TWCERT/CC 資安情資電子報

2022 年 2 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、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、TVN 漏洞公告：TWCERT/CC 為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN) 平台之漏洞嚴重程度前五的產品漏洞資訊。

第 5 章、資安情資分享概況：將上月 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

資安專家發現 Netgear Nighthawk R6700v3 路由器存有多個未修復漏洞

TWCERT/CC

資安專家發現Netgear
Nighthawk R6700v3
路由器存有多個未修復漏洞

資安廠商 Tenable 旗下的資安研究人員，近期發現 Netgear 一款暢銷的路由器 Netgear Nighthawk R6700v3 存有六個尚未修復的漏洞，可能導致駭客完全控制路由器。

這款路由器具有一些專為遊戲用途設計的功能，在市場上相當受歡迎；研究人員在其最新版本的韌體 1.0.4.120 中發現多達六個漏洞，分述如下：

- CVE-2021-20173：存於該裝置的更新功能中，為認證後命令注入漏洞；
- CVE-2021-20174：該裝置 web 介面的所有通訊均透過未加密的 http 進行，用戶登入資訊以明文傳送，可能遭駭侵者竊取；
- CVE-2021-20175：SOAP 介面（port 5000）亦使用未加密的 http 傳輸資料，用戶登入資訊有被竊風險；
- CVE-2021-23147：可透過 UART 連線在未經認證的情形下，以 root 權限執行指令；
- CVE-2021-45732：透過硬寫入的加密常式進行設定操弄，可導致因資安理由而鎖住的設定值遭到竄改；
- CVE-2021-45077：所有該裝置的用戶登入資訊，均以明文儲存於設定

檔中。

另外，研究人員也發現，在這款 Netgear Nighthawk R6700v3 中使用的 jQuery 程式庫 1.4.2 版與 miniDLNA 伺服器版本，都是存有已知資安漏洞的舊版。

雖然 Netgear Nighthawk R6700v3 仍在原廠支援週期內，並不是已經停止支援的老舊機種，不過截至發稿為止，Netgear 尚未針對這些被發現的漏洞提供新版韌體。

資安專家呼籲這款路由器的用戶，應將管理密碼設定為強式密碼，並頻繁檢查原廠是否推出了新版韌體，以便儘速更新。

- CVE 編號：CVE-2021-20173 等 6 個。
- 影響產品(版本)：Netgear Nighthawk R6700v3 韌體版本 1.0.4.120 與較舊版本。

- 資料來源：
  1. Netgear Nighthawk R6700 Multiple Vulnerabilities
  2. Netgear leaves vulnerabilities unpatched in Nighthawk router

第 2 章、 國內外重要資安事件

2.1、資安趨勢

附帶勒贖條件的 DDoS 攻擊，在 2021 年次數與強度大幅增加，製造業是主要受害者

網路基礎建設廠商發表研究報告，指出去年（2021）發生的附帶勒贖條件的分散式服務阻斷攻擊，不論在次數或強度上都明顯增加。

網路基礎建設廠商 Cloudflare 日前發表研究報告，指出去年（2021）發生的附帶勒贖條件的分散式服務阻斷攻擊（Extortion Distributed Denial of Service），不論在次數或強度上，都較往年明顯增加許多。

Cloudflare 指出，在去年第四季，約有 22% 的 Cloudflare 用戶曾遭到附帶勒贖要求的 DDoS 攻擊；駭侵者要求受害者必須支付要求的贖款，否則不會停止 DDoS 攻擊行動。而在前三季，該公司客戶遭到勒贖 DDoS 攻擊的比例，分別為 14%、9%、8%。

如果以月份來統計，Cloudflare 的報告中指出，去年 12 月該公司客戶遭到勒贖 DDoS 攻擊的比例高達 32%，比前一個月成長了一倍，也是全年發生次數最高的一個月。

Cloudflare 的報告也說，和 2020 年相比，2021 年的勒贖攻擊發生次數，也成長了 29%，同季比則大增了 175%。

在攻擊強度方面，Cloudflare 的報告指出，在二月時多半為 200Gbps，到

了九月中則加強到 500Gbps；另一家網路基礎設施業者 Akamai 也曾觀測到強度高度 800Gbps 的 DDoS 攻擊。CloudFlare 更曾觀測到強度高度 2Tbps 的攻擊。

Cloudflare 也說，製造業是去年 HTTP DDoS 攻擊受害最嚴重的業類，去年第四季和第三季相比，製造業遭攻擊的次數增到 641%。

如以攻擊事件發生地來看，這類 DDoS 攻擊來源最多的國家依序為中國、美國、巴西、印度。

- 資料來源：
  1. DDoS Attack Trends for Q4 2021
  2. Extortion DDoS attacks grow stronger and more common

2.2、新興應用資安

2.2.1、全球第四大加密貨幣交易所 Crypto.com 疑似遭駭，損失以太幣達 1,500 萬美元

全球虛擬資幣交易額排行第四的知名加密貨幣交易所 Crypto.com，日前傳出疑似嚴重駭侵事件，初步估計損失金額達 4,600 枚以太幣，以當時價值估計，高達 1,500 萬美元。

Crypto.com 於 1 月 17 日突然宣布「因一小部分用戶帳戶遭到未授權的存取」，因而暫時凍結所有提款服務；該公司同時要求用戶重新登入帳號，並且重置原先的二階段登入驗證。

雖然 Crypto.com 當時強調「所有用戶資金均安全無虞」，但仍有用戶發現自己在 Crypto.com 的錢包中資金被竊；另一方面，Dogecoin「狗狗幣」創辦人 Billy Markus 也指出自己在 Crypto.com 的以太幣錢包「有不明活動」。

另外也有資深加密貨幣投資者表示，自己帳戶內的以太幣被竊走 4.28 枚，損失相當於 15,000 美元；他說他有啟用二階段登入驗噔，因此 Crypto.com 的部分資安防護想必遭到駭侵者的突破。

資安廠商 Peckshield 在深入追究這起事件後，在 Twitter 上發文指出 Crypto.com 的資金損失高達 4,600 枚以太幣，約合 1,500 萬美元；這些損失金額中有一半被匯到 Tornado Cash。

在回應媒體訪問時，Peckshield 強調，目前的數字只是暫時的預估，實際損失一定更加嚴重；不過 Crypto.com 的執行長 Kris Marszalek 表示，所有的用戶資金都沒有任何損失，另外 Crypto.com 交易所也強化了基礎設施的資安

防護能力，並積極展開事件調查，將在調查告一段落後對外公開。

也有 Crypto.com 的用戶表示，一度遭竊的帳戶錢包內資金，之後也返回其帳戶之內。

- 資料來源：
  1. Crypto.com pauses withdrawals due to ‘suspicious activity’
  2. Crypto.com Suffers Hack for At Least $15M in Ethereum

2.2.2、Crypto.com 證實 483 名用戶加密貨幣資金遭不當存取，損失達 3,400 萬美元

全球第四大加密貨幣交易所 Crypto.com，日前於官方部落格中發文證實，日前發生的駭侵事件中，共有 483 位用戶的數位錢包遭外力不當存取，損失達 3,400 萬美元，但已全數補回用戶帳戶內。

Crypto.com 執行長 Kris Marszalek 在接受 Bloomberg 專訪時承認，約有 400 名用戶的帳戶發生異常提領事件；隨後該公司在官方部落格中貼文說明，指出確切的受害用戶有 483 名，被竊資金分別有 4,836.26 枚以太幣（約合 15,132,516 美元）、443.93 枚比特幣（合 18,613,360 美元），以及其他加密貨幣約 66,200 美元，總計損失高達 33,812,346 美元。

在 Crypto.com 提出的報告中指出，不當存取事件發生於今（2022）年 1 月 17 日世界標準時間上午 12:46 分左右，當時該公司的資安監控系統偵測到一部分用戶的帳戶，出現未經授權的活動；這些用戶的資金未經過二階段登入驗證就被轉出。

