TWCERT/CC 資安情資電子報

2022 年 1 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在行政院資通安全處及國家通訊傳播委員會指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 5 章節：

第 1 章、封面故事：上月 TWCERT/CC 所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第 2 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、新興應用資安、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題及軟硬體漏洞資訊。

第 3 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 4 章、TWCERT/CC 為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN) 平台之漏洞嚴重程度前五的產品漏洞資訊。

第 5 章、資安情資分享概況：將上月 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

目錄

第 1 章、 封面故事

「COVID-19」Emotet 社交工程攻擊概述與防範建議

- 社交工程是一種利用人性弱點，透過釣魚郵件、釣魚網站、電話、通訊軟體或社群媒體等方式誘騙使用者上當，以竊取資訊、取得權限，甚至植入惡意程式於受害主機中，以獲取不法利益。
- Emotet 為新型的社交工程攻擊手法，其散布惡意程式的方式以寄送釣魚郵件為主，郵件主旨從過往如發票、轉帳資訊等金融訊息，逐漸發展成結合時事，透過使用者好奇或恐慌的心理，成功達成感染主機之目的。
- Emotet 在逐漸演化的過程中，發展出極難辨識真偽的假冒回覆信件釣魚手法。主要是由於 Emotet 會竊取受害者信箱中之電子郵件，並將其附上帶有惡意程式的附件後，偽裝成受害者回傳給寄件者，在此狀況下寄件者通常在收到回信後不會懷疑，相當容易便落入駭客的陷阱中。
- 2020 年 1 月底，駭客利用震驚全球的「嚴重特殊傳染性肺炎(COVID-19)」疫情，將目標設定為疫情較嚴重之日本，並且偽冒成日本的衛生單位，要求使用者下載附件，以取得最新疫情內容或防護措施，在民眾對疫情的恐慌之下，相當多的民眾都受到了 Emotet 惡意程式的侵駭。
- 為了防範社交工程攻擊，除了不點擊不明連結及下載附件外，更必須確認郵件、電話、訊息甚至來訪者的身分，避免駭客偽冒他人進行社交工程攻擊。
- 電子郵件系統可透過寄件者政策框架及網域驗證郵件，確認使用者身分及

信件的完整性，並透過網域型郵件驗證、報告與一致性機制處理釣魚郵件，減少使用者受騙之機率。

- 對於近期透過「COVID-19」進行的 Emotet 社交工程攻擊，除了需進行相關社交工程防護機制，在收到相關字樣的郵件時，務必提高警覺才能不受騙上當。

一、簡介

社交工程(Social Engineering)，最主要的攻擊模式為駭客透過電子郵件誘騙使用者點擊信件中之不明連結或圖片等，當使用者點擊後，會被導入惡意的釣魚網站中，或將惡意程式植入使用者裝置中，除竊取資料外更可操控裝置以獲取更多的利益。

在不計其數的社交工程惡意程式中，Emotet 為最知名且嚴重的惡意程式之一，會透過釣魚郵件散布惡意程式，其釣魚郵件往往是透過節日、時事等主旨，誘騙使用者點閱後感染。而近期更發現最新的 Emotet 社交工程攻擊，此攻擊是利用目前全球矚目的「嚴重特殊傳染性肺炎(COVID-19)」疫情，透過民眾的恐懼心理，以大幅提升 Emotet 惡意程式的感染率。

Emotet 最早被發現是在 2014 年，當時是透過銀行轉帳或傳輸發票等資訊，提供一網路連結，由於其涉及金融及交易方面的資訊，許多使用者為確保其帳戶和資金的正確性，不疑有他地點擊該不明連結，於是被導入惡意網站並下載安裝 Emotet 惡意程式。

Emotet 的第二版是於 2014 年第三季被發現，其主要是增加了自動轉帳系統(Automatic Transfer System, ATS)功能，可從受害者的金融帳戶中自動竊取資金。在 2015 年 1 月，Emotet 推出了第三個版本，主要攻擊目標為瑞士銀行。此版本增加了避免受到偵測及躲避檢測的功能。2015 年 4 月又提出了第四個版本，主要是針對逐漸興起的雙重認證機制進行規避

2017 年 8 月再次被偵測到新的 Emotet 變種惡意程式。而此次的 Emotet 變種，不似過往僅針對銀行業進行攻擊，而是不侷限任何行業，包括製造

業、食品業及醫療業都受到 Emotet 的攻擊。此外，其攻擊的主要目標地區為美國、英國及加拿大。

而後，Emotet 發展及改版愈發迅速，除了從最初的銀行木馬轉變為針對其他行業或組織的嚴重威脅性惡意程式外，更在發送大量釣魚郵件時修改其郵件主旨和語系。2019 年 4 月 12 日至 16 日期間，Emotet 被偵測到將轉為中文語系的釣魚郵件傳送給台灣地區，使得 2019 年上半年期間，Emotet 成為對台灣企業影響最為嚴重的十大惡意程式之一。

除了地理位置的擴張外，經過數次改版後，Emotet 開始竊取受害主機中的電子郵件內容，並假冒收到信件之受害者寄送回覆信件給寄件人，由於該信件確實為寄件人所發出，且信件內容大抵相同，因此許多收到回覆信件的使用者便不疑有他，點擊並下載信件中的附件，導致 Emotet 惡意程式植入其中並以此將惡意程式擴散得更為廣泛。

隨著 Emotet 不斷地更新其功能，除了針對發票、運輸、金融項目等方式以及寄送假冒的回覆郵件外，Emotet 的釣魚信件開始針對節日或活動，吸引有興趣的使用者點擊其連結。最近最嚴重的，便是駭客透過「嚴重特殊傳染性肺炎」、「COVID-19」、「新型冠狀病毒」、「Coronavirus(冠狀病毒)」等作為主旨，寄送給民眾，假冒提供民眾疫情的資訊及防護措施等，實則誘騙使用者點擊並下載附件檔案，以達到感染和傳播 Emotet 惡意程式之目的。

二、「COVID-19」Emotet 社交工程攻擊

(1)「COVID-19」Emotet 攻擊概述

2020 年 1 月，嚴重特殊傳染性肺炎(Coronavirus Disease, COVID-19)被世界衛生組織(World Health Organization, WHO)宣布為國際關注公共衛生緊急事件，受到全球的矚目，各國紛紛提出相關防疫機制，民眾亦紛紛採取消毒及防護措施。駭客便利用此次的疫情散播相關的網路釣魚訊息，駭客為達到最大的效益，將其攻擊目標設定為疫情相對嚴重的日本地區，透過大眾對疫情

揣揣不安的心態，提升釣魚郵件的成功率。

由於此次攻擊目前主要針對日本地區，其電子郵件中都以日語撰寫，該信件中則有附上一 word 類型之文件，內文會告知使用者，此附件為針對疫情的通知，請收件者務必檢查附件檔案中的內容。當使用者下載並開啟該附件檔案後，附件中的 VBA 巨集腳本將會自動安裝 Emotet 的下載器，且由於該動作均於後台運行，因此使用者往往不知道主機已經安裝並感染了 Emotet 惡意程式。而在主機遭受感染後，將會下載並安裝更多的惡意程式以竊取機敏資訊如憑證、瀏覽紀錄及重要文件等，以及針對金融帳戶進行惡意行為，導致使用者金融上的損失，甚至還會透過受害主機中的聯絡人和歷史的通訊紀錄將惡意程式傳播給更多人。

(2)「COVID-19」Emotet 攻擊比較

對於一般的社交工程手法而言，其觸及受害者的方式相當多元，其中以網路釣魚的電子郵件最為盛行。以往的釣魚郵件是用同樣的主旨、內容，透過殭屍網路等方式大量發送給受害者。然而，Emotet 的主旨會隨著時事變化，甚至透過受害者的帳號傳送釣魚郵件給聯絡人中的其他使用者，以提升對方對該釣魚信件的信任程度。此外，Emotet 甚至還會偽裝成受害者身分回覆該信件給寄件者，並在信件中附上帶有惡意程式的附件，使得對方收到信件並確認是當初所寄送之信件後，便不疑有他地下載其附件，導致 Emotet 的感染效率大幅上升。而受害者在遭到 Emotet 惡意程式感染後，其資料竊取方式是以偵測使用者網路流量及其內容為主，由於該種偵測方式並無明顯造成使用者提升警覺性，且該惡意程式的相關運作都於後台執行，大多數的使用者對於自身已遭受惡意程式感染一無所知。

由於過往的 Emotet 釣魚郵件是以金融類型之主旨為主，大部分的國家、企業或組織都以「發票」、「付款」、「資金變更」等部分進行防護，在針對新冠狀病毒事件所散布之釣魚郵件，是以大眾對病毒疫情的恐懼心理誘騙上當，許多防護就顯得較為不足，其詐騙的成功率也因此提高許多。

三、「COVID-19」Emotet 社交工程攻擊之防護

對於 Emotet 惡意程式的社交工程攻擊。除了一般社交工程之防範方式外，由於 Emotet 散布惡意程式的方式為透過郵件中的附件，因此應阻擋容易帶有惡意程式的檔案，以及禁止帶有郵件系統無法掃描的如 ZIP 壓縮檔的信件，主機也需安裝防毒軟體、防火牆以及電子郵件篩選功能之相關軟體或系統，並定期更新以維護其最佳的防護能量。除此之外，為防範 Emotet 藉由 Office 巨集感染受害主機，因此針對 Office 系統應禁止系統自動執行巨集。

由於 Emotet 會偽裝成回覆信件，導致對方在毫無戒心的情況下感染惡意程式，為避免受騙上當，可透過各種防範機制，驗證電子郵件寄送者的身分，確保信件內容完整性，以大幅降低偽冒他人網域發送釣魚及垃圾郵件的威脅，自然亦減少 Emotet 釣魚郵件帶來的資安問題。

對於組織或企業內的管理者而言，亦須針對一般社交工程進行防範，例如提供員工資安教育訓練，減少甚至避免釣魚郵件的威脅。企業所使用的電子郵件系統必須能過濾垃圾郵件，以減少員工或相關人員觸及釣魚郵件並受騙之機率。此外，企業需針對所有員工設定開放權限等級，並以最低授權為原則，以提供員工足以支應日常作業之授權即可。同時也將內部的網路區隔，避免感染後擴散。除此之外，企業可採用全面性的防護系統，將企業的主機、網路、伺服器、路由器等都涵括於防護系統中，進行全方位的資安防禦，減少社交工程帶來的威脅。

