TWCERT/CC 資安情資電子報

2021 年 7 月份

電子報序言

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

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 6 章節：

第 1 章、封面故事：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、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第 5 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 6 章、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

全球最大食品製造商 JBS Foods，因駭侵攻擊導致生產停擺

全球最大的生鮮牛豬肉食品製造商 JBS Foods，其全球各地子公司同時遭到一起駭侵攻擊，多家工廠因而停止運作。

全球最大的生鮮牛豬肉食品製造商 JBS Foods，其全球各地子公司同時遭到一起駭侵攻擊，包括美國、澳洲、英國等國境內的多家工廠，因而停止運作。

攻擊事件是在上周末發生的，目前澳洲政府已經接獲 JBS Foods 的資安事故通報，正在與 JBS Foods 共同調查事件發生的原因，並且共同設法讓 JBS Foods 旗下的工廠恢復生產。

澳洲農業部長 David Littleproud 在接受媒體訪問時指出，「駭侵者攻擊的目標是用以確保牛肉品質的核心系統，目前澳洲當局與廠商正在努力使其恢復正常，讓消費大眾與海外市場重拾對澳洲牛肉產品的信心。」

澳洲政府也指出，由於這是一起跨國的駭侵攻擊事件，該國相關單位也與其他國家的司法單位密切合作偵辦本案。

雖然 JBS Foods 的發言系統目前還沒有針對這起攻擊事件發表任何說明，不過 JBS Foods 澳洲分公司的執行長 Brent Eastwood，在接受媒體採

訪時，已經確認該公司確實發生駭侵攻擊事件。

資安專家指出，雖然目前還沒有任何關於這次攻擊事件的具體資訊，但根據攻擊是在周末發動的這個特色，專家研判極可能是屬於勒贖攻擊。

澳洲農業部長雖然沒有指明 JBS Foods 公司中的哪些單位遭到攻擊，但他曾警告這次攻擊事件對 JBS Foods 委外生產線、產品物流中心與集貨中心等單位的工作人員，在經濟上可能會遭到嚴重打擊；而澳洲肉品工會昆士蘭分部秘書長 Matt Journeaux 也指出，可能有數千名 JBS Foods 的員工或協力廠商員工，生計將受到這次駭侵攻擊影響。

- 資料來源：
  1. JBS global meat processing operations paralysed by cyber attack
  2. Cyber attack shuts down global meat processing giant JBS
  3. Food giant JBS Foods shuts down production after cyberattack

第 2 章、 資安小知識

勒索軟體防護指南

- 什麼是勒索軟體?

勒索軟體是一種惡意軟體，以加密設備上的文件來威脅受害者，要求受害者支付贖金(通常是加密貨幣)才能解密文件，還會嘗試傳播感染網路上其他設備，無差別或是針對具有高價值的目標攻擊。

勒索軟體的犯罪模式十分成功，因此不斷演變出新的變種或與其它惡意軟體結合形成更有威脅的攻擊行為，可針對各種組織或應用領域進行攻擊，不只會影響到服務或企業的正常運作，甚至可能造成受害企業的倒閉。

- 勒索軟體類型

勒索軟體可以進行無差別的攻擊(Indiscriminate Attack)，即駭客大規模且不加選擇地散布勒索軟體進行攻擊，亦或是針對性的目標式攻擊(Targeted Attack)，鎖定醫療組織、工業企業和運輸等行業，以取得更高的贖金，目標式攻擊使用更複雜的魚叉式網路釣魚(Spear Phishing)或利用進階持續性滲透攻擊(Advanced Persistent Threat, APT)及系統漏洞進行攻擊，以避開日益精進的垃圾郵件過濾系統及資安防護機制。

勒索軟體造成的威脅損害類型為：

1. 資料可用性：是最主要的威脅傷害型態，加密受害電腦中的檔案，要求受害者支付贖金換取解密金鑰，然而即使受害者願意支付贖金，也未必能確保資料完整的恢復。

2. 系統可用性：特徵是阻止受害者存取受感染的電腦或行動裝置，鎖住電腦螢幕與瀏覽器導致無法使用，藉以達到威脅的目標，。

3. 隱私挾持(Doxware)：主要是對資料的機密性造成傷害，駭客將受害者電腦中的資料大量加密和上傳，以洩漏該隱私或機敏資料作為要脅，迫使受害者支付贖金換取資料不外洩。

