供的帳號重設二階段登入驗證碼；受害者如果真的提供這些資料，其登入密碼就會被駭侵者竄改，導致帳號存取權被盜。

- 資料來源：
  1. New TikTok Phishing Campaign Targets Influencer Accounts
  2. TikTok phishing threatens to delete influencers' accounts

2.5、行動裝置資安訊息

2.5.1、BrazKing 特洛依木馬捲土重來，以新技巧繞過資安偵側並降低受害者戒心

資安專家近日發現一個名為 BrazKing 的 Android 特洛伊木馬惡意軟體捲土重來，大規模感染巴西的 Android 手機金融服務使用者，竊取其金融相關資訊。

IBM 旗下的資安專家，近日發現一個名為 BrazKing 的 Android 特洛伊木馬惡意軟體，最近捲土重來，大規模感染巴西的 Android 手機金融服務使用者，竊取其金融相關資訊。

值得注意的是，為了規避愈來愈嚴格的作業系統資安防護功能，以及 Play Store 的惡意軟體防堵機制，這個 BrazKing 惡意軟體，採用了一些前所未見的全新技巧，來規避各種偵測與防堵。

IBM 指出，BrazKing 以發送釣魚簡訊的方式，把受害者導向到一個 https 網站，看起來就比較安全；而這個 https 網站的內容，是假冒 Google 的安全功能，指稱用戶的手機使用老舊的 Android 版本，存有嚴重安全漏洞，必須下載一個 APK 檔加以修補。BrazKing 就是用這種方法，不在 Google Play Store 上架，以規避應用程式商店中的惡意程式碼掃瞄機制。

當用戶下載了假冒為資安修補軟體的惡意程式後，BrazKing 接著又會假冒 Google 的系統通知，要求用戶開啟輔助使用權限；和一般會要求許多權限（例如讀取簡訊內容、螢幕擷取等）的其他「傳統」惡意軟體來看，BrazKing 只要求一項權限，看起來也顯得比較安全。

但透過這項輔助使用權限的開啟，BrazKing 仍可做到許多資料竊取功能，例如它會「拆解」用戶螢幕上顯示的資訊，送到控制伺服器中判斷畫面內容與用途，而不需實際擷取畫面；此外 BrazKing 也能記錄用戶鍵盤輸入、竊取用戶在各金融網站或 App 的登入資訊、讀取簡訊內容，以便攔截二階段登入驗證碼等等。

- 資料來源：
  1. BrazKing Android Malware Upgraded and Targeting Brazilian Banks
  2. Android malware BrazKing returns as a stealthier banking trojan

2.5.2、新發現 Android 惡意軟體，鎖定 Netflix、Instagram、Twitter 用戶發動攻擊

資安專家日前發現全新的 Android 系統惡意軟體，會利用假造的登入頁面，竊取 Netflix、Instagram、Twitter 用戶的信用卡資訊。

資安專家日前發現一個全新的 Android 系統惡意軟體，名為「MasterFred」；這個惡意軟體會利用假造的登入頁面，竊取 Netflix、Instagram、Twitter 用戶的信用卡資訊。

MasterFred 是在 2021 年 6 月時首次有取樣送到 VirusTotal 資料庫，而資安專家也在 11 月初提報了另一個取樣，主要攻擊對象是位於波蘭和土耳其的 Android 用戶。

資安廠商 Avast 分析 MasterFred 後，發現 MasterFred 會利用 Android 系統內的輔助使用 API（Application Accessibility toolkit）來顯示內含詐騙登入頁面的畫面覆疊，以欺騙用戶輸入信用卡資訊。

資安專家指出，利用 Android 系統內的輔助使用 API 來顯示詐騙覆疊畫面，並不是全新的攻擊手法；過去有相當多的惡意軟體，也會利用這種技巧來欺騙用戶。

不過 MasterFred 特別之處，在於同時還夾帶 HTML 覆疊，內含多國語言的詐騙登入頁面；MasterFred 以此來騙取用戶的金融資訊，然後再使用 Onion.ws 暗網閘道器，把竊取的資訊傳送給駭侵攻擊者。

Avast 的資安專家也說，該單位認為在 Google Play Store 中至少有一個 app 含有 MasterFred 惡意軟體；駭侵者很可能也會使用其他 Android 平台上的非 Google 應用程式商店，來散布其惡意軟體。

資安專家呼籲 Android 裝置用戶，在下載任何應用軟體前，應盡量詳加查閱該軟體在 Google Play Store 的用戶評價，負評多的軟體應該避開；並避免從不明來源處安裝應用程式，以降低遭到駭侵者植入惡意程式碼的風險。

- 資料來源：
  1. Avast Threat Labs @AvastThreatLabs
  2. Alberto Segura @alberto__segura
  3. New Android malware targets Netflix, Instagram, and Twitter users

