TWCERT/CC 資安情資電子報

2021 年 10 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、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 3 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、新興應用資安、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題及軟硬體漏洞資訊。

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

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

目錄

第 1 章、 封面故事

網路儲存設備之資安威脅與防護

- 網路儲存設備(Network Attached Storage, NAS)，是一種附加於網路上的儲存設備，透過網際網路，NAS 可以提供使用者隨時隨地存取資料，因此逐漸受到個人或企業的青睞。
- 因 NAS 設備往往會被用來儲存企業或個人的大量資訊，且許多使用者並不會特別針對 NAS 設備進行維護作業，更忽略了聯網設備的資安風險，導致駭客逐漸將攻擊目標轉向 NAS 設備。
- 全球知名的國內 NAS 廠商，都相當重視 NAS 設備的安全性，在逐漸增加的網路攻擊中，廠商會在使用的方便性與安全性之間，取得最佳的平衡。
- 針對 NAS 設備的資安威脅問題，國內 NAS 設備生產廠商已紛紛提出相對應的防護機制及解決辦法，使用者也應提高資安意識，配合資安防護要求，才能營造安全的使用環境。

一、簡介

網路儲存設備(Network Attached Storage, NAS)是一種連接網路提供資料儲存之智慧儲存裝置[1]。NAS 設備，如同其他聯網設備，會透過網際網路對外提供服務。雖然所有聯網設備均面臨不小的資安風險，但由於作為儲存裝置的 NAS，使用者較少特別去維護、更新，因此逐漸成為駭客的攻擊目標，

除了廠商要能緊急應變外，使用者也應針對其 NAS 設備，進行足夠的安全防護。NAS 設備成為攻擊目標的主要原因，概述如下：

1. NAS 設備使用量增多引起攻擊者注意：NAS 的使用數量增加的速度相較其他物聯網裝置快，導致一旦攻擊者發現某一 NAS 設備中的漏洞，即可將攻擊手法應用在相同類型的其他 NAS 設備上，其威脅將會比一般的物聯網裝置更大。
2. NAS 設備儲存的機敏資料誘發攻擊者覬覦：作為儲存裝置的 NAS 設備，往往會儲存大量的資訊，尤其是企業的機敏資訊，這對攻擊者具有相當的誘因。
3. NAS 設備防護機制良莠不齊：雖然大多數廠商注重且提供足夠的安全機制與設定，但仍有少部分廠商防護能力不足，導致 NAS 設備的安全性強弱不一，給攻擊者有可乘之機。
4. NAS 設備所在環境的其他聯網裝置易成破口：除了 NAS 設備本身的安全設定之外，與其相互聯結使用的其他聯網裝置，若沒有足夠的資安防護能力也容易成為入侵管道，再加上許多使用者並不會特別採行必要的資安防護措施，一旦使用到自身防護機制不足的 NAS 設備，即容易被成功攻擊[2]。

基於上述各種原因，以及使用者的輕忽，導致越來越多針對 NAS 系統之惡意程式問世，例如在 2019 年出現的勒索病毒 Cr1ptTor，要求受害者支付定額贖金[3]；以及 2020 年出現之 QSnatch 惡意程式，控制受感染的裝置後進行惡意行為[4]。此等針對 NAS 設備的資安威脅已層出不窮。

二、NAS 資安威脅

為避免資料受損或遺失，在過往，使用者通常會將資料儲存及備份於實體隔離的硬碟或 USB 中，但這些直接儲存裝置需隨時攜帶才能方便使用，反而容易遺失或遭竊。因此，僅需透過網際網路便可備份或存取資料的 NAS 設備，便逐漸受到使用者的歡迎。

然而，這種類似於自建私有雲的 NAS 裝置，雖然其便利性增加許多，但由於該裝置會與網際網路相連結，因此在方便之餘，增加了許多資安風險。

2.1 NAS 常見資安威脅

對於 NAS 而言，雖然廠商會針對其安全性進行一定程度的設計及防護，但其倚賴網際網路的通訊以及雲端共享模式，任何與其連接、相容的網路、裝置及軟體之缺陷，都可能對 NAS 裝置造成資安威脅，甚至使用者的習慣和使用方式，都是影響 NAS 安全性的重大因素。NAS 常見的資安威脅包括：

1. 暴力破解 NAS 裝置的弱密碼：通常 NAS 裝置會提供使用者一組公開的預設密碼，登入後再行更改其密碼。然而，許多使用者會沿用其預設密碼，或是為求方便而使用簡單、低強度的密碼設定，導致攻擊者容易透過暴力破解等攻擊手法，成功取得權限後入侵 NAS 設備。

2. 攻擊者透過開源軟體或其他裝置漏洞入侵 NAS 設備：NAS 設備往往會相容於許多不同類型的聯網裝置，這些裝置本身安全防護不一定足夠，導致一旦該裝置遭到攻擊者入侵，甚至感染惡意程式後，與之連接的 NAS 設備同樣會遭到惡意程式的攻擊。此外，隨著 NAS 設備功能需求越來越多，許多功能會借用開源軟體，以減少開發成本。然而，這些開源軟體的安全性良莠不齊，且非廠商本身可完全控制或修正，相較於注重資安的 NAS 設備本身，開源軟體更容易出現資安漏洞。

3. 針對 NAS 零時漏洞進行攻擊：對於任何系統而言，即便對設備及系統的安全性相當注重，但在諸多的程式碼及其功能中，難免有開發時難以察覺的漏洞存在。而攻擊者透過長時間的觀察或偶然發現其資安漏洞，並且利用這個尚未修補的漏洞進行攻擊，導致 NAS 設備廠商及使用者在第一時間難以防禦而受到攻擊。

雖然國內廠商在 NAS 的發展過程中，對資安漏洞已逐一修補及排除，除了新興的攻擊之外，其基本的防護已經相當完備。然而，即便設備的安全性完備，使用者仍是其安全的不確定性之一，使用者是否按照設備安全規範安裝、執行，或是因為資安意識不足而產生防護上的破口，都是 NAS 設備仍然不時出現資安問題的一大原因。

使用者的疏忽主要是源自於未能及時更新 NAS 設備的軟體系統，許多 NAS 設備使用生命週期長，然而，這些常年使用的 NAS 設備，使用者往往不會特別去維護或修補，仍會因尚存有漏洞而被成功攻擊。

2.2 國內 NAS 資安威脅案例

在國內，大多數的 NAS 廠商都會針對其資訊安全提供基本之防護，甚至以此作為該廠商 NAS 設備之特色進行宣傳及販售，包括多因子驗證、防火牆、防毒軟體等相較於過往 NAS 更多的防護措施。雖然這些廠商都提供了基本防護機制，但資安威脅仍時有所聞：

1. 國內廠商 NAS 遭到勒索病毒威脅：在 2019 年 7 月期間，某國內廠商 NAS 產品受到國外勒索病毒之威脅。攻擊者透過暴力破解 NAS 設備的預設密碼及弱密碼，取得管理員權限，並以此散播勒索病毒要求受害者支付贖金。廠商收到通知後，透過 IP 位址，查找到攻擊者的中繼站伺服器位址，並透過 TWCERT/CC 通報給該國資安單位，最終透過組織間的聯繫和協助，得以在事件尚未大量發生前，解除了資安威脅。

2. 針對國內廠商 NAS 設備之惡意程式攻擊：在 2019 年 11 月期間，出現針對國內特定廠商之惡意程式，該程式在入侵 NAS 裝置後，除了會將設備中的資訊及帳號密碼回傳給攻擊者外，同時也會關閉該廠商提供的防護系統，以便順利進行惡意行為。該廠商很快便提供更新的防護系統，可以偵測 NAS 裝置本身是否已感染惡意程式，並且將其移除。此外，該廠商亦提出對使用者的相

關防護措施建議，提升裝置的安全性及入侵難度，以達到更佳的防護效果[6]。

3. 國內 NAS 設備被當成殭屍網路利用：在 2020 年 3 月間，某國內廠商 NAS 設備被發現設備中用以認證的元件，存有遠端連線之漏洞，攻擊者可透過該漏洞入侵後植入後門程式。而確實有攻擊者透過該漏洞，散播殭屍網路惡意程式，藉此控制受害裝置。該廠商在接獲通報後，立即提出新韌體的更新公告，並針對已經不支援的 NAS 版本，建議將其設備安裝於防火牆防護範圍內，避免直接暴露於網路中[7]。

隨著 NAS 的盛行，以及儲存的機敏資訊越來越多，因此攻擊者開始將 NAS 設備視為極佳的攻擊目標，一旦成功進行駭侵攻擊，所能取得的利益相當大。因此諸多在其他設備中出現的資安威脅，在 NAS 設備上也陸續被發現。

如何在使用方便與安全性兩者之間達到最佳的平衡點，將是所有 NAS 設備廠商努力的目標。

三、NAS 資安防護

對於 NAS 設備，雖然目前尚未有完整的資安防護機制及體系，各廠商所著重及防禦的重點也不盡相同，但大致上的目標及所欲解決的問題都是一樣的，歸納國內廠商針對 NAS 資安威脅所進行的防護做法如下：

1. 開發時的事前檢測與防護：對 NAS 廠商而言，雖然開發者在撰寫程式時已極力避免漏洞或缺陷的產生，但難免有疏漏及盲點存在。因此，許多國內 NAS 廠商會將其撰寫的程式透過其他人員或組織協助檢閱，透過多人的討論及檢查，以減少程式碼中產生的資安漏洞。此外，許多 NAS 廠商亦會透過檢測軟體，進行弱點掃描等測試，並且至少須經數次修正，確認程式碼無誤，方公布給使用者使用。

2. 開源軟體的嚴格監控：隨著NAS設備的功能性需求越來越多，開發者不再是自行撰寫所有程式，許多功能會選擇套用已開發的開源軟體，透過修正、結合，達到增加功能之效果。但這些開源軟體種類繁多，品質也良莠不齊，因此國內諸多廠商都會針對其使用的開源軟體進行嚴格的監控，確認其完整性及安全無虞才導入應用。使用者也應遵循廠商提供的安全規範，不要因為一時便利而關閉或調整相關的防護設定，以免成為資安威脅的破口。

3. 對聯網裝置的支援與控管：國內NAS廠商會針對其支援的聯網裝置，包括路由器、影印機、攝影機等，一旦判斷聯網裝置已經老舊，甚至出現嚴重資安問題，都可能會隨時停止NAS設備支援該裝置或其功能，避免攻擊者輕易透過這些老舊裝置，對NAS設備進行攻擊或入侵。