- 勒索軟體的攻擊途徑

要防範勒索軟體，必須先對勒索軟體的攻擊途徑有所瞭解。勒索軟體感染在完整的攻擊行為中，是屬於末尾的步驟，因此企業如果能在先期發現攻擊跡象，便有可能阻止勒索軟體攻擊，也就是盡早發現憑證盜竊和橫向移動的跡象，可防止勒索軟體悄悄入侵企業網路。

駭客入侵電腦或企業網路的主要方式為：

1. 資安漏洞遭利用：勒索軟體會利用受攻擊目標的資安漏洞直接感染，例如 2017 年的 WannaCry 勒索軟體，掃描檔案分享的 SMB (Server Message Block) 協定漏洞，進而快速感染。若沒有直接可感染的漏洞，則透過可植入後門或提取權限的漏洞來逐步入侵，尤其是 AD (Active Directory)、防毒軟體類型的伺服器，因具有檔案分派安裝權限，遭入侵後，修改其群組原則、工作排程，即可大量派送安裝勒索軟體，達到索取贖金的目標。

2. 網路釣魚攻擊：勒索軟體可能透過釣魚電子郵件或釣魚網站，誘導受害者點擊執行惡意連結與附件，或是針對性的發起魚叉式網路釣魚攻擊，偽裝成合法的組織、企業或關係人，強化受害者點擊執行惡意檔案的誘因，一旦執行惡意附件，勒索軟體就開始對檔案加密，若是惡意連結，則會導向使用者到已掛馬的網頁上，再進行勒索軟體的下載。

3. APT 攻擊：APT 攻擊為潛伏期長且深度隱藏的攻擊手法，攻擊者入侵到內網後，取得管理者帳號密碼等資訊，在內網橫向擴散勒索軟體，再一次性加密多台重要主機資料，將威脅最大化。

4. OT 網路攻擊：在工廠產線的 OT(Operational Technology)網路環境中，勒索軟體會先攻擊 IT 網路設備，而由於 IT 設備與 OT 環境連結，故即使 IT 設備被攻擊不一定會影響到 OT 環境，也可能造成關鍵的工廠操作流程出現問題，例如近期所發生，美國燃油供應商 Colonial Pipeline 遭勒索軟體攻擊而停止服務，甚至讓美國政府宣布進入緊急狀態。

- 如何識別受勒索軟體攻擊?

受到勒索軟體攻擊，初期特徵是因為對大量檔案做加密運算，所以會發現硬碟使用率會大幅提升，另外，受影響的檔案通常會被修改副檔名。

檔案被加密結束後，在大多數的狀況下，因勒索軟體需要向受害者要求贖金，所以會將勒索訊息顯示在設備螢幕上，亦或是留下相關文件，也會有連路方式，讓受害者可以與攻擊者溝通付款的議題。

攻擊者甚至可能威脅要在網上發布數據以迫使受害者支付贖金，例如 MAZE 勒索軟體的攻擊者，公佈了 Hammersmith Medicines Research 的醫療檔案以迫使他們支付贖金。

- 勒索軟體預防措施

一、個人事前預防措施

1. 保護系統

1.1 使用防毒軟體，並及時更新系統、軟體和應用程序：攻擊者通常利用未修補的漏洞來訪問未經授權的系統和網路，以執行後續惡意活動。

1.1.1 應安裝防毒/防惡意軟體並保持其病毒碼/惡意特徵碼更新。每周至少對系統和網路執行一次掃描，並掃描所有收到的文件。

1.1.2 當移動儲存設備連接時應執行防毒掃描。

1.1.3 將系統、應用軟體更新到最新版本，並下載最新的安全更新檔。

1.2 僅在需要時啟用 Microsoft Office 巨集：勒索軟體可能透過惡意 Microsoft Office 檔案感染，誘使受害者啟用巨集以查看檔案內容。

1.3 提高資安意識：這是防止勒索軟體攻擊的關鍵，應提高資安意識及良好的網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，不打開未知或不受信任來源的電子郵件的附件。

