TWCERT/CC 資安情資電子報

2022 年 8 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 6 章節：

第 1 章、封面故事：主題式資訊安全專題分享。

第 2 章、資安活動紀事：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、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第 4 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 5 章、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 6 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

邊界閘道通訊協定(BGP)威脅與防範

- 邊界閘道器協定(Border Gateway Protocol, BGP)，用於在不同的自治系統(Autonomous system, AS)間交換路由資訊。在此協定中，主要是透過維護 IP 路由表以及前綴(Prefix)來實踐自治系統之間的可達性，以達到去中心化的網路自治。
- 由於 BGP 協定本身路由路徑之運作多是建立於各自治系統之間的互信以及正確性。因此若原本應透過路由被導至正確的流量，很可能因為其他自治系統針對 IP 或前綴資訊的設定錯誤，導致其流量被引導到錯誤的目的地，甚至被導入釣魚網站中，遭他人竊取或盜用個人、金融資訊，甚至受到惡意程式的極大威脅。
- 為了減少路由錯誤以及意外劫持的狀況，網際網路工程任務組(Internet Engineering Task Force, IETF)訂定了資源公鑰基礎建設(Resource Public Key Infrastructure, RPKI)標準，針對 AS 進行驗證，確認該 AS 是否有權發布特定的 IP 位址。
- 台灣地區的可信任憑證授權中心(Certification Authority, CA)為台灣網路資訊中心(Taiwan Network Information Center, TWNIC)，向其會員頒發憑證，並且管理一 RPKI 儲存庫，用以驗證 AS 的 IP 位址資源，證明其使用的權利，減少因意外產生的路由問題。
- 2019 年 8 月中，台灣已申請並通過驗證的 IPv4 路由數量已達 74.28%，相

較於全球 15.62%以及亞太區 12.06%之申請並通過驗證之路由數量比例，台灣之 RPKI 施行率在國家通訊傳播委員會(National Communications Commission, NCC)以及 TWNIC 的努力下，成為全球之佼佼者，可以減少常見的路由錯誤以及防止大多數的 BGP 威脅，強化路由資安防護能量。

一、簡介

BGP 概述

邊界閘道通訊協定(BGP)，是一種網路路由協定(Routing Protocol)，提供網際網路的自治系統網域內，彼此之間傳遞封包的最佳路徑，以達到最好的資訊傳遞速度和品質。

BGP 協定主要是透過 Bellman-Ford 距離向量路由演算法，以計算每個自治域的連接設備(BGP Speaker)，透過不斷更新路由資訊，學習並繪製出網路最佳路由的相關拓撲。

BGP 協定發展至今，已經廣被認可為相當穩定和可靠的路由協定。但相對於路由功能，其針對路由安全上之設計則較不穩健，甚至 BGP 路由安全被認為有所缺陷。而 BGP 最主要的安全問題，是存在於路由資訊的傳播部分。由於 BGP 協定本身是設定為默認接受通知中傳遞的所有路由資訊，亦即進行一種無條件信任的路由資訊傳播。當機器錯亂或人為無意或刻意設定錯誤，造成錯誤路由通知傳送給接收方並擴散給與之相連的其他 BGP 連接設備，使得網路流量因錯誤的路由路徑被導往錯誤的目的地，導致網際流量洩漏(Leakage)或挾持(Hijacking)等資安事件。此類安全問題，主要是因為 BGP 協定本身缺乏一套可靠的認證機制，無法對其路由資訊進行驗證，難以保障路由資訊的正確性。相關網路架構示意圖如下：

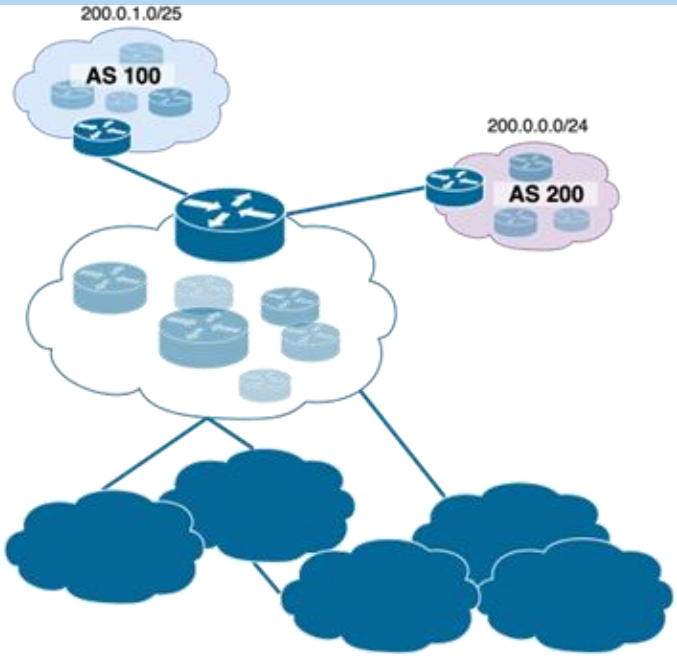

圖 1：BGP 網路架構示意圖

全球 BGP 威脅概況

根據 MANRS 的統計，在 2019 年 1 至 7 月中，全球路由的運作中斷事件總計 17,522 件，其中，共有 8,041 個自治系統產生了一次以上的路由事件，詳細資料如下圖：

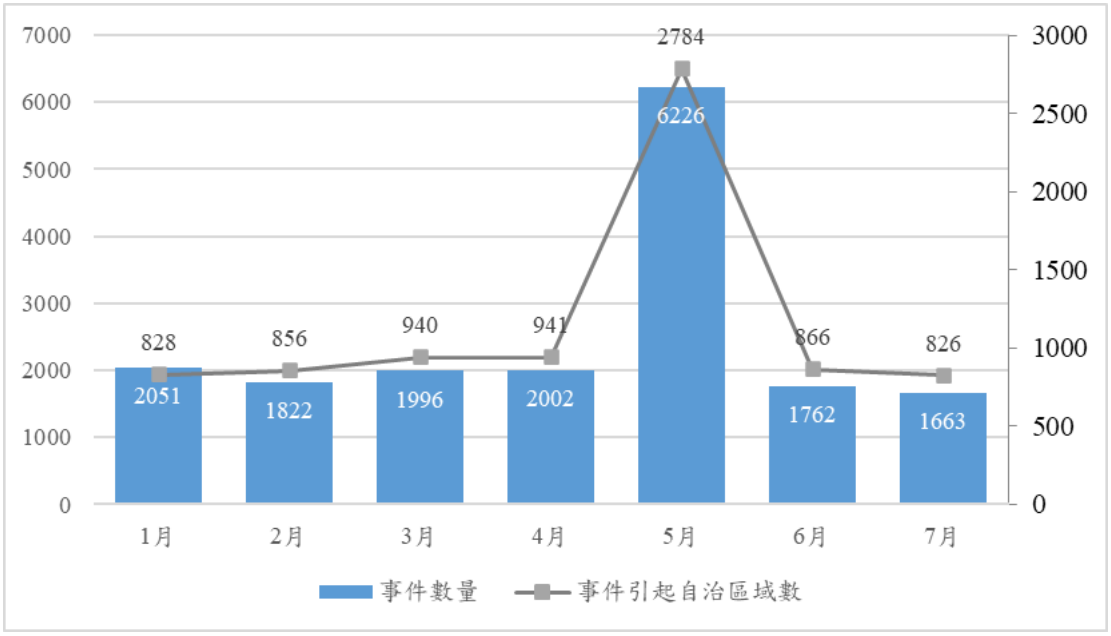

圖 2：全球路由事件 2019 年 1 至 7 月統計

其中，平均每月約有 2,503 次的路由事件，但於 2018 年的統計，顯示該年度僅 12,600 次路由事件，平均每月 1,050 次路由事件，以及 2017 年平均每月 1,162 次路由事件。與前兩年相比，可以很明顯看到 2019 年的前七月中，路由事件的數量有逐漸增長的趨勢。

在全球路由事件中，台灣在 2019 年的 1 至 7 月，共有約 122 起事件有所影響；並且在 7 個月中，總計有 46 個網路自治區域造成了路由事件。詳細資料如下圖：

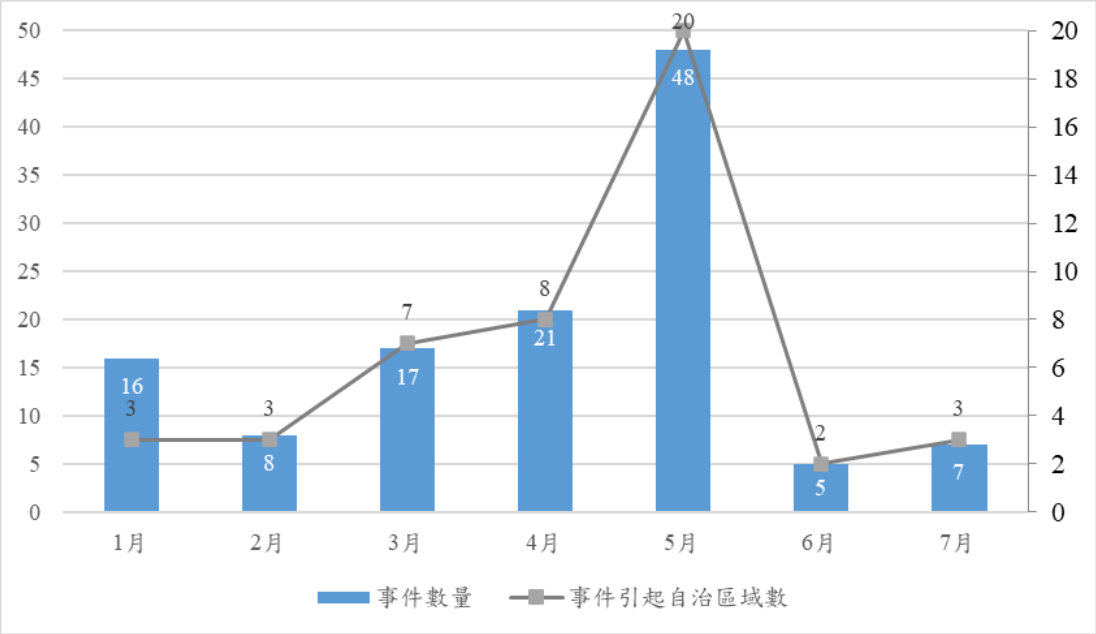

圖 3：台灣路由事件 2019 年 1 至 7 月統計

在台灣的路由事件中，平均每個月約有 17 起路由事件，約為全球的 0.68%。

二、BGP 威脅類型與案例分析

BGP 資安威脅緣由

BGP 劫持是在 BGP 協定中，最為常見也最被廣泛討論的安全威脅。此種威脅模式主要是源因於一個錯誤的前綴資訊的宣告，也就是一個自治系統向外部區域宣告了應不屬於該自身的前綴資訊，亦即向外傳播了一個實際上為

他人所有的 IP 位址區段，導致欲使用該 IP 位址區段的使用者因為其錯誤的宣告，而被引導至錯誤的目的地。BGP 劫持事件發生頻繁，並且往往會因為微小的失誤而嚴重影響大量網路之服務品質，甚至導致服務中斷，若不幸為惡意之 BGP 劫持行為，更可能會讓使用者在不知情的情形下蒙受損失，這些都是網路業者應極力避免產生或遭受影響之嚴重資安威脅。

BGP 資安威脅案例

(1)服務中斷之 BGP 資安威脅事件

- 美國電信業者設定錯誤，Cloudflare 多個代管網站一度服務中斷

2019 年 6 月 24 日，因美國大型電信公司 Verizon 宣告了錯誤的路由資訊，導致 Amazon、Cloudflare、Facebook 的服務中斷，並且 Cloudflare 代管的多個網站—包括 Overcast、WP Engine、Sonassi 以及 Discord 等網路公司的服務中斷近 2 個小時。事件的起因是賓州的一家小型 ISP，由於其公司內部採用了 BGP 優化器以提升內部網路的路由效能，而這些優化的路由資訊理應僅供內部網路使用，但該 ISP 卻誤將資訊宣告給其客戶，再被轉宣告給美國大型電信公司 Verizon，使得在這 2 個小時中，大量的流量都被導向賓州的 ISP，致使許多大型網站的服務因此中斷。此次事件除了檢討電信公司無條件接收且無任何過濾的路由機制，同時也呼籲不要使用 BGP 優化器，因為使用者無法保證這些優化後的 BGP 資訊不會被洩漏出去並導致嚴重的後果。

- 巴西 ISP 設定錯誤，台灣公共 DNS 遭劫持約 3 分鐘

2019 年 5 月初，巴西一家 ISP 對外宣告了 IP 位址 101.101.101.0 以及前綴資訊/24，也就是對外宣告自 101.101.101.0 至 101.101.101.255 的 IP 位址區段均屬於該巴西 ISP 所有。但實際上，101.101.101.101 這個 IP 位址理應屬於台灣的 DNS 服務—Quad101 所有，用以提供使用者免費的 DNS 服務。幸得當時在兩邊溝通之下，流量的錯誤引導情形僅持續了 3 分半鐘，巴西 ISP 立即進行了修正，並未造成重大影響。

➢ 奈及利亞 ISP 劫持 Google 網路流量

2018 年 11 月 12 日，位於奈及利亞的一家小型 ISP，在進行網路升級配置時，錯誤地設定其路由資訊，宣告了應屬於 Google 的前綴資訊，導致 Google 相關服務因誤將其流量導至其他自治系統，其服務因而中斷了約 1 個小時。由於該路由資訊被宣告之後，基於相互信任之原則，中國、俄羅斯等之電信業者很快便採納了該錯誤的路由資訊，導致應前往 Google 的流量在到達中國電信時便被終止，使得封包無法順利前往 Google 取得服務，甚至一度被懷疑為惡意的 BGP 劫持。直至隔(13)日，奈及利亞 ISP 業者 MainOne 方出面道歉，解釋係其錯誤的配置所造成，並聲稱在發現後已立即更正。