Crypto.com 表示，在發現異常活動後，該公司立即暫停所有用戶的提領權限，時間共計約 14 小時，在當天世界標準時間 17:46 恢復提款作業。

Crypto.com 在聲明中指出，該公司於事件發生後，立即導入加強資安措施，除了重置所有用戶的二階段登入驗證設定，用戶必須重新設定新的二階段登入驗證之外，也對新註冊帳戶的新增轉帳地址設定與首次轉帳設定 24 小時延遲，以避免發生攻擊事件時資金立即遭竊，並爭取調查所需時間。

該公司也強調，在這次事件中，所有受害用戶的資金都已補回，用戶沒有實質損失，但該公司並未透露這次攻擊事件的其他細節，例如攻擊者、攻擊手法等資訊。

- 資料來源：
  1. Crypto.com Security Report & Next Steps
  2. On-chain analyst claims Crypto.com hack was closer to $33 million

2.2.3、BlueNoroff 駭侵團體利用假 MetaMask 錢包竊取加密貨幣

俄羅斯資安廠商 Kaspersky 旗下的研究人員，日前發現駭侵團體 BlueNoroff，近來針對世界各國的加密貨幣相關新創發動攻擊，竊取其加密貨幣資產。

Kaspersky 發現，BlueNoroff 的攻擊手法，是先設法入侵受害目標企業的人員通訊之中，以社交工程的手法，誘使目標下載含有惡意程式碼的檔案；該檔案中的惡意程式碼，會利用一個十分老舊的遠端遙控指令漏洞 CVE-2017-1099，來植入第一階段的惡意程式碼，之後駭侵者會再寄送一個假冒需以密碼開啟的檔案給受害者，內含第二階段的惡意程式碼，以在受害者電腦中植入後門。

Kaspersky 說，BlueNoroff 會先以數周時間觀察受害者的使用行為，並且收集用戶電腦上和加密貨幣相關的各種設定檔，以及觀察期間中的按鍵記錄，找出可趁之機。之後再以植入電腦中的惡意程式碼，替換掉如 MetaMask 這類瀏覽器外掛加密貨幣錢包的核心程式碼，以竊取受害者的加密貨幣資產。

BlueNoroff 的駭侵者，會假冒成許多知名加密貨幣相關企業的人員或合作伙伴，並且使用這些企業的商標，以降低目標對象的戒心。

Kaspersky 說，遭到 BlueNoroff 攻擊的加密貨幣新創公司受害者遍布世界各國，包括美國、俄羅斯、中國、印度、英國、烏克蘭、波蘭、捷克、阿拉伯聯合大公國、新加坡、愛沙尼亞、越南、馬爾他、德國、香港等。

資安專家表示，BlueNoroff 雖然過去就曾有多年活動記錄，但外界對其了解甚少；在這次攻擊活動中有明確跡象顯示，該駭侵團體極可能為 APT 團體 Lazarus 的外圍組織。

- 資料來源：
  1. The BlueNoroff cryptocurrency hunt is still on
  2. BlueNoroff hackers steal crypto using fake MetaMask extension

2.3、國際政府組織資安資訊

2.3.1、美國政府要求企業必須保障客戶資料不受 Log4j 漏洞攻擊影響

美國聯邦貿易委員會（Federal Trade Commission, FTC）日前公告，警告任何無法採取行動，有效保護客戶資料不受 Log4j 漏洞影響的企業，將會受到該單位的法律制裁。

FTC 發表的新聞稿指出，Log4j 漏洞（CVE-2021-44228）的影響十分嚴重，對數百萬種消費性產品、企業用軟體與網路服務造成巨大資安危機，且已遭到駭侵者廣泛運用於各類資安攻擊。

FTC 說，依照相關美國法律，包括聯邦貿易委員會法（the Federal Trade Commission Act）與金融服務法現代化法案（Gramm Leach Bliley Act），企業有責任處理已知的軟體資安漏洞。

FTC 指出，2019 年時 Equifax 即因未能立即處理已知的軟體資安漏洞，造成 1.47 億客戶個人資料外洩，因此被判 7 億美元的巨額罰款。

FTC 表示，如果有任何企業未能依法立即處理已知的 Log4j 漏洞，或是未來任何已知的資安漏洞，因而造成顧客資料損害，FTC 將動用一切司法行政能力，對這類企業進行裁罰。

FTC 要求各企業依照美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）提出的指南，加強應對 Log4j 漏洞，包括將使用 Log4j 程式庫的軟體更新至最新版本、依照指南強化資安防護能力與布署、確認所有步驟符合上述法律的要求，並且將相關訊息通報所有相關

關係人，例如軟體供應商、代理商等。

- 資料來源：
  1. FTC warns companies to remediate Log4j security vulnerability
  2. FTC to pursue companies that expose customer data due to not patching Log4j

2.3.2、瑞士軍方禁用所有外國製即時通訊軟體，僅開放國產的 Threema

瑞士軍方日前發布公告，宣布禁止官兵使用外國製作的即時通訊軟體，如 Signal、Telegram、WhatsApp 等，並要求官兵使用瑞士自製的 Threema 作為替代。

瑞士軍方指出，經過審慎的資安評估作業後，作出這項禁用各種外國即時通訊軟體的決定；軍方表示，Threema 不含廣告，且支援端對端加密通訊，安全程度較高，且不會留下任何數位足跡。

由於 Threema 是付費訂閱制服務，瑞士軍方也表示將為全體官兵支付 Threema 的使用費，單一使用者的年費約當 4.4 美元。

資安專家指出，雖然包括 WhatsApp、iMessage、LINE、Signal、Telegram、Facebook Messenger 等知名即時通訊軟體，均有支援端對端加密，但平台仍可能會留存用戶與通訊相關的後設資料（metadata）；而這些資料有可能遭各國政府要求取得。

不同的通訊軟體保留的後設資料不同，有些可能只有用戶註冊日期，但有些可能會包括用戶的 IP 位址、Email 地址、電話號碼，甚至部分通訊內容在內。

另外，雖然有些通訊軟體本身是開源的，但其伺服器端的程式碼仍然不透明，因此仍可能有未知的資訊洩漏風險。

瑞士軍方指出，Threema 的註冊除了不需要手機門號或 Email 地址之外，更重要的是它不受美國雲端服務法的規範，因此美國政府無法要求取得

Threema 的任何資訊，資安專家認為這可能才是瑞士軍方選擇 Threema 的主因。

- 資料來源：
  1. Schweizer Armee verbietet Whatsapp
  2. Swiss army restricts use of messenger apps
  3. Swiss army bans all chat apps but locally-developed Threema

2.3.3、荷蘭資安主管機關警示，仍應提防 Log4j 漏洞資安風險

荷蘭資安主管機關 Nationaal Cyber Security Centrum (NCSC) 日前發出資安警訊，指出目前該機構仍偵測到許多利用 Log4j 漏洞進行的資安攻擊活動，各界仍需提高警覺。

NCSC 官員指出，雖然在去年年底發現 Log4j 漏洞及其嚴重威脅後，已有許多公私單位針對該漏洞進行防護與修補，但駭侵者仍然積極針對尚未採取行動的目標發動各種攻擊活動。

官員說，可以預期這些惡意分子，仍在大規模掃瞄任何可以發動攻擊的目標，並且發動攻擊。

NCSC 指出，該單位仍強烈建議所有公私單位，仔細檢查使用中的系統，是否仍然存有 Log4j 相關漏洞，並且立即進行修補。

此外，NCSC 也呼籲各單位仍應密切注意 Log4j 相關漏洞與攻擊情報，並仔細評估一旦遭到攻擊時，對其營業活動可能造成的衝擊程度，並預做準備，超前布署。

資安專家表示，荷蘭 NCSC 的呼籲相當適時，因為微軟在 1 月 19 日才發表資安情資，指出有一大型機構遭某駭侵團體，試圖以 SolarWinds Serv-U 的 0-day 漏洞侵入該單位的 LDAP 伺服器，並且利用 Log4j 漏洞發動攻擊；但由於該單位的 LDAP 伺服器並不存有 Log4j 漏洞，因此並未得逞。

