TWCERT/CC 資安情資電子報

2021 年 5 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、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 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

OnlyFans 數百名創作者的影片，遭駭侵者分享於 Google Drive

資安專家發現訂閱制內容網站 OnlyFans 上多名成人內容創作者的影片，遭不明駭侵者分享到 Google Drive 上。

資安廠商 BackChannel 旗下的資安專家，近日發現訂閱制內容網站 OnlyFans 上有數百名成人內容創作者，其創作的訂閱者專屬成人影片，遭不明駭侵者分享到 Google Drive 上。

這名資安專家是在一個駭侵相關論壇上，發現一名身分不明的駭侵者，在論壇上張貼了一個 Google Drive 內容共享連結，內含數百名 OnlyFans 上的成人內容創作者拍攝，只供付費訂閱者觀看的大量影片內容。

據資安專家指出，這批被外洩的影片屬於 279 個 OnlyFans 帳號所發布，整個資料量高達 10 GB，內含大量成人內容影片和照片；從檔案日期可得知，大多數流出的影片和相片是在 2020 年 10 月左右上傳的。

資安專家表示，訂閱者往往會自行分享自己付費訂閱的影片等內容，以供親朋好友觀看，但流出的量相當有限；這次內容外洩的數量和波及人數十分龐大；很可能是多個駭侵者把自己搜刮到的內容都放在同一處，或是某個駭侵者掌握了多個資料外洩的來源。

值得注意的是，用來放置這些流出內容的 Google Drive 空間，其帳號屬於舊金山市立學院所有；資安廠商 BackChannel 已經去函敦促該學院自 Google Drive 中移除這些資料。

另外，BackChannel 也特別製作一個查詢工具網站，供 OnlyFans 創作者輸入自己的使用者名稱，查詢看看自己的影片是否也在流出檔案之列。

- 資料來源：
  1. Adult content from hundreds of OnlyFans creators leaked online
  2. Hundreds of OnlyFans Creators had Their Adult Content Published Online
  3. Security Disclosure: hundreds of OnlyFans users' content discovered on Google Drive

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、資安廠商發表 2021 年第一季各大品牌遭冒名發動釣魚攻擊排行榜

資安廠商近期公布各大品牌遭駭侵者用以進行釣魚攻擊的全球統計報告，其中有 39% 是資訊或科技相關品牌。

資安廠商 Check Point 近期發表研究報告，公布各大品牌遭駭侵者冒名用以進行釣魚攻擊的全球性統計報告；其中有 39% 是資訊或科技相關品牌。

這份報告統計 2021 年前三個月，各種釣魚郵件駭侵攻擊假冒的品牌，與在全球發動的相關攻擊次數；報告指出，知名科技巨頭仍為釣魚攻擊者最喜歡假冒的品牌。這些攻擊行動中有高達 65%，都是假借科技巨頭如 Microsoft、Google、Roblox、Amazon、Apple、Dropbox 等，企圖騙取受害者的登入資訊或其他機敏資料。

報告也說，在 2021 年第一季中，有高達 39% 的釣魚攻擊是假冒 Microsoft 來進行的，但總攻擊次數和去年第四季相比微幅下降；2020 年第四季冒用 Microsoft 品牌發動的釣魚攻擊，其占比高達 43%。

而在非科技品牌方面，包括全球運輸業、大型零售通路、金融業者等等也是常被釣魚攻擊者冒名發動攻擊的主要對象。

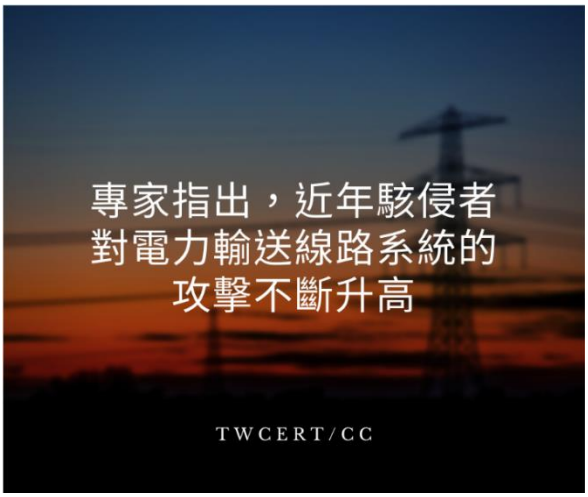
在 Check Point 的報告中，排名前十名最常被冒名的品牌，及其攻擊次數比例，分別為：

- Microsoft（39%）
- DHL（18%）
- Google（9%）
- Roblox（6%）
- Amazon（5%）
- Wells Fargo（4%）
- Chase（2%）
- LinkedIn（2%）
- Apple（2%）
- Dropbox（2%）

這份報告也指出，雖然科技業者在近年來， 一直都是釣魚郵件駭侵者最喜歡冒名的對象，第二名則是運輸業，但今年觀察到銀行業者的被冒名比例快速增加，美國兩家知名的銀行富國銀行（Wells Fargo）和大通銀行（Chase）被冒名比例來到前十名，是過去沒有過的現象；這可能和疫情造成的數位金融服務使用率快速成長有關。

- 資料來源：
  1. (Check Point Blog)Microsoft Continues to be Most Imitated Brand for Phishing Attempts in Q1 2021
  2. Microsoft Continues to be Most Imitated Brand for Phishing Attempts in Q1 2021

2.1.2、專家指出，近年駭侵者對電力輸送線路系統的攻擊不斷升高



專家指出，近年來美國輸電線路與相關基礎建設，遭到駭侵者鎖定攻擊的情形不斷升高，特別是在去年疫情發生後。

北美電力相關專家日前在一場針對供電系統資安問題的研討會中指出，近年來美國輸電線路與相關基礎建設，遭到駭侵者鎖定攻擊的情形不斷升高，特別是在去年疫情發生後。

非營利的「北美電力可靠度公司」（North American Electric Reliability Corporation, NERC）資深副總裁 Manny Cencel，近日在一場名 GridSecCon 2021 的研討會上指出，「雖然確保輸電線路和相關基礎設施的安全性，一直是業者的首要任務，但在過去一年到一年半以來，情況有非常劇烈的變化，而且前所未見。」

Manny Cancel 指出，不論駭侵者是否有特定國家勢力背景，近來的攻擊者都有能力癱瘓整個供電系統和基礎設施；特別是在疫情爆發之後，由於大量員工透過網路遠距工作，更給駭侵者可乘之機，利用其中的弱點來攻擊電力業者。

Manny Cancel 說，在去年年底爆發的 SolarWinds 駭侵攻擊事件，雖然受害的私部門單位中，有不少屬於供電產業的成員，但 Cancel 也指出，電力產業似乎並非這波攻擊事件中的主要目標，因為雖然有 25% 的相關產業業者下載了遭到植入惡意軟體的 SolarWinds 程式碼，但主要的輸電線路尚未發生

過大規模斷電事件。

Cancel 也說，由於供電業者和政府資安單位緊密合作，對於各種監聽或惡意軟體攻擊的情報交換和防範措施得宜，因此降低了遭到攻擊的機會和可能造成的損害。

- 資料來源：
  1. Hundreds of electric utilities downloaded SolarWinds backdoor, regulator says
  2. Experts see 'unprecedented' increase in hackers targeting electric grid

2.2、新興應用資安

新型態惡意軟體透過 Telegram 聊天室散布假破解工具，以竊取加密貨幣

資安廠商日前發表研究報告，指出一個名為 HackBoss，專門竊取加密貨幣的惡意軟體，目前正透過 Telegram 散布全球。

資安廠商 Avast 日前發表研究報告，指出現在一個名為 HackBoss，專門竊取各種加密貨幣的惡意軟體，目前正透過 Telegram 散布全球，且已經造成鉅額損失。