若使用者真的不幸感染 Emotet 惡意程式，則應立即將裝置中安全之檔案進行備份，並針對該裝置中使用的電子郵件信箱及聯絡人發出警訊，提醒相關連絡人避免受騙上當。受感染裝置中使用的郵件信箱、帳號密碼等資訊，都應修改或刪除，避免資料外洩後遭到駭客操縱。

此外，由於 Emotet 本身具有在組織內傳播之能力，因此除了必須立即將確認受感染裝置隔離外，組織內的其餘裝置都應檢查是否遭到波及。而 Emotet 除自身惡意行為外，也會在侵入裝置後自動下載更多的惡意程式，因

此，不僅需檢測 Emotet 感染與否，同時也必須檢測其他相關可能的惡意程式，並且立即進行處理。

由於 Emotet 之釣魚郵件及功能越來越貼近生活，往往以生活中平凡無奇，或是受到特別矚目的事件作為誘餌，誘騙使用者點擊不明連結或下載附件，以達到駭侵之目的。因此，使用者必須要有一定的危機意識，即便該電子郵件看似正常，或是能夠對使用者產生利益或威脅等，都應仔細審視、謹慎處理。否則若使用者沒有社交工程的警覺性，即便使用多完善的防護系統、多強大的防火牆，都可能被駭客透過名為「人」的漏洞趁虛而入。

四、分析與建議

(1) Emotet 會以節日或重大事件做為信件主旨，近期則利用 COVID-19 疫情爆發事件，針對大眾恐慌的心態，誘騙使用者下載附件後感染惡意程式，甚至竊取受感染主機中的信件內容，假冒成受害者，將該郵件附上帶有惡意程式的附件後，回覆給當初的寄送者，導致寄送者難以察覺該郵件曾遭到偽冒，而成為惡意程式的下一個感染者。

(2) 在眾多社交工程攻擊中，最為常見的攻擊手法為透過釣魚郵件誘騙使用者落入陷阱，因此，建議可透過電子郵件系統中的相關防護機制，確認寄送者的身分，確保信件內容完整性，並採取適當處理方式，如此方可減少使用者在難以辨識釣魚郵件的情況下蒙受損失。

(3) 在近期透過 COVID-19 進行的 Emotet 社交工程攻擊中，除了需進行相關社交工程防護機制外，當使用者收到 COVID-19 相關字樣的郵件時，務必提高警覺不受騙上當。同時也盡量關閉 Office 系列的自動啟用巨集功能，避免 Emotet 惡意程式透過巨集感染使用者裝置。

(4) 若不幸遭到 Emotet 感染，建議使用者應立即將安全之文件進行備份、修改主機中電子信箱的密碼等資訊，並且將受感染主機與其他主機或設備隔離，避免惡意程式透過網路傳播出去，招致更多的主機或設備遭受攻

擊。

(5) 由於社交工程主要是透過「人」進行攻擊，因此，不論是何種社交工程攻擊，都應提升使用者的資安意識，提供足夠的知識進行驗證及防護，避免因人為疏失造成額外損失。並且 Emotet 釣魚郵件往往是偽裝成知名人物、企業或政府單位的身分進行攻擊，因此，必須提供民眾對釣魚郵件的辨識方法，例如特殊符號、內容等，以確認該郵件為真正單位所寄送。

(6) 由於社交工程等攻擊手法不斷演進，因此不論是企業、組織或政府單位，都建議應隨時追蹤、更新資安訊息，定期提供相關人員參考，提升其資安防護意識，避免成為攻擊目標時措手不及。

(7) 針對常見且嚴重的惡意程式，建議應定期檢測或從資安組織公開資訊中更新其最新狀態，以加強主機及系統的防護，避免在突如其來大量的惡意程式攻擊下成為受害者。

(8) 當天災或人禍發生時，許多駭客會濫用大眾的愛心、恐慌、擔憂進行詐騙或攻擊，因此當全球重大事件發生時，建議相關資安單位或組織應立即設想駭客可能透過該事件進行的攻擊模式，並以此告知相關單位或大眾，進行即時性的防護及提高防護意識。

(9) 當資安事件爆發或在其他地區爆發時，建議相關單位除了進行立即性的資安意識培訓及宣導，亦必須提供當使用者不幸遭受攻擊時的解決辦法，以避免受害範圍擴散。

- 資料來源：

1. 何謂社交工程？應如何防範?
2. 什麼是社交工程（social engineering ）陷阱/詐騙?
3. Combining Social Engineering & Malware Implementation Techniques
4. Alert (TA18-201A) Emotet Malware

5. New Banking Malware Uses Network Sniffing for Data Theft
6. The Banking Trojan Emotet: Detailed Analysis
7. Emotet
8. EMOTET Returns, Starts Spreading via Spam Botnet
9. Threat Actor Profile: TA542, From Banker to Malware Distribution Service
10. Threat Trends Analysis Report
11. 武漢肺炎口罩之亂, 全聯遭冒用,詐騙集團成立多個假粉專騙個資
12. fe23b30a9296477557f027d4710e81eb1b08d65a1a83b6d81a4ed6128ed6e2a0
13. Coronavirus Goes Cyber With Emotet
14. Increased Emotet Malware Activity
15. マルウエア Emotet への対応 FAQ
16. Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks
17. Increased Emotet Malware Activity
18. 為郵件系統安全把關，新增 SPF, DKIM 和 DMARC 設定以避免有心人士的釣魚攻擊
19. 武漢肺炎疫情通知信,竟是駭客發的!

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、大型釣魚攻擊研究指出，企業經常舉辦的各種資安教育訓練有反效果

瑞士研究單位針對某大企業 14,733 名員工進行的長期研究指出，企業經常採用的釣魚郵件攻擊教育訓練，不但無法讓員工對不明郵件提高警覺，反而會使員工更容易上鉤。

瑞士蘇黎世聯邦理工學院（ETH Zürich）資訊系的研究人員，近來發表一篇關於企業員工與釣魚郵件的研究報告。該報告針對某大企業 14,733 名員工進行的長期研究指出，企業經常採用的釣魚郵件模擬攻擊，不但無法讓員工對不明郵件提高警覺，反而會使員工更容易上鉤。

該研究計畫係與一間匿名大型企業合作進行，針對企業內部的 14,733 名員工，進行長達 15 個月的研究；研究主題希望能夠闡明下列四個問題：哪類員工容易在釣魚攻擊中上鉤、長期來看脆弱點如何演變、各種為提升資安意識進行的內部嵌入式訓練與警告的有效程度，以及員工是否能夠幫助發現釣魚攻擊活動。

報告指出幾個與過去研究類似的結論，但也有一些與過去的理解相反的新發現。

其中一個與過去不同的發現，是這次研究的結果指出，員工性別和釣魚郵件的上鉤率並無相關，而過去的研究認為男性比女性員工更容易上鉤。

此外，這次研究也發現，較年輕與較年長的員工，都容易受到釣魚郵件誘惑而點擊惡意連結；18-19 歲的比例最高，其次是 50-59 歲員工，點擊率最低的是 20-29 歲。

另外研究也指出，工作上必須大量使用客製化軟體，進行各種高重覆性工作的員工，也比較不常使用電腦，或使用的軟體與服務較多樣化的員工，更容易成為釣魚攻擊的破口。

本研究也證實過去的研究，也就是曾經上鉤的員工，有高達 32.1% 會再次點擊惡意連結或開啟含有惡意程式的郵件附檔。

本研究證實了各企業經常舉辦的各種釣魚攻擊防範措施，包括發送摸擬釣魚攻擊，以及非強制性的資安教育訓練，不但無法提高員工的警覺，反而會讓惡意連結的點擊次數上升。

報告也說，如果企業提供員工檢舉釣魚郵件的機制，最高會有近 80% 的釣魚郵件攻擊遭到員工檢舉；這將可大大提高企業防範釣魚攻擊的能力。

- 資料來源：
  1. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study
  2. Large-scale phishing study shows who bites the bait more often

2.1.2、調查報告指出，多數美國企業員工認為密碼造成其生產力下降

資安廠商近日針對密碼對企業員工生產力影響程度發表調查報告，指出多數美國企業員工的生產力深受密碼的影響，有高達 60% 員工認為密碼造成生產力的下降。

資安廠商 Axiad 近日發表一份調查報告，報告針對密碼對企業員工生產力影響程度與曾面進行各項調查，結果指出多數美國企業員工的生產力深受密碼的影響；有高達 60% 員工認為密碼造成生產力的下降。

該報告名為「Axiad 2021 年秋季密碼與生產力調查」（Axiad Fall 2021 Passwords and Productivity Survey），針對美國境內 2,000 名辦公室工作者進行問卷調查，以了解其工作現場上的密碼政策與實作，對其生產力的影響程度。

報告呈現了幾個重要的數字，分列如下：

- 60% 受訪者表示，企業的認證程序曾經造成他們工作的障礙；
- 59% 受訪者曾因無法存取工作用電腦，而必須向 IT 人員求助；
- 48% 受訪者表示曾被限制而無法使用各種生產力工具或工作用通訊軟體（如 Slack）；
- 48% 受訪者表示曾經忘記過登入系統用的密碼；
- 用於解決工作上登入問題的平均所需時間為 4 小時 43 分鐘；
- 15% 受訪者花了超過 9 小時以上，才解決無法登入工作用系統的問題；

- 67% 受訪者知道多重驗證可以當做密碼替代工具；
- 46% 受訪者表示其公司的 IT 人員，從未要求員工使用密碼之外的登入驗證機制；
- 63% 受訪者認為密碼是許多工作障礙的根源；
- 43% 受訪者認為密碼很麻煩；
- 35% 受訪者認為密碼造成潛在資安危機；
- 46% 受訪者認為設定新密碼對其記憶力是一種困難的挑戰；
- 45% 受訪者認為設定新密碼令人感到挫折；
- 35% 受訪者表示很難設定出強度足夠的密碼。

總體來說，報告指出目前以密碼為主的資安控管做法，會令多數員工感到挫折；結果就是使得員工難以適從，導致生產力的下降。

雖然資安專家大力呼籲使用密碼管理工具的好處與重要性，但還是有許多人不知或不會使用，反而選擇寫下密碼，造成另一重資安風險。。

- 資料來源：
  1. Employees say passwords are preventing them from doing their jobs
  2. Do passwords impact productivity?