4. 對使用預設密碼或弱密碼的禁止：國內NAS廠商，幾乎都會針對密碼強度及預設密碼進行嚴格的控管，有些廠商直接停止預設密碼，要求使用者安裝前必須先設定密碼，而有些廠商雖然會提供預設密碼，但會要求必須先更改其預設密碼方能繼續使用。此外，廠商對於使用者所設定之密碼也有強度上之要求，以避免攻擊者可輕易透過暴力破解方式，成功入侵NAS設備。

5. 提供對惡意程式的防護機制：雖然各廠商對惡意程式的防護機制不盡相同，但同樣都是希望能避免使用者因惡意程式而蒙受損失。有些國內的NAS廠商，會透過嚴格的設定規範，避免使用者誤觸及感染惡意程式，甚至會定時監控系統的設定，一旦設定被調整，可能產生資安威脅，系統會立即通知管理者並要求修正。另有廠商則著重於使用者誤觸惡意程式後，如何進行即時的修補，包括對自身系統和檔案的檢測、行為監控以及移除惡意程式等，以避免使用者遭受嚴重的損失。

6. 善用資安通報並即時回饋：國內許多廠商會設立資安團隊，如：產品資安事件應變小組(Product Security Incident Response Team, PSIRT)，當收到任何資安通報之後，能夠立即且精準的針對其產品資安問題進行分析及修補。不論是弱密碼受到暴力破解、開源軟體出現缺陷，或零時漏洞等問題，都能透過廠商及時的回饋與修正，達到最佳的處置與防護。因此，使用者在 NAS 設備遭遇攻擊時，應立即通報 NAS 廠商或國內 TWCERT/CC，透過專業人士的協助，方能獲得徹底的解決。

隨著廠商的逐漸重視，NAS 設備的安全性也不斷提升，從設備本身的安全設定、開源軟體與應用程式的選用，對使用者的要求，到漏洞或事件發生後的應變處理，都有相當的規範。此外，也須提升互聯設備及整體網路環境的安全，使用者更須提高資安意識，方得以放心的使用 NAS 設備。

四、結論與建議

1. 隨著網際網路的發展，NAS 設備逐漸成為儲存設備的主流，但許多 NAS 使用者在觀念上，仍停留在過往單一儲存設備的使用習慣中，忽略了聯網環境下的資安風險，導致 NAS 容易受到惡意攻擊。

2. 國內 NAS 廠商都針對其 NAS 設備之資安威脅，包括弱密碼、開源軟體，以及零時漏洞等問題，提出相對應的防護機制及解決辦法，希望能提供使用者完整安全的使用環境。

3. 由於企業用 NAS 設備會連結許多其他網路裝置，包括路由器、影印機、網路攝影機等，然而此等裝置資安風險較高，需要採行較多的防護措施，對於使用環境相對單純的個人用戶稍顯沉重。因此，建議廠商可進行市場區隔，區分一般使用者及企業用戶之 NAS 設備。對於一般使用者不需提供過多的功能，

亦不須支援太多裝置，以減輕資安風險與防護壓力。

4. 為增強 NAS 設備之功能，廠商會開發或導入許多應用程式，然而有些應用程式常非 NAS 廠商可完全控管，一旦出現資安威脅，將難以排解。因此，建議 NAS 廠商宜儘量以自行開發的系統為主，避免將不可控的開源軟體或第三方應用程式直接內嵌於 NAS 設備中，以降低資安風險。

5. 雖然許多 NAS 設備本身已有諸多資安防護機制，包含透過更新以修補新發現的資安漏洞，然而許多使用者卻無定時更新的習慣，或受駭仍不自知，甚至可能已失去聯絡而收不到廠商的系統更新通知。因此建議 NAS 廠商除了提供自動更新功能之外，可與其他具足夠公信力的組織合作，協助發布或通知使用者定期更新，對於國際間的使用者，也可透過組織間的聯繫，達到通告並做好妥善的資安防護。

- 資料來源：

1. NAS 是什麼?
2. This new ransomware is targeting network attached storage devices
3. Cr1ptT0r Ransomware Targets NAS Devices with Old Firmware
4. CISA says 62,000 QNAP NAS devices have been infected with the QSnatch malware
5. 加州議會通過全美首個 IoT 法案，要求每個 IoT 裝置都要有獨立密碼
6. Response to QSnatch Attacks: Take Actions to Secure QNAP NAS

第 2 章、 資訊安全宣導

電郵易遭駭客竄改遂行詐騙，企業應落實資安防詐教育訓練

國內利用釣魚郵件詐騙的手法持續不斷，其中針對企業進行的竄改商務電子郵件詐騙(Business Email Compromise, BEC)數量也大幅提升，加深了企業的資安風險。

企業進行國際貿易頻繁，與外國供應商或企業合作時常需要聯繫及匯款交易，使駭客有機可趁。駭客會以假冒合作的外國供應商或是高階主管之名義寄送電子郵件，意圖降低收件者戒心，誘騙公司或財務人員轉帳匯款。今年國內就有案例是駭客偽冒一間公司的財務長發送電郵給秘書，以信件內容及會議紀錄誘使秘書信任，進而轉帳至指定帳戶，使公司損失上百萬美元。

這類 BEC 詐騙常見手法是，駭客會先寄送釣魚郵件，以具誘惑性之文字內容誘發員工開啟郵件，並下載夾帶木馬程式、病毒的附件以便暗中竊取 Email 登入資訊。或是誘騙員工點擊惡意連結進入釣魚網站，利用以假亂真的網頁騙取信箱帳密。駭入員工的 Email 之後，駭客會收集並竊取員工來往郵件的內容資訊，接著利用收集到的資訊偽冒身分發送郵件，騙取員工匯款至指定帳戶藉以竊取企業的帳款。

資安廠商 Proofpoint 2020 年的研究報告指出，透過 Email 進行駭侵攻擊是駭客容易進行的攻擊手法之一，因許多企業內仍有不少資安教育訓練或資安意識不足的員工。秘書和會計等會接觸到匯款、交易的企業員工，常被駭客鎖定為竊取 Email 帳密的對象。

- 建議採取資安強化措施

1、建議如果收到聲稱是合作企業或高階主管的電子郵件，務必利用其他管道查明對方身分，或是向其所屬企業確認身分。

2、收到電子郵件務必確認電子郵件地址的正確性，駭客可能將郵件地址的英文字母小寫改成大寫或相似字等方式，偽冒成主管或合作夥伴。

3、不開啟不明寄件者或可疑標題的郵件，勿點擊郵件中的連結及附檔，進入可疑網站不隨意輸入帳密和個資，即使看起來像官方網站，也要確認網址的正確性，以免被駭客利用釣魚網站竊取帳戶資訊或被暗植木馬程式。

4、建議不論個人或企業都應定期將系統進行更新，安裝防毒軟體與防火牆，確保設備軟體處於最新版本，以免被駭客利用資安漏洞進行攻擊。

5、建議企業落實對員工的資安宣導，定期舉辦資安教育訓練及社交工程演練。疫情期間許多企業讓員工遠距在家上班，員工家中設備網路安全防護不足，也是企業應宣導及協助的部分。

- 資料來源：

1. 企業資安隱憂 竄改電郵 年騙逾 2 億
2. 變臉詐騙/BEC- (Business Email Compromise) 商務電子郵件詐騙
3. FBI 警告：愈來愈多駭侵團體駭入 Web Mail，竄改郵件規則，進行 BEC 攻擊
4. 駭客以 Google 表單，針對企業員工發動 BEC 攻擊
5. Ransomware Demands Spike 320%, Payments Rise

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、趨勢科技發表 2021 上半年最新資安攻擊分析報告

資安大廠趨勢科技，日前發表 2021 年年中資安攻擊分析報告，針對 2021 年上半年發現的各種資安威脅趨勢提出分析。

全球資安大廠趨勢科技，日前發表一份名為「2021 年年中資安攻擊」的分析報告，針對 2021 年上半年發現的各種資安威脅案例與趨勢提出分析。

該報告有六個部分，分別為勒贖攻擊、進階持續性威脅（Advanced Persistent Threat, APT）、資安漏洞、Covid-19 肺炎疫情相關詐騙與威脅、雲端與 IoT 資安、威脅總體分析等等。

在 2021 年上半年的勒贖攻擊方面，據該公司統計指出，以各種管道如 Email、URL、惡意檔案等攻擊次數，合計超過 700 萬次；其中以金融產業被攻擊次數最多，高達 15,537 次，甚次為政府單位（10,225 次）、製造業（4,957 次）、醫療保健業（4,802 次）、食品飲料業（2,330 次）。最具威脅的勒贖團體則為 DarkSide、REvil、Hello 等。

在 APT 駭侵團體方面，這份報告列出五大在 2021 年上半年最具威脅的 APT 團體，分別為 TeamTNT、Water Pamola、Earth Vetala、Iron Tiger、Earch Wendigo。以 TeamTNT 來說，主要都是鎖定架構在 Amazon Web

Services 上的各種網站服務或 Kubernetes 容器，竊取其帳號密碼，取得控制權後植入加密貨幣挖礦程式以牟取暴利。Water Pamola 的攻擊手法則由過去以發送釣魚信件為主，改為在各種網路商店的管理介面中，以 XSS 攻擊其漏洞來取得控制權。

在漏洞方面，趨勢科技指出 2021 年上半年最具威脅性的四大漏洞，分別是 ProxyLogon、Microsoft SharePoint 漏洞、各種 VPN 系統漏洞、PrintNightmare 等。

- 資料來源：
  1. 2021 MIDYEAR CYBERSECURITY REPORT
  2. Attacks From All Angles 2021 Midyear Cybersecurity Report

3.1.2、全球製造業公司中，高達 91% 曝露於各式資安攻擊風險之下

資安廠商發表研究報告，2020 年全年統計數字指出，91% 全球製造業均曝險於各式資安攻擊的危險之下，攻擊次數較 2019 年增加達 51%。

資安廠商 Positive Technologies 發表研究報告，2020 年的全年統計數字指出， 91% 全球製造業均曝險於各式資安攻擊的危險之下，且不重覆的攻擊事件次數，較 2019 年增加高達 51%。

該報告指出，在這 91% 曝險製造業中，該公司的駭侵測試工具能夠成功入侵公司系統的比例高達 100%，而駭侵測試工具也能成功取得 75% 這類公司工業控制系統的控制權。