Avast 發表的最新研究報告說 HackBoss 是個非常簡單但十分有效的惡意軟體，目前可能已經竊走高達 560,000 美元等值的加密貨幣。

HackBoss 的開發者在 Telegram 開設一個同樣名為 Hack Boss 的聊天室，以「提供最佳駭客工具」為號召，號稱提供各種可供用戶下載，以破解銀行帳號、社群平台帳號、各種加密貨幣錢包、禮品卡密碼產生器、商用軟體註冊碼產生器等破解工具，但實際上釋出的工具，都只是假冒成這些破解工具，實際上卻是用來竊取加密貨幣的惡意軟體。

這個聊天室目前約有 2,500 名成員加入，每個月通常會有 7 篇新的貼文，每次都會提供一個下載連結，指向偽裝成破解工具的惡意軟體；而其惡意軟體的運作方式非常簡單，就是監控系統剪貼簿，一旦出現了可能是加密貨幣錢包的位址資訊，就把它刪去，並且以駭侵者自己的加密貨幣錢包取而

代之。當受害者需要把加密貨幣轉到其他錢包地址時，用這種方法即可將匯款攔截下來，並且改匯到駭侵者擁有的加密貨幣錢包之中。

Hack Boss 的 Telegram 頻道設立於 2018 年 11 月，除了 Telegram 外，還設立了官方部落格和 YouTube 頻道，甚至購買廣告宣傳，以誘使更多用戶下載這些假的破解工具。

HackBoss 可以竊取的加密貨幣種類超過 100 種以上，但主要行竊得手的加密貨幣種類，則以比特幣、以太幣、萊特幣、狗狗幣（Dogecoin）為主，總金額相當於 56 萬美元以上。

- 資料來源：
  1. HackBoss: A cryptocurrency-stealing malware distributed through Telegram
  2. HackBoss malware poses as hacker tools on Telegram to steal digital coins

2.3、國際政府組織資安資訊

2.3.1、美國國家安全局發表 4 個最新 Microsoft Exchange Server 嚴重漏洞

美國國家安全局最近發布 4 個 Microsoft Exchange Server 嚴重資安漏洞，全部可以導致駭侵者遠端執行任意程式碼；用戶應立即更新以修補漏洞。

美國國家安全局（National Security Agency, NSA）最近發布 4 個 Microsoft Exchange Server 嚴重資安漏洞，全部可以導致駭侵者遠端執行任意程式碼；目前 Microsoft 已經推出資安更新，用戶應立即更新以修補漏洞。

NSA 指出，這四個資安漏洞，都針對機構內架設的 Microsoft Exchange Server，影響版本從 2013 到 2019，含蓋範圍很大。目前尚未有證據指出這些漏洞已遭大規模用於駭侵攻擊，但微軟指出駭侵者很快就會利用這些漏洞，發展出攻擊工具與手法。

這 4 個漏洞的 CVE 編號分別是 CVE-2021-28480、CVE-2021-28481、CVE-2021-28482、CVE-2021-28483，都能夠讓駭侵者直接遠端執行任意程式碼；其中有兩個還能跳過登入驗證程序，讓駭侵者取得足夠的執行權限。

這 4 個漏洞的 CVSS 危險程度評級，最低分的是 8.8/10 分，最高者高達 9.8/10 分；全都屬於「嚴重」等級漏洞。

另一個主管美國國家資安事務的網路安全暨基礎設施安全局（Cybersecirity and Infrastructure Security Agency, CISA），也針對這 4 個新發現的資安漏洞發布命令，要求美國聯邦政府旗下各單位，必須在 2021 年 4 月 16 日上午 12:01 分之前，安裝 Microsoft 提供的更新軟體。

雖然目前還沒有傳出利用這些漏洞發動的攻擊事件，但 CISA 認為駭侵者將會利用逆向工程技術，分析微軟推出的修補軟體，開發出攻擊程式，並針對尚未更新的 Microsoft Exchange Server 發動攻擊。

- 資料來源：
  1. Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
  2. NSA discovers critical Exchange Server vulnerabilities, patch now
  3. CISA gives federal agencies until Friday to patch Exchange servers

2.3.2、新加坡 SingCERT 警告，提防駭侵者利用 Facebook 外洩個資進行釣魚攻擊

針對日前發生的 Facebook 5.33 億用戶個資外洩事件，新加坡政府旗下的資安事件主管機關發出警示，應對接下來可能發生的釣魚攻擊提高警覺。

針對日前發生的 Facebook 5.33 億用戶個資外洩事件，新加坡政府旗下的資安事件主管機關 SingCERT（Singapore Computer Emergency Response Team）發出警示，用戶應對接下來可能發生的各種釣魚攻擊提高警覺，並做好防範措施。

SingCERT 指出，在這次事件中，有 300 萬名以上的新加坡 Facebook 用戶個資也在外洩名單之列；雖然 Facebook 表示造成資料被竊的錯誤，早在 2009 年八月即已修正，但由於這批資料含有許多用戶的連絡資訊，如手機門號、姓名、Email、出生年月日等，很可能遭到駭侵者用以發動進一步的釣魚攻擊，例如：

- 駭侵者可能會利用這些資訊，假扮成他人身分，寄送內含惡意連結的釣魚訊息給用戶；訊息內容可能會是假稱用戶帳號的登入密碼需要重置，或是要求轉帳、其他服務的單次有效密碼（OTP）等等；
- 駭侵者也可能利用這些資訊駭侵用戶在其他服務上的登入資訊，例如重置用戶原本的密碼以盜取帳號登入權，或是假冒用戶本人申請補發銀行金融卡等等；
- 駭侵者也可能利用這些資料，假冒用戶身分購買商品或服務並且盜領、盜

用。

SingCERT 同時敦促用戶做好各種資安防護工作，包括：

- 對於各種可疑的釣魚攻擊提高警覺，在點按 Email 或訊息內的連結時，先檢查網址是否沒有問題，特別是來自不明人士發送的 Email 或訊息；
- 如果可以的話，開啟登入通知功能，當有不明人士或不明裝置試圖登入你的帳號時，你會收到通知；如有二階段登入驗證功能（2FA），也應該啟用；
- 定期更換密碼，建議使用 12 個字元以上且英文、大小寫、數字與符號混合之密碼，同時避免在不同服務之間使用相同密碼；
- 在社群平台上勿分享過多個人機敏資訊，同時應檢視並調高平台上的隱私相關設定，加強個資保護。

- 資料來源：

1. Possible Phishing Campaigns Arising from Facebook's Data Leak

2.3.3、國際執法合作，迫使 Emotet 惡意軟體自我刪除

在國際執法單位共同合作下，自一月起利用緝獲的 Emotet 控制伺服器，逐步在遭感染的電腦系統上執行自我刪除。

在過去造成全球重大資安損害的惡意軟體 Emotet，近來在國際執法單位共同合作下，自一月起利用緝獲的 Emotet 控制伺服器，逐步在遭感染的電腦系統上執行自我刪除。

Emotet 這個惡意軟體，幕後的駭侵組織為「TA542」，又稱「木乃伊蜘蛛（Mummy Spider）」，是個二階段的惡意軟體；電腦系統感染 Emotet 後，會再從控制伺服器上下載安裝不同功能的惡意軟體模組，例如惡名昭彰的 Ryuk 勒贖軟體，便是 Emotet 上的一個模組。

這次的刪除行動，是由德國的聯邦警察署（Bundeskriminalamt）發動，該單位緝獲一批 Emotet 的控制伺服器後，利用這批控制伺服器，對已感染 Emotet 的電腦，發送一個 32 位元 EmotetLoader.dll 檔案，達成移除 Emotet 的任務