2.5.3、近 200 個應用程式商店中的 Android 手機遊戲遭植入 Cynos 木馬惡意軟體

資安廠商發現華為自營的應用程式商店中，有超過 190 種不同的手機應用軟體遭植入 Cynos 木馬惡意程式碼，受害裝置數量可能高達近千萬台。

資安廠商 Dr.Web 近期指出，該公司發現手機大廠華為自營的應用程式商店中，有超過 190 種不同的手機應用軟體，遭駭侵者植入 Cynos 木馬惡意程式碼；據安裝次數統計，受害裝置數量可能高達近千萬台。

這次偵測到的 Cynos 木馬惡意程式為 Android.Cynos.7.origin，是一種修改過的 Cynos 特洛依木馬惡意軟體，主要功能為收集手機用戶的機敏資訊。

Dr.Web 的資安專家指出，Cynos 木馬程式最早的版本出現在 2014 年，至今不斷變種，某些版本的資料竊取功能十分強大，包括攔截簡訊、擅自發送高額付費簡訊、下載並安裝額外惡意軟體模組與其它軟體等。

至於這次發現的 Cynos 版本，則主要以竊取用戶與裝置資訊、顯示廣告為主；且會要求許多與遊戲無關的權限，例如撥打電話。

在華為應用程式商店中，遭發現內含 Cynos 木馬惡意軟體的 Android 手機應用程式，主要以遊戲為主，遍及各種受歡迎的熱門領域，包括各種射擊遊戲、即時策略遊戲、橫向捲軸遊戲、模擬遊戲等，針對俄語、中文和英文用戶發動攻擊，種類達到 190 種以上。

在這 190 種以上遊戲中，有一些的下載次數極高，例如一個稱為「快点躲起来 (Hurry up and hide)」的遊戲，下載安裝次數就高達 200 萬次；另一個

名為「Cat Adventures」的遊戲，下載次數也達 427,000 次。

Dr.Web 已在第一時間通報華為，將這批含有惡意軟體的遊戲，自應用程式商店中下架；不過安裝過這些惡意 app 的用戶，則必須自行移除。在 Github 有一份完整列表可供參考。

- 資料來源：
  1. Android.Cynos on the Huawei AppGallery — Indicators of compromise
  2. New trojan detected on AppGallery app catalog

2.6、軟體系統資安議題

2.6.1、廣為使用的 Npm COA、RC 公用程式庫遭注入惡意程式碼

又有兩個使用十分頻繁的公用程式庫，遭駭侵惡意分子植入惡意程式碼，意圖竊取用戶的登入密碼。

又有兩個使用十分頻繁的公用程式庫 Npm COA 與 Npm RC，被開發者發現遭駭侵惡意分子植入惡意程式碼，意圖竊取用戶的登入密碼。

COA 程式庫之名是 Command-Option-Argument 的縮寫，在 Npm 網站上每周下載量高達 9 百萬次，在 GitHub 上有接近 5 百萬個開放源碼軟體使用了這個公用程式庫。這個程式庫在 Node.js 專案中，是用來爬梳命令列的輸入指令。

開發者會注意到 COA 被注入惡意程式碼，是因為這個程式庫在多年未經更新後（上個版本更新於 2018 年 12 月），突然出現了數個新版本，同時造成許多使用了這個程式庫的 React 開發專案出現問題所致。

經過資安專家分析新版本的 COA 程式碼後，發現 COA 遭到注入惡意程式碼，被注入的惡意程式碼內容和上個月同樣遭到注入的另一 Npm 程式庫 ua-parser-js 大致相同，都是用來竊取使用者的登入密碼。

在開發者與資安專家發現 COA 遭注入惡意程式碼後不久，也發現另一個 Npm 程式庫 RC 也出現了奇怪的新版本；分析後發現 RC 也被注入了相同的惡意程式碼。

如果開發專案使用了含有這些惡意程式碼的公用程式庫，用戶在使用各種瀏覽器如 Chrome、Firefox、Opera、Internet Explorer、Safari 時輸入的密碼將會遭竊；除此之外，用戶使用如 VNC、FTP 連線程式、Email 軟體或線上賭場軟體時的密碼、儲存在電腦中的信用卡資訊也會被竊。

該惡意程式同時也會私下擷取螢幕畫面，並記錄用戶的鍵盤輸入。

- 資料來源：
  1. Error when i install #101
  2. Last release contains malicious code #99
  3. Version 1.2.9 contains malicious code #131

2.6.2、美國猶他州醫學中心發生 58 萬病患個資外洩事件

美國猶他州的猶他影像協會日前發表資安通報，指出該單位遭到駭侵攻擊，超過 58 萬病患的多項個資遭到外洩。

美國猶他州的猶他影像協會（Utah Imaging Associates, UIA）日前發表資安通報，指出該單位遭到駭侵攻擊，超過 58 萬病患的多項個資遭到外洩。

據猶他影像協會發表的通報指出，該單位是在 2021 年 9 月 4 日發現資料外洩事件，並在當天立即採取行動修正錯誤；然而駭侵者的攻擊發動日期早在 8 月 29 日，因此有將近一星期的時間，駭侵者可以在猶他影像協會的系統中任意存取各項資料。

