TWCERT/CC 資安情資電子報

2022 年 12 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，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 7 章節：

第 1 章、封面故事：主題式資訊安全專題分享。

第 2 章、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養

第 3 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 4 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 5 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 6 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 7 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

網路攝影機資安威脅與防護

- 網路攝影機日漸普及且已應用到監督管理層面，深刻影響人們的生活，也因而引發了網路攝影機的資安議題。本文分析網路攝影機主要的資安問題，並探討我國影像監控系統資安標準訂定現況，提出對應之防護建議。

一、簡介

根據美國市場研究與諮詢公司 Grand View Research 於 2020 年 5 月所發布的市場分析研究報告，全球智慧家庭監控攝影機市場規模在 2019 年為 37.1 億美元，並預計從 2020 年到 2027 年，將持續維持 15.7%的複合年均成長率(CAGR)，預測在 2027 年可達到 119 億美元的市場值；而亞太地區由於基礎設施的擴展，預計其攝影機市場將以 16.3%的複合年均成長率增長，其增長率為所有地區之最。

透過網路攝影機，人們可以遠端進行有效的監督與管理，這些通常以 IP 攝影機形式出售的網路攝影機因可以協助人們監視財產、居家環境和寵物生活等而廣受歡迎。除了一般的智慧家庭應用之外，網路攝影機的相關運用更

深入政府機構及企業組織，成為監控工作環境及進行運營管理不可或缺的工具，深刻地影響了人們的生活型態。

然而也因為網路攝影機所監看的畫面曝露在網路環境中，不僅使用者的個人隱私存在遭受侵犯的危險，而網路攝影機管理介面所記錄的機敏資料，如網路分享器登入密碼、電子郵件、用以儲存影像資料的 FTP 伺服器或 NAS 登入密碼等，都可能外洩，這些外洩的機敏資料可能為後續的駭客攻擊打開了大門。

基於安全監控的需求，網路攝影機通常透過網際網路提供 24/7 全天候的監視服務。加上由於影像處理所需，網路攝影機亦具有相較高於其它 IoT 設備的計算能力和良好的網路流量輸出，因此成為駭客攻擊的首要目標。例如著名惡意軟體 Mirai 所構建的殭屍網路，其殭屍大軍主要由數十萬台網路攝影機、家用路由器及網路儲存裝置 NAS (Network Attached Storage) 組成，能同時發動數百 Gbps 的 DDoS (分散式阻斷服務，Distributed Denial-of-Service attack) 攻擊流量，癱瘓受攻擊目標。

二、網路攝影機資安問題

在台灣，隨著環境安全意識及安全需求持續的增加，各式網路攝影機的應用已融入人們的生活當中，然而攝影機的資安問題則有待進一步解決。從著名的網站 insecam 可以發現，台灣有超過 950 支網路攝影機影像遭公布在網站上，攝影的地點包括辦公室內部、工廠作業區、民宅客廳、餐廳、會議室、診所、營業場所等地，有心人士透過網頁瀏覽器即可觀看各式的即時影像。這些隱私問題發生的原因，通常在於使用者沿用了網路攝影機的預設密碼或使用簡單容易猜測的密碼，因此駭客透過掃描網路攝影機的廠牌及型號後，就可以輕易地透過對應的帳號及密碼列表，或進行簡單的密碼猜測，即可成功入侵。

根據 insecam 所公布的資料，美國有超過 4,000 支攝影機畫面遭外洩，韓國以 2,300 支居次，日本及意大利分別為 1,800 支及 990 支，台灣以 969 支位居第 5，緊接其後的是德國、法國、俄羅斯、英國及荷蘭。這些遭入侵的網路攝影機廠牌包括 Axis、Canon、D-Link、Foscam、Hi3516、Panasonic、Sony、Toshiba、Tplink 等。

Insecam 指出，保護網路攝影機畫面隱私的唯一解決方案是設置密碼。然而，大多數網路攝影機預設了眾所週知的使用者帳號及密碼，若使用者未做變更，或變更後的密碼複雜度及長度太弱，駭客即可利用廠牌的預設密碼或暴力破解帳號及密碼，而輕易入侵。例如惡意軟體 Mirai 就是利用設備預設帳號及密碼的弱點，用了 62 個使用者帳號及密碼的組合對物聯網設備進行簡單的暴力攻擊，從而建立了殭屍網路大軍。

網路攝影機的不良設計，加上使用者的資安意識不足，除了讓設備淪為 DDoS 攻擊的幫凶外，也引發了個人隱私遭侵犯的潛在風險。從資安角度而言，任何連接到網際網路的設備都可能遭到駭客入侵。當陌生人可以透過網路攝影機監看居家環境的一舉一動、偷聽對話、跟監受害者的活動時，這對個人隱私是一個嚴重的侵犯。而即使是強化網路攝影機的密碼機制，使用者的錯誤設定亦可能是遭受攻擊因素之一，例如為了方便而設定空白密碼，或是對資安相關設定任意調整，皆可能導致資安功能失效。

隨著雲端網路攝影機的普及，使用者可以將影像傳送到雲端的影像資料庫儲存，實現雲端循環錄影，並讓使用者在稍後隨時回放。因此即使駭客無法直接連接到使用者的網路攝影機，駭客也可以對雲服務發動攻擊竊取影像資料，例如 2021 年 3 月美國新創公司 Verkada 雲端安全監視系統遭駭客入侵一案，導致了 15 萬則安全監控影像外洩，受害者包括特斯拉及軟體技術服務商 Cloudflare 等。而 Verkada 的系統遭入侵一事之所以引起軒然大波，受害者除了國際大廠外，尚包括醫院、警察局、監獄和學校等相關機構。

除了常見的密碼猜測攻擊外，利用網路攝影機本身的資安漏洞也是常見的駭客入侵手法。例如 2019 年研究人員發現的 D-Link 網路攝影機漏洞，不僅可以讓攻擊者透過中間人攻擊，截取雲端伺服器與攝影機之間的串流影像，還可以讓攻擊者將攝影機的合法韌體替換成藏有後門版本的韌體。此外相關的資安漏洞尚包括研究人員在 Foscam 網路攝影機中發現的資安漏洞，這些漏洞可使有人心士在僅知道網路攝影機的 IP 地址的情況下，即可透過緩衝區溢位 (buffer overflow) 獲得 root 權限等。

三、網路攝影機資安防護

綜整前述所提到的資安議題，包括隱私議題、預設密碼、脆弱密碼、錯誤設定、雲端資安、設備弱點等，對於網路攝影機的使用者而言，謹提出以下 9 點資安防護建議：

1. 立即修改網路攝影機的預設帳號及密碼，並將密碼的強度提高，且避免與其它設備共用相同的密碼；
2. 不要在沒有任何資安防護措施(如防火牆等)保護的情況下，將網路攝影機直接曝露在網際網路上；
3. 不要將網路攝影機放置在主要網路上，以免駭客藉由入侵網路攝影機而進入主要網路，造成其它系統受害；
4. 網路攝影機的作業系統及韌體也可能存在資安漏洞，因此關注廠商所公布的漏洞修補程式並及時更新，可杜絕相關的資安漏洞；
5. 使用 SSL 或等效的安全通訊協定對網路連線進行加密，以防範中間人攻擊並避免機敏資料在傳送過程中遭竊；
6. 使用支援影像加密的網路攝影機，以避免有心人士藉由對網路攝影機的臨時

物理接觸，而獲取儲存在記憶卡中的影像內容；

7. 使用支援雙因子認證 (Two-factor authentication，2FA)的網路攝影機，可以大幅降低網路攝影機遭駭客入侵的機率；

8. 注意網路攝影機安置地點，避免鏡頭對著需要高度隱私的區域，對於可經由遠端控制鏡頭旋轉角度的網路攝影機更是要特別留意；

9. 廉價的網路攝影機通常不會考量太多的資安要求與細節，因此價格不應是採購的主要考量。

資安議題亦可透過網路攝影機在開發階段加以強化，使消費者在取得網路攝影機時即具備較高的資安水準。因此，針對網路攝影機的資安標準，台灣資通產業標準協會(TAICS)制定了一系列相關的影像監控系統資安標準，包括：

- TAICS TS 0014-1 v1.0-影像監控系統資安標準-第一部：一般要求
- TAICS TS 0014-2 v2.0-影像監控系統資安標準-第二部：網路攝影機

上述資安標準主要從「實體安全要求」、「系統安全要求」、「通訊安全要求」、「身分鑑別與授權機制安全要求」及「隱私保護要求」等五個安全構面來確保網路攝影機的資訊安全，並於 2019 年 11 月 29 發布成為國家標準 (CNS 16120)。

為確保測試實驗室可透過一致的方式來檢測網路攝影機是否符合上述資安標準，TAICS 發布了下列兩份測試規範，具體明列網路攝影機對應上述資安標準所應通過的測試項目、測試條件、測試方法及測試標準等事項，包括：

- TAICS TS-0015-1 v1.0-影像監控系統資安標準測試規範-第一部：一般要求
- TAICS TS-0015-2 v2.0-影像監控系統資安標準測試規範-第二部：網路攝影機

上述網路攝影機資安認驗證規範運行 3 年之後，截至 2020 年 11 月為止，已有 11 家廠商 36 款網路攝影機取得合格標章，TAICS 根據這期間收集到的產品使用經驗及實驗室測試情境，於 2021 年 2 月發布了「TAICS TS-0014-1 v2.0 影像監控系統資安標準-第一部：一般要求 v2」，並同步更新了相關的測試規範，進一步優化標準需求及測試方法，包括：

1. 調整相關安全需求，例如：

- 新增「5.2.2.2 產品所收集之遙測資料應告知使用者，且未告知之遙測資料不應被收集」；
- 刪除 v1.0 版本的「5.5.1.2 使用者對其儲存的隱私資料擁有刪除之權限和功能」等；
- 調整 v1.0 版本的「5.4.1.5 產品之鑑別機制應採用多因子鑑別」，增加公開金鑰 PKI 鑑別機制，將其修正為 v2.0 版本的「5.4.1.5 產品之鑑別機制應採用 PKI 或多因子鑑別等強鑑別機制」等；

2. 納入更多的測試情境及案例，優化測試方法並增進測試一致性。

鑑於消費性網路攝影機在資安防禦基礎上應更貼近使用者的需求，因此在工業局與網路攝影機產業的支持下，TAICS 於 2021 年 2 月公布了我國消費性網路攝影機的資安產業標準「TAICS TS-0038 v1.0 消費性網路攝影機資安標準」及測試規範「TAICS TS-0039 v1.0 消費性網路攝影機資安測試規範」，其中具體明列資安檢測之測試項目、測試條件、測試方法與測試結果等事項，從「身分鑑別與權限控管」、「已知漏洞安全」、「軟韌體更新」、「資料機密性與完整性」、「系統完整性」、「資源可用性」、「隱私保護」及「警示與紀錄」等八個安全構面做為消費性網路攝影機製造商、系統整合商及物聯網資安檢測實驗室等，進行相關產品檢測技術之參考藍本。惟據了解，目前消費性網路攝影機資安標準尚需要與財團法人全國認證

基金會(TAF)建立認證服務計畫，故目前還未有認可的測試實驗室可提供相關產品檢測服務，協助廠商取得相關資安標章，但可預期的，未來我國市面上的網路攝影機，其資安水準將可達到一定的強度，讓消費者安心採購。

四、分析與建議

網路攝影機與民眾生活息息相關，一旦發生資安問題將影響深遠，因此在任何情況下都不應忽視網路攝影機資安的重要性。為了避免將來遭受隱私外洩的困擾，使用者務必修改網路攝影機所提供的預設帳號及密碼，並且盡可能使用具有一定長度及複雜度的密碼，避免與其它設備共用密碼，及盡量選用支援雙因子或是多因子身分認證(Multi-factor authentication，MFA)功能的網路攝影機，方能將目前常見的密碼猜測攻擊及密碼暴力破解攻擊所帶來的威脅降至最低。

此外，確保所有網路攝影機的韌體都更新至最新版本，關注廠商所發布的資安訊息，及時安裝所有的漏洞修補程式，是防範駭客經由系統漏洞入侵網路攝影機的常見方法。在購買網路攝影機時，信譽良好的廠商會在產品生命週期中，定期或不定期對產品進行軟體或硬體版本更新及發布漏洞修補程式，可降低網路攝影機長期使用的資安風險，廠商所提供的這些售後服務都是消費者在採購前應多加考量的。重視廠商信譽及售後服務，正視產品孤兒所帶來的資安風險，將可減少層出不窮的網路資安問題。

- 資料來源：
  1. Smart Home Security Cameras Market Size, Share & Trends Analysis Report By Product (Wired, Wireless)
  2. Mirai (惡意軟體)
  3. Default Username And Password In Internet of Things
  4. Hackers breach systems of Cloud based Security Camera company Verkada

5. D-Link camera vulnerability allows attackers to tap into the video stream
6. Foscam Issues Patches For Vulnerabilities in IP Cameras
7. 標準及測試規範(物聯網資安-影像監控系統)
8. 測試規範/需求規範/標準

第 2 章、 資安小知識

Middlebox TCP 反射放大 DDoS 攻擊趨勢與防護

- TCP Middlebox 反射攻擊利用防火牆及內容過濾機制的弱點，使其反射並放大 TCP 流量至受害目標，形成有力的 DDoS 攻擊。
- 這種型態的攻擊手法降低了攻擊者實行 DDoS 的門檻，因為攻擊者只需付出相對低的成本，就能創造出巨大的攻擊流量。
- 部份 Middlebox 的行為甚至會幫助攻擊者對受害目標行進行更深的 SYN, ACK, 或 PSH+ACK 泛洪 (flooding) 攻擊。
- 目前 TCP Middlebox 反射攻擊技術仍持續演進，案例亦開始出現，應持續關注並對相關設備進行設定調整或緩解措施。
- 若企業對 Middlebox TCP 反射放大攻擊有相關檢(複)測疑問，歡迎與 TWCERT/CC 聯繫。