資安廠商 Malwarebytes 的資安專家，分析了德國警方發送的自我刪除程式碼後指出，發現這個移除程式做的事情非常簡單：刪除 Emotet 相關的 Windows 服務、移除會自動執行 Emotet 的 Windows 登錄檔中的相關機碼，接著結束執行程序。

據資安專業媒體 BleepingComputer 報導指出，一月時德國聯邦警察署就開始利用手中掌握的 Emotet 控制伺服器，推送自我移除模組；二月時美國司法部也證實，這項計畫中的移除行動，是由德國警方負責，並且與美國聯邦調查局（FBI）密切合作。

不過，美國司法部也指出，這波行動並無法移除其他非 Emotet 安裝的惡意軟體，僅能讓受害者中的 Emotet 模組停止運作，防止 Emotet 下載更多惡意軟體模組發動攻擊。

- 資料來源：
  1. Emotet malware nukes itself today from all infected computers worldwide
  2. #Emotet uninstall routine tested via date hack (system clock changed to sometime after April 25).
  3. Emotet botnet disrupted after global takedown operation

2.4、社群媒體資安近況

2.4.1、5.33 億名 Facebook 用戶個資遭公開免費取用

一批內含 5.33 億名 Facebook 用戶資料的檔案，日前被不明駭侵者免費公開在一個駭侵相關論壇上；其中含有近 78.5 萬名台灣用戶的個資。

一批內含 5.33 億名 Facebook 用戶資料的檔案，日前被不明駭侵者免費公開在一個駭侵相關論壇上，任何人皆可免費下載。這份檔案中含有多達 106 國 Facebook 用戶的多項個資，其中台灣用戶的個資約有近 78.5 萬名，也列在這批外洩資料中。

據美國科技媒體 Insider 報導，Facebook 發言人指出，這批資料很可能是利用 Facebook 在 2019 年間一個發生在「新增朋友」功能的漏洞而取得的；駭侵者可以利用該漏洞得知用戶登錄在 Facebook 的手機門號。資安專家指出，這次外洩的資料，很可能是駭侵者取得 Facebook 用戶手機門號後，以此為基礎，結合其他外洩的用戶個資拼湊而成的。

據資安科技媒體 BleepingComputer 報導，這批資料最先是在 2020 年六月時出現在相關駭侵討論區中，當時駭侵者以 30,000 美元的價格，試圖出售這批資料；駭侵者甚至還設立了一個私人 Telegram 頻道，有興趣購買資料的人，可以在 Telegram 頻道中輸入資料，機器人會根據輸入的資料，輸出一筆對應的完整資料，以供買方驗證之用。

資安專家說，隨著時間過去，駭侵者對資料的開價會日漸調低；可能是因為願意出錢買這批資料的人已經很少，駭侵者無利可圖，於是便免費「開放」這些外洩資料，以在駭侵者社群內博取名聲。

這批資料內含 106 個國家的 Facebook 用戶資訊，欄位包括用戶手機門號、姓名、Facebook ID、性別等；其中甚至包括 Facebook 三名創辦人 Mark Zuckerberg、Chris Hughes、Dustin Moskovitz 的個資在內。

以國別來看，這批資料中的埃及用戶人數最多，達近 4,500 萬人，其次是突尼西亞（近 3,953 萬人）、義大利（近 3,568 萬人）、美國（3,232 萬人）、沙烏地阿拉伯（2,880 萬人）、法國（1,985 萬人）、土耳其（1,964 萬人）、摩洛哥（1,894 萬人）、哥倫比亞（1,796 萬人）、伊拉克（1,771 萬人）。台灣用戶則有 734,807 人名列其中。

- 資料來源：
  1. Facebook Data on 533 Million Users Reemerges Online for Free
  2. 533 million Facebook users’ phone numbers leaked on hacker forum
  3. 533 million Facebook users' phone numbers and personal data have been leaked online

2.4.2、近五億名 LinkedIn 用戶個資，於駭侵者論壇上求售

繼 5.33 億名 Facebook 用戶個資在駭侵相關討論區遭免費公開後，LinkedIn 的近 5 億用戶個資，也被張貼到駭侵討論區中求售。

繼 5.33 億名 Facebook 用戶個資，在駭侵相關討論區遭免費公開後，全球最大的求職求才社群平台 LinkedIn 也有近 5 億用戶個資，被不明駭侵者張貼到駭侵討論區中求售。

資安專家發現在一個知名的駭侵者相關討論區中，有一篇貼文試圖販賣 5 億個以不明方法搜刮而來的 LinkedIn 用戶個資，欄位包括用戶的 LinkedIn ID、 Email 信箱、手機號碼、完整姓名、性別、LinkedIn 個人檔案連結、用戶在其他社群平台的個人檔案連結、工作職稱、經歷、履歷等資訊。

被放上駭侵討論區求售的檔案，一共分成四個；貼文者開價不低於四位數的金額；貼文者另外也釋放出一個含有 200 萬用戶個資料檔案，供有意購買者，以一個 LinkedIn 用戶以若干該討論區點數（約美金 2 元）的價格，用以驗證資料的正確性。

資安媒體 Cybernews 驗證部分資料後，證實不明駭侵者張貼的這批資料，確實是取自 LinkedIn，但目前無法確認貼文者是用什麼方法取得這些資料，也無法得知這些資料是在何時取得的。

雖然這批外洩資料含有相當多 LinkedIn 用戶的個資欄位，但並不包括 LinkedIn 用戶的登入資訊和金流支付資訊；資安專家警告，即使這些資料無法直接用於竊取用戶登入權限，但在駭侵者手中，仍足以用來發動進一步的攻擊，例如魚叉式釣魚攻擊、假冒真實用戶騙取更多資訊的社交工程攻擊，或是用以進行暴力試誤登入等。

- 資料來源：
  1. Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof
  2. Half a billion LinkedIn users have scraped data sold online

2.5、行動裝置資安訊息

2.5.1、超過 50 萬台手機，遭 Joker 惡意軟體感染

超過 50 萬台手機因為下載來自官方應用程式商店 AppGallery 中的 App，遭植入 Joker 惡意軟體，在用戶不知情的情形下訂閱高額行動服務。

資安廠商 Doctor Web 日前發表研究報告指出，共有超過 50 萬台華為手機，因為下載來自官方應用程式商店中的 App，遭植入 Joker 惡意軟體，在用戶不知情的情形下訂閱高額行動服務，同時進行其他駭侵攻擊行為。

研究人員指出，在其官方 Android 應用程式商店 AppGallery 中，一共發現 10 個看起來無害的 App，含有 Joker 惡意軟體程式碼，會私自和駭侵控制伺服器連線，取得多種設定，以及額外的惡意軟體程式模組。

這些埋有惡意程式碼的 App，種類相當多樣，從虛擬鍵盤、攝影工具、Android 桌面管理程式（Launcher）、即時通訊軟體、貼紙軟體、相片調色軟體和手機遊戲等等。一旦安裝這些 App，就會在用戶不知情的狀況下，為用戶訂購高價的線上服務。

這些 App 還會攔截服務訂購時傳送過來的驗證用簡訊，並完成手機簡訊驗證，不讓用戶發現；App 會連上駭侵者架設的控制伺服器，取得工作清單、高價服務的訂閱用網址，以及會模擬用戶操作行為的 JavaScript 程式碼。

Doctor Web 指出，上述的大多數惡意軟體，都來自單一開發者 Shanxi Kuailaipai Network Technology Co., Ltd.；這十支 App 的總共下載次數總合達 538,000 次。

Doctor Web 也說，不只是在 AppGallery 官方應用程式商店中找到內含 Joker 惡意軟體的 App，在 Google Play 官方應用程式商店的其他 App 中，也發現過這類惡意 App。

- 資料來源：
  1. Android.Joker on the Huawei AppGallery - Indicators of compromise
  2. Malware found on the AppGallery app store for the first time
  3. Joker malware infects over 500,000 Huawei Android devices

