TWCERT/CC 資安情資電子報

2022 年 9 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 8 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、資訊安全宣導：針對近期資安議題、TWCERT/CC 服務或配合政府資安政策等進行資安宣導，以提升大眾資安意識。

第 4 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 5 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 6 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 7 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 8 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

分散式阻斷服務攻擊(DDoS)趨勢與防護

- 分散式阻斷服務 (Distributed Denial-of-Service, DDoS)攻擊，是一種由攻擊者利用受操控的大量殭屍網路裝置，對企業伺服器進行頻寬或資源難以負荷之攻擊，導致企業無法順利提供服務之攻擊型態。
- DDoS 攻擊可分為頻寬消耗與資源消耗兩種類型攻擊，雖其針對的目標及執行之手段不盡相同，但所欲造成之影響結果，同樣是讓企業無法提供合法使用者獲得服務。
- 根據統計，2022 年每一季之 DDoS 攻擊數量都比 2021 年來得高，這也顯示不論是企業、組織，甚至資安單位都應開始將 DDoS 攻擊之防禦納入優先需求，以避免在 DDoS 攻擊數量漸增的情況下，遭受攻擊而產生嚴重損失。
- 隨著國內資通設備數量的大量增長，導致國內不論是企業受到 DDoS 攻擊，亦或被操控作為殭屍網路攻擊他國，都時有所聞。因此，如何防範 DDoS 攻擊，將是所有企業及組織迫在眉睫之營運需求。
- 為避免因 DDoS 攻擊而蒙受損失，有諸多產品及服務可供企業安裝及使用，並且可針對各種不同類型之 DDoS 攻擊，透過有效且精確之過濾機制，以及專業之防護服務，達成大幅降低 DDoS 攻擊之影響結果。

一、簡介

分散式阻斷服務(Distributed Denial-of-Service, DDoS)攻擊，是阻斷服務(Denial-of-Service, DoS)攻擊的進階版，駭客發送大量的網路封包或服務請求，使得受害系統主機因網路頻寬超出負荷或耗盡資源而癱瘓，無法提供正常服務。

DDoS 攻擊所欲達成影響結果之模式，主要可分為頻寬消耗及資源消耗兩種攻擊類型[1]：

1. 頻寬消耗型攻擊：此類型 DDoS 攻擊主要是攻擊者會透過傳送大量無效、甚至惡意放大流量的服務請求給受害主機或伺服器，而這些大量的無用請求，會使得主機或伺服器的網路頻寬壅塞，導致一般正常使用者無法順利登入或連線，產生該主機或伺服器癱瘓之後果。

2. 資源消耗型攻擊：此類型 DDoS 攻擊主要是針對受害主機或伺服器本身提供一般使用者服務的資源，攻擊者會透過大量的服務請求，但不讓服務請求完成，而是讓受害主機或伺服器不斷重複這些無效的行為，導致主機或伺服器資源都被用來處理攻擊者的大量無效請求，已無多餘資源可回應一般使用者的請求。

DDoS 攻擊類型，又可細分為多種不同的攻擊模式。頻寬消耗型攻擊的手法眾多，並且大多為透過特殊協定產生之放大攻擊，包括[2][3]：

1. Memcached 放大攻擊：Memcached 是一種分散式之高速資料庫緩衝系統，提供高效率存取及高擴展性，許多企業及網站都已使用以提供更佳的使用者體驗。但此系統本身缺乏認證及安全管理機制，因此容易被攻擊者操控為進行 DDoS 攻擊的利器。攻擊者首先會將大量數據植入暴露於網際網路中的 Memcached 伺服器中，並且偽裝成受害主機之身份，對 Memcached 伺服器進

行請求，而被植入大量資料的 Memcached 伺服器便會將這些資料依據請求傳送給受害主機。大量的資料傳輸除了該受害主機外，亦可能造成其周圍的網路節點無法順利處理，導致受害主機無法順利收到一般使用者的正常請求並回應。此種攻擊之放大係數為 10,000 至 51,000，為所有 DDoS 放大攻擊中放大倍率最高者。

2. NTP 放大攻擊：網路時間協定(Network Time Protocol, NTP)是一種允許主機之間透過封包交換進行系統時間同步之網路協定。但在 NTP 協定中，有一個 monlist 指令，當 NTP 伺服器收到 monlist 請求後，會回傳多筆近期與之通訊的列表，該列表最高限制為 600 筆。而攻擊者便可利用此機制，以偽裝之 IP 位址寄送 monlist 請求給 NTP 伺服器，則 NTP 伺服器便會將至多 600 筆之數據傳送給遭攻擊者偽冒的 IP 位址，導致遭偽冒之受害主機因一次大量的數據傳輸，造成其網路頻寬無法負荷，致使受害伺服器無法正常提供服務。此種攻擊之放大係數為 556.9，為所有 DDoS 放大攻擊中放大倍率次高者。

3. DNS 放大攻擊：在某些特殊的請求中，DNS 伺服器會回應比請求封包更大的封包給請求發起方。而攻擊者便可利用此機制，偽裝成受害主機的身份，向 DNS 伺服器發起放大封包的請求，並且讓 DNS 伺服器回傳大量的放大封包給受害主機，導致受害主機頻寬因此壅塞，致使一般使用者無法順利連線。此種攻擊手法相當常見，其放大倍率為 28 至 54。

DDoS 的攻擊模式，除了上述之頻寬消耗型攻擊外，亦有針對伺服器資源之資源消耗型攻擊，其攻擊模式包括[2]：

1. SYN Flood 攻擊：此種攻擊主要是透過 TCP 連線之三向交握時，伺服器端在收到 SYN 封包後，便會回應請求端並保留一通信埠提供請求端連線之用，並

在收到請求端確認的 ACK 訊息後開始後續連線作業。然而，攻擊者卻利用此機制，傳送偽冒來源 IP 位址之 SYN 請求封包給受害伺服器，而受害伺服器會回應給偽冒 IP 位址並且保留連接埠，然而，在伺服器等待回應的期間，攻擊者仍會大量持續傳送 SYN 請求封包，且這些封包的偽冒來源 IP 讓伺服器無法順利收到回覆，導致其連接埠逐漸因 SYN 請求而分配完畢，因而產生無其他連接埠可供一般使用者使用了。

2. 應用層 DDoS 攻擊：應用層為提供使用者完整的服務，伺服器回應請求時所進行的動作也會較其他層來得更多，因此需要消耗更多資源，例如使用者一個簡單的網頁存取請求，伺服器就必須先進行資料庫的查詢、API 的調動，才能生成網頁，甚至可能還需驗證請求端的憑證，其所需耗費的資源較請求端超出許多。因此，攻擊者便可透過此機制，以殭屍網路大量傳送應用層之請求封包給受害伺服器，導致受害伺服器不堪負荷而中斷正常的服務。

3. 低速緩慢攻擊(Low and Slow Attack)：此種攻擊主要是透過相當冗長的請求過程，佔據受害伺服器之服務資源，拉長服務時間，卻又保持其速率不讓連線超時，使得受害伺服器無法對一般使用者提供服務。低速緩慢攻擊所需之頻寬較小，且難以與一般流量區分，相較於大規模流量之 DDoS 攻擊，此種攻擊不容易被發現，卻仍會導致受害伺服器服務被拖慢，進而產生服務中斷之問題。

根據上述六種攻擊手法，雖攻擊者所利用之工具或協定不盡相同，但均會造成受害主機或伺服器無法負荷，使得服務中斷，嚴重影響企業運行。

二、分散式阻斷服務攻擊案例

隨著個人電腦、行動裝置，甚至物聯網裝置的數量大量增長，攻擊者在植入惡意程式後可操縱的設備數量大量增加，雖然越來越多的伺服器或主機所能承載流量負荷的能力也越來越大，但仍趕不及攻擊者傳送惡意大量封包的增長速度，因此 DDoS 攻擊之資安事件仍常有所聞。而該類型之攻擊手法常見於國際之資安事件，在國內發生之案例亦不少，除了國內企業或組織遭受 DDoS 的攻擊外，亦有許多為國內防護不足之設備遭攻擊者利用，藉以作為跳板攻擊其他企業或國家。依上述，就國內外相關重大案例彙整如下：

國內企業/組織遭受 DDoS 攻擊案例

1. 國內政府機關遭 Op Taiwan 活動之 Anonymous Asia DDoS 攻擊[7][8]：

在 2015 年 7 月，當時對於學生課綱之相關爭議不斷，導致許多大小不一抗爭活動持續延燒，而當時駭客組織 Anonymous Asia 在 Facebook 專頁表態支持反課綱學生，並且透過 DDoS 方式陸續攻擊我國諸多政府機關以及相關民間組織。此次攻擊活動被命名為 Op Taiwan，且 Anonymous Asia 除了國內成員外，同時也號召菲律賓、加拿大、香港、中國大陸及美國等各地匿名者團體，於 2015 年 8 月 1 日針對我國政府機關及相關組織共同發動 DDoS 攻擊。在遭受攻擊的一週期間，各機關陸續採取阻擋攻擊來源、新增阻擋設備及限制頻寬等措施，以緩解攻擊產生之影響；同時藉由網際網路接取服務業者獲得通報單位處理國內攻擊來源，以及透過 TWCERT/CC 針對他國攻擊來源進行通報及處理。此次事件，Anonymous Asia 宣稱其已經成功攻擊 14 個政府機關以及數間民間組織，所幸此次攻擊並未造成嚴重損失及後果。

2. 國內多家券商遭 DDoS 攻擊勒索虛擬貨幣[9]：

在 2017 年 2 月，國內逾十間證券公司收到署名為 Armada Collective 寄送之勒索信件，威脅要求該證券公司支付七至十個比特幣，以當時市價換算，約為新臺幣 27 至 30 萬元，否則便會進行 DDoS 攻擊癱瘓這些證券公司之網

站。實際上，在一月底股市休市沒多久，便出現了零星災情，在開春交易首日更出現達 800Mbps 之攻擊流量，而攻擊者揚言此僅為試探性攻擊，如若證券公司不支付款項，便會在四天後之 2 月 7 日發動 TB 等級之攻擊。金管會立即出面協調 NCC、國內三家網際網路接取服務業者以及行政院資安處，嚴密監控相關網際網路流量，預前防範以降底可能的損害風險。在預告日的前一天，證券公司出現第二波災情，一直持續至預告當日，另有三家證券公司成為 DDoS 新的攻擊受害者，所幸當日並未出現攻擊者預告之 TB 級攻擊，最大僅出現 GB 等級攻擊，並且大多數證券公司在受到攻擊後，於半小時內便都恢復正常運作，並未產生嚴重的損失。雖然此次攻擊未出現嚴重的受害者，但也顯示著新興勒索攻擊的出現，讓 DDoS 攻擊成為企業所需防堵的主要目標之一。

3. 國內多家主機代管商遭大規模 DDoS 攻擊使得網站服務遭受影響[10]：

在 2020 年 9 月，國內多家主機代管商遭到大規模之 DDoS 攻擊，最早出現於 9 月 19 日傍晚，第一家受害廠商於其官網中證實遭受攻擊，並且攻擊狀況於隔日開始逐漸增長，一天內就有遭遇三波攻擊的情形，每次持續約 1 至 2 小時，導致諸多網站服務受到影響。但此次攻擊事件尚未結束，另有兩間廠商分別在 22 日及 23 日於其 Facebook 粉絲專頁中表示公司正遭受嚴重 DDoS 攻擊。此次攻擊較為特殊之處，是攻擊來源之 IP 位址均來自於國內，因此許多針對國外 IP 位址進行 DDoS 防護之機制無法涵蓋。尤其此次攻擊來源 IP 位址多為視訊監控錄影主機(Digital Video Recorder, DVR)，而當時大部分 DVR 設備多為使用弱密碼及開啟 Telnet 服務之設備，使得攻擊者入侵難度大幅降低，易於遭駭成為殭屍網路之設備。

物聯網裝置/設備遭利用對境外進行 DDoS 攻擊

1. 大量網路攝影機遭駭以對他國網路公司進行 DDoS 攻擊[11][12]：

在 2016 年 10 月，美國網路效能管理公司 Dyn 遭到極為大量之 DDoS 攻

擊，此事件主要是由受 Mirai 惡意程式感染之殭屍網路進行攻擊，涉及數千萬個 IP 位址，其攻擊流量最高達到 1.2 Tbps，成為 DDoS 攻擊歷史中，數一數二大規模之攻擊事件。在攻擊期間，使用 Dyn 域名服務之諸多網站，如 Twitter、Amazon、Spotify、Netflix 以及華爾街日報等知名網站，都無法順利提供服務。同時，也導致 Dyn 總計有 8%客戶被迫暫停服務。在此事件中，殭屍網路主要由逾五十萬台的網路攝影機所組成，然而，在其中卻有為數不少的網路攝影機之 IP 位址來自國內。其原因為這些網路攝影機提供 Telnet 連網功能，加上預設帳號密碼並未強制要求使用者修改，導致攻擊者得以透過遠端操縱這些網路攝影機，進行此次極大流量之 DDoS 攻擊。