此外，微軟與英國健保署（NHS）也曾在一周前分別發布同類事件的資

安通報，指出有疑似 DEV-0401 駭侵團體，針對網路上的 VMware Horizon 伺服器的 Log4kj 漏洞，發動 Night Sky 勒贖攻擊。

- 資料來源：
  1. Houd aandacht voor Log4j
  2. Dutch cybersecurity agency warns of lingering Log4j risks

2.3.4、加拿大外交部遭駭侵攻擊，部分服務無法運作

加拿大外交部（Global Affairs Canada）日前遭到不明來源的駭侵攻擊，使該部轄下的電腦系統服務遭到阻斷而無法使用。

據加拿大國庫委員會秘書處（Treasury Board of Canada Secretariat）、加拿大共同服務（Shared Services Canada）和加拿大通訊安全局（Communications Security Establishment）聯合指出，在上周某個時間點，加拿大外交部的系統遭到不明攻擊；在展開調查後，確認遭到攻擊的日期為今（2022）年 1 月 19 日。

相關單位指出，雖然加拿大外交部的部分網路服務系統，因遭到攻擊而中斷服務，但該部門的重要系統仍然運作如常。目前正在加緊調查事件原因，並且加快系統修復進度。

加拿大政府指出，這些系統均備有各種針對資安攻擊的監控、偵測與調查工具，可以快速分析攻擊活動並立即處理。

不過，由於調查工作仍在進行之中，加拿大官方並未針對駭侵攻擊事件的原因，以及攻擊來源等資訊提供詳細說明。加拿大國庫委員會秘書處也說，目前除了加拿大外交部外，尚未觀察到有其他加拿大政府機關遭到類似攻擊的跡象。

就在這次駭侵事件發生之前，加拿大資安主管機關 Canadian Centre for Cyber Security 才發布一則資安通報，指出有一個叫做 Wiper 的惡意軟體，正

在針對烏克蘭相關公私單位發動攻擊，提醒加拿大所屬相關單位提高警覺。不過目前尚無法證實兩者之間是否直接相關。

- 資料來源：
  1. TBS Canada @TBS_Canada
  2. Wiper malware targeting Ukrainian organizations
  3. Canada's foreign affairs ministry hacked, some services down

2.4、社群媒體資安近況

2.4.1、Telegram 成為販賣不法金融資訊熱門管道

資安廠商 Cybersixgill 旗下的研究人員最近指出，具備端對端加密，匿名且隱密性相當高的 Telegram 通訊軟體，現已成為網路罪犯用以販賣不法金融資料的熱門管道。

由於 Telegram 目前全球用戶高達五億，再加上平台或聊天頻道的管理多半較為鬆散，只會刪除極端主義者的言論，因此近來成為資安犯罪分子用來販賣竊得金融資訊的熱門入口。

專家說，架設一個用來販賣資料的暗網網站，比起在 Telegram 設立群組的難度要高很多，觸及潛在用戶的能力也比較差，因此在 Telegram 上比較容易快速找到願意出錢購買不法金融資訊的買家。

再者，Telegram 群組在銷售完成後可以輕易放棄或刪除，比起暗網網站的處理上要方便不少，也能讓這類不法交易更不容易遭到追蹤，交易更加安全，因而大行其道。

Cybersixgill 的專家，在 Telegram 分析各種和金融資料或洗錢相關的關鍵字，發現 PayPal 帳號是在各種遭竊金融資訊中占比最高的一種，接下來依序是大通銀行（Chase）、西聯匯款（Western Union）、富國銀行（Wells Fargo）、花旗銀行（CITI）、美國銀行（Bank of America）、美國運通（American Express）、匯豐銀行（HSBC）、VISA、MasterCard 等金融服務的信用卡 / 帳戶資訊。

專家指出，PayPal 最受這些人頭帳戶買家的青睞，是因為相較於其他銀行或匯款服務來說，PayPal 用來購買一些不易追蹤的貨幣用以進行洗錢，是較為方便的。

另外，透過 Telegram 販賣的金融資訊中，信用卡資訊的比例依然很高，特別是附有 CVV/CVV2 驗證碼的資訊更為搶手，每張信用卡的價格可以從 10 美元到 1500 美元之譜。

- 資料來源：
  1. Telegram: A Cybercriminal Hotspot – Compromised Financial Accounts
  2. Telegram is a hotspot for the sale of stolen financial accounts

2.4.2、Purple Fox 惡意軟體藉 Telegram 安裝程式散布

資安廠商 Minerva Labs 旗下的資安專家，發現 Purple Fox 惡意軟體，藉由遭到竄改的 Telegram 社群通訊軟體 Windows 安裝程式散布。

資安廠商 Minerva Labs 旗下的資安專家，近期發現一個名為 Purple Fox 的惡意軟體，藉由遭到竄改的 Telegram 社群通訊軟體 Windows 安裝程式散布，可能導致駭侵者進一步在受感染裝置中植入惡意程式碼。

資安專家發現的 Telegram 惡意安裝程式，是一個編譯過的 AutoIt 指令檔，名為「Telegtam Desktop.exe」，內含兩個部分；一個是真正的 Telegram 安裝程式，另一個則是惡意軟體的下載工具。

受害者執行這個遭到竄改的安裝程式時，會同時在用戶的「C:\Users\Public\Videos\」下新增一個名為「1640618495」的資料夾，然後連接到駭侵者設立的控制伺服器，下載一個 7z 工具程式與 RAR 壓縮檔；接著 7z 工具程式就會將壓縮檔中的惡意程式碼檔案解壓縮到用戶電腦的「ProgramData」資料夾中。

用戶的 Windows 登錄檔內，還會新增一個機碼，以常駐執行惡意軟體；另外也會安裝多個檔案，以阻止 UAC 與 360AV 的執行，避免 Purple Fox 遭到發現。

據 Minerva Labs 表示，目前還不清楚 Purple Fox 透過哪些管道散布，但有許多類似假冒正版程式的惡意軟體，會透過 YouTube 影片下的留言、討論

區的的垃圾貼文、盜版軟體下載網站等管道來散布。

資安專家呼籲社會大眾，下載安裝軟體時，必須確認是經由官方網站或可信賴的來源進行，不要在可疑的網站或社群空間中點按連結以安裝軟體，以避免遭到惡意軟體攻擊。

- 資料來源：
  1. Malicious Telegram Installer Drops Purple Fox Rootkit
  2. Purple Fox malware distributed via malicious Telegram installers

2.5、行動裝置資安訊息

2.5.1、iOS 惡意軟體可假裝重開機，以盜用相機鏡頭與麥克風進行盜錄監視

資安廠商 ZecOps 旗下的資安專家，近來發現一種特殊方法，可以在不知不覺間啟用 iPhone 的照相機和麥克風，進行惡意盜錄與監控。

資安廠商 ZecOps 旗下的資安專家，近來發現一種特殊方法，可以在不知不覺間啟用 iPhone 的照相機和麥克風，進行惡意盜錄與監控；甚至還可誤導用戶誤以為 iOS 裝置已關機，實際上繼續進行暗中監控。

ZecOps 的資安專家發展出的概念證實實作（Proof of Concept, PoC）特洛依木馬程式，證實了惡意軟體可以在用戶嘗試關機以結束惡意軟體運作時，攔截用戶的關機動作（同時按下休眠與音量放大按鈕），播放一段以假亂真的關機動畫，讓用戶誤以為手機已關機，實際上照相鏡頭與麥克風仍在暗中運作，而且不會顯示任何 iOS 作業系統預設的相機 / 麥克風運作中警示。

另外，這個概念證實程式也能透過各種方式，阻止用戶深度重置手機，讓惡意程式本身可以持續執行，而用戶也會誤以為手機已經關機並重置。

而當用戶進行手機開機動作時，該木馬也會顯示假冒的開機流程動畫，讓用戶誤以為手機已經重新開機；事實上用戶手機從來沒有真正進入關機模式，因此惡意軟體得以持續進行影像與聲音的暗中監控。