(2)錯誤路線之 BGP 資安威脅事件

➢ 歐洲行動網路流量被導至中國電信事件

2019 年 6 月 6 日時歐洲行動網路的封包因錯誤的路由宣告，被導至中國電信(China Telecom)。此次事件主要是起因於瑞士數據代管業者 Safe Host，將錯誤的路由資訊宣告給與之合作並建立專用線路的中國電信，而中國電信在收到了有誤之路由資訊後，就成為進入 Safe Host 的唯一節點，導致大量的歐洲電信服務—包括瑞士、荷蘭以及法國的電信都受到影響。此次的 BGP 劫持事件持續了約 2 小時，此期間使用者投訴其網路明顯感覺到上網速度變慢，甚至連不上某些特定伺服器。雖然此次事件並未嚴重影響 ISP 的服務和運作，但為了避免類似的事件頻繁發生，代表著路由的基本保護措施是相當必要的。

➢ 台灣智慧光網設定錯誤，造成中華電信服務異常

2018 年 11 月 19 日，台灣中華電信網路發生連接部分國外網站服務延遲或中斷之現象，但 Google、Youtube、Facebook 以及國內網站不受影響。經查證後發現，其原因為台灣智慧光網在進行路由設定調整時有誤，並將其錯誤的路由資訊宣告給中華電信，導致中華電信聯外流量被導至台灣智慧光網，

又因臨時驟增的流量湧入台灣智慧光網之網路，導致使用者在瀏覽國外網站時產生了壅塞之情形，使得中華電信客戶在訪問國外網站時，產生反應遲緩或服務中斷之狀況。中華電信人員發現後，立即停止與台灣智慧光網之網路連接，回復正常路由。此次事件持續了約 30 分鐘，中華電信已和台灣智慧光網建立路由異動相關標準作業程序，避免類似事故的再次發生。

(3)惡意攻擊之 BGP 資安威脅事件

- 駭客進行 BGP 劫持攻擊，目標為美國三家支付處理公司

2018 年 7 月，美國三家支付處理公司 Datawire、Vantiv 以及 Mercury 分別遭受駭客 BGP 劫持攻擊。第一次攻擊始於 7 月 6 日，是由一家印尼的 ISP 業者所公告，該攻擊持續了約 30 分鐘，主要目標為 Vantiv 以及 Datawire 支付系統，幸得此次攻擊的宣告傳播範圍不大，未造成嚴重影響。第二次攻擊係於 7 月 10 日發動，主要是透過馬來西亞的 ISP 業者宣告錯誤的路由資訊，在 22:17 時，針對 Mercury 支付系統進行了第一波攻擊，持續了約 30 分鐘；而在 23:37 時再次進行了第二波攻擊，雖然此次僅持續了 15 分鐘，但針對的目標更廣、影響範圍更大。在同一天，Vantiv 及 Datawire 也遭受到長達 3 小時的另一波 BGP 劫持攻擊。同月 12 日，馬來西亞 ISP 業者又宣告了錯誤的路由資訊，再次劫持了 Vantiv 以及 Datawire 的流量，並且持續了約 3 個小時。然而此次攻擊中，Datawire 已經注意到其路由遭到劫持，並聲稱相同的路由資訊已重新控制其所屬的 IP 區段和路由資訊。而根據甲骨文(Oracle)公司的研究資訊，他們認為此次事件與 2018 年 4 月的 Amazon AWS DNS 劫持事件相當相似，因此認為此次攻擊只是一個開始，若不試圖解決 BGP 的安全問題，未來將會有更多且更嚴重的 BGP 劫持事件發生。

- Amazon DNS 遭劫持，駭客盜走約 15 萬美元以太幣

在去(2018)年 4 月 24 日，Amazon 的 DNS 伺服器遭駭客劫持約 2 小時，並將其流量導入假冒的網路錢包網站 MyEtherWallet 中，從不知情的受害者處

竊取了約 15 萬美元的以太幣。之後，Amazon AWS 發出聲明澄清，其服務以及 Route53 DNS 並沒有遭到駭客入侵或盜用，是 Amazon 的上游 ISP 遭到駭侵攻擊，並向外宣告了錯誤的 Route53 DNS 路由資訊，導致其部分流量被導入至惡意網站中。事後，MyEtherWallet 也發出聲明，建議使用者先改以 Cloudflare DNS 伺服器使用其服務，並確保網站的 SSL 憑證標明「MyEtherWallet Inc.」，以避免因釣魚網站而蒙受損失。

三、BGP 資安威脅防禦機制

網路路由器安全管理

為了防範路由器本身遭駭客入侵並利用，除了對 BGP 協定進行安全強化外，同時也必須針對路由器進行規範和要求，以達到較高的防護能量。根據國家通訊傳播委員會(NCC)之相關技術規範，其提出了下列要點有關網路路由器基本安全標的：

1. 稽核紀錄：應產生內容完整之稽核紀錄，並可識別每筆紀錄是由哪一位使用者所產生。
2. 加解密金鑰及演算法：應透過加解密演算法產生並使用之金鑰，以及透過加解密演算法為遠端連線提供防護。
3. 殘餘資訊：每次使用時，應清除完畢前此使用之相關資訊，避免前次使用之相關資訊之外洩風險。
4. 鑑別機制：應記錄並管理通行碼的任何管理機制，例如通行碼的長度及更換頻率等；並須具備並運行任何鑑別之機制，例如當使用者登入或未登入時之權限，或避免在鑑別過程中將任何資訊洩露於顯示器上等。除此之外，當使用者連續鑑別失敗時，應拒絕該使用者後續之要求，並進行後續行為管理。
5. 安全功能行為：將其安全功能的變動和設置權限，設定為僅有授權之管理者

方能進行更動。

6. 管理功能規格：應具備本機登入或遠端登入管理功能，以及驗證韌體更新、更新前驗證之管理功能。

7. 安全角色：對於使用者，其應接受經過授權之管理者角色，並可設定使用者為管理者。但對於管理者角色，雖可透過本機或遠端登入，但預設應不允許管理者透過遠端登入。

8. 失效保全：啟動後，若其自我測試發生錯誤，應確保加解密金鑰以及使用者之任何相關資訊均仍處於被保護狀態。

9. 重送攻擊：若發現重送之封包，應拒絕接收。

10. 通行碼保護：應避免以明文方式儲存及顯示其通行碼。

11. 可信賴之時戳：應具備可信賴之時戳，正確地紀錄稽核紀錄的日期時間。

12. 可信賴更新：應具備檢測並查詢是否有更新的韌體版本，並且可以透過授權之管理者進行更新程序。除此之外，應具備一機制，在韌體更新前，驗證該更新版本之真偽。

13. 安全功能自我測試：其啟動後，應進行安全功能自我測試，確保其服務可正常運作。

14. 資源配置：應針對同時登入之管理者數量以及同時連結之無線用戶數進行資源配置之上限設定。

15. 登入連線鎖定/終止：當管理者登入後，其閒置時間超過其允許之時間值，則若該連線為本地連線，應鎖定或終止該連線，並確保鎖定時不會洩漏任何管理者之資訊，且需再次鑑別方能解除鎖定。反之，若為遠端連線，則應立即

終止該遠端連線。此外，應允許管理者自行終止其連線。

16. 存取預設標語：管理者可設定登入畫面及提醒事項並於登入時顯示。

17. 金鑰保護：防止金鑰共享及不得提供讀取各種金鑰之指令。

BGP 安全管理功能

為增加 BGP 的安全性，以及減少意外造成之路由安全威脅和風險，有幾項針對 BGP 協定的設置，可以減少此類因意外造成的問題：

1. 需限制最大路由數量(Prefix-Limit)，限制接收的路由資訊之網段數量，對減少全表路由洩漏以及自身內存耗盡等問題，具有相當助益；或是限制自身宣告的網段數量，亦可減少因配置錯誤等造成之路由問題之影響程度。

2. BGP 路由管理應注意並防護駭客偽造網段、欺騙他人來源 IP 位址之惡意行為，例如反欺騙(Anti-Spoofing)機制。

3. 除了驗證來源 IP 位址之外，應同時具備 BGP 宣告網段正確性之驗證，例如資源公鑰基礎建設(Resource Public Key Infrastructure, RPKI)機制。

RPKI 概述

有鑑於 BGP 劫持事件以及路由錯誤設定的情形經常發生，網際網路工程任務組(IETF)訂定了一套用以解決大部分路由相關安全問題的資源公鑰基礎建設(RPKI)標準。RPKI 標準主要適用於保護網際網路路由基礎建設，尤其針對 BGP 協定，提供了網際網路號碼資源資訊(例如 IP 位址等)連結到信任錨(Trust Anchor)的方法，也就是連接到一個可信的第三方並進行相關的驗證，以確保資訊的正確性。

- 路由來源授權(ROA)

為了確保路由資訊的正確性，RPKI 允許單位發布路由來源授權(Route Origin Authorization，ROA)，用以證明所收到的路由資訊中的 IP 位址和 ASN 是正確的組合。ROA 本身是一個經過加密簽章的物件，標明了 ASN 和 IP 地址及前綴資訊的對應關係，當一個自治系統發布了一個前綴資訊時，便可以透過 ROA 去驗證該自治系統是否有權利發布這個前綴資訊。

- 資源公鑰基礎建設(RPKI)

RPKI 標準可以透過認證網際網路資訊，以作為確保路由安全的一種模式。此標準允許區域網際網路註冊管理機構—例如亞洲區的機構為亞太網絡信息中心(Asia-Pacific Network Information Centre，APNIC)—的成員可簽發 RPKI 資源憑證以及列出其持有的網際網路號碼資源，並存於 RPKI 資料庫中，而這些資源便可以提供驗證，作為安全性的有效證據。亦即當一路由接受到新的路由資訊宣告時，若該自治系統已經佈署了 RPKI，便可以自 RPKI 資料庫中下載新路由資訊宣告的憑證以及 ROA 資訊，從而判斷此路由資訊宣告是否有效，減少路由錯誤以及防止大部分的 BGP 劫持。

根據美國國家標準暨技術研究院的統計數據，2019 年 8 月中，全球 IPv4 路由數量之 RPKI 統計，約有 15.62%的路由申請 ROA 並通過驗證，但有 0.83%之比例申請 ROA 卻尚未通過驗證，此外，有約 83.55%之路由數尚未申請 ROA、亦即並未施行 RPKI。詳細資訊如下圖：

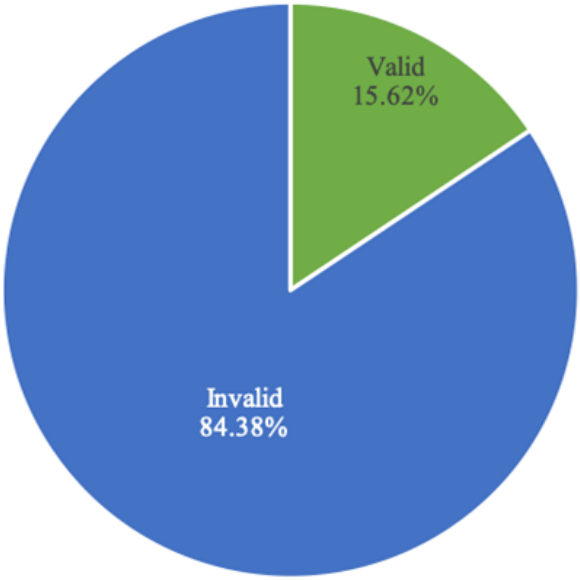

圖 4：全球 IPv4 RPKI 統計圖(以路由數量計)

而亞太區的 IPv4 路由數量 RPKI 統計值，有 12.06%的路由數已申請 ROA 並通過驗證，但有 1.45%尚未通過驗證，此外，有 86.49%並未施行 RPKI。詳細資訊如下圖：

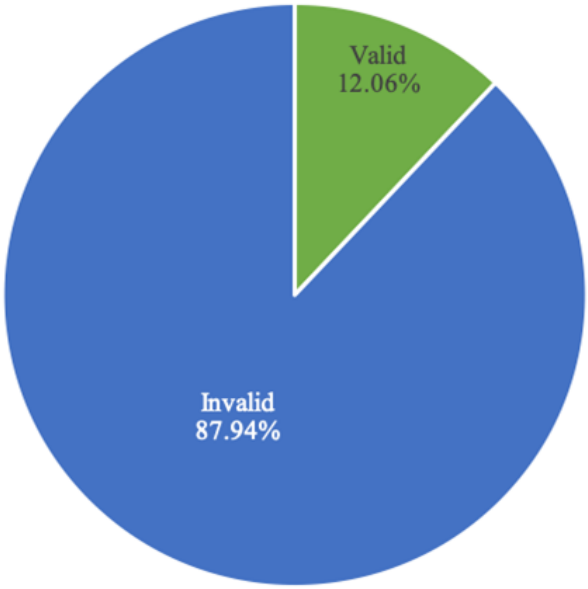

圖 5：亞太區 IPv4 RPKI 統計圖(以路由數量計)

國內 RPKI 推行概況

在台灣，RPKI 主要由國家通訊傳播委員會推動，其 RPKI 目前主要的憑

證授權中心為台灣網路資訊中心(TWNIC)，TWNIC 會向其會員、也就是其資源持有者發放憑證，並且持有者可以透過 TWNIC 的管理系統進行 RPKI 相關資源的增修以及操作。