2.2、新興應用資安

2.2.1、駭客利用盜版 Windows、Office 註冊機 KMSpico 夾帶惡意軟體 CryptBot

資安廠商發現有駭侵者透過一個名為 KMSpico 的惡意軟體，意圖竊取 Windows 用戶電腦中的加密貨幣資產。

資安廠商 Red Canary 旗下的資安專家，最近發現有駭侵者透過一個名為 KMSpico 的惡意軟體發動大規模攻擊，意圖竊取 Windows 用戶電腦中的加密貨幣資產。

Red Canary 的資安專家指出，KMSpico 入侵 Windows 電腦的方式，是透過破解 Microsoft Windows 與 Office 的授權保護，讓用戶可以免費使用盜版的 Windows 和 Office，以此引誘用戶安裝執行 KMSpico。這種軟體即為俗稱的「註冊機」。

Red Canary 說，他們觀察到不少公司的 IT 人員，不願意購買足額的 Windows 與 Office 授權，反而利用 KMSpico 來非法啟用 Windows 與 Office 給企業內部員工，造成該惡意軟體的大量散布。

KMSpico 主要功能是破解各種軟體的啟動授權限制，但同時夾帶各種廣告軟體或惡意軟體，安裝到想使用盜版軟體的用戶 Windows 電腦中。若用「KMSpico」為關鍵字進行 Google 搜尋，就會看到許多相關連結，都試圖裝扮成 KMSpico 的官方網站，引誘用戶點按下載。

在這次 Red Canary 發現的案例中，駭侵者將加密貨幣相關惡意軟體 Crtpybot 利用 CypherIT 包裝得十分嚴密，再加入 KMSpico 的酬載中，以致多數掃毒軟體不易掃出；接著再執行一段同樣防護嚴密，能在偵測到防毒沙盒環境時自動停止執行的程式碼，以安裝 CryptBot。

用戶的 Windows 一旦感染 CryptBot，該惡意程式就會自各種瀏覽器和加密貨幣錢包中收集用戶的機敏資訊與加密資產資訊，並且自加密貨幣錢包中竊走加密資產。

資安專家表示，個人與公司行號都不應貪圖盜版的小利，使用這類破解工具，反而引狼入室，造成更大的損失。

- 資料來源：
  1. KMSPico with extra spice
  2. Malicious KMSPico installers steal your cryptocurrency wallets

2.2.2、去中心化加密貨幣金融服務 Badger 遭駭，被竊數位資產總值高達 1.2 億美元

去中心化加密貨幣金融平台 Badger 傳遭駭侵者竊走鉅額數位資產，據報遭竊的比特幣與以太幣，總價值合計超過 1 億 2000 萬美元。

去中心化加密貨幣金融服務（Decentralized Finance, DeFi）平台 Badger，日前傳遭駭侵者竊走鉅額數位資產；據報遭竊的比特幣與以太幣，總價值合計超過 1 億 2000 萬美元。

去中心化金融服務是透過區塊鏈上的智慧合約，以自動執行的方式，提供用戶各種加密貨幣存款、貸款、融資等金融服務，是近年來十分熱門的加密貨幣金融服務類型。

據區塊鏈分析業者 PeckShield 表示，該公司是最先發現這筆鉅額竊案的業者；據 PeckShield 的觀察報告指出，在 Badger 緊急關閉該公司的智慧合約系統前，駭侵者從 Badger 用戶的帳號中，一共竊走 2,100 枚比特幣，以及 151 枚以太幣，以竊取發生當時的市場幣價來估算，總損失金額高達 1 億 2,030 萬美元。

PeckShield 也說，該公司觀察到有一位 Badger 用戶，個人就被竊走多達 900 枚比特幣，損失高達 5,000 萬美元以上。

多家加密貨幣相關媒體指出，在 Badger 的官方 Discord 社群頻道上，有一些用戶指出，駭侵者是利用了 Badger 使用者界面的一個資安漏洞，以取得

用戶錢包的控制權，並且藉以竊走存在用戶錢包中的數位資產。

Badger 在竊案發生後，僅對外表示已經緊急暫停所有帳戶的交易功能，並正在進行內部調查，有結果後會對外公開說明，但尚未提供任何關於漏洞與遭駭過程的資訊。

2021 年以來已經發生多起針對加密貨幣平台的駭侵竊盜事件，造成極為巨大的財損；例如 PolyNetwork 遭竊達 6 億美元、Cream Finance 遭竊 1 億 3,000 萬美元、Liquid 遭竊 9,400 萬美元。而 Cream Finance 今年更是三次發生駭侵竊盜事件，總損失合計高達近 2 億美元。

- 資料來源：
  1. PeckShield Inc. @peckshield
  2. ฿adgerDAO @BadgerDAO
  3. Hackers steal $120 million from Badger DeFi platform

2.3、國際政府組織資安資訊

2.3.1、Apache Log4j 漏洞影響巨大，美國資安主管機關通令政府單位立即修復

由於 Apach Log4j Java 程式庫 0–day 漏洞造成的影響十分巨大且嚴重，美國資安主管機關發出命令，要求美國聯邦政府各單位，限期於 12 月 24 日前修復完成。

由於 Apach Log4j Java 程式庫 0-day 漏洞 CVE-2021-44228 造成的影響十分巨大且嚴重，美國資安主管機關「資安暨關鍵基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA）日前發出命令，要求美國聯邦政府各單位，務必立即測試並處理該漏洞，限期於 12 月 24 日前必須修復完成。

CISA 除了發出限期更新命令外，也發布對應 Apache Log4j 漏洞的處理修復指南；指南中詳細說明了 Log4j 的問題、攻擊弱點、測試方式與更新手續，以供美國公私營單位參考辦理。

CISA 也表示，目前正在加緊列出所有可能存有 Log4j 漏洞的主要軟體供應商及其受影響產品，並將會在上述漏洞處理修復指南的網頁中，詳細列出所有其受影響產品、服務，以及其可更新的資訊。

目前 CISA 在 GitHub 上維護一個名為「CISA Log4j (CVE-2021-44228) 漏洞指南」的專案頁面，其中已經列出大量存有此漏洞的重要軟體產品與服務，其中包括許多廣泛使用的知名雲端服務與軟體產品，例如 Akamai SIEM

Splunk Connector、Amazon OpenSearch、Amazon EC2、Atlassian Jira Server & Data Center、Broadcom Symantech IT Management Suite、Checkpoint CloudGuard、Cisco Duo、Cisco BroadWorks、ElasticSearch 所有產品、以及 Fortinet、Sophos、McAfee、TrendMirco、VMware 等多種雲端服務在內。

另一方面，資安廠商 Check Point 指出，該公司觀察到駭侵者利用 Log4j 漏洞發動的攻擊頻率，正在以驚人的速度快速增加。據該公司的資料，在 12 月 10 日當天，也就是在漏洞公開之初，約觀測到數千起試圖鎖定 Log4j 漏洞的攻擊活動，漏洞公開後 24 小時則上升到近 20 萬次攻擊，在 72 小時後更增加到 83 萬次以上，可見 Log4j 對全球資安的巨大威脅。

- 資料來源：
  1. Apache Log4j Vulnerability Guidance
  2. CISA Log4j (CVE-2021-44228) Vulnerability Guidance
  3. The Numbers Behind Log4j Vulnerability CVE-2021-44228

2.3.2、駭侵團體 Nobelium 現在利用 SolarWinds 漏洞發動大規模釣魚攻擊

法國資安主管單位日前發布資安警訊，指出有一個駭侵團體，利用去年造成極大資安風暴的 SolarWinds 漏洞，鎖定法國多個單位發動攻擊。

法國資安主管單位 ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information）日前發布資安警訊，指出有一個駭侵團體 Nobelium，利用去年造成極大資安風暴的 SolarWinds 漏洞，鎖定法國多個單位發動攻擊。

ANSSI 指出，Nobelium 的攻擊行動，係由 2021 年 2 月開始進行，主要的攻擊對象，是法國所屬的各單位。Nobelium 透過去年造成極大資安風暴的 SolarWinds 漏洞，駭入多個法國所屬組織內容，再以這些組織的名義對外發送含有惡意軟體的 Email。

另外，許多法國境內單位也收到來自外國組織的惡意電子郵件，ANSSI 認為這些可能也都是由 Nobelium 駭侵團體所為。

ANSSI 說，Nobelium 利用多個架設在國內外的虛擬專屬主機（Virtual Private Servers, VPS）來發動對法國組織的駭侵攻擊；其中一部分主機係由法國的雲端運算服務商 OVH 提供，其他的主機則位在同樣遭受 Nobelium 攻擊的國家境內。

為提高法國各單位對抗此波攻擊的能力，ANSSI 提供資安防護加強指南給各單位參考，用以提升其內部 Windows Active Directory 與其伺服器的資安

設定，以降低遭到攻擊得逞的機率。

ANSSI 也建議各單位開始限制電子郵件夾檔的執行，以避免遭到釣魚郵件中夾藏的惡意程式碼攻擊。

- 資料來源：
  1. RAPPORT MENACES ET INCIDENTS DU CERT-FR
  2. POINTS DE CONTRÔLE ACTIVE DIRECTORY

2.3.3、美國 FBI 自 REvil、GandCrab 勒贖團體追回 230 萬美元贖款

美國聯邦調查局（FBI）日前宣布追回一批勒贖駭侵團體 REvil 獲取的不法贖金，金額高達 230 萬美元。

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前宣布追回一批勒贖駭侵團體 REvil 獲取的不法贖金，總金額高達 230 萬美元。

這筆贖金是從某個與 REvil 與 GandCrab 勒贖團體相關的犯罪組織處追回。FBI 查獲一個該組織用以存放贖金的 Exodus 加密貨幣軟體錢包，內部存放的不法所得，高達 39.89139522 枚 Bitcoin。

FBI 是在 2021 年 8 月時緝獲這筆勒贖贖金，當時價值美金 150 萬元；在 FBI 對外公布本案的時間點，這批 Bitcoin 的價值高達 230 萬美元。

雖然 FBI 並未對外說明如何取得該加密貨幣軟體錢包的控制權，但資安專家認為 FBI 應該是掌握了駭侵團體設定的加密貨幣軟體錢包密語組合，才能存取內部存放的數位資產。

FBI 的通報中載明了該加密貨幣軟體錢包原本的擁有者 Email 地址，資安專家根據該 Emai 地址，指出該擁有者可能與 GandCrab 與 REvil / Sodinokibi 有關，在駭侵界以「Lalartu」之名廣為認識。