資安專家指出，Apple 於 iOS 15 推出的手機尋找功能，讓 iPhone 即使處在關機狀態下，藍牙晶片也還是處在低功率運作狀態下，因此才能回應來自

網路或其他方式的搜尋需求，包括發出聲音、傳送所在地資訊等。

專家表示，用戶千萬不要相信這些裝置會真的完全關機，除非移除電池或徹底破壞裝置；而過去用戶以關機來停止惡意軟體運作的作法，也將失去效果。

- 資料來源：
  1. Persistence without “Persistence”: Meet The Ultimate Persistence Bug – “NoReboot”
  2. ZecOps/public
  3. iOS malware can fake iPhone shut downs to snoop on camera, microphone

2.5.2、Apple 修復可能造成 iPhone、iPad 無法使用的 doorLock DoS 漏洞

Apple 近日推出針對所謂「doorLock」DoS (Denial of Service，即服務阻斷攻擊）漏洞的資安更新；該漏洞可能導致用戶的 iPhone 與 iPad 無法使用，用戶應立即更新。

該漏洞的 CVE 編號為 CVE-2022-22588，存於 iOS、iPadOS 14.7 與之後版本的 HomeKit 智慧家庭延伸核心組件之中。資安專家先前發現，攻擊者可利用這個漏洞，以特製（超過 50 萬字元）的 HomeKit 智慧裝置名稱誘發漏洞，造成服務阻斷效果，使得用戶的 iPhone 與 iPad 陷入無法使用的狀態。

遭此攻擊的 iPhone 和 iPad ，即使重新開機，只要一登入用戶的 iCloud 帳號，就會再次載入惡意 HomeKit 裝置的資訊，再次造成當機。用戶設備必須完全重置為出廠狀態，並刪除機內所有資料與設定，才能恢復正常；如果用戶沒有備份資料，就會遭到資料滅失的損害。

HomeKit 是 Apple 推出的智慧家庭框架，可讓 iOS、iPadOS 用戶發現、連接並使用各種家用聯網智慧裝置。

受此漏洞影響的 iOS 與 iPadOS 裝置，包括 iPhone 6s 與後續機種、iPad Pro 全機種、iPad Air 第 2 代與後續機種、iPad 第 5 代與後續機種、iPad mini 第 4 代與後續機種，以及 iPod Touch（第 7 代）。

Apple 於新推出的 iOS 15.2.1 與 iPadOS 15.2.1 中修復這個漏洞，用戶應立即更新，以避免裝置遭駭侵者利用此漏洞發動攻擊而無法使用。

- 資料來源：
  1. About the security content of iOS 15.2.1 and iPadOS 15.2.1
  2. doorLock
  3. Apple fixes doorLock bug that can disable iPhones and iPads

2.5.3、新版 Android 惡意軟體 BRATA 會先竊取手機資訊，接著清空手機

資安廠商 Cleafy 旗下的資安專家，近期發現 Android 惡意軟體 BRATA，最近推出最新版本，不但會竊取更多手機用戶的資訊，還會在竊取資訊後刪除手機內部的資料。

BRATA 的最初版本是由卡巴斯基是在 2019 年發現，當時主要以 WhatsApp 感染巴西的 Android 手機用戶，會竊取用戶手機中的各種資料，包括螢幕擷圖、各種裝置資訊、使用者輸入的內容，還具有串流功能，可以把用戶即時操作一五一十都傳回控制伺服器。

現今傳播的新版 BRATA，主要針對英國、波蘭、義大利、西班牙、中國與拉丁美洲諸國的手機用戶，竊取其裝置內的行動金融服務資訊；不同的變種病毒鎖定不同金融服務，甚至潛藏於不同的 app 中，針對特定用戶進行攻擊。

報告也說，這個版本的 BRATA 甚至會先掃瞄用戶手機中安裝的防毒防駭軟體，並加以刪除或停用，再進行資料竊取。

另一家資安廠商 Cleafy 旗下的資安研究人員，則發現新版 BRATA 可以取得手機的即時 GPS 地理座標資訊，換言之可用以追蹤受害用戶的移動軌跡。

Cleafy 也指出，BRATA 在成功入侵並竊得資料，或是發現自己是在虛擬環境中執行時，會將手機恢復到出廠設定；因此受害者手機中的所有資料，都會全部遭到刪除清空。

資安專家指出，避免受到這類惡意軟體感染的最佳方式，就是不安裝不明來源的 APK 檔案；只在具有較佳保護的應用程式商店，如 Google Play Store 安裝手機軟體，並在執行前先以防毒工具掃瞄。

- 資料來源：
  1. How BRATA is monitoring your bank account
  2. Android malware BRATA wipes your device after stealing data

2.6、軟體系統資安議題

2.6.1、針對 QNAP NAS 裝置攻擊的 Qlocker 勒贖軟體，再度發動大規模攻擊

去年曾針對台灣網路儲存大廠 QNAP 各型網路儲存裝（Network Attached Storage，NAS）裝置，發動大規模攻擊的 Qlocker 勒贖軟體，近期據報又開始進行世界性的攻擊。

據資安專業媒體 BleepingComputer 報導指出，該媒體是在今（2022）年 1 月 6 日起觀測到 Qlocker 再次開始攻擊行為；受到攻擊的 QNAP NAS 裝置，如同去年的攻擊行動，裝置內儲存的檔案，會遭到駭侵者以 .7z 壓縮軟體加密壓縮，且每個資料夾內都會被新增一個 !!!READ_ME.txt 勒贖信檔案，表示受害者所有的檔案均已遭加密。

勒贖信中也要脅，受害者若不到指定的 Tor 暗網網址 gvka2m4qt5fod2fltkjmdk4gxh5oxemhpgmnmtjptms6fkgfzdd62tad.onion 中，依指示支付 0.02 到 0.03 枚比特幣的贖金，就無法取得解密用的密碼。

BleepingComputer 統計指出，去年 Qlocker 發動的攻擊中，一個月內就取得超過 35 萬美元的不法獲利；當時的贖款是 0.01 比特幣，依當時幣價約為 500 美元。

據 QNAP 針對 Qlocker 新攻勢發布的資安通報指出，未感染的用戶，應立即使用內建的 Security Conselor 檢查 NAS 裝置是否曝露於外網，如檢查結果出現「The System Administration service can be directly accessible from an external IP address via the following protocols: HTTP」的文字，表示該裝置可由

外網直接透過未加密的 http 連線連入，風險較高，應儘速依該通報指示，關閉路由器的 Port Forwarding 功能，關閉對外的 Port 80 與 443，並且關閉 NAS 的 UPnP 功能，並升級至最新版作業系統與應用程式，以避免外網直接連入。

QNAP 也提醒用戶，QNAP 確認惡意程式使用近期已修補的漏洞進行攻擊，建議各位用戶盡快進行更新。

- 資料來源：
  1. 立即採取資安防護行動，確保 NAS 資料安全
  2. Qlocker ransomware returns to target QNAP NAS devices worldwide
  3. QLocker2 (QNAP NAS) Ransomware .zip

2.6.2、新一波針對 QNAP 裝置的 DeadBolt 勒贖攻擊正在蔓延，建議用戶立即更新

一波針對 QNAP NAS 網路儲存裝置的全新勒贖攻擊，名為 Deadbolt，目前正在全球快速蔓延，用戶應立即提高警覺。

一波針對 QNAP NAS（Network Attached Storage）網路儲存裝置的全新勒贖攻擊，名為 Deadbolt，目前正在全球快速蔓延；QNAP 用戶應立即提高警覺，避免裝置內的檔案遭到加密。

據資安媒體 BleepingComputer 的報導指出，Deadbolt 是在今（2022）年 1 月 25 日開始針對全球各地的 QNAP NAS 發動勒贖攻擊；用戶的 NAS 裝置如果遭到入侵，不僅所有檔案都會被加密，副檔名會變成「.deadbolt」，且用戶會在登入頁面看到一個黑底的畫面，載明該裝置中的檔案均已遭到加密。

在被竄改的登入畫面中，駭侵者說這不是針對 QNAP NAS 裝置個人發動的攻擊，而是因為廠商的資安防護不適當。

用戶如果想要解鎖遭加密的檔案，必須依駭侵者的指示，支付 0.03 枚比特幣的贖金（約合新台幣 30,500 元）；不過目前無法證實支付了贖金後，駭侵者真的會提供可資解密的金鑰。