自台灣 RPKI 開始施行後，直到 2019 年 8 月中，以台灣 IPv4 路由數量統計，目前已有 74.28%申請 ROA 並通過驗證，有 25.72%的路由尚未申請 ROA。詳細資料如下圖：

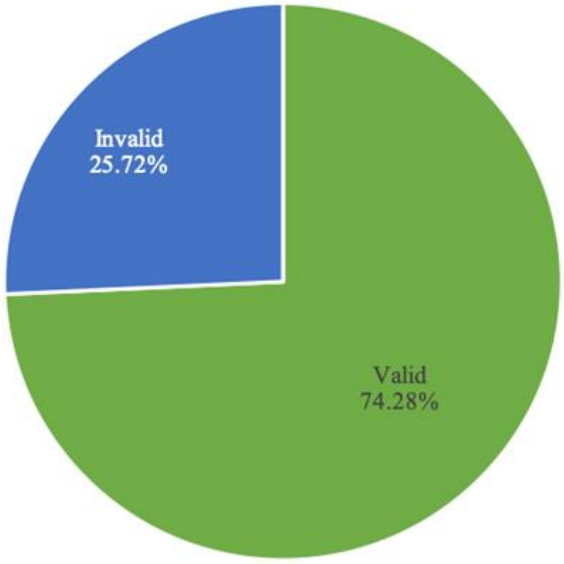

圖 6：TWNIC IPv4 RPKI 統計圖(以路由數量計)

台灣的 RPKI 申請並通過驗證之比例，遠高於全球的 15.62%以及亞太地區平均之 12.06%，可見台灣網際網路使用各界對路由安全有足夠之警覺性，同時也願意為了增進自身之網路安全和品質，與國家通訊傳播委員會以及 TWNIC 攜手合作，減少 BGP 路由問題，強化台灣的網路安全體系。

各國 RPKI 推行概況

根據 RIPE NCC 之統計，截至 2019 年 8 月中旬，台灣 IPv4 路由 RPKI 普及率高達 74.28%，在全球 258 個 ccTLD (country code Top-Level-Domain)中位居第 17 名，詳細資訊如下表：

表 1：全球 RPKI 普及率狀況表

名次	Country	國家	IPv4 Prefix Valid	IPv4 位址統計
1	MH	馬紹爾群島	100	4,096
2	BL	聖巴泰勒米	100	1,536
3	AD	安道爾	100	52,224
4	EC	厄瓜多	98.41	2,658,048
5	MV	馬爾地夫	95.45	84,224
6	FO	法羅群島	91.67	44,032
7	CR	哥斯大黎加	89.85	2,600,704
8	GF	法屬圭亞那	88.89	22,528
9	YE	葉門	86.32	180,224
10	UY	烏拉圭	84.63	2,441,216
11	BT	不丹	80	33,280
12	VE	委內瑞拉	77.28	6,816,000
13	TR	土耳其	76.82	16,717,056
14	MN	蒙古	76.07	242,432
15	EU	歐盟	75	13,824
16	CO	哥倫比亞	74.86	17,407,232
17	TW	台灣	74.28	35,689,728
18	WS	薩摩亞	73.33	18,432
19	AL	阿爾巴尼亞	72.8	407,552
20	LK	斯里蘭卡	71.79	554,240
27	IL	以色列	61.65	7,723,520
36	FR	法國	44.32	83,077,392
43	SG	新加坡	38.54	13,791,488
46	NL	荷蘭	37.75	48,804,328
76	TH	泰國	25.39	9,150,976
78	DE	德國	24.71	123,684,480
96	VN	越南	17.51	15,995,392
99	CA	加拿大	16.64	70,375,168
126	US	美國	5.02	1,605,584,384
127	JP	日本	4.47	204,431,616
132	ID	印尼	3.7	18,576,640

根據表 1 之數據，在全球 258 個 ccTLD 中，部分國家本身之 IPv4 數量較少，因而較容易施行 RPKI，達到較高之 RPKI 普及率。然而，由表中觀察台灣所屬之 IPv4 數量是 RPKI 普及率前 20 名中數量最多者，可見台灣之 RPKI 施行頗具成效，是為全球 RPKI 普及程度中之佼佼者。

四、分析與建議

面對網路日新月異的發展，其設計架構等缺點也隨之浮出，管理者必須維持警覺性，預防因意外的失誤導致網路服務的中斷或影響。並應避免使用 BGP 優化器等非規範內允許之額外設備，以免因意外洩漏而導致嚴重的網路事故。

未來 BGP 相關攻擊的數量可能持續增加，因此廠商除了必須要隨時監控自身網路狀況，也必須結合上下游供應商以及網路業者，建立密切合作以達到彼此相互監督、互助之效益。

在規範上，為了防止 BGP 劫持相關事件，建議網路相關業者儘速設定並通過 RPKI 驗證，如此便可透過 ROA 的內容驗證，確認對方是否有權宣告該路由區段。除可減少意外的路由錯誤，更可以防止多數的 BGP 劫持事件。

截至 2019 年 8 月中，根據 RIPE NCC 的統計，台灣網路產業業者已有高達 74.28%的施行比例，遠高於全球的 15.62% RPKI 施行比例，顯示台灣路由防護體系已臻完備。目前台灣區主要憑證授權中心 TWNIC 透過 RPKI 服務系統，提供台灣 ISP 業者申請並設定 ROA 以及相關驗證，以確保台灣路由安全。

根據 RIPE NCC 的統計，截至 2019 年 8 月中，台灣 RPKI 施行比例為全球 17 名，已成為全球 RPKI 普及率之佼佼者外；透過 RPKI 之驗證，減少大多數的 BGP 路由意外， 同時大幅降低 BGP 劫持之資安威脅，讓台灣的路由網路防護體系更加完善。

- 資料來源：

1. BGP for All
2. What Is BGP? | BGP Routing Explained
3. Border Gateway Protocol
4. BGP 安全研究
5. A survey among network operators on BGP prefix hijacking.
6. Mutually Agreed Norms for Routing Security
7. CloudFlare 多個代管網站因 BGP 路由洩露，一度無法連線
8. How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

9. Verizon BGP 路由泄漏，亞馬遜、Facebook 及眾多區塊鏈交易所受到影響
10. 近期 BGP 劫持事件頻傳，即早發現可減少影響範圍
11. 奈及利亞 ISP 網路配置出包，Google 流量因路由洩露而被導至中國
12. BGP 路由洩露將歐洲行動流量導至中國電信
13. 意外發生！大量歐洲網路流量被導向中國長達 2 小時
14. 1 月 19 日因台灣智慧光網公司路由調整作業有誤造成中華電信 HiNet 部分連接國外服務異常之補充說明
15. U.S. Payment Processing Services Targeted by BGP Hijacking Attacks
16. BGP/DNS Hijacks Target Payment Systems
17. 駭客劫持亞馬遜 DNS，盜走 15 萬美元以太幣
18. ETH 與以太坊錢包介紹(一)：網頁錢包 MyEtherWallet
19. 無線區域網路路由器資通安全檢測技術規範
20. 資源公鑰基礎建設(Resource Public Key Infrastructure，RPKI) 的介紹
21. 路由來源授權(Route Origin Authorization，ROA)的介紹
22. 資源公鑰基礎建設(RPKI)進行路由起源授權(ROA)於國際推行
23. Global Prefix/Origin Validation using RPKI
24. RIPE Network Coordination Centre
25. Distribution Reports

第 2 章、 資安活動紀事

資安防護及案例分享研討會-桃園場

活動時間：111.07.19(二) 14:00~16:30

活動議程：

時　間	議程內容
13:30 ~ 14:00	活動報到
14:00 ~ 14:30	TWCERT/CC 服務範疇及案例分享 TWCERT/CC 專業講師
14:30 ~ 16:20	遠距辦公與工控資安防護重點 中揚資訊股份有限公司 唐世智 資深管理顧問
16:20 ~ 16:30	Q & A

由 TWNIC、TWCERT/CC 主辦的資安防護及案例分享研討會於 7 月 19 日假桃園觀音工業區服務中心 2 樓訓練教室舉辦。因全球疫情升級，遠距辦公的普及，讓企業更直接地面對資安漏洞與威脅，員工使用個人電腦透過

Wi-Fi 連接到公司內網，保護終端設備的資訊安全，將成為企業的最大挑戰。希望透過本次研討會介紹台灣電腦網路危機處理暨協調中心(TWCERT/CC)免費資安通報的服務內容，並邀請專業講師探討「遠距辦公與工控資安防護重點」，企業加強產線工控資安意識，做好防護避免因小失大。

研討會首先針對「TWCERT/CC 服務範疇及案例分享」，由 TWCERT/CC 曲承則工程師首先與企業人士分享各種類型資安威脅案例：釣魚網站威脅新聞案例以及釣魚網站辨別方式；殭屍網路運作方式以及提醒面對殭屍電腦的防護建議；近期重大更新提醒，若系統已停止支援，電腦將失去官方安全更新，因而暴露在有安全風險的環境，因此建議務必盡快更新。接著曲工程師針對勒索軟體攻擊案例分享：MS Proxy Logon 為微軟史上揭露最嚴重的 RCE 資安漏洞，TWCERT 已接獲超過 200 筆 IP 受駭，建議措施首先透過微軟提供安全性更新檔進行系統更新，如發現入侵跡象應進行鑑識準備，不關閉主機、隔離網路連線、取得主機映像檔等措施。後續曲工程師詳細說明 TWCERT/CC 提供的服務：資安事件通報規劃的流程與方法、資安事件通報填寫內容以及訂閱情資電子報等服務內容。

研討會第二個議程邀請中揚資訊股份有限公司唐世智資深管理顧問，分享主題為「遠距辦公與工控資安防護重點」。首先由居家辦公這個議題來切入，為對抗疫情台灣企業開始有居家辦公需求，減少人與人之間接觸降低疫情的健康風險，因此企業部門背負更大 IT 挑戰。唐顧問說明遠端桌面連線安全性，提出經常使用 Windows 內建遠端連線或 TeamViewer 軟體，駭客將透過網路掃描找尋開放的網路並暴力破解攻擊，建議強化方式從第一步確認需控管的範圍排點資安現況，第二步再擴大端點設備的管控，建議從事前、事中、事後進行保護措施，並提升 RDP 基本防護盡可能僅透過 VPN 提供存取，唐顧問總結提出居家辦公 9 大安全技巧來提醒企業關注遠端連線對資安的重要性。另唐顧問針對工控資安防護重點，強調未來工廠機台聯網 IT 與 OT 疆界模糊，勒索攻擊漏洞須關注事中阻斷，不再只是使用防火牆作為 OT 工控資安防禦，必須考量整合防火牆與實體隔離設備之單向傳輸技術。最後

唐顧問簡單分享導入 IEC62443 工控標準證書，因應物聯網發展，以減少工控資安的風險。

最後議程 Q&A 時段，線上與會的企業人士相當踴躍提出詢問。首先第一個問題詢問「想了解加入聯盟的方式及實際對公司的好處？」TWCERT/CC 曲工程師答覆：可透過 TWCERT/CC 官網上有詳細申請規章，並下載聯盟申請書，再將貴公司用印完成申請書與證明文件寄至 TWCERT/CC 信箱，大約需要 1~2 周審核時間，申請會員資格歡迎一般企業、法人團體、公私立機關。加入聯盟有優先資安預警等優點，透過提早接收 IOC 入侵指標，得知中繼站 IP 位址提早加入於貴司防火牆，可提早實施防護措施降低被攻擊可能性。

第二個問題「如果公司網路被攻擊如何通報 TWCERT/CC 以及 TWCERT/CC 如何提供協助服務」曲工程師答覆：可以於 TWCERT/CC 官網上填寫簡易資安事件通報，將有專員連繫公司先行了解資安事件狀況，給予初步事件調查的建議，未來若需要後續相關協助處理，將會引薦國內專業資安單位協助事件調查。

第三個問題「現在遠距會議的軟體很多，該怎麼選擇安全性高的遠距會議軟體」中揚資訊唐顧問答覆：市面上會議軟體很多基本有安全防護，一般建議減少使用大陸軟體，企業遠端連線時建議使用跳板機並進行監控，方便後續發生資安事件能借由 Log 調查來源控管。

第四個問題「請問 Local 端以 VPN 連線公司 VDI 環境想執行雙因素驗證，有什麼建議的解決方案或想法?」唐顧問答覆：加密通道 VPN 是常見的防護方法，一般建議可以加裝 SSL 強化通道安全，另外 VDI 提供雙因子認證可加購這個部份來強化，或是購買市面上單一線路系統 SSO，選擇多種驗證的方式都可強化公司資安。

本次場資安防護及案例分享研討會桃園場共 59 人與會，經由兩位專業講師的資安探討，與會人員皆受益良多，以及認識 TWCERT/CC 詳細的服務內

容。經會後問卷調查統計，與會的企業人士對本場研討會的內容、講師專業度及場地滿意度等皆十分滿意。

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、多國 APT 駭侵者假扮記者駭入媒體，情況日趨嚴重

Proofpoint 發表研究報告，指出多個國家的 APT 駭侵團體，近年來開始採用各種方法針對各國媒體發動駭侵攻擊行動，包括針對記者的魚叉式釣魚攻擊，或是假扮記者監控重點目標等。

資安廠商 Proofpoint 日前發表研究報告，該公司旗下多位資安專家聯合撰文，指出多個國家的「進階持續性威脅」（Advanced Persistent Threat, APT）駭侵團體，近年來開始採用各種方法針對各國媒體發動駭侵攻擊行動，包括針對記者的魚叉式釣魚攻擊，或是假扮記者監控重點目標等，情況日趨嚴重，各國政府與新聞媒體暨從業人員，應特別提高警覺。