2.5.2、iOS 兒童遊戲內藏詐騙賭博惡意程式碼

一名行動應用程式開發者發現一支名為 Jungle Run 的 iOS 兒童遊戲軟體，實際上是一個加密貨幣賭場，用以騙取用戶的財物。

行動應用程式開發者 Kosta Elefheriou，近期發現一支名為 Jungle Run 的 iOS 兒童遊戲軟體，表面上看起來無，實際上卻是一個加密貨幣賭場，用以騙取用戶的財物。

這名位於美國的開發者發現，Jungle Run 平時看起來是一支設計很平凡的遊戲軟體，但他只要將手機的連線以 VPN 改為使用土耳其、哈薩克或義大利等國的境內 IP 連線，這支 App 就會搖身一變，變成一個以加密貨幣進行賭博遊戲的線上賭場。

當使用 VPN 切換到土耳其境內 IP 連線時，這支詐騙 App 甚至會播放詐騙廣告，假稱得到 CNN 土耳其語版新聞採訪推薦。

資安專家表示，把詐騙賭場包裝在看起來無害的 App 中，限定某些國家的連線才能開啟，這種手法前所未見，甚至可以騙過以審核嚴格聞名的 Apple 官方應用程式商店 App Store；這表示簡單的人類創意就可以騙倒機器學習演算法，所以釣魚詐騙攻擊和社交工程，永遠都比複雜先進的惡意軟體更加有效。

Elefheriou 指出，Jungle Run 的開發者除了這支遊戲外，也在 Apple 官方的應用程式商店上架另一支同樣含有詐騙賭場「功能」的應用程 Magical Forest Puzzle。

目前 Apple 已經將這兩支 App 下架移除，但顯然這兩支 App 的上架已有一段時間；而在 App Store 中的用戶評價欄中，已有用戶抱怨被這支 App 騙走錢財。

這類詐騙行動應用程式在過去就經常出現在 Apple 和 Google 的官方應用程式商店中，除了像本例的賭場詐騙外，諸如詐騙廣告點擊、資料竊取與監聽、背景挖礦、訂購高價服務、盜取登入資訊等惡意攻擊手法，可說層出不窮；用戶下載安裝任何軟體，都需提高警覺，先檢閱其他用戶的評價內容，以免上當。

- 資料來源：
  1. This iOS Game Secretly Turns Into a Gambling App
  2. iOS Kids Game Morphs into Underground Crypto Casino

2.5.3、德國研究人員發現 Apple AirDrop 存有個資外洩隱患

德國研究人員近期發表針對 Apple AirDrop 無線傳輸協定安全性的研究報告，指出 AirDrop 在進行通訊交握期間，可能會洩露用戶相關個資。

德國達姆施塔特工業大學（Technische Universität Darmstadt）資訊科學系的研究人員，近期發表一篇報告，針對 Apple AirDrop 無線傳輸協定安全性進行研究；報告指出 AirDrop 在進行通訊交握期間，可能會洩露用戶相關個資。

達姆施塔特工業大學的兩組研究人員，在研究分析 AirDrop 的傳輸流程時，發現 AirDrop 預設的傳輸對象，必須同時存在於傳輸兩者的手機通訊錄內；為了驗證所需，在檔案傳輸開始之前的交握（handshaking）程序中，AirDrop 會互相傳送經過雜湊加密運算的用戶手機門號和 Email 地址，兩者相符後才會開始傳輸檔案內容。

研究人員指出，由於 Apple 在 AirDrop 交握流程中使用的雜湊演算法不夠完整，因此攻擊者只要與遭攻擊者距離夠近，處於 Wi-Fi 無線網路訊號範圍內，攻擊者可以使用一台電腦來發動交握程序，進而利用諸如暴力試誤法等方式，破解雜湊加密並還原出被攻擊者的手機門號與 Email 地址。

研究報告指出，該團隊早在 2019 年 5 月，即將這份發現提報給 Apple 知悉，但未收到回應，因此該團隊認為這個問題可能尚未得到解決；該團隊建議 AirDrop 用戶，在不使用時應該關閉 AirDrop，避免遭攻擊者以這種方法取得機敏資訊。

另外，該團隊也自行推出類 AirDrop 的傳輸應用程式，稱為「PrivateDrop」；PrivateDrop 引進更強效的加密演算法，可以更為有效的保護用戶個資，避免遭有心人攔截；交握所需時間僅比原生的 AirDrop 拉長不到一秒。

- 資料來源：
  1. Apple AirDrop shares more than files
  2. How WhatsApp, Signal & Co Threaten Privacy
  3. AirDrop Primer

2.6、軟體系統資安議題

2.6.1、國內企業接連遭勒索攻擊，建議落實資安防護措施

國內大型企業接連傳出遭 REvil 勒索軟體攻擊，並被駭客要求支付高額贖金。

首先是今年 3 月國內電腦大廠旗下歐美分公司，傳出疑似遭到 REvil 勒索軟體攻擊，要求的贖金高達五千萬美元。資安廠商 Advanced Intel 專家指出，觀察到 REvil 對受害企業發動的攻擊，可能是針對 Microsoft Exchange Server 的資安漏洞 ProxyLogon 發動此次攻擊。

該駭客組織並於網路上公開疑似竊自受害企業的機敏資料，包含財務報表、銀行帳目及銀行往來的通聯記錄等文件。針對外傳的攻擊行動，受害企業並未證實，但其表示已將近來在全球分支單位發生的各種異常狀況，向司法單位和資安相關單位提報。

4 月，國內一家電子代工製造大廠也傳出遭 REvil 勒索軟體入侵，駭客聲稱已取得受害企業的代工客戶產品資訊、員工及客戶資料等，要求贖金高達五千萬美元。該駭客組織於暗網上公開數張竊取自受害企業其代工客戶的產品設計圖，並威脅若不立即進行聯繫，就要公開銷售更多產品設計圖及個資等相關資料。

據國外媒體報導，該駭客組織在向受害企業要求贖金未果之後，轉而威脅受害企業之客戶支付贖金買回被竊取的資料，但受害企業及其客戶皆未發表回應。針對此次傳出遭勒索軟體攻擊事件，受害企業回應，公司的資安團隊已和外部第三方資安專業公司合作，並將偵測到的異常情形通報政府相關單位，同時配合司法單位展開調查。目前此起資安事件，並未影響企業生產與營運活動。

- 建議採取資安強化措施

1. 建議將 Exchange Server 依微軟提供的最新版本進行更新，以免遭駭客利用官方已公告之漏洞發動攻擊。平時應確保作業系統、防毒軟體及應用程式等皆更新到最新版本。
2. 定期將檔案進行備份，並符合備份 321 原則，至少備份 3 份檔案、使用 2 種不同媒體儲存以及其中 1 份存放於異地。
3. 若不幸遭勒索軟體入侵，建議先將受害主機進行網路隔離，避免擴大感染，並評估受損狀況即時向相關單位進行通報。

近年來勒索軟體攻擊事件頻傳，國內外多家大型企業皆傳出相關案例，並被要求支付高額贖金才能取回被竊資料，建議企業做好相關資安防護措施，定期對員工進行資安宣導和教育訓練，提供員工資安意識。

- 資料來源：

1. Computer giant Acer hit by $50 million ransomware attack
2. Acer reportedly hit with $50 million ransomware demand
3. Acer Reportedly Targeted by Ransomware Gang
4. REvil gang tries to extort Apple, threatens to sell stolen blueprints
5. REvil ransomware gang allegedly hacks Quanta Computer, steals Apple blueprints