2. 大量裝置遭用以對他國金融機構進行 DDoS 攻擊[13][14]：

在 2016 年 11 月，俄羅斯 5 間銀行遭到大量 DDoS 攻擊，這 5 間銀行分別於不同時間點遭受攻擊，平均攻擊時間為 1 小時，最長的攻擊則持續了 12 個小時之久。根據統計，此次事件中，攻擊者是透過遭受特定惡意程式感染之殭屍網路進行攻擊，這些殭屍網路包含逾 2 萬 4 千台以上不同的設備，並且在這些大量的殭屍網路設備中，有一半以上的設備來自美國、台灣、印度及以色列，其中一部份為使用弱密碼之物聯網裝置，顯示諸多使用弱密碼的裝置，早已成為攻擊者利用的工具而不自覺。DDoS 攻擊可利用的設備數量也隨之增加，雖然許多企業的伺服器能提供的資源也大幅增長，但在攻擊類型及流量都急劇成長的情況下，仍然難以在短時間內負荷攻擊者所帶來的惡意流量，因此仍造成受 DDoS 攻擊的企業，其服務仍會產生中斷之現象。

隨著網路設備的種類和數量不斷增加，攻擊者進行 DDoS 攻擊可利用的設備數量也隨之增加，雖然許多企業的伺服器能提供的資源也大幅增長，但在攻擊類型及流量都急劇成長的情況下，仍然難以在短時間內負荷攻擊者所帶來的惡意流量，因此仍造成受 DDoS 攻擊的企業，其服務仍會產生中斷之現象。

為避免 DDoS 攻擊造成企業的服務中斷，除了增加伺服器所能提供之資

源外，應針對異常大流量封包進行過濾及時防堵，以降低中斷服務及流失客戶之風險。

三、分散式阻斷服務攻擊之防護

為避免企業因遭受 DDoS 攻擊而對其服務產生嚴重影響，企業應設立相關防護機制及設備，從最初的異常流量偵測、流量分析，以及後續的攻擊處理及回應等，都是為防禦 DDoS 攻擊應建立之系統，使企業在不影響正常流量的情況下阻絕惡意流量的攻擊，方能維持企業系統順利運行。而針對 DDoS 攻擊之頻寬消耗和資源消耗兩種類型，其所需之系統、設備及機制卻不盡相同，因此，彙整兩種類型之 DDoS 攻擊所需防護相關工具如下[15]：

1. 頻寬消耗 DDoS 攻擊：

- 交換器(Switch)：大部分的交換器都具有速率限制以及存取控制(Access Control List, ACL)機制，能控制欲流入伺服器之流量，進行相關限制，避免網際網路頻寬無法負荷。甚至有些交換器還提供如過濾有問題封包之 Bogon Filter 與 Deep Packet Inspection，可針對諸多如偽冒他人 IP 位址之 Memcached DDoS 攻擊、NTP DDoS 攻擊，以及 DNS 放大攻擊等進行初步辨識及過濾。
- 路由器(Router)：大部分的路由器都具有速率限制以及存取控制(ACL)機制，避免突然湧入的大流量封包造成服務中斷。並且可啟用入口過濾(Ingress Filtering)機制，針對封包之來源 IP 位址進行檢測和過濾，避免偽造 IP 位址之 Memcached DDoS 攻擊、NTP DDoS 攻擊，以及 DNS 放大攻擊。
- 網路流量清洗(Flow Cleaning)：為了能在不影響企業資源的情況下阻擋

惡意流量，企業可將大量的流量導入清洗中心(Cleaning Center)進行分析和隔離。流量清洗服務主要有：常駐防禦及動態防禦兩種，前者將企業所有流量一律導入清洗中心全時進行分析，後者則是平常不做流量導入，一旦偵知有攻擊發生時，立即機動將流量導入進行分析。清洗中心在收到流量後，會透過其監測設備和防護系統，將合法流量及惡意流量區隔，再導回企業本身提供服務。此種防護機制，其所能防護之 DDoS 攻擊種類，主要由提供服務之廠商所建立之設備和機制所定，目前大多數服務商已可針對 Memcached DDoS 攻擊、NTP DDoS 攻擊，以及 DNS 放大攻擊等提供清洗防護。

2. 資源消耗 DDoS 攻擊：

- 防火牆(Firewall)：防火牆為系統最基本之防護工具，並且隨著防火牆防護類型及準確性的提升，管理員除了設定可阻擋特定網路協定、Port 及 IP 位址等資訊外，甚至有許多防火牆能透過大數據或人工智慧模式，辨別網際網路流量是否異常，並且針對異常流量進行阻擋和示警，以便在不影響正常合法流量通過的情況下，有效阻絕 DDoS 攻擊。防火牆主要可針對資源消耗類型之 DDoS 攻擊，例如 SYN Flood 攻擊及應用層 DDoS 攻擊等類型，透過辨識流量內之攻擊封包並進行隔絕，以達成降低 DDoS 攻擊威脅之目的。
- 交換器(Switch)：大部分的交換器都具有速率限制以及存取控制(Access Control List, ACL)機制，亦可針對封包延遲進行 Traffic Shaping 機制，能防範低速緩慢攻擊與 SYN Flood 攻擊；同時，交換器也有針

對應用層惡意請求造成之應用層 DDoS 攻擊防禦之 Delay Binding 功能，得以在第一時間偵測惡意封包並進行相對應之防護。

- 路由器(Router)：具有速率限制以及存取控制(ACL)機制，並且可啟用入口過濾(Ingress Filtering)機制，針對封包中來源 IP 位址進行檢測和過濾，避免偽造 IP 位址之 SYN Flood 等攻擊。
- 入侵防禦系統(Intrusion-Prevention Systems, IPS)：入侵防禦系統主要是透過特殊特徵比對，對異常流量進行阻擋及防護之系統。可針對特殊性質以及特定通訊協定方式之 DDoS 攻擊，例如 SYN Flood 及應用層 DDoS 攻擊等進行防護
- 網路流量清洗(Flow Cleaning)：其所能防護之 DDoS 攻擊種類，雖主要需由提供服務之廠商所建立之設備和機制所定，但大多數提供流量清洗之廠商，都可針對大部分常見 DDoS 攻擊進行防護，包括 SYN Flood 攻擊、應用層 DDoS 攻擊及低速緩慢攻擊等類型，以提供客戶完整、乾淨的網路環境。

綜上所述，DDoS 攻擊已成為攻擊者最常使用的攻擊手段之一，企業為避免在遭受 DDoS 攻擊後蒙受嚴重損失，必須建置相關防護系統和設備，以利在攻擊事件發生第一時間察覺並有效防制，減少攻擊所帶來之影響。隨著 DDoS 攻擊所能利用之裝置及手法類型越來越多樣化，雖然企業可自行建置防禦設備和機制，但其防禦效果如何仍存有疑慮。因此，許多國內廠商紛紛推出針對 DDoS 攻擊之防禦服務，全方位協助企業從裝置的選擇、安裝，到即時監控以及事件處理等工作，讓企業得以建立更為完善之 DDoS 攻擊防護系統與機制，可參考表 1：國內企業 DDoS 防禦服務彙整表。

表 1：國內企業 DDoS 防禦服務彙整

企業	頻寬消耗 DDoS	資源消耗 DDoS
台灣大哥大	骨幹網路端過濾攻擊，避免頻寬壅塞。	建置多層次清洗設備提供服務，針對網路第三、四及第七層可進行深度分析過濾。
中華電信	HiNet 骨幹網路建置 DDoS 攻擊防禦設備，緩解 DDoS 造成企業頻寬壅塞。	具有多層次 DDoS 防護機制，透過攻擊封包分析及主動偵測防護機制，有效阻擋 DDoS 攻擊。
戰國策集團	基礎設施保護，保護關鍵基礎設施防堵基於協議的 DDoS 攻擊，諸如透過 DNS 進行流量放大之攻擊。	Web 應用程序防護是基於雲的 DDoS 防護服務，是建立在內容傳遞網路 (Content Delivery Network, CDN)的防火牆，自動偵測 DDoS 攻擊，以保護網站和 Web 應用程式的安全性。
遠傳電信	流量清洗服務，透過其過濾機制區分合法與惡意流量，即時攔阻惡意流量，僅讓合法流量通過傳入企業端。	Anti-DDoS 攻擊是透過隱藏企業的 IP 位址，遠傳會以中介者之角色傳送及過濾通訊請求，以降低惡意封包傳入企業之機率。
天空數位	針對 DDoS 攻擊之防禦伺服器，最大可抗 4,700 Gbps 流量。	伺服器可針對網路第三至第四層的 DDoS 攻擊流量進行偵測防禦，並可於五分鐘內緩解流量壓力，針對來自 DNS 的 DDoS 攻擊，則可於 10 分鐘內緩解。

資料來源：[16][17][18][19][20]

由上可知，許多資安單位及網際網路接取服務業者多已推出相關防護機制和設備，讓企業得以透過與之合作，大幅降低 DDoS 攻擊所帶來之威脅，從而提升整體網際網路之安全。

四、分析與建議

DDoS 攻擊種類、數量及手法類型眾多，企業難以透過單一機制和系統進行全面防範，甚至開始出現透過 DDoS 攻擊癱瘓企業服務後，進行金錢勒索等行為，因此企業已將 DDoS 攻擊防護列為營運的重要目標。

為從根源杜絕 DDoS 攻擊，應減少攻擊者可操縱的殭屍網路數量，尤其在近期物聯網的發展快速，在便利性提升的狀況下，其資安防護往往尚未完備。因此，建議從一般使用者到企業本身，在建置、安裝任何裝置時，都應審慎進行安全性評估及做好完善的防護設定，尤其避免使用預設密碼或弱密

碼，以保障設備本身之安全性，避免被駭成為殭屍網路之一員。

為避免企業受到 DDoS 攻擊後，其服務受到嚴重之損害衝擊，應儘量減少可能受影響之區域和嚴重程度。建議企業應針對其提供服務之任何應用程式及資源，不應公開並減少開放不必要的通信埠（port），以便在事件發生時可快速因應並專注處理範圍。此外，建議企業可透過內容傳遞網路(Content Delivery Network, CDN)或負載平衡器等方式，減少因大流量封包而對設備之關鍵運行部分產生影響之風險。

為避免企業在受到 DDoS 攻擊後，其伺服器因無法負荷大流量封包而產生服務中斷之狀況，建議企業應建立具有彈性的伺服器或雲端伺服器廠商，一旦出現 DDoS 攻擊事件，可即時增加伺服器和網際網路頻寬等資源，加強負荷能量，甚至透過備援伺服器提供服務，減少企業在受到 DDoS 攻擊後無法運行之問題。

由於許多 DDoS 攻擊中，大量的殭屍網路往往來自於不同的國家，因此建議企業除了防禦外，我國業界也需建立與國外資安單位之聯繫，例如透過 TWCERT/CC 與國外 CERT 組織建立溝通橋樑，以便能在第一時間與攻擊來源之國家進行通報，從根源解決 DDoS 攻擊威脅。

- 資料來源：

1. DDoS 攻擊是什麼？ 弄懂常見 DDoS 攻擊手法與防禦措施
2. 什麼是 DDoS 攻擊？
3. UDP-Based Amplification Attacks
4. DDoS attacks in Q2 2022
5. DDoS attacks in Q1 2022
6. DDoS attacks in Q4 2021
7. 淺談匿名者網路攻擊事件與防範作為

8. 臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件
9. 臺灣多家主機託管商遭 DDoS 攻擊，元兇是國內 IP 疑大量 DVR 設備遭入侵
10. 【資安周報第 47 期】傀儡網路氾濫，臺灣成為全球 DDoS 攻擊幫兇
11. DDoS attack on Dyn costly for company: claim
12. DDoS attack on the Russian banks: what the traffic data showed
13. Russian banks hit by cyber-attack
14. 多層次 DDos 防禦
15. DDoS 防護服務
16. 抗 DDOS 攻擊服務
17. 遠傳 Imperva Application Security
18. 防禦伺服器 / DDOS PROTECTION SERVER