報告中指出，由於新聞媒體經常握有各種尚不為外界所知的情報和機敏資訊，也有許多重要的採訪對象，極具駭侵監控價值與誘因，因此新聞媒體本身及其從業人員，以及重要的採訪諮詢對象，都是各國 APT 駭侵團體的重點攻擊目標。

報告中指出，目前已證實一個稱為「Zirconium」（TA412）的駭侵團體，自 2021 年初起就透過魚叉式釣魚信件，鎖定美國多個媒體旗下的記者進行駭侵攻擊，以釣魚信件植入惡意軟體，收集記者本人所在地、IP、ISP 等資

訊，並竊取記者的通訊內容；而自 2022 年 2 月起，Zirconium 集中火力攻擊專門報導烏俄戰爭的記者群。

報告也指出，自 2022 年 4 月起，另一個駭侵團體 TA459，針對追蹤報導阿富汗外交政策的媒體與其人員發動攻擊，以稱為 Chinoxy 的惡意軟體藏於信件中的 RTF 檔中。

駭侵團體 TA404 則於 2022 年春起，開始透過詐騙挖角方式，攻擊媒體從業人員；駭侵團體 TA482 則試圖竊取媒體與人員使用的社群平台帳號。

報告也指出，駭侵團體 TA453 的攻擊方式不太一樣，是假冒成媒體記者，對重要的中東政策研究學者寄出假稱採訪的釣魚信件；而駭侵團體 TA456 則是假冒 Fox News 與 Guardian 來發送釣魚電子報，在電子報中夾藏惡意連結。

由於媒體掌握相當多的未公開情報，對社會也具有較大影響力，因此媒體組織本身與其從業人員，都應加強防範各種駭侵攻擊；經常受訪的人士也應提高警覺，確認訪問者的身分，勿隨意開啟郵件附檔與連結。

- 資料來源：
  1. Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media
  2. Hackers pose as journalists to breach news media org’s networks

3.1.2、資安統計指出，2022 年第 2 季遭冒名用於釣魚攻擊的最大品牌仍為 LinkedIn

資安廠商公布 2022 年第 2 季釣魚攻擊統計，常被駭侵者冒名用於釣魚攻擊的品牌中，求職社群網站 LinkedIn 高居首位。

資安廠商 Check Point 日前公布 2022 年第 2 季釣魚攻擊統計，在常被駭侵者冒名用於釣魚攻擊的全球各大品牌中，求職社群網站 LinkedIn 仍然如先前的統計一樣高居首位，且冒名比例遠高於其他品牌。

Check Point 的報告指出，和上一季的數字相比，雖然 LinkedIn 的冒名釣魚比例自 52% 下降到 45%，但仍然高居所有常遭冒名品牌的第一名。

其他在這次冒名榜上的大品牌，及其遭冒名的比例，分別為 Microsoft（13%）、DHL（12%）、Amazon（9%）、Apple（3%）、Adidas（2%）、Google（1%）、Netflix（1%）、Adobe（1%）、HSBC（1%）。

報告說，駭侵者最常冒名 LinkedIn 寄送給用戶的釣魚郵件，通常是假冒「你的檔案本周已有 100 人瀏覽」，或是「你有一封新的未讀訊息」之類的通知信件；而寄件者的 email address 通常看起來會很像 LinkedIn 官方的支援服務或資安團隊所發。

有些其他冒名 LinkedIn 的釣魚信，則會詐稱用戶獲得免費升級至 LinkedIn Pro 專業版，或是詐稱進行系統升級，甚至指稱用戶因違反使用條款而將遭停權，以誘使用戶點按信中的惡意連結。

用戶點按惡意連結後，即會被導入到釣魚網頁，誘使用戶輸入其 LinkedIn 的登入資訊；駭侵者再利用該登入資訊，來對受害者在 LinkedIn 上

的同事或有價值的目標，發動進一步的駭侵攻擊。

建議收到疑似釣魚攻擊的不明郵件時，切勿點按信中的惡意連結或開啟不明檔案，應先確認寄件人 Email Address 的正確性，或是直接忽略該信件。

- 資料來源：
  1. LinkedIn Still Number One Brand to be Faked in Phishing Attempts while Microsoft Surges up the Ranki
  2. LinkedIn remains the most impersonated brand in phishing attacks

3.2、新興應用資安

3.2.1、資安廠商揭露 NFT 遊戲平台 Axie Infinity 三月被駭 5.4 億美元原因

NFT 遊戲平台 Axie Infinity，曾於今年三月時發生駭侵事件；區塊鏈媒體調查指出，該起攻擊事件係由 APT 組織 Lazarus 成員混入平台竊得重要金鑰所致。

全球熱門 NFT 遊戲平台 Axie Infinity，曾於今（2022）年三月時發生損失高達 5.4 億美元的駭侵事件；日前一家名為 The Block 的區塊鏈專業媒體發表調查報告，指出該起攻擊事件係由 APT 組織 Lazarus 成員應徵該平台資深工程師職務，混入平台後進而竊得重要金鑰所致。

Axie Infinity 是目前全球熱門的 NFT 遊戲平台之一，主打「邊玩邊賺」模式，玩家只要在平台內購買以 NFT 型式販售的虛擬寵物和道具，即可透過對戰和寵物養成買賣來賺取利潤。最熱門時每日活躍用戶高達 270 萬人，每周交易額高達 2.14 億美元；甚至在菲律賓等東南亞國家，更有許多人靠替玩家代練虛擬寵物維生。

The Block 在近日推出的調查報告中說，該平台遭駭是因為 APT 團體成員，以空頭公司透過求職求才社群平台 LinkedIn，對 Axie Infinity 內部資深工程師進行高薪挖角，並發給獲得「錄取」的 Axie Infinity 工程師一個含有惡意程式碼的 PDF 檔做為錄取通知書，藉以駭入 Axie Infinity 使用的以太坊區塊鏈側鏈 Ronin 的系統內。

該報告指出，Lazarus 的駭侵者在成功入侵 Ronin 的系統後，很快就在 3 月 23 日取得了在 Ronin 上負責驗證交易的 9 個驗證者中的其中 5 個，因而可以控制交易驗證。資安專家表示，Axie Infinity 的區塊鏈交易問題不只是出在驗證者數量過少，更是因為這些驗證者都集中在一處，不夠分散，因此才會讓駭侵者一次掌握過半的驗證者，可以任意操作交易結果。

在 3 月發生的該起駭侵攻擊中，Lazarus 共取得高達 173,600 枚以太幣，以及 2,550 萬枚 USDC 穩定幣，以當時幣價來看，相當於 5.4 億美元，是一次十分成功的魚叉式釣魚攻擊。

鑑於駭侵者用以植入惡意軟體的手段愈見多元，建議掌握大量金流或用戶個資的公私單位，都必須加強釣魚攻擊的對抗能力，並且嚴格要求工作者禁止利用工作用電腦存取私人資源。

- 資料來源：
  1. How a fake job offer took down the world’s most popular crypto game
  2. Popular NFT Marketplace Phished for $540M

3.2.2、區塊鏈音樂平台 Audius 遭駭，損失達 600 萬美元

去中心化區塊鏈音樂平台 Audius，據傳於上周末遭到駭侵攻擊，導致 1,800 萬枚 AUDIO 代幣遭竊，換算成美元的損失高達 600 萬美元。

該平台於 7 月 24 日在 Twitter 上發表聲明，指出該公司已發現系統遭到不當存取；該公司暫時停止部分系統功能運作，以防駭侵者進一步攻擊。

該平台於隔日發表事件調查報告，指出駭侵者係利用其合約啟動模組中的一個漏洞發動攻擊，導致社群儲備資金有近 1,850 萬枚 AUDIO 代幣遭到竊走；此外駭侵者還試圖利用去中心化平台的投票機制，發動四個將所有社群儲備代幣轉帳至駭侵者錢包的投票，其中三個投票通過，一個未能通過。

Audius 平台是一個透過以太坊區塊鏈架設的串流音樂平台；音樂創作者在 Audius 平台上分享音樂時，可賺取 AUDIO 代幣；而用戶聆聽平台上的音樂或分享音樂，也可以賺取代幣。

駭侵者在竊得這批代幣後，隨即在去中心化交易所 UniSwap 中交易其竊得的代幣，將其交換為隱匿行蹤能力更佳的 Tornado Cash 代幣；但出售金額僅為 107 萬美元，其價值減損高達六分之五。

該公司表示，其系統於 2020 年 8 月與 2021 年 10 月兩度通過兩家不同區塊鏈資安公司的稽核，但沒有任何一家發現這次遭駭侵者利用的漏洞。

該公司目前系統已恢復運作，但代幣質押與委任的部分智慧合約功能仍

在修復中，尚未開放使用。

由於這類加密貨幣平台漏洞，經常可能造成用戶的鉅額資金損失，建議加密貨幣投資人應避免將資產過度集中於單一平台或協定，且應妥善保管數位錢包的恢復短語。

- 資料來源：
  1. Audius @AudiusProject
  2. Hackers steal $6 million from blockchain music platform Audius

3.3、國際政府組織資安資訊

3.3.1、CISA 發布五個影響工業控制系統漏洞資安警訊

美國 CISA 發布 5 個影響工業控制系統的漏洞資安警訊，要求使用這些工業控制系統的生產單位，應立即修補漏洞。

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 5 個影響工業控制系統的漏洞資安警訊，要求使用這些工業控制系統的生產單位，應立即依通報中的處理方式修補漏洞，以免遭到駭侵者利用這些漏洞發動攻擊。

第一個漏洞警訊指出的漏洞，存於 Inductive Automation Ignition 8.1.9 與 7.9.21 之前的較舊版本內，其漏洞 CVE 編號為 CVE-2022-1704，CVSS v3 漏洞危險程度評分為 8.5 分（滿分為 10 分）；該漏洞可導致駭侵者能夠存取系統內的檔案，造成機敏資訊外洩。

第二個漏洞警訊共含 4 個漏洞，其中有 3 個存於 Honeywell Safety Manager 所有版本內（CVE-2022-30315、CVE-2022-30313、CVE-2022-30316），另一個漏洞 CVE-2022-30314 存於 R160.1 前的較舊版本中，其 CVSS v3 漏洞危險程度評分為 7.7 分（滿分為 10 分）。這批漏洞可導致駭侵者能夠進行系統組態、操弄韌體，其至遠端執行任意程式碼。

第三個漏洞警訊共含 2 個漏洞，均存於 Honeywell Saia Burgess PG5 PCD 所有版本內，其 CVSS v3 漏洞危險程度評分為 7.6 分（滿分為 10 分）。這批漏洞可導致駭侵者跳過身分認證進行系統組態操弄。

第四個漏洞警訊共含 2 個漏洞，均存於 MOXA NPort 5110 版本 2.10 內，其 CVSS v3 漏洞危險程度評分為 8.2 分（滿分為 10 分）。這兩個漏洞可導致駭侵者變更記憶體內的數值，並且造成機器設備無法操作。

第五個漏洞警訊共含 3 個漏洞，均存於 Mitsubishi Electrics MELSEC 與 MELIPC 系列多個版本內，其 CVSS v3 漏洞危險程度評分為 7.5 分（滿分為 10 分）。這三個漏洞可導致駭侵者利用設備發動 DoS 攻擊，系統必須重新啟動才能修復。

建議採用上列工業控制系統的業者，應立即按照 CISA 在各該漏洞通報的處理建議進行必要處分，例如更新韌體版本或強化資安設定。

- 資料來源：
  1. ICS Advisory (ICSA-22-207-01)
  2. ICS Advisory (ICSA-22-207-02)
  3. ICS Advisory (ICSA-22-207-03)
  4. ICS Advisory (ICSA-22-207-04)
  5. ICS Advisory (ICSA-21-334-02)

3.3.2、西班牙警方逮捕涉嫌攻擊該國核安警報網路的駭侵者

西班牙警方發布通報，宣布逮捕兩名據信涉嫌於去年三月與六月間駭侵該國輻射警報系統網路的駭侵者；相關單位已經展開進一步的偵訊。

據報導，這兩名嫌犯先前曾在該國負責維運輻射警報系統網路部門「民眾保護與緊急事件指揮總署」（General Directorate of Civil Protection and Emergencies, DGPCE）的外包業者工作，對於整個系統的運作，以及如何駭入，具有深厚的知識。

兩名嫌犯遭控訴試圖非法存取 DGPCE 所屬網路，企圖刪除輻射警報網路系統在控制中心的 web 應用程式。

兩名嫌犯也涉及攻擊分布於西班牙全國各地的輻射偵測設施；全國八百多組輻射偵測設施中，有三百多組遭其攻擊，無法於中央輻射警報系統連線並傳輸資料。

該單位是在 2021 年 6 月起發現系統遭到攻擊，在與西班牙警方協同偵辦長達一年後，才掌握兩名犯嫌的行蹤並予以逮捕，同時緝獲多台可能與犯行相關的電腦與網通設備。

據報導，西班牙境內目前共有 7 座運作的的核反應爐，發電量占該國總電力需求的 20%；而其輻射偵測設施的任務，是發現突然增高的輻射量，以立即找出原因予以處理；該系統共有 800 多個分布在西班牙各地的輻射偵測設施，以電話線與 DGPCE 總部連線，回報即時輻射偵測數值。

該兩名嫌犯成功使 300 多個輻射偵測設施離線無法運作，使得政府無法即時反應潛在的核能安全事故；對於該國核能安全造成嚴重威脅。

建議針對這類可能造成嚴重公共安全事故的關鍵基礎設施與其防護系統，應加強其實體與資安防護能力，同時加強在離職人員的考核，以嚴防滲透與不當存取，以及惡意破壞行為。

- 資料來源：
  1. La Policía Nacional detiene a los presuntos autores del sabotaje informático a la Red de Alerta a la
  2. Spain arrests suspected hackers who sabotaged radiation alert system

