



TWCERT/CC 資安情資電子報

2021 年 11 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、活動紀事：TWCERT/CC 主辦或參與之資安活動及訓練課程等。

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、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 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
	Microsoft Azure 雲端服務遭史上最大流量 DDoS 攻擊，瞬間流量高達 2.4Tbps..	1
第 2 章、	活動紀事	3
	TWCERT/CC 參與亞太區 APCERT CYBER DRILL 2021 演練	3
第 3 章、	國內外重要資安事件	5
3.1、	資安趨勢	5
3.1.1、	VirusTotal 分析 8,000 萬筆勒贖案例	5
3.1.2、	今年針對俄羅斯企業的 DDoS 攻擊，次數較去年大增 250% 以上.....	7
3.2、	新興應用資安	9
3.2.1、	Coinbase 因簡訊二階段驗證系統錯誤，導致六千名用戶資產遭竊	9
3.2.2、	OpenSea NFT 交易所漏洞，造成用戶加密貨幣遭竊.....	11
3.3、	國際政府組織資安資訊	13
3.3.1、	全球 31 國宣示共同投入打擊加密貨幣非法匯兌與洗錢管道.....	13
3.3.2、	美國資安主管機關示警：供水暨廢水處理設施正遭到強力勒贖攻擊.....	15
3.3.3、	美國推出新禁令禁止駭侵工具出口，以防用於資安攻擊與人權侵害.....	17
3.3.4、	荷蘭警方發函警告駭侵者停止行動，回頭是岸，以免遭司法控訴.....	19
3.4、	社群媒體資安近況	21
3.4.1、	駭侵團體經常利用釣魚信件，以 Cookie 竊取軟體強奪 YouTuber 帳號	21
3.4.2、	全球最大遊戲直播平台 Twitch 遭駭，多項資料遭駭侵者公開.....	23
3.4.3、	YouTube 遭駭客上傳惡意影片，內含登入資訊竊取惡意軟體連結	25
3.5、	行動裝置資安訊息	27
3.5.1、	韓國第二大電信業者 KT Corporation 因路由設定錯誤發生服務中斷....	27
3.5.2、	Google 推出 10 月 Android 資安修補例行更新，修復 41 個資安漏洞	29
3.5.3、	上千萬 Android 用戶遭 151 支惡意 App 攻擊，擅自訂閱高價服務	31
3.6、	軟體系統資安議題	33
3.6.1、	APT 駭侵團體 ChamelGang，攻擊多國能源、航空產業與政府機關	33
3.6.2、	NPM UA-Parser-JS 遭植入惡意軟體，會竊取用戶資訊或暗中挖礦.....	35

3.6.3、	國內電腦設備品牌大廠遭兩次駭侵攻擊，多種內部機敏資訊遭竊.....	37
3.7、	軟硬體漏洞資訊	39
3.7.1、	Apache HTTP Server 修復可導致指定路徑外檔案遭竊的 0-day 漏洞	39
3.7.2、	微軟要求系統管理員更新 PowerShell，修補 WDAC 資安防護跳過漏洞	41
3.7.3、	軟推出 10 月 Patch Tuesday 資安修補包，修復多個嚴重及 0-day 漏洞.	43
3.7.4、	QNAP 修復導致駭客遠端注入、執行任意程式碼的 NAS 應用程式漏洞	45
第 4 章、	資安研討會及活動.....	47
第 5 章、	2021 年 10 月份資安情資分享概況	53

第 1 章、封面故事

Microsoft Azure 雲端服務遭史上最大流量 DDoS 攻擊，瞬間流量高達 2.4Tbps



Microsoft Azure 雲端服務發表資安通報，指出該服務於今（2021 年）8 月時遭到破記錄強大 DDoS 攻擊，瞬間最大資料流量高達每秒 2.4Tbps。

Microsoft Azure 雲端服務日前發表資安通報，指出該服務於今（2021 年）8 月時遭到破記錄的強大分散式服務阻斷（Distributed Denial of Service, DDoS）攻擊，瞬間最大資料流量高達每秒 2.4Tbps；所幸系統成功抵擋這波攻擊，客戶的網站和數位服務並未受到影響。

Microsoft Azure 的網路架構資深主管指出，這波攻擊是同時由超過 70,000 個主要位於亞太地區的僵屍網路節點同步發動攻擊，這些攻擊節點分布於馬來西亞、越南、台灣、日本、中國與美國境內，主要的攻擊目標為 Microsoft Azure 在歐洲地區的某個客戶。

該主管指出，這次 DDoS 攻擊行動主要分為三波攻擊，首先是瞬間流量高達 2.4Tbps 的第一波攻擊，之後的兩波攻擊，其瞬時流量則略有降低，分別為 0.55Tbps 與 1.7Tbps；該主管說 Azure 的攻擊抵禦架構成功擋下這三波攻擊，Microsoft Azure 服務並未因攻擊而發生阻斷。

先前 DDoS 攻擊的瞬間最大流量記錄，是發生在 2020 年 2 月；一次針對 Amazon AWS 系統的攻擊，該次攻擊的瞬間最大流量為 2.3Tbps。

在這次高達 2.4Tbps 的大流量攻擊發生數日後，發生了另一次同樣打破記錄的攻擊活笏；該攻擊係由一個稱為 Meris 的僵屍網路發動，目標是一家將銀行金融服務託管於 Yandex 雲端服務的俄羅斯銀行；其最大同時連線要求數量高達每秒 2,180 萬次。

- 資料來源：

1. Business as usual for Azure customers despite 2.4 Tbps DDoS attack
2. Microsoft said it mitigated a 2.4 Tbps DDoS attack

第 2 章、活動紀事

TWCERT/CC 參與亞太區 APCERT CYBER DRILL 2021 演練



亞太區電腦緊急事件回應小組(Asia Pacific Computer Emergency Response Team, APCERT)於今年(2021)舉辦之 APCERT CYBER DRILL 2021 資安演練活動，已於 8 月 25 日完美落幕。

本次資安演練主題為「提供因釣魚郵件及產業鏈攻擊受害企業之協處與事件調查(Supply Chain Attack Through Spear-Phishing - Beware of Working from Home)」，是以真實資安事件為基礎，將疫情期間企業面臨之資安威脅做為演練情境，參與團隊需處理一個由魚叉式釣魚郵件引發的供應鏈攻擊事件。

本次總共有來自 19 個 APCERT 亞太經濟體，包括台灣、澳洲、不丹、汶萊、中國、香港、印度、印尼、日本、南韓、寮國、馬來西亞、緬甸、菲律賓、新加坡、斯里蘭卡、泰國、越南、東加、哈薩克斯坦、突尼西亞、非洲，共 25 個電腦資安事件處理小組參與了此次演練。亦有來自其他的機構如伊斯蘭合作組織電腦網路危機處理小組、非洲電腦網路危機處理小組的成員，如貝南、埃及、約旦、摩洛哥、奈及利亞、巴基斯坦、突尼西亞的電腦緊急應變小組參與。

台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team /Coordination Center, TWCERT/CC)作為台灣參與此次 APCERT Drill 演練的代表團隊之一，認真達成每個階段的任務目標，為 25 個參與單位中唯一成功完成本次演練各任務。透過參與國際合作的大型演練有助於 TWCERT/CC 優化情資分享流程及事件應變能力，強化台灣資安能量的同時促進資安跨域聯防的正向發展。

- 相關連結：

1. APCERT CYBER DRILL 2021 “SUPPLY CHAIN ATTACK THROUGH SPEAR-PHISHING - BEWARE OF WORKING FROM HOME -”

第 3 章、國內外重要資安事件

3.1、資安趨勢

3.1.1、VirusTotal 分析 8,000 萬筆勒索案例



VirusTotal 近期發表研究報告，自 8,000 萬筆勒索攻擊案例，分析全球勒索攻擊的樣態，並提出分析報告。

據報告指出，這些資料係來自 233 個國家，每天收集 200 萬份以上的報告檔案，累積長達 16 年之久。其中和近年來的勒索攻擊相關的資料筆數達 8,000 萬份以上。

報告說，自 2020 年起開始收集到和勒索相關的報告檔案，顯示有 140 國以上的 VirusTotal 用戶曾遭到勒索攻擊；在這段期間內，有 130 種不同的勒索攻擊軟體家族曾經發動過勒索攻擊。

在勒索攻擊的密度方面，2020 年第一季與第二季，由於 GandCrab 勒索活動十分活躍，形成兩波攻擊高峰；而在 2021 年第二季，由於 Babuk 勒索的大規模活動，又形成另一攻擊高峰。