一、簡介

(1)反射放大 DDoS 攻擊與其流程

分散式阻斷服務(Distributed Denial-of-Service, DDoS)攻擊，為駭客發送大量的網路封包或服務請求，使得受害系統或主機因無法負荷頻寬或耗盡資源

而癱瘓，無法提供正常服務。關於 DDoS 攻擊可參考另一篇 分散式阻斷服務攻擊(DDoS)趨勢與防護。

DDoS 攻擊主要可分為頻寬消耗及資源消耗兩種攻擊類型，一般新聞媒體所報導之巨大流量攻擊多屬於頻寬消耗類型，此類型攻擊者會透過傳送大量無效的服務請求給受害主機或伺服器，使得網路頻寬壅塞，導致一般使用者無法順利登入或連線，產生主機或伺服器癱瘓之後果。

攻擊者通常會利用大量的殭屍電腦同時發出攻擊，而要產生如此大流量的攻擊，仍是一個難度很高的挑戰，於是出現了反射放大的攻擊技術，透過中介設備或服務將初始流量放大後送給受害者，其放大倍數從數倍到上百倍不等，也因此近年來屢屢刷新攻擊流量記錄，本文所探討的 Middlebox 反射放大攻擊即為此類的新型攻擊技術。

放大攻擊式的 DDoS 是由攻擊者發送少量的資料，經由其他設備將資料數量放大後送給受害目標，攻擊者會將初始的攻擊封包（通常是某種服務的請求封包）中的來源 IP 位址偽造成受害目標的 IP 位址，而後將該請求封包送給用於放大流量的服務或伺服器，使該服務再依據偽造的 IP 回應大量的資料給受害目標，如下圖所示。

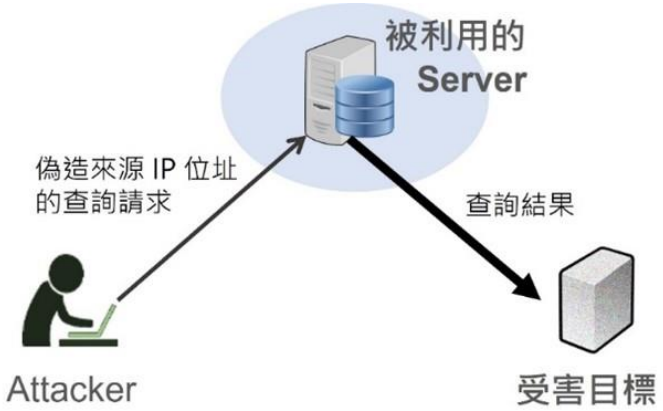


圖 1、傳統的反射放大攻擊

通常反射放大攻擊只能利用 UDP 協定，不能利用 TCP 協定來進行，這是因為 TCP 通訊依賴三向交握以建立連線，但攻擊者需將來源 IP 改為受害者的 IP，中介的服務/伺服器會在收到 TCP 建立連線請求(SYN 封包)後，將後續

三向交握的回應(SYN-ACK 封包)傳送給受害者，而受害者也無法完成後續步驟，導致攻擊者無法再繼續發送請求封包。

因此，目前對反射放大 DDoS 攻擊的防護機制除了較為一般性的防護規則外，其它特定的規則多是針對 UDP 來設計的。

(2)Middlebox 反射放大 DDoS 攻擊

近期因 Middlebox 設備漏洞研究而興起的 DDoS 攻擊技術，由於國內企業採用了相當多的相關設備，故於本節介紹該攻擊技術概念。

A、Middlebox 介紹

網路通訊的設計原則之一是，由通訊雙方的終端設備來解析並處理封包，傳輸過程中所經過的網路設備僅負責將封包送往正確的目的地，不查看或修改封包內容。

然而因應 Internet 的快速發展，為了解決網路擴展的瓶頸、提升傳輸效能、增加通訊安全等目標，網通業者在網路設備上引進流量操控的功能，用於檢查、過濾、更改封包，已不僅是轉發的功能，這種類型的網路設備稱為 Middlebox。

常見的 Middlebox 設備有網路位址轉譯器 (Network Address Translation，NAT) 、內容過濾系統 (Content Filtering System)、入侵偵測/防護系統 (Intrusion Detection/Prevention System，IDS/IPS)、代理及反向代理 (Proxy/Reverse Proxy) 等

B、執行 DPI 的 Middlebox 特性

部份類型的 Middlebox 對於封包的檢查與操作，為了執行深度封包檢測 (Deep Packet Inspection, DPI)，除了作用於封包的各層標頭之外，還深入到載荷 (payload)層次，這類 Middlebox 通常是入侵檢測/防護以及內容過濾的資安系統，角色是流入內部網路封包的內容把關者。

依據流入封包內容的不同，Middlebox 會採取不同的行為，從簡單的放行/丟棄，到內容竄改、趨勢統計分析、AI 資訊預測、對外部通訊者發送回應資訊等等。這種 Middlebox 通常只會檢視或操作單一方向的流量（由外向內），也就是非對稱路由 (Asymmetric Routing)，而忽視 TCP 的有效性。

舉例而言，一個未與內部伺服器完成 TCP 三向交握的外部終端對該伺服器發送了一個 HTTP GET 請求，若位於 Middlebox 之前的防火牆因故未能阻擋該封包流入，那麼因 Middlebox 內沒有連線的 state table，無法得知這是一個 TCP 狀態異常的封包，就不會警覺到異常，持續對該封包進行處理。

雖然以上所舉的例子，在實務上因為防火牆不會讓未建立連線的 TCP 封包流入，所以幾乎不可能發生，但 Middlebox 這種單向檢查的特性，讓人有了想像的空間，因而產生了 TCP Middlebox 反射放大攻擊的技術。

Middlebox 反射攻擊的設計思維來自於設備不會確認 TCP 三向交握的正確性，因此 Middlebox 反射攻擊是一種 TCP 的反射式攻擊，這與前述章節所說明利用 UDP 的反射放大 DDoS 攻擊有所差別

- TCP 的 Middlebox 反射攻擊基於下列三項要素：
  1. 攻擊者將服務請求夾帶於 TCP 三向交握封包內（特別是 TCP SYN）；
  2. Middlebox 無視 TCP 三向交握封包不應夾帶服務請求，仍然正常的進行後續處理流程；
  3. 後續處理流程中，Middlebox 在回應請求時，處理了被夾帶的服務請求內容，導致回應內容大增，形成放大攻擊。

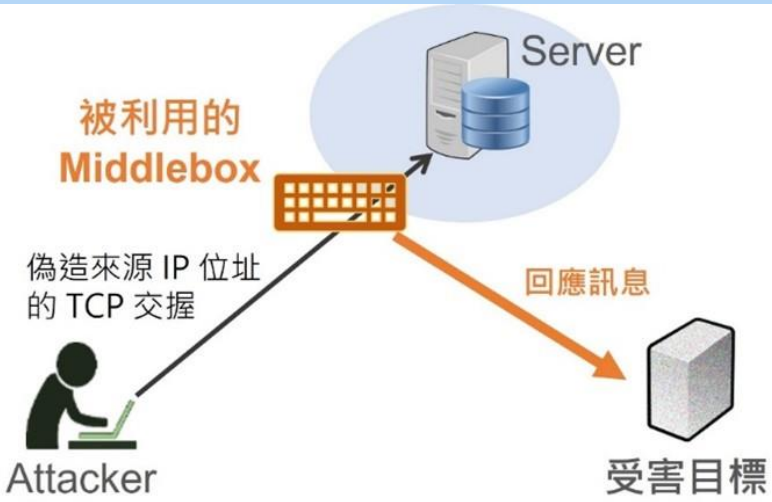


圖 2、利用 Middlebox 的 TCP 反射放大攻擊

- 於前述章節中提到，傳統的反射放大攻擊之所以無法藉由 TCP 來進行，是因為攻擊者送出的服務請求必須仰賴正常的 TCP 連線，而在偽造來源 IP 位址的前提下，TCP 連線是絕對無法被成功建立的，但在 Middlebox 的利用上，是在 TCP 三向交握內夾帶服務請求，放入了可被放大的資料。
- 攻擊者要解決的另一個難題是：即使將服務請求作為載荷夾帶於 TCP 三向交握的封包內，伺服器仍然不會有任何回應。因作為採用 TCP 通訊的兩個終端，資料傳輸是在交握成功、連線建立之後才會進行的，這是 TCP 通訊的基本精神之一。
- 因此攻擊者利用擁有 DPI 能力的 Middlebox。TCP 協定雖未禁止 TCP 三向交握封包夾帶載荷，但實務上這種情況少之又少，所以 Middlebox 並未確認有夾帶載荷的 TCP 封包是否已成功建立連線，導致 TCP 三向交握封包夾帶載荷並不正常，但 Middlebox 仍持續處理了攻擊者的服務請求，收下攻擊封包並剖析處理，滿足了第二個要素。
- 最後，對於送出的、已偽造了來源 IP 位址的服務請求（夾帶於 TCP 三向交握封包中），攻擊者需要引起剖析者 (Middlebox) 的「激烈回應」，來達成 Middlebox 回應大量訊息的目標。只要夾帶對 Middlebox 而言會引起檢測反應的敏感關鍵字，Middlebox 就會回應相對大量的資料給受害目標；這些資料通常會是禁制、警告、或是法律資訊，以完整網頁的方式呈現。這樣就完成了第三個要素。

二、TCP Middlebox 反射攻擊案例

[國內案例]

下圖顯示攻擊者發出一個 TCP SYN 封包，其中來源 IP 位址偽造成受害目標的 IP 位址 X.X.X.X，目的 IP 位址 Z.Z.Z.Z 為某 Middlebox 保護的伺服器所分配到的對外 IP 位址。這個 TCP SYN 封包夾帶了載荷，內容是一個 HTTP GET 請求，存取不存在的 URL。

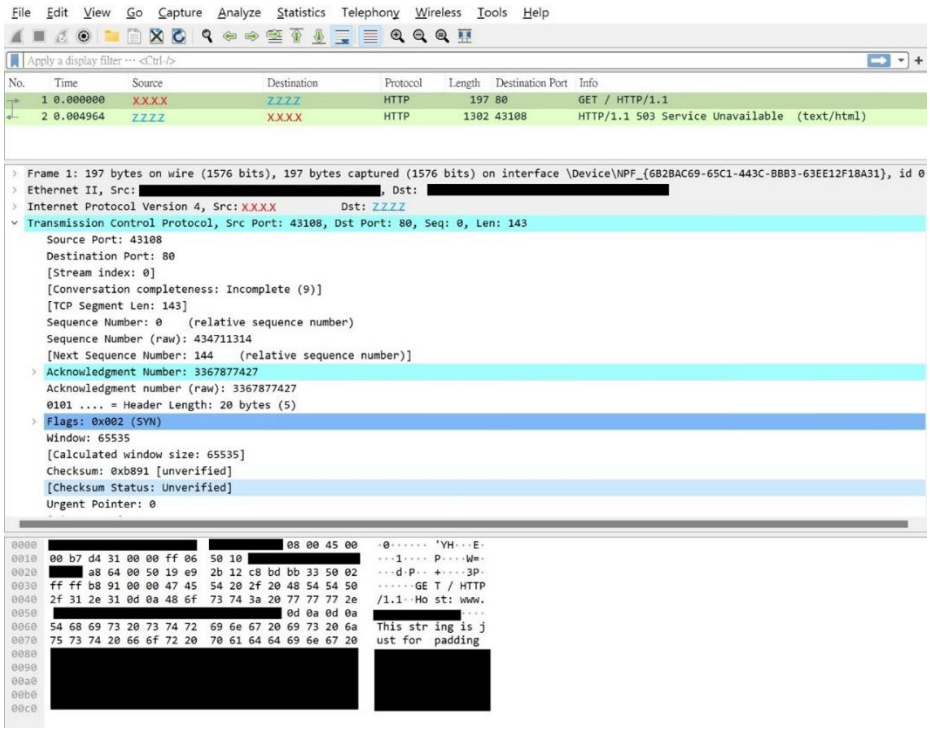


圖 3、攻擊者發送一個帶有 HTTP GET 請求的 TCP SYN 封包

Middlebox 收到這個 TCP SYN 封包之後，回應了一個 HTTP 狀態碼 503（服務無法使用）的封包，其中夾帶一個網頁附帶許多錯誤資訊；整個封包大小為 1302 bytes。此時並沒有正常的 TCP 連線被建立，但 Middlebox 仍然回了一個 PSH, ACK 封包給受害目標。

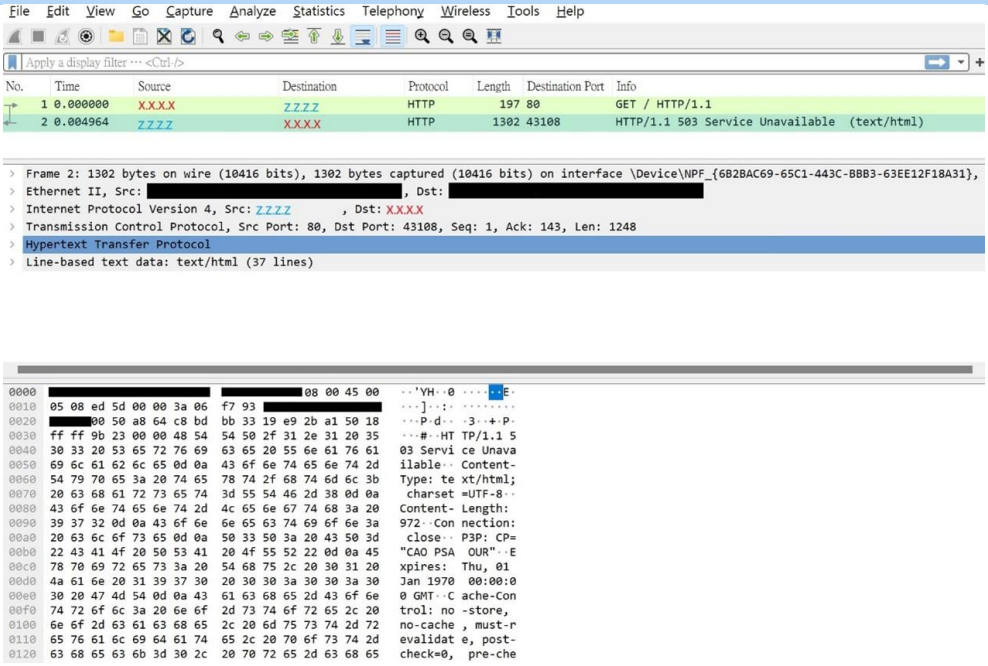


圖 4、Middlebox 將回應反射給受害目標

在這個案例，攻擊者送出 143 bytes 的資料，而 Middlebox 回應了 1248 bytes 的資料給受害目標；單就 payload 而言，放大了 8.7 倍。事實上，攻擊的放大倍率仍可再提高，如在攻擊者送出的 TCP SYN 封包夾帶較多數量的資料；例如將夾帶的資料量改為 100 bytes，那麼此例的放大倍率即超過 12 倍。