3.4、社群媒體資安近況

3.4.1、駭侵者利用 Twitter Android App 漏洞，竊得 540 萬名用戶資料求售

資安媒體 Restore Privacy 日前發布新聞，指出資安專家發現有駭侵者在駭侵相關論壇上出售 540 萬 Twiiter 用戶的個資；該批個資係透過 Twitter Android App 中的一個漏洞取得。

據 Restore Privavy 指出，駭侵者很可能是利用 Twitter Android App 中的一個漏洞來取得這些個資。該漏洞可讓任何人在不需任何驗證的情形下，只要提供電話號碼或 Email 信箱，即可取得用戶的 Twitter ID，這相當於取得該用戶的登入名稱。

有了這個 Twitter ID 後，駭侵者就可以取得用戶在其個人檔案中輸入的各種資訊，並且利用這些資訊，進一步取得更詳細的個資，並在駭侵相關論壇上出售這批資訊，要價 3 萬美元。

Twitter 官方尚未證實這起資安事件，但資安媒體根據部分流出的資訊進行驗證，發現這些個資屬實的可能性相當高。

資安專家指出，駭侵者除了可以出售這批個資牟利之外，還可以進一步利用這些個資，發動進一步的攻擊，例如釣魚攻擊等等。

雖然該漏洞已在今（2022）年 1 月 13 日就獲得修復，但資安媒體與試圖出售資料的駭侵者聯絡時，駭侵者表示資料是於去（2021）年開始收集的。

由於這類可歸因於社群平台或服務商的漏洞，用戶比較難以防範，因此用戶應避免在社群平台上公開個人或服務機構相關的機敏資訊（如真實姓

名、 Email 地址、電話號碼、重要證件編號、居住地址、所在地等），以避免駭侵者以類似手法竊得個資。

- 資料來源：
  1. Verified Twitter Vulnerability Exposes Data from 5.4 Million Accounts
  2. Hacker selling twitter account data of 54 million users for 30k.

3.4.2、駭侵者竊取經驗證的 Twitter 帳號，發送詐騙帳號停權訊息

資安媒體報導指出，近來有駭侵者竊取經過官方驗證的 Twitter 帳號發送詐騙訊息，騙取 Twitter 帳號登入資訊。

資安媒體 BleepingComputer 報導指出，該刊發現近來有駭侵者竊取經過官方驗證的 Twitter 帳號，然後利用這些帳號發送詐騙訊息，假稱用戶即將遭到停權，藉以騙取其 Twitter 帳號登入資訊。

這些被利用的官方驗證帳號，是經由 Twitter 官方審核過，可證明其真實存在，且具備一定程度社群影響力的帳號；在其帳號處會顯示一個特別的藍色勾勾標誌。

由於這類帳號並不容易取得，又有 Twitter 官方背書保證，通常會有較多的追蹤者，也容易取得大眾的信任，因此特別容易成為駭侵者的目標。

以這次事件來說，BleepingComputer 的記者 Sergiu Gatlan 在其 Twitter 帳號收到一封來自經驗證帳號的私訊，私訊內容假冒 Twitter 官方的支援團隊，指稱收訊人因為曾在 Twitter 上發表過仇恨言論，因此將於 48 小時內將該帳號予以停權；若用戶想要申訴以撤回停權處分，需點按訊息中的短網址連結。

該名記者為了追蹤這則釣魚假訊息，點按了訊息中的短網址連結，即被導向到一個看起來極為類似 Twitter 支援中心的登入畫面，但其呈現在瀏覽器中的網址，並非 Twitter 官方的 twitter.com 網域。

記者試著輸入該刊擁有的測試用 Twitter 帳號，該頁面就利用 Twitter API 取得該帳號在 Twitter 使用的頭像，加強用戶的信任感，並進一步要求輸入登入密碼。

資安專家指出，這類盜用知名人士經驗證帳號進行的詐騙，近日有逐漸增加的趨勢；因此各種社群平台用戶收到這類可疑訊息時，務必再三確認真偽，切勿輕信內容而誤點連結。

- 資料來源：
  1. Verified Twitter accounts hacked to send fake suspension notices
  2. Cory Doctorow @doctorow

3.4.3、駭侵者利用 Facebook 廣告散布 Google Play 中的惡意廣告 App

資安廠商發現有駭侵者利用 Facebook 廣告，散布上架至 Google Play Store 中的多個廣告惡意軟體。

資安廠商 McAfee 旗下的研究人員，近日發現有駭侵者利用 Facebook 廣告來散布上架至 Google Play Store 中的多個廣告惡意軟體；這些惡意 App 目前已有 700 萬次下載安裝。

McAfee 的報告指出，這幾個成功上架到 Google Play Store 的廣告惡意軟體，偽裝成多種用戶可能需要的類型，包括 Android 系統清理工具、手機執行效能提升工具等等，但實際上不但缺少宣稱的功能，本質上更是廣告惡意軟體。

報告指出，這些廣告惡意 App 係濫用 Contact Provider Android 組件，該組件可讓裝置與線上服務之間互相傳輸資料；每次安裝軟體時都會呼叫該組件，這些廣告軟體便趁機啟用廣告推送程序，讓用戶以為廣告是由他們新安裝的 App 所顯示的。

為了避免遭到用戶刪除，這些廣告 App 還經常更換其顯示圖示與名稱，偽裝成 Android 系統設定或 Play Store 應用程式，以混淆用戶視聽。

McAfee 指出，目前所知這些惡意 App 共有 13 種；由於 Facebook 廣告的散布助力，總下載次數高達 700 萬次以上；這 13 種 App 在 Google Play Store 中的名稱如下：

- Junk Cleaner
- EasyCleaner
- Power Doctor
- Super Clean
- Full Clean
- Fingertip Cleaner
- Quick Cleaner
- Keep Clean
- Windy Clean
- Carpet Clean
- Cool Clean
- Strong Clean
- Meteor Clean

McAfee 表示，受害用戶最多的國家包括南韓、日本、巴西等，但全世界各地也都有不少受害者。

建議用戶在下載各種 Android App 前，應仔細閱讀評價，如發現可疑之處，或有許多用戶給予負面回饋，應避免下載；對於透過社群平台廣告宣傳的 App，亦應提高警覺。

- 資料來源：
  1. New HiddenAds malware affects 1M+ users and hides on the Google Play Store
  2. Facebook ads push Android adware with 7 million installs on Google Play

3.5、行動裝置資安訊息

3.5.1、Google Play Store 中再現惡意軟體，下載次數達 300 萬次

資安廠商發表研究報告，指出發現多個 Google Play Store 中的各類 Android 應用程式，內含一個會偷偷幫用戶訂閱高價服務，藉以賺取不法利益的惡意軟體 Autolycos。

資安廠商 Evina 旗下的資安專家 Maxime Ingrao 近日發表研究報告，指出發現多個 Google Play Store 中的各類 Android 應用程式，內含一個會偷偷幫用戶訂閱高價服務，藉以賺取不法利益的惡意軟體 Autolycos；這些應用程式的總下載次數已經超過 300 萬次，Android 用戶需特別提高警覺。

據指出，Autolycos 這個惡意軟體，會在用戶不知情的情形下，悄悄透過遠端瀏覽器開啟 URL，而不使用 Webview，以避免遭到裝置上作業系統與防毒防駭軟體的偵測，用戶本人也更難以發現。

Maxime Ingrao 指出，目前已知至少有 8 個含有 Autolycos 惡意軟體的 Android 應用程式，在 Google Play Store 中上架，其中有 6 個已遭 Google 下架，其名稱與下載次數分別如下：

- Vlog Star Video Editor (com.vlog.star.video.editor) – 1 百萬次
- Creative 3D Launcher (app.launcher.creative3d) – 1 百萬次
- Wow Beauty Camera (com.wowbeauty.camera) – 10 萬次
- Gif Emoji Keyboard (com.gif.emoji.keyboard) – 10 萬次

- Freeglow Camera 1.0.0 (com.glow.camera.open) – 5 千次
- Coco Camera v1.1 (com.toomore.cool.camera) –1 千次

Maxime Ingrao 於 2021 年 6 月發現這些含有 Autolycos 惡意軟體的應用程式後，立即通報 Google 進行處理；Google 雖然當時回應表示將進行處理，但過了 6 個月後，只移除了 8 個惡意 app 中的 6 個，另外還有 2 個 App 直到 Maxime Ingrao 近日公布其發現後才予以下架，分別是 Funny Camera by KellyTech 以及 Raxer Keyboard & Theme by rxcheldiolola，各有 50 萬次下載。

建議用戶即使在官方管道下載 App，也應注意檢視用戶評價與評論，如發現評價中有異常之處，應避免下載安裝該 App。

- 資料來源：
  1. Maxime Ingrao @IngraoMaxime
  2. New Android malware on Google Play installed 3 million times

3.5.2、資安專家發現 ExpressLRS 漏洞，可用以挾持無人機

資安廠商發現一種通用於無人機遙控器與機體間，無線通訊的開源通訊協定 ExpressLRS 存有資安漏洞。

資安廠商 NCC Group 旗下的資案專家，近日發現一種通用於無人機遙控器與機體間無線通訊的開源通訊協定 ExpressLRS 存有資安漏洞，可導致駭侵者跳過配對過程，直接挾持其他人所有的無人機。

據報告指出，ExpressLRS 是一種高效能的開源無線電控制連線公用程式，可透過 900MHz 與 2.4GHz 公眾無線頻道來控制各種無線電裝置，並且廣泛使用於各型無人機或無人遙控載具上。

研究人員說，在 ExpressLRS 進行控制器與遙控裝置的連線時，使用一種稱為「綁定短語」（binding phrase）的方式當做配對用的金鑰，而 binding phrase 金鑰的設計目的並非為了資安，而是要避免與其他無線控制裝置相互衝突。該金鑰係寫入於韌體中。

研究人員指出，他們找到一種方法用以破解該密鑰：先取得共享於控制器與遙控裝置之間的部分識別資訊，然後運用一種結合分析與暴力試誤法的軟體，找出完整的識別資訊後，即可跳過裝置間的配對過程，直接控制目標遙控裝置。

研究人員指出，一旦這種駭侵技術遭到大規模濫用，很可能造成無人載具隨時面臨被挾持的風險，甚至於失控墜毀。

為強化 ExpressLRS 的傳輸安全性，建議用戶不要在控制連線期間傳送任何 UID 資訊，以免遭到駭侵者攔截資料並算出連線金鑰；另外也建議無線遙控載具廠商強化其亂數產生器，以更安全的演算法計算出更難以破解的亂數，以增加暴力試誤的難度與所需時間。

- 資料來源：
  1. Technical Advisory – ExpressLRS vulnerabilities allow for hijack of control link
  2. Hack Allows Drone Takeover Via ‘ExpressLRS’ Protocol

3.5.3、Google Play 中藏有三種惡意 Android 軟體，下載次數達 30 萬次

資安廠商指出 Google Play Store 中發現 3 種不同的 Android 惡意軟體，藏身於多個 Android App 之中，總下載次數達 30 萬次以上。

資安廠商 ZScaler 旗下的研究單位 ThreatLabz，日前發表研究報告，指出 Google Play Store 中發現 3 種不同的 Android 惡意軟體，藏身於多個 Android App 之中，總下載次數達 30 萬次以上。用戶若不慎下載安裝這些軟體，就會遭惡意軟體各種不同形態的攻擊。

第一種惡意軟體稱為「Joker」，用戶一旦感染這種惡意軟體，Joker 即會竊取用戶 Android 裝置內的多種資訊，包括簡訊內容、通訊錄中的聯絡人資訊，還會擅自訂購多種高價服務，造成用戶行動帳單費用暴增。

已知 Joker 藏身於多達 50 個 Google Play Store 中上架的 App 內，其中有一半以上是通訊軟體；由於這類 App 需要用戶給予較多存取權限（例如麥克風、攝影機、相簿、通訊錄、電話撥打、簡訊讀寫與傳輸等），因此往往是惡意軟體藏身的首選。

第二種惡意軟體稱為「Facestealer」，顧名思義，該惡意軟體專以釣魚網頁竊取用戶的 Facebook 登入資訊。

資安專家指出，Facestealer 藏身於一個叫做 Valina Snap Camera 的拍照 App 中，下載次數約有 5,000 次。

第三種惡意軟體名為「Coper」，也是一種資訊竊取惡意軟體，除了會攔截用戶的簡訊內容外，也會竊取鍵盤輸入字元、透過畫面覆疊誘使用戶輸入機敏資訊、發送惡意簡訊，並將攔截到的內容傳回駭侵者設立的控制伺服器。

ZScaler 指出有一個叫做 Unicc QR Scanner 的 App 內含 Coper 惡意軟體，感染裝置約在 1,000 台左右。

建議用戶即使透過官方的 App 商店下載安裝手機軟體，也應提高警覺，於下載前仔細檢閱說明與用戶評價；如果 App 出現可疑行為，如要求輸入各種登入資訊，或要求過多權限，也應立即停用並移除。

- 資料來源：
  1. Joker, Facestealer and Coper banking malwares on Google Play store
  2. Malicious Android apps with 300K installs found on Google Play

3.5.4、Roaming Mantis 惡意軟體針對多國跨平台行動裝置用戶發動釣魚攻擊

資安廠商 SEKOIA 日前指出，一波稱為 Roaming Mantis 的大規模攻擊行動，正在多個國家進行中。

資安廠商 SEKOIA 日前指出，一波稱為 Roaming Mantis 的大規模攻擊行動，正在多個國家進行中；現在更針對兩大平台行動裝置用戶發動惡意軟體植入與釣魚攻擊，意在騙取用戶的金融資產。