第 2 章、 資安小知識

網頁置換(Website Defacement)攻擊防護與應變措施

網頁置換(Website Defacement)攻擊：駭客入侵受害網頁伺服器並將受害設備之原網頁替換成其它駭客自製的網頁，常見於有政治動機的「網路抗議者」、激進駭客(Hacktivism)用來傳播訊息或是用以炫耀技術、戰績。例如知名的網頁置換揭露平台 zone-h，擁有大量國際駭客所分享之成功攻陷並置換的網頁快照資料庫，遭到網頁置換之主因通常為網站或伺服器設備出現漏洞，因此遭駭客侵入與控制。

2022 年 8 月全台陸續發生若干網路攻擊事件，其中公共空間廣告看板因受駭而遭受傳遞惡意假訊息，學校及政府網頁遭置換等攻擊事件。因此，網站管理人員可參考，本中心所提供的網站安全防護建議以及應變措施。

網站安全防護建議（Identify 、Protect and Detect）

1. 制定網站事件應變處理作法，準備好維護頁面與演練導向流程。
2. 制定基本安全策略並持續執行：

- 加強網站管理者的密碼強度或複雜度、多因子認證(Multi-factor authentication，MFA)，並且定期更新密碼。

- 審視或以掃描軟體確認網站目錄的使用者存取權限狀況。
- 定時進行網站備份、資料庫備份，落實 3-2-1 備份原則。

3. 網頁應用安全防護措施：

- 網站開發時，應要求開發商納入原始碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)。
- 網站上線後，應定期檢視網站建置環境及所使用之套件以及外掛程式等所屬廠商之更新支援狀況，並保持最新；如發現廠商公布不再支援更新修補，應即檢討可用性以及替換方案。

4. 系統安全防護措施：

- 網站伺服器的作業系統及應用程式務必安裝最新版的安全更新，並定期進行弱點掃描。
- 安裝防火牆以及防毒軟體，並正確設定防火牆規則，保持防毒軟體掃毒引擎與病毒碼更新至最新。
- 關閉不必要之網路服務，建立密碼時使用複雜度高之強密碼規則。

遭受網頁置換攻擊應變措施（Respond and Recover）

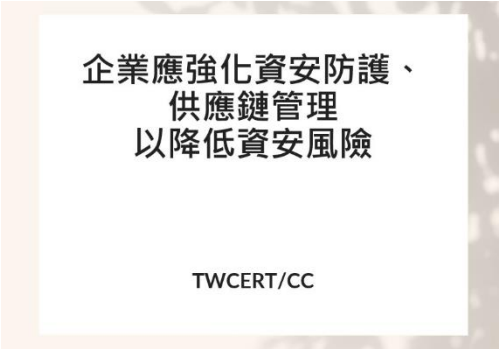
1. 立即關閉網站，並導向維護頁面。
2. 評估攻擊影響範圍，啟動相關應變程序。
3. 向警調單位報案尋求協助，並通報 TWCERT/CC。
4. 確認入侵根因與途徑，或進行鑑識處理。
5. 如確認資料庫未受影響，或有攻擊時間點之前的資料庫備份，可以備份或原

始的網站程式與資料庫重新運行網站。

- 對重新運行之網站，依入侵原因進行漏洞修補、權限設定、密碼變更等動作。
- 網頁重新上線，並持續監控相關活動紀錄，以確認無其它的攻擊或惡意程式植入情形。

第 3 章、 資訊安全宣導

3.1.1、企業應強化資安防護、供應鏈管理，以降低資安風險



美國眾議院議長裴洛西 111 年 8 月 2 日訪台，全台陸續發生若干網路攻擊事件，包含政府網站、伺服器受到 DDoS 攻擊、以及超商與公共空間廣告看板因受駭而傳送惡意假訊息。

TWNIC 台灣網路資訊中心管理 .tw 國家頂級網域營運，我們高密度監控國家頂級網域運作情況。在 2 日至 3 日間國家頂級網域 DNS 最大查詢量每秒約八萬五千筆, 其中近 75%訊務量為惡意攻擊封包，這些 IP 位址持有者主要來自美國與中國雲端業者，其中美國雲端業者佔比 54.8%，中國業者佔比 44.2%。

在廣告看板受駭遞送惡意假訊息方面，企業採取與廣告業者合作推播廣告內容，由於廣告業者普遍資訊專業人力不足，可能採用中國廠商之軟體導致系統受駭。目前受駭單位均已報案並進行後續相關調查程序。TWCERT/CC 為政府與企業之間資安協防與情資分享主要窗口，我們鼓勵企業強化資安防護，勿使用勿下載來源不明的軟體及網通設備，為避免不必要的資安風險，建議企業可採取以下措施：

1. 部署資安防禦設備，如防火牆等，阻擋不明的網路連線。
2. 定期進行資安檢測以維護軟體及設備。

3. 採用連網產品前，選用符合資安標章的連網產品，並利用資安管理法的資安要求來規範供應商，以提升產品及服務的基本資安品質。

4. 如需協助可聯繫 TWCERT/CC (twcert@cert.org.tw)，TWCERT/CC 可協調電信業者或政府部門進行聯防，或是協調資安廠商及專家資源協助相關調查。

3.1.2、近期偽冒政府機關網域發送勒索用戶之詐騙郵件

本中心近期接獲民眾收到勒索郵件的通報，該郵件來源為駭客偽冒政府機關網域發送詐騙郵件。郵件內宣稱駭客已取得用戶電子郵件的訪問權限、於用戶的電子設備植入惡意軟體，並取得用戶所有的通訊與活動紀錄。接著表明擁有用戶的私密影片，若不希望影片外流必須支付特定數量的比特幣，否則將會公開用戶的私密影片至其親友。

提醒民眾，收到此類詐騙郵件請勿匯款，建議先聯繫相關單位進行求證，或是至 TWCERT/CC 官網進行通報。

郵件特徵：

1. 郵件來源為偽冒政府機關網域(如圖 1)。

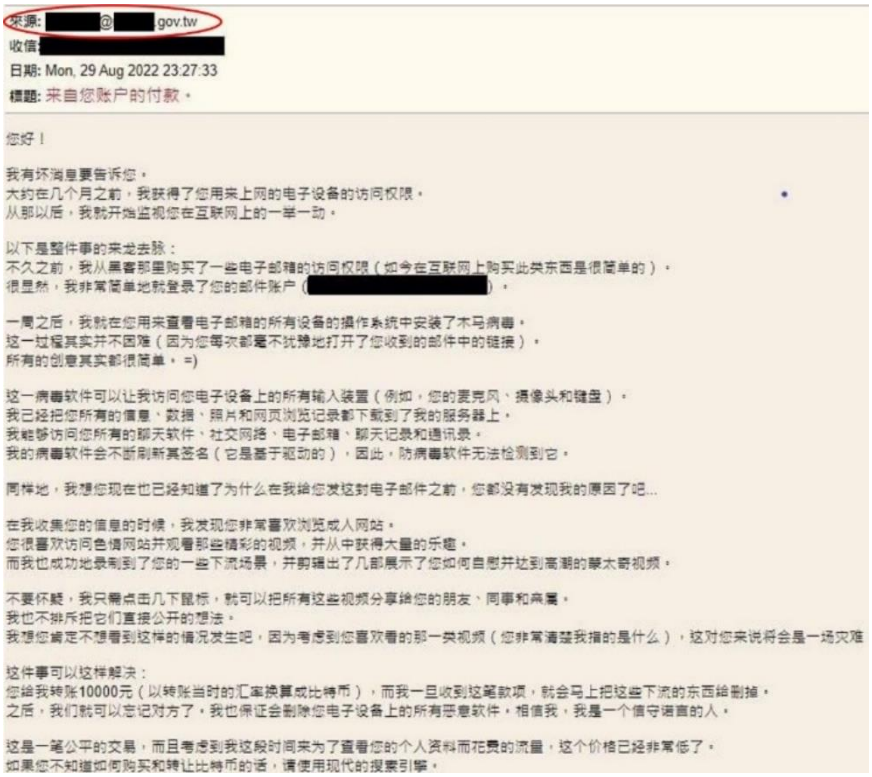


圖 1、偽冒政府機關網域發送之詐騙郵件

2. 郵件內容表示已在用戶的設備植入惡意軟體、取得用戶的電子郵件，以及所有在電腦網路上的活動紀錄。

3. 要求支付特定數量的比特幣至指定帳戶，否則會將私密影片外流。

TWCERT/CC 提供以下防護建議：

1. 建議立即將郵件中提到密碼的系統進行密碼更改，並且定期更換密碼(使用 12 個字元以上之英文、數字與符號混合之密碼)。

2. 不隨意點擊信件中的任意連結、附件或檔案，以避免遭植入惡意軟體。

3. 收到偽冒政府機關網域發送之郵件，建議聯繫相關單位求證，或是撥打 165 反詐騙諮詢專線尋求協助。

4. 至 TWCERT/CC 官網進行資安通報。

第 4 章、 資安活動紀事

111 年資安聯盟會員線上會議(111.06.22)

活動時間：111.06.22(三)

台灣電腦網路危機處理暨協調中心(TWCERT/CC)，在行政院資通安全處及國家通訊傳播委員會指導下，於 111 年 6 月 22 日透過線上方式舉辦會議。會議首先由 TWNIC 副執行長兼 TWCERT/CC 計畫主持人丁綺萍代表致歡迎詞，說明 TWCERT/CC 除作為我國國內外緊急資安事件通報處理組織，另一重要工作就是建立可信賴的資安情資分享機制，TWCERT/CC 在國家通訊傳播委員會的指導下會員數已成長到 650 餘家，期望透過資安聯盟，成員可彼此交換資安情資，並針對營運面遭遇資安問題或近期發現之重要資安議題進行探討與分享，以達資安聯防之目的，進而強化台灣整體資安防護能力。

接著由國家通訊傳播委員會吳銘仁副處長代表貴賓致辭，吳副處長提到 TWCERT/CC 的任務，除了提升會員數，成為我國企業資安事件通報及協處窗口，亦是我國國際資安聯繫窗口。希望透過與會員分享國內外資安情資與實務經驗，強化資安聯防體系，降低企業資安風險，建構我國安全網路環境。

本次會議第一個議程由奧義智慧科技創辦人邱銘彰分享「AD 入侵路徑可視化」，Windows Active Directory (AD) 是企業 IT 與資安管理最核心的關鍵

之處，可謂是保護企業資安的重中之重，同時也是最難以理解的陰暗角落。在這場議程中，奧義智慧將從 AI 技術的角度切入，深入探索平時難以觸及的 AD 安全議題，從量化到量測、全面洞悉 AD 潛在的安全隱患，並分享如何利用 AI 技術結合紅、藍隊演練思維，協助企業勾勒出能有效強化防護的資安邊界。第二個議程由 BV 資訊安全部/首席資安專家林上智分享「如何打造安全的開源供應鏈-OpenChain 開源軟體安全保證參考規範」，此次分享介紹 OpenChain 開源軟體安全保證參考規範的關鍵要求，組織可透過相關要求打造開源安全供應鏈，並在不同組織間建立信任以交換由開源軟體組成的解決方案。第三個議程則由聯盟成員網擎資訊劉中仁研發協理分享「談 Mail Server 之攻防實錄與技術分析」，電子郵件是單位或企業不可或缺的服務，其中 Mail server 在大部分情況下都會開放從外網存取，富含資訊金礦又對外開放的特性就成為了駭客攻擊的首選目標之一。網擎(Openfind) 在台灣長期經營電子郵件相關服務，擁有許多政府及企業客戶，無可避免的必須經常面對這些攻擊的挑戰。透過分享真實發生的攻擊的案例、揭露 Linux 系統後門程式等手法、以及介紹防堵及更新情資的做法，若能透過彼此分享交流情資，必能更有效的抵擋來自外在的攻擊。

第 5 章、 國內外重要資安事件

5.1、資安趨勢

調查指出，三分之一英美企業每周都遭到勒贖攻擊威脅

一項由資安廠商進行的資安調查，針對英美兩國大型企業的資安報告指出，有近三分之一受訪公司，每星期至少遭受一次勒贖攻擊；部分企業甚至每天都遭到勒贖攻擊。

該調查名為「2022 衝擊：勒贖攻擊與應對措施完備度」的報告，由兩家資安廠商 Menlo Security 與 SAPIO Research 針對英國與美國總共 505 家 1000 名員工以上廠商的 IT 決策主管進行調查，了解各該廠商在針對企業勒贖攻擊所進行的準備完備程度、對企業造成的影響，以及對 IT 決策主管個人本身的衝擊。

在調查報告中指出，由於勒贖攻擊近年來日益泛濫，攻擊強度和頻率不斷提升，有 41% 受訪單位表示，其資安團隊的資安知識與技巧，已經不足以對應這些資安攻擊；另有 39% 受訪單位也擔心資安團隊的能力可能無法抵擋這類攻擊。