在攻擊目標的地理分析方面，VirusTotal 報告指出，從以色列收集到的勒索攻擊案例最多，和基數相比多了近六倍，其次是南韓、越南、中國、新加坡、印度、哈薩克、菲律賓、伊朗、英國等。

在 VirusTotal 發現的 130 種不同的勒索攻擊家族中，發動攻擊最頻繁的是最近已停止活動的 GandCrab，在前十名的勒索攻擊家族中佔比高達 78.5%；其次為近來開始大規模發動攻擊的 Babuk (7.61%)、Cerber (3.11%)、Matsnu (2.63%)、WannaCry (2.41%)、Congur (1.52%)、Locky (1.29%)、Tescrypt (1.12%)、Rkor (1.11%)、Reveton (0.70%)。

- 資料來源：

1. RANSOMWARE IN A GLOBAL CONTEXT
2. We analyzed 80 million ransomware samples – here's what we learned

3.1.2、今年針對俄羅斯企業的 DDoS 攻擊，次數較去年大增 250% 以上



俄羅斯最大電信業者日前發表研究報告，指出自今年起針對俄羅斯企業發動的分散服務阻斷攻擊（DDoS）次數，和去年同期相比大增 2.5 倍以上。

俄羅斯最大電信業者 Rostelecom 日前發表研究報告，指出自今年起針對俄羅斯企業發動的分散服務阻斷攻擊（Distributed Denial of Service, DDoS）發生次數，和去年同期相比，大增 2.5 倍以上。

Rostelecom 的報告中指出，該公司於 2021 年 9 月記錄到俄羅斯有史以來最嚴重的 DDoS 攻擊次數；針對俄羅斯企業發動的 DDoS 攻擊次數，在該月發生的次數即佔今年以來所有攻擊次數的 90%，嚴重程度不容忽視。

過去三年的前三季，針對俄羅斯企業的 DDoS 攻擊次數不斷以倍數成長；2019 年的 DDoS 攻擊次數尚低於 10,000 次，到了 2020 年突破 20,000 次大關，而在 2021 年前三季發生的 DDoS 攻擊次數接近 45,000 次。

若以遭到攻擊的對象來分析，2020 年時遭到 DDoS 攻擊的，主要是遊戲相關產業，這是因為 2020 年時疫情開始肆虐，許多人因封城而關在家中之故；到了今年，遭到攻擊的大宗產業則變成線上交易、金融服務與公部門相關單位。

從攻擊強度來看，和去年相比，今年的 DDoS 攻擊強度比去年加強了 26%，攻擊持續時間也從去年的持續 3 天增加到今年的 4.5 天；原因是來自受駭侵團體控制並用以發動攻擊的僵屍網路，其規模和節點數量持續擴大之故。

從攻擊手法的類型來看，前三大攻擊類型和過去相同，分別是 UDP 洪水攻擊（41%）、FRAG 攻擊（22%）與 SYN 洪水攻擊（20%）。

- 資料來源：
 1. Отчет о DDoS-атаках на российские компании в 1-3 квартале 2021 года
 2. DDoS attacks against Russian firms have almost tripled in 2021

3.2、新興應用資安

3.2.1、Coinbase 因簡訊二階段驗證系統錯誤，導致六千名用戶資產遭竊



全球第二大的加密貨幣交易所 **Coinbase**，日前發生駭侵者利用該公司多階段登入驗證錯誤，致使六千多名顧客存在該交易所中的加密貨幣遭竊的事件。

在 Coinbase 發送給受害用戶的說明中指出，這次攻擊事件發生在 2021 年 3 月與 5 月之間；駭侵者透過先前取得的用戶帳號與個人資料，包括 Email 地址、登入密碼、電話號碼來存取受害者的帳戶，並且竊走存在帳戶內的加密貨幣。

Coinbase 表示，駭侵者係利用該公司的簡訊帳號存取權取回系統的漏洞，透過簡訊取得回復帳號所需的二階段登入驗證碼。

至於這次駭侵事件中，駭侵者是如何先行取得受害用戶的各項帳戶內個資，Coinbase 並未確認原因；但 Coinbase 認為這些用戶曾經遭到駭侵者以釣魚攻擊手法騙取相關登入資訊與個資的可能性相當高；在今年（2021）1 月時，也曾發生過駭侵者透過釣魚郵件與假冒 Coinbase 登入網站的攻擊事件。

由於駭侵者可以存取受害用戶的 Coinbase 帳戶，因此除了加密貨幣被竊之外，這些受害用戶存於 Coinbase 的各種資料，包括全名、Email 地址、住家地址、出生年月日、帳號活動使用的連線 IP、交易記錄、持有資產與帳戶餘額等資訊，也都全部遭駭侵者掌握。

這起駭侵事件中，遭受損失的六千多名 Coinbase 用戶被竊的加密貨幣總額有多少，Coinbase 並未對外公開，而在寄發給受害用戶的道歉信件中，Coinbase 表示會全額賠償用戶被竊的損失。

- 資料來源：

1. Subject: Unauthorized Access to Your Coinbase Account
2. Hackers rob thousands of Coinbase customers using MFA flaw

3.2.2、OpenSea NFT 交易所漏洞，造成用戶加密貨幣遭竊



資安廠商發現熱門 NFT 交易所 OpenSea 存有一個漏洞，駭侵者可以藉以竊走 NFT 交易者錢包中所有的加密貨幣。

資安廠商 Check Point 旗下資安研究人員，近日發現熱門「非同質性加密貨幣」(Non-Fungible Token, NFT) 交易所 OpenSea 存有一個漏洞；駭侵者可以透過特製的 NFT，藉以竊走 NFT 交易者錢包中所有的加密貨幣。

資安專家指出，駭侵者發動攻擊的方法相當簡單，只要製作一個含有惡意程式碼酬載的 NFT，等待受害者打開該 NFT 來檢視內容即可。

Check Point 在發現許多 OpenSea 用戶遭駭後，開始研究 OpenSea 的平台機制。專家發現 OpenSea 帳號係透過第三方加密貨幣錢包軟體（如 MetaMask）來運作，用戶的任何動作，例如在某個 NFT 藝術品上按讚，都會觸發錢包軟體對 OpenSea 發出登入要求。

Check Point 的資安專家，上傳一個夾帶有一段 JavaScript 惡意程式碼的 SVG 檔到 OpenSea 平台上，然後點按該圖檔，瀏覽器便會自動開啟一個新頁籤，並且在一個名為 storage.opensea.io 的網域中執行這段 JavaScript 程式碼；而資安專家便在 SVG 中安插另一段程式碼，可以直接開啟用戶的加密貨幣錢包。

因此，資安專家指出，攻擊者可以藉由空投活動，發送夾帶惡意程式碼的特製 NFT，讓受害者誤以為自己獲得 NFT 空投獎勵，駭侵者即可讓受害者開啟其加密貨幣錢包；此時可以再顯示另一個彈跳視窗，內含發送錢包內加

密貨幣到駭侵者指定位址的指令，如果受害者不細檢閱內容，按下發送按鈕，就會將自己的加密貨幣轉帳給駭侵者。

Check Point 在發現此漏洞後，於 9 月 26 日通知 OpenSea；雙方的資安人員很快在 1 小時後修復此漏洞；但目前無法估計因此漏洞造成的損失總額。

- 資料來源：

1. Check Point Research Prevents Theft of Crypto Wallets on OpenSea, the World's Largest NFT Marketplac
2. OpenSea NFT platform bugs let hackers steal crypto wallets

3.3、國際政府組織資安資訊

3.3.1、全球 31 國宣示共同投入打擊加密貨幣非法匯兌與洗錢管道



全球 31 國在反勒索攻擊國際會議上共同聲明，將採取行動，加強查緝各種遭勒索駭侵團體用以進行贖款金流的加密貨幣支付管道。

全球 31 國的資安與執法單位，在日前於線上舉辦的反勒索攻擊國際會議（Counter-Ransomware Initiative）上共同聲明，將採取行動，加強查緝各種遭勒索駭侵團體用以進行贖款金流的加密貨幣支付管道，以打擊日益猖獗的勒索攻擊事件。

這個會議是由美國白宮國家安全會議（The White House National Security Council）發起，以因應勒索攻擊對全球關鍵基礎設施帶來的嚴重威脅。

參加此一國際會議的國家，除了美國以外，還有澳大利亞、巴西、保加利亞、加拿大、捷克、多明尼加共和國、愛沙尼亞、歐盟、法國、德國、印度、愛爾蘭、以色列、義大利、日本、肯亞、立陶宛、墨西哥、荷蘭、紐西蘭、奈及利亞、波蘭、韓國、羅馬尼亞、新加坡、南非、瑞典、瑞士、烏克蘭、阿拉伯聯合大公國、英國。