2. 保護資料

2.1 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料建議以儲存媒體進行離線儲存。

2.2 啟用 Windows 受控制資料夾存取功能：微軟已在 Windows10 中內建有資料夾的存取控制功能，但預設並未啟用，需手動調整設定。其功能是限制只有安全的應用程式才能存取特定資料夾，防止勒索軟體對資料進行加密或竊取。

二、企業組織事前預防措施

企業或組織除前述措施外，需要採取更為積極的方法來保護系統和資料。

1. 保護系統

1.1 強化具派送功能伺服器安全：防毒軟體中控、AD 伺服器、資產管理系統等因具有軟體派送功能，更需注意安全更新，並密切觀察其群組原則或工作排程不正常異動狀況。

1.2 最小化開放埠的設置：勒索軟體可能會利用對外曝露的服務和開放埠（例如 RDP 埠 3389 和 SMB 埠 445）在網路中傳播，除了確認其開放的必要性外，還應確認使用這些服務的對象為可信任。

1.3 實施網路分段區隔並監控流量。

1.3.1 在實施網路分段區隔後，如果某一區段受到威脅，至少可限制勒索軟體在網路中的傳播。

1.3.2 監控任何可疑連接的網路流量，並阻止任何與已知惡意 IP、URL 的網路連線行為。

1.3.3 在工控環境，更應將 IT 與 OT 環境實施強烈的網路分段區隔措施，避免造成工安問題。

1.4 實施應用程序控制：應考慮安裝可控制應用程序、目錄白名單的軟體，僅允許執行已批准的程序，以防止惡意軟體程序被執行。

1.5 人員的最小使用權限：為了減少攻擊者獲得管理權限的機會，應該：

1.5.1 控制和限制存取權限，僅限於需要完整存取權限才能執行工作的人員獲得授權。

1.5.2 為管理者以外的使用者提供工作所需的最低權限。

1.5.3 查看和管理所有使用戶帳戶的使用情況，並禁用非活動帳戶。

1.5.4 實施多因子身份驗證。

1.6 提高資安意識：應定期對員工進行培訓，建立良好資安意識及網路使用習慣，並進行社交工程演練，提高訓練成效。

1.7 監控可疑活動：監控可疑掃描活動和未經授權的登錄嘗試，對防止遭到攻擊具有極大幫助。

2. 保護資料

2.1 加密重要或敏感資料：應對重要或敏感資料進行加密，如果資料被竊取，可以使攻擊者難以處理這些資料，另外，某些勒索軟體僅對常用文

件類型（例如圖檔和文檔）起作用，則加密還可以防止它們檢測到文件。

2.2 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料必須離線儲存且不能連接到既有企業網路中，可防止勒索軟體透過網路影響備份資料。

2.2.1 3-2-1 備份原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。

2.3 定期維護關鍵系統的映像檔：虛擬機或服務器的映像檔包括預先配置的作業系統和相關的應用軟體，當發生攻擊，而需要重建系統，可以利用這些映像檔達到快速部署恢復。

3. 準備事件應變計劃

3.1 在事件發生之前，制定事件應變計劃並進行演練，以測試計劃是否可行是非常重要的。在受到攻擊時難以即時判斷正確作法，透過已制定好的計劃並實施，將有助於員工了解要採取的行動，並確定各項系統與環境的恢復優先等級。

3.2 如在工控環境，不只是 IT 環境需要制定事件應變計畫，更應依據設備機台特性分類制定各別的事件應變計畫，以完善整體安全。

- 被感染後的應變措施

大多數被勒索軟體加密的資料難以被破解，但可採取以下步驟降低影響：

1. 立即斷開受感染設備與所有網路的連接，無論是有線、無線還是基於行動網路。在非常嚴重的情況下，可考慮關閉 Wi-Fi、禁用任何核心網路連接（包括交換機）以及斷開 internet 連接。
2. 重置包括密碼在內的權限憑證。
3. 確認受感染設備已完全的清除並重新安裝作業系統。

4. 在利用備份進行還原之前，需確認該備份沒有任何惡意軟體，如果已非常確認備份和連接它的設備是乾淨的，則恢復工作應該只從備份進行。

5. 將設備連接到乾淨的網路，以便下載、安裝和更新作業系統和所有其他軟體。

6. 安裝、更新和執行防毒軟體。

7. 監控網路流量並執行防毒掃描以確定是否仍有感染。

8. 大多數被勒索軟體加密的資料難以被破解，但仍可嘗試透過勒索軟體名稱、副檔名等資訊，檢閱該病毒的類型，在 no more ransom project 的網站上，尋找可信任資安單位提供的解密工具。