Positive Technologies 指出，駭侵者只要有機會進入公司內部網路，100% 的案例中都能成功竊得用戶登入資訊，並且控制被害公司的重要系統；在 69% 的案例中，駭侵者可以成功竊得受害公司的各類機敏資訊，包括公司員工與合作伙伴的重要資訊、往來 Email 內容、各式內部機密文件；75% 的案例可以入侵該公司內網中的重要技術相關網路；56% 的案例中可以實際控制該公司的工業製造用控制系統，造成生產活動受阻。

Positive Technologies 也分析出幾個製造業公司資安風險偏高的關鍵因素，包括對連外網路存取的保護不足、內部製造用網路系統的資安防護能力不足、裝置設定與配置的錯誤或不妥當、網路元件或流量控管不當、密碼設定強度不足或未定期更換，導致易受字典攻擊、使用的軟體系統過時且未能頻繁更新等等。

Positive Technologies 在報告中歸納指出，由於製造業的產值龐大，因此對駭侵者來說是十分有吸引力的攻擊目標。在攻擊手法日益精進之下，企業愈來愈難單靠自己的力量來防範各類資安攻擊。

- 建議採取資安強化措施

1、建議企業訂定密碼設定規範，使用 12 個字元以上，且英文、數字與符號混合之密碼，並定期將密碼進行更換。

2、定期更新電腦系統及軟體，確保系統、軟體及設備皆處於最新版本，避免駭客透過已知的資安漏洞進行駭侵攻擊而造成企業重大損失。

3、除了安裝防毒軟體及防火牆，建議企業將內部網路進行分段隔離、進行使用者權限管控，並依照業務需求分割網路，以提升不同網段間的安全性，防範滲透感染其他主機與系統。

- 資料來源：

1. Information security risks at industrial companies
2. Positive Technologies: 91% of Industrial Companies Open to Cyber-Attacks

3.2、新興應用資安

3.2.1、Cream Finance 去中心化加密貨幣交易所遭駭

去中心化加密貨幣交易所 Cream Finance 遭不明駭侵者入侵，竊走價值超過 2,900 萬美元的資產。

去中心化加密貨幣交易所 Cream Finance，於 8 月 30 日在 Twitter 貼文公布，該交易所遭不明駭侵者入侵，一共竊走價值超過 2,900 萬美元的資產。

根據 Cream Finance 的貼文指出，被竊走的加密貨幣資產，分別是 418,311,571 枚 AMP 代幣（總值相當於 2,510 萬美元），以及 1308.09 枚以太幣（總值相當於 415 萬美元）。

該交易所也表示，駭侵者是針對該交易所的「閃電借貸」（Flash Loan）功能，發動「重新進入攻擊」（Reentrancy Attack）。所謂閃電借貸是一種在以太坊區塊鏈上執行的智慧合約，Cream Finance 的用戶可以透過此合約，快速獲得貸款以進行後續套利投資，之後再行還款的服務。

據區塊鏈資安專家指出，這次攻擊行動中，駭侵者使用的「重新進入攻擊」，是利用該智慧合約的軟體錯誤，在交易獲得確認或否決之前，以迴圈的方式不斷重覆提領資金。

區塊鏈資安專家也確認 Cream Finance 這次攻擊事件中，駭侵者是利用以太坊存於其 ERC-777 智慧合約標準規範中的一個已知漏洞；過去也有多家去中心化交易所遭駭侵者利用此漏洞發動重新進入攻擊，因而造成加密貨幣資產遭竊。

區塊鏈資安專家說，今年（2021）已發生的各種加密貨幣駭侵攻擊中，針對去中心化金融服務（DeFi, Decentralized Finance）平台的攻擊活動，佔比高達 76%，用戶財損將近 5 億美元；各種去中心化金融服務平台，必須開發出類似防火牆之類的資安防護措施，以對應這類漏洞可能導致的駭侵攻擊行動。

- 資料來源：
  1. Cream Finance @CreamdotFinance
  2. Cryptocurrency Crime and Anti-Money Laundering Report, August 2021
  3. Hackers steal $29 million from crypto-platform Cream Finance

3.2.2、美國財政部制裁涉嫌為勒贖攻擊者洗錢的加密貨幣交易所

美國財政部最近針對涉及協助勒贖團體成員洗錢的加密貨幣交易所 SUEX 發出制裁命令，以打擊日益嚴重的勒贖攻擊與國際洗錢管道。

美國財政部最近宣布，針對涉及協助勒贖團體成員洗錢的加密貨幣交易所 SUEX，發出制裁命令，以打擊日益嚴重的勒贖攻擊與國際洗錢管道；這是首度有加密貨幣交易所遭到美國政府的制裁。

被美國財政部點名的 SUEX 交易所，雖然總部登記於捷克共和國境內，但實際營運並不在捷克，而是在俄羅斯的莫斯科與聖彼得堡，以及其他中東據點運作。

據美國財政部指出，SUEX 過去至少涉及為 8 次以上的勒贖攻擊提供金流服務，其已知的加密貨幣交易記錄中，高達 40% 以上都和不法分子的洗錢交易有關。

這是美國政府首次針對加密貨幣交易所發動制裁，目的在於打擊日益猖獗的勒贖攻擊金流與國際洗錢管道；美國財政部指出，2020 年這類與勒贖攻擊有關的加密貨幣洗錢交易，總金額高達 4 億美元，是 2019 年的 4 倍以上。

據區塊鏈統計公司 Chainalysis 的觀測資料指出，SUEX 自 2018 年 2 月成立以來，一共收到高達 4.81 億美元的比特幣轉入帳款，其中有相當大的比例和勒贖攻擊金流有關；包括 Ryuk、Conti、Maze 等勒贖團體，在 SUEX 的轉帳總額高達 1,300 萬美元，和加密貨幣詐騙相關的轉帳總額則有 2,400 萬美元，透過暗網進行的各種不法交易，也達到 2,000 萬美元以上。

美國財政部長葉倫指出，勒贖攻擊與其他駭侵攻擊，使美國不分大小企業都蒙受重大損失，對美國經濟也形成直接的威脅；美國政府會持續打擊這類不法分子，採取各種方法，包括制裁與監管手法，來破壞、嚇阻並預防勒贖攻擊。

- 資料來源：
  1. Publication of Updated Ransomware Advisory; Cyber-related Designation
  2. Treasury Takes Robust Actions to Counter Ransomware
  3. US sanctions cryptocurrency exchange used by ransomware gangs

3.2.3、Firefox 出現假冒 Safepal Wallet 錢包外掛，受害者遭竊 4,000 美元

有一個 Mozilla Firefox 上的惡意外掛程式 Safepal Wallet，會竊取用戶的加密貨幣；目前已造成用戶損失。

有一個 Mozilla Firefox 上的惡意外掛程式 Safepal Wallet，會竊取用戶的加密貨幣；不但在 Mozilla 外掛程式網站上存在已久，也已造成用戶損失。

一位暱稱為 Cali 的 Mozilla Firefox 用戶，日前在 Mozilla 支援討論區上發文，指出自己在 Mozilla Add-ons 外掛程式網頁中安裝了這個叫做 Safepal Wallet 的外掛加密貨幣錢包後，不久就發現自己存放在錢包內的所有加密貨幣餘額變成 0；檢查轉帳記錄後，發現有高達 4,000 美元的加密貨幣，都被私下轉帳到其他錢包位址之中。

據資安專業媒體 BleepingComputer 報導指出，Safepal Wallet 外掛程式存在 Mozilla Add-ons 網頁中已長達 7 個月，最初上架日期為 2021 年 2 月 16 日。

據 Mozilla 的規定，任何要上架到 Mozilla Add-ons 的瀏覽器外掛程式，「都必須接受 Moziila 不定期的審查」；但 Mozilla 並未明確指出是否會審查所有外掛程式的安全性，也沒有透露審查方式或標準。

BleepingComupter 報導指出，Safepal Wallet 的行動裝置應用程式，在 Apple App Store 與 Google Play Store 均有上架，都是由官方上架且經過審核，屬於安全且正常的 App，因此上架到 Mozilla Add-ons 的外掛程式，很可能是駭侵者上傳的假冒外掛程式。

BleepingComputer 旗下的資安研究人員，也發現了一個可能與此詐騙外掛程式相關的網域名稱，其網站會假冒為 Safepal Wallet 的支援網頁，要求用戶輸入 Safepal Wallet 的 12 詞帳號恢復密語；當用戶輸入恢復密語後，該網站不會有任何反應，很可能已將恢復密語偷偷傳送到駭侵者的資料庫中。

- 資料來源：
  1. Got hacked by the add-on called Safepal Wallet!
  2. Malicious 'Safepal Wallet' Firefox add-on stole cryptocurrency

3.3、國際政府組織資安資訊

3.1.1、美國資安主管單位，針對 VPN 安全強化，推出採購與設定指引

美國資安主管機關 CISA 與 NSA 聯合發布 VPN 資安強化指引，幫助各公私單位加強 VPN 對抗外國勢力駭侵攻擊的能力。

美國資安主管機關網路安全暨基礎設施安全局（Cybersecurity & Infrastructure Security Agency, CISA）與國家安全局（National Seurity Agency, NSA），近日聯合發布 VPN 資安強化指引，旨在協助各公私單位加強 VPN 對抗外國勢力駭侵攻擊的能力。

CISA 與 NSA 在新聞稿中指出，VPN 伺服器是進入各種重要受保護網路的入口，因此經常成為各種駭侵團體攻擊的首選；過往有許多受國家力量資助的「進階持續威脅」（Advanced Persistent Threat, APT）駭侵團體，利用各種 VPN 解決方案的資安漏洞與不當設定，不但可以竊取人員登入資訊、遠端執行任意程式碼、破解經由加密傳輸的資訊、攔截破譯傳輸內容、竊取機敏檔案等等。

該指引詳細列舉了如何選擇安全的 VPN 連線服務，以及強化連線安全性的設定方式，以避免 VPN 遭到駭侵攻擊成功；包括選用由「國家資訊保障伙伴」（National Information Assurance Partnership）經過測試驗證通過的 VPN 產品、導入例如多階段登入驗證以強化登入驗證機制、隨時即時套用各種資安修補更新，以及停用非 VPN 相關功能等方法，以盡力強化 VPN 對抗駭侵攻擊的能力。

新聞稿說，這份指引係提供給美國政府旗下各單位如國防部、國家安全體系（National Security Systems）與各種國防工業基地等單位參考遵循之用，

在這份指引列出的 VPN 合格產品列表中，列出一共 225 種合格產品與服務，包括硬體產品型號、其作業系統或韌體版本等資訊，以供意欲提升資安防護等級的公民營單位參考採購。