BleepingComputer 的報導中指出，目前該刊掌握的受害者至少有 15 位，並不特定分布在某一地區；而所有遭 Dealbolt 攻擊的 QNAP NAS，都是直接與 Internet 連接，可由內網外部存取的。

此外，駭侵者也在上述的登入畫面中，放了一段「致 QNAP 重要訊息」段落；訊息中說該公司顧客之所以會遭到駭侵攻擊，是因為其產品存有一個不明 0-day 漏洞；如果 QNAP 支付 5 枚比特幣（約新台幣 510 萬元），駭侵者會提供該 0-day 漏洞的相關資訊與詳細分析報告；但如果 QNAP 支付 50 枚比特幣（約新台幣 5100 萬元），即可取得能為所有受害顧客解密的主要金鑰，以及上述的 0-day 漏洞資訊。

資安專家呼籲，各種 NAS 裝置用戶，應立即更新系統至最新版本，並且避免將 NAS 裝置直接連上 Internet，以免遭到攻擊。

QNAP 也表示，經過 QNAP PSIRT 調查，為防止 DeadBolt ransomware 與其他惡意程式攻擊，QNAP 建議使用者參考資安通報立即更新 QTS。

以下為推薦的 QTS 版本：

- QTS 5.0.0.1891 build 20211221 and later
- QTS 4.5.4.1892 build 20211223 and later
- QuTS hero h5.0.0.1892 build 20211222 and later
- QuTScloud c5.0.0.1919 build 20220119 and later

QNAP PSIRT 會持續追蹤惡意程式動向，並提供使用者與資安社群相關資訊。

- 資料來源：
  1. [RANSOMWARE] Deadbolt
  2. Wireless-News @news_wireless
  3. New DeadBolt ransomware targets QNAP devices, asks 50 BTC for master key
  4. Resolved Vulnerability in QTS and QuTS hero

2.6.3、微軟推出 2022 年一月份 Patch Tuesday 軟體更新修補包，共修補 97 個漏洞

微軟公司推出 2022 年一月「Patch Tuesday」資安修補包，一共修復多達 97 個漏洞，其中更有 6 個 0-day 漏洞。

微軟公司日前推出例行資安更新的 2022 年一月「Patch Tuesday」資安修補包，一共修復多達 97 個漏洞，其中更有 6 個 0-day 漏洞；資安專家呼籲微軟各種產品用戶應立即更新。

在這 97 個得到更新的漏洞中，有 9 個列為「嚴重」等級，另有 88 個列為「重要等級」；依其屬性列表如下：

- 41 個漏洞屬於執行權限提升漏洞；
- 9 個漏洞屬於跳過資安防護功能漏洞；
- 29 個遠端執行任意程式碼漏洞；
- 6 個資訊外洩漏洞；
- 9 個服務阻斷漏洞；
- 3 個詐騙假冒漏洞。

9 個嚴重等級的漏洞，分別為 ：

- CVE-2022-21846：Microsoft Exchange Server 遠端執行任意程式碼漏洞；

- CVE-2022-21840：Microsoft Office 遠端執行任意程式碼漏洞；
- CVE-2022-21917：HEVC 影音延伸組件遠端執行任意程式碼漏洞；
- CVE-2022-22947：開源 Curl 組件遠端執行任意程式碼漏洞；
- CVE-2022-21857：Active Directory 網域服務權限提升漏洞；
- CVE-2022-21898：DirectX 繪圖核心遠端執行任意程式碼漏洞；
- CVE-2022-21912：DirectX 繪圖核心遠端執行任意程式碼漏洞；
- CVE-2022-21907：HTTP 協定堆疊遠端執行任意程式碼漏洞；
- CVE-2022-21833：虛擬機器 IDE 磁碟權限提升漏洞。

此外，六個得到修補的 0-day 漏洞，目前尚未傳出遭到大規模利用於駭侵攻擊的情報。

- 資料來源：
  1. January 2022 Security Updates
  2. Microsoft January 2022 Patch Tuesday: Six zero-days, over 90 vulnerabilities fixed
  3. Microsoft January 2022 Patch Tuesday fixes 6 zero-days, 97 flaws

2.6.4、資安廠商發現多起間諜軟體攻擊，針對大型製造業竊取各種登入資訊

資安廠商卡巴斯基，近日發現最近多起針對製造業發動的間諜軟體駭侵攻擊；這些攻擊者意圖竊取各種登入資訊，用於進一步的駭侵攻擊，或是售出牟利。

卡巴斯基說，近來這些攻擊的特徵，是使用各種現成的間諜軟體工具，例如 AgentTesla/Origin Logger、HawkEye、Noon/Formbook、Masslogger、Snake Keylogger、Azorult、Lokibot 等，來進行短時間的攻擊，以避免遭到發現。

卡巴斯基將這類攻擊稱為「anomalous」，以與一般較長期的攻擊活動區別；據其觀察報告指出，這波攻擊每次的持續時間，約為 25 日左右，而一般典型的間諜軟體駭侵攻擊，多半持續數月到數年之久。

報告也說，這波攻擊與其他間諜軟體的攻擊，有一個很大的不同，就是選擇使用 SMTP 而非 HTTPS，作為惡意軟體與控制伺服器連線的通訊協定。卡巴斯基說，採用 SMTP 是很特別的選擇，因為 SMTP 僅能進行單向傳輸，也只能傳送文字檔，無法傳送其他型態的二進位或非文字檔。但是 SMTP 可以輕易混在一般網路傳輸流量之中，不易遭到發現，而且使用簡便。

在駭侵技術分析中，卡巴斯基表示，駭侵者使用魚叉式釣魚攻擊，先竊得登入資訊，再以該登入資訊進一步入侵企業內網，而且駭侵者會將先前駭入企業的 Email 信箱，當做是控制伺服器使用，以發動新攻擊，這樣可以有效避免企業防毒防駭系統的偵測。

卡巴斯基的報告也指出，觀察到的製造業受害者相當多，約有 2,000 個企業 Email 帳號被當做控制伺服器；竊得的資訊也被放到暗上待價而沽，其中包括許多 Email RDP、SMTP、SSH、cPanel、VPN 帳號登入資訊。

- 資料來源：
  1. Campaigns abusing corporate trusted infrastructure hunt for corporate credentials on ICS networks
  2. ‘Anomalous’ spyware stealing credentials in industrial firms

2.6.5、跨國國防工業製造廠 Hensoldt 證實遭勒贖軟體 Lorenz 攻擊

總部位於德國的大型跨國國防工業製造廠 Hensoldt，在英國的數個旗下事業單位的電腦系統，日前遭到勒贖軟體 Lorenz 的攻擊。

該公司專門生產各種軍用、航太、安全等應用領域的各型感測器；也是美軍各種武器系統的合約生產製造商。該公司生產的雷達陣列、航空電子設備、雷射測距儀等各種裝置，廣泛搭載於美國陸軍、海軍陸戰隊、國民兵等單位使用的各型戰車、船艦、直升機等武器系統之上。

該公司發言人於 1 月 12 日 對資安媒體 BleepingComuter 證實，其設於英國的附屬單位電腦系統遭到 Lorenz 勒贖軟體駭入，但未透露關於這起駭侵事件進一步的資訊。

資安專家表示，Lorenz 駭侵團體設於暗網上，專門用以公開竊得資訊的「勒贖官網」，已將 Hensoldt 列入「已成功駭入」名單之中，且標示為「已支付贖款」；這表示該公司或其他人已經按照勒贖不法分子的要求支付不明數額的贖金，以避免該公司的各種攸關多國國防機密的相關資料遭到公開。

不過，Lorenz 已在其暗網中的「勒贖官網」中列出許多疑似竊取自 Hensoldt 的資料加密壓縮檔；該組織聲稱已經上傳近 95% 自 Hensoldt 竊得的檔案。

據資安專家表示，Lorenz 與其他勒贖駭侵組織類似，都會以公布竊取資料作為要脅，以提高收到贖金的比例；而 Lorenz 要求的贖金相當高，約在 50 萬美元到 70 萬美元之間。