資安專家指出，像 Lalartu 這類的駭侵者，會利用 GandCrab 和 REvil 架設的「勒贖即服務」（Ransomware-as-a-Service, RaaS）來針對特定目標發動

勒贖攻擊；由 GandCrab、REvil 等「服務提供者」研發勒贖軟體、提供支付工具，並架設洩露竊得資訊專用的網站，利用此類「服務」的駭侵者，則負責找到駭侵對象加入入侵，並散布勒贖軟體。一旦受害者支付贖金，「服務提供者」可分得兩成到三成的贖金，其餘則由駭侵者取得。

- 資料來源：
  1. UNITED STATES'COMPLAINT FOR FORFEITURE
  2. Tracking Down REvil's "Lalartu" by utilizing OSINT methods

2.4、行動裝置資安訊息

2.4.1、資安專家指出，廉價兒童智慧手錶是資安與隱私惡夢

資安廠商分析市場上專為兒童配戴設計的智慧手錶產品，發現多個資安與隱私漏洞；有些產品甚至會擅自收集並傳送資料，造成嚴重資安危機。

資安廠商 Dr. Web 日前發表研究報告，指出該公司旗下資安專家分析市場上多款專為兒童配戴設計的智慧手錶產品，發現多個資安與隱私漏洞；有些產品甚至會擅自收集並傳送資料，造成嚴重資安危機。

Dr. Web 檢驗了四款兒童專用智慧手錶，分別為 Elari Kidphone 4G、Wokka Lokka Q50、Elari FixiTime Lite、Smart baby Watch Q19；這些智慧手錶均採用 Android 作業系統，在俄羅斯市場十分暢銷。

Dr. Web 指出，Elari Kidphone 4G 有三個隱藏的軟體模組，每隔八小時會自動傳回多項資料到某一台中央伺服器，回傳的資料包括 SIM 卡資訊、地理座標、裝置資訊、通訊錄連絡人清單、安裝的 app 列表、簡訊數量、通話記錄等。

Dr. Web 表示，有這些隱藏的軟體模組，即可以在用戶不知情的情形下，在手錶上遠端安裝更多惡意軟體或顯示廣告，或是進行遠端監控。

另一款 Wokka Lokka Q50 由於價格便宜，僅 15 美元即可購得，因此也非常暢銷；然而 Dr. Web 的資安專家不但發現其預設密碼「123456」過於脆弱，且這款手錶同樣會把各種資料傳回到位於俄羅斯的伺服器，甚至在傳送

過程中完全沒有進行加密處理，而是以明文傳送。

專家指出，由於 Wokka Lokka Q50 的資安防護近乎不存在，因此駭侵者可輕鬆發動中間人攻擊，輕易透過簡訊取得受害者的 GPS 位置座標、遠端竊聽受害者周邊的各種聲音，甚至將官方伺服器的 IP，竄改為駭侵者擁有的控制伺服器，輕鬆攔截所有資訊。

其他兩款兒童智慧手銀，亦有類似的資安問題存在，包括以明文擅自上傳各種裝置資訊，以及幾無保護力的預設密碼。

專家呼籲家長應避免採購價格過於便宜，且無法提供資安保護能力證明的兒童智慧手錶，以免包括兒童所在位置的各種資訊遭竊，反而危及兒童的資訊與人身安全。

- 資料來源：
  1. Doctor Web discovered vulnerabilities in children’s smart watches
  2. Smartwatches for children are a privacy and security nightmare

2.4.2、芬蘭政府警告 Android 用戶，小心惡意軟體 Flubot 的惡意簡訊

芬蘭政府資安主管機關，日前針對廣大 Android 用戶發出嚴重資安警訊，指出該國的 Android 用戶正面臨大規模 Flubot 惡意軟體攻擊活動。

芬蘭政府資安主管機關「國家資安中心」（National Cyber Security Centre, NCSC-FI），日前針對廣大 Android 用戶發出嚴重資安警訊，指出該國的 Android 用戶正面臨大規模 Flubot 惡意軟體攻擊活動。

正在芬蘭肆虐的惡意軟體 Flubot，是一種專門進行金融詐騙的惡意軟體，除了會竊取用戶手機上的各種個人資訊、偷窺通訊錄連絡人清單、擅自讀取簡訊內容、盜打電話之外，還會以畫面覆疊的方式，竊取用戶在各種金融服務網站或 App 上輸入的登入帳密，並傳送到駭侵團體的控制伺服器上。

Flubot 在芬蘭發動攻擊的手法，是利用遭感染的 Android 手機，大量發送垃圾簡訊給通訊錄上的人員，假稱有未接聽的語言留言，並在簡訊中點按連結以聽取留言；實際上用戶會被導至一個存有惡意 APK 軟體的網站，以在受害者的 Android 手機上安裝 Flubot 惡意軟體。

至於 iPhone 或其他系統用戶，如果點按該惡意連結，則會被導到一個詐騙網站，試圖騙取用戶輸入信用卡資訊，但不會安裝任何惡意軟體。

芬蘭資安主管當局指出，這次是 Flubot 今年在芬蘭發動的第二波攻擊行動，在 24 小時內發送超過 70,000 封圾垃簡訊，比前一波發生在六月時的攻擊，規模更為龐大。當局預估未來數天內會有幾十萬到幾百萬封垃圾簡訊；且攻擊也極可能自芬蘭擴散到全球各國。

當局呼籲 Andoird 手機用戶必須提高警覺，切勿點按不明簡訊內的任何連結；如果不慎遭植入惡意軟體，且在感染後操作過任何網路金融服務，應立即將手機徹底還原至出廠狀態，同時通知相關銀行或金融機構。若有任何財物損失，也應立即向警政單位報案。

- 資料來源：
  1. NCSC-FI issued a severe alert on malware being spread by SMS
  2. NCSC-FI @CERTFI

2.5、軟體系統資安議題

2.5.1、TP-Link 家用路由器 TL-WR840N 嚴重 RCE 漏洞，遭駭侵者植入 Dark Mirai

資安廠商發現，近期有駭侵者鎖定 TP-Link 一款暢銷家用路由器的資安漏洞發動攻擊，在路由器中植入 Dark Mirai 僵屍網路惡意軟體。

資安廠商 Fortinet 近日發表資安通報，指出該公司旗下的資安研究人員，近期觀察到有駭侵者鎖定 TP-Link 一款暢銷家用路由器的資安漏洞發動攻擊，在路由器中植入 Dark Mirai 僵屍網路惡意軟體。

本次駭侵攻擊針對的 TP-Link 家用路由器機種為 TP-Link TL-WR840N EU V5，於 2017 年上市，是一款頗受消費者歡迎的家用路由器。

駭侵者係利用該款路由器舊版韌體中的一個資安漏洞 CVE-2021-41653 來發動攻擊；駭侵者只要在該路由器管理界面中的 IP 位址輸入方框中輸入特製的酬載資訊，即可誘發此一漏洞，進而遠端執行任意程式碼。

CVE-2021-41653 的 CVSS 危險程度分數高達 9.8 分（滿分為 10 分），危險程度評級為最高等級的「嚴重」等級（Critical）。

在 Fortinet 觀察到的攻擊活動中，駭侵者利用 CVE-2021-41653 漏洞，強制路由器下載並執行一段名為「tshit.sh」的惡意程式碼，接著再透過後續的兩個要求，下載 Mirai 變種僵屍網路惡意軟體的二進位碼。

雖然駭侵者必須先知道路由器管理界面的登入資訊，才能使用上述手法發動攻擊，不過絕大多數的這類路由器使用者，都不會特別注意資安須知，

並在啟用路由器後立即修改管理者登入密碼，更不會經常更新韌體與作業系統，因此駭侵者可以透過廠商預設的管理登入密碼，即可輕鬆完成駭侵程序。

TP-Link 已於 2021 年 11 月 12 日推出新版韌體，將此漏洞修復完成；資安專家呼籲該款產品用戶，應立即將產品韌體更新至最新版本，以避免自己的裝置遭駭侵者利用來發動 DDoS 攻擊。

- 資料來源：
  1. CVE-2021-41653 Detail
  2. MANGA aka Dark Mirai-based Campaign Targets New TP-Link Router RCE Vulnerability
  3. Dark Mirai botnet targeting RCE on popular TP-Link router

2.5.2、資安廠商已觀察到利用 Log4j Java 嚴重 0-day 漏洞發動的勒贖攻擊

在 Log4j Java 嚴重漏洞消息公開後，資安專家首次觀察到有疑似利用此漏洞發動的勒贖攻擊活動。

在近期 Log4j Java 嚴重漏洞消息公開，且已有利用此漏洞的大量各式資安攻擊發生後，資安專家首次觀察到有疑似利用此漏洞發動的勒贖攻擊活動。

這個嚴重的 Log4j Java 0-day 資安漏洞 CVE-2021-44228，由於可以輕易利用，再加上使用極為廣泛，在上周公開後，引發極大的資安風暴。雖然 Apache Foundation 立即推出修復版本，但各種不同規模大小的服務與軟體，還需要一段時間才能全面更新；在這段期間，多個資安廠商與研究機構，就已發現大量各型利用此漏洞發動的攻擊，從植入惡意軟體、釣魚攻擊、服務阻斷攻擊、挖礦程式、僵屍網路等，可謂無奇不有。

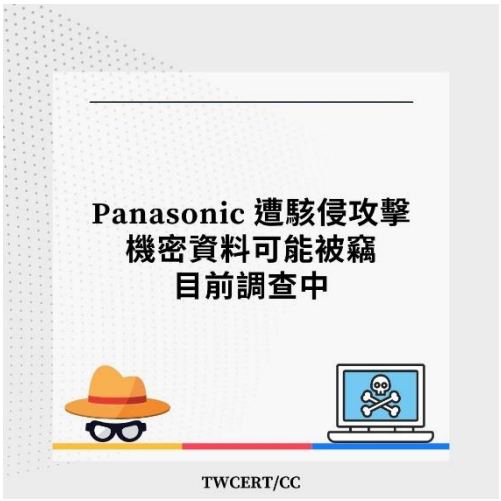
近日資安廠商 Bitdefender 就發表了一份研究報告，指出該公司觀察到首例例用 Log4j 發動的勒贖攻擊事件；該駭侵團體會利用 Log4j 漏洞，從一台伺服器中下載一個名為 Khonsari 的 .NET 勒贖攻擊程式碼，將受害電腦中的所有檔案全部加密。