- 資料來源：
  1. Selecting and Hardening Remote Access VPN Solutions
  2. Product Compliant List: 225 Matches
  3. NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs

3.3.2、駭侵團體 TrickBot 成員在南韓被捕，將引渡至美國受審

惡名昭彰的駭侵團體 TrickBot 犯罪分子，在試圖離開南韓時遭警方逮捕。

一名疑似惡名昭彰的駭侵團體 TrickBot 旗下的犯罪分子，在試圖搭機離開南韓時遭警方逮捕；目前正準備引渡至美國，接受進一步的司法審訊。

據南韓媒體 KBS 報導，這名遭南韓警方逮捕的犯罪嫌疑人，是俄羅斯籍的男性軟體開發人員。他因為受到 COVID-19 疫情影響，無法離開南韓，護照又即將過期；在等待其護照更新約一年半後，於近期搭機離開南韓境內時，因美國方面的引渡要求，遭到南韓警方逮捕。

司法單位認為這名開發者，涉嫌於 2016 時為駭侵團體 TrickBot 進行開發工作，參與開發一個網路瀏覽器專案；當時他住在俄羅斯境內。

駭侵團體 TrickBot 是全球知名的惡意軟體集團，開發多種惡意軟體，包括 TrickBot、BazaLoader、BazaBackdoor、PowerTrick、Anchor 等；這些惡意軟體大多用於攻擊企業所屬網路，以竊取內部機敏資訊，並且部署、發動勒贖攻擊。

近年來多起大型全球勒贖攻擊事件都和 TrickBot 駭侵團體有關，包括著名的 Ryuk 與 Conti 勒贖軟體，據稱都來自 TrickBot。

但該名男性開發者在南韓高等法院出庭應訊時指稱，自己並不知道僱用他的單位是駭侵團體；他說他的工作內容與工作手冊，並沒有涉及惡意軟體

的開發。

該名開發者的俄羅斯律師，正在試圖避免該名開發者遭南韓引渡至美國；該律師說，一旦該名開發者被引渡至美國，就很難倖免於嚴重的司法控訴。

- 資料來源：
  1. TrickBot gang member arrested after getting stuck in South Korea due to COVID-19 pandemic
  2. TrickBot gang developer arrested when trying to leave Korea

3.3.3、南非司法部遭勒贖攻擊，所有電腦系統全面停擺，被迫改以人工作業

南非司法部日前遭嚴重勒贖攻擊，所有電腦系統內的檔案均遭加密，對內與對外電子化服務全面停擺。

南非司法部（Department of Justice）日前遭嚴重勒贖攻擊，所有內部網路中的電腦系統所存檔案均遭到加密而無法存取，導致該單位對內與對外的電子服務全面停擺。

據南非司法部發言人 Steve Maglangu 表示，這次攻擊行動發生於 9 月 6 日，造成該單位內部網路中的檔案全部遭到加密，單位內部員工與外部公眾都無法存取這些檔案，因此造成該單位的電子化服務無法正常運作。

具體受到影響的業務範圍，包括無法開立各種政府公文、暫停保釋程序、Email 系統與網站系統均無法使用等等。

南非司法部發言人 Steve Maglangu 指出，該單位立即啟動緊急狀況程續，除了正在努力復原系統之外，為確保重要功能仍能繼續運作，包括各種文書的開立，以及法庭的運作，都暫時回復到人工作業模式；但子女扶養費（Child maintainance payment）的支付目前嚴重受阻。

Steve Maglangu 也表示，目前無法確定所有系統何時能夠恢復正常運作；目前該單位正在設立一個全新的 EMail 系統，並將員工逐步轉移至新系統上。不過南非司法部沒有透露任何這次攻擊行動的細節資訊，包括攻擊者身分、攻擊手法等，目前都不得而知。

南非司法部指出，目前沒有任何跡象顯示司法部資料外洩並遭濫用，也

沒有任何駭侵團體出面宣稱發動這次攻擊；但資安專家指出，從南非司法部系統恢復所需的甚長時間，加上轉移到新的 Email 系統，研判該單位並未支付贖金給勒贖攻擊者。

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

3.4、社群媒體資安近況

3.4.1、本年至今的社群平台網路愛情詐騙，造成損失高達 1.33 億美元

美國聯邦調查局發布最新資安通報，指出今年到目前為止，各種以愛情邂逅為主的網路詐騙案，在美國造成的損失金額已高達 1.33 億美元。

美國聯邦調查局（Federal Bureau of Investigation, FBI）發布最新資安通報，指出今年到目前為止，各種以愛情邂逅為主的網路詐騙案數量大幅增加，在美國造成的損失金額已高達 1.13 億美元。

FBI 說，這種類型的線上詐騙，通常是在社群平台上，使用假冒的身分，對潛在受害者頻送秋波，讓受害者卸下心防，以為自己與對方墜入情網後，詐騙者再利用其信任，進行各種金錢為主的詐騙活動，例如要求受害者轉帳，甚至套取其金融相關機敏資訊或登入資訊等。

某些案例中，當詐騙者收到受害者的轉帳後，還會進一步以看似可以快速獲取豐厚利潤的套利投資機會，誘騙受害者參與投資；等到受害者真的投資了，又會以各種理由阻止受害者收取利潤或撤回投資金額，然後就人間蒸發，讓受害者追討無門。

FBI 說，這不只會讓受害者人財兩失，更會對受害者的心理健康帶來嚴重傷害。

據 FBI 的統計數字，從 2021 年 1 月 1 日起至 7 月 31 日，FBI 的網路犯罪檢舉中心（FBI Internet Crime Complaint Center, IC3）一共接獲 1,800 件以

上的網路愛情詐編檢舉通報，相關的損失金額合計高達 1.33 億美元以上。

FBI 建議網路用戶應該以下列方式，保護自己不受這類線上愛情詐騙影響，包括絕對不要與這類人進行任何金錢交易或投資、不要輕易揭露自己的金融相關資訊，包括銀行帳號、身分證件字號等、對於各種承諾不合理高獲利的線上金融投資機會，必須特別提高警覺、也不要輕信任何人提供的快速獲利投資機會。

- 資料來源：
  1. Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams
  2. FBI: $113 million lost to online romance scams this year

3.4.2、發動自社群平台針對支付服務的攻擊，2021 第 2 季比前季增五倍以上

資安廠商指出，來自社群媒體平台，針對支付服務發動的各種攻擊，光在 2021 年第 1 季到第 2 季之間，暴增五倍以上。

資安廠商 Atlas VPN 日前發表研究報告指出，來自社群媒體平台，針對支付服務發動的各種駭侵攻擊活動，光在 2021 年第 1 季到第 2 季之間，暴增高達 561.8%。

Altas VPN 這份研究報告，係與 PhisLabs 合作推出；據 PhisLabs 的資安研究人員表示，在 2021 年第 2 季，透過社群平台發動的各種網路駭侵活動。針對的行業種類增減比較，除了上述支付系統大增 561.8% 之外，依增加幅度，依序為醫療保健業（187.8%）、廣播電視媒體（112.5%）、加密貨幣（13%）、信用合作社（4.9%）。

但也有不少行業，在 2021 年第 2 季遭社群平台相關駭侵攻擊的次數，較 2021 年第 1 季減少；包括銀行業（10.2%%）、電子商務（-19.7%）、電信業（-23.5%）、電腦軟體（-49.2%）、網路約會（-52.3%）。

該研究報告也揭露了 2021 年第 2 季，透過社群平台發動的各種攻擊類型比例，其中詐騙佔最大宗，高達 45.6%，其次為假冒他人或品牌身分（21.8%%）、網路攻擊（19.1%）、資料竊取（13.2%%）、實體威脅（0.3%）。

該報告指出，過去在各種網路攻擊的樣態中，來自社群平台的攻擊，並不是最主要的攻擊來源；然而在 2021 年第 2 季的統計數字，可以看出網路犯

罪分子使用社群平台發動攻擊的也開始增加；在 2021 年 1 月時，Atlas VPN 偵測到的社群平台攻擊案例，每月有約 33.6 件，到了 2021 年 6 月則增加到近 50 件。

- 資料來源：
  1. Social media threats for payment services jump over 550% in 2021 Q2
  2. Atlas VPN Finds Social Media Threats For Payment Services Rise Over 550% in 2021 Q2

3.5、行動裝置資安訊息

3.5.1、資安研究人員研製幾可亂真的 USB-C 傳輸線

資安研究人員自製出一條外觀與一般 Lightning 傳輸線完全無異，但內含特製晶片，可以攔截用戶輸入資訊，並無線傳輸至 2 公里之外的駭侵用傳輸線。

一位資安研究人員自製出一條外觀與一般 Lightning 傳輸線完全無異，但內含特製晶片，可以攔截用戶輸入資訊，並透過無線網路，將竊得資訊傳輸至一英哩之外的駭侵用傳輸線。

這名資安研究人員自稱為 MG。MG 推出的這條名為「O.MG」的傳輸線，一端是標準的 USB-C 插頭，另一端則是相容於 Apple 多種產品的 Lgntning 插頭。在 MG 發表的測試影片中，示範了當這條 O.MG 駭侵傳輸線連上 Mac 電腦與 Magic Keyboard 鍵盤後，該傳輸線就會變成一個 Wi-Fi 無線網路熱點，並建立起一個用來傳輸駭侵資訊的無線網路。駭侵者可在最遠達 2 公里處，打開一個瀏覽器界面，遠端接收用戶在該鍵盤上輸入的所有字元。

O.MG 建立的 Web 界面，除了可以竊取用戶的鍵盤輸入字元外，也可以輕易植入各種酬載程式碼；甚至可以設定在當失去連線時自動停止執行酬載程式，或是執行自我毀滅程式，自動清除酬載，以免遭到發現。

MG 推出的這條「O.MG」駭侵傳輸線，實際上是第二代「產品」。該產品的第一代係使用插頭體積較大的 USB-A 對 Lightning 界面；許多人認為日益普及的 USB-C 界面，其體積較小，不足以放置額外的駭侵用晶片電路；但

MG 仍然將之成功實作。

USB-C 版本的 O.MG 駭侵傳輸線，不只可以插在 Apple 的 Magic Keyboard 上竊取資訊，也可以單獨將其 USB-C 插頭插入各種支援 USB-C 界面的平板電腦或手機上。