在第三方資安公司的協助之下，該單位已展開對這次駭侵攻擊的事件調查；目前已知資料可能遭竊的病患人數，共有 582,170 人，遭到不當存取的資料欄位與項目如下：

- 病患姓名；
- 郵寄地址；
- 出生年月日；
- 社會安全號碼（Social Security Number）；
- 健康保險編號（Health Insurance Policy Number）；
- 各種醫療資訊，包括醫師處置、診斷與處方記錄。

猶他影像協會在調查後指出，每個病患可能遭到外洩的資料欄位不同，有些比較少；此外該單位目前也沒有接獲任何這批資料遭到曝光或被外界駭侵團體利用的情報。

不過，資安專家指出，不能因此排除這批大量病患資料，被駭侵者以私下交易或交換的方式「流通」的可能性。

猶他影像協會針對此次病患資料遭竊事件的受害者，透過 IDX 提供免費 12 個月的信用異常通報服務；當用戶的信用卡遭到盜刷或盜用時，即可立即發出警訊。

資安專家表示，醫療機構擁有大量病患的健康與財務資訊，往往是駭侵者最喜歡發動攻擊的目標；但很多醫療院所在 IT 與資安的投資相對不足，有些甚至根本沒有相關人力配置，造成醫療單位的駭侵事件層出不窮。

- 資料來源：
  1. Utah Imaging Associates, Inc. Notifies Indivdiuals of Data Security Incident
  2. More than 500,000 Utahns' sensitive information possibly hacked
  3. Utah medical center hit by data breach affecting 582k patients

2.7、軟硬體漏洞資訊

2.7.1、國內 IC 設計公司修復 Android 手機晶片竊聽漏洞，影響 30% Android 裝置

台灣大型 IC 設計公司修復一系列存於其 Android 手機處理器內的漏洞，這些漏洞可能導致駭侵者竊聽手機通話、執行任意程式碼、提升執行權限等。

台灣的大型 IC 設計公司日前發表資安通報，修復一系列存於其 Andoird 手機處理器內的漏洞，這些漏洞可能導致駭侵者竊聽手機通話、執行任意程式碼、提升執行權限等。

這一系列漏洞最早是由資安廠商 Check Point 發現，其中有三個漏洞 CVE-2021-0662、CVE-2021-0663、CVE-2021-0664 已於 2021 年 10 月修復，另一個漏洞 CVE-2021-0673 將在下個月的更新中修復。

資安專家指出，該公司的手機處理器，在處理音訊的設計上，是交給一個獨立的「數位信號處理器」（Digital Signal Processor, DSP）來負責，以便提升音質，同時降低對 CPU 的負荷。

資安專家說，音訊驅動程式與 CUP，在將音訊處理工作交給 DSP 時，並非直接溝通，而是透過 IPI 訊息轉傳給系統控制處理器（System control processor, SCP）；這一系列漏洞就發生在這段過程，使得惡意程式碼可以在音訊晶片上執行其程式碼。

Check Point 的資安專家，利用逆向工程解析之後，指出駭侵者將可利用這一系列漏洞進行執行權限提升，甚至可以執行任意程式碼，並且竊取用戶

的 Android 手機通話內容及各種機敏資訊。

資安專家表示，雖然該公司已經推出修復程式，但由於採用此處理器的 Android 手機數量非常龐大，許多機種又屬於較老舊或較小規模廠商的產品，可能早已停止其手機作業系統的更新，因此將會有許多用戶的手機無法修補這些漏洞。

- CVE 編號：CVE-2021-0661 等
- 影響產品：各型採用該公司處理器的 Android 手機
- 解決方案：安裝各手機廠商推出之最新作業系統更新版（如有提供）

- 資料來源：
  1. Looking for vulnerabilities in MediaTek audio DSP
  2. Mediatek eavesdropping bug impacts 30% of all Android smartphones

2.7.2、資安專家發現可跳過 CVE-2021-34484 修補程式的 0-day 漏洞

資安專家發現一個影響所有 Windows 版本的 0-day 漏洞，可讓駭侵者藉以提升自身執行權限。

獨立資安專家 Abdelhamid Naceri 日前發現一個影響所有 Windows 版本的 0-day 漏洞，可以跳過 Microsoft 日前釋出的資安漏洞修補程式，讓駭侵者藉以提升自身執行權限。

在八月時 Microsoft 針對 CVE-2021-34484 推出了修補程式；該漏洞稱為「Windows 用戶檔案權限提升漏洞」，也是由同一位獨立資安研究人員 Abdelhamid Naceri 發現的；駭侵者可利用這個漏洞，來提升自我的執行權限。

Abdelhamid Naceri 最近發現 Microsoft 推出的修補程式並不完整，仍然含有可被跳過的漏洞，在某些條件下，駭侵者仍然可以利用這個漏洞來提升執行權限，接著發動進一步的駭侵攻擊。

Abdelhamid Naceri 將他的發現進一步發展成可用以發動攻擊的概念證明模擬程式，並上傳到 Github 上供資安從業人員進行研究。他指出，利用這個漏洞，駭侵者將可以取得系統權限；影響的範圍則為 Windows 所有的版本，包括 Windows 10、WIndows 11、Windows Server 2022 等。