不過，企業資安團隊最擔心的，是企業員工往往忽視公司的各種資安建

議與規範，任意點擊各種惡意連結，或隨意開啟含有惡意程式碼的信件夾檔；有這項擔憂的在調查單位中比例高達 46%。

另外，也有 26% 的資安團隊受訪者，擔心自己會因為公司遭到各類攻擊得逞，因而遭到解僱。

在勒贖攻擊本身方面，一半以上的受訪企業表示，在過去 18 個內都曾遭到成功的勒贖攻擊，而企業系統內的用戶與潛在用戶，包括企業員工、合作夥伴、供應商、合約人員等，通常都是攻擊發生的脆弱點；此外，也有十分之一的受訪廠商表示，無法確實掌握勒贖攻擊的針對目標。

報告也指出三大最常遭到勒贖攻擊的脆弱點，分別是 Email（54%）、桌機或筆電的瀏覽器（49%），以及行動裝置（39%）。

建議各企業應該加強防範勒贖軟體的軟硬體設置與人員教育訓練，同時設法提高資安人員的待遇與士氣，以免第一道防線崩潰，造成更大的資安危機。

- 資料來源：
  1. Assessing ransomware readiness in 2022
  2. One-third of organizations experience weekly ransomware attacks

5.2、新興應用資安

5.2.1、駭客利用 Google Sites 與 Microsoft Azure Web App 發動釣魚攻擊

資安廠商 Netskope 旗下的研究人員，近來發現有駭侵者利用 Google Sites 與 Microsoft Azure Web App 等雲端服務架設仿冒網站，用於攻擊加密貨幣投資者，以竊取其加密資產。

報告指出，駭侵者的攻擊手法，是事先利用上述的雲端服務來架設多個仿冒知名加密貨幣錢包或交易所入口的釣魚網站，然後利用留言機器人在各大加密貨幣相關社群的討論區中大量發送含有這些釣魚網站連結的留言；用戶如果不慎誤信連結，即可能將自己的錢包或交易所登入資訊輸入到釣魚網站中。

報告指出，由於駭侵者選擇使用 Google 和 Microsoft 的服務，因此這些網站的網域名稱就是 Google 與 Microsoft 所屬的網址；這樣不但垃圾留言較不易遭到自動垃圾留言清除機制刪除，甚至還能取得很好的 SEO 效果。實測發現，一些駭侵者設立的釣魚網站，連往往會在 Google 搜尋結果中名列前茅。

報告說，這些釣魚網站攻擊的對象，是大型加密貨幣交易所與知名加密

錢包的用戶，例如 Coinbase、MetaMask、Kraken、Gemini 等。駭侵者企圖利用這些假入口網站來騙取用戶的交易所與加密錢包的登入資訊與錢包復原短語，以完全控制用戶的數位資產。

報告指出，這些假網站還包括假的二階段登入驗證頁面，會要求用戶輸入手機號碼；待用戶輸入手機號碼後，假網站會顯示一個假的錯誤訊息，宣稱用戶因違反安全守則，帳號已遭停用；用戶必須按下頁面中的「詢問專家」按鈕，接著會有假冒的客服人員與用戶線上對談，誘使用戶開啟 Team Viewer 等遙控軟體，竊取用戶收到的二階段驗證碼。

建議加密貨幣投資者不要在任何社群網站中點按宣稱是官方網站的連結，且應注意連結本身是否為真實的網域名稱。

- 資料來源：
  1. Abusing Google Sites and Microsoft Azure for Crypto Phishing
  2. Phishing attack abuses Microsoft Azure, Google Sites to steal crypto

5.2.2、駭侵者利用未知漏洞，一夕竊走數千個錢包中的 Solana 代幣

近年來十分熱門的 Solana 區塊鏈平台，日前發生嚴重駭侵事件；目前已知近 8,000 個去中心化錢包遭到駭侵者攻擊，竊走存放的 Solana 代幣，損失達數百萬美元。

Solana 平台指出，在 8 月 3 日世界標準時間上午 5 時左右發生的駭侵攻擊事件中，有 7,767 個 Slope 和 Phantom 去中心化錢包遭到攻擊，內部存款遭到不當存取；包括其行動版裝置與瀏覽器外掛程式版本，都未能倖免。

而據區塊鏈分析平台 Elliptic 統計，受到影響的錢包數量接近 7,936 個，包括 SOL 代幣、近 300 種以 Solana 區塊鏈建構的各種代幣與 NFT 的損失總金額則高達 520 萬美元。

Solana 指出，目前正在調查整起事件，尚無法推論駭侵者是透過何種方式，利用哪些漏洞發動攻擊；不過 Elliptic 指出漏洞很可能是發生在錢包軟體端，而非 Solana 區塊鏈平台上；因為所有被駭的交易，都由錢包真正用戶的私鑰進行數位簽署，因此可能是駭侵者透過錢包本身的漏洞，取得受害者擁有的私鑰來竊取加密貨幣資產。

此外另有一個線索支持這種推論：使用 Solflare 和 Trust Wallet 的用戶，

並未受到本次駭侵攻擊的影響。硬體錢包（即所謂冷錢包）內的資產也未受影響。

資安專家推論指出，能夠一次取得這麼多用戶的私鑰來進行攻擊，其駭侵手法很可能是透過供應鏈攻擊，或是利用某個瀏覽器的 0-day 漏洞，或是錢包產生私鑰時使用的亂數產生器內的漏洞。

建議加密貨幣投資者應避免將大額資產存放在網路或軟體錢包（即所謂熱錢包）中，應使用離線儲存的硬體錢包（冷錢包），以避免類似攻擊事件，造成鉅額資金損失。

- 資料來源：
  1. Solana Status @SolanaStatus
  2. Over $5.8 Million Drained in Solana Wallet Exploit
  3. Solana Wallet Hack: Here’s What We Know So Far

3.2.3、APT 駭侵者假扮知名加密貨幣交易所 Coinbase，提供假工作機會以攻擊專家

資安廠商 Malwarebyte 近日發現著名的 APT 駭侵團體 Lazarus，最近假冒知名加密貨幣交易所 Coinbase 之名，在求職社群網站 LinkedIn 上對加密貨幣專家傳送假的工作機會，藉以發動攻擊。

Malwarebyte 旗下的資安專家 Hossein Jazi 日前在推特上發文，指出 APT 駭侵團體 Lazarus，自本（2022）年 2 月起，開始在 LinkedIn 上假冒為全球最大級加密貨幣交易所 Coinbase，鎖定多名加密貨幣專家，對其發送假的工作機會。

駭侵者貼出的假職缺為 Coinbase 產品安全部門（Product Security）的工程經理（Engineering Manager），並且在職務說明中放置一個看似是 PDF 文件檔，但實際上是個含有惡意軟體的 Windows 可執行檔；用戶打開這個檔案，會開啟一個看起來很像是 PDF 文件檢閱工具的視窗，其中顯示該職缺的說明，但實際上會執行惡意程式碼。

資安專家指出，Lazarus 駭侵團體過去有多次針對金融機構與加密貨幣相關單位的駭侵攻擊記錄；近年來包括諸多用戶的加密貨幣錢包、多家交易所、NFT 交易市場等，都曾有遭到 Lazarus 駭侵攻擊的記錄。

今年 7 月時 Lazurus 亦曾透過與本次類似的手法，針對熱門 NFT 遊戲 Axie Infinity 公司的工程師發送假的工作機會邀約，實則透過惡意軟體入侵工程師使用的裝置，進而竊走高達 6.17 億美元的以太幣與 USDC 代幣。

Malwarebyte 研判，Lazarus 這次假冒 Coinbase 發送假職缺的攻擊活動，很有可能是重施攻擊 Axie Infinty 的故技，意圖藉此駭入更多加密貨幣相關產業的電腦系統，藉以竊取更多加密資幣資產。

建議在金融與加密貨幣相關產業的工作人員，應對各種不明連結和檔案提高警覺，避免因點擊或開啟不明連結與檔案，讓駭侵者趁機駭入公司系統內，造成重大損失。

- 資料來源：
  1. Jazi @h2jazi
  2. North Korean hackers target crypto experts with fake Coinbase job offers

5.3、國際政府組織資安資訊

5.3.1、德國工商協會遭大規模駭侵攻擊，所有服務均被迫停用

德國工商協會（The Association of German Chambers of Industry and Commerce, DIHK）日前因遭到大規模駭侵攻擊，被迫暫停旗下所有 IT 系統服務，造成其數位服務、電話、電子郵件伺服器等全面停擺。

DIHK 是由德國超過 300 萬家工商業共 79 個協會合組的大型工商業組織，提供法律、顧問、外貿宣傳、教育訓練、區域經濟發展、常務支援等服務。

據 DIHK 日前發表的資安通報指出，該會受到外部駭侵攻擊影響，為了讓 IT 團隊能夠儘速找出解方，同時建構防線，因此必須暫停各項服務。

DIHK 總經理 Michael Bergmann 也在該會於 LinkedIn 的公開頁面上發表聲明，指出攻擊發生於 8 月 3 日，造成相當嚴重的影響；該會目前正在逐步排除問題並恢復各項服務，但何時才能完全復原，尚不得而知。

DIHK 並未對外公開本次攻擊的細節，雖然外界推測可能是遭遇勒贖攻擊，但目前還沒有主要的勒贖團體對外宣稱針對 DIHK 發動攻擊。

德國媒體 Heise.de 的報導則認為這次攻擊並非針對德國某特定地區發動，因為 DIHK 在德國各地的分支機構，例如北萊因-西發里亞、下薩克森尼、巴伐利亞、科隆等地的分會也都證實系統因攻擊而無法運作。

鑑於勒贖或其他類型的駭侵攻擊，不只針對單一廠商目標發動攻擊，具有重要功能與地位的產業聯合組織也在其攻擊目標之列，因此這類單位亦應提高警覺，加強資安防護，以避免一整個國家的產業都同時受到影響。

- 資料來源：
  1. Cyberangriff: IHK-Verbände weitgehend offline, auch telefonisch nicht erreichbar
  2. German Chambers of Industry and Commerce hit by 'massive' cyberattack

5.3.2、澳洲政府起訴監控惡意軟體 Imminent Monitor 開發者

澳洲政府日前起訴一個製作並販賣監控惡意軟體 Imminent Monitor 的 24 歲澳洲籍軟體開發者，該惡意軟體曾販售給超過 128 國的 14,500 人，用於不當監控受害者並竊取多種機敏資訊。

澳洲警方近日發布新聞稿，指出該名開發者創作的監控軟體，有許多暴力犯與各種犯行購買，可用於遠端遙控受害者的裝置、竊取裝置上的多種資訊，包括用戶輸入資訊、儲存於裝置內的檔案與資料、擷取螢幕畫面、自用戶裝置的 webcam 錄影錄音等等。

警方表示，Immienet Monitor 是自 2013 年開始對外販賣，當時該開發者年僅 15 歲；開發者以遠端管理軟體的名義宣傳 Imminent Monitor，且售價相當便宜，只需 25 美元即可購得永久使用權，甚至包括客戶服務在內。

雖然 Imminent Monitor 表面上看似正常的遠端管理工具，但在駭侵相關論壇和客服內容中，開發者卻以「Shockwave」為名做為招徠，強調其駭侵能力。

2019 年 4 月，在某個駭侵相關論壇中，有一篇討論 Shockwave 突然消失的貼文；貼文作者推測 Shockwave 的作者可能已遭到逮捕；該文同時警告

Shockwave 的使用者亦有遭到追緝的可能。

除了澳洲警方的逮捕行動外，2019 年 11 月時，歐洲刑警組織（Europol）亦展開一波針對 Imminent Monitor 不法使用者的打擊行動，逮捕 13 名大量使用者，並且查獲 430 台相關設備及宣傳用網域等。

建議個人或公司行號如有遠端設備管理需求，應購買信譽良好的大公司產品，切勿購買來路不明的軟體產品或服務，以免發生此類糾紛。

- 資料來源：
  1. AFP charges man with creating global spyware tool
  2. Australia charges dev of Imminent Monitor RAT used by domestic abusers

5.4、社群媒體資安近況

5.4.1、Twitter 證實遭駭侵者利用 0-day 漏洞取得 540 萬用戶資料

知名社群平台 Twitter 日前證實近日發生一起資料外洩事件，約有 540 萬用戶資料，遭駭侵者利用一個現已修補完成的 0-day 漏洞竊走。

該入侵事件發生於去（2021）年 12 月；資安專業媒體 BleepingComputer 當時報導有駭侵者在駭侵相關論壇上張貼文章，意圖出售自 Twitter 竊得的 5,485,636 筆用戶資料。