- 資料來源：
  1. O.MG CABLE - LIGHTNING TO USB-C
  2. This Seemingly Normal Lightning Cable Will Leak Everything You Type

3.5.2、Apple 修補可能用於 NSA Pegasus 間諜軟體的 0-day 漏洞

Apple 緊急修復 iOS 中的 2 個 0-day 漏洞，該漏洞過去曾遭間諜軟體 Pegasus 大規模用於攻擊 iPhone 與 Mac 裝置，以進行竊聽與資料竊取。

Apple 推出用於新版 Mac、iOS 裝置的作業系統更新，以緊急修復 iOS 中的 2 個 0-day 漏洞，該漏洞過去曾遭以色列間諜軟體 Pegasus 大規模用於攻擊 iPhone 與 Mac 裝置，以進行竊聽與資料竊取。

獲得修復的 2 個 0-day 漏洞分別是 CVE-2021-30860 與 CVE-2021-30858；CVE-2021-30860 是存於 iOS 與 macOS 中 CoreGraphics 子系統的整數溢位漏洞，駭侵者可利用特製的 PDF 檔案誘發此漏洞，在 iOS 與 macOS 中執行任意程式碼。

另外，CVE-2021-30858 則是一個存於 WebKit 瀏覽器核心引擎中的「使用已釋放記憶體」（use after free）漏洞；駭侵者可利用特製的網頁，在 iPhone 與 Mac 電腦上 執行任意程式碼。

資安廠商 Citizen Lab 的研究人員指出，這兩個漏洞過去都曾遭駭侵者大規模濫用，特別是以色列科技保全公司 NSA 開發的 Pegasus 惡意間諜軟體，可能涉及利用這兩個 0-day 漏洞，讓某些國家的情報單位，針對特定人士進行大規模監聽。

Apple 這次推出的大規模更新，在作業系統方面包括 iOS 14.8、iPad OS 14.8、iPod Touch、Mac 各型電腦、Apple Watch 等硬體裝置；舊版的 macOS Catalina 與 macOS Mojave 中的 Safari 瀏覽器也有更新版本推出，用戶應立即

透過系統更新進行漏洞修補，以免遭駭侵者繼續利用未更新的漏洞攻擊。

- 資料來源：
  1. Apple security updates
  2. Apple fixes iOS zero-day used to deploy NSO iPhone spyware
  3. Apple Issues Emergency Fix for NSO Zero-Click Zero Day

3.5.3、Google 推出 2021 年 9 月 Android 資安漏洞更新

Google 近期推出 2021 年 9 月 Android 資安修補包，一共修復 40 個資安漏洞，其中包括多個嚴重等級漏洞。

Google 近期推出 2021 年 9 月 Android 資安修補包，一共修復多達 40 個資安漏洞，其中包括多個嚴重等級漏洞；Android 裝置用戶應隨時注意裝置原廠推送的更新通知，一有更新可用，即應立刻更新。

在這次 Android 資安修補包分成兩批。9 月 1 日推出的第一批修補包，解決掉的嚴重等級漏洞中，包括一個存於 Android 8.1、9、10、11 等多個版本 Framework 組件的漏洞，其 CVE 編號為 CVE-2021-0687；Google 在這次的資安通報中指出，遠端駭侵者可以利用一個特製的檔案來誘發此漏洞，造成永久性的服務阻斷（permanent denial of service）。

Google 在 Framework 中還修復了多達 6 個其他資安漏洞，都列為「高」等級危險程度；其中有 5 個可讓駭侵者提升執行權限，1 個為資訊不當洩露。

而在第二批於 9 月 5 日推出的 Android 資安修補包中，一共修補了 23 個資安漏洞，分布於 Android 作業系統中的 Kernel、MediaTek、Unisoc、Qualcomm、Qualcomm close-sourced 等多個組件之內。

其中有 7 個嚴重等級的漏洞發生在 Qualcomm closed-source 組件中，此次一併獲得修復。

雖然 Google 定期針對 Android 系統推出資安修補包，但由於用戶手上的 Android 裝置，內部的 Android 系統多半都是原廠修改過的版本，無法直接套用 Google 的更新包，只能接收來自原廠的系統更新；因此用戶應特別注意裝置是否收到原廠系統更新，如有即應立即更新；也應停止使用原廠不再提供更新服務的老舊裝置。

- 資料來源：
  1. Android Security Bulletin—September 2021
  2. Google Android Security Update Patches 40 Vulnerabilities

3.6、軟體系統資安議題

3.6.1、美國一離職員工侵入公司系統，刪除 21 GB 資料

一名原任職於美國紐約信用合作社的離職員工，在遭該單位解僱後，侵入原任職單位的電腦系統，惡意刪除 21 GB 的重要資料。

一名原任職於美國紐約信用合作社（New York Credit Union）的離職員工 Juliana Barlie，在遭該單位解僱後，侵入原任職單位的電腦系統，惡意刪除 21 GB 的重要資料，目前已遭司法單位起訴。

據檢查官 Jacquelyn M. Kasulis 指出，Juliana Barlie 原本在紐約信用合作社擔任遠距工作的兼職員工，在今年 5 月 19 日遭該單位解僱後，於 2 天後以原有的系統登入資訊進入該單位的伺服器，以指令刪除多筆重要業務相關資料。

據調查報告指出，雖然紐約信用合作社的人員，曾要求外包該單位資訊業務的公司，刪除該離職人員的登入權限，但顯然該外包廠商並未及時切實執行；導致 Juiliana Barlie 仍可利用原本工作時設定的登入資訊，登入紐約信用合作社的工作用電腦系統。

Juliana Barlie 於 5 月 21 日登入系統後，以近 40 分鐘的時間，一共刪除了 21.3 GB 的資料，包括近 20,000 個檔案，以及 3,500 個資料夾；而被刪除的資料中，許多是該單位的客戶貸款申請資料，甚至還包括該單位為防範勒贖攻擊而安裝的資安防護軟體。

當事人 Juailiana Barlie 甚至還在數日後，以簡訊將他刪除紐約信合社檔案一事告訴朋友。

雖然紐約信用合作社擁有某些被刪除資料的備份檔案，但仍需額外花費一萬美元左右，以復原遭惡意刪除的檔案；該信用合作社的客戶貸款作業也因而受到影響，許多客戶被迫使用紙本作業申請或繳付貸款餘額。

- 資料來源：
  1. UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK
  2. Fired NY credit union employee nukes 21GB of data in revenge

3.6.2、近期微軟、Apple、Chrome、Adobe 發布修補程式，建議儘速更新

Microsoft、Apple、Google、Adobe 等國際大廠，請關注並盡快進行更新。

請注意，在更新之前，請確保您已備份系統與重要文件。

Microsoft：

2021 年 9 月 14 日，Microsoft 針對 Windows 與相關產品發布安全性更新，修補了數十個安全漏洞，其中包括 4 個”嚴重”等級的漏洞。

編號 CVE-2021-40444 的漏洞，它會影響 Windows 10 和許多 Windows Server 版本上 Internet Explorer(IE)的“MSHTML”組件，Microsoft 警告該漏洞已被利用發起攻擊。

CVE-2021-36965 是關於處理 Wi-Fi 自動連接的“WLAN AutoConfig”的漏洞，雖然要利用該漏洞有些許限制，攻擊者與目標必須在同一個 Wi-Fi 網路中，但仍可能造成極大危害。

CVE-2021-28316 與 CVE-2021-36965 類似，皆是“WLAN AutoConfig”的漏洞，此漏洞可以繞過安全機制的防護。

CVE-2021-38639 和 CVE-2021-36975 皆屬於本地端執行的漏洞，雖然在 CVSS 評分上會比遠端執行低，但因其影響大部份的 Windows 版本，所以也應被重視且進行更新。

Apple：

2021 年 9 月 13 日，Apple 推出 1 項緊急更新，修正”zero-click”iOS 漏洞(CVE-2021-30860)，在某些 Apple 設備上開啟文件時執行命令，NSO Group 即是使用此漏洞來安裝間諜軟體，遠程監控手機設備。

Google：

2021 年 9 月 13 日，Google 發布了新版本的 Chrome 瀏覽器，修復九個漏洞，在更新的狀況上，可留意位址欄右側是否出現“更新”選項卡。如果關閉瀏覽器已有一段時間，可能會看到“更新”按鈕從綠色變為橙色，然後變為紅色。綠色表示有可用更新已過兩天；橙色表示已過去四天，紅色表示已在更新上落後一周或更長時間。可以將 Chrome 完全關閉並重新啟動即會自動進行更新。

Adobe：

Adobe 近日亦發布了 Reader、Acrobat 和大量其他產品的新版本。

- 資料來源：
  1. Microsoft Patch Tuesday, September 2021 Edition

3.6.3、沉寂一時的勒贖團體 REvil，再度開始活動

發動過許多大規模勒贖攻擊，但於數個月前突然停止運作的勒贖團體 REvil，近日又重起爐灶，再次開始發動攻擊。

惡名昭彰，在近發動過許多大規模勒贖攻擊， 造成全球各企業組織嚴重損失，但於數個月前突然停止運作的勒贖團體 REvil，近日又重起爐灶，再次開始發動攻擊。

據資安專業媒體 BleepingComputer 報導指出，REvil 原本在 Tor 加密網路上設一個用來展示進行中勒贖攻擊，並警告受害者贖款支付期限的網站，原本自六月該單位發動基於 Kaseya VSA 遠端管理系統漏洞的勒贖攻擊後，自七月起就一直處於關閉狀態；但在 9 月 7 日開始，該網站再度恢復運作；隔天起受害者便可登入該網站，與 REvil 駭侵團體「協商」贖金支付金額。

九月初該網站恢復運作後，有接近一星期的時間，沒有刊登新的勒贖攻擊相關訊息；然而在近日該網站不但恢復運作，資安廠商 VirusTotal 也收集到新的 REvil 勒贖攻擊使用的惡意軟體樣本。

另一方面，REvil 勒贖團體成員，也重新出現在某些駭侵相關論壇中；過去經常代表 REvil 駭侵團體的帳號「UNKN」沒有出現，但有另一個自稱是「REvil」的 ID 指出，該團體的消聲匿跡，是因為他們認為 UNKN 可能遭司法單位逮捕，再加上其發動駭侵使用的基礎設施遭各國司法單位緝獲，該團體因而停止運作；該代也說，之前司法單位宣稱取得的 Kaseya 勒贖解密金鑰，其實是該團體的某個成員對外洩露的。