不過其他資安專家在分析這個新發現的漏洞時，指出要利用此一漏洞發動攻擊，必須滿足某些條件；駭侵者必須先取得其他用戶的登入資訊，包括帳號與密碼，才能觸發此一漏洞，因此該 0-day 漏洞可能不會造成駭侵者大

規模濫用於攻擊活動。

Microsoft 也指出，該公司已經獲悉此漏洞的存在與其影響，將會在近期予以處理，以保護用戶的安全。。

- 影響產品：Windows 各版本，包括 Windows 10、Windows 11、Windows Server 2022。

- 資料來源：
  1. CVE-2021-34484 bypass as 0day (Abdelhamid Naceri @KLINIX5)
  2. All Windows versions impacted by new LPE zero-day vulnerability

2.7.3、Windows 10 最新 0-day 權限提升漏洞，已有非官方修補工具可用

一個近期發現，可讓駭侵者用以提升本地端執行權限的 Windows 10 0-day 漏洞，得到非官方的修補方案；Windows 用戶可套用此解決方案，以暫時避免遭駭侵者以此漏洞發動攻擊。

一個近期發現，可讓駭侵者用以提升本地端執行權限的 Windows 10 0-day 漏洞 CVE-2021-24084，在最近得到非官方的修補方案；Windows 用戶可套用此解決方案，以暫時避免遭駭侵者以此漏洞發動攻擊。

這個編號為 CVE-2021-24084 的 0-day 漏洞，發生在 Windows 10 版本 1890 與其後版本的「行動裝置管理服務」（ Mobile Device Management Service ）子系統內。先前微軟已經於本年二月推出資安修補軟體，但最近資安專家 Abdelhamid Naceri 於六月時發表研究報告，指出微軟推出的修補工具，並不能完全解決此問題，駭侵者仍可利用其他方式跳過安全修補，將自己的本地端執行權限提升到管理員等級。

雖然微軟在六月時就接獲相關通報，但直到最新的 2021 年 11 月 Patch Tuesday 資安修補包中，仍然未能就此漏洞進行完整修補。

不過，一個名為 0patch micropatching service 的非官方組織，日前針對這個 0-day 漏洞推出了非正式版的修補程式，適用於以下 Windows 10 版本：

- Windows 10 v21 H1 （ 32 與 64 位元版 ）；
- Windows 10 v20 H2 （ 32 與 64 位元版 ）；
- Windows 10 v2004 （ 32 與 64 位元版 ）；

- Windows 10 v1909（32 與 64 位元版）；
- Windows 10 v1903（32 與 64 位元版）；
- Windows 10 v1809（32 與 64 位元版）。

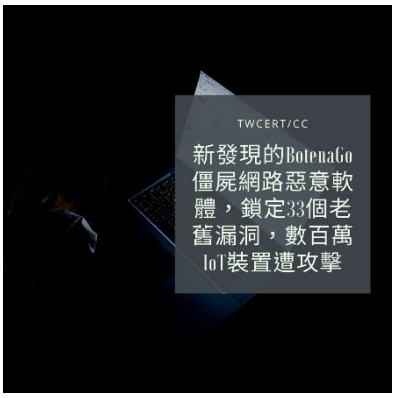
值得注意的是，這個非官方修補工具，暫不支援 Windows 10 21H2（即目前 Windows 10 的最新版本），另外 Windows 10 v1803 與 Windows Server 不包含此漏洞，因此無需套用。

資安專家建議 Windows 用戶可視情形，安裝此非官方修補程式，以避免遭到駭侵者利用此 0-day 漏洞發動攻擊。

- CVE 編號：CVE-2021-24084
- 影響產品：Windows 10 v21 H1（32 與 64 位元版）；Windows 10 v20 H2（32 與 64 位元版）；Windows 10 v2004（32 與 64 位元版）；Windows 10 v1909（32 與 64 位元版）；Windows 10 v1903（32 與 64 位元版）；Windows 10 v1809（32 與 64 位元版）。
- 解決方案：依 0patch 提供之步驟安裝更新檔即可。

- 資料來源：
  1. Fixing what’s really important.
  2. CVE-2021-24084 An unpatched information disclosure in Microsoft Windows
  3. Abdelhamid Naceri @KLINIX5

2.7.4、新發現的 BotenaGo 僵屍網路惡意軟體，鎖定 33 個老舊漏洞



資安專家發現一個新的僵屍網路惡意軟體 BotenaGo，利用 33 個已知的老舊資安漏洞，鎖定數百萬台 IoT 設備發動攻擊。

大型電信業者 AT&T 旗下的資安專家，近日發現一個新的僵屍網路惡意軟體 BotenaGo，利用 33 個已知但並未全面獲得修補的老舊資安漏洞，鎖定數百萬台 IoT 設備發動攻擊。

資安專家指出，BotenaGo 主要鎖定的對象，包括各種網路路由器、數據機（Modem）、網路儲存裝置（Network Attached Storage，NAS）等，其中有一些裝置是由台灣廠商生產製造。