[國外 Akamai 案例]

國外 Akamai 的研究報告“TCP Middlebox Reflection: Coming to a DDoS Near You”[1]，描述了 TCP Middlebox 放大攻擊的實例。

上節所提到的案例中，Middlebox 未特別偵測流經的封包是 TCP 三向交握封包，而將其視為一般的封包以對夾帶的資料進行處理並回應。

除了這種行為外，某些 Middlebox 的奇特行為讓攻擊者能更有效率的進行攻擊，以奇特形容是因目前尚未能瞭解 Middlebox 進行如此不盡合理的處理緣由。此行為是，這些 Middlebox 在收到帶有載荷的 TCP SYN 封包後，會以另一個或多個帶有載荷的 TCP SYN 封包作為回應發送給受害目標。這造成了一個無窮循環的 TCP 反射放大攻擊，這不代表會是一個無窮大的流量，但可以更快速的提升放大倍率。

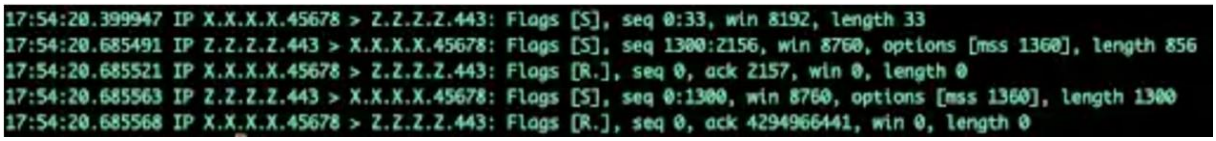


圖 5、Middlebox 以 TCP SYN 作為回應並忽略送來的 RST 封包

在上圖中，攻擊者偽造了來源 IP 位址 (X.X.X.X) 後，將帶有載荷、長度為 33 bytes 的 TCP SYN 封包送往 Middlebox (IP 位址 Z.Z.Z.Z)。特別之處在於第二步：Middlebox 對受害目標發送了一個新的 TCP SYN 封包，長度為 856。受害目標收到這個帶有資料的 SYN 封包之後，回應了 RST 封包。然而 Middlebox 再送了另一個 SYN 封包，長度為 1300；受害目標亦再回應一個 RST 封包。

這個例子可以看出此 Middlebox 的兩個特殊行為：(1) 它對受害目標發送了多個帶有資料的 SYN 封包；(2) 它無視受害目標送來的 RST 封包。在 Akamai 的報告裡，提到某些 Middlebox 除了有如下圖所示的送出帶有資料的 SYN 封包給受害目標外，當它收到受害目標回應的 RST 後，會再次送出那個引起受害目標回送 RST 封包的 SYN 封包，如此，不斷循環的形成無窮的 TCP 反射放大攻擊。

下圖顯示了以上案例的進一步操作。在上個案例中，攻擊者預先得知欲攻擊對象所開啟的 TCP 監聽埠（此例埠號為 45678），並在帶有載荷的 SYN 封包內，將來源 IP 位址偽造成 X.X.X.X、來源埠號設定為 45678、目的埠號設定為 80，然後送給 Middlebox (IP 位址 Z.Z.Z.Z)。

圖 6、Middlebox 將放大封包反射至受害目標有開啟 TCP 服務的埠

Middlebox 於是反射了兩個放大回應，以 TCP SYN 封包發送給受害目標，目的埠號是 45678。由於受害目標確實監聽了埠 45678，所以回傳 SYN-ACK 給 Middlebox，而 Middlebox 不會完成此三向交握，造成 TCP 半開放狀態 (half-open state)。從後續的流量可看出，攻擊者隨後又對 Middlebox 的不同埠號發送了相同的 SYN 封包，如此即形成受害目標端的資源消耗。

[更多的 Middlebox 反射放大攻擊方法]

除了以「目前 Middlebox 的 TCP 反射放大攻擊發生於 TCP 三向交握」為前提來發動反射放大攻擊外，Maryland 大學及 Colorado Boulder 大學的研究學者於 2021 年八月也提出其它基於 Middlebox TCP 反射放大的方法[2]。在這篇論文被公開不久之後，就出現實際應用於攻擊的案例。

Kevin Bock et al. [2] 的論文裡，觀察到其他 4 種可以引起 Middlebox 放大回應的方式，下表顯示了 5 種用來引起 Middlebox 回應的方式，其中角括號括起者，表示攻擊者發送 2 顆 sequence number 相續的封包。表格中的 PSH 及 PSH+ACK 方式，以標準的 TCP 協定實作方式來說，應無法成立攻擊，然而 Bock 等人的實驗卻顯示仍有反射放大的現象，顯然全球仍存在許多未符合 TCP 協定標準實作的 Middlebox 設備。

表 1、不同 TCP 類型封包引起的 Middlebox 回應統計

發送方法	回應比例 %	最大放大倍率
<SYN; PSH+ACK>	69.5%	7455X
<SYN; PSH>	65.7%	24X
PSH	44.6%	14X
PSH+ACK	33.1%	21X
SYN	11.4%	572X

資料來源：[2]

以下簡要描述這幾種方式。

< SYN; PSH+ACK> : 這個方法是指，攻擊者先對 Middlebox 送出一個正

常、不帶任何載荷的 TCP SYN 封包，其 sequence number 為 s，而後立刻再向 Middlebox 送一個帶有 HTTP GET 請求的 PSH+ACK 封包，sequence number 為 s+1。這兩個封包的來源 IP 位址均被偽造成受害目標的 IP 位址。從 Middlebox 的角度來看，這樣的兩個封包如同三向交握發起後，缺少 server 端的 SYN+ACK 及 client 端的 ACK，然後 client 直接發送 TCP 封包 (PSH+ACK)。但因為這個 PSH+ACK 的序號是正確的 (s+1)，Middlebox 仍會將之視為正常封包來處理。這種攻擊手法產生了最高比例的 Middlebox 回應，最高放大倍率達 7455 倍。

< SYN; PSH> : 這個方法與上一個方法類似，差別只在於所送出的第二個封包是 PSH 而不是 PSH+ACK。對這個方法做出回應的 Middlebox 比例，與上一個方法差不多，但沒有很極端的放大比例。

PSH : 這個方法只單獨送出一個帶有敏感資訊的 HTTP GET 請求，以 PSH 方式送給 Middlebox。對這種封包做出回應的 Middlebox 數量比預期多，但放大比率不高。

PSH+ACK : 與前一種方式的差別在於多設定了 ACK 旗標。所有對這個方式做出回應的 Middlebox，也會對 < SYN; PSH+ACK> 的方式做出回應，且回應的封包內容完全一樣。可以說 < SYN; PSH+ACK> 的方式涵蓋了 PSH+ACK 的方式。

SYN : 這種方式就是本文前半章節所描述的手法，將帶有敏感資訊的 HTTP GET 請求附於 TCP SYN payload 後發送給 Middlebox。雖然 Middlebox 回應的比例不高，但其中有 Middlebox 發送的放大回應達 572 倍。

三、Middlebox TCP 反射放大 DDoS 攻擊之防護建議

Middlebox 在網路架構中的角色定位即是分析防護機制，因此很難有完美的 Middlebox TCP 反射放大攻擊的防護方法，因為這涉及 Middlebox 設計通則 – 許多 Middlebox 就是被設計作為只檢視特定方向的封包流，而忽略流經

的封包是否屬於正常的 TCP 連線。然而仍然有一些緩解手段，可以減輕或是避免某些 Middlebox 被利用的可能

A.從 Middlebox 本身調整緩解

- 採用可檢視雙向流量的 Middlebox：部份作為內容過濾的 Middlebox 其功能整合在網路 Gateway 裡。這種 Middlebox 有能力判斷 TCP 連線狀態，而只處理或是將資訊注入到那些已建立有效 TCP 連線的封包裡。
- 將要注入到封包內的警告或說明資訊，降到最低的大小：Middlebox 在攔截到敏感資訊的存取要求時，以完整網頁的形式注入了大量資料到回覆封包裡，造成很高的放大倍率。建議調整這種情況下的回覆資料量，或是將回覆的網頁實作在另一台網頁伺服器上，而 Middlebox 僅送出一個 HTTP redirect 封包。
- 只過濾向外的流量：部份 Middlebox 的目的不在於保護內部網路資源，而在於限制內部網路設備對外部網路資源的存取。例如，某些管理政策嚴格的企業，禁止員工在公司內部網路瀏覽 Internet 上的特定資訊。這種情況下，Middlebox 就無須對由外部網路流往內部網路的流量進行攔截並作出回應，以避免被外部攻擊者利用作為反射攻擊。
- 不作任何的放大：只讓 Middlebox 回送一個 RST 來關閉連線也是一個簡潔有力的方式。

B.從防火牆進行緩解

上面幾點是針對 Middlebox 的緩解措施。如果 IT 或網管人員無法對 Middlebox 進行設定，就只能嘗試由防火牆的 ACL 來阻擋可疑封包：丟棄任何流入的、帶有載荷的 TCP SYN 封包。Akamai 提供了一個作為參考的防火牆 ACL。

deny tcp any eq 80 host x.x.x.x match-all +syn -ack packet-length gt 100

[注意事項]

- 攻擊者可能對任一埠發送帶有載荷的 TCP SYN 封包。上述防火牆 ACL 作為參考用途，只顯示作用於埠 80 的情況，可參考調整。
- 攻擊者發送的 TCP 封包，不限定於 SYN。上述防火牆 ACL 作為參考用

途，只顯示作用於 TCP SYN 封包的情況，可參考調整。

- 攻擊者發送給的偽造封包不一定會大於 100 bytes。正常不帶載荷的 TCP 封包，大小多為 60 bytes。上述防火牆 ACL 作為參考用途，只顯示了作用於封包大於 100 bytes 的情況，可參考調整。

四、分析與建議

以往進行 TCP Middlebox 反射放大攻擊的攻擊者，創建帶有觸發敏感資訊存取警示的 HTTP 請求，作為載荷夾帶於 TCP SYN 包並送往 Middlebox。在這些 HTTP 請求標頭內包含了不存在，或是不被允許存取的域名。當這些封包被送往 Middlebox 後，一旦決定處理這些封包，Middlebox 通常會回覆帶有 HTTP 標頭的封包，甚至整個 HTML 頁面。

這種回覆機制如同反射並放大攻擊者的封包給受害目標，某些 Middlebox 作出的回覆有著驚人的放大倍率。目前除了藉由 TCP SYN 封包來進行 Middlebox 反射放大攻擊外，已有研究人員提出了使用 < SYN; PSH+ACK> 的新手法，使得防範 Middlebox 反射放大攻擊更為困難。

為了防範 Middlebox 被利用作為反射放大攻擊的跳板，最好採用具有判斷 TCP 連線有效性的設備，並不要對帶有資料的 TCP SYN 封包進行內容處理。在攔截敏感資料的存取要求時，於回覆封包中所注入的警告或限制資料要盡可能的小。IT 或網管人員也可在防火牆建立阻擋規則，將異常大小的 TCP SYN 封包丟棄。

Middlebox 的反射放大攻擊屬於新興的 DDoS 攻擊，也因 Middlebox 的設備角色，致使在防護難度更加提升，且攻擊手法持續演進，這類型攻擊是必須持續關注的。

若企業對 Middlebox TCP 反射放大攻擊有相關檢(複)測疑問，歡迎與 TWCERT/CC 聯繫。

- 資料來源：

1. Akamai. TCP Middlebox Reflection: Coming to a DDoS Near You.
2. Kevin Bock, Abdulrahman Alaraj, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin. Weaponizin
3. Jack Edge. Weaponizing middleboxes.
4. Ravie Lakshmanan. Hackers Begin Weaponizing TCP Middlebox Reflection for Amplified DDoS Attacks
5. Shadowserver Foundation. Over 18.8 million IPs vulnerable to Middlebox TCP reflection DDoS atta
6. Shadowserver Foundation. Vulnerable DDoS Middlebox Report.