不過據 BleepingComputer 獲得的情資指出，司法單位對於 REvil 之前的消失，也感到十分驚訝；另一段可能是由資安研究人員與 REvil 成員的網路對話，也指出該團體的短暫消失，「只是暫時休息一下」。

無論如何，REvil 近年來活動最明目張膽，也犯下最多大型勒贖攻擊案件的駭侵團體；各公私營單位都應嚴加防範，避免成為其勒贖攻擊的受害者。

- 資料來源：
  1. ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83
  2. REvil ransomware is back in full attack mode and leaking data

3.6.4、微軟團隊發現 BulletProofLink 駭侵團體，提供訂閱制釣魚攻擊服務

微軟近日發表資安通報，指出該公司發現一個大型「釣魚即服務」，提供自動化進行釣魚攻擊的訂閱制服務。

微軟公司旗下的資安研究單位 Microsoft 365 Defender Threat Intelligence Team 近日發表資安通報，指出該公司發現一個大型「釣魚即服務」（Phishing-as-a-service, PhaaS），提供自動化進行釣魚攻擊的訂閱制服務。

微軟指出，該服務背後的駭侵團體被稱為 BulletProofLink，也稱為 BulletProftLink 或 Anthrax；該團體提供的釣魚攻擊「服務」，包括提供計次付費「釣魚工具組」（Phishing Kits），內含基本釣魚信件與登入資訊詐騙網站的範本與樣式，以及訂閱制的長期服務，內容除了上述範本與樣式外，還包括釣魚信件發送、詐騙網站託管、代客竊取登入資訊、登入資訊擴散，以及「完全無法偵測」的連結與記錄檔等。

微軟說，該單位發現由這個駭侵團體發動的釣魚攻擊中，使用了極多新登記的子網域，其中一起攻擊事件中使用的子網域數量就高達 30 萬個；另外該「服務」更提供 100 種以上的釣魚信件與網站範本，用來假冒許多知名品牌與服務。

微軟表示，Bulletproftlink 團體設立的 ICQ 討論群組，去年時共有 1,618 名成員，內含許多該服務與被竊登入資訊的潛在買主。

微軟也指出，BulletProofLink 團體除了販售釣魚服務之外，這些「客戶」利用該服務發動攻擊所取得的登入資訊或其他機敏資訊，也會被該團體

取回，存入該團體設立的另一系列伺服器，以再次用於發動攻擊，提高該團體的不法獲利。

- 資料來源：
  1. Catching the big fish: Analyzing a large-scale phishing-as-a-service operation
  2. Microsoft Warns of a Wide-Scale Phishing-as-a-Service Operation

3.7、軟硬體漏洞資訊

3.7.1、微軟針對 CVE-2021-40444 嚴重 0-day 漏洞推出暫時解決方案

微軟緊急推出針對一個嚴重 0-day 漏洞的暫時解決方案；該漏洞可導致駭侵者攻擊 Office 365 與 Office 2019，並且遠端執行任意程式碼。

微軟日前緊急推出針對一個嚴重 0-day 漏洞的暫時解決方案；該漏洞可導致駭侵者攻擊 Windows 10 上的 Office 365 與 Office 2019，並且遠端執行任意程式碼。

該漏洞的 CVE 編號為 CVE-2021-40444，其 CVSS 危險程度評分高達 8.8 分（滿分為 10 分），主要受影響的微軟產品，以 Windows 家族作業系統（包括 Windows Server 2008、Windows 8.1 一直到 Windows 10 的各版本）上的 Office 365 與 Office 2019。

該漏洞存於 MSHTML 子系統中，這是一個用來繪製畫面輸出的瀏覽器元件，也用於 Microsoft Office 文件之中；駭侵者可利用內含惡意 ActiveX 控制項目的特製 Microsoft Office 文件檔案來誘發此漏洞。要是受害者開啟含有惡意 ActiveX 控制項目的 Office 文件時，即可能遭到攻擊。

不過微軟也指出，如果用戶是以預覽模式，或是透過 Office 365 中的 Application Guard 來開啟從網路上下載的惡意 Office 文件檔案，由於是處於唯讀狀態，且 Application Guard 預設會將不受信任的文件隔離開來，不可使用連線資源或本機的檔案系統，因此將不會受到攻擊。

另外，如果電腦系統上安裝有啟用中的 Microsoft Defender Antivuris 以及 Defender for EndPoint（版本 1.349.22.0 及更新版本），系統也能受到保護，不會遭到 CVE-2021-40444 的攻擊。

用戶可參照微軟提出的暫時解決方案，編輯登錄檔以停用 ActiveX 控制項目。

- CVE 編號：CVE-2021-40444
- 影響產品/版本：包括 Windows Server 2008、Windows 8.1 一直到 Windows 10 的各版本上的 Office 365 與 Office 2019。
- 解決方案：依微軟指示停用 ActiveX 控制項。

- 資料來源：
  1. Microsoft MSHTML Remote Code Execution Vulnerability
  2. Microsoft shares temp fix for ongoing Office 365 zero-day attacks

3.7.2、多家廠商 SoC 產品中的藍牙堆疊含嚴重 BrakTooth 漏洞

資安專家發現十多家廠商產製的單晶片系統，其內部的藍牙連線堆疊存有嚴重資安漏洞 BrakTooth，可導致駭侵者藉以發動多種資安攻擊行動。

資安專家日前發表研究報告，指出發現十多家廠商產製的單晶片系統，其內部的藍牙連線堆疊，存有非常嚴重的資安漏洞（稱為「BrakTooth」），可導致駭侵者藉以發動多種資安攻擊行動。

來自新加坡科技與設計大學的資安研究人員，日前發表針對 BrakTooth 的詳細研究報告；報告指出他們發現 13 家廠商推出的單晶片系統（System-on-a-chip, SoC），其中的藍牙堆疊都存有 BrakTooth 漏洞。

被指含有 BrakTooth 漏洞的 SoC 產品，廣泛用於各種智慧型手機、車用資訊娛樂系統（Infotainment System）、筆記型電腦、桌上型電腦、平板電腦、視聽器材（如電視、音響、藍牙喇叭、藍牙耳機等）、家用娛樂裝置、無線鍵盤、無線滑鼠、玩具、工業設備（如可程式邏輯控制器 PLC）等，數量可能多達十億台以上。

報告也說，生產這些含漏洞 SoC 產品的廠商，包括 Intel、Texas Instruments、Qualcomm、Zhuhai Jieli Technology、Cypress、Bluetrum Technology、Actions Technology、Espressif Systems、Harman International、Silabs 等公司推出的共十三種 SoC 產品。

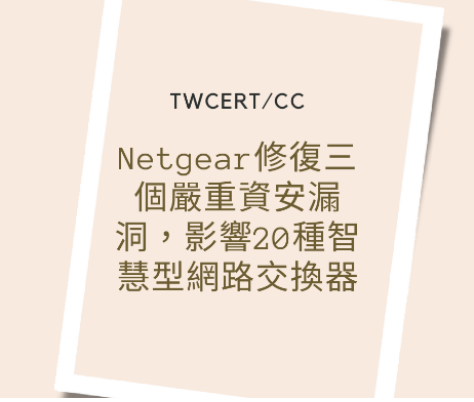
研究人員說，BrakTooth 漏洞可讓駭侵者藉以發動多種攻擊活動，包括分散式服務阻斷（Distributed Denial of Service, DDoS）攻擊、造成用戶裝置發生「死結」（deadlock）而無法使用藍牙連線、遠端執行任意程式碼等。

這一系列漏洞被指派到多達 20 個 CVE 編號，其中包括 Espreessif Systems、Cypress、Bluetrum Technology 等公司的產品已推出對應的修補程式，其他也有多家公司正在撰寫修補軟體。

- 解決方案：各藍牙產品用戶應注意更新訊息，以及時更新受影響的裝置。

- 資料來源：
  1. BRAKTOOTH: Causing Havoc on Bluetooth Link Manager
  2. Bluetooth BrakTooth bugs could affect billions of devices

3.7.3、Netgear 修復三個嚴重資安漏洞，影響 20 種智慧型網路交換器



全球網通產品大廠 Netgear 修復影響其二十種智慧型交換器的三個嚴重資安漏洞，駭侵者可利用這些漏洞，完全控制交換器設備。

全球網通產品大廠 Netgear 日前推出韌體更新，修復影響其多達二十種智慧型交換器的三個嚴重資安漏洞；駭侵者可利用這些漏洞，完全控制交換器設備。

這三個將獲修復的漏洞，分別由資安研究人員命名為 The Demon’ s Cries、Draconian Fear、Seventh Inferno，目前暫無 CVE 編號，但都可能造成這些智慧型交換器的控制權限遭駭侵者取得，進而針對企業內網發動進一步攻擊行動。

Demon’ s Cries 漏洞的 CVSS 分數高達 8.8 分（滿分為 10 分），據資安專家指出，該漏洞可讓駭侵者跳過登入驗證程序，駭侵者可藉以取得管理者的登入資訊，並且完全掌控受害的交換器設備。

資安研究人員指出，該漏洞存於 Netgear Switch Discover Protocol 之內；研究人員發現一種可以跳過其登入驗證程序的方法，不過駭侵者必須先進入企業內部網路，才能利用這個漏洞。

Draconian Fear 的 CVSS 分數為 7.4 分，駭侵者如果與管理者使用同一個 IP，或假造一個和管理者相同的登入用 IP，即可攔截 Netgear 交換器 web 界面傳送的資訊封包，並且利用其來源檢查的漏洞，進入管理介面之中。

研究人員尚未針對第三個漏洞 Seventh Inferno 推出詳細分析，不過 Netgear 已針對旗下二十種受到這批漏洞影響的機種，推出更新版本的韌體；使用 Netgear 交換器的用戶，應依照 Netgear 資安通報的說明，檢查交換器的型號與版本是否列入受影響名單之列，並且儘速更新。

- 影響產品/版本：參見 Netgear 資安通報。
- 解決方案：更新至最新版本韌體。

- 資料來源：
  1. Security Advisory for Multiple Vulnerabilities on Some Smart Switches, PSV-2021-0140, PSV-2021-0144,
  2. Demon's Cries vulnerability (some NETGEAR smart switches)
  3. Draconian Fear vulnerability (some NETGEAR smart switches)
  4. Netgear Smart Switches Open to Complete Takeover