大會指出，目前已公開的勒索攻擊贖款，透過加密貨幣轉帳支付的總金額，在最近兩年達到 5 億美元以上，其中 2020 年全年為 4 億美元，2021 年第一季為 8,000 萬美元。因此，針對這些地下加密貨幣匯兌管道實施嚴格查緝，將可有效打擊勒索團體的不法獲利來源，達成實質嚇阻勒索駭侵攻擊的

目標。

大會指出，目前全球各國針對此類加密貨幣不法匯兌與洗錢的執法行動與強度不一，使得勒索攻擊團體仍有機可乘；這次大會會後，將會加強各國之間在虛擬資產與反洗錢等作業之間的協調；各國的金融監理、金融調查、司法與執法單位之間的監理、監督、調查、執法的行動將會更為一致。

- 資料來源：

1. Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting
2. Governments worldwide to crack down on ransomware payment channels

3.3.2、美國資安主管機關示警：供水暨廢水處理設施正遭到強力勒索攻擊



美國資安主管機關近日發出資安通報，警告美國各地的自來水供水與廢水處理機構，應對近期發生中的駭侵攻擊提高警覺。

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) 近日發出資安通報，警告美國各地的自來水供水與廢水處理機構，應對近期正在發生的駭侵攻擊提高警覺。

該警訊指出，美國各資安相關單位，包括聯邦調查局 (Federal Bureau of Investigation, FBI) 、 CISA 、環保署 (Environmental Protection Agency, EPA) 、國家安全局 (National Security Agency, NSA) 近期發現一些已知或未知的駭侵團體，已開始針對美國各地的供水與廢水處理單位使用的資訊系統 (IT) 和營運技術 (OT) 發動各式駭侵攻擊。

供水與廢水處理系統，為美國法定 16 種關鍵基礎設施之一，一旦遭駭擊攻擊造成這些設施無法正常運作，恐將造成極嚴重的後果，並對國家安全、經濟安全與公共衛生造成劇烈影響。

在這份警告中列出多個過去曾發生過的供水系統攻擊事件，例如 2021 年 8 月時，駭侵者利用 Ghost 變種勒索軟體，攻擊加州一處供水 / 廢水處理單位、2021 年 7 月時緬因州的供水 / 廢水處理單位遭到 ZuCano 勒索軟體攻擊、2021 年 3 月則是內華達州的供水 / 廢水處理單位遭不明勒索軟體攻擊。

2019 年 3 月時，在堪薩斯州也發生過離職員工利用尚未失效的登入資訊，企圖在供水系統中投放毒性物質的案件，所幸及時發現，未能得逞。

資安主管機關特別要求美國各地的供水 / 廢水處理單位人員，應採取行動，避免遭到駭侵攻擊；這些行動包括不可點擊可疑連結、保護並監控 RDP 連線、立即並隨時更新作業系統與應用軟體、使用強式密碼與多階段登入驗證等。

- 資料來源：

1. Ongoing Cyber Threats to U.S. Water and Wastewater Systems
2. CISA outlines cyberthreats targeting US water and wastewater systems
3. US government discloses more ransomware attacks on water plants

3.3.3、美國推出新禁令禁止駭侵工具出口，以防用於資安攻擊與人權侵害



美國商務部旗下的產業與安全局日前發布命令，禁止美國企業將各種駭侵工具出口或轉售給任何可能透過惡意駭侵活動，以強化威權統治與侵害人權的對象。

美國商務部（US Department of Commerce）旗下的產業與安全局（Bureau of Industry and Security, BIS）日前發布命令，禁止美國企業將各種駭侵工具出口或轉售給任何可能透過惡意駭侵活動，以強化威權統治與侵害人權的對象。

該命令將在 90 天內生效，將會以國家安全與反恐為由，有效禁止各種資安產品的出口與轉售，將包括各種相關軟體與硬體工具在內。

該命令同時也附帶新規定的資安產品出口授權例外名單（License Exception Authorized Cybersecurity Exports），列出各種資安與駭侵相關工具的禁止出口國名單；要出口相關產品到這些國家，包括中國與俄羅斯等國，必須事先取得主管機關授權同意。

產業與安全局（BIS）官員表示，美國政府反對濫用技術以侵害人權，或進行各種惡意網路攻擊活動；新推出的規定將有助於確保美國企業的產品與服務，不會被用於加強這些威權專制活動。

產業與安全局強調，禁止出口的這些資安與駭侵相關產品，經常被各專制政權用以進行監控、間諜活動，以及各種阻擾網路正常運作的攻擊活動等等。

該局也說，這項規定符合瓦森納協議（Wassenaar Arrangement）的精神，該協議規範西方各國針對傳統武器及軍商兩用貨品的多邊出口進行管制，有 40 個國家簽署這項協議。

美國商務部長 Gina M. Raimondo 也指出，新規定主要是為了防止惡意駭侵者使用這些工具，針對美國公私單位發動攻擊，傷害美國的國家安全；美國將會持與各國合作，阻止這類技術擴散並用於各種資安攻擊與人權侵害活動。

- 資料來源：

1. THE DEPARTMENT OF JUSTICE'S IT SYSTEM ATTACKED BY RANSOMWARE
2. Ransomware encrypts South Africa's entire Dept of Justice network

3.3.4、荷蘭警方發函警告駭侵者停止行動，回頭是岸，以免遭司法控訴



荷蘭警方日前發函給近三十個涉嫌利用網路攻擊服務，意圖發動 DDoS 攻擊的「客戶」，告知如果繼續發動網路攻擊，將面臨司法控訴。

荷蘭警方日前發函給近三十個涉嫌利用網路攻擊「服務」網站，意圖針對特定目標發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）攻擊的「客戶」，告知如果繼續發動網路攻擊，將面臨司法控訴。

荷蘭警方發送給這些攻擊者的信件內文指出，警方已經將這些攻擊者登錄在案，如果未來持續發生類似的攻擊事件，警方將會正式將攻擊者移送法院偵辦；攻擊者如不立即停止攻擊行動，將面臨後續的司法行動，包括正式定罪、留下犯罪記錄、攻擊工具（如電腦或 / 及筆電）將遭沒入等。

所有接獲荷蘭警方通知的「客戶」，都使用 minesearch.rip；該網站提供這些客戶各種發動 DDoS 攻擊的「服務」和工具，可以讓攻擊者選擇要攻擊的對象；目前該網站已經停止運作，警方也正在調查該網站涉及的攻擊事件。

多名攻擊發動者，過去曾透過該網站的「服務」，對多個公私部門的目標發動 DDoS 攻擊得逞。去年 7 月 30 日，荷蘭警方搜索兩個 19 歲嫌疑人的住處，這兩人疑為該網站的關係人。荷蘭警方於去年 10 月一口氣查緝並下線了 15 個用以發動 DDoS 攻擊的網站。

警方說，採用這種先行警告的方式，是希望給予這些可能十分年輕的攻擊發動者一個改過向善的機會；有些年輕人只是想要證明自己的技術能力，

荷蘭警方同時提供多種類似白帽駭客的計畫，包括電腦軟硬體、遊戲與網路犯罪的白帽駭侵活動，以期導正這些年輕駭侵者，將其技能用於正途之上。

- 資料來源：
 1. Kopers van DDoS-aanval krijgen waarschuwing van cybercrimeteam
 2. Dutch police send warning letters to DDoS booter customers

3.4、社群媒體資安近況

3.4.1、駭侵團體經常利用釣魚信件，以 Cookie 竊取軟體強奪 YouTuber 帳號



Google 發表資安通報警告 YouTube 創作者，應嚴加提防各種會竊取 YouTube 登入資訊與 cookie 的惡意軟體與駭侵攻擊。

Google 近日發表資安通報，警告全球 YouTube 創作者，應嚴加提防各種會竊取 YouTube 登入資訊與 cookie 的惡意軟體與駭侵攻擊，以免自己苦心經營的 YouTube 頻道遭到駭侵者奪取。

Google 的威脅分析團隊 (Google Threat Analysis Group) 在報告中指出，該團隊自 2019 年起開始針對各種意圖詐取錢財，針對 YouTube 創作者發動釣魚攻擊的駭侵活動進行調查與查緝工作。

報告說，該團隊發現一個駭侵團體組織，自某俄語駭侵討論區中招募組織成員，鎖定經營有成的 YouTuber，詐稱提供合作機會，要 YouTuber 試用新推出的測試版防毒軟體、VPN、音樂播放程式、相片編輯軟體、線上遊戲等，接著透過這些「測試用軟體」中夾帶的惡意軟體，竊取 YouTuber 苦心經營的 YouTube 頻道控制權，之後用以轉售牟利，或是用來推廣各種加密貨幣相關詐騙活動。