Twitter 這個 0-day 資安漏洞，使任何人都可以利用用戶登錄在 Twitter 個人檔案中的各種資料，包括電話號碼、Email 帳號等等當做查詢索引，查出用戶的帳號 ID 後，繼而可以取得更多用戶資訊，例如在 Twitter 中使用的顯示名稱、登入名稱、所在地、追蹤人數、頭像圖片網址等各種資訊。

據 BleepingComputer 當時的報導指出，駭侵者打算將這批 540 萬名用戶的資訊，以 30,000 美元的價格出售，而至少有兩組駭侵團體在經過議價後，買走這些資訊。

Twitter 直到 8 月 5 日證實確實發生該 0-day 漏洞遭駭侵者用於竊取用戶個資的事件；在其聲明中表示該公司於 2022 年 1 月在一場漏洞發現懸賞活動

中，得知該漏洞可用於竊取用戶個資的報告，於 6 月修補好這個漏洞。

Twitter 指出，這次資料外洩事件中，並沒有任何用戶的登入密碼遭到外洩，但該公司也無法確切計算出到底有多少名用戶的個資遭到竊取。

建議各社群平台用戶應儘可能不要在個人檔案中填寫過多可供鎖定個人身分的資訊，並且應啟用二階段登入驗證，以避免社群帳號或其上的個資遭到攻擊。

- 資料來源：
  1. An incident impacting some accounts and private information on Twitter
  2. Twitter confirms zero-day used to expose data of 5.4 million accounts

5.4.2、部分 Slack 用戶因邀請連結雜湊遭外洩而需重設密碼

受到廣泛採用的企業即時通訊服務 Slack，日前通知部分用戶，因為修復了一個邀請連結雜湊外洩的錯誤，必須重置這些客戶的登入密碼。收到這項通知的用戶，約占 Slack 所有用戶數的 0.5%。

Slack 表示，該漏洞會在用戶產生或取消邀請連結時，會傳送一個經過雜湊運算的密碼；雖然要從雜湊值反向運算，以得到正確密碼的機率相當低，再加上駭侵者必須密集監聽 Slack 伺服器的網路傳輸資訊，但這仍屬於不安全的資料傳輸方式。

該漏洞是由未公開的獨立資安研究人員，於 7 月 17 日向 Slack 通報；Slack 獲報後立即修復改漏洞，且重置可能受影響用戶的登入密碼。

據 Slack 的資安通報指出，任何曾在 2022 年 4 月 17 日到 7 月 17 日間產生邀請連結或撤消邀請的用戶，其 Slack 登入密碼都已重置，用戶必須重新設定新的登入密碼，才能再次登入其 Slack 帳號。

Slack 指出，使用暴力試誤法，仍有可能將雜湊值反向運算，以得出正確的密碼內容，因此 Slack 為加強密碼安全，仍然必須重置部分用戶的登入密碼。

Slack 表示，有疑慮的用戶，可以透過其資安通報網頁內提供的連結，下載自己的登入及使用記錄，以檢視是否遭到不當存取。

即使不容易透過雜湊值反向算出正確密碼，Slack 仍建議所有用戶使用強式密碼、啟用二階段登入驗證功能，並且避免在不同服務之間使用相同密碼，以避免自己的帳戶遭到駭侵者不當存取。

- 資料來源：
  1. Notice about Slack password resets
  2. Slack resets passwords after exposing hashes in invitation links

5.5、行動裝置資安訊息

5.5.1、Facebook 發現 APT 駭侵者透過全新 Android 惡意軟體發動攻擊

Facebook（Meta）日前發表 2022 年第二季資安威脅對抗報告（Q2 2022 Adversarial Threat Report），其中指出該公司發現兩個先進持續性威脅（Advanced Persistent Threat, APT）駭侵團體，利用新的 Android 惡意軟體發動的大規模駭侵攻擊活動。

在報告中指名的兩個 APT 團體，分別是「Bitter APT」和 APT36（又名 Transparent Tribe）；報告說觀察到這兩個 APT 團體都利用 Facebook 這樣的社群平台，透過利用假帳號與被害人加為朋友，引誘被害人到外部平台下載安裝惡意軟體，來進行監控駭侵攻擊。

APT 36 在惡意軟體中利用可跳過雙重身分驗證機制的漏洞，來監控印度政府相關目標並竊取情報；而 BItter APT 則在 2022 年 5 月被發現針對孟加拉政府的目標，以能夠遠端執行任意程式碼的惡意 App 來進行監控與情報竊取。

另外，Meta 的報告也指出，Bitter APT 涉及針對紐西蘭、印度、巴基斯

坦、英國等國家的目標，發動綿密的社交工程攻擊，目標是讓被監控對象安裝惡意軟體；其手段結合了短網址、遭駭網站和第三方檔案儲存服務等。

Meta 也說，Bitter APT 利用一個名為 Dracarys 的 Android 惡意軟體，結合非官方版本的 YouTube、Signal、WhatsApp 等常用 App，誘使用戶安裝後，接著濫用 Android 系統中的輔助使用功能，在用戶不知情的狀況下竊取各種資訊，包括通話記錄、通訊錄、裝置內檔案、簡訊、地理座標、裝置資訊，並且私下拍照、開啟麥克風，甚至安裝 App。

Meta 也說 Dracarys 能夠逃過目前各種防毒防駭軟體的偵測，因此防不勝防。

鑑於各類針對行動裝置的惡意軟體不斷推陳出新，用戶不應完全依賴防毒防駭軟體，應養成良好的使用習慣，不隨意安裝來源不明的應用軟體，以免遭到惡意軟體的植入。

- 資料來源：
  1. Quarterly Adversarial Threat Report
  2. Facebook finds new Android malware used by APT hackers

5.5.2、Google Play Store 中藏有 35 種 Android 惡意 App，下載次數達 200 萬次

資安廠商 Bitdefender 日前發表調查報告，指出該公司於 Google Play Store 中再次發現多達 35 種惡意 App，會先以特定功能吸引 Android 用戶安裝，於安裝後開始發動各種攻擊，並立即變更 App 名稱與圖示，使用戶難以發現並移除。

在 Bitdefender 的報告中指出，該公司以即時活動分析法，找出這批具有潛在危害的惡意 App；而這 35 個 App 主要都是所謂的惡意廣告 App，會在用戶手機中顯示大量廣告，藉以賺取廣告點閱分潤。

報告也指出，這 35 支 App 使用自有框架來顯示廣告內容，而這樣的架構也有利於駭侵者於日後透過惡意 App 下載更多惡意程式碼，或是自我更新，讓這些惡意 App 具有更多元的攻擊能力。

而這些惡意 Android App 擁有多種避免偵測與用戶移除的手法，例如安裝完成後，立刻把原本的圖示換成一個齒輪圖示，並且將自身的 App 名稱變更為「Settings」，讓用戶以為該惡意 App 是系統設定程式；一旦用戶點按該 App 圖示，該 App 會立即顯示一個大小為 0 的像素，以自畫面上消失，然後立即啟動真正的系統設定 App，藉以混淆用戶視聽。

這 35 個惡意 Android 共由使用者下載安裝達 200 萬次以上，其名單如下：

- Walls light – Wallpapers Pack (gb.packlivewalls.fournatewren)
- Big Emoji – Keyboard 5.0 (gb.blindthirty.funkeyfour)
- Grand Wallpapers – 3D Backdrops 2.0 (gb.convenientsoftfiftyreal.threebord er)
- Engine Wallpapers (gb.helectronsoftforty.comlivefour)
- Stock Wallpapers (gb.fiftysubstantiated.wallsfour)
- EffectMania – Photo Editor 2.0 (gb.actualfifty.sevenelegantvideo)
- Art Filter – Deep Photoeffect 2.0 (gb.crediblefifty.editconvincingeight)
- Fast Emoji Keyboard APK (de.eightylamocenko.editioneights)
- Create Sticker for Whatsapp 2.0 (gb.convincingmomentumeightyverified.re algamequicksix)
- Math Solver – Camera Helper 2.0 (gb.labcamerathirty.mathcamera)
- Photopix Effects – Art Filter 2.0 (gb.mega.sixtyeffectcameravideo)
- Led Theme – Colorful Keyboard 2.0 (gb.theme.twentythreetheme)
- Animated Sticker Master 1.0 (am.asm.master)
- Sleep Sounds 1.0 (com.voice.sleep.sounds)
- Personality Charging Show 1.0 (com.charging.show)
- Image Warp Camera
- GPS Location Finder (smart.ggps.lockakt)

據資安媒體 BleepingComputer 報導指出，Google Play Store 尚未完全下架上列惡意軟體。

為避免在官方 Google Play Store 仍安裝到惡意 app，建議用戶在點按下載安裝前，應詳細查閱該 App 的評價與用戶意見，若發現疑問，切勿安裝下載。

- 資料來源：

1. Real-Time Behavior-Based Detection on Android Reveals Dozens of Malicious

Apps on Google Play Store

2. Android malware apps with 2 million installs found on Google Play

5.5.3、SOVA Android 金融惡意軟體新增勒贖功能，會將 Android 手機資料加密

資安廠商 Cleafy 近日發表研究報告，指出該公司發現 SOVA Android 金融木馬惡意軟體，在最近推出的「新版本」第 5 版中，加上了針對 Android 手機的勒贖功能，除了原本的金融詐騙功能外，還加上將 Android 手機內部資料加密的勒贖功能，以進一步強化其攻擊能力。

據 Cleafy 指出，SOVA 在 2011 年 9 月首次出現時，該公司就將其列入觀察清單之列，發現該惡意軟體的開發十分有節奏且快速，且開發能量有愈來愈強大的趨勢。

SOVA 於 2022 年 3 月時推出第 3 版，加上了攔截二階段驗證碼、竊取 Cookie 等功能，同時擴大其詐騙覆疊的針對銀行數量，有更多銀行網頁或 App 會遭其使用畫面覆疊手法「蓋台」，用以竊取用戶輸入的登入資訊。

2022 年 7 月時 SOVA 的第 4 版已能透過覆疊，竊取 200 家銀行用戶的登入資訊，甚至加上 VNC 遠端遙控功能，也能擷取用戶手機畫面、複製貼上檔案、執行點按與滑動動作，甚至重構其 Cookie 竊取程式碼，能竊取 Gmail、GPay、Google Password Manager 的密碼；對抗防毒軟體掃瞄的能力也大幅提高。

最近出現的第 5 版，則加上了勒贖程式碼，能以 AES 演算法加密用戶手機內的檔案，加上 .enc 的副檔名。

雖然據 Cleafy 的報告指出，SOVA 第 5 版尚未傳出大量發動攻擊的案例，但對所有 Android 用戶來說，都是必須嚴防的資安威脅，因此 Android 用戶應避免在官方 Play Store 之外的地方下載軟體，更不要任意安裝 apk 檔案，以免遭到惡意軟體植入，蒙受重大損失。

- 資料來源：
  1. SOVA malware is back and is evolving rapidly
  2. SOVA malware adds ransomware feature to encrypt Android devices

5.6、軟體系統資安議題

5.6.1、資安廠商發現 Python 官方程式庫 PyPI 內含多種惡意軟體套件

資安廠商 Check Point 近日發現，廣受 Python 開發者愛用的程式庫 PyPI，遭駭侵者植入多種惡意軟體套件供人下載安裝；用戶如果將之安裝在自己的電腦上，駭侵者即可輕易竊得電腦中的各種機敏資訊，包括登入資訊或 API 金鑰，開發者不可不慎。

Check Point 在近日發表的專文中指出，由於 PyPI 可以很容易的透過單行指令來安裝各種軟體套件，非常便捷，因此近來成為駭侵者的攻擊目標。

Check Point 說，這類具攻擊的具體手法是，駭侵者上傳一些含有惡意程式碼的套件，並偽裝成安裝者眾多的熱門 Python 套件，以魚目混珠的手法，誘使開發者下載安裝在自己的開發用設備上，駭侵者即可得逞。

Check Point 的資安團隊，一共在 PyPI 中發現 10 個含有惡意程式碼的程式套件，分別如下：

- Ascii2text
- Pyg-utils

- Pymocks
- PyProto2
- Test-async
- Free-net-vpn
- Free-net-vpn2
- Zlibsrc
- Browserdiv
- WinRPCexploit

Check Point 指出，近期這類利用惡意程式開發套件，來進行供應鏈攻擊的案例，有愈來愈多的趨勢；發生在本（2022）年 6 月的 Pygrata 攻擊事件，即是駭侵者利用這種手法來竊取用戶 AWS 登入資訊與多種環境變數的案例。

建議開發者在利用 PyPI 這類程式庫安裝套件時，應詳細閱讀文件，確認套件名稱、版本、發行者的真實性，以免誤安裝到惡意程式庫。

- 資料來源：
  1. CloudGuard Spectral detects several malicious packages on PyPI – the official software repository fo
  2. PyPi python packages caught sending stolen AWS keys to unsecured sites