資安專家說，Lorenz 勒贖團體是從去（2021）年 4 月時開始活躍，針對全世界大型公司進行勒贖活動，已有多家大小規模不等的公司受害。

- 資料來源：
  1. Lorenz ransomware gang stolen files from defense contractor Hensoldt
  2. Defense contractor Hensoldt confirms Lorenz ransomware attack

2.7、軟硬體漏洞資訊

2.7.1、多款市售家用路由器內含漏洞，可導致駭客透過 USB 裝置遠端執行任意程式碼

資安廠商 SentinelOne 旗下的資安專家，近日發現多款家用路由器，內含一個 NetUSB 嚴重資安漏洞，可導致駭侵者用於遠端執行任意程式碼。

資安廠商 SentinelOne 旗下的資安專家，近日發現包括 Netgear、TP-Link、Tenda、Western Digital、D-Link、Edimax 在內的多款家用路由器，內含一個 NetUSB 嚴重資安漏洞，可導致駭侵者用於遠端執行任意程式碼。

該漏洞發生在這些路由器使用的 KCodes NetUSB 核心模組；該功能用於路由器上附帶的 USB 插槽，讓網內用戶可以透過網路共享該 USB 裝置的資源。

SentinelOne 發現，KCodes NetUSB 核心模組的程式碼中，並不會驗證核心記憶體分配呼叫的大小值，因此很容易造成整數溢位錯誤；駭侵者可以利用這個漏洞進行越界資料寫入，並且遠端執行任意程式碼。

SentinelOne 指出，他們發現來自 Netgear、Tenda、Western Digital、D-Link、Edimax 的部分市售暢銷家用路由器，都同樣含有這個漏洞；不過由於這些廠牌推出的路由器款式甚為多樣，且多數都附有 USB 插孔，因此該報告並未明確指出是哪些機種受到 CVE-2021-45388 的影響。

SentinelOne 說，他們在去年 9 月發現此漏洞後，立即向該程式模組開發廠商 KCodes 提報，去年 11 月時 KCodes 將修復漏洞的程式碼提供給各路由

器廠商，供其更新產品韌體之用。

在 SentinelOne 對外公開此漏洞前，Netgear 已針對旗下三款路由器產品 D7800、R6400v2、R6700v3 推出含有修復版本的新版韌體。

資安專家呼籲上述廠牌家用路由器用戶，務必經常注意並更新至最新版韌體；未來若有必要更換產品時，也盡可能選擇更新頻繁，且支援周期較長的產品與品牌。

- CVE 編號：CVE-2021-45388
- 影響產品：Netgear、Tenda、Western Digital、D-Link、Edimax 附有 USB 插孔的部分市售暢銷家用路由器。
- 解決方案：多數廠牌暫無，用戶應隨時升級至最新版韌體。

- 資料來源：
  1. CVE-2021-45608 | NetUSB RCE Flaw in Millions of End User Routers
  2. KCodes NetUSB bug exposes millions of routers to RCE attacks

2.7.2、WordPress 推出 5.8.3，修復多個嚴重漏洞

WordPress 開發團隊近日推出最新的 WordPress 5.8.3 版本，一共修復四個漏洞，其中有三個的危險評分較高，請用戶立即更新至最新版本。

得到更新的四個 WordPress 資安漏洞如下：

- CVE-2022-21661：本漏洞屬於 SQL 指令注入漏洞，駭侵者可透過惡意外掛程式或佈景主題，利用 WP-Query 來注入惡意指令；本漏洞的 CVSS 危險程度評分高達 8 分（滿分為 10 分）。
- CVE-2022-21662：本漏洞屬於 XSS 跨站指令碼漏洞，低權限的用戶（如文章作者）可以在文章網址代稱（post slug) 欄位中植入惡意後門程式碼，取得網站控制權；本漏洞的 CVSS 危險程度評分高達 8 分。
- CVE-2022-21664：本漏洞屬於 SQL 指令注入漏洞，駭侵者可透過 WP_Meta_Query 核心類別來注入惡意程式碼；本漏洞的 CVSS 危險程度評分高達 7.4 分。
- CVE-2022-21663：本漏洞屬於物件注入漏洞，駭侵者必須先取得管理者帳號權限，才能利用此漏洞發動攻擊，因此本漏洞的 CVSS 危險程度評分較低，為 6.6 分。

除了 CVE-2022-21664 的漏洞，自 WordPress 4.1.34 開始就存在外，其餘的漏洞都從 WordPress 3.7.37 就已存在。資安專家表示，目前尚未接獲有任何攻擊行動係利用此次更新的四個漏洞來進行的情資。

WordPress 的開發公司 Automattic 指出，自 2013 年推出的 WordPress 3.7 版起，均包含自動更新程式；建議所有用戶立即更新至最新版 WordPress 5.8.3，同時不要停用自動更新功能。

- CVE 編號：CVE-2022-21661 等
- 影響產品：WordPress 3.7.37 (CVE-2022-21661、21662、21663）、4.1.34 (CVE-2022-21664) 至 5.8.2 之間所有版本。
- 解決方案：更新至 WordPress 5.8.3 及其後版本。

- 資料來源：
  1. WordPress 5.8.3 Security Release
  2. WordPress 5.8.3 security update fixes SQL injection, XSS flaws

2.7.3、Apple 修復兩個可用於駭侵 iOS、iPadOS 與 macOS 裝置的 0-day 漏洞

Apple 日前修復兩個可用於駭入用戶 iOS 與 macOS 裝置的 0-day 漏洞，一個可以遠端執行任意程式碼，另一個可用於追蹤使用者。用戶應立即更新裝置，以避免相關資安攻擊風險。

第一個獲得修補的漏洞，其 CVE 編號為 CVE-2022-22587，是發生於 IOMobleFrameBuffer 的記憶體崩潰漏洞；受影響的裝置包括多種 iOS、iPadOS 與 macOS 裝置，如 iPhone 6s 與後續機種、iPad Pro 全機種、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第七代、執行 macOS Monterey 的所有 Mac 機種。

駭侵者可利用此漏洞，在受駭裝置以上 kernel 權限遠端執行任意程式碼。

Apple 公司在軟體更新說明中表示，該公司已知悉此漏洞可能已遭不肖分子積極利用於駭侵攻擊活動。

第二個獲得修補的漏洞為 CVE-2022-22594，存於 iOS 與 iPadOS 中的 Safari WebKit 的 IndexDB 組件中，Safari 在對輸入字串進行驗證時發生漏洞；駭侵者可利用此漏洞取得用戶的各種可識別資訊，對用戶的瀏覽行為進行即時追蹤。

受此漏洞影響的 iOS 與 iPadOS 裝置，包括 iPhone 6s 與後續機種、iPad Pro 全機種、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第七代。

這兩個 0-day 均於日前 Apple 發行的 iOS 15.3 與 iPadOS 15.3 資安更新中獲得修補，各類 Apple 產品用戶，均應立即將作業系統更新至最新版本，以避免裝置因含有上述資安漏洞，因而曝露於高度駭侵攻擊風險之中。

- CVE 編號：CVE-2022-22587、CVE-2022-22594
- 影響產品：iPhone 6s 與後續機種、iPad Pro 全機種、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第七代、執行 macOS Monterey 的所有 Mac 機種。
- 解決方案：更新至 iOS、iPadOS 15.3 與後續版本、macOS Monterey 12.2 與後續版本。

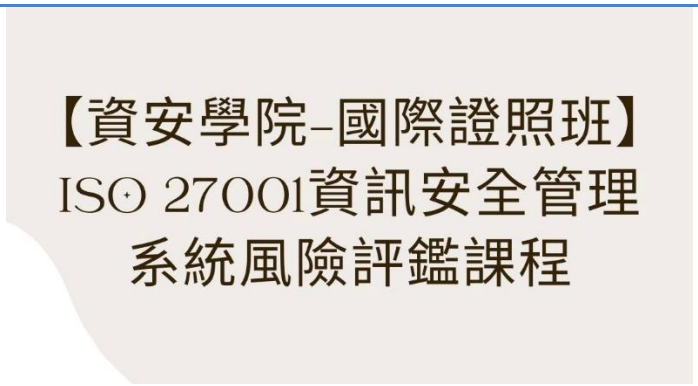
- 資料來源：
  1. About the security content of iOS 15.3 and iPadOS 15.3
  2. About the security content of macOS Monterey 12.2
  3. Apple fixes new zero-day exploited to hack macOS, iOS devices