3.7.4、Netgear 修復多款路由器嚴重漏洞，可導致駭侵者遠端執行任意程式碼

Netgear 近日修復存於多款無線路由器的嚴重資安漏洞；該漏洞可導致駭侵者遠端執行任意程式碼。受影響機種用戶應立即進行韌體更新，以修復此一嚴重漏洞。

全球網通大廠 Netgear 近日發表資安更新，修復存於多款無線路由器的嚴重資安漏洞 CVE-2021-49847；該漏洞可導致駭侵者遠端執行任意程式碼。受影響機種用戶應立即進行韌體更新，以修復此一嚴重漏洞。

該漏洞存於 Netgear 提供用戶進行家長分級內容控制的軟體「Circle」之內。資安專家指出，在進行 Circle Patental Control Serive 的更新過程中，攻擊者可以透過中間人攻擊手法取得某些 Netgear 路由器的 root 權限，並且執行任意程式碼。

攻擊者在利用 Circle 漏洞前，必須先進入該路由器下的內部網段，並且能夠攔截該路由器的網路通訊封包，才能利用此漏洞發動攻擊。

資安專家說，雖然 Netgear 的路由器本身並未預設開啟家長內容分級控制功能，但在路由器的作業系統中，相關的服務更新 daemon Circled 預設是開啟運作的，因此駭侵者仍有機會在未啟用家長控制功能的 Netgear 路由器上利用此漏洞。

資安專家說，一旦駭侵者成功利用此漏洞控制 Netgear 路由器，即可透過該路由器之下的內部網路，找到其他可以對其發動攻擊的目標，並且發動其他類型的駭侵攻擊；例如發動近來相當嚴重的 PrintNightmare 攻擊活動，或是各種勒贖攻擊。

受影響的 Netgear 路由器款式共有 11 種，多半為家用 / 小型辦公室使用的機種，型號包括 R6400v2、R6700、R6700v3、R6900、R6900P、R7000（1.0）、R7000（1.3）、R7850、R7900、R8000、RS400 等。

- CVE 編號：CVE-2021-40847
- 影響產品/版本：R6400v2、R6700、R6700v3、R6900、R6900P、R7000（1.0）、R7000（1.3）、R7850、R7900、R8000、RS400 等，詳見 Netgear 資安通報網頁。
- 解決方案：更新韌體至最新版本。

- 資料來源：
  1. Mama Always Told Me Not to Trust Strangers without Certificates
  2. Welcome to NETGEAR Support
  3. Netgear fixes dangerous code execution bug in multiple routers

3.7.5、Exchange Autodiscover 錯誤，導致取得十萬 Windows 用戶登入資訊

資安研究人員發現一個基於 Microsoft Exchange Autodiscover 協定設計與實作錯誤的駭侵方法，可以輕易取得十萬個 Windows 用戶登入資訊。

資安廠商 Guardicore 的研究人員，日前發現一個基於 Microsoft Exchange Autodiscover 協定設計與實作錯誤的駭侵方法，可以輕易取得全球十萬個以上 Windows 用戶登入資訊。

據研究人員指出，Microsoft Exchange Autodiscover 的功能，可以根據企業內部預先定義好的設定值，自動組態設定用戶的 Email 應用程式；用戶在其 Email 應用程式（例如 Outlook）中輸入帳號密碼後，應用程式會把登入資訊傳送到多個 Exchange Autodiscover URL，以進行驗證與組態，並將結果傳回使用者的 Email 應用程式；但如果使用者的應用程式無法驗證上述 URL，就會根據一些預先定義的規則，創造一些可能存有 Exchange Autodiscover 機制的 URL，例如 http://Autodiscover.com/Autodiscover/Autodiscover.xml。

研究人員指出，問題就出在這些由 Email 應用程式自行產生的 URL，可能是不被信任的網域伺服器；因此擁有這些網域的控制者，就有可能收到由 Email 應用程式傳來要求驗證的用戶登入資訊。

Guardicore 為此註冊了多個網域，例如 Autodiscover.com.br、Autodiscover.com.cn、Autodiscover.com.co、Autodiscover.es、Autodiscover.fr、Autodiscover.uk 等，看看可以攔截到多少由 Microsoft Exchante 用戶 Email 應用程式誤傳來的登入資訊；結果在 2021 年 4 月 20 日

到 2021 年 8 月 25 日的四個多月間，收集到來自全球近 10 萬個不重覆 Windows 用戶的登入帳號與密碼。

- 解決方案：資安專家建議，在微軟正式推出更新程式前，各企業應在防火牆或 DNS 伺服器中阻斷任何 autodiscover.[tld] 的對外連線，以免 Email 應用程式向外輸出用戶登入帳密，並遭駭侵者取得以發動攻擊。

- 資料來源：
  1. Autodiscovering the Great Leak
  2. Hundreds of Thousands of Credentials Leaked Due to Microsoft Exchange Protocol Flaw
  3. Microsoft Exchange Autodiscover bugs leak 100K Windows credentials
  4.

3.7.6、微軟 9 月 Patch Tuesday 更新包，一次修復 86 個各式漏洞

微軟推出 2021 年 9 月分例行性「Patch Tuesday」軟體更新，一共修復多達 86 個各式漏洞，其中更有 2 個 0-day 漏洞在內。

微軟日前正式推出 2021 年 9 月分例行性「Patch Tuesday」軟體更新修補包。在這次例行性的更新中，一共修復多達 86 個各式漏洞，其中更有 2 個 0-day 漏洞在內。

這 86 個漏洞中，其中有 26 個發生於 MIcrosoft Edge 瀏覽器，其餘 60 個散見在微軟 Windows、Office、Azure 等軟體或服務中。若從漏洞的性質來看，有 27 個漏洞屬於權限提升類漏洞、2 個為安全防護繞過漏洞、16 個遠端執行任意程式碼漏洞、11 個資訊洩露漏洞、1 個服務阻斷漏洞、8 個假冒詐騙漏洞。

在這次修復的兩個 0-day 漏洞中，CVE-2021-36968 是發生在 Windows DNS 系統中的漏洞，可導致駭侵者提升執行權限。這個漏洞目前還沒有傳出遭到大規模用於攻擊的情資。

另一個 0-day 漏洞 CVE-2021-40444 則已遭到駭侵者大規模用於駭侵攻擊。這個漏洞發生在 Microsoft MSHTML 系統中，駭侵者可利用此漏洞遠端執行任意程式碼。典型的攻擊手法是透過特製的 Word 文件檔案，在受害者電腦中安裝一個惡意 DLL 檔案，接著在該電腦中安裝一個 Cobalt Strike beacon，藉以遙控該 Windows 電腦，並且竊取各種檔案與資料。

另外此次修復的漏洞中，有三個危險程度較高，被列為「嚴重」等級的漏洞，分別是發生在 Open Management Infrastructure 的遠端執行任意程式碼漏洞 CVE-2021-38647、發生在 Windows Scripting Engine 的記憶體崩潰漏洞 CVE-2021-26435、發生在 Windows WLAN AutoConfig Service 的 遠端執行任意程式碼漏洞 CVE-2021-36965。

- 解決方案：強烈建議微軟各種軟體與服務用戶，應立即透過系統更新功能來修補漏洞，以避免駭侵者透過已知漏洞發動攻擊。

- 資料來源：
  1. Microsoft September 2021 Patch Tuesday
  2. Microsoft Patch Tuesday, September 2021 Edition
  3. Microsoft September 2021 Patch Tuesday fixes 2 zero-days, 60 flaws

第 4 章、 資安研討會及活動

HITCON Pacific 2021	
活動時間	**2021/10/27 - 2021/10/28**
活動地點	**線上觀看**
活動網站	**https://docs.google.com/forms/d/e/1FAIpQLSfnKq80w4N_Lk7nkpl-dyzHgTIvhx6JX0j8GCutbvfSlfYjvw/viewform**
活動概要	 **主辦單位：社團法人台灣駭客協會(HITCON)、CHROOT** 協辦單位：台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 10 月 27、28 日兩天，線上 20 場資安研討會，任您挑選免費聽課。 今年 HITCON Pacific 以資安的強韌力 × 復原力 × 實踐力為核心，匯集當前海內外頂尖、深入的資安議題、可實踐應用的資安解決方案為主軸，將帶給您深度學習。 直接線上申請公司票： 票價：免費 需以任職公司的信箱至申請表單提交報名申請，經主辦單位審核，符合資格者始完成報名。 聯絡我們：若有任何票務問題請告知大會服務信箱 pacific@hitcon.org

HITCON 2021 台灣駭客年會	
活動時間	**2021/11/26(Fri) - 2021/11/27(Sat)（10/10 截止售票）**
活動地點	**中央研究院人文社會科學館(台北市南港區研究院路二段 128 號)**
活動網站	**https://hitcon.kktix.cc/events/hitcon-2021**
活動概要	 **主辦單位：社團法人台灣駭客協會(HITCON)** 【 HITCON 2021 台灣駭客年會熱烈售票中 】 HITCON（台灣駭客年會）是國內最具技術含量的資安研討會，我們有別於一般商業性質濃厚的研討會，台灣駭客年會提供一個舞台，讓駭客們有機會與大家分享最新、最深入的資安技術，且面對面交換經驗、自由的對談。 今年年會由主題「Work from home, hack into home」帶出 COVID-19 的爆發，改變了人們的生活習慣，使 Working From Home 成為必要的選項，而我們的日常生活也被進一步推向虛擬世界。精彩議程從居家的資訊安全，到企業與組織的防護模式轉變，延伸至各國間的資安聯防，HITCON 將是鏈結亞洲乃至全球大眾生活不可或缺的橋樑，因此我們邀請更多駭客一同參與、探索，挖掘更多的漏洞，推進資安的發展！ 除了精彩絕倫的技術議程外，亦規劃一系列資安相關的活動，包含虛實整合的資安解謎遊戲「駭客貓歷險記」、技術比拼的「煉蠱大賽」、蘊藏各種秘密的「Bounty House」、模擬駭客村落的「Village」、幫助你在求職路上更順利的「資安人力系列活動」，使每一位對資安有興趣的朋友，無論是專家駭客或入門者，都得以在這場盛會中有所收穫、盡興而歸。 『在純技術的領域裡面沒有黑與白，我們認為駭客是代表著高超的技術、挑戰的精神！』 HITCON 是駭客們的聚會，在這你可以體驗到真正的駭客文化，我們歡迎所有對資訊安全有興趣的朋友，一同參與這一年一度的駭客盛會！