5.6.2、資安研究人員發現存於 Linux 核心長達 8 年的 Dirty Cred 漏洞

美國西北大學的資安研究人員團隊，近來發現 Linux 核心中有一個存在長達 8 年未被發現的漏洞「Dirty Cred」，可能導致駭侵者提升執行權限，並可遠端執行任意程式碼。

該漏洞的 CVE 編號為 CVE-2022-2588，存於 Linux 核心內對於 cls_route 篩選器的實作中，屬於已釋放記憶體漏洞（use-after-free）。駭侵者如果取得本機的 CAP_NET_ADMIN 權限，即可利用此漏洞以進一步提升執行權限，造成系統崩潰或執行任意程式碼。

同一組研究人員，日前在於 Black Hat 資安研討會上揭露另一個存於 Linux 核心版本 5.8 及後續版本的「Dirty Pipe」漏洞（CVE-2022-0847），可輕易繞過 Linux 諸如隨機核心位址與指標完整性檢查等安全機制，利用 Linux 核心的管線機制，在任意檔案中注入資料；而新發現的 Dirty Cred 則不需利用 Linux 核心管線機制，因此使用更加簡便，破壞能力也更大。

研究人員指出，Dirty Cred 的運作原理，是將無權限的核心登入資訊更換成有權限者，無需在核心 heap 中覆寫任何重要資料欄位，只要利用 heap 記憶體重新使用機制，即可取得更高的執行權限。

研究人員也已透過概念證實程式，在 Linux 與 Android 系統上成功實作利用 Dirty Cred 的駭侵攻擊手法。

目前 Linux 開發團隊仍在針對此漏洞發展修補方式，尚未釋出更新；研究人員指出，在虛擬記憶體中將具備權限的登入資訊與不具備權限的登入資訊隔開，以防止跨快取攻擊，可能可以防止駭侵者利用 Dirty Cred 漏洞發動攻擊。

- 資料來源：
  1. New Linux Exploit ‘Dirty Cred’ Revealed at Black Hat
  2. 'DirtyCred' Vulnerability Haunting Linux Kernel for 8 Years

5.6.3、某汽車供應商在 2 週內連遭 3 次勒贖攻擊

資安廠商 Sophos 旗下的資安研究團隊，日前發表案例報告指出，有某家大型汽車業供應商在本（2022）年 5 月時，在 2 星期內連續遭到 3 次勒贖攻擊，造成其系統遭到入侵，檔案亦遭加密。

Sophos 的報告指出，雖然連續兩次的勒贖攻擊愈來愈常見，但這是該公司第一次發現連續三次不同的駭侵攻擊接連發生，而且都使用同一個資安弱點發動攻擊。

報告說，三次勒贖攻擊分別是 Lockbit、Hive 與 ALPHV/BlackCat，都利用該公司防火牆的一個設定上的錯誤，利用 Remote Desktop Protocol（RDP）入侵該公司內網的網域控制器。

5 月 1 日時，LockBit 和 Hive 分別在該公司內網中，利用合法的 PsExec 和 PDQ 布署工具，來散布其勒贖軟體酬載，並在 2 個小時之內就將十多個該公司內部系統的檔案完成加密；其中 LockBit 還把該公司檔案竊取出來，並上傳到 Mega 雲端檔案分享服務上。

隔 2 星期後，正當該公司的 IT 團隊仍在試圖回復系統時，BlackCat 駭侵者也利用和先前相同的防火牆設定漏洞，利用 RDP 入侵同一套網域控制器，

並安裝遠端遙控工具 Atera Agent，接著就在一小時半內利用 PsExec 布署其勒贖酬載，並且利用竊得的登入資訊，將六台電腦中的資料竊走後進行加密。

BlackCat 駭侵者甚至還在完成資料竊取和加密犯行後，刪除 Windows Events Logs，這使得後續的入侵調查與資料復原工作變得更為困難。

Sophos 在報告中也說，由於 Hive 和 Lockbit 的攻擊只相差兩小時，不同的勒贖軟體可能同時在系統中執行，因此某些檔案遭到重覆加密，次數高達 5 次之多。

由於企業遭到駭侵攻擊的次數日漸頻繁，像上例這樣短期間遭不同駭侵者透過同一漏洞連續攻擊的可能性將愈來愈高，因此公私單位應該立即封鎖 VNC 和 RDP 連線，僅使用 VPN 進行連線，並且必須啟用多階段登入驗證。

- 資料來源：
  1. Lockbit, Hive, and BlackCat attack automotive supplier in triple ransomware attack
  2. Automotive supplier breached by 3 ransomware gangs in 2 weeks

5.6.4、Google 指出駭客利用工具可下載 Gmail、Yahoo!、Outlook 收件匣中的郵件

Google 旗下資安研究團隊 Threat Analysis Group （TAG）旗下的研究人員 Ajax Bash，日前發表研究報告指出，駭侵團體 APT35（又名「Charming Kitten」）利用一種新開發的駭侵工具 Hyperscrape，能夠竊取目標對象的 Gmail、Yahoo! Mail、Outlook 等網路信箱的登入資訊，並且竊取信箱內部的郵件內容。

研究人員指出，該團體專門針對所謂「高度危險用戶」做為駭侵目標，一共鎖定約二十多名伊朗境內人士或單位，自 2020 年起就開始利用 Hyperscrape 來對這些目標進行監控。

研究人員也說，Google 長期監控 Charming Kitten 的駭侵行為，發現該組織多年來針對特定目標進行帳號竊取、植入惡意軟體等駭侵監控行動；且 Hyperscrpae 工具的開發工作也持續不斷。

報告指出，Hyperscrape 會利用先前竊得的登入資訊，登入受害者的 Email 信箱，先將用戶選擇的界面語言改為英文，接著開始下載用戶信箱收件匣內的郵件，以 .eml 檔案格式一封一封下載，並將原本未讀的郵件重新設定

為未讀狀態；然後將界面語言還原為用戶的原始設定，最後再刪除 Google 寄發的帳號活動異常警告信件。這樣用戶就難以查覺信件已經遭竊。

Google 的報告中指出，雖然 Hyperscrpae 在技術上並無任何創新之處，但卻能有效配合 Charming Kitten 的駭侵行動而持續開發。

雖然 Hyperscrape 本身只針對鎖定的監控對象，但類似的個資竊取手法可能由其他駭侵團體用來攻擊任何人，因此網路信箱用戶應特別提高警覺，務必使用強式密碼，並啟用二階段登入驗證，以防範駭侵者輕易取得登入資訊。

- 資料來源：
  1. New Iranian APT data extraction tool
  2. Google says Iranian group using tool to download Gmail, Yahoo!, Outlook inboxes

5.6.5、二階段驗證碼產生器 Authy 因 Twilio 遭駭，部分帳號遭駭侵者不當存取

使用者眾多，功能與 Google Authenticator 相似的二階段驗證碼產生器 Authy，經證實在本（2022）年 8 月初 Twilio 遭到駭侵攻擊時，有部分帳號資訊遭到駭侵者竊走；因此駭侵者將可取得這些用戶在各種網路服務在使用時須輸入的二階段驗證碼。

Authy 是由 Twilio 公司於 2015 年併購的服務，主要服務是一種簡單好用的二階段驗證碼產生器，由於可以方便地跨平台同步用戶須產生驗證碼的服務帳號，不必逐一輸入或掃瞄二維條碼，因此相當受到歡迎。

Twilio 最近開始針對該公司在 8 月初遭到的駭侵攻擊事件進行調查，調查證實共有 93 名 Authy 用戶的帳號遭到駭侵者不當存取；這也表示駭侵者將可取得這些用戶在登入各種服務時使用的二階段驗證碼，這樣即可輕易竊取這些服務的帳號控制權。

Twilio 表示為了減低影響層面，該公司立即撤銷了未授權裝置上的 Authy 驗證相關資訊，並與受影響的使用者聯絡，建議採取以下策略：

- 檢查利用 Authy 產生驗證碼的帳號與服務，是否出現不正常的存取或

使用情形。

- 移除任何未經授權裝置的 Authy 連結，阻止其使用 Authy 產生驗證碼。
- 設定一台備份裝置，然後暫時停用 Authy 的跨裝置使用功能。

雖然此次受影響的 Authy 使用者人數相對較少，但類似攻擊事件仍有可能再次發生；為避免自己的二階段驗證碼遭駭侵者取得，用戶可依上列建議策略操作，隨時注意保護自己的二階段驗證碼不會外洩。

- 資料來源：
  1. Incident Report: Employee and Customer Account Compromise
  2. Twilio breach let hackers gain access to Authy 2FA accounts

5.6.6、德國電工產品製造商 Semikron 遭勒贖駭侵攻擊

德國大型電工產品製造商，總部設於德國紐倫堡的 Semikron，日前發布資安通報，指出該公司遭到駭侵攻擊，公司內網部分設施的檔案遭到加密，且有部分資料遭竊。。

Semikron 共有約 24 間辦公室、8 座生產廠房，分布於德國、巴西、中國、法國、印度、義大利、斯洛伐克、美國等地，員工約有 3,000 名，2020 年的營業額達 4.61 億美元。該公司為全球主要的電工產品製造商，其風力發電機的全球市占率達 35%。

該公司於本（2022）年 8 月 1 日發表資安通報，指出該公司「遭到專業駭侵團體的資安攻擊」；目前該公司正在調查整起事件的起因。

德國聯邦資安署（German Federal Office of Information Security）也指出，該駭侵團體威脅將要公開 Semikron 被竊的資料；而資安媒體 BleepingComputer 則指出，據該刊掌握的情資，顯示對 Semikron 發動攻擊的駭侵團體是 LV Ransomware，該組織宣稱自 Semikron 竊得高達 2TB 的機密文件。

Semikron 表示，目前已會同德國官方相關單位進行案件偵辦，也已委請

第三方資安公司進行資料與系統復原，希望能將對客戶、員工、協力廠商的影響降到最低；不過該公司沒有透露進一步的駭侵事件訊息，包括具體的損失、駭侵者要求的贖金等。

有鑑於針對製造業者的駭侵攻擊行動層出不窮，往往造成可觀的損失，包活生產與營運受阻、機密資料外洩等，業者應即加強資安防護投資與教育訓練，並建構完整的備份復原系統，提高類似事件的防禦能力。

- 資料來源：
  1. Nürnberg, 01.08.2022
  2. Semiconductor manufacturer Semikron hit by LV ransomware attack

5.7、軟硬體漏洞資訊

5.7.1、VMware 要求系統管理員立即修補身分驗證繞過資安漏洞

虛擬技術大廠 VMware 日前發布資安通報，要求使用該公司各項軟體系統的管理者，立即進行軟體更新，以修復一個可以繞過身分驗證的嚴重資安漏洞。

這個漏洞的 CVE 編號為 CVE-2022-31656，由資安廠商 VNG Security 旗下的研究人員 Petrus Viet 發現，影響遍及 VMware Workspace ONE Access、Indentity Manager、vRealize Automation 等產品。

該漏洞屬於身分驗證繞過漏洞，駭侵者可利用該漏洞跳過系統的登入驗證程序，在未經授權的情形下進入系統，並可取得系統管理員權限。該漏洞的 CVSS 漏洞危險程度評分高達 9.8 分（滿分為 10 分），其漏洞危險程度評級列為最高的「嚴重」(Critical) 等級。

該公司指出，系統管理員必須依照 VMSA 的指示，立即修補或處理該漏洞。

除了 CVE-2022-31656 外，VMware 同時也修補多個資安漏洞，包括可導

致駭侵者遠端執行任意程式碼的 CVE-2022-31658、CVE-2022-31659、CVE-2022-31665)，以及可讓駭侵者取得 root 權限的 CVE-2022-31660、CVE-2022-31661、CVE-2022-31664 等。

VMware 指出，如果單位採用 ITIL 進行變更管理，則這些修補會被視為「緊急變更」。

建議使用上述 VMware 產品的用戶，應立即依指示更新系統，修補上述漏洞，以免遭到駭侵者利用尚未修補完成的漏洞發動攻擊。

- CVE 編號：CVE-2022-31656 等
- 影響產品/版本：VMware Workspace ONE Access、Indemtity Manager、vRealize Automation 等產品。
- 解決方案：依照 VMSA 的指示，立即修補或處理該漏洞。

- 資料來源：
  1. VMSA-2022-0021
  2. VMSA-2022-0021: Questions & Answers
  3. VMware urges admins to patch critical auth bypass bug immediately