不過資安專家指出，這次勒贖攻擊事件中，駭侵者沒有留下任何交付贖金的聯絡資料，因此也有可能只是駭侵團體用來進行測試，未來可能還會出現更大規模的真正勒贖攻擊。

此外，Microsoft 旗下的資安研究單位 Microsoft Threat Intelligence Center（MSTIC）也發布資安通報，指出該單位觀察到有駭侵攻擊利用 Log4j 漏洞，在受害電腦中植入 Cobalt Strike 信標惡意軟體，可下載不同的惡意程式碼酬載，以進行進一步的駭侵。

- 資料來源：
  1. Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation
  2. Technical Advisory: Zero-day critical vulnerability in Log4j2 exploited in the wild

2.5.3、Panasonic 遭駭侵攻擊，機密資料可能被竊，目前調查中



日本最大電化製品製造廠 Panasonic，日前發表資安通報，表示該公司發現長期遭到不明駭侵者入侵，造成部分資料可能遭竊。

日本最大電化製品製造廠 Panasonic，於 11 月 26 日發表資安通報，表示該公司發現內部網路系統長期遭到不明駭侵者入侵，造成部分資料可能遭竊。

據 Panasonic 發表的簡單聲明指出，該公司是在 11 月 11 日發現社內部網路遭到不明第三方的不當存取，隨即採取補救措施，阻止不明駭侵者進一步存取該公司內部網路資源；該公司也立即展開內部調查作業，並且向相關主管機關通報相關駭侵事件。

聲明中沒有具體說明這次駭侵事件的細節，該公司僅表示已配合外部資安廠商與專家，會同進行調查，以了解駭侵事件造成的實際損害，以及是否有危及社會基礎設施的情形。

根據日本放送協會（Nippon Housou Kyokai, NHK）報導指出，Panasonic 公司內部伺服器遭外界不當存取，是從 2021 年 6 月 22 日到 11 月 3 日之間多次發生，目前還無法確認是否有與社內工作人員或顧客，甚至是產品企畫、研發、製造、販售等相關機密資料遭竊。

報導也說，Panasonic 是以自行開發的技術來保護資料安全，目前正在會同資安專家調查損害情形，若有進一步的訊息，將會儘速向外界說明。

日本多家大型製造業者，近年來飽受各種駭侵攻擊之苦；包括川崎重工、日本電氣（NEC)、三菱電機、神戶製鋼、Pasco、Olympus 等企業，都曾遭到駭侵攻擊或勒贖攻擊，往往造成其日本本社與世界各國分社、工廠被迫停止作業。

- 資料來源：
  1. 当社ファイルサーバへの不正アクセス発生について
  2. パナソニック 不正アクセス受ける 情報流出ないか確認急ぐ
  3. パナソニックがハッカーによる社内ネットワークへのアクセスでデータ流出を確認

2.5.4、西班牙第二大啤酒廠 Damm 因勒索攻擊而被迫停產

西班牙第二大啤酒釀造廠 Damm 一座主要的啤酒釀造廠，因為遭到勒贖駭侵攻擊而被迫停產。

西班牙第二大啤酒釀造廠 Damm 一座位於巴塞隆納附近的主要啤酒釀造廠，日前因為遭到勒贖駭侵攻擊而被迫停產。

據 Damm 公司發言人指出，該廠的電腦系統在 2021 年 11 月 9 日晚上遭到來源不明的勒贖駭侵攻擊，攻擊持續了數個小時之久，導致這座位於巴塞隆納附近 El Prat de Llobregat 的啤酒工廠完全癱瘓。

該公司發言人指出，其 IT 工程人員很快排除部份障礙，讓一部份的生產線重新開始運作；該公司也表示很快就能恢復 100% 產能。該工廠一年可以釀造多達 7 億公升啤酒。

不過關於這起勒贖駭侵事件的各種細部資訊，包括是哪個駭侵團體、發動何種駭侵攻擊、攻擊手法、要求的贖金，以及該公司是否同意支付贖金等，該公司都未對外公開。

Damm 也沒有說明是否向當地執法單位發出通報並尋求協助，甚至連當地的警察單位也未證實 Damm 是否曾來報案。

該公司生產的 Estrella Damm Lager 在歐洲是相當受歡迎的啤酒品牌，該公司產品也透過許多酒吧、餐廳等通路販售；該公司指出，由於市場上的存貨相當充裕，這次的駭侵攻擊並沒有造成供應短缺或斷貨問題。

西班牙境內近期頻傳針對大型機構發動的勒駭侵事件。今年 10 月，巴塞隆納大學也遭到一起勒贖攻擊，而在今年上半年，西班牙政府所屬的多個就業輔導機構，也因為駭侵攻擊而無法正常運作。

歐盟曾在今年 10 月發表一份資安通報，指出由於肺炎疫情和歐洲各國的封城措施，使得在家工作的人數大增，也讓網路犯罪更為猖獗，甚至還有不少「工作機會」招募駭侵者。

- 建議採取資安強化措施

1、建議國內企業可參考 antiransom.tw 勒索軟體防護專區的防護指南與檢核表，以預防駭侵攻擊。

2、勒索軟體防護專區提供事前-勒索軟體預防措施、事中-被勒索軟體攻擊時的應變措施以及事後-回復階段的作法。

3、若不幸遭受攻擊，也可向調查局或刑事局報案尋求協助，並通報 TWCERT/CC。建議將攻擊事件資訊藉由 TWCERT/CC 進行分享，以幫助國內外其它企業組織防範相關攻擊，減少勒索軟體的影響。

- 資料來源：

1. CYBER ATTACK HALTS BEER PRODUCTION AT BARCELONA’S DAMM BREWERY
2. Cyber attack turns off the taps at Barcelona’s Damm brewery

2.5.5、瑞典汽車大廠 VOLVO 遭不當存取，汽車設計機密資料可能遭竊

瑞典汽車製造大廠 VOLVO 日前發表資安通報，指出該公司的部分研究開發資料，可能因為內部伺服器遭駭而外洩。

瑞典汽車製造大廠 VOLVO 日前對外發表資安通報，指出該公司的部分研究車輛設計開發相關資料，可能因為內部伺服器遭到駭侵攻擊而外洩。

該公司在聲明稿中指出，在公司所擁有的檔案庫中，有一個遭到不明第三方的不當存取；在展開內部調查後，確認遭到不當存取的檔案庫中，存放的是該公司的各種研究開發相關檔案。

聲明中也指出，該公司已經確認這批檔案遭竊，可能對該公司未來的營運造成衝擊。

不過 VOLVO 也在聲明表示，目前該公司已會同獨立的第三方專家，針對整起入侵與資料遭竊事件進行調查；以目前的調查結果來看，暫時不會對任何顧客車輛或個人資料的安全性造成威脅。

據資安專業媒體 BleepingComputer 指出，雖然 VOLVO 並未說明任何關於此次駭侵攻擊的細節，但已有一個名為 Snatch 的勒贖組織出面宣稱犯下此案。

Snatch 說，他們是在 2021 年 11 月 30 日時入侵 VOLVO 公司的內部檔案系統，並在這次駭侵活動中竊取了 VOLVO 公司的機密資訊。

Snatch 同時也公布了部分竊得檔案的螢幕擷圖，甚至還公開了部分被竊檔案；遭到公開的檔案大小達 35.9 MB。

BleepingComutper 針對 Snatch 公開的資訊，向 VOLVO 公司進行求證，但 VOLVO 公司拒絕提供進一步的評論，僅表示資安是該公司全球研發與營運中最重要的一環，針對任何形式的各種資安事件，該公司都都嚴肅以對。

- 資料來源：
  1. Notice of cyber security breach by third party
  2. Volvo Cars discloses security breach leading to R&D data theft

2.5.6、QNAP 發表資安通報，指出有惡意軟體攻擊其 NAS 裝置以挖掘比特幣

台灣網路儲存設備大廠威聯通發表資安通報，有一個惡意軟體專門針對 QNAP 的網路儲存裝置發動駭侵攻擊，以竊取用戶的運算資源進行比特幣挖礦。

台灣網路儲存設備大廠威聯通（QNAP）日前發表資安通報，指出目前有一個惡意軟體，專門針對 QNAP 的網路儲存裝置（Network Attatched Storage，NAS）發動駭侵攻擊，以竊取用戶的運算資源進行比特幣挖礦。

通報指出，被成功駭入的 QNAP NAS 裝置，會由惡意軟體啟動一個名為「oom_reaper」的處理程序，最高可佔用高達 50% 的 CPU 資源，其核心程序的 PID 高於 1000 以上。

由於這個挖礦程序會擅自使用大量系統資源，因此用戶不但會感受到 NAS 正常作業的反應變慢，也會造成零組件長期處於重度工作負荷之下，不但會提高工作溫度，更為耗電，也會使內部組件更容易發生故障。

QNAP 指出，如果用戶懷疑自己的 NAS 裝置遭到惡意軟體用以進行比特幣挖礦，可以先重新啟動 NAS 系統，如此就有可能移除或停止該惡意軟體的執行。

另外，QNAP 也建議所有該公司 NAS 產品使用者，採取以下步驟，以提高資安防護能力，降低 NAS 裝置遭駭侵攻擊的機率：

- 經常升級作業系統 QTS 或 QuTS hero，盡量保持在最新版本；
- 安裝官方提供的資安掃瞄軟體 Malware Remover 並更新至最新版本；
- 管理者與其他使用者帳號，均應使用強式密碼；
- 各種安裝在 NAS 上的應用軟體，均應更新至最新版本；
- 如果可能，勿讓 NAS 裝置直接曝露在外部 Internet 網路上；如果必須如此，應避免使用系統預設的 port 443 與 8080。

QNAP 官方也提供了資安防護操作指引，供用戶參考。

- 資料來源：

1. Investigating Bitcoin Miner [oom_reaper]
2. What is the best practice for enhancing NAS security?
3. Bitcoin Miner [oom_reaper] targets QNAP NAS devices

2.6、軟硬體漏洞資訊

2.6.1、Log4j Java 程式庫的嚴重 0-day 漏洞，恐將造成極大資安危機

資安專家發現廣為使用的 Log4j Java 程式庫，內含嚴重的 -0-day 資安漏洞，可導致遠端執行任意程式碼。

資安專家近日發現廣為使用的 Log4j Java 程式庫，內含嚴重的 -0-day 資安漏洞 ，可能導致駭侵者用於發動攻擊，遠端執行任意程式碼；由於此程式庫的使用率極高，專家指出恐將造成嚴重的資安危機。