SEKOIA 指出，Roaming Mantis 的攻擊行動，過去曾在德國、台灣、南韓、日本、美國、英國等地大肆發動攻擊，現階段則是重點集中在攻擊法國境內的行動裝置用戶。

SEKOIA 說，該公司是在今（2022）年 2 月份開始觀測到 Roaming Mantis 於歐洲的駭侵攻擊活動；近來該攻擊的形態則是以詐騙簡訊進行。如果 Android 用戶誤點簡訊中的惡意連結，就會將惡意軟體下載到裝置內；如果是 iOS 用戶點按惡意連結，則會被導向到一個釣魚網頁，誘使用戶輸入其 Apple 帳號登入資訊。

SEKOIA 在報告中分析，安裝在 Android 手機中的軟意軟體稱為 XLoader (MoqHao) 酬載，功能非常強大，能夠進行諸如遠端遙控、資訊竊取、發送垃圾簡訊等操作。

目前針對法國用戶發送的垃圾簡訊，其內容是詐稱有貨物包裹即將寄達受害者，需要受害者點按連結，以進行進一步的確認並指定送達地點。法國

境內用戶會因其使用的手機平台，而有上述的不同攻擊方式，而法國境外的用戶，只會看到 404 錯誤頁面。

SEKOIA 的觀測報告指出，在 Roaming Mantis 這波針對法國用戶的攻擊中，已觀測到高達 7 萬個不重覆 IP 存取駭侵者設立的控制伺服器，並發出 XLoader 惡意軟體下載要求；iOS 的釣魚頁面存取數量不明，但想必會比 Andoird 更多。

建議行動裝置用戶收到不明簡訊時，切勿點擊內含連結，應直接將該不明簡訊設定為垃圾內容；如不慎誤點連結，也不要下載安裝任何軟體，或輸入任何登入資訊。

- 資料來源：
  1. Ongoing Roaming Mantis smishing campaign targeting France
  2. Ongoing 'Roaming Mantis' Smishing Campaign Hits Over 70,000 Users in France

3.6、軟體系統資安議題

3.6.1、Microsoft：一場針對上萬企業發動的釣魚攻擊，跳過多階段登入驗證成功入侵

Microsoft 發表研究報告指出，一波進行中的大規模釣魚攻擊，鎖定 10,000 家以上公私單位發動駭侵攻擊。

Microsoft 日前發表研究報告，指出目前正有一波進行中的大規模釣魚攻擊，鎖定 10,000 家以上公私單位發動駭侵攻擊；特別的是，該攻擊可以挾持受害者的 Office 365 登入驗證程序，即使是以多重驗證機制保護的登入程序亦可破解。

據 Microsoft 的資安通報指出，駭侵者使用了可以挾持 Office 365 登入程序頁面的釣魚入口網頁，當受害者收到釣魚信件，點按信件中的釣魚連結後，就會被導到釣魚網頁入口，在竊得用戶輸入的登入資訊和操作階段 cookie 後，還會透過代理（proxy）手段，將收到的多重驗證碼輸入頁面轉給用戶，由用戶輸入驗證碼後，再由駭侵者「代為登入」後，駭侵者即可進入目標系統中，進行進一步的駭侵攻擊。

Microsoft 在報告中稱這種攻擊手法為 Adversary-in-the-middle(AiTM），且這種攻擊手法可以使用如 Evilginx2、Modlishka、Muraena 等多種開源釣魚攻擊工具來進行自動化操作。

Microsoft 指出，該公司透過分析來自 Microsoft 365 Defender 的各種資料，發現自 2021 年 9 月起，這類 AiTM 攻擊便大量出現，攻擊對象超過 10,000 家以上公私單位。

為抵禦日益增加的 AiTM 攻擊，Microsoft 建議使用以憑證為基礎，且支援 Fast ID Online (FIDO) 2.0 的多重登入驗證流程，同時也要特別注意可疑的登入以及信箱活動，並且以條件限制未登錄的裝置或不在信任白名單內的 IP 存取內網資源。另外，終端用戶也應避免點擊或開啟疑似釣魚郵件中的連結與附件。

- 資料來源：
  1. From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial frau
  2. Microsoft: Phishing bypassed MFA in attacks against 10,000 orgs

3.6.2、QNAP 提醒用戶近期出現針對密碼強度不足的裝置發動之 Checkmate 勒贖攻擊

QNAP 近來發現一波新的 Checkmate 勒贖攻擊；主要針對使用者密碼強度不足，且對外網啟用 SMB 連線服務的裝置進行攻擊。

台灣專業網路儲存設備廠 QNAP (威聯通)推出各型網路儲存裝置（Network Attached Storage, NAS），近來發現一波新的 Checkmate 勒贖攻擊；該攻擊主要針對使用者密碼強度不足，且對外網啟用 SMB 連線服務的裝置進行攻擊。

在 QNAP 發表的資安通報中指出，Checkmate 勒贖攻擊主要針對如上所述，開啟了 SMB Windows 檔案分享服務，且裝置直接連上 Internet 的 NAS 裝置，發動字典檔暴力試誤登入攻擊；如果裝置使用預設登入帳號與弱密碼，就很可能遭到駭侵者成功登入，並將裝置上的檔案進行加密。

QNAP 在資安通報中表示，目前正在調查該駭侵事件；該通告也針對本駭侵攻擊的防範方式提出建議。

QNAP 各型 NAS 裝置用戶，應依 QNAP 資安通報與資安專家的建議，立即採取以下行動：

- 避免直接讓裝置的 SMB 服務在外部 Internet 上曝露；如需自外網連線裝置的 SMB 協定，可參照該公司提供的操作指南，透過 VPN 連線來進行資料存取。
- 停用 SMB 1。

- 將使用中的 QNAP 裝置更新到最新版 QNAP 作業系統。
- 立即審視所有 NAS 上的使用者帳號，確認密碼強度足夠。
- 定期備份檔案並執行檔案快照作業。
- 將系統預設的 admin 帳號停用，改用其他不容易被猜到的帳號設定為系統管理員專用帳號。
- 在系統防火牆中設定規則，將多次嘗試登入失敗的 IP 列入黑名單，禁止再次連線。

- 資料來源：
  1. Checkmate Ransomware via SMB Services Exposed to the Internet
  2. QNAP warns of new Checkmate ransomware targeting NAS devices

3.6.3、駭侵者透過 Sality 惡意軟體，破解多廠牌工控設備的登入密碼

資安廠商發現有駭侵者在網路上販售可破解多個廠牌工業控制設備中，可程式化邏輯控制器登入密碼的軟體。

資安廠商 Dragos 旗下的資安專家，近日發現有駭侵者在網路上販售可破解多個廠牌工業控制設備（Industrial Control System, ICS）中「可程式化邏輯控制器」（Programmable Logic Controller, PLC）登入密碼的軟體，受影響產品的製造商遍及歐美日韓各大廠牌，嚴重影響各種工業設備的安全。

據報告指出，駭侵者在其社群媒體帳號中宣稱，能夠破解各大廠牌 PLC 與人機介面（Human-machine Interface, HMI）的登入密碼，受影響的廠牌包括 Automation Direct、Omron、Siemens、Fuji Electric、Mitsubishi、LG、Pro-Face、Allen、Bradley、Weintek、ABB、Panasonic 等。

據 Dragos 指出，該公司是在研究分析發生於 Autoation Direct 生產的 DirectLogic PLC 相關資安事件時，發現了有破解軟體可利用該裝置的一個已知漏洞，來取得登入密碼。

Dragos 同時指出，該破解軟體也會試圖安裝一個名為 Sality 的惡意軟體，可在使用者的電腦中建立一個同儕僵屍網路，用以發動後續的各種駭侵攻擊。

資安專家說，Sality 是一個頗有歷史的老舊惡意軟體，除了可以下載額外酬載、竊取宿主電腦內的資訊外，也能透過 Windows 網路、外接式儲存裝置等來進行散布，以發動各式不同的駭侵攻擊。

Dragos 表示，如果工業製造廠的工程師，為了快速找出 PLC 的登入密碼，而濫用這類破解工具，就很可能造成整個工業製造系統的資安危機。

建議各製造業者應嚴令禁止使用這類來路不明的密碼破解工具，如需取回密碼，應依正規管道尋求原廠支援；製造業者對工業系統的資安防護能力亦應加強，當有人員便宜行事，導致惡意軟體入侵時，才能予以偵測防範。

- 資料來源：
  1. The Trojan Horse Malware & Password “Cracking” Ecosystem Targeting Industrial Operators
  2. Password recovery tool infects industrial systems with Sality malware

3.6.4、搭載 Intel H81 晶片組的部分主機板發現 UEFI rootkit 惡意軟體

資安廠商發現搭載 Intel H81 晶片組的部分主機板產品，其 UEFI 的韌體程式碼中發現 CosmicStrand 的 rootkit 惡意軟體。

資安廠商 Kaspersky 日前發現，搭載 Intel H81 晶片組的部分主機板產品，其 UEFI 的韌體程式碼中發現一個名為 CosmicStrand 的 rootkit 惡意軟體，且可追溯至 2016 年底。

UEFI（Unified Extensible Firmware Interface）是主機板韌體與作業系統的溝通橋樑，是電腦開啟電源時最先執行的程式碼；執行完此程式碼後，才會載入作業系統與後續的資安防護軟體，因此 UEFI 內的 rootkit 惡意軟體，不只開發難度高，也十分難以偵測移除。

這次由 Kaspersky 資安專家發現的 ComicStrand rootkit 惡意軟體，會修改作業系統載入程序，取得電腦控制權限，並在 Windows 核心中直接執行下載自駭侵控制伺服器的惡意酬載。

資安專家表示，ComicStrand 與另一家資安廠商奇虎 360 在 2017 年發現的另一個 rootkit 惡意軟體十分接近，可以視為該惡意軟體的變種；而 Kaspersky 也指出，發現 CosmicStrand rootkit 的主機板，同樣都採用 Intel H81 晶片組，因此可以推測駭侵者可能利用 Intel H81 晶片組內的一個漏洞，來進行 CosmicStrand 的開發與布署。

Kaspersky 目前發現含有此 rootkit 的主機板，均為 2013 至 2015 間生產的舊品，目前早已停產。

Kaspersky 說明，目前尚難以發現駭侵者是用什麼手法在主機板中注入 CosmicStrand rootkit，因為必須進行裝置實體操作，才能在韌體中注入惡意軟體；目前推測是駭侵者散布含有惡意程式碼的韌體更新程式，來進行 CosmicStrand 的散布。

建議進行任何軟硬體的系統更新時，切勿使用來路不明的更新工具；請務必自產品官方網站或內建更新機制進行更新，以免感染此類惡意軟體。

主機板製造廠商也建議：

1. 客戶購買二手主機板，立即上網下載最新的官方 BIOS image 更新。若無法更新或提示型號不對，可送鄰近維修點辨認處理。
2. 若需要硬體層級的保護，可採用具有 Intel Boot Guard 或 Intel Platform Firmware Resilience 功能的主機板，並啟動 UEFI Secure Boot 功能確保 trust chain，能抵擋 ROM 元件被更換或直接燒錄的攻擊。。

- 資料來源：
  1. CosmicStrand: the discovery of a sophisticated UEFI firmware rootkit
  2. CosmicStrand UEFI rootkit found on ASUS and Gigabyte motherboards

3.7、軟硬體漏洞資訊

3.7.1、Microsoft 推出 2022 年 7 月 Patch Tuesday 資安更新包，共修復 84 個漏洞

Microsoft 發布 2022 年 7 月的例行性資安更新包；共修復多達 84 個資安漏洞，包含 1 個 0-day 漏洞。

Microsoft 日前發布 2022 年 7 月的例行性資安更新包（Patch Tuesday）；在這次發表的資安更新包中，一共修復多達 84 個資安漏洞，包含 1 個 0-day 漏洞，更有 4 個漏洞屬於嚴重（Critical）等級。

各種 Microsoft 軟體產品的用戶與系統管理員，應立即按照指南進行更新，以減少遭駭侵者利用已知漏洞發動資安攻擊的風險。

這次 Microsoft Patch Tuesday 更新修復的漏洞，依漏洞類型區分如下：

- 執行權限提升漏洞：52 個。
- 資安防護功能跳過漏洞：4 個。
- 遠端執行任意程式碼漏洞：12 個。
- 資訊洩露漏洞：11 個。
- 分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）漏洞：5 個。

這次修復的 1 個 0-day 漏洞為 CVE-2022-22047：存於 Windows CSRSS 的執行權限提升漏洞，Microsoft 在本次資安通報中指出，該漏洞能讓駭侵者成功取得系統執行權限，由 Micrisoft 內部的資安研究單位 Microsoft Threat

Intelligence Center 與 Microsoft Security Response Center 共同發現；Microsoft 證實該漏洞已遭外界駭侵者大規模濫用於發動攻擊。

- CVE 編號：
- 影響產品/版本：
- 解決方案：資安專家指出，駭侵者經常利用已公開但未經修補完成的漏洞發動攻擊，因此建議各類微軟產品的用戶，應該立即依指示更新至最新版本，以免未及修補的漏洞，成為駭侵攻擊的破口。

- 資料來源：
  1. Latest Servicing Stack Updates
  2. Microsoft Patch Tuesday

3.7.2、Django 修復可用以注入指令的嚴重資安漏洞

開源 Python 網路框架程式庫專案 Django，修復一個嚴重資安漏洞 CVE-2022-34265，駭侵者可利用該漏洞來進行指令注入。

開源 Python 網路框架程式庫專案 Django，日前推出更新版本，修復一個嚴重資安漏洞 CVE-2022-34265，駭侵者可利用該漏洞來進行指令注入；由於使用 Django 的網站與網路應用程式多，用戶應立即更新以修補該漏洞。