第 3 章、 資安研討會及活動

《數位人權研討會》剖析元宇宙發展痛點：資訊安全與數位人權	
活動時間	2022 年 2 月 14 日（一）14:00 - 17:00
活動地點	臺大校友會館　4 樓會議室（臺北市濟南路一段 2-1 號 4 樓）
活動網站	https://www.accupass.com/event/2201050729181065808149
活動概要	 **主辦單位：國家人權委員會、中華民國數位金融交易暨資料保護協會** 國家人權委員會與中華民國數位金融交易暨資料保護協會共同舉辦《數位人權研討會》，本次研討會將以「剖析元宇宙發展痛點：資訊安全與數位人權」作為核心軸，邀請各界學者及實務工作者探討在現實與虛擬界線模糊的元宇宙世界中，如何建置資訊安全防禦、實踐數位人權及維護資安隱私，並結合探討區塊鏈等議題，提出元宇宙發展後將會面臨的挑戰及因應策略。 全球數位化時代來臨，惟我國數位基礎建設不足，部分地區數位應用落差巨大，個別單位或公司的高度數位化，造就的是一座又一座的數位孤島，數位發展不足地區，各項社會資源與功能無法銜接，而造成數位人權低落窘境。 為推廣數位人權觀念，國家人權委員會與中華民國數位金融交易暨資料保護協會將共同舉辦四場《數位人權研討會》，邀請各界學者及實務工

	作者分享多元跨領域觀點，結合各方專業知識及實際經驗，共同探討在高度數位化的時代，如何藉由科技面對多元變化形態、數位未來之際。 2022 第二場《數位人權研討會》 在現實與虛擬界線模糊的元宇宙世界中，如何建置資訊安全防禦、實踐數位人權及維護資安隱私，並結合探討區塊鏈等議題，提出元宇宙發展後將會面臨的挑戰及因應策略。 ※四場演講 x 一場綜合與談 ➢ 行政院　唐鳳政務委員 ➢ 國家人權委員會　范巽綠委員 ➢ 台灣大學資訊工程學系　廖世偉副教授 ➢ 中華民國數位金融交易暨資料保護協會　蔡一郎理事 ➢ 開放文化基金會　李欣穎執行長 ➢ 中華民國數位金融交易暨資料保護協會　翁仲和副理事長

從撞庫事件看金融資安需求變化	
活動時間	**2022 年 2 月 24 日 星期四 14:00~16:10**
活動地點	**線上論壇 (報名後另行提供上線連結)**
活動網站	**https://newera17031.activehosted.com/index.php?action=social&chash=697e382cfd25b07a3e62275d3ee132b3.3260&nosocial=1**
活動概要	 **主辦單位：資安人媒體** 【數位金融資安線上講堂】從撞庫事件看金融資安需求變化 根據世界經濟論壇(WEF)2020 年的全球風險報告指出, 資安風險將會是未來的兩大風險之一, 加上這兩年新冠疫情肆虐以來，加速改變了金融服務轉型，金融業者越發仰賴數位科技，資訊安全對業者甚至客戶的威脅也日與俱增。過去除了過去最常見的阻斷服務（DDoS）、標靶式攻擊（APT）、詐騙簡訊結合偽冒網站（Scam SMS and Fake Website) ,近期勒索軟（Ransomware）、釣魚郵件（Phishing）、撞庫攻擊(Credential Stuffing Attack)等攻擊事件更是層出不窮, 一旦疏忽將會對金融市場造成莫大的影響。 金融市場的穩定發展, 對國家經濟成長至關重要,政府也意識到金融數位化過程中資安的急迫性與重要性, 超前佈署首度提出「金融資安行動方案」,內容中也提到面對數位金融的新興科技應運, 更應該意識到資安防護的重要性, 這次論壇我們可以由去年 11 月所發生的 6 家卷商與 1 家期貨商發生的撞庫事件來探討如何透過 AI 的資安方案快速建立攻擊防線。

【資安學院-國際證照班】ISO 27001 資訊安全管理系統風險評鑑課程	
活動時間	**3/2（三）~3/3（四）兩日共計 12 小時**
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/Course/Detail/2713**
活動概要	 **主辦單位：中華民國資訊軟體協會** 課程說明：現今企業競爭已從有形到無形，資訊（Information）更是企業核心的無形資產；為維護此資產，尤其企業組織欲建立資訊安全系統，首重風險管理，此課程提供一套完整的風險分析及風險處理程序，藉由學習如何將資產分類，並判斷其價值與重要性，做出脆弱性及威脅分析，瞭解如何將風險管理與資訊安全結合，進而以系統化的風險分析，做好資訊安全的風險管理。 課程大綱： ➢ 認識風險：風險背景及來源 ➢ 風險評估（Risk Evaluation）：可能性及衝擊分析 ➢ 風險評鑑（RA）方法論介紹 ➢ 風險評鑑實地演練 ➢ 資產分類與鑑別 ➢ 風險處理（Risk Treatment）手法與技巧 ➢ 威脅、脆弱性之鑑別 ➢ 建立資訊安全風險管理系統 ➢ 測驗

課程對象：

- 已瞭解 ISO/IEC 27001 資訊安全管理系統要求者
- 資訊安全管理人員、部門主管、高階主管
- 企業組織內負責導入資訊安全管理系統之人員
- 風險管理的分析與執行人員
- 有志成為資訊安全管理系統顧問師的人員

活動聯絡人：廖資深專員 maureen.liao@ cisanet.org.tw

(02)2553-3988 Ext：388

講師：BSI 台灣分公司專業合格之講師授課

教材：英、中對照教材及試卷

證書：BSI 原廠授證。課程測驗通過後，將由 BSI 台灣分公司授予證書；測驗未通過者，本會則將發「結業證書」乙只。

注意事項：本課程需全程參與，不可請假或缺席，請假或缺席時數者不予考試及發證，敬請保留完整上課時間。

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布漏洞嚴重程度前五名之漏洞資訊如下表：

樂衍 樂晴牙醫管理系統 - Hard-coded Credentials	
TVN / CVE ID	TVN-202201004 / CVE-2022-22056
CVSS	9.8 (Critical)
影響產品	樂衍 樂晴牙醫管理系統 ver.2.8.5
問題描述	樂晴牙醫管理系統管理者帳號密碼以明文方式 Hard-code 於網頁原始碼中，導致遠端攻擊者不須登入，即可取得管理者權限，並控制系統或中斷服務。
解決方法	聯繫樂衍進行版本更新
公開日期	2022-01-14
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5510-45d71-3.html

樂衍 樂晴牙醫管理系統 - SQL Injection	
TVN / CVE ID	TVN-202201003 / CVE-2022-22055
CVSS	9.8 (Critical)
影響產品	樂衍 樂晴牙醫管理系統 ver.2.8.5
問題描述	樂晴牙醫管理系統存在 SQL Injection 漏洞，遠端攻擊者不須權限，即可於登入頁面欄位注入 SQL 指令，取得管理者權限，並任意操作系統或中斷服務。
解決方法	聯繫樂衍進行版本更新
公開日期	2022-01-14
相關連結	https://www.twcert.org.tw/newepaper/cp-151-5509-80f05-3.html

Hicos 自然人憑證客戶端元件版本 - Command Injection	
TVN / CVE ID	TVN-202201006 / CVE-2020-12775
CVSS	9.8 (Critical)
影響產品	Hicos 自然人憑證客戶端元件版本 Windows 平台版本 <= 3.0.0 macOS 平台版本 <= 1.3.4.12
問題描述	Hicos 自然人憑證客戶端元件未對特定網址之傳送指令功能參數進行特殊字元過濾，遠端攻擊者不須登入，即可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令，並導致阻斷系統與終止服務。
解決方法	至 MOICA 內政部憑證管理中心官網下載最新版
公開日期	2022-01-31
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-5695-421a7-3.html**