這個 0-day 漏洞的 CVE 編號為 CVE-2021-44228，命名為「Log4Shell」或是「LogJam」；任何系統若執行 Log4j 2.0-beta9 到 2.14.1 之間的版本，都有可能遭到駭侵者遠端執行任意程式碼，而且無須通過任何登入驗證程序。

這個 Log4j 0-day 漏洞的 CVSS 危險程度評分高達滿分 10 分。

該漏洞是由阿里雲的資安研究團隊發現，並在第一時間通報開發出 Log4j Java 程式庫的 Apache 基金會；但在資安研究專家於 Github 上公布針對此一漏洞開發出的駭侵概念證實（Proof of Concept）程式碼後，資安廠商馬上就觀測到有駭侵者開始掃瞄 Internet 上可能存有此漏洞的主機；現在更有駭侵者開始利用此一漏洞，發動大規模的惡意軟體植入攻擊。

由於 Log4j Java 程式庫的使用範圍極廣，因此專家預期可能對許多仍採用 Java 的各種網路服務業者造成極大的資安危機，被點名的業者包括

Apple、Amazon、Cloudflare、Twitter、Steam、Minecraft、百度、騰訊、滴滴、京東、網易、Tesla、Google、VMware、UniFi、Webex、LinkedIn 等大型網路服務業者。

Log4j 的開發者 Apache Foundation 已經緊急推出 Log4j 2.15.0 版本，解決了 CVE-2021-44228 的漏洞；任何使用本程式庫的單位，均應立即更新到最新版本，以對應已有駭侵團體大規模利用此漏洞發動攻擊的資安風險。

- CVE 編號：CVE-2021-44228
- 影響產品：Log4j 2.0-beta9 到 2.14.1 之間的版本
- 解決方案：更新 Log4j 2.15.0 版本

- 資料來源：
  1. CVE-2021-44228 Detail
  2. Apache Log4j 2 CVE-2021-44228
  3. Hackers start pushing malware in worldwide Log4Shell attacks
  4. New zero-day exploit for Log4j Java library is an enterprise nightmare
  5. Apache Log4j 2

2.6.2、Apple 修補 iOS 15.2 嚴重 RCE 漏洞，可導致駭客在 15 秒內挾持裝置控制權

Apple 推出 iOS 15.2，修復可讓駭侵者於 15 秒內即可破解的漏洞；該漏洞可導致駭侵者快速破解裝置保護，遠端執行任意程式碼。

Apple 近期推出的 iOS 15.2 新版作業系統更新，修復一個可讓駭侵者於 15 秒內即可破解的漏洞 CVE-2021-30955；該漏洞存於舊版 iOS 系統中的 Mobile Safari 瀏覽器，可導致駭侵者快速破解裝置保護，遠端執行任意程式碼。

該漏洞曾在 2021 年 10 月於中國成都的「天府杯」資安大賽中，由一個名為「崑崙實驗室」的資安團隊，以 15 秒的時間，利用此漏洞快速完成「越獄」，破解最新上市且搭載當時最新 iOS 15.0.2 版本的 iPhone 13 Pro。

據資安專家表示，CVE-2021-30955 漏洞不只出現在 iOS 行動作業系統內，包括 Mac 電腦使用的作業系統 macOS，也含有此漏洞。

Apple 於近日推出一系列作業系統更新版本，包括 iOS 15.2、macOS Monterey 12.1、macOS Big Sur 11.6.2、macOS Catalina 資安更新 2021-008、iPadOS 15.2、tvOS 15.2、watchOS 8.3 等，除了解決上述的 CVE-2021-30955 嚴重 RCE 漏洞外，還更新了另外 8 個其他漏洞，較重要的如下列：

- CVE-2021-30927、CVE-2021-30980：使用已釋放記憶體的漏洞，可導致駭侵者以核心權限執行任意程式碼；

- CVE-2021-30937、CVE-2021-30949：均為記憶體崩潰漏洞，可導致駭侵者以核心權限執行任意程式碼；
- CVE-2021-30993、CVE-2021-30983：均為緩衝區溢位漏洞，可導致惡意程式或位於特定網路位址的駭侵者執行任意程式碼。

各型 Apple 裝置用戶，應立即更新至上述最新版本作業系統，以修復上述已知漏洞。

- CVE 編號：CVE-2021-30955 等
- 影響產品：使用非最新版作業系統之 iPhone、iPad、Mac 電腦、Apple TV、Apple Watch
- 解決方案：更新至 iOS 15.2、macOS Monterey 12.1、macOS Big Sur 11.6.2、macOS Catalina 資安更新 2021-008、iPadOS 15.2、tvOS 15.2、watchOS 8.3 及後續版本

- 資料來源：
  1. About the security content of iOS 15.2 and iPadOS 15.2
  2. About the security content of macOS Monterey 12.1
  3. iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security
  4. Apple iOS Update Fixes Cringey iPhone 13 Jailbreak Exploit

2.6.3、資安專家發現多個 Wi-Fi、藍牙晶片內漏洞，可導致駭侵者竊取密碼與資料

資安專家近期發現存於現用 Wi-Fi 與藍牙晶片中的多個資安漏洞，可導致駭侵者用於竊取裝置密碼與各種資料。

多個資安研究機構的資安專家，近期聯合發表研究報告，指出研究人員發現存於現用 Wi-Fi 與藍牙晶片中的多個資安漏洞，可導致駭侵者用於竊取裝置密碼與各種資料。

來自德國達姆城大學（University of Darmstadt）、義大利布雷西亞大學（University of Brescia）、義大利國立大學校際電信聯合會（National, Inter-University Consortium for Telecommunications, CNIT）、行動網路資安實驗室（Secure Mobile Networking Lab）等單位，近期共同發表研究報告，指出現在廣為使用的各廠 Wi-Fi + 藍牙行動通訊裝置晶片中，共有 9 個資安漏洞，可讓駭侵者發動各種攻擊，包括遠端執行任意程式碼、空中（Over-the-air）發動服務阻斷攻擊（DoS）、擷取網路密碼，以及讀取機敏資訊。

共有三家供應商的 Wi-Fi + 藍牙晶片含有這些漏洞，包括 Broadcom、Cypress（CVE-2020-10368、CVE-2020-10367、CVE-2019-15063、CVE-2020-10370、CVE-2020-10369）、Silicon Labs（CVE-2020-229531、CVE-2020-29533、CVE-2020-29532、CVE-2020-29530）。

研究報告指出，市面上各種內建 Wi-Fi 無線網路與藍牙無線通訊的裝置，通常採用單晶片解決方案，在晶片中含有分別對應 Wi-Fi、藍牙、LTE 通

訊的模組，也各自有各自的資安保護程序；然而這些單晶片解決方案也有不少資源是由這些通訊模組所共享的，例如天線和無線電頻譜等。

在單晶片中共享資源，目的是為了降低能耗與延時，提升通訊的傳輸吞吐量，但也造成駭侵攻擊者的可趁之機；這份報告即證實了可以利用這些不同通訊組件之間的共享橋接部分來發動攻擊。

報告中詳列多部因採用這三家廠商晶片而可遭駭入的裝置，例如 Apple iPhone 6、7、8、X、XR、11、SE2、Samsung Galaxy S6、S8、S10、S20 等系列、MacBook Pro 2016、Macbook Pro/Air 2019-2020 等極為暢銷的機種。

目前各大廠牌仍在研究修復這些晶片漏洞的方案，在更新方案推出前，專家建議用戶移除非必要的藍牙裝置配對與 Wi-Fi 網路，在公共場所避免使用 Wi-Fi，改使用 4G 或 5G 行動網路，即可降低遭駭侵者利用這批漏洞發動攻擊的風險。

- 資料來源：
  1. Attacks on Wireless Coexistence: Exploiting Cross-Technology Performance Features for Inter-Chip Pri
  2. Bugs in billions of WiFi, Bluetooth chips allow password, data theft

2.6.4、微軟推出 2021 年 12 月 Patch Tuesday 更新修補包，共更新 67 個漏洞

微軟最新推出 12 月的「Patch Tuesday」資安更新修補包，一共修復多達 67 個資安漏洞，其中更有 6 個 0-day 漏洞；各種微軟產品用戶，應立即更新至最新版本。

在這 67 個得到修復的資安漏洞之中，依漏洞類型來區分的話，其類型及數量如下：

- 執行權限提升漏洞：21 個；
- 遠端執行任意程式碼漏洞：26 個；
- 資訊洩露漏洞：10 個；
- 服務阻斷攻擊漏洞：3 個；
- 詐欺假冒漏洞：7 個。

若以嚴重程度來區分，共有 7 個漏洞歸類為嚴重（Critical）等級，其餘 60 個則為重要（Important）等級。

至於此次修復的 6 個 0-day 漏洞中，較嚴重且已知遭到駭侵者利用於攻擊行動的，共有兩個 0-day 漏洞，其中較嚴重的是 CVE-2021-43890，屬於 Windows AppX 安裝程式的漏洞，先前已有多個惡意軟體散布攻擊案例係利用此漏洞發動攻擊，包括惡名昭彰的 Emotet、TrickBot 與 BazarLoader 等。

另一個較嚴重的 0-day 漏洞則是 CVE-2021-41333。本漏洞發生於 Windows Print Spooler 子系統，可用以提升駭侵者的執行權限，先前也曾遭駭侵者用於發動攻擊，而且利用此漏洞的程序相當簡易。

微軟這次 Patch Tuesday 修復的漏洞，涵蓋的微軟產品相當多元，包括 Microsoft Office、Microsoft PowerShell、Microsoft Windows、Microsoft Edge Browser 等；採用這些微軟產品的用戶或系統管理者，應立即套用適用的產品更新，以避免駭侵者利用已知的漏洞發動攻擊而造成損失。

- 資料來源：
  1. Security Update Guide
  2. Microsoft December 2021 Patch Tuesday: Zero-day exploited to spread Emotet malware

2.6.5、海康威視監視產品，遭僵屍惡意軟體 Moobot 駭入，用以發動 DDoS 攻擊

資安廠商發現一個名為 Moobot 的惡意軟體，透過海康威視多項監視器產品的一個資安漏洞廣為散布。

資安廠商 Fortinet 日前發表研究報告，指出該公司發現一個名為 Moobot 的惡意軟體，透過海康威視（Hikvision）多項監視器產品的一個資安漏洞廣為散布。