6. Apple ransomware leak corroborates 2021 MacBook Pro ports: HDMI, MagSafe, SD card slot

7. 世界備份日(World Backup Day)：三二一原則

2.6.2、Qlocker 駭侵者，五天內不法獲利高達 26 萬美元

近日造成全球 QNAP NAS 裝置大規模感染的惡意勒贖軟體 Qlocker，其幕後主使者在短短五天之內賺取的不法獲利，已經高達美金 26 萬元以上。

近日造成全球 QNAP 網路儲存設備（Network Attached Storage, NAS）裝置大規模感染，用戶檔案遭壓縮並加上密碼鎖定的惡意勒贖軟體 Qlocker，其幕後主使者在短短五天之內賺取的不法獲利，已經高達美金 26 萬元。

這波 Qlocker 感染潮自上周一開始在全球各地蔓延；值得注意的是，其他類似勒贖攻擊者所使用的勒贖軟體，多半需要花費較多時間開發，但 Qlocker 攻擊者卻是利用廣為用戶使用的 7zip 壓縮程式，透過 QNAP 設備的 RCE 漏洞 CVE-2020-36195，遠端執行 7zip 程式，將用戶儲存在 NAS 中的檔案壓縮後加上解壓密碼，幾乎毫不費力。

攻擊者選擇攻擊對象的方式也很簡單。由於許多 NAS 用戶都會將其裝置連上 Internet，以便異地遠端存取檔案，但這些設備多半是由家庭或中小企業擁有，在資安防護與相關設定、備份等專業能力較為薄弱，因此攻擊者只要掃瞄整個 Internet，找出對 Internet 開放連線，可以遠端登入的 QNAP NAS 設備，即可鎖定這些裝置發動攻擊。

雖然 QNAP 在此之前數日，已經推出修補 CVE-2020-36195 的資安修補更新程式，但只要用戶未能在第一時間更新自己的裝置，就很可能成為駭侵者的攻擊對象；這也就是為何 Qlocker 能夠在短短數日之內，快速駭入眾多 QNAP NAS 裝置進行攻擊。

另外一個特色是，多數的勒贖攻擊多半鎖定大型企業，要求高達數十萬美金的高額贖金；但 Qlocker 則反其道而行，每台被駭入的裝置，只要求 0.01 枚比特幣的解密贖款，相當於台幣 15,000 元。多數受害者可能會認為金額不高，因此選擇花錢消災；也因此 Qlocker 駭侵者累計獲得的不法利益，就積少成多。

據資安專家研究指出，Qlocker 駭侵者一共使用 20 個比特幣錢包收取贖款，目前約有五百多名受害者支付贖金，累計不法獲利為 5.26 枚比特幣，約 260,000 美元左右。

- 資料來源：
  1. A ransomware gang made $260,000 in 5 days using the 7zip utility
  2. Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices

2.6.3、印度數位支付公司否認 KYC 用戶資料因駭侵而外洩

印度數位支付業者 Mobikwik 日前發生嚴重用戶資料外洩事件，多達 8TB 以上用戶資料遭不明駭侵者在暗網上公開，但該公司否認發生資安事故。

印度最大的數位支付業者 Mobikwik，日前遭資安專家指出該公司發生嚴重用戶資料外洩事件，多達 8TB 以上用戶資料，遭不明駭侵者在暗網上公開，但該公司否認發生資安事故。

獨立資安研究人員 Rajshekhar Rajaharia 於今年二月底時，在 Twitter 上發布貼文和截圖，指出他發現來自 Mobikwik 的大量用戶資料，被不明駭侵者部分公布於暗網，同時試圖出售這批資料。

被指為竊自 Mobikwik 的這批用戶資料，包括多種個人資料與金融相關資訊；其中包括超過一億人的住址、電話號碼、Email、經雜湊加密的用戶密碼，以及約四千萬名用戶的銀行帳戶與信用卡資訊等。該批資料還包括約 350 萬名印度用戶的 KYC（Know your customer）資料。

試圖出售這批資料的駭侵者，甚至還提供一個查詢頁面，可讓有意購買的人輸入要查詢的個人電話或 Email 地址，檢視和輸入資料相關的其他資料欄位；但由於查詢的網路流量太大，甚至出現資料爬蟲試圖搜刮資訊，該查詢欄位目前已遭撤下。

針對 Rajshekhar Rajaharia 的指證，以及媒體的後續相關報導，Mobikwik 一再極力否認，多次發表聲明指出該公司並未發生資料外洩事件，所有用戶資料都非常安全；針對用戶質疑自己的資料可在暗網上查到，該公司表示任何用戶都可以把自己的資料上傳到網路上的各個平台。

該公司也說，已會同第三方資安公司進行調查，沒有發現資料遭竊的證據。

- 資料來源：
  1. Rajshekhar Rajaharia(TWITTER)
  2. MobiKwik(TWITTER)
  3. MobiKwik Suffers Major Breach — KYC Data of 3.5 Million Users Exposed
  4. Leading Indian fintech platform MobiKwik denies data breach

2.6.4、法國電子製造大廠 Asteelflash 遭勒贖攻擊

法國電子製造業大廠 Asteelflash 日前遭到勒贖攻擊，駭侵者使用 REvil 勒贖軟體發動攻擊。

法國電子製造業大廠 Asteelflash 日前遭到勒贖攻擊，駭侵者使用 REvil 勒贖軟體發動攻擊，要求贖金高達 2,400 萬美元。

Asteelflash 是法國首屈一指的電子製造服務（Electronics Manufacturing Services, EMS）廠商，主要專精於電子產品的設計製造，以及印刷電路版設計製造。

據 Asteelflash 於 2021 年 4 月 2 日發布的新聞稿指出，該公司的 IT 部門於三月底的例行性資安檢查中，發現該公司部分系統遭到 REvil 駭侵軟體攻擊；該公司立即採取行動，避免 REvil 持續擴大感染，但這次駭侵攻擊已造成該公司內部網路停止正常運作。

該公司表示，在經過各方專家與 IT 部門的調查後，沒有發現勒贖軟體持續活動的跡象，也沒有發現任何資料遭竊取流出的證據；該公司的主要生產設備已經重新啟動，恢復生產作業。

Asteelflash 表示，該公司並未和發動攻擊的駭侵者進行任何接觸。

根據資安媒體 BleepingComputer 的報導指出，該網站追蹤到一個可能和這次攻擊事件有關的線索；一個疑似由 REvil 勒贖軟體開啟的 Tor 網頁，內容記載了這次攻擊要求的贖金；原本要求的贖金，在贖金交付期限過期後，已經提高一倍，成為 94,084.32 顆門羅幣，約合美金 2,400 萬元。

在這個 Tor 網頁中存有 REvil 駭侵者與 Asteelflash 的短暫交談內容；在交談中駭侵者出示一個名為 asteelflash_data_part1.7z 的檔案，用以證明檔案確實竊取自 Asteelflash 公司，但之後雙方並未繼續進行對話。

- 資料來源：
  1. [PRESS RELEASE] Cyber Security Incident Update
  2. Ransomware : Asteelflash résiste à la pression de Revil/Sodinokibi
  3. Asteelflash electronics maker hit by REvil ransomware attack

2.6.5、全球大型化妝品製造公司 Pierre Fabre 遭到 REvil 勒贖攻擊

全球最大的法國化妝品製造大廠 Pierre Fabre 日前遭到 REvil 勒贖軟體攻擊，駭侵者要求贖金高達 2,500 萬美元。

全球最大的法國化妝品暨藥品製造大廠 Pierre Fabre，日前遭到 REvil 勒贖軟體攻擊，駭侵者要求的贖金高達 2,500 萬美元。

Pierre Fabre 在受攻擊後數日發布的新聞稿中指出，該公司是於 3 月 31 日遭到勒贖攻擊，攻擊導致該公司多數生產線停擺，但位於法國 Tarn 地區，主要生產藥品與化妝品有效成分的 Gailac 工廠並未受到影響。