Link Resolution Before File Access	
TVN / CVE ID	TVN-202201005 / CVE-2022-22262
CVSS	7.7 (High)
影響產品	ASUS ROG Live Service V1.2.18.0
問題描述	ROG Live Service 刪除安裝產生的 temp 檔案之功能存在 Improper Link Resolution Before File Access 漏洞，Local 端攻擊者不需權限，可以建立未預期的 symbolic link 指向系統資料夾路徑，因該功能未對欲刪除路徑進行檢查，即可刪除任意系統檔案，可能導致系統服務異常。
解決方法	Update ASUS ROG Live Service version to 1.3.3.0
公開日期	2022-01-31
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-5693-f108f-3.html**

ASUS VivoMini/Mini PC - improper input validation	
TVN / CVE ID	TVN-202201001 / CVE-2022-21933
CVSS	6.7 (Medium)
影響產品	ASUS VivoMini/Mini PC 受影響產品清單： ASUS VC65-C1 BIOS version < 1302 ASUS PB60V BIOS version < 1302 ASUS PB60G BIOS version < 1302 ASUS PB60S BIOS version <1302 ASUS PA90 BIOS version < 1401 ASUS PB50 BIOS version < 902 ASUS PB60 BIOS version < 1502

	ASUS PB61V BIOS version < 601 ASUS TS10 BIOS version < 609 ASUS PN40 BIOS version < 2201 ASUS PN60 BIOS version < 808 ASUS PN30 BIOS version < 320 ASUS UN65U BIOS version < 618
問題描述	ASUS VivoMini/Mini PC 設備存在 improper input validation 漏洞，Local 端的攻擊者獲得作業系統權限後，利用 BIOS 系統管理中斷(System Management Interrupt，簡稱 SMI)修改記憶體，導致可執行任意程式碼，藉以控制系統或中斷服務。
解決方法	BIOS Update，詳細請見 https://www.asus.com/content/ASUS-Product-Security-Advisory/
公開日期	2022-01-20
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-5547-34bc4-3.html**

第 5 章、 2022 年 1 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。

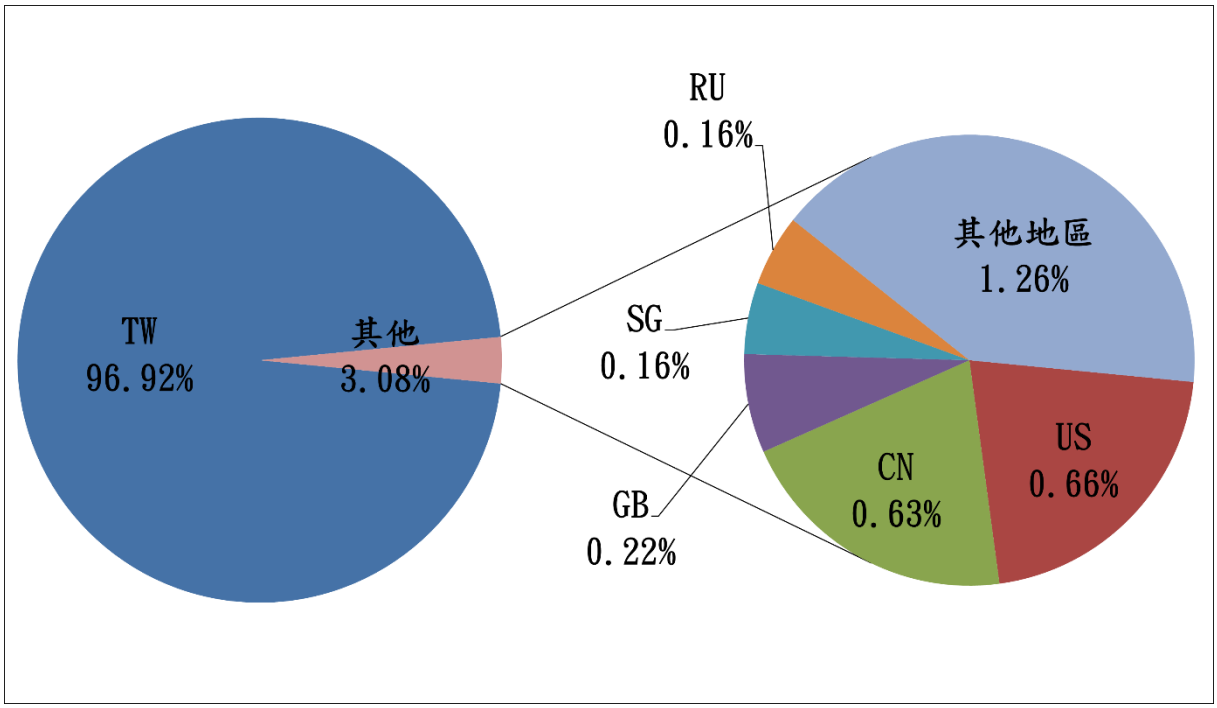


圖 1、分享地區統計圖

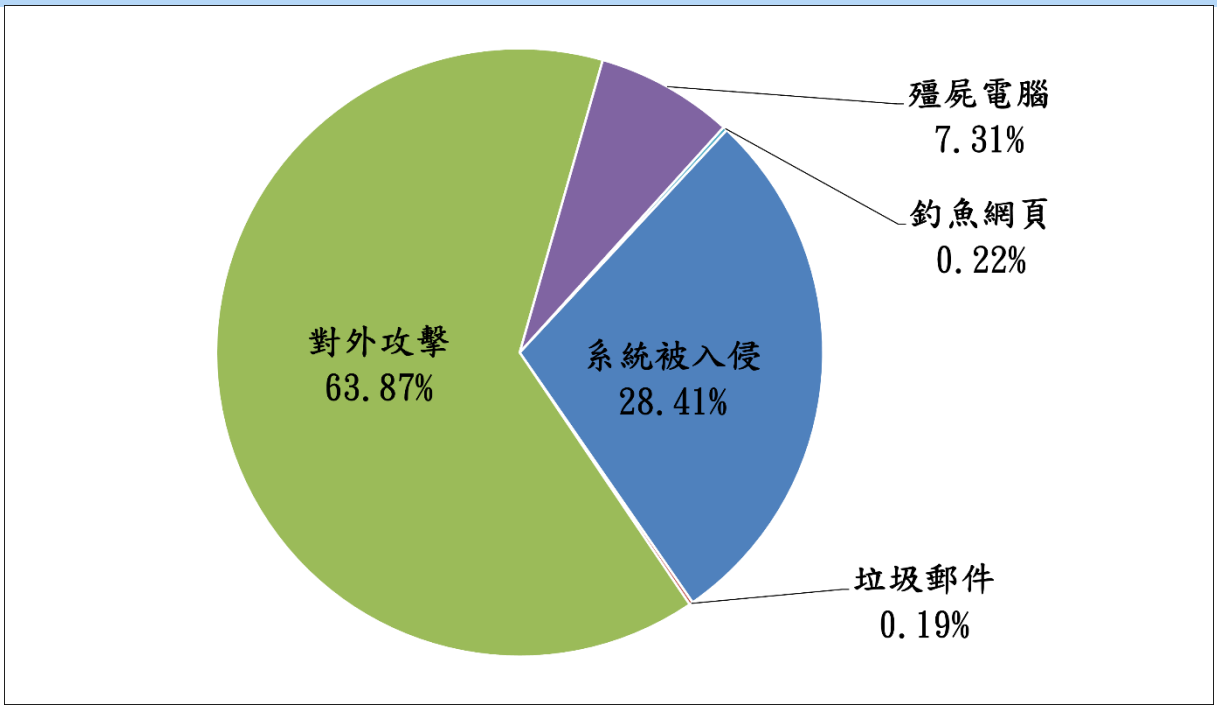


圖 2、分享類型統計圖

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：**2022 年 2 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**