CVE-2022-34265 由資安廠商 Aeye Security Lab 旗下的資安專家 Takuto Yoshikai 發現，漏洞係存於 Django 的主要分支、版本 4.1 beta、4.0 與 3.2 之中，該漏洞屬於 SQL 資料庫指令注入漏洞，駭侵者可透過傳入特定的 Trunc(kind) 和 Extract(lookup_name) 參數誘發此漏洞，並且注入指令進行攻擊。

該漏洞的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），危險程度評級則為「嚴重」（Critical）等級。

不過 Django 表示，就算用戶採用的是有此漏洞的版本，如果用戶的網站與應用程式有針對 lookup name 與 kind 選擇進行輸入檢查限制，就可能不受此漏洞的影響，因為駭侵者將無法傳送惡意參數。

Django 於近日推出的 Django 4.0.6、Django 3.2.14，已將此 CVE-2022-34265 漏洞修補完成；另外針對主要分支、4.1、4.0、3.2 等舊版也推出修補工具。

由於採用 Django 框架開發的網站和網路應用程式非常多，如果有駭侵者大規模利用此漏洞發動攻擊，可能帶來很大的損失；因此採用 Django 的開發者與網站管理者，應對上線產品進行徹底檢查與必要的升級或修補，以避免遭到攻擊，造成損失。

- CVE 編號：CVE-2022-34265
- 影響產品/版本：Django 的主要分支、版本 4.1 beta、4.0 與 3.2。
- 解決方案：升級至 Django 4.0.6、Django 3.2.14 或套用修補工具。

- 資料來源：
  1. Django security releases issued: 4.0.6 and 3.2.14
  2. CVE-2022-34265
  3. Django fixes SQL Injection vulnerability in new releases

3.7.3、Google 修復 Chrome 中一個已遭用於攻擊的 0-day 漏洞

Google 發表的新版 Chrome for Windows 103.0.5060.114，修復了一個高度危險的 0-day 漏洞，已知該漏洞已遭駭侵者大規模濫用於駭侵攻擊。

Google 日前發表的新版 Chrome for Windows 103.0.5060.114，修復了一個高度危險的 0-day 漏洞，已知該漏洞已遭駭侵者大規模濫用於駭侵攻擊。這是 Google Chrome 今年修復的第 4 個 0-day 漏洞。

這個得到修復的漏洞，編號為 CVE-2022-2294，是一個存於 WebRTC (Web Real-Time Communications）組件內的 heap 緩衝區溢位錯誤，由資安廠商 Avast Threat Intelligence 團隊旗下的資安專家 Jan Vojtesek 於日前發現並提報給 Google。

資安專家指出，該漏洞可用於造成程式崩潰，甚至可遠端執行任意程式碼；該漏洞的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分）；危險程度評級則為「嚴重」（Critical）等級。

Google 目前已經釋出的新版 Chrome for Windows 103.0.5060.114，已經修復此一漏洞，Google 表示目前已知有駭侵者利用該漏洞發動大規模攻擊，而在大多數用戶都更新到最新版本前，攻擊可能還會持續發生。

建議 Google Chrome 用戶應立即透過 Chrome 內部的自我更新或手動更新機制，儘速將 Chrome 版本更新到最新版本，以避免未修補的漏洞遭到駭侵者用於攻擊。

- CVE 編號：CVE-2022-2294
- 影響產品/版本：Chrome for Windows 103.0.5060.114 之前版本。
- 解決方案：升級至 Chrome for Windows 103.0.5060.114 與之後版本。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google patches new Chrome zero-day flaw exploited in attacks

3.7.4、Google Chrome 0-day 漏洞遭用於攻擊中東新聞記者

資安廠商發現一家惡意軟體公司 Candiru，利用 Google Chrome 一個 0-day 漏洞製作惡意軟體「DevilsTongue」。

資安廠商 Avast 日前發表資安通報，指出該公司旗下的資安專家，日前發現一家惡意軟體公司 Candiru，利用 Google Chrome 一個 0-day 漏洞製作惡意軟體「DevilsTongue」，專門用以駭侵中東國家多名媒體記者與重要人士。

被 Candiru 公司用來製作 DevilsTongue 惡意軟體的 Google Chrome 0-day 漏洞，其 CVE 編號為 CVE-2022-2294，屬於 WebRTC 的 heap-base 暫存器溢位漏洞；駭侵者可誘使受害者前往特製的網站，誘發溢位錯誤後即可遠端執行任意程式碼。

該漏洞的 CVSS 漏洞危險程度分數為 8.8 分（滿分為 10 分），危險程度評級則為「高」（high）。

Avast 在報告中指出，雖然 Google 已於今（2022）年 7 月 4 日發布新版 Google Chrome 並修復本漏洞，但 Avast 發現有許多該公司的中東客戶遭到由 Candiru 開發的 DevilsTongue 透過此漏洞發動攻擊，進一步分析後發現攻擊對象有多數都位於黎巴嫩，其中有許多是新聞記者。

Avast 說，除了黎巴嫩外，Candiru 的攻擊對象還分布在土耳其、葉門、巴勒斯坦等地，攻擊對象十分集中，屬於一種水坑式釣魚攻擊。

報告說，駭侵者誘使列為攻擊目標的新聞從業人員進入其特製的惡意網站，導致其感染惡意軟體；接著開始竊取被害者的多種機敏資訊，包括語

言、時區、螢幕資訊、裝置類型、瀏覽器外掛程式、推薦來源、裝置記憶體、cookie 功能等等。目前還不清楚駭侵者具體竊走哪些資料，但針對新聞記者的資安攻擊，目的多半是為了收集情報。

建議可能接觸機密情資的個人與單位，均應加強對各式釣魚攻擊的防範能力與意識，包括不任意點按不明連結，不任意開啟不明郵件夾檔，仔細檢視寄件人資訊等等，且應隨時升級至最新版本軟體與韌體，避免駭侵者利用未修補漏洞發動攻擊。

- CVE 編號：CVE-2022-2294
- 影響產品/版本：Google Chrome 版本 103.0.5060.114 之前版本。
- 解決方案：升級至 Google Chrome 版本 103.0.5060.114 與後續版本。

- 資料來源：
  1. The Return of Candiru: Zero-days in the Middle East
  2. Chrome zero-day used to infect journalists with Candiru spyware

第 4 章、 資安研討會及活動

111 年下半年資安職能訓練	
活動時間	詳細日期、課程及地點請點此參閱活動網站。
活動地點	請參閱活動網站。
活動網站	https://ctts.nccst.nat.gov.tw/NewsDetail/155
活動概要	111年下半年 資安職能訓練 **主辦單位：行政院資通安全處** 一、目的：為協助資通安全責任等級 A、B、C 級公務機關符合「資通安全管理法-資通安全責任等級分級辦法」有關資通安全職能評量證書之要求，爰辦理資安職能訓練，以提升資通安全管理法納管機關資安專職(責)人員之資安專業知識與技能。 二、參加對象：資通安全管理法納管對象之資安專職(責)人員。 三、科目規範：為強化資安專職(責)人員職能訓練學習成效，依「資安職能訓練發展藍圖」學習路徑(基礎→專業)，自本(111)年 7 月 1 日起資安職能訓練增加科目先備條件如下： (一)未持有「資通安全概論」評量有效證書者，僅可報名「基礎」科目(即「資通安全概論」)。 (二)持有「資通安全概論」評量有效證書者，可報名「專業」科目，續依課程發展藍圖分策略面、管理面、技術面報名，並取得資安職能評量證書。

四、班別

7 月 14 日 10:00 開放報名。 (本訓練不需會員資格)

補助班：限資安職能補助名單者報名。費用由行政院補助 50%，餘由派訓機關支付。

全額班：受訓費用由派訓機關全額支付。

五、聯絡人

中國文化大學：張先生，(02)2700-5858 轉 8203

臺北醫學大學：梁小姐，(02)6638-2736 轉 1304

健行科技大學：陳小姐，(03)458-1196 轉 3765

國立中興大學：朱小姐，(04)2285-5506

逢甲大學：朱小姐，(04)2451-7250 轉 2407

朝陽科技大學：張小姐，(04)2465-3000 轉 511

崑山科技大學：鄭先生，(06)272-7175 轉 321

六、其他

各班次各機關限派 2 名，每班總額 30 人，報名額滿其餘列為備取。報名者經審核後符合訓練資格者，由訓練機構通知繳費，未收到繳費通知皆列為備取名單。

收到繳費通知，請於訓練啟始 5 日前完成付款，逾期或未完成繳費，視同放棄，將由訓練機構依備取順序遞補。

8/16 資安線上實作 - IoT 資安檢測實務	
活動時間	2022/8/16 (二) 09:10~16:20 (總課程時數 6 小時)
活動地點	台南沙崙資安服務基地 C115 攻防教室 (台南市歸仁區歸仁十三路 6 號 1 樓)
活動網站	https://www.acw.org.tw/News/Detail.aspx?id=3240
活動概要	 **主辦單位：經濟部工業局** 認識 OWASP IoT Project ! 實機 IoT 設備檢測演練 ! 此課程將會從 OWASP IoT 相關專案為主軸，內容將著重於檢測相關技術，協助學員可以透過檢測的工具對物聯網設備進行測試，來了解設備是否有可能存在的資安相關風險議題。 授課講師：微智安聯 許清雄 資深技術經理 學習對象：資安人員、系統管理人員、資安檢測人員 課程大綱： OWASP IoT Project 介紹 IoT 資安檢測工具操作 IoT 設備檢測實作 聯絡人：06-3032260 分機 537 鄭小姐 / katrina@itri.org.tw

物聯網資安研討會暨場域參訪	
活動時間	111 年 8 月 18 日 (星期四) 13:30-16:00
活動地點	資安暨智慧科技研發大樓 A122 會議室 (台南市歸仁區歸仁十三路 6 號 1 樓)
活動網站	https://www.acw.org.tw/News/Detail.aspx?id=3243
活動概要	 **主辦單位：經濟部工業局** 隨著 5G、IoT 新興資訊科技的迅速發展，駭客不斷研發新型態惡意程式，也持續尋找可能的突破點，進而造成企業面臨新型態的資安攻擊往往都無法有效的偵測及防禦，因而導致許多資安問題的產生，嚴重造成企業營運中斷及財務上的損失。 本次研討會邀請國內專家從資安標準、物聯網資安趨勢及產品資通安全等多個層面進行分享，並結合場域資安應用展示，觀摩資安廠商、系統整合商實際導入驗測之資安產品/服務，裨益與會人士掌握標準安全法規與產品安全軟硬體防禦機制，作為未來進行資安風險控管及因應對策擬定之參考。 活動議程：請點此。 活動聯絡窗口：鄭小姐 (06)3032260#537/ katrina@itri.org.tw

HITCON PEACE 2022 台灣駭客年會	
活動時間	2022 年 08 月 19 日 (五) - 2022 年 08 月 20 日 (六)
活動地點	南港展覽館 2 館 7 樓 / 台北市南港區經貿二路 2 號
活動網站	https://hitcon.org/2022/
活動概要	 **主辦單位：經濟部工業局、社團法人台灣駭客協會 (HITCON)、CHROOT** 會議時間： 2022 年 08 月 19 日 (五) - 2022 年 08 月 20 日 (六) 詳細議程、購票資訊及報名方式，請點此至活動網站查看。

8/25 資安線上實作 - 太陽光電系統資安風險評估機制之建立與應用	
活動時間	2022/8/25 (四) 09:10~16:20 (總課程時數 6 小時)
活動地點	台南沙崙資安服務基地 C115 攻防教室 (台南市歸仁區歸仁十三路 6 號 1 樓)
活動網站	https://www.acw.org.tw/News/Detail.aspx?id=3241
活動概要	 **主辦單位：經濟部工業局** 能源系統資安防禦實機演練！ 再生能源是國家重大能源政策，其中太陽能發電發電量快速提升，隨著太陽光電案場智慧化與連網化的發展趨勢，讓太陽能光電系統也成為駭客攻擊的標的之一。本課程將介紹太陽能光電場域的資安風險評估機制，並對攻擊手法進行介紹及實際演練。 授課講師：工研院資通所 陳宣同工程師 / 台電綜合研究所 陳鳳惠主任 學習對象：資安人員、系統管理人員、資安檢測人員 課程大綱： 第一單元 介紹阻斷服務攻擊 (DOS) 將阻斷服務攻擊進行分類 (DOS、DDOS、DRDOS) 介紹常見阻斷服務的攻擊手法

	第二單元 介紹分散式阻斷服務攻擊 (DDoS) 與常見攻擊手法 介紹分散反射式阻斷服務攻擊 (DDoS) 與常見攻擊手法 介紹常見的阻斷服務攻擊的防護策略 第三單元 能源系統資安攻擊案例 ICS 資安風險評估方法論 PV 案場資安風險評估 太陽光電變流器資安檢測程序 活動聯絡人：06-3032260 分機 537 鄭小姐 / katrina@itri.org.tw