報告指出，這些惡意軟體一旦安裝在目標用戶的電腦上，就會竊取瀏覽器中的相關 cookie，並上傳到駭侵者擁有的控制伺服器內；用來竊取 cookie 的軟體，很多都可直接在 Github 上取得。

該團隊指出，該團隊與 Gmail 和 YouTube 團隊合作，自 2021 年 5 月起，截獲 99.6% 透過 Gmail 傳遞的這類釣魚郵件，阻擋的釣魚信件多達 160 萬封，並對 2,400 個可能夾帶惡意軟體的信件夾檔發出警訊，同時成功取回近 4,000 個被駭侵團體奪取的 YouTube 帳號。

Google 指出，YouTuber 應該提高警覺，不要任意點擊任何不明的連結，同時以二階段登入驗證來保護自己的 YouTube 帳號，以免苦心經營的頻道遭人輕易竊走。

- 資料來源：
 1. Phishing campaign targets YouTube creators with cookie theft malware
 2. Google: YouTubers' accounts hijacked with cookie-stealing malware

3.4.2、全球最大遊戲直播平台 Twitch 遭駭，多項資料遭駭侵者公開



一名匿名駭客宣稱駭入遊戲直播平台 Twitch，取得該站網站、應用程式等所有原始碼、影音直播主付款記錄、專屬開發工具等重要資料。

一名匿名駭客宣稱成功駭入全球最大遊戲社群直播平台，數年前被 Amazon 收購的 Twitch，取得該站網站、應用程式等所有原始碼、影音直播主付款記錄、專屬開發工具等重要資料。

該名駭侵者在美國鄉民網站 4chan 貼出一個容量高達 125GB 的 torrent P2P 檔案分享連結，該批檔案經多家媒體與多位資安專家證實，確實是自 Twitch 內部流出的檔案。

這批外洩檔案的詳細內容，包括 Twitch 整個網站的原始程式碼、可追溯至開站初期的所有程式碼變更記錄、自 2019 年起支付給影音直播主的付款記錄、Twitch 在各桌機、手機與電視遊樂器平台的應用程式、內部專用的開發工具、內部使用的 Amazon Web Services 服務、包括 IGDB 與 CurseForge 等 Twitch 旗下所有產品與頻道、Amazon Game 服務尚未推出上市的 Steam 競爭產品 Vapor、Twitch 為了防駭使用的「紅隊」駭侵模擬測試工具等。

許多人透過 torrent P2P 下載工具取得該批檔案後，也發現這批資料中甚至包括已加密的用戶登入密碼。

Twitch 在接受媒體採訪時表示，該公司確實知道所有資料全部遭外洩一事，並指出駭侵事件可能發生於 2021 年 10 月 4 日；該公司正在緊急調查整起事件的原因與過程，並將隨時公告最新調查結果。

資安專家指出，鑑於用戶密碼也已遭竊，建議所有 Twitch 用戶，務必盡速變更登入密碼，並且啟用二階段登入驗證，以防止帳號遭到取得外洩資訊的不明駭侵者利用於資安攻擊。

- 資料來源：

1. Twitch@Twitch
2. Twitch source code and creator payouts part of massive leak
3. The entirety of Twitch has reportedly been leaked

3.4.3、YouTube 遭駭客上傳惡意影片，內含登入資訊竊取惡意



資安廠商發現有駭侵團體大量製作

YouTube 影片，在影片描述中夾帶惡意軟

體連結，用以騙取受害者的各種登入資訊。

資安廠商 Cluster 25 旗下的資安研究人員，近來發現有駭侵團體大量製作 YouTube 影片，在影片描述中夾帶惡意軟體連結；受害者如果不慎點擊，各種登入資訊就會遭到竊取。

研究人員指出，以 YouTube 影片來吸引觀眾點擊惡意連結，是常見的駭侵攻擊手法；其攻擊手法是在 YouTube 中大量放置各種熱門主題影片，例如常見軟體或服務的操作方式、如何免費挖掘比特幣、破解正版軟體保護、遊戲作弊密技、VPN 使用方法等等。

研究人員表示，這次發現的 YouTube 惡意連結攻擊，主要是以特洛伊木馬惡意軟體的植入，來竊取受害用戶使用在各種軟體與服務的登入資訊。

研究人員說，最近發現的大規模 YouTube 影片攻擊活動，在同一時間內有兩波同時進行；其中一波是以 RedLine 惡意軟體為主，另一波使用的惡意軟體則是 Raccoon Stealer。

研究人員發現這波攻擊行動，散布惡意 YouTube 影片的速度極快；他們觀察到在短短 20 分鐘以內，某個遭駭侵團體控制的惡意 YouTube 帳號，就新建了 81 個 YouTube 頻道，上傳的影片數量高達 100 支。

另外，駭侵團體還會使用竊得的受害者 Google 帳號，在 YouTube 中上傳更多含有惡意連結的影片，進一步擴大接觸潛在受害者的範圍，也使 Google

/ YouTube 更不容易查緝這類惡意影片。

Google 表示已經獲悉這些案例利用 YouTube 發動駭侵攻擊的情形，且正在阻擋這類活動的擴散；資安專家也指出，這個案例顯示在網路上下載來路不明軟體的潛在危險性。包括 Google 與資安專家都呼籲用戶，從網路上下載任何軟體時，應多方確認安全性，包括是否自軟體發行商的官方管道下載、網址是否正確等，千萬不要貪小便宜下載盜版或破解軟體。

- 資料來源：

1. YouTube Users Beware: Malicious Videos Spread Password Stealing Malwares—Here's How to Avoid
2. Massive campaign uses YouTube to push password-stealing malware

3.5、行動裝置資安訊息

3.5.1、韓國第二大電信業者 KT Corporation 因路由設定錯誤發生服務中斷

TWCERT/CC

韓國第二大電信業者
KT Corporation
因路由設定錯誤
發生服務中斷

韓國電信業者 KT Corporation 日前發生大規模通訊中斷事件，導致全韓國近 1650 萬用戶無法使用其電信與網路通訊服務，時間長達 40 分鐘。

韓國第二大電信業者 KT Corporation 日前發生大規模通訊中斷事件，影響範圍遍及韓國全境，導致全韓國近 1650 萬用戶無法使用其電信與網路通訊服務，時間長達 40 分鐘。

這次斷訊事件導致韓國各地依賴網路通訊的相關公共服務與事業受到影響，許多學生無法透過視訊會議上課、網路送餐服務無法運作、各地醫療機構無法存取病患的病歷資料、商家的信用卡刷卡收單業務也無法運作。

由於最近經常發生電信業者與其他公私營單位，因為遭到駭侵者發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）的事件，首爾市政府資安調查團隊，在事件發生後立即前往 KT Corporation 總部進行調查；不過 KT Corporation 稍後對外界表示，事件的發生是因為內部路由設定錯誤，造成服務中斷所致。

KT Corporation 雖然在 40 分鐘內修復這次斷線事件，但並沒有對外說明路由設定錯誤的原因；不過外界推測很可能是因為 BGP 路由設定錯誤，才造成服務中斷。

BGP 設定錯誤對網路服務可能造成極大影響，例如最近 Facebook 就因為 BGP 設定發生錯誤，導致 Facebook 旗下所有服務，包括 Facebook 本身、Messenger、Instagram 和 WhatsApp 服務全面停擺達數小時之久，造成該公司與生態系中其他第三方廠商與用戶的損失。

此外，在 KT 斷線期間，用戶大量湧入韓國另外家主要電信業者 SK Telecom 與 LG Uplus，也造成這兩家業者的網路服務發生過載現象，連線品質與穩定程度也遭到衝擊；甚至讓外界懷疑這兩家電信業者也同時遭到 DDoS 駭侵攻擊。

- 資料來源：

1. KT suffers major network outage nationwide
2. Routing error caused network outage, South Korean telco KT says

3.5.2、Google 推出 10 月 Android 資安修補例行更新，修復 41 個資安漏洞

Google推出2021年10月Android
資安修補例行更新，修復41個資安漏洞



TWCERT/CC

**Google 近期推出 Android 2021 年 10 月
資安更新，一共修補 41 個各種資安漏洞，
其中有三個屬於嚴重等級。**

Google 近期推出 Android 2021 年 10 月資安更新，一共修補 41 個各種資安漏洞，其中有三個屬於嚴重等級，其他的漏洞則屬於高等級。

在這次的例行資安漏洞修補更新中，三個屬於「嚴重」（critical）等級的漏洞分別是：

- CVE-2021-0870：存於 Android 系統中，可導致駭侵者在具有系統權限的執行程序中，遠端執行任意程式碼；
- CVE-2020-11264：存於高通（Qualcomm）無線網路子系統的嚴重資安漏洞；
- CVE-2020-11301：同樣存於高通的無線網路子系統內，在安全的網路內可接受未加密（純文字）的資料。