第 3 章、 資安活動紀事

資安防護及案例分享研討會-台中場

活動時間：111.11.18(五) 14:00~16:30

活動議程：

時間	議程	主講者
13:30 ~ 14:00	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	網路與資訊安全管理實務分享	漢翔航空工業股份有限公司 方一定處長 阮文聰組長
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 11 月 18 日於經濟部加工出口區管理處中港分處三樓訓練教室舉辦。鑒於製造業邁向工業 4.0 設備聯網，促使 IT 與 OT 匯流，讓工控環境成為駭客熟悉易攻的場域，更因 OT 機台難以長時間停機定期修補與更新，且企業遭受攻擊將連帶影響供應鏈廠商，導致製造業的資安管理陷入困境。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)免費資安通報的資源，並邀請專業講師探討「網路與資訊安全管理實務分享」，從工業 4.0 機聯網資安防護至供應鏈資安管理，讓企業建立 OT 資安管理新思維。

首先由 TWCERT/CC 曲承則工程師講授「TWCERT/CC 服務範疇及案例分享」，特別分享與企業人士分享各類型資安威脅案例。內容涵蓋釣魚網站威脅攻擊中如何進行識別及留意警示訊息；DDoS 攻擊強調了殭屍網路背後的獨特力量，企業更應採取防護做好安全設定；針對各大瀏覽器的近期重大更新做相關提醒；勒索軟體攻擊案件及建議措施。由此可見，在網路時代下資安即國安已成事實，曲工程師建議大家面對勒索攻擊可有以下措施：首先一定要使用防毒軟體並即時更新系統、實施網路分段區隔並監控流量、僅在需要時啟用 Microsoft Office 巨集、必須要加密重要或敏感資料、更需要安排定期進行檔案備份。接續詳細介紹說明 TWCERT/CC 資安服務內容：資安事件通報、網路釣魚通報、產品漏洞通報、惡意檔案檢測，並鼓勵企業一同申請加入 TWCERT/CC 資安聯盟與訂閱情資電子報，企業可第一手取得資安情資與優先預警的資訊，以預防類似事件發生。

接著研討會第二個議程特別邀請漢翔航空工業股份有限公司方一定處長以及阮文聰組長一同講授「網路與資訊安全管理實務分享」。首先由方一定處長針對資安事件頻傳如何資安防護處理、IoT 設備的風險如何管控以及企業資安防護所面臨的挑戰進行講解。根據工研院統計，多數來自內部技術能量不足、公司對於資安投資報酬率缺乏了解，以及內部員工缺乏資安意識所導致，另一因素更是來自於對企業主而言導入資安其效果難以量化，僅能以遭受攻擊後停機停工時間之損失進行量化，而非增加企業營業額或製程效率等。方處長提出善用政府資源提升企業資安防護能力之建議，企業資安評級協助建立持續性強化資安的生態環境快速掌握風險，推動資安管理制度落實機敏資料分級管制及加密。

接下來由阮文聰組長繼續講授資訊安全多方面防護及機制，建議企業做「資安檢測與弱點掃描」，透過檢測來了解企業內部機台是否正在執行不安全之軟體。最後建議企業做「資安管理面的規劃」包含了資安健檢，檢視公司內部資安網絡的建置、防火牆、郵件設定並強化企業人員資訊安全訓練開始進行資安環境的建立。最後簡單分享導入 ISO27001 資訊安全管理系統，以

提升企業信譽及管理效率。

最後議程 Q&A 時段，參與企業人士踴躍提出詢問：首先第一個問題詢問「請問中小型製造業是否有相對應的資安方案?」方處長回覆最簡單方式以設定防火牆來阻斷部分網站瀏覽，再來是郵件於非必要盡可能不要有對外的功能，都是足以達到防護，當然如同剛提到人員訓練提升認知也是很重要。第二個問題「請問如果公司內部先前沒有相關的文件，公司內部未來要自己做政策文件的話，怎麼從 0 開始建置呢？」方處長回覆可依 ISO27001 條文防護條件制定成資訊管理作業要點，建立公司內部簡單作業文件，提供企業全員共同遵循。第三個問題「若要導入 ISO27001，通常會找專門的顧問公司協助嗎?」方處長回覆企業有足夠預算當然可找專業顧問協助導入。

本場研討會為實體與線上同步舉辦共 105 人與會，經由三位講師的資安探討，與會人員皆受益良多，以及認識 TWCERT/CC 詳細的服務內容，與會者對於本場研討會內容、講師專業度、場地滿意度等表達為滿意。

第 4 章、 國內外重要資安事件

4.1、資安趨勢

ESET 公布 2022 全球中小企業資安防護調查報告

資安廠商 ESET 日前公布一份調查報告「2022 ESET SMB Digital Security Sentiment Report」，指出 2022 全球中小企業面臨日漸複雜的混合式工作形態，以及愈來愈嚴重的資安攻擊威脅，對於企業能夠有效抵擋資安攻擊的信心並不高。

據 ESET 表示，在 COVID-19 疫情與烏俄戰爭後，中小企業面對工作形態的轉變，愈來愈多公司採用混合辦公室與遠距上班的工作形態，大量借助各種網路工具來維持公司運作的結果，例如利用遠端桌面遙控協定 (Remote Desktop Protocol, RDP) 或是各種雲端儲存與運算服務，也造成駭侵者可攻擊的弱點大量增加。

ESET 的報告指出，2022 年偵測到的資安威脅，年成長率達 20%；其中網頁攻擊成長 28%，透過 Outlook 進行的釣魚信件登入釣魚攻擊更成長 66%。

ESET 在調查報告中指出，在這種情況下，2022 年接受調查的全球中小企業，有 32% 備有資安攻擊偵測與處理解決方案，也有 33% 中小企業表示未來一年內將考慮建置這類系統。

不過報告也指出，中小企業受限於營運規模與營收相對較少，對於自身 IT 防護能力的信心相當低落；僅有 32% 中小企業認為自己的 IT 團隊具備足夠的資安防護知識、僅有 30% 中小企業該為自己的公司可以快速應對資安威脅，立即辨識、隔離威脅並適當反應；僅有 27% 中小企業認為自己能在攻擊發生後進行詳細分析，以強化弱點。

建議中小企業應根據自身的需求與能力，尋求專家提供資安防護規畫與布署，採用最適合的防禦策略，以免因攻擊而蒙受無法負荷的重大損失。

- 資料來源：
  1. Toward the cutting edge: SMBs contemplating enterprise security
  2. 2022 ESET SMB Digital Security Sentiment Report

4.2、新興應用資安

4.2.1、駭客利用物聯網裝置中停止維護的 web server 漏洞攻擊能源產業

Microsoft 日前指出，近期發現一個早在 2005 年就停止更新，但仍廣泛運用於各種物聯網（Internet of Things, IoT）裝置中的 web server 軟體 Boa，其中含有多個漏洞，證實已經遭到駭侵者用於攻擊能源產業中的多個組織。

Microsoft 在近期發表的資安通報中指出，該公司持續觀察到駭侵者試圖透過 Boa 中的各種漏洞，針對全球多個能源產業公司發動各種攻擊。駭侵者可以利用這些漏洞遠端執行任意程式碼，並發動進一步的攻擊。

Microsoft 指出，早已停止維護的 Boa web server 內含多個漏洞，包括可任意存取檔案的 CVE-2017-9833，以及可能造成資訊外洩的 CVE-2021-33558 等。而 Boa web server 仍廣泛用於全球各種 IoT 裝置中，例如網路攝影機、路由器等。

資安廠商 Recorded Future 也在四月時發現，駭侵團體 RedEcho 利用 Boa web server 的漏洞，入侵多家印度電力公司的網路監視器，作為駭侵攻擊的控

制伺服器後，進一步攻擊其電網控制裝置；該組織也成功透過網路監視錄影機的漏洞，入侵印度某個國家緊急應變系統，以及某家大型跨國物流業者的子公司。

據資安媒體 Bleeping Computer 利用 Shodan 工具掃瞄全球網路的結果，顯示全球仍有近 90 萬台裝置使用 Boa web server，其中設備數量最多的是越南，有近 172,000 台，印度有近 107,000 台，其次是南韓（約 100,000 台）、台灣與巴西（約 60,000 台）。

建議各關鍵基礎設施公私單位，應在例行的資安維護中定期檢視各連網裝置使用的軟體或韌體是否已停止維護，且應在無法取得更新後儘速停用並汰舊換新，以免舊漏洞無法更新，成為駭侵攻擊破口。

- 資料來源：
  1. Vulnerable SDK components lead to supply chain risks in IoT and OT environments
  2. Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group
  3. Hackers breach energy orgs via bugs in discontinued web server

4.2.2、新發現 KmsdBot 惡意軟體進行加密貨幣挖礦與 DDoS 攻擊活動

網路基礎架構公司 Akamai 旗下的資安研究人員，近來發現一個全新的侵入型惡意軟體 KmsdBot，會利用防護力薄弱的登入資訊，以 SSH 連線登入受害主機，進行加密貨幣挖礦與分散式服務阻斷（Distributed Denial of Service, DDoS）攻擊。

據 Akamai 發表的研究報告指出，該公司發現 KmsdBot 會鎖定包括遊戲公司、科技公司、豪華轎車生產廠商，甚至資安防護廠商等產業進行攻擊。

Akamai 觀察到 KmsdBot 發動的 DDoS 攻擊首例，是針對遊戲公司 FiveM；該公司讓玩家可以自行設立「俠盜獵車手」（Grand Theft Auto）Online 的私人伺服器，而 KmsdBot 鎖定該公司的服務，進行 Layer 4 與 Layer 7 的攻擊。

針對 KmsdBot 運作模式的分析則指出，該惡意軟體 kmsdx 會先進行掃瞄程序、軟體更新以及背景加密貨幣挖礦，同時也會與駭侵者設立的控制伺服器連線，然後下載一批登入資訊，試圖以掃瞄到的開放 SSH 連接埠來進行連線。

在加密貨幣挖礦方面，KmsdBot 使用的是更名過的 xmrig 挖礦程式，通常用來挖掘難以追蹤流向與收發者的 Monero 加密貨幣。

Akamai 的報告也指出，這個 KmsdBot 是跨平台的，可以感染 Winx86、Arm64、mips64、X86_64 等不同平台。

建議不論個人或企業，均應避免使用防護能力薄弱的登入帳密，除應開啟多階段登入驗證外，也應確保系統與軟體經常更新至最新版本，且應關閉所有不應對外開放的 Telnet、FTP、SSH 連接埠。

- 資料來源：
  1. KmsdBot: The Attack and Mine Malware
  2. KmsdBot, a new evasive bot for cryptomining activity and DDoS attacks

4.2.3、美國司法部將涉嫌利用交易系統漏洞，竊取 50,000 枚比特幣的駭侵者定罪

美國司法部（Department of Justice）於 2022 年 11 月 4 日公開宣布，將一名涉嫌自 Silk Road 暗網市集竊取高達 50,000 枚以上比特幣的駭侵者定罪，罪嫌將面臨至少 20 年徒刑。

這名嫌疑人的名字是 James Zhong，美國司法部指出 Zhong 涉及於 2012 年 11 月時「利用提領處理流程的漏洞」，多次從 Slik Road 暗網超額提領比特幣，總額高達 51,351.9 枚比特幣，換算後高達 33 億美元。

美國司法部控訴 Zhong 的罪名是洗錢罪；他過去在惡名昭彰的暗網市集「Silk Road」任職，這個地下網路市集現已停止營運，其營運期間在 2011 年到 2013 年間，專門交易各種非法產品，全盛時期有 100,000 名以上會員。

Zhong 承認利用 Silk Road 交易系統的時間差漏洞，利用此漏洞即可多次重覆提領同一筆資金；Zhong 利用 9 個比特幣帳號，先存入 200 到 2,000 枚比特幣，接下來快速同步發動 140 筆提領作業，從系統提領出 50,000 枚比特幣，再轉到其他錢包以混淆資金流向。

美國司法部指出，除了比特幣贓款外，還在 Zhong 的住處發現大批財物，包括高達 661,900 美元的現金、價值 174 枚比特幣的實體比特幣高加索

硬幣、金條、銀條與金幣等。

美國司法部指出，現今的加密貨幣金流追蹤技術已相當成熟，再加上該局幹員鍥而不捨的辦案精神，終於將罪嫌繩之以法。

建議各個可以使用加密貨幣進行交易或提供金融服務的公私單位，都需與具備經驗的第三方資安查核單位合作，對系統程式碼的安全性進行嚴格測試，並加強內控，以杜絕類似監守自盜事件再次發生。

- 資料來源：
  1. U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection W
  2. U.S. unmasks hacker who stole 50,000 bitcoins from Silk Road

4.3、國際政府組織資安資訊

4.3.1、美國白宮召開國際會議，共同對抗勒贖攻擊

美國白宮日前宣布，將於 2022 年 10 月 31 日起，舉辦第二屆「啟動對抗勒贖攻擊國際高峰會」（International Counter Ransomware Initiative Summit），結合各國力量，共同加強對於勒贖攻擊的防禦與打擊力量。

據美國白宮在記者會上的說明，這次為期兩天的高峰會，將以實體方式舉辦，邀請多達 36 個國家以及歐盟的資安領域專家和相關領導人士，分為五組，討論不同領域間如何強化對抗日益猖獗的勒贖攻擊，並且嚇阻在幕後發動勒贖攻擊的犯罪分子。

一位美國政府高層人士在記者會上指出，「勒贖攻擊確實是全球性的問題，已經見到勒贖攻擊不論在複雜度或攻擊發生次數的成長，都遠較防禦與防治能力的成長為快」。

官員也指出，這次高峰會不只是政府對政府間的會談，同時也邀請私部門共同參與，有 13 家全球大型企業指派代表與會，包括 Microsoft、Palo Auto Networks、Siemens、SAP、Crowdstrike、Mandiant 等，希望能促成公私部門在對抗勒贖攻擊時，合作能夠更加密切。

這次會議分成五個小組進行討論，「韌性」議題由印度與立陶宛主持、「防治」議題由澳洲主持、「虛擬貨幣」議題由新加坡與英國主持、「公私部門合作」議題由西班牙主持、「國際合作」議題由德國主持。

參加本次高峰會的國家除主辦國美國外，也包括奧地利、比利時、巴西、保加利亞、加拿大、克羅埃西亞、捷克、多明尼加共和國、愛沙尼亞、歐盟、法國、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、挪威、波蘭、南韓、羅馬尼亞、南非、瑞典、瑞士、烏克蘭、阿拉伯聯合大公國。

- 資料來源：
  1. White House seeks international cooperation to thwart growing ransomware threat
  2. Background Press Call by a Senior Administration Official Previewing the Second International Counte
  3. White House aims to ‘redouble’ global push against ransomware