BotenaGo 主要利用的漏洞編號，和存有這些漏洞的裝置分別如下：

- CVE-2015-2051、CVE-2020-9377、CVE-2016-11021： D-Link 路由器；
- CVE-2016-1555、CVE-2017-6077、CVE-2016-6277、CVE-2017-6334：Netgear 裝置；
- CVE-2019-19824：採用 Realtek SDK 的各廠牌路由器
- CVE-2017-18368、CVE-2020-9054： Zyxel 路由器與 NAS 裝置；
- CVE-2020-10987： Tenda 產品；
- CVE-2014-2321: ZTE 數據機；
- CVE-2020-8958: Guangzhou 1GE 光纖網路終端單元。

資安專家指出，這些漏洞大多屬於相當老舊的漏洞，但已經售出的各式 IoT 裝置，比軟體系統更不容易獲得大規模資安更新，因此市面上仍有大量未曾更新的裝置，成為這類駭侵攻擊的目標。

- 資料來源：
  1. AT&T Alien Labs finds new Golang malware (BotenaGo) targeting millions of routers and IoT devices
  2. BotenaGo botnet targets millions of IoT devices with 33 exploits

2.7.5、600 萬台英國 Sky 寬頻用戶端路由器的資安漏洞，修復期間長達 17 個月

英國 Sky 寬頻服務提供用戶使用的 600 萬台路由器，其中存有的資安漏洞，在 2020 年年底發現後，花了長達 17 個月才大致完成修補工作。

英國 Sky 寬頻服務（Sky Broadband）提供用戶使用的 600 萬台路由器，其中存有幾個資安漏洞，在 2020 年年底由資安廠商發現並提報後，Sky Broadband 並未立即處理，直到 2021 年 10 月底才完成 99% 受影響裝置的資安修補工作，用戶曝險期間長達 17 個月之久。

該漏洞是個「DNS 重新綁定」（DNS Rebinding）漏洞。駭侵者可以攻擊所有未曾變更預設管理介面登入帳密的 Sky Broadband 路由器，引誘用戶進入一個含有惡意程式碼的網站中，藉以利用此漏洞，入侵用戶內部網路中的各項裝置，包括竊取資料，或是攻擊用戶內網中的其他設備。

該漏洞是由資安廠商 Pen Test Partners 於 2020 年 5 月 11 日發出資安通報，並立即通報給 Sky Broadband；當時 Sky Broadband 表示已獲悉該漏洞的存在，並計畫於 2020 年 11 月時修復此漏洞。

然而該公司卻因為忙於 COVID-19 肺炎疫情之下，英國各地封城造成的寬頻服務需求暴增，因而沒有及時於計畫明定的 2020 年 11 月推送更新修補程式。Sky Broadband 過了幾個月後才推出修補程式，直到 2021 年 5 月時，修補完成比例僅有 50%。

資安廠商 Pen Test Partners 發現 Sky Broadband 怠於進行漏洞修補，於是在今年 8 月時對媒體公開其發現，希望透過輿論的力量，來壓迫 Sky

Broadband 加速漏洞更新腳步。最後在本年 10 月 22 日時，Sky Broadband 才對外表示已經更新了 99% 存有此漏洞的裝置。

- 資料來源：
  1. SkyFail. 6 million routers left exposed
  2. Six million Sky routers exposed to takeover attacks for 17 months

2.7.6、微軟推出 2021 年 11 月 Patch Tuesday 例行資安更新包

Microsoft 推出 2021 年 11 月的例行性軟體更新包 Patch Tuesday，各種 Microsoft 軟體系統的使用者與管理者，應立即套用相關更新。

Microsoft 推出 2021 年 11 月的例行性軟體更新包 Patch Tuesday，一共修復多達 55 個資安漏洞，更包括 6 個 0-day 漏洞。

以漏洞的嚴重程度來說，在這 55 個此次獲得修補的漏洞中，共有 6 個漏洞列為嚴重（Critical）等級，其於 49 個列為重要（Important）等級。若以漏洞類型來分，各類資安漏洞的數量如下：

- 權限提升漏洞：20 個；
- 資安防護功能跳過漏洞：2 個；
- 遠端執行任意程式碼漏洞：15 個；
- 資訊洩露漏洞：10 個；
- 服務阻斷漏洞：3 個；
- 假冒詐騙漏洞：4 個。

在這 55 個資安漏洞中，還包括 6 個 0-day 漏洞，需要立即修補；其中有兩個分別存於 Microsoft Exchange Server 和 Microsoft Excel 的漏洞，已遭駭侵團體大規模予以濫用，分別是：

- CVE-2021-42292：存於 Microsoft Excel 的資安防護功能跳過漏洞；

- CVE-2021-42321：存於 Microsoft Exchange Server 的遠端執行任意程式碼漏洞。

另外 4 個 0-day 漏洞中，有 2 個是存於 Windows Remote Desktop Protocol (RDP) 的資訊洩露漏洞，另 2 個是存於 3D Viewer 的遠端執行任意程式碼漏洞。這 4 個漏洞目前尚未傳出遭到駭侵者大規模用於攻擊活動的情報。