5.7.2、Cisco 修復 VPN 產品中兩個嚴重遠端執行任意程式碼漏洞

網通大廠 Cisco 近日發表資安通報，表示已修復旗下 Small Business VPN 路由器系列中兩個可導致駭侵者用以遠端執行任意程式碼，甚至用來發動 DoS 攻擊的漏洞 CVE-2022-20842 與 CVE-2022-20827。

這兩個漏洞存於上述 Cisco VPN 裝置的 Web 管理介面與 Web 篩選器的資料庫更新功能，發生原因為未能針對輸入資訊進行完整的驗證。這兩個漏洞的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分）。

在 CVE-2022-20842 方面，駭侵者可透過特製的 HTTP 輸入資訊來觸發此漏洞，藉以使用 root 權限於作業系統內達端執行任意程式碼，並可造成系統重新載入，達成 DoS 攻擊的效果。

受到 CVE-2022-20842 影響的 Cisco Small Business 路由器機種，RV340、RV345 1.0.03.26 與較舊版本。

CVE-2022-20827 的方面，駭侵者可以特製的資訊輸入到其 Web 篩選器的資料庫更新功能，來觸發這個漏洞，即可以 root 權限在作業系統內遠端執行任意程程式碼。

受到 CVE-2022-20827 影響的 Cisco Small Business 路由器機種，包括 RV160、RV260 版本 1.0.01.05，以及 RV340、RV345 1.0.03.26 版本。

這兩個漏洞都不會觸發任何反應，也不會出現需要使用者操作的互動，因此駭侵者可在用戶不知情的情形下發動攻擊。不過目前尚未傳出這兩個漏洞遭到駭侵者大規模濫用的消息。

建議使用上述 Cisco Small Business 路由器的用戶，應立即透過更新工具，更新到最新版本韌體，以免未修補的漏洞遭到駭侵者用於攻擊。

- CVE 編號：CVE-2022-20842、CVE-2022-20827
- 影響產品/版本：CVE-2022-22842：RV340、RV345 1.0.03.26 與較舊版本。
  CVE-2022-22827：RV160、RV260 版本 1.0.01.05，以及 RV340、RV345 1.0.03.26 版本。
- 解決方案：
  - CVE-2022-22842：RV340、RV345 升級到 1.0.03.28 與後續版本。
  - CVE-2022-20827：RV160、RV260 升級到 1.0.01.09 與後續版本；RV340、RV345 升級到 1.0.03.28 與後續版本。

- 資料來源：
  1. Cisco Small Business RV Series Routers Vulnerabilities
  2. Cisco fixes critical remote code execution bug in VPN routers

5.7.3、超過 80,000 台以上監視攝影機，因漏洞而曝露於外網

資安研究單位 CYFIRMA 旗下的研究人員，近日發表研究報告，指出有超過 80,000 台海康威視監視攝影機，因內含一個嚴重的指令注入資安漏洞 CVE-2021-36260，使得駭侵者可輕易取得其影像資料，並且取得裝置控制權。

報告指出，駭侵者可利用此漏洞，傳送一個特製的訊息給含有此漏洞的海康威視裝置內的 web 伺服器，從而控制受駭裝置。

據 CYFIRMA 的報告指出，受此漏洞影響而存有弱點的 80,000 多台海康威視攝影機，普遍分布在全球多個國家，其中以中國、美國、越南、英國、烏克蘭、泰國、南非、法國、荷蘭、羅馬尼亞等國的數量最多。

CYFIRMA 說，雖然該漏洞在 2021 年 9 月就由海康威視於新版韌體中予以修復，但由於多數用戶都沒有經常更新 IoT 裝置韌體的習慣，導致至今仍有超過 100 國、2,300 以上使用該品牌產品的單位，其裝置都還在使用有漏洞的舊版韌體，造成極大的資安風險。

在 2021 年 12 月，一個使用 Mirai 惡意木馬程式碼的 Moobot 僵屍網路，

就曾利用此漏洞與過去在海康威視裝置中發現的其他漏洞，發動大規模的 DDoS 攻擊；而在 2022 年 1 月，美國資安主管機關 CISA 也將 CVE-2021-36260 列為近來最常用於攻擊的資安漏洞之一。

建議採用各種連網 IoT 裝置的用戶，應經常注意資安單位與原廠發布的資安通報與更新消息，一但有相關的軟硬體更新發布，即應立即更新；切勿在設備安裝完成後就棄之不顧，這些裝置就很容易成為遭到各式駭侵攻擊的進入點。

- CVE 編號：CVE-2021-36260
- 影響產品/版本：請見海康威視資安通報網頁。
- 解決方案：更新至最新版本韌體。

- 資料來源：
  1. Security Notification - Command Injection Vulnerability in Some Hikvision products
  2. Hikvision Surveillance Cameras Vulnerabilities

5.7.4、Apple 修復 iPhone 與 Mac 上 2 個 0-day 漏洞

Apple 日前發表新版 iOS 15.6.1、iPadOS 15.6.1 與 macOS Monterey 12.5.1，修復兩個已遭大規模用於攻擊的 0-day 漏洞；所有 iPhone、iPad、Mac 用戶應立即更新，以避免遭駭侵者透過未修補漏洞發動攻擊得逞。

獲得修復的 2 個 0-day 漏洞，都存在於 iOS、iPad OS 和 macOS 中。第一個漏洞為 CVE-2022-32894，存於作業系統核心內，是一個越界資訊寫入漏洞；駭侵者可透過該漏洞，以作業系統核心權限執行任意程式碼。

由於核心權限極大，因此取得核心權限執行的惡意程式，幾乎可以毫無限制地取用任何系統與軟硬體資源；亦即完全控制受駭的裝置。不過駭侵者需取得本機使用權，才能誘發此漏洞。

CVE-2022-32894 的 CVSS 危險程度評分為 8.4 分，危險程度評級為「高」。

第二個 0-day 漏洞 CVE-2022-32893 則發生在 iOS、iPad OS、macOS 中 WebKit 組件之中，該組件是系統預設瀏覽器 Safari 的核心，也會用在各種能

存取 web 資源的 app 內。漏洞本身也是一種越界資訊寫入錯誤，發生於 Safari 對 html 內容的處理過程。

Apple 指出，該漏洞可讓駭侵者以特製的惡意網站來誘發，並藉以執行任意程式碼。該漏洞的 CVSS 危險程度評分亦為 8.4 分，危險程度評級為「高」。

此外，Apple 也指出，這兩個 0-day 漏洞顯然已遭駭侵者大規模濫用於駭侵攻擊之上，惟目前仍無這兩個漏洞造成任何損害或具體攻擊事件的情資。

由於 iPhone、iPad 與 Mac 的使用人數眾多，為避免用戶遭到駭侵者利用這些未修補漏洞發動攻擊，建議用戶應立即自官方管道更新作業系統。

- CVE 編號：CVE-2022-32894、CVE-2022-32893
- 影響產品/版本：執行 macOS Monterey 的各型 Mac 電腦、iPhone 6s 與後續機種、iPad Pro 全機種、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第 7 代。
- 解決方案：升級至 macOS Monterey 12.5.1 與後續版本、iOS 15.6.1 與後續版本、iPad OS 15.6.1 與後續版本。

- 資料來源：
  1. About the security content of macOS Monterey 12.5.1
  2. About the security content of iOS 15.6.1 and iPadOS 15.6.1
  3. Apple security updates fix 2 zero-days used to hack iPhones, Macs

第 6 章、 資安研討會及活動

俄烏戰爭對未來網路衝突的意涵	
活動時間	2022 年 9 月 13 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/20220913/
活動概要	 **主辦單位：TWNIC、Nii、TWIGF** 俄羅斯與烏克蘭為期數個月的衝突期間，除砲火外，在網路空間中的攻防也同樣激烈；甚至在俄羅斯軍隊入侵前數小時，烏克蘭就開始遭到前所未見的惡意軟體襲擊，由俄羅斯所支持的駭客集團鎖定烏克蘭的基礎設施、政府機構、銀行資訊系統進行破壞所竊取資料；烏克蘭也有所反擊，而在包括網路義勇軍及盟國的加入後，讓整個網路戰場變得更為複雜。 在網路上的雙邊爭鋒相對也不只是透過惡意軟體，還包括以假訊息為基礎的資訊戰攻防。大量假訊息傳送至烏克蘭前線的士兵們，以及俄羅斯境內的媒體，製造了假的「真相」，也帶來了混淆、混亂跟恐慌。 有人認為，俄烏戰爭鞏固了未來全球武裝衝突中都將包含網路戰的論述；也有人認為未來網路戰會因此更為複雜與具破壞性，而網際網路與社群媒體也將被武器化。 本場次邀請三位專家介紹有關網路在這場俄烏戰役中所扮演的角色，包括中性的網路與社群媒體如何被武器化，未來有關網路衝突國際規則可能的發展方向，以及這些變化對台灣社會、政府與民眾的啟示又為何？

	時間：2022 年 9 月 13 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 14:05-14:45 專題演講一「俄烏戰爭下的網路駭侵樣貌與經驗學習 」：楊千旻法務協理 (台灣微軟公司) 14:45-15:25 專題演講二「俄烏衝突中被武器化的社群媒體 」：游知澔 共同主持人 (IORG 台灣資訊環境研究中心) 15:25-16:05 專題演講三「 俄烏網路衝突下的國際法發展可能 」：楊長蓉 博士 (國防安全研究院國防戰略與資源研究所)

面對地緣政治網路攻擊，全面檢視公部門與關鍵基礎設施資安曝險	
活動時間	2022 年 9 月 14 日(三) 14:00-15:30
活動地點	線上
活動網站	https://www.informationsecurity.com.tw/seminar/2022_imperva/index.htm
活動概要	 **主辦單位：資安人** 8 月對於資安從業人員特別公部門絕對是緊繃的一個月。從美國眾議院議長裴洛西 2 日訪台後，中央機關、警政、鐵路、電力、金融單位與重要企業都陸續遭到網路攻擊。台電更證實其外網 8 月 3 日攻擊次數就高達 490 萬次，已超越 6、7 月總攻擊次數。在財團法人台灣網路資訊中心 (TWNIC) 的監控下，在 8 月 2 日

	至 3 日間，.tw 國家頂級網域 DNS 最大查詢量每秒約 8 萬 5 千餘筆，其中近 75% 訊務量為惡意攻擊封包。各種現象顯示，網路攻擊、資訊戰爭已經是地緣政治衝突中影響民生最關鍵領域之一。 而駭客組織 APT 27 也宣稱掌握有台灣設備的零日漏洞、政府資料和大量連網設備資料。這是一場持久戰，身為資安的一分子，資安人媒體希望透過這次論壇呼籲大家檢視這次的攻防，關注系統與交換資料安全，及關鍵基礎設施的防護。大家一起聯防，持續提升資安防禦之應變能力，強化國家整體韌性。

線上資安專題講座-金融資安政策與人才培育	
活動時間	2022 / 09/ 17（六） 14:00 - 16:00
活動地點	線上舉辦(活動前一天會提供會議連結至報名者的電子信箱)
活動網站	https://isipevent.kktix.cc/events/e58d0573-copy-6
活動概要	 **主辦單位：教育部先進資通安全實務人才培育計畫** 教育部先進資通安全實務人才培育計畫在 09/ 17（六） 14:00 - 16:00，舉辦「線上資安專題講座」，希望落實資安觀念向下扎根，並鼓勵年輕學子投入資訊安全領域，本次邀請金管會/主任秘書-蔡福隆，將分享「金融資安政策與人才培育」的專題講座，趕緊手刀手報名吧！錯過可惜！！

	【活動時程表】 13:30 - 14:00 講師、與會者報到入場 14:00 - 14:05 活動開場 14:05 - 15:30 專題講座 15:30 - 15:50 QA 座談時間 15:50 - 16:00 結語

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** 9/20 - 9/22 台北南港展覽二館 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。

TWIGF 2022 網路韌性的挑戰與契機：地緣政治、WEB 3.0 與中介者治理	
活動時間	2022/9/27(二)、9/28(三)
活動地點	台北文創 6F
活動網站	https://www.igf.org.tw/?page_id=7893
活動概要	 **主辦單位：TWIGF、TWNIC** 臺灣網路治理論壇是一個將網路多方利益關係群體，包括政府、學術社群、技術社群、公民社群、民營企業等，聚集在一起共同討論網路公共政策的溝通互動平臺。自 2015 年首屆論壇起，在不斷激發各社群參與力量之下，每年持續推動舉辦，藉此促進和鼓勵網路公共政策在跨領域或部門(國際/國內)或多方利害關係人的群體討論。

	2022 年論壇議題 主題：網路韌性的挑戰與契機：地緣政治、WEB 3.0 與中介者治理 子題： ➢ 地緣政治的衝突與回應 ➢ 新興技術與 Web 3.0 ➢ 網路關鍵資源與安全 ➢ 人權：隱私權、資料保護與新興議題 ➢ 中介者治理