4.3.2、歐洲多國警告世足球迷，避免使用主辦國政府提供的 App，以防個資遭到濫用

包括挪威、法國、德國等多個歐洲國家的數位與資安部門，日前對即將前往本屆世足賽主辦國觀賽的球迷提出警告：主辦國卡達政府提供的兩種官方 App「Ehteraz」與「Hayya」，會收集許多個資；如果必須安裝這些 App，務必小心謹慎，建議使用「可拋棄式手機」來安裝。

「Ehteraz」是由卡達公共衛生部推出的 Covid-19 追蹤軟體，可顯示用戶與其他染疫確診者的接觸史；而「Haaya」則是由該國政府針對世界盃足球賽開發的 App，球迷可憑此 App 購買門票、入場觀戰，並且免費搭乘大眾交通工具如捷運或公車。

挪威資料保護署日前指出，這兩個應用程式可以存取的資料類型過多；該單位也提出警告，指出卡達政府可能會利用這兩個 App 取得用戶個資，甚至監控目標用戶的所在地。

法國數位部副部長也在 Twitter 上發文，提供由法國國家資訊自由委員會（Commission Nationale de l'Informatique et des Liberté）提供的資安自我保護檢核表，了解如何在旅途中保護行動裝置的資安。

德國聯邦資料保護與資訊自由署（Bundesbeauftragten für den Datenschutz und die Informationsfreiheit，BfDi）也指出，「Ehteraz」和「Hayya」能夠存取的資料種類，遠多於該應用程式在 App Store 中資料使用狀況的說明，兩個 App 中有一個會收集用戶資料，另一個會阻止裝置進入睡眠模式，還會將資料上傳到集中化伺服器。

BfDi 也建議，只有在必要的情形下才安裝使用這兩個 App，且最好使用可拋棄式手機來安裝，避免個資外洩。

- 資料來源：
  1. Voyager en dehors de l'UE : la checklist de la CNIL pour protéger votre téléphone, ordinateur ou tab
  2. Stellenangebote
  3. Germany says nein to Qatari World Cup spyware, err, apps

4.3.3、美國政府發現有駭客利用 Log4Shell 漏洞駭入聯邦政府單位，進行加密貨幣挖礦

美國政府資安主管機關聯邦調查局（Federal Bereau of Investigation，FBI）與網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），日前聯合發布資安通報，指出一個名稱未知，由伊朗政府於幕後支持的駭侵團體，日前利用 Log4Shell 漏洞，駭入某美國聯邦政府民事執行分支單位（Federal Civilian Executive Branch，FCEB）的主機，植入惡意軟體 XMRig，利用該主機資源進行加密貨幣挖礦。

報告指出，駭侵者係利用該單位未經修補的 VMware Horizon 伺服器，透過 Log4Shell（CVE-2021-44228）遠端執行任意程式碼漏洞，來植入惡意軟體。

報告也表示，伊朗駭侵者同時也在遭到攻擊的伺服器上設立了 reverse proxy，以維持該惡意軟體持續存於該 FCEB 的內網之中。

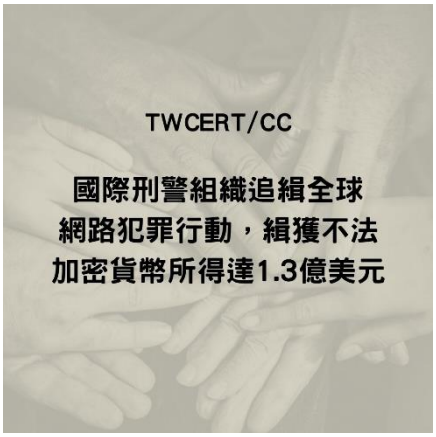
FBI 與 CISA 也表示，所有尚未修補單位所有 VMware 系統之 Log4Shell 漏洞的單位，都應該假設本身已遭長期駭侵攻擊，應立即聯絡 FBI 與 CISA 開始進行內網惡意軟體與漏洞調查。

FBI 與 CISA 指出，在 Log4Shell 漏洞於去（2021）年 12 月被發現已來，至今仍有許多應立即修補漏洞的公私單位系統未能修補；有國家勢力支持的多組駭侵者，至今也持續不斷進行掃瞄，以發現可資攻擊的系統進行攻擊。

建議各公私單位的系統管理者，隨時注意漏洞與更新訊息，並在軟體系統可以更新時立即更新，以免遭到駭侵者利用未修補的已公開漏洞發動攻擊。

- 資料來源：
  1. Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential
  2. US govt: Iranian hackers breached federal agency using Log4Shell exploit

4.3.4、國際刑警組織追緝全球網路犯罪行動，緝獲不法加密貨幣所得達 1.3 億美元



國際刑警組織（INTERPOL）日前發表公告，公布近日執行的一波全球不法網路犯罪打擊行動成果，一共緝獲不法加密貨幣所得高達 1.3 億美元。

這波執法行動的行動代號是「HAECHI III」，共有 30 個國家與地區的警察單位加入合作。於 2022 年 6 月 28 日起開始執行，到 11 月 23 日止，際刑警組織在行動中逮捕的網路犯罪分子近一千人。

國際刑警組織在公告中指出，這波跨國網路犯罪打擊行動，共逮捕 975 名嫌犯，涉及的各式網路犯罪案件高達 1,600 件；國際刑警組織也封鎖了近 2,800 個由這些網路犯罪分子操控，用於各種金融犯罪的銀行與虛擬資產帳戶。

在這次破獲的網路犯罪類型方面，包括愛情詐騙、語音釣魚、性虐待、投資詐騙、網路賭博與跨國洗錢等。

國際刑警組織也指出，這波執法行動也發現投資詐騙案件數量較過往大幅增加，主要利用內容經過加密的即時通訊，來誘使受害者使用加密貨幣錢包進行轉帳付款。其中一個主要案件，國際刑警組織分別在希臘與義大利各

逮捕一名韓國人；這兩人涉嫌從 2,000 名韓國受害者詐騙高達 2,800 萬歐元。

國際刑警組織也指出，另一個由澳洲與印度警方偵辦的網路犯罪集團，對受害者自稱是國際刑警組織幹員，要求受害者透過金融機構、加密貨幣交易所或點數卡來繳納罰金，不法所得約 160,000 美元。印度警方破獲該集團設於印度境內的電話中心，除緝獲多個加密貨幣錢包外，也掌握諸多犯罪證據。

此外，國際刑警組織也指出，先前設立的國際洗錢快速反應防制協議（Anti-Money Laundering Rapid Response Protocol，ARRP），在這次行動中成效卓著，自本年 1 月起，已經追回 1.2 億美元的網路犯罪不法所得。

建議一般用戶如果發現自己可能遭到這類網路詐騙案，應立即報警處理，透過國際合作，共同扼止日益猖獗的跨國網路犯罪活動。

- 資料來源：
  1. Cyber-enabled financial crime: USD 130 million intercepted in global INTERPOL police operation
  2. Interpol seized $130 million from cybercriminals worldwide

4.4、社群媒體資安近況

4.4.1、Twitter 宣布對認證帳號收費，各種釣魚攻擊伺機發動詐騙攻擊

隨著社群平台 Twitter 在日前由 Elon Musk 收購，並宣布要針對認證帳號收取每月 8 美元費用後，專業資安媒體 BleepingComputer 最近發現以此收費為由，針對已認證帳號持有人發動的釣魚攻擊，數量也大幅增加。

Twitter 在由 Tesla 執行長 Elon Musk 在日前完成全資收購後，Elon Musk 為改善 Twitter 財務狀況，宣布將對擁有官方身分認證（即俗稱「藍勾勾」）的使用者，加收每月 20 美元的費用，稍候又宣布降為每月 8 美元。

BleepingComupter 發現，在 Twitter 這一系列收費公告發表之後，以此為由針對已認證使用者的釣魚攻擊就大幅增加。

這一波針對 Twitter 身分認證使用者的釣魚攻擊，和其他名目的釣魚攻擊十分類似；被列為攻擊目標的 Twitter 身分認證使用者會收到假冒為 Twitter 官方的釣魚信件，內容指稱根據本平台的新身分認證措施，用戶必須在某個時限內點按信中的釣魚連結，重新進行身分認證，否則將撤銷其已通過認證

的資格。

當用戶點按信中的釣魚連結後，會被導到一個幾可亂真的釣魚網頁，誘騙用戶輸入自己的 Twitter 登入資訊。

資安專家指出，不只是這波趁 Twitter 宣布收費為由的釣魚攻擊，事實上各社群平台的官方認證帳號，經常是各類釣魚攻擊的駭侵目標，因為擁有這種已認證帳號的用戶，多半屬於重要公部門、企業品牌、政治人物、演藝人員、新聞媒體、網紅等追蹤者較多，影響力較大的單位或個人；駭侵者透過釣魚攻擊取得帳號控制權後，就可以發動各種後續攻擊，例如散布假新聞或惡意軟體、進行金融詐騙等。

建議擁有社群平台官方帳號管理權限者，務必開啟多階段登入認證，並對各種號稱平台官方發送的 email、簡訊、貼文等提高警覺，絕不隨意點按不明連結，且不可將登入資訊隨意提供他人。

- 資料來源：
  1. New Phishing Email Exploits Twitter's Plan to Charge for Blue Checkmark
  2. As Twitter brings on $8 fee, phishing emails target verified accounts

4.4.2、Twitter 推出每月 8 美元帳號認證標誌後，出現大量加密貨幣詐騙的已認證帳號

Twitter 為了增加營收，日前推出每月 8 美元帳號認證計畫，但該計畫在推出後就遭到多個駭侵團體濫用，利用公信力較高的認證帳號來發動加密貨幣詐騙攻擊。

過去 Twitter 的認證帳號必須經由 Twitter 團隊驗證後才能取得，以一個藍色勾勾圖示來識別真實的政府、政治人物、媒體、網紅、品牌、運動員、明星、意見領袖等。

在 Twitter 由 Tesla 執行長 Elon Musk 全資收購後，為改善 Twitter 的財務狀況，Twitter 在 2022 年 11 月初起，針對美國、加拿大、英國、澳洲與紐西蘭用戶推出每月付款 8 美元即可取得認證圖示的計畫；然而該計畫卻於一開始就遭到駭侵團體濫用於加密貨幣詐騙活動。

資安專業媒體 BleepingComputer 報導指出，駭侵者先以任意 Twitter 帳號註冊並加入每月 8 美元認證計畫，在其帳號上顯示認證標誌後，立即就將該帳號的顯示名稱（Display Name）改為假冒對象，然後張貼詐騙訊息。

一個案例是某個實際帳號為 @SzAt_0 的帳號，在取得認證圖示後，立即將頭像與顯示名稱改為 Twitter，假冒為 Twitter 官方帳號進行加密貨幣詐騙，

以高額加密貨幣空投活動誘使用戶輸入自己的錢包位址與恢復短語。

另一個案例是透過 8 美元認證計畫的假帳號，將自己偽裝成 Twitter 新擁有人 Elon Musk。

由於 Twitter 這個 8 美元認證計畫推出後，反而造成許多假冒帳號也能取得認證圖示，因此 Twitter 目前已緊急處置，暫時禁止取得認證的帳號變更其顯示名稱，以防止有人在取得認證圖示後改變顯示名稱，用於假冒或詐騙活動。

建議用戶在社群媒體上檢視內容時，應對過度優惠或高額獎勵的訊息提高警覺，即使發文帳號具有認證圖示，也很可能是由駭侵者假冒，或帳號本身遭到挾持盜走。

- 資料來源：
  1. About Twitter Blue
  2. An $8 mess — Twitter Blue 'verified' accounts push crypto scams

4.5、行動裝置資安訊息

4.5.1、Google Play Store 中的 Android 檔案管理類多個 App 內含 Sharkbot 金融木馬

資安廠商 Bitdefender 近期發表研究報告指出，該公司旗下的資安團隊發現 Google Play Store 內有多個檔案管理類 App，實際上內含一個名為 Sharkbot 金融木馬惡意軟體，針對英國、義大利等國手機用戶，竊取用戶登入網路銀行的帳號密碼。

報告指出，Sharkbot 是一個危險的惡意軟體，用戶不慎下載含有 Sharkbot 的應用程式後，Sharkbot 會在用戶登入自己的網路銀行帳戶時，顯示假的登入頁面，蓋過真正的登入頁面，伺機竊取用戶的登入資訊，並傳送到駭侵者處。

這批由 Bitdefender 發現的 Adnroid 惡意軟體，都屬於和金融服務無關的檔案管理類應用程式；駭侵者用來申請上架的應用程式本身不含任何惡意程式碼，在通過 Google Play Store 的審核後並安裝到用戶的 Android 手機上後，才會取得惡意程式碼。

資安專家指出，由於這些軟體都是工具類軟體，因此在向用戶要求較多存取權限時，比較不易引發用戶警覺。

Bitdefenfer 指出，這批惡意 Android App 包括 X-File Manager、FileVoyager、LiteCleaner M 等等。以 X-File Manager 來說，僅在偵測到用戶的 SIM 卡屬於英國和義大利電信業者時，才會啟動惡意程式碼，因此可算是一種目標式攻擊行動；但其他 Sharkbot 惡意軟體的攻擊對象，還包括其他國家如伊朗、德國等地的用戶。

在該報告發表後，這批惡意 Android 應用程式已遭下架。

由於這類內含惡意軟體的行動應用程式，往往能夠逃過官方機制，順利上架到 Google Play Store，因此用戶必須啟動手機中的 Play Protect 服務；當發現應用程式為惡意軟體時可自動移除，且應安裝大廠出品的防毒防駭軟體，以偵測 App 的異常活動。

- 資料來源：
  1. Android SharkBot Droppers on Google Play Underline Platform's Security Needs
  2. Android file manager apps infect thousands with Sharkbot malware