【資安學院】政府受駭案例與反思	
活動時間	**10/21 18:30-21:30（共計 3 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NQ==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** ● 課程大綱： -政府企業資安威脅種類 -資安攻擊入侵思維 -實際案例 1：我國重要油品事業近期遭勒索病毒案 -實際案例 2：其它政府機關遭駭客入侵案 -個人資安防護議題 ● 課程對象： -企業資訊部門 -提供資訊安全服務之業務、專案、技術與決策等主管及人員 -對本課程有興趣，欲提升資安專業知能者。 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 -每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 -以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

【資安學院】資安事故處理實務	
活動時間	**10/27（三） 09:00-17:00（共計 7 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NA==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** ● 課程說明：本課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務。 ● 課程大綱：端點勒索軟體與 APT、網站入侵、雲端線上服務、行動與物聯網裝置、資料庫和資料外洩等事故案件解析、報告撰寫。 本課程需自備筆電、並具備 VMware 環境 ● 課程對象： 資安(訊)主管、資訊安全管理人員、系統管理人員、網路管理人員 具備 1 年以上實務操作經驗與資安事件調查知識尤佳 ● 活動聯絡人：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

加密技術的應用如何在隱私與安全間取得平衡?	
活動時間	**2021 年 10 月 27 日（三）14:00-16:00**
活動地點	**本活動採線上視訊會議方式辦理**
活動網站	**https://www.twsig.tw/20211027/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 加密技術的廣泛使用，其複雜性往往使得執法機構在打擊犯罪與維護國家安全面臨了極大挑戰，許多恐怖份子及犯罪集團皆利用端點對端點加密技術進行通訊，並藉此躲避司法調查與相關起訴，因此使得執法人員無法針對重犯罪內容與活動採取相對應之執法行動，進而影響個人及國家安全。 今年 7 月，歐洲刑警組織 Europol、歐洲司法組織 Eurojust、法國與荷蘭之警方及司法單位共同發表聯合聲明，宣布摧毀組織型犯罪經常使用 EncroChat 加密通訊網路，並藉由攔截與分析訊息內容，因而成功在各國逮捕了上百名涉嫌販毒、謀殺或暴力犯罪的嫌犯。在此事件後，多數執法單位更加相信，加密通信技術的濫用是其犯罪活動的主要推動者。 各國政府呼籲，建立「合理、彈性」的技術方案，協助執法機關在必要且合乎比例的授權下，以可讀、可用格式存取內容，且受到強大監督，並能提供政府或其相關單位協助，以加速合法存取內容，如此一來才能保護社會免受犯罪、恐怖主義和其他危害；人權觀察家則認為，一旦提供「解密金鑰」將弱化我們的數位安全，並危害民眾隱私；科技業者表示，這將對保護使用者隱私的加密技術帶來巨大危機，原本為使用者提供的端對端加密服務，理應連業者自身都無法破解，也唯有如此，使用者的私人對話才能受到真正的保護。 保護人民隱私與安全，是建立於法律基礎之上，本座談將邀請不同利害關係人，在合法授權、比例原則及監督機制前提之下，探討有關加密與隱私之間的關係，歡迎各界一起加入討論。 主辦單位保留議程更改權利，若有變動以網站公告為主。

【資安學院】國際資安標準與攻擊趨勢分享	
活動時間	**11/10 09:00-12:00（共計 3 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/2678**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 隨著 5G 網路逐漸普遍，更快的網路速度與低延遲的特性可能會催生新的殺手級應用，許多企業早已磨拳霍霍、準備在市場大放異彩。在新的技術與應用發展的過程當中可能帶來新的資訊安全與個人隱私問題，當企業將產品與服務快速地推向市場同時，如何降低其中造成的資安風險已成為企業首要必須解決的問題。 雖然近年來有越來越多的資安標準與認證，但是許多企業在面對這些資安標準、要求及認證時，仍然不知從何做起。本次課程將會解析常見的產品與服務資安標準內容，讓大家可以快速了解資安標準與認證的主軸。 除此之外，近年來勒索軟體的大肆活動，也讓企業不得不投入更多的資源到這場與駭客的軍備競賽。本次課程透過分享近年來國際資安攻擊的實例案例，讓大家了解駭客攻擊趨勢的發展，作為日後強化企業資安防護能力的參考。 課程大綱：國際資安威脅與案例分享、國際資安標準解析與應用、企業資安防護框架介紹 課程對象：企業資訊部門 / 提供資訊安全服務之業務、專案、技術與決策等主管及人員 / 對本課程有興趣，欲提升資安專業知能者。 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw　Tel: (02)2553-3988 Ext：388 每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

第 5 章、 2021 年 9 月份資安情資分享概況

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

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

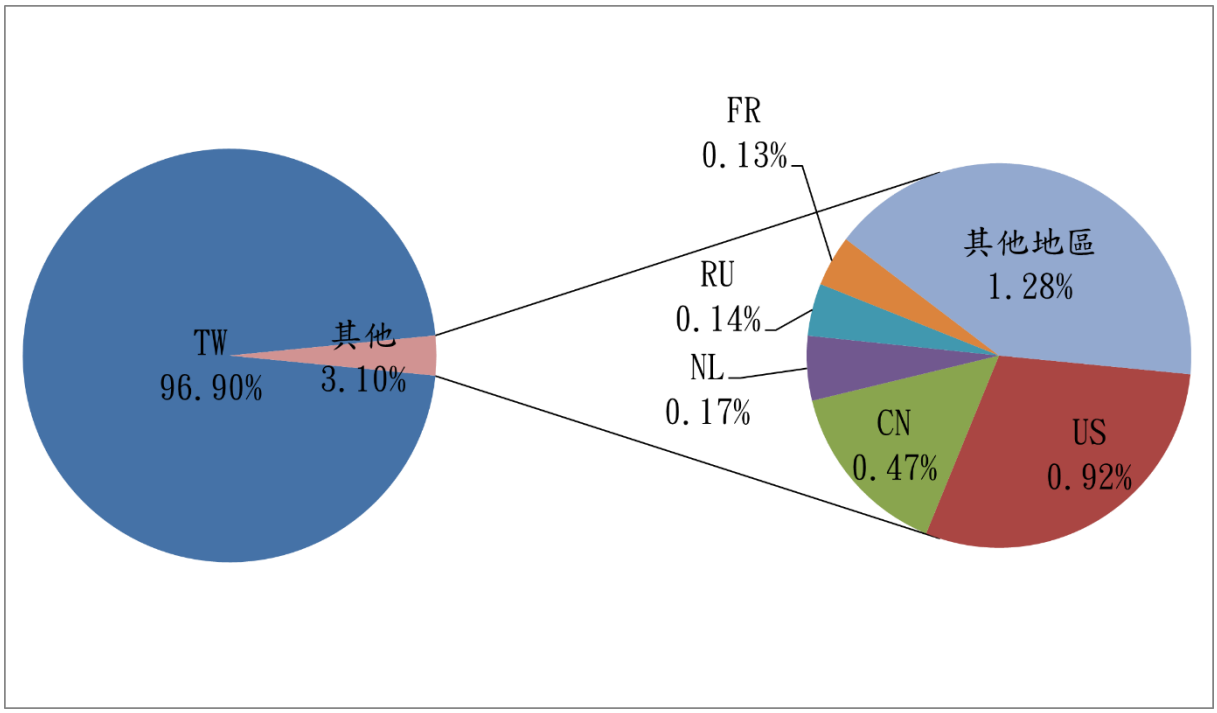


圖 1、分享地區統計圖

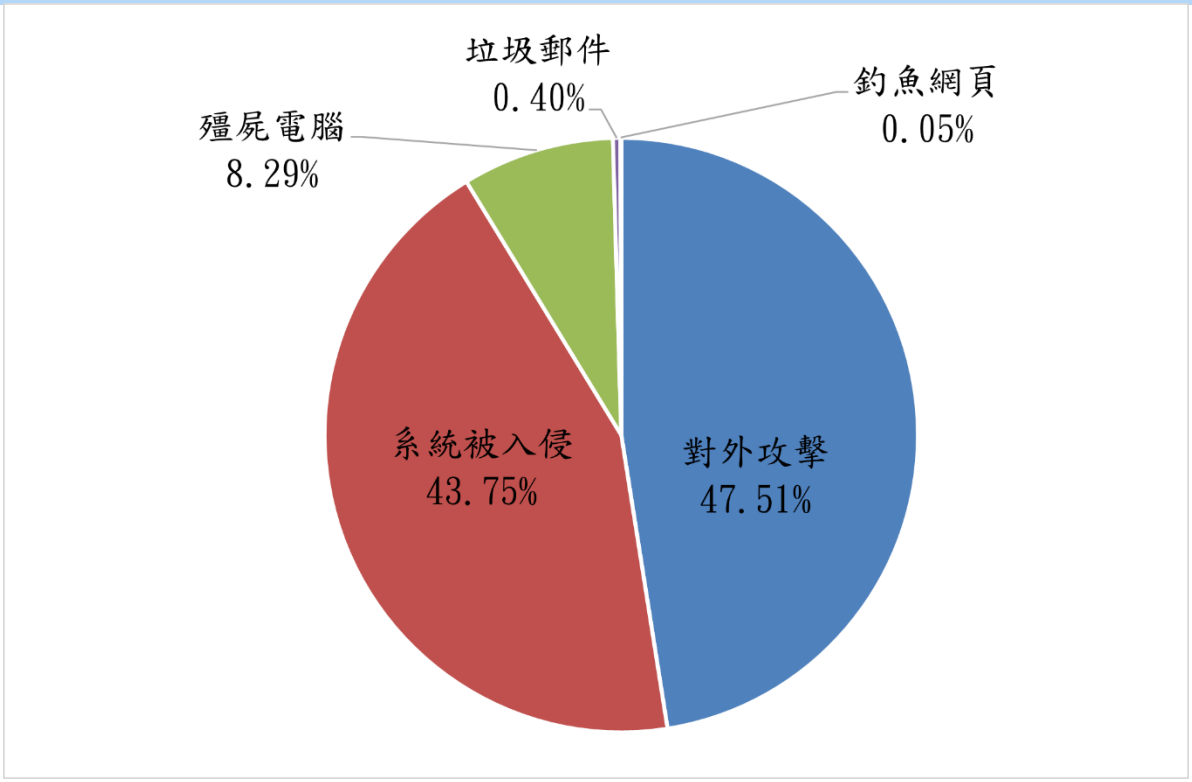


圖 2、分享類型統計圖

發行單位：**台灣電腦網路危機處理暨協調中心**
(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：**2021 年 10 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**