9. 可尋求外部資安專業單位協助事件處理。

10. 建議將攻擊事件資訊藉由 TWCERT/CC 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。

第 3 章、 資訊安全宣導

留意實聯制 QR Code 詐騙，發送簡訊前須確認正確的傳送對象

因疫情升溫，指揮中心宣布疫情警戒至第三級，民眾外出到公共場所需進行實聯制登記。因此行政院也推出簡訊實聯制，民眾免填個資，只需掃描 QR Code 並傳送簡訊至 1922，即可記錄足跡。

店家張貼於店外的簡訊實聯制 QR Code，有遭有心人士隨意更換成惡意連結的風險，使民眾連結至釣魚網頁或傳送簡訊到高額付費號碼，以騙取個資或錢財。

警政署也於 165 全民防騙粉絲專業提醒以下注意事項：

1. 為防止張貼於店外的 QR Code 遭有心人士更換，建議店家務必要不定期進行檢查，以確認連結的正確性。
2. 建議店家於非營業時間，將 QR Code 實聯制公告收入店內保管。
3. 民眾在傳送簡訊時也需注意，傳訊的對象應確認為「1922」再傳送。

165 全民防騙也提醒民眾可以加入疾管署推出的疾管家官方 LINE 帳號，使用其掃描功能以辨識是否為 1922 簡訊實聯制的 QR Code。若掃描後出現不明網址或要求安裝程式，務必通知店家確認 QR Code 正確性並且不要點擊，以免手機遭植入惡意軟體，或連結到釣魚網頁被騙取個資。

- 資料來源：
  1. 你知道嗎 疾管家官方 line 帳號的掃描功能可以辨識「假」簡訊實聯制 QR Code
  2. 店家將 QR Code 張貼於店門外，務必不定期檢查，以防遭不肖人士更換
  3. 發送實聯制前先注意，詐騙集團偷換 QR Code 讓民眾傳到高額付費電話
  4. 簡訊實聯制驚傳「假 QR Code 詐騙」！警政署呼籲：掃碼後一定要確認 1 數字
  5. 不肖人士偷換實聯制 QR Code 掃描後恐傳訊到高額付費號碼

第 4 章、 國內外重要資安事件

4.1、資安趨勢

4.1.1、統計公布 2020 年提報 CVE 漏洞數量最多的 20 大企業、產品與漏洞類型

一個長期觀測統計各科技大廠產品漏洞提報情形的網站，公布去年（2020）提報漏洞數量最多的前 20 大廠牌、產品與漏洞類型。

長期觀測統計各科技大廠產品漏洞提報情形的網站 stack.watch，公布去年（2020）提報漏洞至 CVE 資料庫數量最多的前 20 大廠牌、產品與漏洞類型。

以產品來說，排行榜中的前 10 名，以及其提報漏洞數量，分別為：

1. Microsoft Windows 10 (802)
2. Microsoft Windows Server 2016 (790)
3. Microsoft Windows Server 2019 (743)
4. Google Android (696)
5. Debian Linux (510)
6. Microsoft Windows Server 2012 (443)
7. Microsoft Windows 8.1 (435)
8. Microsoft Windows RT 8.1 (429)
9. Fedora Project Fedora (398)

10. Microsoft Windows 7 (386)

以廠牌來說，排行榜中的前 10 名，以及其提報漏洞數量，分別為：

1. Microsoft (1188)
2. Google (950)
3. Oracle (822)
4. Debain (510)
5. Red Hat (403)
6. Fedora Project (398)
7. OpenSuse (389)
8. Apple (381)
9. IBM (338)
10. Cisco (307)

此外，該網站也據依據漏洞類型提供了排行榜，包括通報數量與佔比如下：

1. XSS (1938, 11.4%)
2. 權限管理不當 (1073, 6.3%)
3. 輸入字串驗證不當 (989, 5.8%)
4. 資訊洩露 (977, 5.7%)
5. 記憶體崩潰 (811, 4.8%)
6. 越界讀取 (566, 3.3%)
7. 緩衝區溢位 (530, 3.1%)
8. Shell 注入 (424, 2.5%)
9. SQL 指令注入 (413, 2.4%)