4.5.2、發現 Google Play Store 中的惡意 Android App，會用來註冊多種服務的假帳號

資安廠商 Evina 旗下的研究人員，近期發現一個位於 Google Play Store 的 Android 惡意軟體 Symoo，在受害者下載安裝後，會成為幫助駭侵者大量註冊各種網路服務假帳號的工具。

研究人員指出，Android 裝置用戶一旦安裝了 Symoo，該裝置就會被當作一個簡訊「中繼點」；Symoo 會利用用戶的手機門號大量註冊 Microsoft、Google、Instagram、Telegram、Facebook 等網路服務的假帳號，用戶會不停收到註冊這些帳號時系統發送的單次有效密碼（One-Time Password, OTP）。

Evina 的報告說，用戶在安裝 Symoo 時，該 App 會要求用戶授予存取簡訊的權限；由於 Symoo 在軟體說明中自稱是一種「簡單易用的簡訊工具」，因此用戶多半會不疑有他；接下來 Symoo 會要求用戶輸入手機號碼，並顯示一個假的資源載入中畫面；這個畫面上的進度非常緩慢，而 Symoo 就會利用這個時間來註冊假帳號，並將手機收到的雙重驗證碼傳送給駭侵者。

此外，研究人員還發現 Symoo 用來傳送驗證簡訊內容的網域，也由另一個稱為「Virtual Number」的 App 使用；而 Virtual Number 的開發者還推出了另一個提供「暫時手機門號」的 App ActivationPW，該 App 宣稱可讓用戶以

不到 50 美分的價錢，獲得一個可用來驗證帳號註冊的門號；研究人員懷疑 ActivationPW 就是使用 Symoo 來進行簡訊驗證。

建議 Android 用戶即使是在官方的 Google App Store 中下載任何軟體，均應提高警覺，細閱用戶評價與反應；如發現有人反應該軟體有問題，切勿下載安裝。

- 資料來源：
  1. Maxime Ingrao @IngraoMaxime
  2. Misleading Android App Symoo Reads & Forwards SMS To Account Creation App
     Malicious Android app found powering account creation service

4.5.3、駭侵者竄改 Android 版 OpenVPN app，內含間諜惡意軟體

資安廠商 ESET 日前發表研究報告，指出該公司的資安研究專家，近期發現有駭侵者長期利用植入惡意軟體的 SoftVPN 和 OpenVPN 等兩種 Android VPN app，來散布含有惡意程式碼的假軟體，自受害者的行動裝置中竊取各種機敏資訊。

據 ESET 報告指出，涉嫌散布間諜 VPN 軟體的是一個被稱為「Bahamut」的進階駭侵團體，據稱該團體提供「租用」服務，讓想發動攻擊的人出錢來進行攻擊。

報告說，Bahamut 針對市面上正常版本的 Android 版 SoftVPN 和 OpenVPN app 進行重新包裝，植入惡意軟體後，利用幾可亂真的網站來散布 APK 檔；用戶如果不查，自這些假網站下載安裝 APK 檔，即會遭到惡意軟體感染。

報告指出，目前發現的這類惡意 App 均未在 Google Play Store 上架。

該報告說，用戶一旦不慎安裝這兩個假冒的 VPN App，其中的間諜程式碼會竊取受害者手機中的多種機敏資訊，包括通訊錄、通話記錄、詳細所在地點座標、簡訊對話內容，並監控用戶透過如 Signal、Viber、WhatsApp、

Telegram、Facebook Messenger 等即時通訊軟體的訊息內容，以及手機內的各種檔案。

ESET 也觀察到共有 8 種不同 Bahamut 假冒 VPN 的版本，顯示該惡意軟體的開發工作十分積極，不斷推出新版本。

據 ESET 指出，Bahamut 這波攻擊活動可能屬於目標鎖定式攻擊行動，雖然初始的攻擊方式仍有待調查，但通常會利用釣魚 Email、釣魚簡訊、社群平台或即時通訊來進行，誘使目標下載惡意軟體。

建議 Android 手機用戶應絕對避免自非官方管道（如不明網頁、社群平台連結、Email 連結）等安裝任何 APK 檔案，以避免安裝類似惡意軟體，並遭到駭侵攻擊。

- 資料來源：
  1. ESET Research: Bahamut group targets Android users with fake VPN apps; spyware steals users' convers
  2. Hackers modify popular OpenVPN Android app to include spyware

4.5.4、4 個惡意 Android App 被發現存於 Google Play Store，總下載次數超過 100 萬次

資安廠商 Malwarebyte 日前發表研究報告，指出該公司旗下的資安專家，發現有 4 個惡意軟體成功於 Google Play Store 上架；這四個惡意軟體會將用戶導向到假網站竊取資訊，或是在背景點擊廣告以賺取假點金佣金。

這四個惡意 Android App 分別是：

- Bluetooth Auto Connect：下載次數超過 100 萬次；
- Bluetooth App Sender：下載次數超過 5 萬次；
- Driver: Bluetooth, Wi-Fi, USB：下載次數超過 1 萬次；
- Mobile Transfer：Smart Switch：下載次數超過 1,000 次。

這些惡意軟體還會顯示通知，誘騙用戶下載更多惡意軟體並安裝到其手機中；而 Malwarebyte 的報告也指出，上列四個惡意 Android 軟體在 Goole Play Store 中所列出的開發者「Mobile apps Group」，過去有兩次在 Google Play Store 中上架惡意軟體的記錄，然而 Google Play Store 至今並未針對該開發者帳號進行任何停權處分，使得該帳號仍能繼續於 Google Play Store 內上架惡意軟體。

據 Malwarebyte 的報告指出，這批惡意軟體會在安裝後 72 小時才開始顯示大量廣告與釣魚連結，接著每兩小時就會開啟多個瀏覽器分頁，顯示更多類似廣告；甚至當用戶未使用手機時，該惡意軟體仍然會開啟分頁，因此當用戶隔了一陣子再開啟手機時，就會發現瀏覽器已經開啟大量分頁，全是惡意廣告或釣魚網站內容。

建議 Android 手機用戶，即使在官方的 Google Play Store 內下載軟體，仍不可掉以輕心；下載安裝前先仔細閱讀用戶評價，如果較多差評就要避免下載。

- 資料來源：
  1. Malware on the Google Play store leads to harmful phishing sites
  2. Malicious Android apps with 1M+ installs found on Google Play

4.6、軟體系統資安議題

4.6.1、歐洲最大銅製品工廠 Aurubis 遭駭，IT 系統下線以防損害擴大

歐洲最大，也是全球第二大銅製品生產大廠 Aurubis 於 2022 年 10 月 28 日遭到駭侵攻擊，導致該公司被迫關閉其多處據點的 IT 系統，以防止損害進一步擴大。

總部位於德國漢堡，全球員工近 6,900 人的 Aurubis，日前在官網上發表資安通報，指出該公司部分廠區遭到不明駭侵攻擊；該公司目前正在會同有關單位進行調查，且為避免損害進一步擴大，已關閉部分 IT 系統的運作。包括精煉生產線與環保相關設備仍保持運作，而原料入廠與產品出廠則改採人工作業。

該公司表示，維持原料進廠與成品出廠數量在正常水準不受影響，是該公司目前的首要目標，因此部分生產流程在相關自動化系統修復之前，均改為人工操作；但該公司也表示，目前無法估計何時才能修復受損系統，全面恢復正常作業。

該廠也表示，正在努力復原該廠與上下游供應鏈與客戶之間的正常通訊管道；目前唯一可用的通訊方式是電話。

該廠尚未提供任何有關此次駭侵攻擊事件的詳細資訊，包括駭侵攻擊的形態、攻擊管理與具體的損失等，僅對外表示這次攻擊「明顯屬於針對金屬工業與礦業更大規模攻擊的一環」；不過資安專家普遍認為 Aurubis 這次的攻擊應屬勒贖攻擊。

Aurubis 並非大型金屬礦業公司遭到駭侵攻擊的首例，早在 2019 年 3 月，全球最大鋁業公司之一的 Norsk Hydro 就曾遭到 LockerGoga 勒贖攻擊，造成其 IT 系統被迫離線。

針對製造業發動的駭侵攻擊，往往會造成生產與供應鏈的衝擊；建議各製造業者應正視駭侵攻擊的可能性，除加強資安防護能力外，重要的製造相關系統不宜直接與 Internet 連線。

- 資料來源：
  1. Update on cyber attack at Aurubis
  2. Largest EU copper producer Aurubis suffers cyberattack, IT outage

4.6.2、駭侵團體利用超過 42,000 個網域偽裝為可口可樂、麥當勞等知名品牌，發動大規模詐騙攻擊

資安廠商 Cyjax 日前發表調查報告，指出該公司旗下的資安專家，近來發現駭侵團體 Fangxiao，利用一個具有超過 42,000 個網域的龐大網路，偽裝為多個全球知名品牌，利用假抽獎活動等方式，誘騙受害者安裝廣告或約會等惡意軟體，進行進一步駭侵攻擊。

根據 Cyjax 的報告，Fangxiao 駭侵團體早在 2017 年就開始發動攻擊活動，歷年以來共假冒超過 400 個以上知名品牌，包括可口可樂、麥當勞、Knorr、Uniliver、Shopee、Emirates 等，領域遍及零售、銀行與金融服務、旅遊、醫療、運輸、財經、能源等部門。

Cyjax 指出，自 2022 年 3 月起，Fangxiao 駭侵團體至少使用 24,000 個以上網域，用來放置各種 Landing 網頁與問卷調查，以高額獎賞為誘餌，誘使用戶上當而連入該詐騙網域。

Cyjax 也指出，該駭侵團體多數用來發動詐騙攻擊的網域，都使用如 .top、.cn、.cyou、.xyz、.work、.tech 等頂級網域；這些網域多半在 GoDaddy、NameCheap 和 Wix 註冊，並透過 Cloudflare 來隱藏。

為了產生大量連往其詐騙網站流量，Fangxiao 每天約註冊 300 個全新的詐騙網域。而為避免用戶感覺異常，這些問卷都還有限時回答計時器，以讓受害者專注於回答問題而放鬆警戒。

Cyjax 也發現 Fangxiao 在一個上架於 Google Play Store 中的 App「Booster Lite - RAM Booster」中放置詐騙網站的廣告；該 App 已被下載超過 1000 萬次。

建議用戶在瀏覽網站或使用內置廣告的 App 時，必須對於提供不正常高額獎賞的廣告提高警覺；若打著知名品牌旗號，最好到其官網或官方社群帳號查詢，該活動是否確實由官方舉辦，勿輕易點擊並參加活動。

- 資料來源：
  1. Fangxiao: a Chinese threat actor
  2. 42,000 sites used to trap users in brand impersonation scheme

4.6.3、趨勢科技發現 APT 團體 Earth Preta (Mustang Panda) 針對多國目標發動魚叉式釣魚攻擊

資安廠商趨勢科技（Trend Micro）日前發表研究報告，指出 APT 團體 Earth Preta（又名 Mustang Panda），近期針對多個國家的政府、教育、研究機構等特定目標發動魚叉式釣魚攻擊。

根據趨勢科技的報告指出，受到攻擊的國家遍及世界各國，但以亞太地區為主，受害最嚴重的國家包括緬甸、澳洲、菲律賓、日本、台灣等。

趨勢科技的報告說，Earth Preta 使用假的 Google 帳號寄送魚叉式釣魚信件，來散布惡意軟體；這些惡意軟體會以郵件中的 Google 文件連結來放置，而郵件中宣稱夾有自不明處竊得的「機密」或「秘密」內容文件，以此吸引潛在受害者開啟含有 TONEINS、TONESHELL、PUBLOAD 等惡意軟體的連結。

受害者一旦開啟這些文件，惡意軟體就會透過一種稱為 DLL side-loading 的技術，暗中植入電腦背景運作，接著進一步下載更多惡意軟體酬載。

報告指出，Earth Preta 利用這些惡意軟體進行網路監控，並且自受害者電腦中竊取更多機密文件，並用於日後針對不同對象的魚叉式釣魚攻擊之上。

在趨勢科技觀測到的 597 個案例中，有高達 83.90% 的案例針對政府機關與司法單位進行攻擊，針對教育單位的攻擊案例佔 6.90%，針對商業經濟組織的有 6.20%、政治組織的有 2.20%，其他的為 0.80%。

為避免遭到駭侵團體以魚叉式釣魚攻擊鎖定特定人士，各公私單位中重要的高風險對象，建議應加強資安意識與訓練，切勿任意開啟不明電子郵件或點按不明連結，以免重要情報或資訊遭到竊取，甚至危及人身安全。

- 資料來源：
  1. Chinese 'Mustang Panda' Hackers Actively Targeting Governments Worldwide
  2. Earth Preta Spear-Phishing Governments Worldwide

4.6.4、LockBit 勒贖團體宣稱攻擊德國汽車用品大廠 Continental

LockBit 勒贖攻擊團體日前宣稱，該團體對德國知名的跨國汽車用品製造大廠 Continental （在台灣的品牌名稱為「馬牌」）發動勒贖攻擊，並且竊取其機敏資訊。

LockBit 勒贖團體並在其網站中公開一部分竊自 Continental 的資料，並威脅該公司若不在 22 小時內同意該團體的要求，就要公開所有竊得的資料。

Continental 的公關行銷副總裁 Kathryn Blackwell 在接受資安專業媒體 BleepingComputer 採訪時，並未證實該公司是否遭到 LockBit 團體的勒贖攻擊，也沒有透露該公司是否已與 LockBit 接觸。

Continental 曾在 2022 年 8 月 24 日發表新聞稿，指出該公司的 IT 系統遭到資安攻擊且被成功入侵；該公司於 8 月初發現遭駭侵攻擊後，立即採取應變措施，除即刻恢復正常運作外，也與外部資安專家合作調查案情始末。該公司的生產並未受阻，IT 系統也並未受損。

不過時至今日，該公司仍未提供 8 月駭侵攻擊事件的具體說明，也未證實此次駭侵事件與 8 月時的駭侵攻擊事件是否有關。該公司也拒絕提供這次遭 LockBit 駭侵事件的任何情資。