Moobot 是惡名昭彰的僵屍網路惡意軟體 Mirai 的一個變種，當受害裝置感染後，會將裝置變成其僵屍網路大軍的一員，接受駭侵團體的指令，針對特定目標發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）。

據 Fortinet 的研究報告指出，Moobot 係利用海康威視多種監視器產品的 web server 當中的一個漏洞 CVE-2021-36260 來入侵；這個漏洞是屬於一種指令注入漏洞，駭侵者遠端將一個含有惡意指令的特製訊息發送到存有此漏洞的海康威視裝置，即可誘發此漏洞，並且注入惡意程式碼進行感染。

Fortinet 的報告中指出，攻擊海康威視產品的方式十分簡單，甚至不需要通過任何登入驗證程序，只要把特製的攻擊訊息發送給目標裝置即可得逞。

Fortinet 說，Moobot 在感染後，還會修改一些常用指令，例如重新啟動裝置用的「reboot」指令，導致管理者無法重新啟動遭到駭侵的裝置。

Fortinet 指出，雖然 CVE-2021-36260 這個漏洞，已經在海康威視於 2021

年 9 月時推出的新版韌體中予以修復，但由於多數 IoT 產品擁有者幾乎不會在產品開始使用後隨時更新韌體，因此市面上仍存在數量極多的未修補產品，成為駭侵者的絕佳目標。

資安專家呼籲各種 IoT 裝置的管理者，必須經常檢視擁有產品是否推出資安更新，並且確保產品維持在最新版本，以免成為駭侵者用來發動攻擊的目標與工具。

- CVE 編號：CVE-2021-36260
- 影響產品：海康威視多款監控用產品
- 解決方案：升級至原廠提供最新版韌體

- 資料來源：
  1. Mirai-based Botnet - Moobot Targets Hikvision Vulnerability
  2. Security Notification - Command Injection Vulnerability in Some Hikvision products

2.6.6、多達 27 個資安漏洞，存於雲端服務的遠端 USB 裝置掛載軟體 Eltima SDK 內

資安廠商發現一個常用於雲端服務的遠端 USB 裝置掛載軟體 Eltima SDK，內部存有高達 27 個資安漏洞，不過目前尚未發現有駭侵者利用這漏洞發動攻擊。

資安廠商 Sentinel Labs 旗下的資安專家，近日發現一個常用於雲端服務的遠端 USB 裝置掛載軟體 Eltima SDK，內部存有高達 27 個資安漏洞，不過目前尚未發現有駭侵者利用這漏洞發動攻擊。

Eltima SDK 廣泛使用於多家雲端運算業者提供的虛擬作業系統桌面服務；由於全球肺炎疫情，使得許多公司讓員工遠距工作，並透過這類虛擬作業系統服務，讓員工可以使用企業專屬的各種軟體與系統。

而 Eltima SDK 的功能，就是讓這類遠距使用虛擬作業系統桌面的用戶，可以將各式 USB 裝置插上自己的電腦，透過該 SDK 掛載到虛擬作業系統的檔案系統中，進行檔案存取或其他功能。

據 Sentinel Labs 指出，由於 Eltima SDK 中的漏洞，駭侵者將有可能藉由遠距用戶掛載的 USB 裝置，藉機駭入雲端服務者提供的虛擬作業系統內，使其資安防護功能失效，甚至進一步駭入企業內網，發動各種如資料竊取、竊聽監控、勒贖等駭侵攻擊行動。

Sentinel Labs 在發現這批漏洞的第一時間，就通報給 Eltima，Eltima 也已全數修復這些漏洞；然而使用 Eltima SDK 的雲端服務廠商及其產品為數眾

多，仍待逐一升級。

以下是使用受影響版本 Eltima SDK 的雲端服務列表：

- Amazon Nimble Studio AMI 2021/07/29 之前版本
- Amazon NICE DCV, 2021.1.7744 (Windows)、2021.1.3560 (Linux)、2021.1.3590 (Mac) 2021/07/30 之前版本
- Amazon WorkSpaces agent, v1.0.1.1537, 2021/07/31 之前版本
- Amazon AppStream client 1.1.304, 2021/08/02 之前版本
- NoMachine 所有 Windows 產品 v4.0.346 至 v.7.7.4 之間版本 (v.6.x 正在修復中)
- Accops HyWorks Client for Windows: v3.2.8.180 與之前版本
- Accops HyWorks DVM Tools for Windows: 3.3.1.102 與之前版本 (Accops HyWorks 部分 v3.3 R3 之前版本)
- Eltima USB Network Gate 9.2.2420 到 7.0.1370 之間版本
- Amzetta zPortal Windows zClient
- Amzetta zPortal DVM Tools
- FlexiHub 5.2.14094 至 3.3.11481 之間版本
- Donglify 1.7.14110 至 1.0.12309 之間版本

各企業如有使用上列雲端服務廠商提供的遠端桌面環境，應立即更新至已修復的版本。

- CVE 編號：CVE-2021-42972 等共 27 個
- 解決方案：立即將雲端服務廠商提供的遠端桌面環境更新至已修復的版本

- 資料來源：
  1. USB Over Ethernet | Multiple Vulnerabilities in AWS and Other Major Cloud Services
  2. 27 flaws in USB-over-network SDK affect millions of cloud users

第 3 章、 資安研討會及活動

第一屆後量子密碼論壇	
活動時間	2022 年 1 月 14 日 (五) 09:00 ~ 16:50
活動地點	集思北科大 2 樓感恩廳 (台北市大安區忠孝東路三段 1 號 2 樓)
活動網站	https://pqc.ithome.com.tw/
活動概要	 **主辦單位：iThome** 國際頂尖密碼學家齊聚臺灣 本論壇邀請到多位國際頂尖密碼學家，其研發之後量子密碼演算法已進入 NIST 最終決選階段，有望成為世界標準。 此外，更有國內後量子密碼的實作企業，從各個面向協助政府、銀行、企業提早布局，遵循世界標準與規範，保護交易、個資、智慧財產及機敏資訊。 量子電腦已成定局，量子破密隨之而來，後量子密碼實現量子資安 當全世界聚焦於量子電腦對科技、政治和經濟等面向帶來的價值，資安學者已經證實量子電腦能在短時間內破解威脅以 RSA 和 ECC 為基礎的公鑰密碼系統，即將全面影響下一代金融、IoT、網際網路、通訊相關應用，對交易、個資、智財等機敏資料產生極高資安風險，現在就必須開始未雨綢繆進行標準演算法的轉換、硬體設備與中介軟體的升級，標準轉換勢在必行： ➢ 政府、銀行、企業未來該如何超前部署，替換既有公鑰密碼系

	統以符合世界標準？ ➢ 如何掌握並盤點單位內的密碼服務、金鑰及憑證？ ➢ 金鑰如何被使用，其生命週期該如何被管理？ ➢ 單位內的數位資產將存放至何時，其價值是否已進行風險評估？

原生安全強勢升級 ー VMware NSX 3.2 重磅登場	
活動時間	**1/19(三) 14:00**
活動地點	**線上講堂**
活動網站	**https://event.ithome.com.tw/live/vm220119/index.html?utm_source=edm&utm_medium=itweb&utm_campaign=vmware**
活動概要	 **主辦單位：VMware** 隨著數位轉型浪潮席捲，我們的生活、工作情境，已與資訊技術息息相關，連帶使資安威脅如影隨形跟隨你我，大從國家、社會及產業，小至企業、部門或個人，都迫切需要提升資安保護。 傳統重於外掛、孤立、被動的安全技術，往往因代理 (Agent) 過多導致資源消耗，因方案各自為政缺乏統一控制視圖，亦因防護範圍受限、僅能被動回應新態攻擊，造成整體防禦力不足。有鑒於此，VMware 提出「原生安全」(Intrinsic Security) 新訴求，強調以內建、整合、主動的新特色，形塑「零信任」防禦思維，幫助企業打造更完善的資安防護體系。 如今伴隨 VMware NSX 3.2 新版問世，一舉新增分散式防火牆 (微分段)、南北向防火牆 (Gateway Firewall)、IDPS、沙箱、NTA (Network Traffic Analysis) 多項功能，可望搭配 vSphere 原生的 VMware Workload Security，讓企業無論從網路端到系統主機內，皆可達到有效聯防、縱深防禦。

	因此，VMware 將於 2022 年 1 月 19 日舉辦「VMware 週三線上講堂 ー 原生安全強勢升級 ー VMware NSX 3.2 重磅登場」線上研討會，一方面詳細介紹 VMware NSX 3.2 新增功能，二方面將以某政府 A 級機關為情境，藉由攻防演練，闡釋如何善用零信任架構對抗入侵行為。 敬邀您參與本線上講堂，完整領略 VMware 原生安全、零信任架構的奧妙，讓您的企業練就牢不可破的堅強防禦力，從容應對各種資安威脅的侵襲！ 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 精采課程 主題一：VMware NSX 3.2 發表及主要功能介紹 主題二：常見駭客攻擊手法及因應對策案例分享

預見未來-當 AI 防禦遇上 AI 攻擊-資安現況與未來趨勢	
活動時間	**2022-01-27**
活動地點	**工研院台北館前學習中心**
活動網站	**https://college.itri.org.tw/all-events-2/C1B48809-9C42-430A-B6E5-E6FB94017207.html?utm_medium=crssearch&utm_source=college**
活動概要	 **主辦單位：工研院產業學院** 聯絡資訊：溫郁佳/03-5743864 報名截止日：2022-01-25 課程介紹：透過資訊安全現況及未來趨勢分享、透過常見 AI 攻擊、防護手法、自駕車資安事件等案例，讓學員了解資安策略思維與實務作法。 課程特色/目標：透過各領域資安案例解析，讓學員熟悉資安產業發展現況與 AI 在資安攻擊與防護上之應用趨勢。 課程對象：資安管理人員、資安工程師、資安研究員 講師簡介： 現職：定威科技有限公司總經理、資安顧問 經歷： 資訊安全工程師、講師及資安顧問等 行政院國家資通安全會報-技術服務中心資安工程師 漢昕科技股份有限公司資安顧問

軒振科技有限公司資安顧問

中央、地方機關、學校等，資訊安全管理、網路安全及專案經驗工程師與講師

專長： 電訊管理、資訊網路、資訊安全、滲透測試、電腦鑑識

課程大綱

全球疫情下的黑色產業鏈發展趨勢 AI 進行網路犯罪(以子之矛，攻子之盾)AI 攻擊手法，插入噪音就能破壞語音辨識系統 AI 進化超 AI 智能家電安全性實務案例分析 智能住宅安全性實務案例分析 車聯網安全性實務案例分析 穿戴式裝置安全性實務案例分析 車聯網入侵案例分析