資安專家呼籲，各種 Microsoft 軟體系統的使用者與管理者，應立即套用相關更新，以降低遭到駭侵者利用已知而未修補漏洞發動攻擊的風險。

- 資料來源：
  1. November 2021 Security Updates
  2. Microsoft Patch Tuesday, November 2021 Edition
  3. Microsoft November 2021 Patch Tuesday fixes 6 zero-days, 55 flaws

第 3 章、 資安研討會及活動

零信任資安講堂	
活動時間	**10/12(二)~12/14(二)**
活動地點	**線上**
活動網站	**https://zerotrust.ithome.com.tw/index.html**
活動概要	 **主辦單位：iThome** 一起迎向未來十年資安顯學：Zero Trust 零信任資安 面對越來越險峻的網軍破壞攻擊，以及網路犯罪組織肆無忌憚、層出不窮的勒索惡行，企業組織必須改變傳統的資安防禦思惟，才能扭轉長久以來攻防不對稱的劣勢。該如何轉變呢？答案就在未來十年的資安顯學：零信任資安架構（Zero Trust Architecture）。 零信任資安趨勢的重要性，從今年 5 月初 2021 CYBERSEC 臺灣資安大會的主題「TRUST: redefined 信任重構」，即可窺之一二。緊接著，美國總統拜登在 5 月中簽署網路安全強化指令，直接要求聯邦政府機構翻遵循 NIST SP 800-207 零 a 信任資安架構準則，限時在 2024 年前轉換至現代化的零信任資安架構，以抵禦日益強大且足以動搖國家安全的網路攻擊。此舉更加證實政府與企業採納零信任資安的必要性與迫切性。無獨有偶，近期英國國家資安中心 NCSC 也發布零信任資安架構設計指南，鼓勵政府機構與民間企業採納零信任資安。 在歐美先進國家紛紛邁向現代化零信任資安架構的風潮下，零信任資安將是

	未來十年、甚至廿年的資安顯學。因此，繼 CYBERSEC 2021 臺灣資安大會揭開零信任資安序幕後，iThome 緊接著成立「零信任資安學堂」主題專區，匯集最新的零信任資安趨勢與學習資源， 並推出零信任資安講堂 Webinar，以最專業、最強大的講師陣容，徹底解析零信任資安的觀念、準則、設計方法，以及打造零信任架構的最新技術。講堂首季內容豐富，陣容強打，錯過可惜，請立即以下方連結報名。 收看方式：請於首播前上線報名，待主辦單位確認您的報名資料後，將於活動前夕提供線上專屬收視連結，請於開播前登入以利準時參與課程。 適合對象 ：企業 IT、企業 MIS 及資訊相關同仁。 連絡洽詢 ：02-2562-2880 #3631 簡小姐 （ 週一至週五，上午 10:30 ~ 12:00，下午 2:00 ~ 5:00 ） 11/30（二） 14:00 - 14:30 從紅隊角度看零信任資安 11/30（二） 14:30 - 15:10 NIST 零信任架構的網路安全策略之旅 12/07（二） 14:00 - 14:30 打通導入零信任資安架構的關鍵 12/07（二） 14:30 - 15:10 以軟體定義防護基礎，落實零信任安全設計 12/14（二） 14:00 - 14:30 零信任架構帶給企業資安的機會與挑戰 12/14（二） 14:30 - 15:10 新型態遠端辦公大挑戰，如何建構「零信任」

2021 FORTINET 數位 x 資安轉型論壇【資安嘉年華】	
活動時間	**2021 年 12 月 15 日 8:30~17:30**
活動地點	**華山 1914 文化創意產業園區（東 ABC 館）**
活動網站	**https://m.fortinet.com.tw/site/2021-security-carnival/**
活動概要	 **主辦單位：FORTINET** 【活動介紹】 2021 FORTINET 數位 x 資安轉型論壇【資安嘉年華】 為您實現足以信賴的數位世界 Digital Security, everywhere you need it 疫情所帶來的改變，並非絕對的負面。如同許多企業在這段時間發現了遠距辦公對於員工和企業本身的益處，而決定在生活逐漸恢復正常的現況下，持續採用混合辦公的模式來進行業務的營運。這意味著，多數的企業員工將可能在任何地方從事工作。然而相對的，這也讓企業延展出更多新的網路邊緣需要進行安全防護。令人擔憂的是，當企業加速數位轉型與邁向多雲服務的同時，資安需要覆蓋的攻擊面也爆發性增加。網路環境的日益複雜，讓資安人員面臨重大挑戰。 誠摯地邀請所有資安人員參與 Fortinet 2021 年度盛會「資安嘉年華」。我們將在會中探討： ➢ 從 CEO 觀點看資安與供應鏈資安發展趨勢 ➢ 如何更細緻地進行用戶和設備存取控管 ➢ 如何著重端點持續性的安全檢測與響應 ➢ 如何防止進階持續性威脅與勒索病毒攻擊