關鍵基礎設施實作課程(含攻防演練實作)	
活動時間	2022/09/27 09:40~16:40
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 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) 主辦單位：經濟部工業局 執行單位：財團法人資訊工業策進會 課程聯絡人：李小姐 / doralee@iii.org.tw / 02- 66073299

2022 玉山 · 安碁資訊資安論壇【企業營運制勝關鍵，資安治理創價佈局】	
活動時間	2022-09-27(二) 14:00 ~ 16:20
活動地點	台灣台北市中正區中山南路 11 號 (張榮發基金會國際會議中心 602 會議室)
活動網站	https://www.accupass.com/event/2208180737041036993111
活動概要	 **主辦單位：台灣玉山科技協會、安碁資訊** 面對科技風險的瞬息萬變，企業如何在既有資安投資下維持企業既有防禦優勢，以及如何兼顧資料保護與企業營運目標。 為此，【台灣玉山科技協會】與【安碁資訊(股)公司】特別辦理資安論壇，由【安碁學苑】講師群從資安治理的角度，探討企業

	挑戰與對策，並且分享資安防禦及資料保護治理框架實務做法，透過企業整體資安的設計與規劃，和資訊風險決策的敏捷作法，以其協助企業提升治理單位對資訊安全狀態的可視性，進行更有效的資訊安全管理與投資，並使企業得以遵循外部要求，貢獻價值與治理單位及其利害相關者，以達到企業永續發展的韌性。 推薦與會人員 | 企業資訊安全長 (CISO) 企業資訊安全專責單位主管 (BISO) 企業資訊長 (CTO) 企業資訊安全主管 (ISO)

《歐立威科技 2022 研討會》9/29|Elastic Security：監測 x 告警，揪出潛在威脅！	
活動時間	2022-09-29(四) 11:00 ~ 12:00
活動地點	線上
活動網站	https://www.accupass.com/event/2208310346161209105423F
活動概要	 **主辦單位： Elastic NV、歐立威科技** 近年來企業面臨資訊安全威脅層出不窮的困境，亟需完整的資安解決方案杜絕潛在風險。 Elastic 參與多年 MITRE ATT&CK 評比，提供企業專業的資訊安全防護，融合了機器學習邁向 AI Security 自動化。企業僅需安

	裝 Elastic Agent 並且可即時收容資訊安全所需資料，進行資訊安全管理、自動化監測與告警，減低企業資訊安全風險與管理成本。 歐立威科技攜手 Elastic 參展 2022 台灣資安大會，特別舉辦本場資安研討會，介紹 Elastic Security 資訊安全的最佳實踐，更全面地介紹 Elastic 最新的資安解決方案，歡迎報名本場活動！ 活動時間：2022-09-29(四) 11:00 ~ 12:00 此活動為線上活動，購票後可於票券頁進入直播連結。

臺灣資安大會_ISIP 校友活動	
活動時間	2022 / 09/ 20 (二) 13:30 - 16:30
活動地點	南港展覽館 2 館 4 樓 Cyber Talent 專區
活動網站	https://isipevent.kktix.cc/events/52fe828d-copy-1
活動概要	 **主辦單位：教育部先進資通安全實務人才培育計畫** 「臺灣資安大會 ISIP 校友活動」來囉！在 CYBERSEC 2022 臺灣資安大會活動中，教育部先進資通安全實務人才培育計畫將舉辦臺灣資安大會 ISIP 校友活動，誠摯地邀請校友們一同參與，本次活動將邀約 6 位傑出校友於活動中分享他們資安職涯的心路歷程，歡迎校友們踴躍參加！

	【活動時程表】 13:30-14:30 長官及貴賓致詞 14:30-14:50 教育部先進資通安全實務人才培育計畫-計畫簡介 14:50-16:30 教育部先進資通安全實務人才培育計畫傑出校友-職涯經驗分享 Check Point/羅煜賢 中華資安國際股份有限公司/王凱慶 杜浦數位安全股份有限公司/莊人傑 群暉科技股份有限公司/林思辰 奧義智慧科技股份有限公司/黃禹程 戴夫寇爾股份有限公司/林昆立 (依照單位名稱首字筆劃排序)

第 7 章、 TVN 漏洞公告

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

樂衍 樂薪人資管理系統 - Hard-coded password	
TVN / CVE ID	TVN-202208001 / CVE-2022-38116
CVSS	9.8 (Critical)
影響產品	樂衍 樂薪人資管理系統 2022/6/6 前的版本
問題描述	樂薪人資管理系統以明文方式 Hard-coded 資料庫的帳號密碼於網頁原始碼中，使遠端攻擊者不須權限，可以查看與修改系統資料，甚至中斷服務。
解決方法	詢問樂衍相關漏洞修補建議
公開日期	2022-08-30
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6460-2bb02-3.html**

HGiga OAKlouds 行動入口網 - SQL Injection	
TVN / CVE ID	TVN-202208003 / CVE-2022-38118
CVSS	8.8 (High)
影響產品	OAKlouds 行動入口網(OAKSv2、OAKSv3)會議室管理模組，受影響之套件版號： OAKlouds-mol_metting-2.0 <= OAKlouds-mol_metting-2.0-163 OAKlouds-mol_metting-3.0 <= OAKlouds-mol_metting-3.0-163
問題描述	OAKlouds 行動入口網之會議室系統功能參數未對使用者輸入進行驗證，遠端攻擊者取得一般使用者權限後，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	OAKlouds 行動入口網(OAKSv2、OAKSv3)會議室管理模組，修正的套件版號： OAKlouds-mol_metting-2.0 >= OAKlouds-mol_metting-2.0-164 OAKlouds-mol_metting-3.0 >= OAKlouds-mol_metting-3.0-164

公開日期	2022-08-30
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6461-25c4b-3.html

沛盛資訊 OMICARD EDM 行銷發送系統 - Path Traversal-1	
TVN / CVE ID	TVN-202206009 / CVE-2022-32963
CVSS	7.5 (High)
影響產品	沛盛資訊 OMICARD EDM v5.8~v6.0
問題描述	OMICARD EDM 轉發檔案功能存在 Path Traversal 漏洞，遠端攻擊者不須權限，即可利用此漏洞繞過身分認證機制，讀取任意系統檔案。
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-151-6371-05bdc-3.html

第 8 章、 2022 年 8 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。

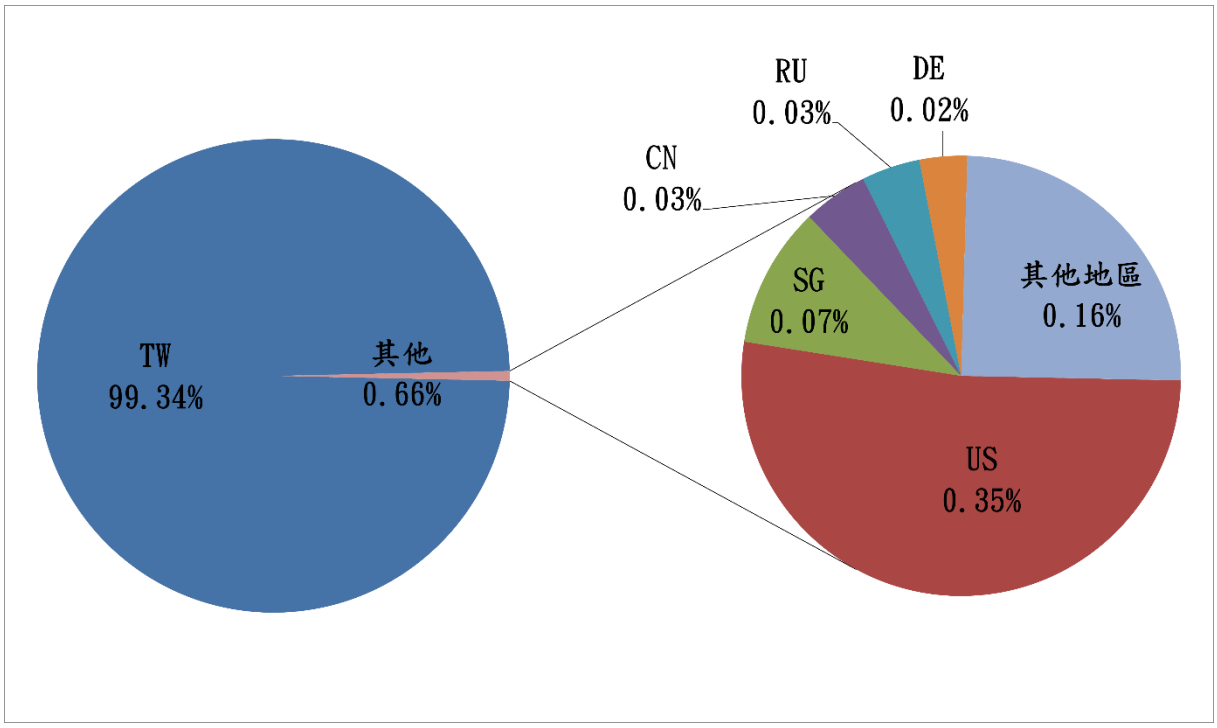


圖 1、分享地區統計圖

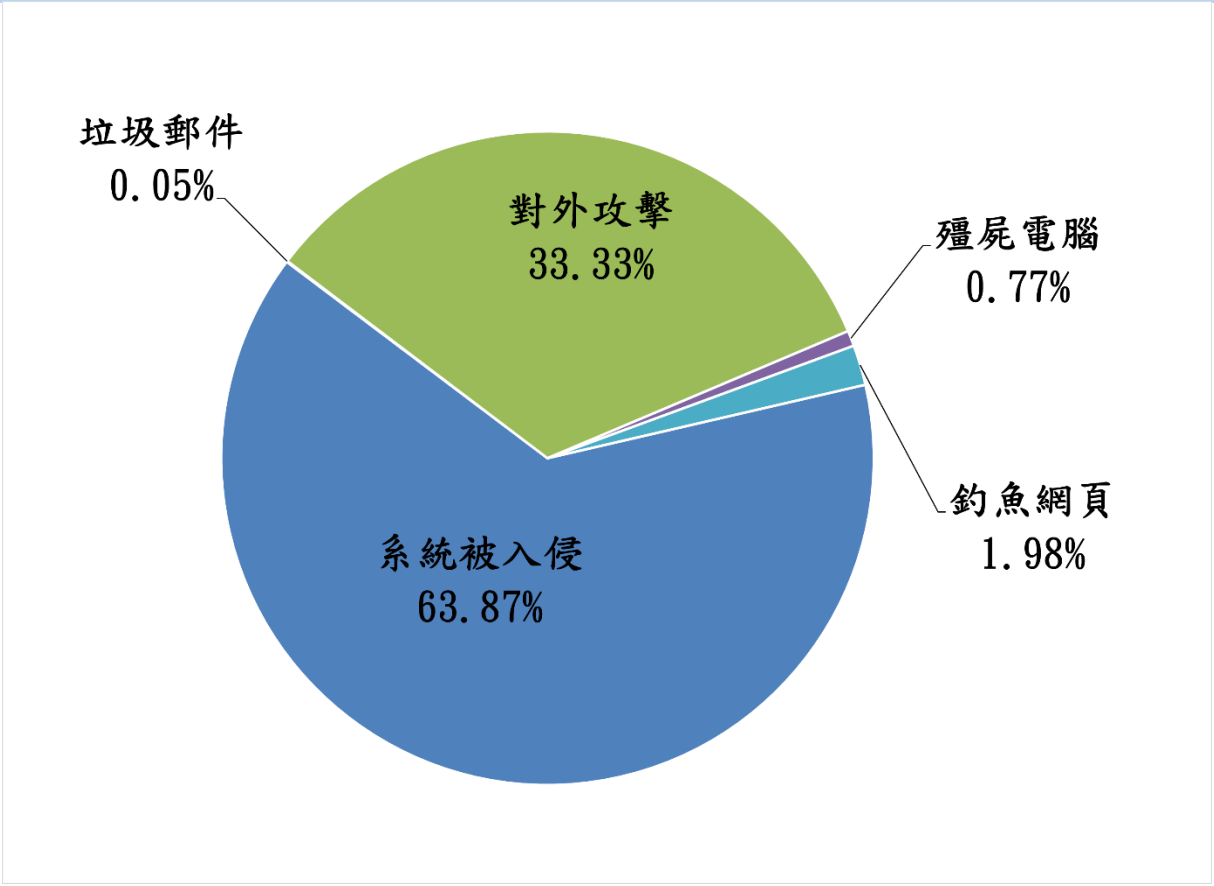


圖 2、分享類型統計圖

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 9 月 8 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**