不過資安專家指出，由 LockBit 在網頁上威脅要公開 Continential 資料的做法來研判，Continental 極可能尚未與 LockBit 接觸，或是已拒絕該駭侵團體的要求。

近年來大型企業遭到勒贖攻擊並遭公開資料的案例日漸增加，建議各企業應確實加強資安防護措施與人員教育訓練，以免因系統遭駭而造成生產作業停擺，甚至因資料外洩而蒙受重大損失。

- 資料來源：
  1. Continental Informs – Cyberattack Averted
  2. LockBit ransomware claims attack on Continental automotive giant

4.7、軟硬體漏洞資訊

4.7.1、Google 緊急推送 Chrome 更新，解決一個高危險 0-day 漏洞

Google 日前緊急推送電腦版 Chrome 瀏覽器更新，以修補近期發現的嚴重 0-day 漏洞。已知該漏洞已遭到外界駭侵者大規模濫用於攻擊活動中。

這個 CVE-2022-4135 是存於繪圖處理器（Graphic Processing Unit）的 heap 緩衝記憶體溢位錯誤，由 Google 旗下資安團隊 Threat Analysis Group 發現。一般來說，這類錯誤屬於記憶體漏洞，可讓攻擊者繞過系統限制寫入資料；而這個 CVE-2022-4135 漏洞可以讓攻擊者存取限制區域內的資訊，並遠端執行任意程式碼。

Google 目前沒有明確說明這個漏洞的成因與運作方式；Google 表示等到多數用戶都更新到新版 Chrome 後，才會公開這個漏洞的相關詳細資訊。

Google 也在最近發表的資安通報中指出，該公司已經知道有駭侵攻擊活動利用此 0-day 漏洞發動攻擊。

這個漏洞是 Google Chrome 在 2022 年發現的第 8 個 0-day 漏洞，其餘 7 個 0-day 漏洞分別是 CVE-2022-3723、CVE-2022-3075、CVE-2022-2856、

CVE-2022-2294、CVE-2022-1364、CVE-2022-1096、CVE-2022-0609。

Google 推出的新版 Chorme 瀏覽器，Windows 版本號碼為 107.0.5304.121/122，Mac/Linux 版本則為 107.0.5304.122；這些新版本已修復上述的 CVE-2022-4135 0-day 漏洞，用戶在開啟 Chrome 瀏覽器時應會自動進行更新。

由於 Google Chrome 的市佔率高，用戶使用時應特別留意，如有可用更新，應立即套用，以免遭駭侵者利用未及更新的漏洞發動攻擊。

- CVE 編號：CVE-2022-4135
- 影響產品/版本：107.0.5304.121/122 之前版本。
- 解決方案：更新至 107.0.5304.121/122 或後續版本。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google pushes emergency Chrome update to fix 8th zero-day in 2022

4.7.2、Microsoft 推出 2022 年 11 月 Patch Tuesday 資安修補包

Microsoft 日前推出 2022 年 11 月例行資安更新修補包「Patch Tuesday」，共修復 68 個資安漏洞，其中有 11 個是屬於「嚴重」危險程度的漏洞，另有 6 個 0-day 漏洞已知遭用於駭侵攻擊。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：27 個；
- 資安防護功能略過漏洞：4 個；
- 遠端執行任意程式碼漏洞：16 個；
- 資訊洩露漏洞：11 個；
- 服務阻斷（Denial of Service）漏洞：6 個；
- 假冒詐騙漏洞：3 個。

上述在這次 Patch Tuesday 中獲得修補的漏洞，並未包括兩個於 11 月 2 日公開的 OpenSSL 漏洞。

本月修復的 6 個已遭濫用 0-day 漏洞如下：

- CVE-2022-41128：Windows Scripting Languages 遠端執行任意程式碼漏洞；
- CVE-2022-41091：Windows Mark oof the Web 資安防護功能跳過漏洞；
- CVE-2022-41073：WIndows Print Spooler 權限提升漏洞；
- CVE-2022-41125：Windows CNG Key Isolation Service 權限提升漏洞；
- CVE-2022-41040：Microsoft Exchange Server 權限提升漏洞；
- CVE-2022-41082：Microsoft Exchange Server 遠端執行任意程式碼漏洞。

鑑於 Microsoft 軟體產品眾多，所有用戶與系統管理者應立即套用這次的 Patch Tuesday 資安更新，以免遭駭侵者利用已知的未修補漏洞發動攻擊，造成不必要的損失。

- CVE 編號：CVE-2022-41128 等
- 影響產品/版本：Microsoft 多種軟體產品，詳見其資安通報。
- 解決方案：更新至最新推出的軟體資安更新版本。

- 資料來源：
  1. 安全性更新導覽
  2. Microsoft November 2022 Patch Tuesday fixes 6 exploited zero-days, 68 flaws

4.7.3、駭侵團體利用 Windows 新 0-day 漏洞跳過資安檢查並植入惡意軟體

資安廠商 ANALYGENCE 旗下的資安專家，近來發現一波利用 Windows 最新 0-day 漏洞來跳過 Windows 內建資安防護功能 Mark of the Web (MoTW)，進而在受害系統上植入 Qbot 惡意軟體的攻擊活動。

Mark of the Web 是 Windows 內建的資安防護機制之一，Windows 會針對從網路上下載的檔案，或是 Email 中的夾檔，建立額外的檔案屬性，包括檔案原始出處、推薦者與下載 URL 等資訊。用戶如欲開啟具有 MoTW 的檔案時，Windows 會額外顯示一個警告視窗，詢問用戶是否確實要開啟檔案。

資安專家在分析近期一波利用釣魚郵件散布 Magniber 勒贖軟體的攻擊行動時，發現了該駭侵者利用 Windows 一個新的 0-day 漏洞，防止用戶在開啟含有惡意程式碼的檔案時，看到 Windows 的 MoTW 提醒視窗。

該攻擊手法係利用一個在 Microsoft 支援文件中提到的 base64 編碼簽署區塊，來為惡意軟體的 JavaScript 程式碼檔案進行簽署；如此用戶在開啟惡意檔案時，Windows 就不會顯示 MoTW 警告訊息，而會直接開啟檔案。

資安專家也指出，近期的 QBot 惡意軟體釣魚攻擊，原本利用 ISO 檔格式來放置惡意軟體，這是因為 Windows 不會對 ISO 檔進行 MoTW 附加動

作；但在 2022 年 11 月的 Patch Tuesday 中，Microsoft 修復了這個錯誤，因此駭侵者改使用上述最新的 0-day 漏洞來跳過 MoTW 機制。

據資安媒體 BleepingComputer 指出，Microsoft 在 10 月時已經得知該 0-day 漏洞的存在且遭到多場駭侵攻擊濫用的情形；預計 12 月的 Patch Tuesday 中將可針對此 0-day 漏洞進行修補。

- 解決方案：由於各種軟體與作業系統的 0-day 漏洞難以避免，用戶除應在可更新時立即更新，以修補已知 0-day 漏洞外，不任意點按連結或開啟不明檔案，也能加強自身的資安防護。

- 資料來源：
  1. Will Dormann @wdormann
  2. New attacks use Windows security bypass zero-day to drop malware

4.7.4、多個組織因 Fortinet 嚴重身分認證略過漏洞而遭駭侵攻擊

資安廠商 Cyble 日前發表研究報告，指出該公司的網路掃瞄機制，發現分布全球超過 10 萬台 Fortinet 出品之 FortiGate 防火牆，曝露在一個嚴重身分認證略過漏洞 CVE-2022-40684 的風險之下；目前已傳出有駭侵者利用此一漏洞發動攻擊。

CVE-2022-40684 是一個存於多款 Fortinet 網通產品（如 FortiOS、FortiProxy、FortiSwitchManager）之內的嚴重漏洞，駭侵者可以特製的 HTTP 或 HTTPS 連線要求，來觸發此一錯誤，跳過系統身分認證程序，在管理介面進行各種操作。

Cyble 在報告中進一步指出，駭侵者可以利用這個漏洞，在管理員用戶帳號上新增一個 SSH 金鑰，駭侵者即可以管理者的身分和權限，以 SSH 連入受害系統內，並且攻擊內部網路其他裝置和 IT 環境。

報告中指出，駭侵者可以進行的操作，包括修改管理員的 SSH 金鑰以登入受攻擊系統、新增本機用戶、變更網路設定、更改封包路由、下載系統設定檔、竊取封包以攔截機敏資訊、並將各種設定資訊情報輸出到暗網上販售。

受此漏洞影響的 FortiOS 與 FortiProxy 版本號碼均為 7.0.0 到 7.2.1 的中間各版，FortiSwitchManager 則為 7.2.0 與 7.0.0。

這個漏洞的 CVSS 危險程度評分高達 9.6 分（滿分為 10 分），危險程度分級為最高等級的「嚴重」；Fortinet 原廠已在十月上旬針對 CVE-2022-40684 推出官方版本的更新與暫時處理方案。

建議使用 Fortinet 上述產品的單位，除應立即升級至最新版本，以套用漏洞修補方案外，也應針對內部網路進行網段分割，以防止已入侵的駭侵者進一步攻擊內網其他裝置。

- CVE 編號：CVE-2022-40684
- 影響產品/版本：FortiOS/FortiPproxy：7.2.1、7.2.0、7.0.6、7.0.5、7.0.4、7.0.3、7.0.2、7.0.1、7.0.0；FortiSwitchManager：7.2.0、7.0.0。
- 解決方案：依照 Fortinet 提供的指引，變更部分設定並升級置最新版本。

- 資料來源：
  1. Multiple Organisations Compromised By Critical Authentication Bypass Vulnerability In Fortinet Produ
  2. FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface

第 5 章、 資安研討會及活動

TANET 2022 WORKSHOP PROGRAM -「第二屆數位鑑識、醫療私密與網駭安全」	
活動時間	111 年 12 月 15-17 日 星期四-星期六
活動地點	國立台北商業大學桃園校區
活動網站	https://tanet2022.esam.io/
活動概要	 **主辦單位：TANET** Aim and Scope 本年度首次結合 TANET 與 ICS 兩大年度盛會，臺灣網路網路研討會（Taiwan Academic Network Conference, TANET）每年由各大學輪流舉辦，至今已第二十八屆。TANET 邀請國內資訊相關從業人員於研討會中發表優質論文，提供產官學研資深專家互相交流及經驗分享的平台，對我國資訊學術面及實務面技術的最新發展有相當大的助益。

Jamf Nation Taipei｜2023 全球資安模型 CIO/CISO 高峰會	
活動時間	12/15（四） 14:00 - 16:40
活動地點	華南銀行國際會議中心 201 會議室
活動網站	https://jamf.kktix.cc/events/jamfnation2022
活動概要	 **主辦單位：Jamf Software** 2023 年世界經濟與政治發生變化，商務模式也會隨著轉變。在變動的環境中，Apple 與 Jamf 於全球協助超過 67,000 個組織建立堅韌有彈性 (Resilient) 的 IT 環境，讓企業在面臨重大的變故時，也可維持企業高度的行動力 (Mobility) 。 研討會議程： 場次時間 12/15(四) 14:00-16:40(活動開始前 30 分鐘開放入場) 14:00-14:10 開場分享 - 數位發展部 數位產業署 呂正華 署長 14:10-14:50 景氣挑戰下的企業資安策略 - Apple 企業市場負責人 14:50-15:30 資安架構成功案例分享 - HTC 宏達電、奧義智慧科技 15:30-15:50 休憩時間，享用美味茶點 15:50-16:30 全球成功資安模型解構 - Jamf 亞太地區市場負責人 16:30-16:40 Apple 獎項抽獎

HITCON GIRLS 2022 資安女力專題講座-女性主管經驗談	
活動時間	2022.12.17（六）14:30 - 17:00
活動地點	集思台大會議中心 蘇格拉底廳 - 台北市大安區羅斯福路四段 85 號 B1（近捷運公館站）
活動網站	https://hitcon.kktix.cc/events/hitcongirlsworkexperience2022
活動概要	 **主辦單位：HITCON GIRLS、教育部先進資通安全實務人才培育計畫** 【活動介紹】 沒錯！女性主管經驗談回來囉！ 求職、在職都會有點徬徨對吧？那來聽聽女性主管怎麼說吧！ HITCON GIRLS 與 教育部先進資通安全實務人才培育計畫 聯合主辦第三屆女性主管經驗談分享活動， 我們將會邀請重量級講師 【活動資訊】 活動名稱：資安女力專題講座-女性主管經驗談

	指導單位：教育部資訊及科技教育司 主辦單位：HITCON GIRLS、教育部先進資通安全實務人才培育計畫 參與方式：索取免費現場票券 活動日期：2022.12.17（六）14:30 - 17:00 報到時間：14：00 - 14：30 活動地點：集思台大會議中心 蘇格拉底廳 - 台北市大安區羅斯福路四段 85 號 B1（近捷運公館站） 【活動時程表】 14:00 - 14:30 講師、與會者報到入場 14:30 - 14:50 活動開場（HITCON GIRLS Turkey & Hazel 共同創辦人 、中央大學 資訊工程學系 林家瑜 教授） 14:50 - 15:50 女性主管經驗談（一）林佩靜 國泰金控 副總經理 - 經營自己的專業 15:50 - 16:10 休息時間 16:10 - 16:40 女性主管經驗談（二）林雅芳 Google 台灣總經理 - 學習、歸零、再學習，成為一個「不怕迷路」的人 16:40 - 17:00 講師聯合座談 Panel Discussion（林佩靜 副總經理、林雅芳 總經理、林家瑜 教授）