新聞稿也強調，該公司在確認遭到攻擊的 24 小時內，即將受損情形控制住；該集團的資訊系統立即切換到「待機模式」，以避免惡意軟體進一步擴散；另外重要藥品和化妝品的供應，以及相關行政與業務人員的作業，均未受到影響。但新聞稿並沒有說明這次駭侵攻擊的形態（沒有提到為勒贖攻擊），也沒有提及該公司是否有和勒贖團體接觸。

據資安專業媒體 BleepingComputer 報導，該刊觀察到的各種證據，證實此次攻擊是由 REvil 勒贖團體發動的另一波鎖定全球大型企業的攻擊活動；該刊在事件發生後，就掌握了一個 REvil 用來收取勒贖金的 Tor 網頁，駭侵者在其中說已經掌握來自 Pierre Fabre 的內部資料。

在這個網頁上同時也顯示了 REvil 要求的贖金，原本是 2,500 萬美元，但在支付期限過後，Pierre Fabre 顯然沒有繳付贖金，因此要求的贖金已經倍增到 5,000 萬美元。

REvil 近來針對全球知名大型企業發動過多場勒贖攻擊，近來的攻擊對象包括國內的大型資訊業者與法國大型電子製造廠 Asteelflash，對全球業者造成嚴重的資安威脅。

- 資料來源：
  1. Pierre Fabre continues to ensure its products are available to patients and consumers
  2. Leading cosmetics group Pierre Fabre hit with $25 million ransomware attack

2.7、軟硬體漏洞資訊

2.7.1、華碩發布伺服器韌體更新公告(ASMB8-iKVM、ASMB9-iKVM)

華碩重視用戶資訊安全，近期已針對搭載 ASMB8-iKVM、ASMB9-iKVM 之華碩伺服器產品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，以達到最佳的伺服器安全防護。

若需進一步技術支援，請洽華碩電腦伺服器技術支援單位。

- CVE 編號：CVE-2021-28175 ~ CVE-2021-28209

- 資料來源：
  1. TVN (Taiwan Vulnerability Note) 漏洞公告
  2. ASUS Product Security Advisory
  3. ASUS 聯絡我們

2.7.2、QNAP NAS 已修復漏洞，遭 Qlocker 發動大規模勒贖攻擊

近來出現一波針對 QNAP 網路儲存裝置的大規模勒贖攻擊，用戶裝置中的檔案會遭壓縮密碼鎖定，受害者人數正在快速擴大。

近來出現一波針對台灣領導品牌之一 QNAP（威聯通）網路儲存裝置（Network Attached Storage, NAS）的大規模勒贖攻擊，用戶裝置中的檔案會遭壓縮加上密碼鎖定，受害者人數正在快速擴大。

據資安專業媒體 BleepingComupter 報導指出，這波勒贖攻擊使用的惡意軟體，名為 Qlocker，自 2021 年 4 月 19 日起觀測到其攻擊活動的足跡，受害者數量同時快速增加，世界各國陸續傳出受害災情回報。

用戶的 QNAP NAS 裝置 一旦感染 Qlocker，NAS 中的所有檔案便會被惡意軟體使用 7zip 壓縮並加上密碼保護；惡意軟體執行壓縮工作時，用戶可以在 QNAP NAS 管理介面中的資源監視器畫面中，看到有個 7z 程式的執行緒。

當 Qlocker 完成壓縮作業後，會在用戶的 NAS 中留下一個未加密的文字檔「!!!READ_ME.txt」，並在其內文中要脅用戶透過 Tor 加密瀏覽器繳付贖款 0.01 枚比特幣，以取得解壓縮用的密碼。

雖然有資安專家很快找到 Qlocker 的漏洞，藉以查出解密用的密碼，但這個漏洞很快就被駭侵攻擊者修補完成。

據 BleepingComputer 報導，QNAP 指出 Qlocker 很可能是利用 QNAP 原廠已於 4 月 16 日更新修復的 CVE-2020-36195 漏洞發動攻擊；這個漏洞可讓攻擊者注入指令，同時遠端執行任意程式碼。

QNAP 在官方資安通報中指出，「使用者若受到勒索病毒影響，或觀察到勒索病毒執行中，並正在加密檔案，應保持 NAS 開機狀態、立即安裝並使用最新版 Malware Remover 進行惡意軟體掃描、並聯繫 QNAP 技術支援單位取得協助。」

對於尚未遭到 Qlocker 攻擊的用戶，QNAP 也建議用戶「應立即安裝並使用最新版 Malware Remover 進行惡意軟體掃描，變更所有使用者密碼為高強度密碼，並更新 Multimedia Console、Media Streaming Add-on 及 Hybrid Backup Sync 三個 App 至最新版。」

- 資料來源：
  1. 回應 Qlocker 勒索病毒攻擊事件：立即採取行動，保護 QNAP NAS
  2. New vulnerabilities discovered allow access to user data and complete takeover
  3. Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices

2.7.3、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，iOS 與 Mac、Apple Watch 裝置用戶應立即更新。

Apple 於日前緊急推出 iOS 14.5.1、macOS Blg 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：
  1. 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。
  2. iMac、Mac Pro、Macbook、Macbook Air、Macbook Pro 等多種 Mac 電腦。
  3. 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

2.7.4、VMware 修復管理者登入資訊外洩漏洞

VMware 近日修復旗下 vRealize Operations Manager 產品的資安更新版本，修復一個可能造成駭侵者成功竊得管理者登入資訊的漏洞，用戶應立即更新至最新版本。

虛擬運算方案大廠 VMware 近日發布資安通報，指出該公司已推出針對旗下 vRealize Operations 產品的資安更新版本；新版修復一個可能造成駭侵者成功竊得管理者登入資訊的高危險資安漏洞，用戶應立即更新至最新版本。

這個資安漏洞存於 VMware vRealize Operations Manager 系列產品中，該產品可讓用戶管理各種私有雲、公有雲或混合環境，特色是結合人工智慧技術，可做到自動管理。

該漏洞是由資安廠商 Positive Technology 旗下的資安專家所發現，並提報此漏洞給 VMware；這個漏洞存於 vRealize Operations Manager API 中，屬於伺服器端連線要求偽造漏洞（Server Side Request Forgery)；駭侵者可利用這個漏洞，無需經過登入手續或使用者互動，就可以用很簡單的手法竊得管理者登入資訊，便於發動進一步的駭侵攻擊。

這個漏洞的 CVE 編號為 CVE-2021-21975，其 CVSS 危險程度評分高達 8.6 分，屬於嚴重危險等級。主要影響的 vRealize Operations Manager 版本為 7.5.0、8.0.0、8.0.1、8.1.0、8.1.1、8.2.0、8.3.0。

VMware 在其發布的資安通報中，針對不同 vRealize Operations Manager 版本提供了暫時解決方案與資安更新檔案；使用上述版本 vRealize Operations Manager 的用戶，應即按照 VMware 官方的說明與指示進行更新，或使用暫時解決方案，以避免駭侵者透過此漏洞發動攻擊的風險。

- CVE 編號：CVE-2021-21975
- 影響產品/版本：VMware vRealize Oerations Manager 7.5.0、8.0.0、8.0.1、8.1.0、8.1.1、8.2.0、8.3.0。
- 解決方案：套用官方推出的暫時解決方案，並更新到最新版本。

- 資料來源：
  1. Advisory ID: VMSA-2021-0004.1
  2. CVE-2021-21975
  3. VMware fixes bug allowing attackers to steal admin credentials

2.7.5、Google 修復 Android 系統中可導致遠端執行任意程式碼的嚴重漏洞

Google 於近日推出 2021 年 4 月份 Android 系統資安更新，一共修復 30 個大小漏洞，其中包括一個可能導致駭侵者遠端執行任意程式碼的嚴重漏洞。