自拜登數位資產政策，一探臺灣數位金融之機會與挑戰	
活動時間	2022 年 8 月 29 日 , 14:00-16:00
活動地點	IEAT 國際會議中心 8 樓綜合教室/Webex 會議室
活動網站	https://www.twsig.tw/20220829/
活動概要	 **主辦單位：TWNIC、TWIGF、NII** 美國總統拜登今年 3 月簽署的數位資產（Digital Assets）行政命令中定義了 6 項關鍵優先事項：消費者、投資者及企業權益保障；保護美國及全球財務系統穩定；打擊非法金融；提升美國在全球金融及經濟競爭領導地位；普惠金融，以及負責任創新等，並具體要求近 20 個聯邦機構在期限內提交評估報告並研擬相關草案，對打造美國數位資產、建構央行數位貨幣（CDBC）及相關金融系統、經濟影響與社會衝擊等議題進行多面向研究。 行政命令也進一步闡釋「數位資產」包含了不同形式的央行數位貨幣，以及其他透過分散式帳本技術提供的數位金融資產及具有支付、投資、匯兌或交換資金等功能之數位工具，例如加密貨幣及穩定幣等。由於數位資產對美國及全球具有廣泛且長遠的影響，拜登政府在該行政命令要求由總統國家安全事務助理（APNSA）及總統經濟政策助理（APEP）負責統籌協調相關聯邦機構，在獨立聯邦監管機構（如聯邦準備系統理事會、聯邦貿易委員會等）協助下，全面性地從金融系統影響及監管、立法及犯罪偵查、環境及能源、國家安全、國際合作及美國競爭力等議題提出分析報告並制定行動計畫。 拜登的跨部會數位資產戰略規劃，代表了加密貨幣、央行數位貨

	幣等數位資產不可抵擋之發展趨勢外，也彰顯美國政府對數位資產之重視；臺灣近年也已開始就相關法規展開研究，惟跨部門的數位資產討論相對少。 面對著全球金融系統數位化浪潮，本場活動將邀請國內不同利害關係人，探討臺灣在數位資產發展規劃中所面臨的困境、可能的契機，以及如何透過公私協力運作方式，共同在技術架構設計、金融穩定、支付系統、法規環境、人權保障、普惠金融及國家安全等各方面作出必要調整，建構出符合最大公共利益的數位金融應用環境。 合作單位：LINE 時間：2022 年 8 月 29 日 , 14:00-16:00 地點：IEAT 國際會議中心 8 樓綜合教室/Webex 會議室 ****本活動採實體與線上同步進行**** 議程 14:00–14:05　活動介紹 14:05–15:45　焦點座談 15:45–16:00　現場問答

CYBERSEC 2022 臺灣資安大會	
活動時間	9/20 - 9/22
活動地點	台北南港展覽二館
活動網站	https://cyber.ithome.com.tw/
活動概要	 **主辦單位：iThome** 數位轉型 資安升級 生存在滾動式常態時代，我們正在參與一場永不止息的轉型旅程。 未來，數以萬計的低軌衛星於地球上空環繞，串聯起全球高速資訊網絡；各式無人載具在地球的各個空間自主運行，交織成高效運輸網路；人們，在虛擬世界與現實世界穿梭自如。在數位轉型的推波助瀾下，實體世界與網路空間逐漸融為一體，萬物的運作再也脫離不了晶片、程式碼與網路，而眼下的資安議題，不再只是單純的資訊安全，而是觸及人身安全、國家安全與全球安全的迫切課題。 全球數位轉型已是進行式，全新的資安威脅來勢洶洶、迫在眉梢。現在，就是做出改變，全面升級資安作為的時候。舉凡提升資安治理、普及資安意識、精進資安防禦、強化資安韌性，或是資安產業升級、資安人才活化、供應鏈安全的鞏固，都關乎國家、企業與產業數位轉型的未來。CYBERSEC 2022 臺灣資安大會，誠摯邀請大家一起集思廣益，共同擘畫更安全、更安心的數位未來。 詳細活動資訊及報名方式。請點此至活動網站查看。

關鍵基礎設施實作課程(含攻防演練實作)	
活動時間	見活動概要
活動地點	沙崙資安服務基地 1 樓攻防演訓教室 (台南市歸仁區歸仁十三路 6 號)
活動網站	https://www.acw.org.tw/News/Detail.aspx?id=3229
活動概要	 **主辦單位：經濟部工業局** 近年來，工控(ICS)及 OT 相關的網路攻擊事件頻傳，駭客亦開始針對關鍵基礎設施單位，包括政府、醫療保健、油氣水電、交通、金融等發起持續攻擊，被攻擊的結果除造成營運中斷或金錢、聲譽損失外，更有可能影響國家安全與人民生命安全。 為提升關鍵基礎設施操作人員熟悉資安防護基準與防護措施，經濟部工業局委託資策會辦理關鍵基礎設施實務操作演訓課程，結合沙崙資安基地工控實測場域，進行實際演練與操作攻防演練實作，學習工控封包分析並撰寫偵測規則驗證攻擊情境，實訓演練真實的防禦架構，培養業者實務防護能力。 ➢ 2022/09/27 09:40~16:40 [第四場]關鍵基礎設施實作課程 課程聯絡人：李小姐 / doralee@iii.org.tw / 02- 66073299

第 5 章、 TVN 漏洞公告

鼎新電腦 BPM - SQL Injection	
TVN / CVE ID	TVN-202206001 / CVE-2022-32456
CVSS	9.8 (Critical)
影響產品	鼎新電腦 BPM <= v5.8.6.1
問題描述	鼎新電腦 BPM 之部分功能參數未對使用者輸入進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	Update version to 5.8.8.1
公開日期	2022-07-11
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6286-3030a-3.html

繹宇數位科技 MailHunter Ultimate 電子郵件行銷追蹤分析系統 - Deserialization of Untrusted Data	
TVN / CVE ID	TVN-202207007 / CVE-2022-35223
CVSS	9.8 (Critical)
影響產品	繹宇數位科技 EasyUse MailHunter Ultimate 電子郵件行銷追蹤分析系統 <= 2020
問題描述	繹宇數位科技 MailHunter Ultimate 之反序列化功能未恰當進行檢查，遠端攻擊者不須權限，可以將序列化格式的惡意 Payload 填入 Cookie 中，進行反序列化時觸發 Insecure Deserialization 漏洞，導致執行任意程式碼、任意系統操作或中斷服務。
解決方法	聯繫繹宇數位科技進行版本更新
公開日期	2022-07-29

相關連結	https://www.twcert.org.tw/newepaper/cp-151-6365-b056c-3.html

沛盛資訊 OMICARD EDM 行銷發送系統 - SQL Injection	
TVN / CVE ID	TVN-202206010 / CVE-2022-32964
CVSS	9.8 (Critical)
影響產品	沛盛資訊 OMICARD EDM v5.8~v6.0
問題描述	OMICARD EDM 之 API 功能參數未對使用者輸入進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	聯繫沛盛資訊進行版本更新
公開日期	2022-08-04
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6372-f61bc-3.html

沛盛資訊 OMICARD EDM 行銷發送系統 - Use of Hard-coded Credentials	
TVN / CVE ID	TVN-202206011 / CVE-2022-32965
CVSS	9.8 (Critical)
影響產品	沛盛資訊 OMICARD EDM v5.8~v6.0
問題描述	OMICARD EDM 使用 Hard-code 的 Machine Key，遠端攻擊者不須權限，可以利用 ViewState 進行反序列化攻擊，執行任意程式碼。
解決方法	聯繫沛盛資訊進行版本更新
公開日期	2022-08-04
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6373-34d51-3.html

健保卡網路服務元件 - Stack-based Buffer Overflow-1	
TVN / CVE ID	TVN-202207001 / CVE-2022-35217
CVSS	7.8 (High)
影響產品	健保卡網路服務註冊網站供下載受影響版本之平台與相對應 MD5 HASH： Windows： Setup.zip MD5 驗證碼：dae0509e5aabde2f110ce8418af67cf7
問題描述	健保卡網路服務元件未作封包 Header 的長度驗證，導致 Stack-based buffer overflow 漏洞，使區域網路內的攻擊者，以一般使用者權限利用此漏洞，並執行任意程式碼、任意系統操作或中斷服務。
解決方法	至健保卡網路服務註冊網之下載點下載最新版本
公開日期	2022-07-29
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6353-31470-3.html**

第 6 章、 2022 年 7 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。

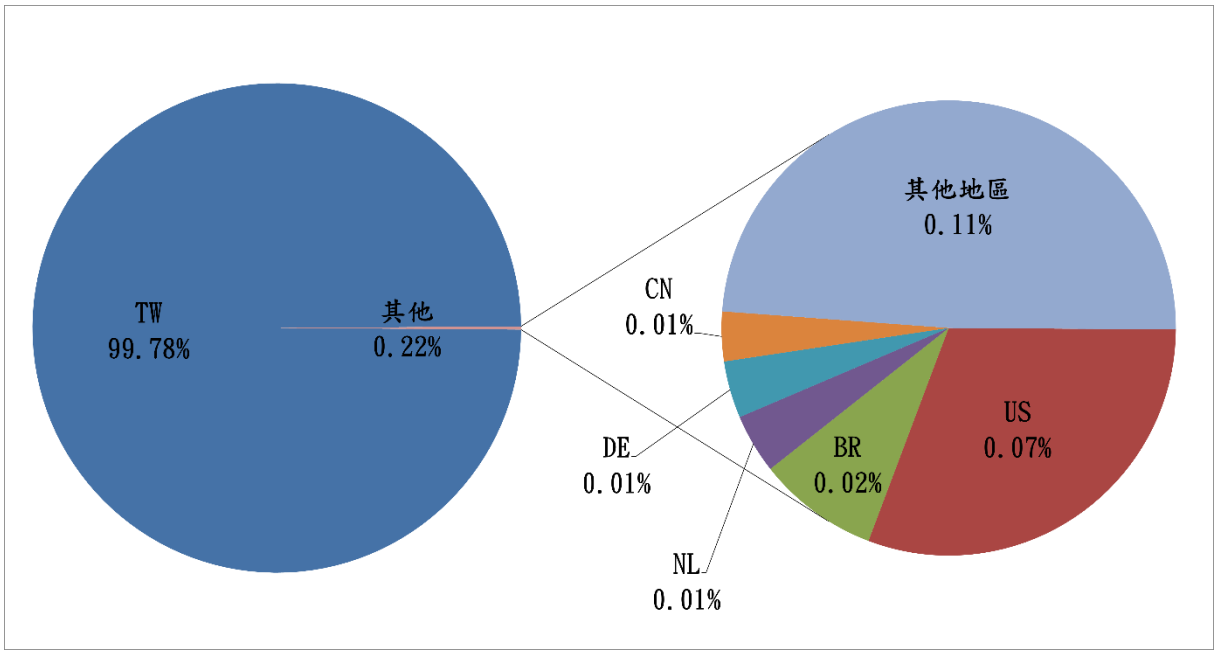

圖 1、分享地區統計圖

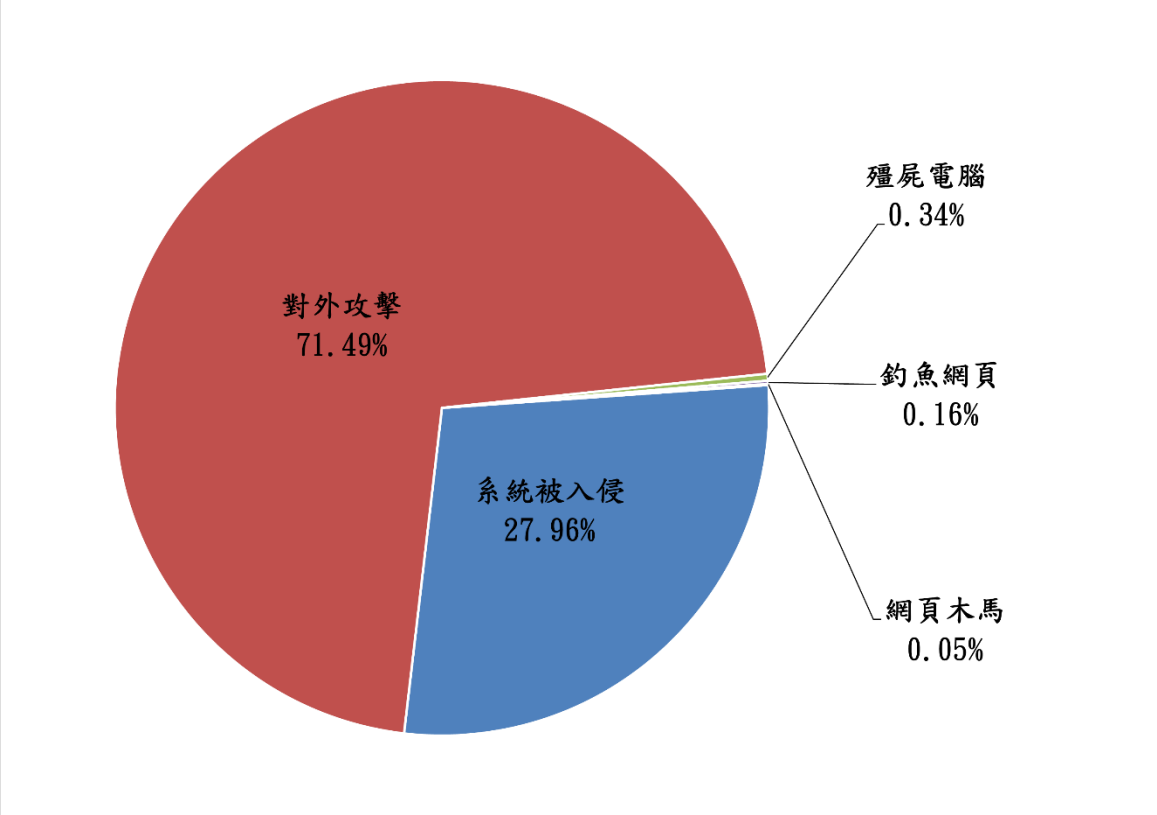

圖 2、分享類型統計圖

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 8 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**