	我們相信，無論在網內或網外，企業需要更細緻地進行用戶和設備存取控管，尤其是對於外部的應用服務。此外，企業也必須著重端點持續性的安全檢測與響應，才能真正安全地讓企業網路延展到遠端工作環境，實現得以隨處辦公（Work From Anywhere）的需求。 而 Fortinet 的安全織網 Security Fabric，是一個全方位、整合協作且能夠實現自動化的網路安全防護架構，不僅保護您數位轉型、數位創新的使用者體驗、防止進階網路威脅與攻擊，更能簡便有效地達到網路安全監看和控管，在資安人才短缺的情況下，依然為您實現足以信賴的數位世界。 豐富精彩的內容，將在一日內完整提供於您。誠摯地邀請您參與我們的活動，相信您也不會想錯過。 【受邀對象】 本次活動專爲負責以下領域的工程師、專業人士、顧問和部門負責人而設：IT 網路與安全 / 資訊安全中心 / 資料中心營運 / 數據安全營運 / IT 稽核與風險管理 報名截止日：12/6 (一) 17:00《視報名情況將可能提前截止報名》 活動方式：預先報名，現場核對身份後免費入場《主辦單位保留資格審核權》

為企業數位轉型打造高安全、高可用、高效能的網路環境	
活動時間	**2021/12/22 14:40 ~ 15:10**
活動地點	**線上**
活動網站	**https://webinar.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 活動時間：2021/12/22 14:40 ~ 15:10 為企業數位轉型打造高安全、高可用、高效能的網路環境 隨著超過 90% 的互聯網流量加密，隱藏在加密流量中的惡意軟體攻擊急劇增加，企業必須立即採取行動來遏止攻擊。 近年來 DDoS 攻擊的強度、頻率和複雜度不斷增加，而企業使用的大多數防禦技術和方法都難以跟上當今 DDoS 攻擊的演進和持續性，企業必需採取新世代的方法來解決 IoT 物聯網攻擊日益嚴重的威脅。 陳志緯 / A10 Networks 台灣區技術總監

預見未來-當 AI 防禦遇上 AI 攻擊-資安現況與未來趨勢	
活動時間	**2022-01-27**
活動地點	**工研院台北館前學習中心**
活動網站	**https://college.itri.org.tw/all-events-2/C1B48809-9C42-430A-B6E5-E6FB94017207.html?utm_medium=crssearch&utm_source=college**
活動概要	 **主辦單位：工研院產業學院** 聯絡資訊：溫郁佳/03-5743864 報名截止日：2022-01-25 課程介紹：透過資訊安全現況及未來趨勢分享、透過常見 AI 攻擊、防護手法、自駕車資安事件等案例，讓學員了解資安策略思維與實務作法。 課程特色/目標：透過各領域資安案例解析，讓學員熟悉資安產業發展現況與 AI 在資安攻擊與防護上之應用趨勢。 課程對象：資安管理人員、資安工程師、資安研究員 課程大綱 全球疫情下的黑色產業鏈發展趨勢 AI 進行網路犯罪(以子之矛，攻子之盾)AI 攻擊手法，插入噪音就能破壞語音辨識系統 AI 進化超 AI 智能家電安全性實務案例分析 智能住宅安全性實務案例分析 車聯網安全性實務案例分析 穿戴式裝置安全性實務案例分析 車聯網入侵案例分析 集科技與智慧，超乎你想像的未來車 AI 人工智慧將主宰未來汽車產業的發展 L3 級別自動駕駛技術介紹 5G 技術(車聯網應用)介紹 電子外後視鏡介紹 上線控剎車介紹 平視顯示器（HUD）介紹 輪轂電機介紹 注意力輔助系統介紹 超級鎂介紹 地下數據挖掘介紹 電動車無線充電介紹 AI 車聯網安全主動防護技

	術(ACC、車道偏移輔助) 報名資訊 主辦單位：工研院產業學院 舉辦地點：工研院產業學院(台北實際地點以上課通知為準)、使用 Webex 軟體數位同步 舉辦日期：110/1/27 (三)9:30~16:30（6 小時） 課程費用：訂價：每人 $5,500 元、早鳥優惠:4,800 元 開課 14 天前或同一公司三人(含)以上報名：每人$ 4,500 元 同步數位 (本同步數位課程無補課機制) 報名方式：線上報名或以 Mail 方式寄至 Alisa.wen@itri.org.tw 課程洽詢：Alisa.wen@itri.org.tw；溫小姐 專線：03-5743864