Google 於近日推出 2021 年 4 月份 Android 系統資安更新，一共修復超過 30 個大小資安漏洞；其中更包括一個可能導致駭侵者遠端執行任意程式碼的嚴重等級資安漏洞。各廠牌 Android 手機用戶，應注意手機原廠發表的修補更新訊息，當原廠發布資安更新時，應立即更新至最新版本韌體。

這個可能導致駭侵者遠端執行任意程式碼的漏洞，其 CVE 編號為 CVE-2021-0430，存於 Android 的系統組件之中；駭侵者可以透過特製的檔案觸發此漏洞，以擁有特權的執行程序遠端執行任意程式碼。

CVE-2021-0430 這個漏洞的 CVSS 危險程度評分高達 8.8 分，屬於「嚴重」（critical）等級；主要影響的 Android 版本為 Android 10 和 Android 11 等兩個版本。

在這波 Android 資安更新中，Google 是分成兩次發行的；4 月 1 日先推出的 Android 更新中，共有 12 個漏洞的危險程度等級為「高」（high）等級，其中有 9 個存於 Framework 組件中，另外有 3 個存於 Media 組件中，可讓駭侵者提升執行權限，或是竊取相關資訊。

4 月 5 日時 Google 再次推出一波 Android 資安更新，一共修復 18 個資安漏洞，其中包括存於系統組件的 2 個高危險資安漏洞、存於核心組件的 2 個高危險漏洞，其他漏洞則存於 MediaTek、Qualcomm 開源與閉源組件等。

由於 Google 推出的 Android 資安更新包，只適用於如 Google Pixel 等使用原生 Android 系統的裝置，其他主要品牌如 Samsung、Asus、Xiaomi 等各廠自行推出的 Android 裝置，必須等候原廠推出系統更新，因此用戶應隨時注意各原廠發布的更新訊息，即時更新 Android 手機至最新版本。

- CVE 編號：CVE-2021-0430
- 影響產品/版本：Android 8.1~11 各版本
- 解決方案：除採用原生 Android 系統手機（如 Pixel）可直接套用更新外，其餘各品牌 Android 手機需等待原廠推出更新

- 資料來源：
  1. Android Security Bulletin—April 2021
  2. Google Patches Critical Code Execution Vulnerability in Android

2.7.6、Google Chrome 90 新版修復多個資安漏洞

近日即將推出的 Google Chrome 版本 90，修復多達 9 個資安漏洞，其中包括數個高危險等級，可能造成駭侵者遠端執行任意程式碼。

Google 近日即將推出的 Google Chrome 版本 90，修復多達 9 個資安漏洞，其中包括數個危險程度列為高危險等級的漏洞，這些漏洞有可能讓駭侵者可以遠端執行任意程式碼；用戶應立即更新所有 Chromium 瀏覽器。

在這些漏洞中，最嚴重的是 CVE-2021-21227 這個漏洞；發現這個漏洞的是資安廠商 Singular Security Lab 旗下的研究員。據 Google 的更新說明文件指出，CVE-2021-21227 是存於 Google Chrome V8 引擎中的一個錯誤，由於未能對資料進行充分檢查，導致駭侵者有可能透過此漏洞，遠端執行任意程式碼。

不過研究人員也指出，這個漏洞必須和其他的資安漏洞合併使用，否則就無法跳過 Chrome 的記憶體沙盒，也無法觸及任何在沙盒之外執行的應用程式與系統資源；不過如果該漏洞利用的程式本身有較高執行權限，或是用戶自行關閉沙盒保護機制，那就可以直接存取系統發動 RCE 攻擊。

Google 這次推出的新版 Google Chorme 90.0.4430.93，也修復了多個其他漏洞，包括 CVE-2021-21232、CVE-2021-21233、CVE-2021-21228、CVE-2021-21229、CVE-2021-21230、CVE-2021-21231 等等；對應的作業

系統版本包括 Windows、Mac、Linux 等主流作業系統。

此外，市場上有多種使用與 Google Chrome 同一開源程式碼基礎 Chromium 的多種瀏覽器，如 Microsoft Edge、Brave、Vivaldi、Sidekick 等，也應一併更新。請用戶注意近期各瀏覽器的更新訊息，一旦有新版可供下載，請立即安裝，以修補這些已知資安漏洞，降低遭到駭侵攻擊的風險。

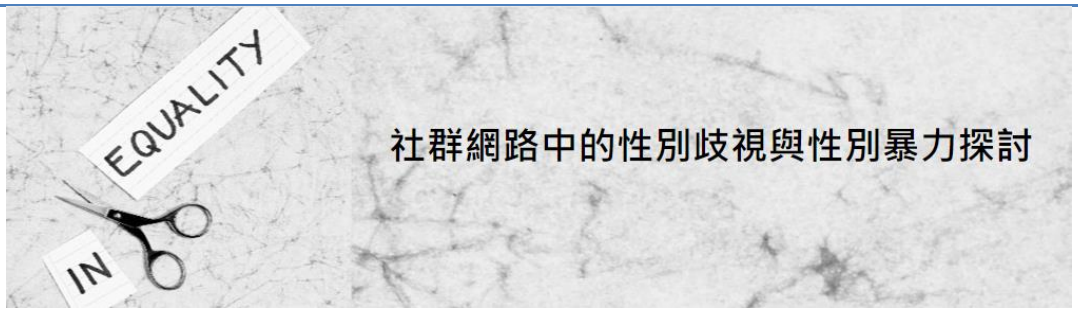
- CVE 編號：CVE-2021-21227 等
- 影響產品/版本：Google Chrome（Chromium）版本 90 之前
- 解決方案：更新到 Google Chrome（Chromium）版本 90 或更新版本

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google Patches Yet Another Serious V8 Vulnerability in Chrome
  3. Google Chrome V8 Bug Allows Remote Code-Execution

第 3 章、 資安研討會及活動

第一屆後量子密碼論壇	
活動時間 **活動地點**	**因疫情影響，原訂 5/21 舉辦的第一屆後量子密碼論壇將延期舉辦，詳情請見活動網站。**
活動網站	**https://pqc.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 國際頂尖密碼學家齊聚臺灣 本論壇邀請到多位國際頂尖密碼學家，其研發之後量子密碼演算法已進入 NIST 最終決選階段，有望成為世界標準。 此外，更有國內後量子密碼的實作企業，從各個面向協助政府、銀行、企業提早布局，遵循世界標準與規範，保護交易、個資、智慧財產及機敏資訊。 量子電腦已成定局，量子破密隨之而來，後量子密碼實現量子資安

【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.cisanet.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** 因應疫情升級，原授課時間 5/26 更改為授課時間 7/2。 聯絡窗口： 0225533988 分機 388　廖資深專員　maureen.liao@cisanet.org.tw 報名截止： 2021-05-26 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

社群網路中的性別歧視與性別暴力探討(線上座談)	
活動時間	**2021 年 5 月 26 日（三） 14:00-16:00**
活動地點	**僅提供線上視訊服務**
活動網站	**https://www.twsig.tw/20210526/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** *因應疫情升溫為加強防疫，本場次僅提供線上視訊服務，現場不開放民眾入場。 *線上參與會議室連結將於活動前一日公告於本網站，並主動寄送予報名者。 **活動背景** 聯合國婦女署曾出版「對婦女與女孩的網路暴力」（Cyber Violence against Women and Girls）調查報告，並將網路性別暴力分成：非法入侵他人電腦取得個資、竊取盜用他人身份、監視與追蹤他人、騷擾與威脅、網路誘拐，以及惡意散佈他人資料與隱私等六類。又根據國內的婦女救援基金會調查，近一成民眾的性私密影像曾被外流，更有大量黑數的影像在色情網站流竄，而受害者中有高達九成為女性。 女性並非性別暴力的唯一受害者。在資訊網路社會的多元發展下，不同的性別弱勢族群也成為性別歧視與性別暴力事件的受害者，並造成許多不容忽視的傷害結果。 台灣民眾在網路空間中是享有言論自由與意見表達的，在不違背此精神的前提下，本活動將針對性別弱勢在網路社群平臺上面對的暴力與歧視次文化現