Google 這次修復的 41 個漏洞，目前都沒有接獲已遭駭侵者大規模濫用的報告，也沒有發現利用這些漏洞發動攻擊的惡意軟體。

另外，Google 固定在每月 5 日例行推出的每月 Android 資安漏洞更新修補，雖然並不針對特定 Android 版本發行，而是適用於 Android 8.1 到 Android 11 均可適用，然而各 Android 用戶裝置內的 Android 作業系統，大多

是由各該裝置廠商修改維護，因此用戶尚需等待裝置廠商推送作業系統更新時，才能得到修補；用戶需密切注意裝置更新通知，並在收到通知後立即進行更新。

鑑於有許多老舊的 Android 裝置早已被原廠列為終止支援機型，這類裝置多半無法取得來自原廠的系統資安漏洞更新；如果用戶的 Android 裝置過於老舊，也應考慮汰除更換，以免成為資安攻擊的目標。

- 資料來源：

1. Android 安全公告 - 2021 年 10 月
2. Android October patch fixes three critical bugs, 41 flaws in total

3.5.3、上千萬 Android 用戶遭 151 支惡意 App 攻擊，擅自訂閱高價服務



資安廠商近日再次發現有多支 Android App 內含惡意訂閱軟體，會在用戶不知情的情況下，偷偷訂閱高價服務，造成用戶損失。

資安廠商 Avast 旗下的資安研究人員，近日再次發現有高達 151 支 Android App，內含惡意訂閱軟體，會在用戶不知情的情況下，偷偷訂閱高價服務，造成用戶損失。

Avast 的資安研究人員稱這波攻擊行動為「UltimaSMS」。研究人員指出攻擊者透過 151 支假裝成各種熱門類型的 Android App，包括購物優惠、遊戲、自定鍵盤、QR Code 掃描工具、影片與相片編輯工具、騷擾電話阻擋工具、相機特效濾鏡等等，吸引用戶下載安裝。

當用戶安裝好這些惡意 Android App 後，這些 App 會讀取手機的某些資料，如 IMEI 設備編號或所在地座標資訊，自動切換到用戶使用的語系後，接著要求用戶輸入手機號碼與 Email 地址，以「啟用軟體的功能」。

這些惡意軟體取得受害者的手機號碼，並且取得必要的權限同意後，就會暗地裡訂閱某個透過簡訊提供的高價服務，訂閱費用高達每月 40 美元；攻擊者可以從這些訂閱服務的分潤機制來獲取不法暴利。

Avast 說，由駭侵者用來發動攻擊的 151 支 App 中，有高達 80 支在 Google 官方的 Play Store 中上架成功；儘管這些 App 在 Google Play Store 中獲得的用戶評價極差，許多 App 甚至不提供任何宣稱的功能，但下載量還是十分驚人，合計高達 1,000 萬次以上。

根據 Sensor Tower 的統計指出，這些惡意 Android App 的受害者，以埃及、沙烏地阿拉伯、巴基斯坦等國的人數最多，合計達 700 萬人，美國也有近 17 萬人受害。

- 資料來源：
 1. UltimaSMS: A widespread premium SMS scam on the Google Play Store
 2. Millions of Android users targeted in subscription fraud campaign

3.6、軟體系統資安議題

3.6.1、新發現 APT 駭侵團體 ChamelGang，攻擊多國能源、航空產業與政府機關



資安廠商發現新的 APT 駭侵團體，長期系統化的方式，攻擊俄羅斯、美國、印度、尼泊爾、台灣、日本等國家的政府機關、能源產業、航空業與其他製造業。

資安廠商 Positive Technologies 旗下的資安研究團隊 Positive Technologies Expert Security Center (PT ESC)，日前發表研究報告，指出該單位的資安專家，近來發現新的進階持續威脅 (Advanced Persistent Threat, APT) 駭侵團體，長期以系統化的方式，持續攻擊俄羅斯、美國、印度、尼泊爾、台灣、日本等國家的政府機關、能源產業、航空業與其他製造業。

PT ESC 的資安專家指出，雖然俄羅斯等國的能源產業和航空產業，原本就是駭侵團體經常攻擊的目標，但該單位這次發現的攻擊行動，對這些產業造成嚴重的損害；去年發生的攻擊案件中，84% 的攻擊行動，其目標為資料竊取；這些企業的防護措施無法有效提供保護能力，以致駭侵者成功入侵的機率高達九成以上。

PT SEC 進一步指出，該團體每次成功的駭侵攻擊，不但可以竊走重要的公司機密資料，包括客戶、上下游協力廠商和員工的機敏資訊、郵件通訊內容與內部文件之外，還能取得重要伺服器與基礎設施裝置的控制權。

這個新發現的 APT 駭侵團體稱為「ChamelGang」，在一次攻擊活中，該團體利用一個早就由 RedHat 在四年前修補完成的老舊 RCE 漏洞 CVE-2017-

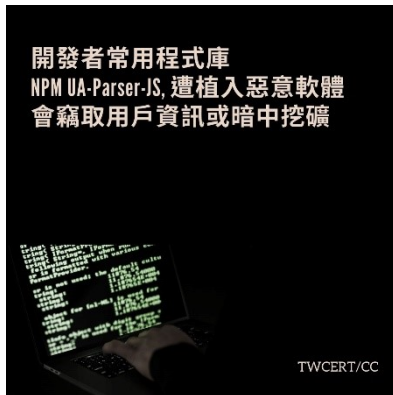
12149，先入侵子公司用的開源軟體，再以極快的速度，在兩周後成功入侵母公司系統，自目錄伺服器中取得密碼字典檔與管理者權限，在系統中活動長達三個月，竊取各種資料而未遭發現。

其他攻擊案例也包括使用 Microsoft Windows Server 日前被發現的嚴重漏洞 ProxyShell 發動攻擊，躲過多數防毒防駭系統的偵測，成功攻破受害公司的郵件伺服器。

- 資料來源：

1. Positive Technologies Uncovers New APT Group Attacking Russia's Fuel and Energy Complex and Aviation
2. New cyber-criminal group discovered targeting government servers, fuel, energy and aviation companies

3.6.2、NPM UA-Parser-JS 遭植入惡意軟體，會竊取用戶資訊或暗中挖礦



程式開發者經常使用的某個 NPM 程式庫，近日遭到駭侵者植入惡意軟體，用以挖掘加密貨幣，或是竊取用戶登入資訊。

程式開發者經常使用的 NPM 程式庫 UA-Parser-JS，近日遭到駭侵者植入惡意軟體，用以發動供應鏈攻擊，利用受害用戶的設備挖掘加密貨幣，或是竊取用戶登入資訊。

被植入惡意軟體的 NPM 程式庫，是經常用於爬梳瀏覽器的 user agent 資訊，以確認網站瀏覽訪客使用的瀏覽器類型、解析引擎、作業系統、處理器、裝置類型或型號等資訊之用。

這個程式庫經常用於各種 Windows、Linux 軟體開發上，在 2021 年 10 月的每周下載次數高達 2,400 萬次，有數千個軟體開發專案，都使用了 UA-Parser-JS 程式庫，使用者包括 Facebook、Microsoft、Amazon、Instagram、Google、Slack、Mozilla、Discord、Elastic、Intuit、Reddit 等知名公司、軟體與服務。

據專業資安媒體 BleepingComputer 報導指出，駭侵者事先竊得了 NPM 伺服器的登入權限，接著在本月 22 日將含有惡意程式碼的 NPM UA-Parser-JS 程式碼上傳到伺服器中；隔天該專案的合法擁有者 faisalman 在 Github 上發文，指出他的 Email 信箱突然遭到來自數百個網站的垃圾郵件攻擊，這才發現他控制的 NPM 帳號已經被竊。

faisalman 指出，經過調查後，發現 UA-Parser-JS 的 0.7.29、0.8.0、1.0.0 等三個版本，都遭到駭侵者植入惡意軟體；BleepingComputer 的報導也列出多個可能受到影響的軟體，包括 Firefox、Apple Safari、Outlook、FileZilla、Opera、Chrome 等使用非常普遍的軟體都包括在內。