幣圈資安必備知識，如何安全投資加密貨幣？	
活動時間	2022/12/18 (日) 15:00-17:00
活動地點	台北市松山區延壽街 330 巷 7 弄 3 號 （ACE 台北門市）
活動網站	https://www.accupass.com/event/22120106380416167461 26
活動概要	 **主辦單位：Asia Blockchain Media (ABM)** 過去在投資加密貨幣時，大多數人皆以方便操作及量化工具使用為主，進而將過多資產放置在中心化交易所，導致這次破產事件多人受害，對投資加密貨幣喪失信心，究竟該如何避免多年辛苦累積的資產，一夕之間不見，增強安全防護程度，你絕對不能錯過這堂課！ 【透過這堂課你將學到】 1.瞭解區塊鏈加密原理 2.選取最適合自己的資產保護方式 3.破解迷思，學會判斷 【活動議程】 14:30-15:00 進場報到 15:30-16:50 如何安全投資加密貨幣

	16:50-17:00 會後交流 QA 時間：2022/12/18 (日) 15:00-17:00 （14:30 開放報到） 活動地點：台北市松山區延壽街 330 巷 7 弄 3 號 （ACE 台北門市）

VMware 週三線上講堂 VMware 深化容器安全，輕鬆攔阻複雜攻擊行為	
活動時間	12/21(三)14:00
活動地點	線上
活動網站	https://event.ithome.com.tw/live/vm221221/index.html?utm_source=edm&utm_medium=itweb&utm_campaign=vmware
活動概要	 **主辦單位：** VMware 週三線上講堂 VMware 深化容器安全，輕鬆攔阻複雜攻擊行為 在數位轉型浪潮席捲下，許多企業發現自己的應用架構已經過時，與專家倡議的敏捷、原雲生、微服務等概念，完全不在同一個世界，因而大刀闊斧推動應用現代化改造。讓不少開發、IT 維運人員，連帶積極擁抱容器或 Kubernetes 技術，從原本的生澀無知、一知半解，到現在的駕輕就熟，逐漸成為工作日常的一部份。 然而隨著研究人員發現到的容器漏洞越來越多，安全事件的發生

	頻率也越來越高，不禁讓開發人員、IT 維運乃至資安人員深感惶恐，只因為容器資安風險似乎比預期來得多，舉凡安全漏洞、設定錯誤、映像檔感染等等，都會留給駭客可乘之機。更麻煩的是，從容器應用開發、部署到運行環境，每一個環節都可能出現安全破口，需要防禦的範圍既廣且深，難免掛一漏萬、顧此失彼。 有感於容器安全已成為當前棘手議題，VMware 將於 12 月 21 日舉辦「VMware 週三線上講堂 ─ VMware 深化容器安全，輕鬆攔阻複雜攻擊行為」，深入剖析容器環境可能遭遇的資安威脅與挑戰，並闡述 VMware 如何深化容器安全解決方案，進而伴隨著容器的生命週期，自始至終層層把關，讓所有的弱點或錯誤設定，都在容器應用上線前消理殆盡。關心容器安全風險影響業務靈活性與上市速度的您，請務必報名參加！ 活動資訊： 免費參加，請事先完成線上報名 洽詢專線：(02)2562-2880 分機 3631 VMware 活動小組

滲透測試應用實務班	
活動時間	112 年 1/7-1/8，週六日白天 9:00 ~12:00,13:00~17:00 ，共 2 天、計 14 小時。報名截止日：2023/01/05
活動地點	工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準!
活動網站	https://college.itri.org.tw/Home/LessonData/950E70E8-322D-44B3-AB67-8075E84A45C6
活動概要	 **主辦單位：工業技術研究院** 近年來駭客透過應用系統與軟體的漏洞所造成之資安事件層出不窮，軟體開發/管理人員面對資安事件應盡速應變並從安全軟體開發強化產品安全性。軟體開發/管理人員透過了解攻擊原理與步驟，進而可辨識惡意攻擊行為。 本課程設計除透過瞭解資訊安全所面臨之風險與處理方法，駭客可能之攻擊手法，藉以學習如何採取相對應之控制措施之外，並由滲透測試與資安偵測與監控之實務操作，讓學員學習到有效的資安防禦實務! 課程特色/目標 ➢ 了解網頁/系統應用程式攻擊流程以及資安檢測相關技巧。 ➢ 理解駭客攻擊思維並具備資安攻防實務技巧。 ➢ 掌握資安事故，並熟悉既有資安應變措施。

	課程對象 ➢ 資安管理人員、OT(Operation Technology) 維運人員 ➢ 系統管理人員、網路管理人員 ➢ 資安 (訊) 主管 課程注意事項：請學員自備筆電上課 課程大綱 ➢ 環境工具介紹。 ➢ 資訊蒐集：此部分將介紹如何蒐集滲透目標對象的服務版本及系統相關資訊。 ➢ 漏洞偵測與利用：此部分將介紹如何針對滲透目標對象的可能存在之 CVE 或其他常見漏洞進行偵測及利用該漏洞進行攻擊。 ➢ 後門植入及提權攻擊：此部分介紹駭客如何利用各類後門程式對滲透目標對象建立遠端控制及如何進一步提權。 ➢ 實際案例介紹：從我國近期油品事業遭勒索病毒案、政府機關遭入侵滲透案中研析駭客進行滲透之手法，提供學員進行反思。

第 6 章、 TVN 漏洞公告

科風 UPSMON PRO - Broken Authentication	
TVN / CVE ID	TVN-202208004 / CVE-2022-38119
CVSS	9.8 (Critical)
影響產品	科風 UPSMON PRO v2.57
問題描述	UPSMON PRO 服務網址未進行身份驗證，遠端攻擊者不須帳號密碼進行登入，輸入已知服務網址繞過身份認證機制，即可使用管理者功能，藉以控制系統或中斷服務。
解決方法	聯繫科風進行版本更新
公開日期	2022-11-10
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6678-e9fbe-3.html

華苓科技 Agentflow BPM 企業流程管理系統 - Arbitrary File Upload	
TVN / CVE ID	TVN-202210010 / CVE-2022-39036
CVSS	9.8 (Critical)
影響產品	華苓科技 Agentflow BPM V.4.0.0.1183.552
問題描述	Agentflow BPM 檔案上傳功能未過濾 URL 參數中的特殊字元，遠端攻擊者不須登入即可上傳任意類型的檔案，並執行任意程式碼，藉以控制系統或中斷服務。
解決方法	參考華苓科技官方說明進行版本更新
公開日期	2022-11-10
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6682-21207-3.html

華苓科技 Agentflow BPM 企業流程管理系統 - Broken Access Control	
TVN / CVE ID	TVN-202210012 / CVE-2022-39038
CVSS	8.8 (High)
影響產品	華苓科技 Agentflow BPM V.4.0.0.1183.552
問題描述	Agentflow BPM 企業流程管理系統之文件表單功能未進行適當的權限控管，遠端攻擊者以一般使用者權限登入後，變更使用者名稱即可登入任意帳號，控制系統或中斷服務。
解決方法	參考華苓科技官方說明進行版本更新
公開日期	2022-11-10
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6684-53149-3.html

村榮資訊 雷電 MAILD Mail Server -- Formula Injection	
TVN / CVE ID	TVN-202211001 / CVE-2022-41675
CVSS	8.0 (High)
影響產品	村榮資訊 雷電 MAILD Mail Server v4.7
問題描述	雷電 MAILD Mail Server 網站的表單匯出功能未檢查所匯出的 CSV 檔案內容，遠端攻擊者以一般使用者權限登入後，可以將惡意程式注入到表單中，當其他使用者下載表單時，會取得惡意的 CSV 檔案，觸發任意程式碼執行，並對系統進行任意操作或中斷服務。
解決方法	更新版本至 v4.7.4 以上
公開日期	2022-11-29
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6738-b78f4-3.html

科風 UPSMON PRO - Cleartext Transmission of Sensitive Information	
TVN / CVE ID	TVN-202208007 / CVE-2022-38122
CVSS	7.5 (High)
影響產品	科風 UPSMON PRO v2.57
問題描述	UPSMON PRO 使用 HTTP 傳輸協定，以明文的方式進行傳輸，未經授權的遠端攻擊者，可以利用此漏洞取得敏感資訊。
解決方法	聯繫科風進行版本更新
公開日期	2022-11-10
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6681-e9650-3.html**

第 7 章、 2022 年 11 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

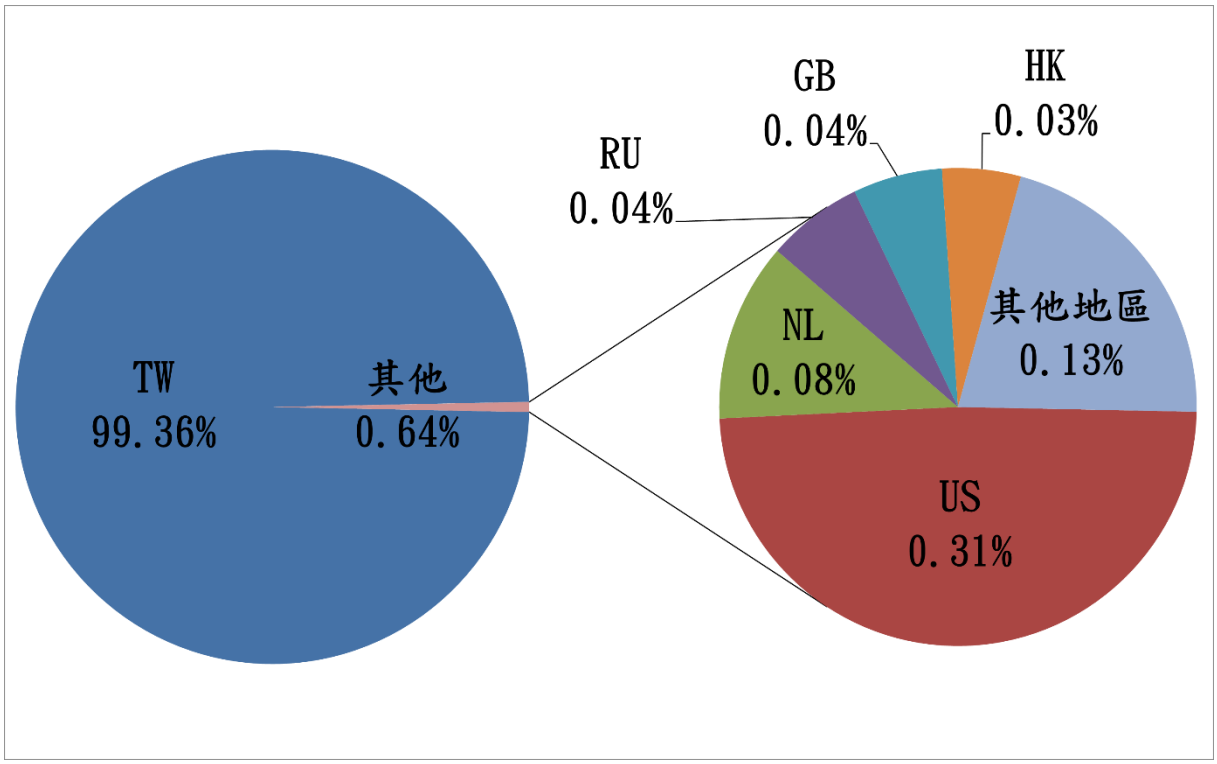


圖 1、分享地區統計圖

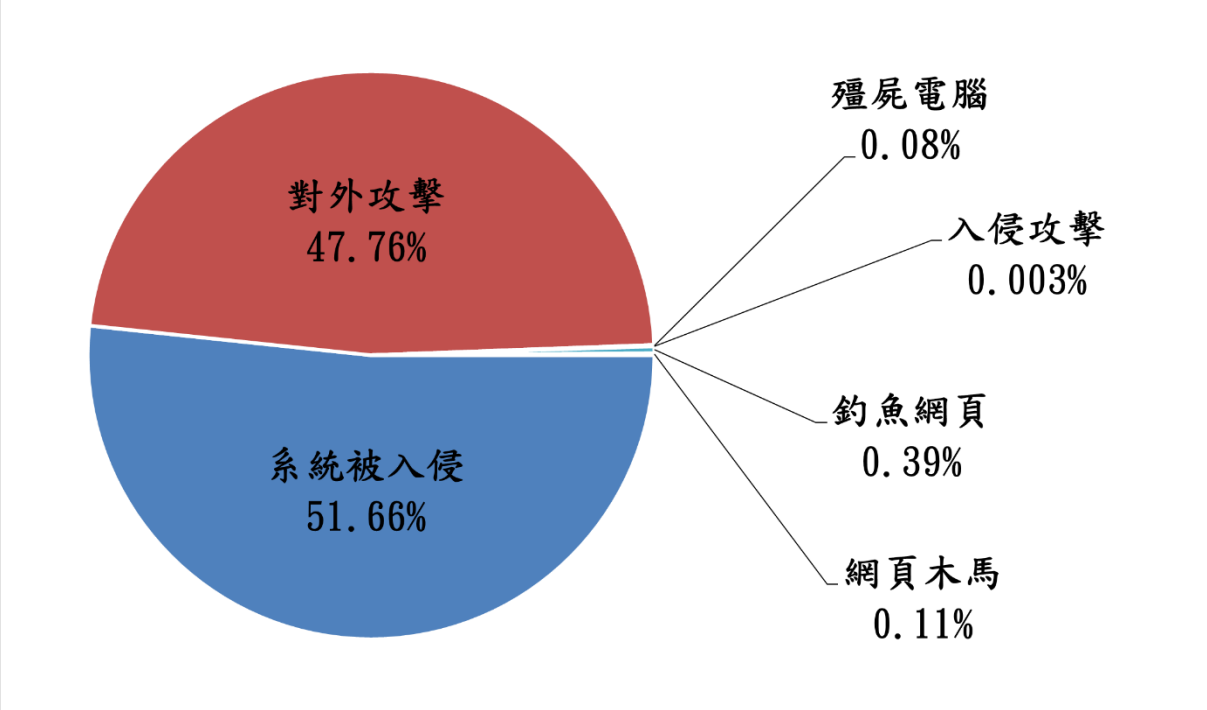


圖 2、分享類型統計圖

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 12 月 9 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**