第 4 章、 2021 年 11 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。

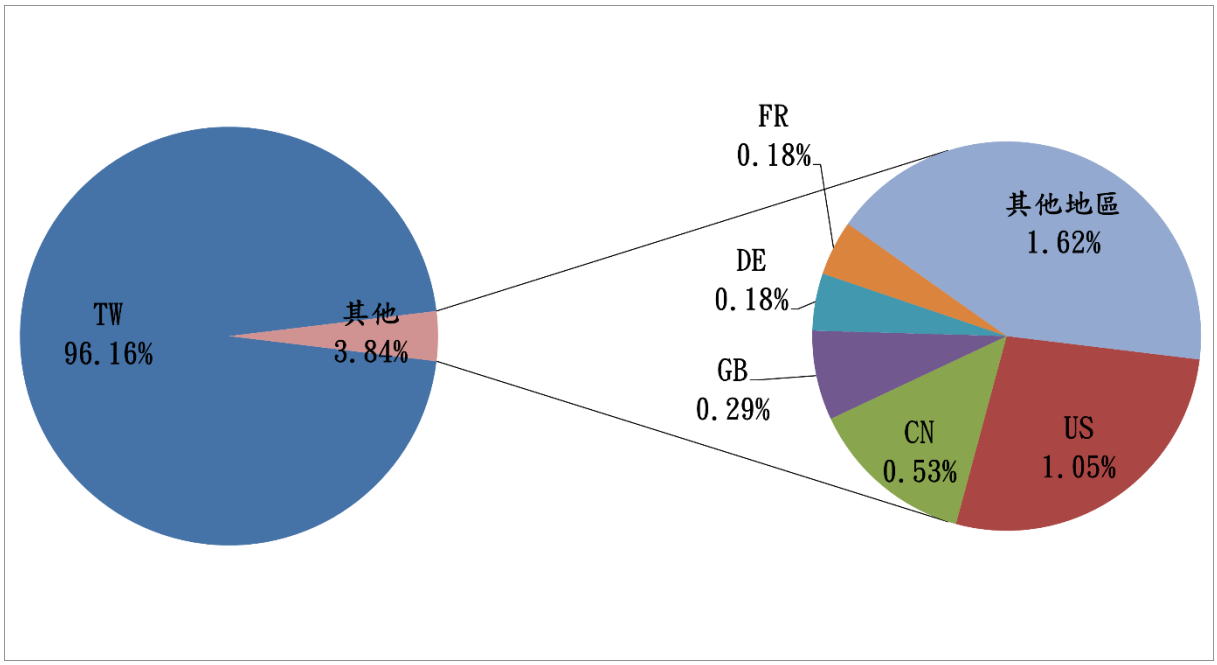


圖 1、分享地區統計圖

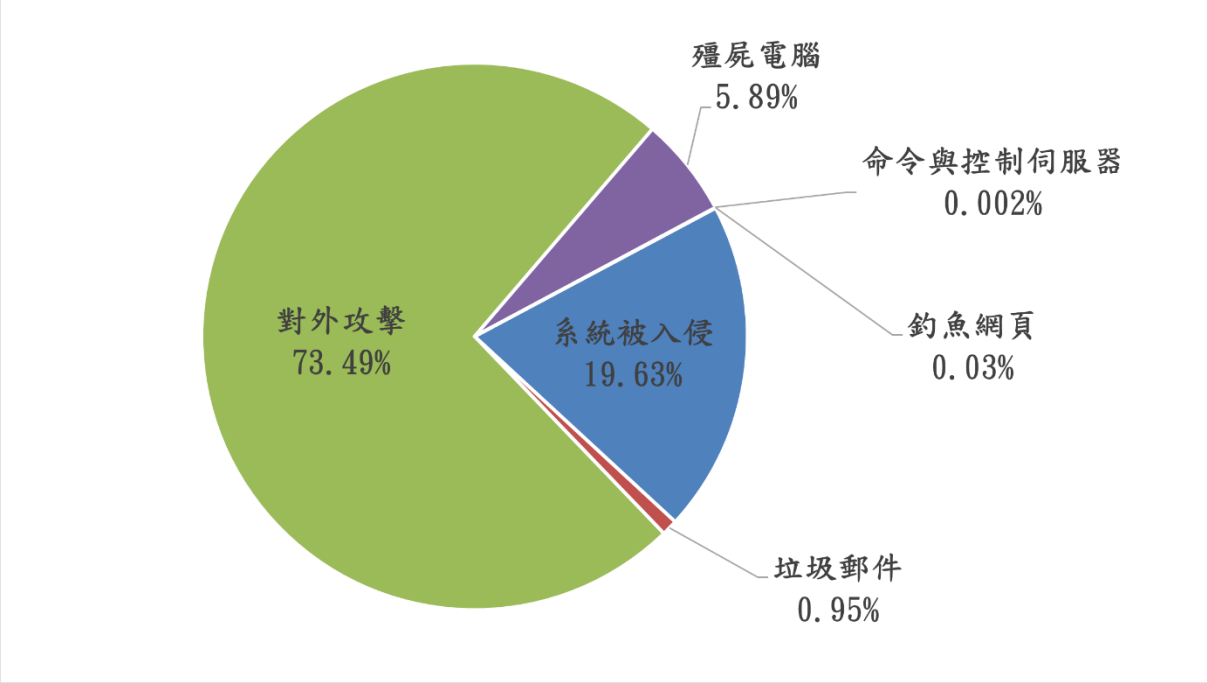

殭屍電腦
5.89%
命令與控制伺服器
0.002%
釣魚網頁
0.03%
系統被入侵
19.63%
對外攻擊
73.49%
垃圾郵件
0.95%

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 12 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**