目前 NPM 已經緊急推出修復的 UA-Parser-JS 程式庫，版本分別為 0.7.30、0.8.1、1.0.1；使用受影響版本的開發者，應立即撤回已發行的版本，改用未遭植入惡意軟體的新版 UA-Parser-JS 重新編譯；一般用戶如果發現自己的 Windows 系統上有 jsextension.exe 或 create.dll，應立即刪除並更改自己使用的各種密碼，而 Linux 用戶則應掃描系統上是否存有 jsextension 檔案，如果發現亦應立即刪除並修改自己的各種登入密碼。

- 資料來源：

1. Security issue: compromised npm packages of ua-parser-js (0.7.29, 0.8.0, 1.0.0) - Questions about de
2. Popular NPM library hijacked to install password-stealers, miners

3.6.3、國內電腦設備品牌大廠遭兩次駭侵攻擊，多種內部機敏資訊遭竊



國內電腦設備品牌大廠於一周內，連續遭到同一駭侵團體兩次發動駭侵攻擊；該公司已緊急下線存有漏洞的伺服器。

國內電腦設備品牌大廠於一周內，連續遭到同一駭侵團體兩次發動駭侵攻擊；該公司已緊急下線存有漏洞的伺服器，但駭侵者說，該公司在其他國家的據點，仍有漏洞可資發動攻擊。

發動最近這兩波攻擊的駭侵團體自稱為「Desorden」。Desorden 在成功入侵該公司在印度據點的售後服務伺服器後，曾經發信給媒體記者高調宣傳此事；不到一星期後，資安媒體 BleepingComputer 再次收到 Desorden 來信，指出該團體再次成功駭入該公司所屬的伺服器，這次的受害者是在台灣的總部電腦設備。

據 BleepingComputer 的報導指出，Desorden 駭侵團體自稱，於 10 月 15 日時自該公司台灣的伺服器中竊得員工資料與產品相關資訊；該團體還展示了內部入口網站的圖片，以及含有員工登入資訊的 CSV 檔案。

Desorden 在首次駭入印度據點時，從該公司的伺服器中竊得超過 60GB 的資料，資料內容包括各種客戶、企業內部資料與財務資料、供應商與零售商登入該公司系統用的登入資訊等等。

在印度的駭侵事件發生後，該公司對外表示已立即開始進行調查，並對公司所屬系統進行資安掃描；但一周後台灣總部的系統再次遭同一駭侵團體駭入。Desorden 駭侵團體宣稱，不會對第二次的駭侵攻擊要求額外贖金；但

他們指出在馬來西亞和印尼據點的伺服器，仍舊存有漏洞，可以用來發動攻擊。

- 建議採取資安強化措施

1. 使用防毒軟體，並及時更新系統、軟體和應用程式：攻擊者通常利用未修補的漏洞來訪問未經授權的系統和網路，以執行後續惡意活動。
2. 若不幸遭受駭侵攻擊，建議立即斷開受感染設備與所有網路的連接，無論是有線、無線還是基於行動網路。在非常嚴重的情況下，可考慮關閉 Wi-Fi、禁用任何核心網路連接及交換機，以及斷開 internet 連接。
3. 定期將資料進行備份，並依照 3-2-1 備份原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。利用備份進行還原之前，需確認該備份沒有含惡意軟體，若已經確認備份和連接它的設備是乾淨的，則恢復工作應該只從備份進行。
4. 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；遭受攻擊後，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. Acer hit with second cyberattack in less than a week, Taiwanese authorities notified
2. Acer hacked twice in a week by the same threat actor
3. 勒索軟體防護專區

3.7、軟硬體漏洞資訊

3.7.1、Apache HTTP Server 修復可導致指定路徑外檔案遭竊的嚴重 0-day 漏洞



Apache HTTP web server 遭發現已大規模用於駭侵攻擊的嚴重 0-day 資安漏洞，可能有超過十萬台網頁伺服器曝露於攻擊風險中；Apache 已緊急修復此漏洞。

廣獲全球網站管理者採用的開源網頁伺服器軟體 Apache HTTP web server，日前遭發現已大規模運用於駭侵攻擊的嚴重 0-day 資安漏洞；可能有超過十萬台網頁伺服器曝露於攻擊風險中；Apache 已緊急修復此漏洞。

存有此 0-day 漏洞的 Apache web server 版本為 2.4.49，該漏洞為一種路徑穿越與檔案洩露漏洞；駭侵者可以利用此漏洞來存取指定 root 路徑之外，且未設定為禁止存取的檔案；這可能會造成駭侵者取得網站的各種機密檔案，例如原始碼或 CGI 程式碼等等。

這個 0-day 漏洞據報已遭駭侵者大規模濫用於攻擊活動。據 Shodan 的研究報指出，在整個 Internet 上有超過 112,000 台安裝存有漏洞 Apache web server 的網站，曝露於攻擊風險之中，而這些網站遍布全球各地。

Apache 在發現 CVE-2021-41773 與 CVE-2021-42013 漏洞後，先是緊急推出 Apache HTTP Server 2.4.50，但很快發現這個新版本的修補能力不夠完整，駭侵者還是可透過類似的方法來發動攻擊，取得指定路徑外的檔案；Apache 很快又推出了更新的 Apache HTTP Server 2.4.51 版，以完全解決該漏洞造成的風險。

採用 Apache HTTP Server 的網站管理者，應立即採取行動，將使用中 Apache HTTP Server 的版本，更新至 2.4.51 及其後版本，以避免遭到駭侵者利用此 0-day 漏洞發動攻擊。

- CVE 編號：CVE-2021-41773、CVE-2021-42013
- 影響產品/版本：Apache HTTP Server 2.4.49 與 2.4.50
- 解決方案：升級至 Apache HTTP Server 2.4.51 及之後版本

- 資料來源：
 1. Apache HTTP Server 2.4 vulnerabilities
 2. Over 100,000 Apache HTTP Servers Affected by Actively Exploited Zero-Day Flaw
 3. Apache emergency update fixes incomplete patch for exploited bug

3.7.2、微軟要求系統管理員更新 PowerShell，以修補 WDAC 資安防護跳過漏洞



Microsoft 要求系統管理者立即採取行動，修補 PowerShell 7 的兩個資安漏洞，以防止駭侵者利用這兩個漏洞，跳過 WDAC 的資安防護功能。

Microsoft 日前發布資安通報，要求系統管理者立即採取行動，修補 PowerShell 7 的兩個資安漏洞，以防止駭侵者利用這兩個漏洞，跳過 Windows Defender Application Control 的資安防護功能，取得未編碼的純文字登入資訊。

Windows Defender Application Control (WDAC) 是一種用來防止惡意軟體執行的機制，啟動 WDAC 後，只有受信任的應用程式與驅動程式可以執行，而 PowerShell 會限制只能存取部分 Windows API。

然而駭侵者可以利用 CVE-2021-0951 這個漏洞，讓 PowerShell 以完整權限來執行任意程式碼，不會受到 WDAC 的監控與限制。

另一個漏洞 CVE-2021-41355 則是存於 .NET 核心的資訊洩露錯誤，可導致登入資訊以純文字格式傳送到非執行 Windows 作業系統的其他平台上。

CVE-2021-0951 的 CVSS 危險程度評分為 6.7 分（滿分為 10 分），主要影響 PowerShell 7 與 PowerShell 7.1 兩個版本；而 CVE-2021-41355 則為 5.7 分，影響的是 PowerShell 7.1 版本。

用戶可以在命令列模式下輸入「`pwsh -v`」，來檢視自己 Windows 系統上的 PowerShell 是哪一個版本；Microsoft 建議系統管理員應該將 PowerShell 升

級至 7.0.8 與 7.1.5 兩個版本，以避免遭到駭侵者透過這兩個漏洞發動駭侵攻擊。

- CVE 編號：CVE-2021-0951、CVE-2021-41355
- 影響產品/版本：PowerShell 7、7.1
- 解決方案：升級至 PowerShell 7.0.8 與 7.1.5

- 資料來源：
 1. Microsoft Security Advisory CVE-2020-0951: Windows Defender Application Control Security Feature Byp
 2. Microsoft Security Advisory CVE-2021-41355 | .NET Core Information Disclosure Vulnerability #26
 3. Windows Defender Application Control Security Feature Bypass Vulnerability
 4. .NET Core and Visual Studio Information Disclosure Vulnerability

3.7.3、軟推出 10 月 Patch Tuesday 資安修補包，修復多個嚴重及 0-day 漏洞



Microsoft 推出 10 月份例行性資安更新修補包「Patch Tuesday」，修復 74 個資安漏洞及 4 個 0-day 漏洞，用戶應立即套用更新。

Microsoft 近日推出 2021 年 10 月份例行性資安更新修補包「Patch Tuesday」，一共修復多達 74 個資安漏洞，其中更包括 4 個 0-day 漏洞，用戶應立即套用更新。