	象，探討包括網路是否助長或惡化既有的暴力和歧視？協助弱勢團結、集起捍衛自己的助力？整個台灣網路社群，以及涉及的不同的利害關係人或團體，又如何彼此教育、合作，應對包括未經同意散布私密性影像、言語暴力、性威脅、性霸凌等仰賴網路而茁壯的性別暴力行為？

2021 網路治理研習營	
活動時間	**擇期舉行**
活動地點	
活動網站	**https://www.igcamp.tw/**
活動概要	 **主辦單位：NII** 由於近日疫情嚴峻，為維護講師及學員的健康，以及全力配合政府防疫措施，本研習營將待疫情穩定後再擇期舉行，錄取學員的名額將予以保留，造成您的不便，敬請見諒。 **活動簡介** 疫苗護照和 AI 等科技應用如何兼顧數位時代的人權保護？網路及社群平臺對於新聞生態、言論自由和內容秩序該承擔什麼公共責任？又富可敵國但提供免費服務的科技巨頭應被課徵數位稅並強制分拆嗎？以及當國家遭到重大網路攻擊時可以主動進行反擊嗎？如果您關心這些網路政策議題，歡迎報名「2021 網路治理研習營」免費課程活動，除了帶您探討當前重要的網路治理議題外，還有機會贏得多項獎學金！ 新冠肺炎疫情讓全球見證網路對當今社會的至關重要。然而，就在網路科技協助我們建立疫情社會「新常態」的同時，卻也衍生侵犯人權、破壞安全、製造社會衝突等新型態的濫用行為，這些問題唯有透過所有多方利害關係人（multi-stakeholder）的溝通對話，才能找到最佳治理方案。因此，不論您是來自政府部門、民間企業、學研單位、公民團體，或是仍在大專院校就學，

	如何因應數位變革所帶來的契機與挑戰，需要您的積極參與。 「2021 網路治理研習營」為一日免費研習活動，透過專題講習、案例探討、分組演練等方式，帶您認識數位人權、數位經濟、媒體與內容、網路安全等重要議題，以及如何參與這些議題的政策討論。所有學員都有機會贏得新臺幣 2,000 元~10,000 元的獎學金。活動名額有限，敬請把握報名良機！

第 4 章、 2021 年 4 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。

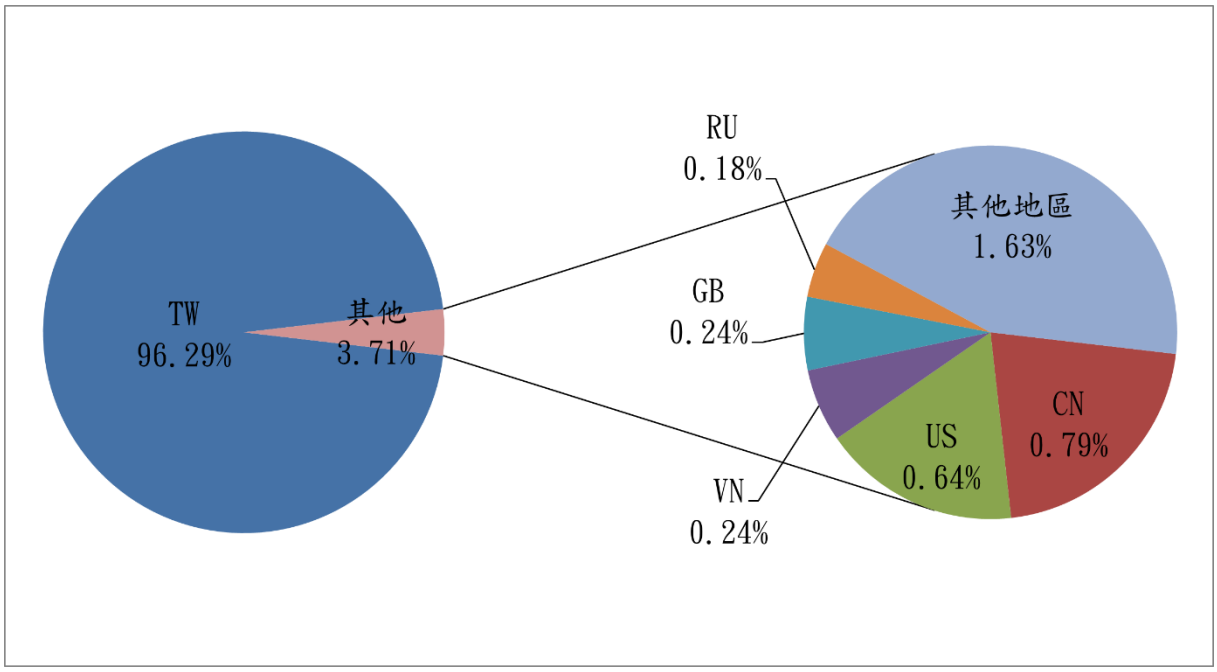


圖 1、分享地區統計圖

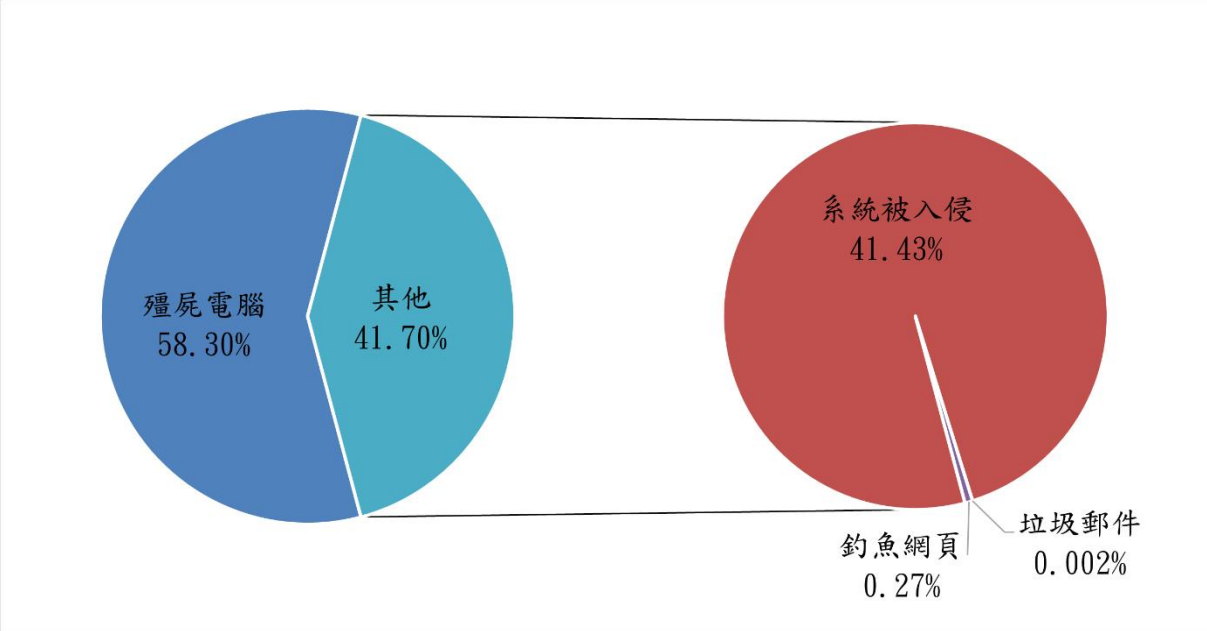


圖 2、分享類型統計圖

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 5 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**