集科技與智慧，超乎你想像的未來車 AI 人工智慧將主宰未來汽車產業的發展 L3 級別自動駕駛技術介紹 5G 技術(車聯網應用)介紹 電子外後視鏡介紹 上線控剎車介紹 平視顯示器（HUD）介紹 輪轂電機介紹 注意力輔助系統介紹 超級鎂介紹 地下數據挖掘介紹 電動車無線充電介紹 AI 車聯網安全主動防護技術(ACC、車道偏移輔助)

報名資訊

主辦單位：工研院產業學院

舉辦地點：工研院產業學院(台北實際地點以上課通知為準)、使用 Webex 軟體數位同步

舉辦日期：110/1/27 (三)9:30~16:30（6 小時）

課程費用：訂價：每人 $5,500 元、早鳥優惠:4,800 元

開課 14 天前或同一公司三人(含)以上報名：每人$ 4,500 元

同步數位 (本同步數位課程無補課機制)

報名方式：線上報名或以 Mail 方式寄至 Alisa.wen@itri.org.tw

課程洽詢：Alisa.wen@itri.org.tw；溫小姐 專線：03-5743864

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布漏洞嚴重程度前五名之漏洞資訊如下表：

4MOSAn GCB Doctor - Unrestricted Upload of File	
TVN / CVE ID	TVN-202112002 / CVE-2021-44159
CVSS	9.8 (Critical)
影響產品	4MOSAn GCB Doctor version <= 20210811(2.0)
問題描述	4MOSAn GCB Doctor 之檔案上傳功能未作恰當的權限管控，遠端攻擊者不須登入即可上傳任意類型的檔案，包括 webshell 檔案，並執行任意程式碼，對系統進行任意操作或中斷服務。
解決方法	Update 4MOSAn GCB Doctor version to 20210916(v2.0)
公開日期	2021-12-17
相關連結	**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44159**

程曦資訊整合 文字客服 - Arbitrary File Upload	
TVN / CVE ID	TVN-202112006 / CVE-2021-44164
CVSS	9.8 (Critical)
影響產品	聯繫程曦資訊詢問受影響版本
問題描述	文字客服系統檔案上傳功能之 URL 未過濾特殊字元，遠端攻擊者不須登入，可繞過檢查檔案類型功能，上傳惡意腳本並執行任意程式碼，藉以控制系統或中斷服務。
解決方法	聯繫程曦資訊進行版本更新
公開日期	2021-12-17
相關連結	**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44164**

全景 MOTP(Mobile One Time Password) - SQL Injection	
TVN / CVE ID	TVN-202112003 / CVE-2021-44161
CVSS	8.8 (High)
影響產品	全景 MOTP v3.5 以上且含 HA 管理網頁之版本 （不含 HA 管理網頁版則不受影響）
問題描述	全景行動動態密碼系統之特定功能參數未對使用者輸入進行驗證，區域網路內的攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	聯繫全景軟體進行版本更新
公開日期	2021-12-28
相關連結	**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44161**

日月晶耀 神網電腦終端防護系統 - Improper Authentication	
TVN / CVE ID	TVN-202109021 / CVE-2021-45917
CVSS	8.0 (High)
影響產品	日月晶耀 神網電腦終端防護系統 < 7.20.0401
問題描述	神網電腦終端防護系統 Agent 端接收 Server 請求之功能未做適當的身份驗證，攻擊者取得一般使用者權限後，登入區域網路內有安裝該系統 Agent 的電腦，取得註冊表資訊即可偽造 Server 請求，對另一台 Agent 電腦進行任意程式碼執行，藉以控制系統或中斷服務。
解決方法	聯繫日月晶耀進行版本更新
公開日期	2021-12-30
相關連結	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45917

程曦資訊整合 文字客服 - Path Traversal	
TVN / CVE ID	TVN-202112004 / CVE-2021-44162
CVSS	7.5 (High)
影響產品	聯繫程曦資訊詢問受影響版本
問題描述	文字客服系統下載 LOGO 檔案之功能含有 Path Traversal 漏洞，該功能網址參數未進行特殊字元的過濾，遠端攻擊者不須登入，即可下載任意系統檔案。
解決方法	聯繫程曦資訊進行版本更新
公開日期	2021-12-17
相關連結	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44162

第 5 章、 2021 年 12 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。

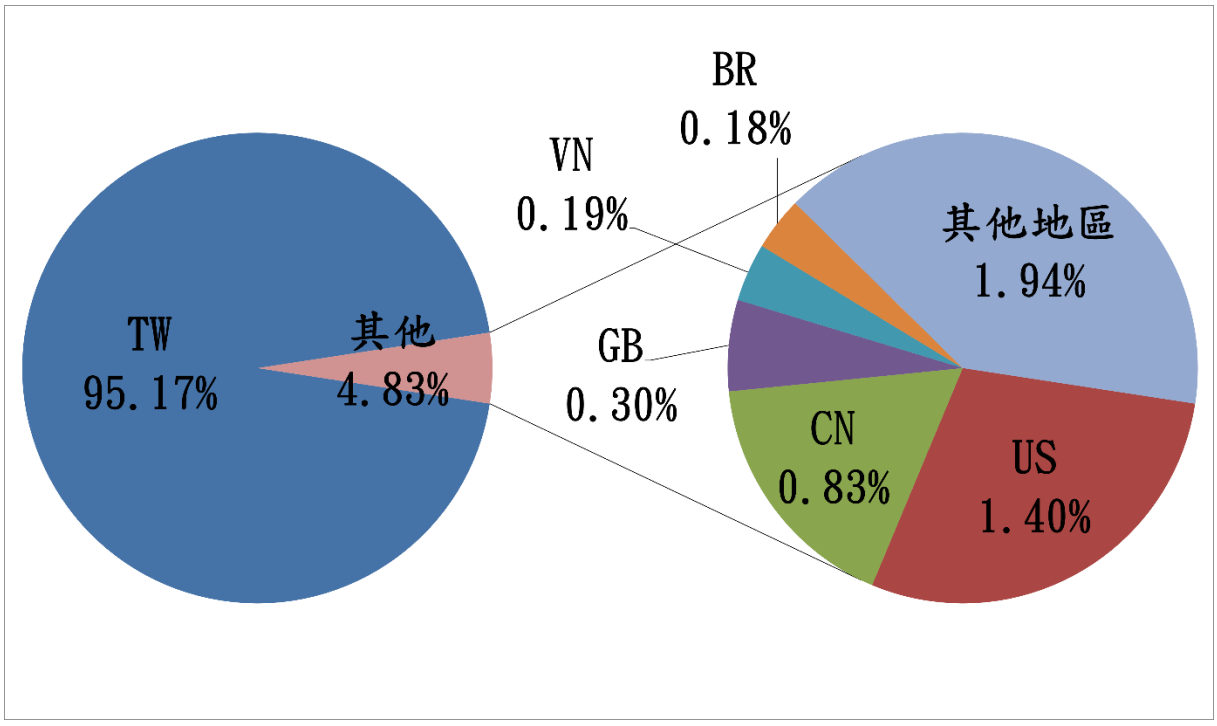


圖 1、分享地區統計圖

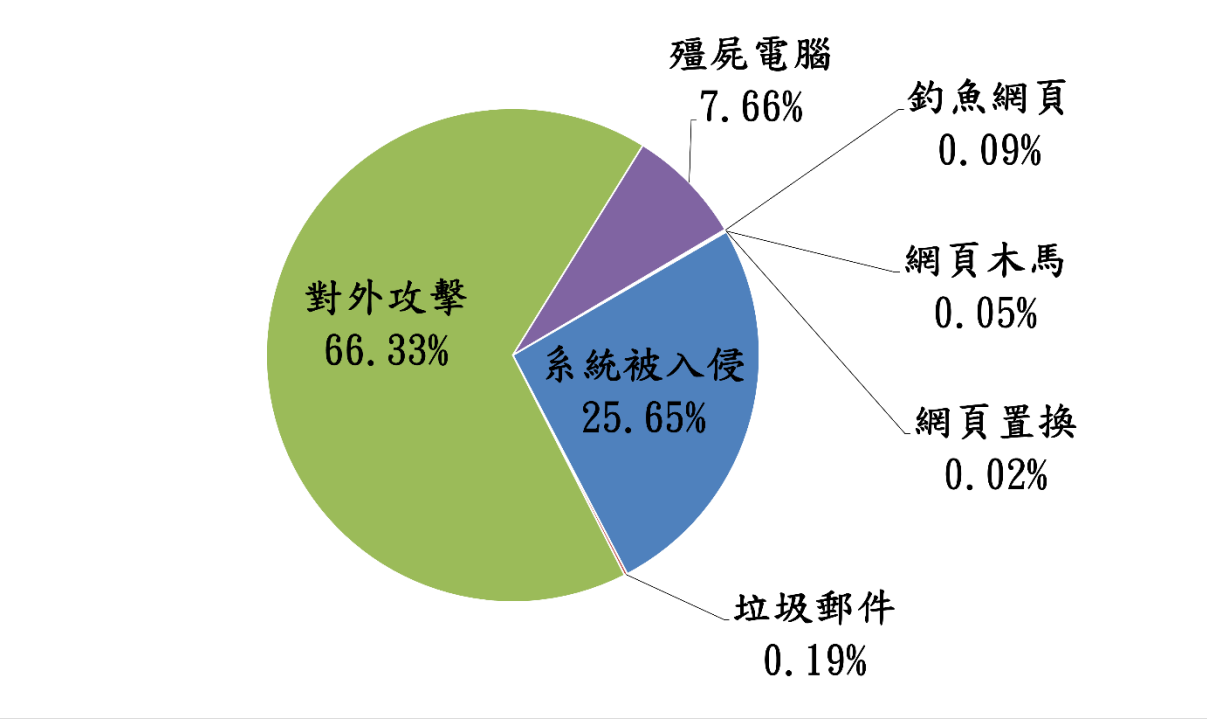

殭屍電腦
7.66%
釣魚網頁
0.09%
網頁木馬
0.05%
網頁置換
0.02%
系統被入侵
25.65%
對外攻擊
66.33%
垃圾郵件
0.19%

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 1 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**