這次的 Patch Tuesday 資安漏洞修補包，除了上述的 74 個更新外，還有另外 7 個屬於 Microsoft Edge 的資安更新；以修補完成的漏洞類型來看這 81 個漏洞，分別如下：

- 執行權限提升漏洞：21 個；
- 資安功能跳過漏洞：6 個；
- 遠端執行任意程式碼漏洞：20 個；
- 資訊外洩漏洞：13 個；
- 服務阻斷漏洞：5 個；
- 詐騙假冒漏洞：9 個。

值得注意的是，在這批修復的資安漏洞中，共有 4 個 0-day 漏洞如下：

- CVE-2021-40449：Win32K 權限提升漏洞；這個漏洞據報已遭駭侵者

大規模濫用於發動攻擊；

- CVE-2021-40469：Windows DNS Server 遠端執行任意程式碼漏洞；
- CVE-2021-41335：Windows Kernel 權限提升漏洞；
- CVE-2021-41338：Windows AppContainer 防火牆規則資安功能跳過漏洞。

在嚴重程度方面，這次 Patch Tuesday 中有三個漏洞屬於「嚴重」等級，分別為：

- CVE-2021-40486：Microsoft Word 遠端執行任意程式碼漏洞；
 - CVE-2021-40461：Windows Hyper-V 遠端執行任意程式碼漏洞；
 - CVE-2021-38672：同樣是 Windows Hyper-V 遠端執行任意程式碼漏洞。
- 解決方案：由於本次更新檔案極多，建議所有微軟產品用戶，應立即透過系統更新功能，下載安裝這次資安漏洞修補包，以避免遭駭侵者透過已知漏洞發動攻擊。
 - 資料來源：
 1. Microsoft October 2021 Patch Tuesday: 71 vulnerabilities, four zero-days squashed
 2. Microsoft October 2021 Patch Tuesday fixes 4 zero-days, 71 flaws

3.7.4、QNAP 修復可導致駭侵者遠端注入、執行任意程式碼的 NAS 應用程式漏洞



台灣 NAS 大廠 QNAP 修復多個資安漏洞，可能致使駭侵者遠端注入並執行各種惡意程式碼，藉以發動資安攻擊。

台灣網路儲存設備（Network Attached Storage, NAS）大廠 QNAP（威聯通），日前發表資安更新修補，修復多個資安漏洞；這些漏洞可能致使駭侵者遠端注入並執行惡意程式碼，藉以發動各種資安攻擊。QNAP 各型 NAS 設備用戶，應立即更新受影響的軟體至最新版本，以套用更新。

在這批獲得修復的漏洞中，有三個屬於危險程度相當高的「跨網站指令碼」執行（Cross-site scripting, XSS）漏洞，其 CVE 編號分別為 CVE-2021-34354、CVE-2021-34356、CVE-2021-34355。這些漏洞存於版本號碼早於 5.4.10、5.7.13、6.0.18 等 Photo Station 應用軟體內，以及版本號碼早於 2.1.5 的 Image2PDF 應用軟體內。駭侵者可利用這些 XSS 漏洞，遠端注入惡意程式碼，永久儲存在受害用戶的 NAS 裝置內。

另外，QNAP 此次也針對某些已經停產且停止支援的舊款影像監控解決方案，修補一個可能致使駭侵者遠端執行惡意程式碼，甚至取得裝置控制權的嚴重漏洞；該漏洞的 CVE 編號為 CVE-2021-34352，發生在 QVR IP 影像監控裝置的韌體內。

QNAP 資安通報中提供了 QNAP NAS 設備用戶更新這些漏洞的指引；如果用戶裝置中安裝了 Photo Station 或 Image2PDF 應用程式，只要以 admin 登入裝置，開啟 App Center，接著搜尋 Photo Station 與 Image2PDF，再按下更

新按鈕即可。

QNAP 也提供了 QVR 影像監控裝置的韌體更新指引，用戶先以 admin 帳號登入 QVR 控制介面，然後進入 Control Panel > System Settings > Firmware Update，先檢查是否有新版韌體，然後按下更新按鈕即可。

- CVE 編號：CVE-2021-34354、CVE-2021-34356、CVE-2021-34355、CVE-2021-34352 等
- 影響產品/版本：Photo Station 5.4.10、5.7.13、6.0.18 之前版本、Image2PDF 2.1.5 之前版本
- 解決方案：更新至最新版本
- 資料來源：
 1. Resolved Stored XSS Vulnerabilities in Photo Station CVE-2021-34354 | CVE-2021-34356
 2. Resolved Stored XSS Vulnerability in Photo Station CVE-2021-34355
 3. Resolved Command Injection Vulnerabilities in QVR

第 4 章、資安研討會及活動

企業資安防護及案例分享研討會

活動時間 2021/11/12 (五) 13:00 – 16:30

活動地點 高雄市楠梓區加昌路 600 之 11 號

活動網站 <https://tacert.mis.nsysu.edu.tw/p/412-1257-135.php>

企業資安防護及案例分享研討會

主辦單位：TWNIC、TWCERT/CC

活動概要

本次研討會將介紹台灣電腦網路危機處理暨協調中心(TWCERT/CC)服務內容，希望企業能充分利用政府資安資源，推動企業資安事件通報、惡意檔案檢測服務等免費服務。此外，本研討會也邀請中華資安國際的講師，探討「資安檢測實務分享」以及「社交工程介紹與案例分享」，透過員工資訊安全的培訓，提升員工資安意識，加強企業資安的防護能力。

議程：

13:00~13:30 報到

13:30~14:00 資安威脅案例與企業資安事件通報應變制度簡介

(含 TW-ISAC 平台功能說明) 講師：TWCERT/CC

14:00~14:10 中場休息

14:10~15:10 資安檢測實務分享 講師：中華資安國際講師

15:10~15:20 中場休息

15:20~16:20 社交工程介紹與案例分享 講師：中華資安國際講師

16:20~16:30 Q&A

CLOUDSEC 2021	
活動時間	11/16 ~ 11/18
活動地點	線上活動
活動網站	https://www.trendmicro.com/zh-tw/campaigns/cloudsec-events.html
活動概要	 主辦單位：Trend Micro Reimagine your cloud 業界資安好手企盼的年度盛會 CLOUDSEC 2021 融合全球與台灣當地的資安議題，您可以更自由、彈性選擇適合自己的工作角色和專業能力。 Day 1 (11/16): 全球趨勢和資安洞察 (英文議程) Day 2 (11/17) : 資安威脅前瞻研究，產業領袖分享，資安生態協作與運作實務 (中文議程) Day 3 (11/18) : TECHNICAL PRACTICE - CLOUDSEC CHALLENGE (英文議程)

IRCON 2021

活動時間 2021/11/22-11/25

活動地點 台南市歸仁區歸仁十三路一段 6 號

活動網站 <https://ircon.nchc.org.tw/>



主辦單位：財團法人國家實驗研究院

特色議程

活動概要

COVID-19 的侵襲重創全球經濟，許多企業營運因此停擺，迫使企業必須加速興起數位轉型。期間因遠距辦公的資安攻擊破口，成了駭客入侵企業網路竊取商業機密，近期更趁勢透過大量造假的疫情相關訊息而作亂，這些潛藏的資安隱憂，僅是採取零信任(Zero Trust)的架構，就能保護企業免於資安威脅？不僅如此強化資安的人才培育和研發能量，建構資安的風險意識、擁有覺察威脅的敏銳度並掌握攻擊全貌，儼然成為當前最重要的課題。

- IRCON 2021 資安人才培訓課程 11/22 (一)
- IRCON 2021 臺灣資訊安全事件應變研討會 11/23-24 (二、三)
- 智慧科技成果展 11/23-24 (二、三)
- 車聯網資安趨勢 11/24 (三)
- SP-ISAC 資安沙龍 11/23 (二)
- CDX 使用者會議 & CDX3.0 Workshop 11/24-25 (三、四)

企業如何因應資安危機？

活動時間 2021/11/24(三) 19:00-21:00

活動地點 線上 Google meet

活動網站 <https://www.accupass.com/event/2110221346541244283653>



主辦單位：中華民國中小企業經營發展協會

資訊安全於現在生活的重要性，若沒有注意，會產生什麼可能的影響？

活動概要

網路上哪些行為，可能面臨的法律問題；如果使用非公司指定之通訊軟體導致的洩密的法律問題；使用網路圖片或浮水印外洩之法律問題；網路檔案未經授權拷貝之法律問題；乃至郵件外洩、下載之後拷貝後法律問題；進而使用盜版軟體以及未經授權之軟體法律問題。

企業若真正遇到資訊安全的危機，可以怎麼處理？

什麼情況下會遇到個人或是企業的資訊安全？

活動時間：2021-11-24(三) 19:00 ~ 21:00

活動地點：此活動為線上活動，購票後可於票券頁進入直播連結。本活動使用 Google meet 進行直播課程。

HITCON 2021 台灣駭客年會

活動時間 2021/11/26(Fri) - 2021/11/27(Sat)

活動地點 中央研究院人文社會科學館(台北市南港區研究院路二段 128 號)

活動網站 <https://hitcon.org/2021/>

活動概要

主辦單位：社團法人台灣駭客協會(HITCON)

【 HITCON 2021 台灣駭客年會活動搶先報 】

覺得 HITCON 很神祕嗎？

覺得 HITCON 2021 活動很多嗎？

現在搶先報來啦！

HITCON 駭客貓歷險記 (Hacker Cat Adventure)：為 HITCON 2021 獨立開發的虛實整合尋寶遊戲，利用整個會場為活動場地，透過劇情、解謎與資安等要素所組成的實境解謎遊戲，藉由駭客貓的視角認識 HITCON 2021 並促進各方交流。

- Round Table：為了提升 HITCON 探討議題的深度和高度，首度嘗試舉辦圓桌會議，活動安排於第一天中午，分成資安長、金融、智慧製造及跨國金融資安等不同桌次主題，並邀請相關主題的重要人士、領導人士共同用餐和分享，每桌安排一位桌長協助主題分享，並贈予受邀出席者禮物作為致謝。
- HITCON Village：今年的活動將仿造海外研討會的 Village，現場會有各種企業、社群參與，並提供豐富的主題，希望透過實作題與互動帶領會眾一窺不同面向的資安技術與議題，也體驗駭客生活圈的樂趣。
- 資安人力系列活動：與求職徵才服務企業合作，於大會期間提供人才提供履歷健檢、轉職諮詢、職涯諮詢，協助學生、求職人士和資安相關企業進行媒合，提供資安產業的人才與職缺媒合。
- HITCON Online 虛擬會場：2021 虛擬會場再次登場，承襲去年的精神，簡化系統設計，以網頁做為介面降低使用門檻及難

度，除了原有提供線上會眾與贊助商交流的平台，本次也作為實體會場的延伸，加入線上的活動和大會活動帶來不同的虛實整合遊戲體驗，期望帶給會眾不一樣的線上體驗。

- 煉蠱：這是一個 2020 好評延續的大會活動，根據駭客精神和技巧所設計的比賽，利用知識和想像力打敗對手成為最強蠱王吧，煉蠱 2.0 等你來挑戰！

■ HITCON 2021

日期：2021/11/26(Fri) - 2021/11/27(Sat)

地點：中央研究院人文社會科學館

進入活動官網：<https://hitcon.org/2021/>

第 5 章、2021 年 10 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。

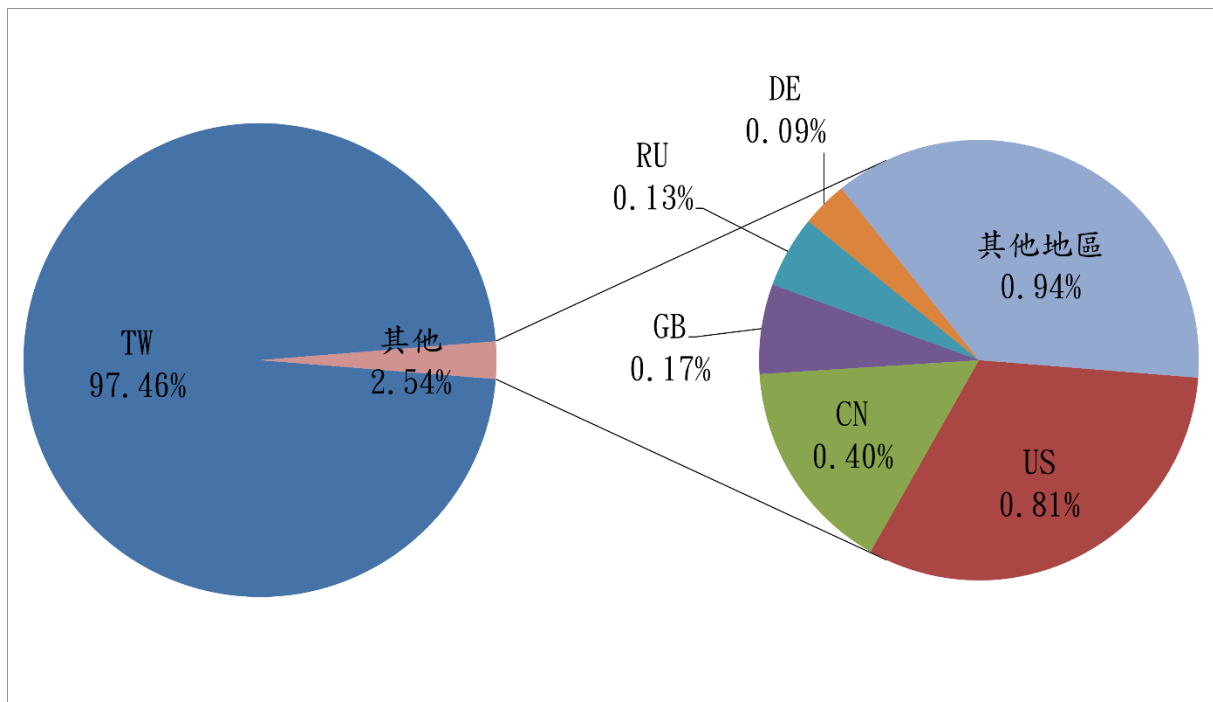


圖 1、分享地區統計圖

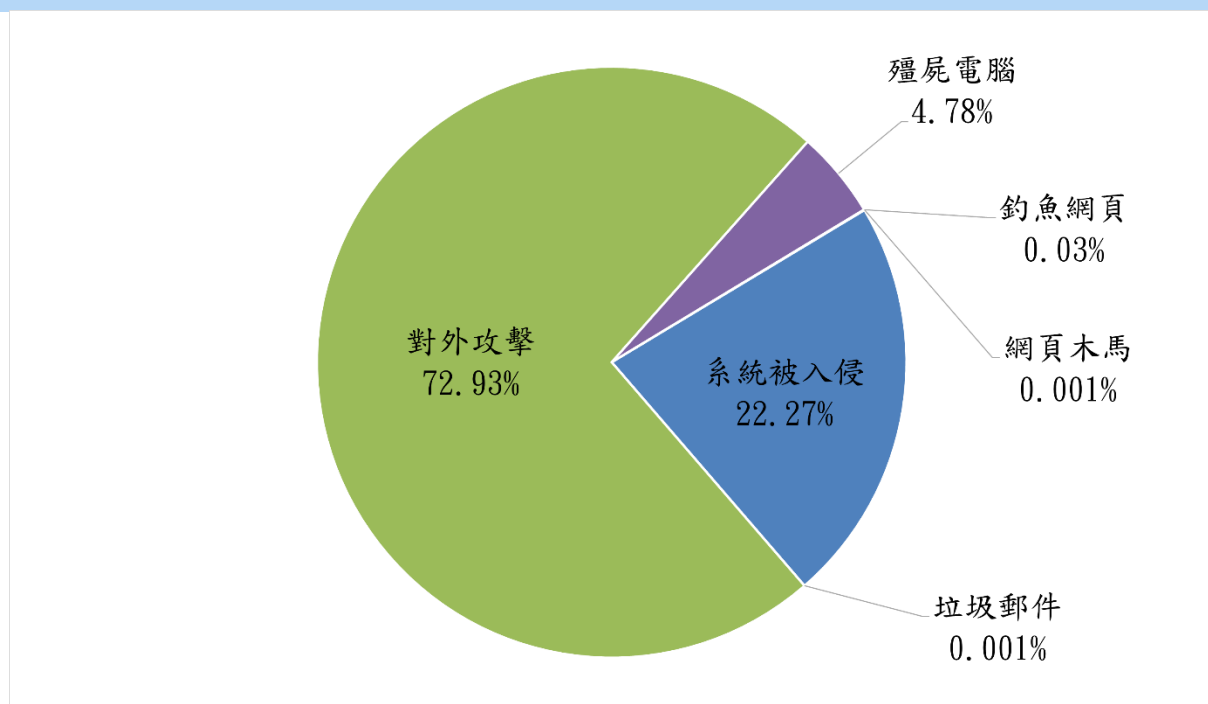


圖 2、分享類型統計圖

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 11 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](https://twitter.com/TWCERTCC)