10. 古典緩衝區溢位 (364. 2.1%)

其餘 11 至 20 名的產品、廠牌與漏洞類型，可在該站的詳細報告中檢視。

- 資料來源：
  1. New Windows 10 Security Shock As 1,000 Vulnerabilities Revealed
  2. 2020 Security Vulnerability Report

4.1.2、勒贖團體自黑市買受害對象初步駭入成果，形成「駭侵產業生態系」

愈來愈多駭侵勒贖團體，自黑市的其他駭侵者購買他們駭入對象的初步駭侵成果，再進行進一步的勒贖攻擊，形成駭侵產業生態系。

資安廠商 Proofpoint 旗下的資安專家發現，近來有愈來愈多駭侵勒贖團體，自駭侵黑市的其他駭侵者處，購買他們駭入對象的初步駭侵成果，再用以發動進一步的勒贖攻擊，儼然形成一個駭侵產業生態系。

據 Proofpoint 日前發表的研究報告指出，這類駭侵者之間的「垂直整合」，已經發展成一個利潤豐厚的「產業生態系」；一些較小規模的駭侵者，先針對某些受害者發動駭侵攻擊；其他主要駭侵團體再向其購買「使用權」，進一步發動更大規模的攻擊。

Proofpoint 說，日前對美國的燃油運輸造成極大危害的 Colonial Pipeline 勒贖駭侵事件，即是透過這種「上下游」駭侵者的交易來進行的。

Proofpoint 表示，該公司目前發現至少有 10 個駭侵團體，涉及進行所謂的「前期駭侵攻擊」；這 10 個駭侵團體先以釣魚信等各種手法，入侵受害目標，將惡意軟體植入受害單位後，接著便待價而沽，在黑市中尋找願意出價接手的大型駭侵團體。

大型駭侵團體接下來即可利用這些「預先布署」的惡意軟體，傳送發動後續攻擊使用的酬載勒贖工具來發動攻擊，而不需要自行發現受害者的資安漏洞。

Proofpoint 指出，2021 年上半年至少有 20% 針對金融產業進行的後門勒贖攻擊，是採用這種「垂直分工」的方式來進行。

Proofpoint 在報告中也列出了 TA800、TA577、TA569、TA551、TA570、TA547、TA544、TA571、TA574、TA575 等 10 個觀察到的前端駭侵團體，及其使用的駭侵手法、駭侵工具，以及後續的「客戶」等詳細資料。

- 資料來源：
  1. The First Step: Initial Access Leads to Ransomware
  2. Researchers: Booming Cyber-Underground Market for Initial-Access Brokers

4.2、新興應用資安

4.2.1、資安廠商指出 2021 年加密貨幣最新駭侵手法

資安廠商近期指出 2021 年駭侵者可能會利用來竊取加密貨幣的多種手法；加密貨幣的投資人或持有人，應特別提高警覺。

資安廠商 Digital Shadows 旗下的 Photon Research Team 研究團隊，近期整理多個資安相關研討會上發表的論文，指出 2021 年駭侵者可能會利用來竊取加密貨幣的多種手法；加密貨幣的投資人或持有人，應特別提高警覺。

Digital Shadows 指出，近年來加密貨幣十分熱門，其總市值已經高達 1 兆 7000 億美元；許多投資人只見到獲利機會就大舉投入，但未必事先做好應有的準備，包括認識加密貨幣的運作原理，以及可能涉及的資安與駭侵風險。這相當於為駭侵者敞開一扇有利發動攻擊的方便之門。

報告指出 2021 年駭侵者可能最常用以攻擊加密貨幣的手法，共有四種；第一種是透過反向代理伺服器（reverse proxy）來發送釣魚郵件，並且破解二階段登入驗證：當用戶點按釣魚信中的假連結時，reverse proxy 伺服器會一邊發送以假亂真的登入頁面，讓用戶輸入帳密並收到二階段驗證要求，接著 reverse proxy 再將真的登入帳密和二階段驗證碼發送給真正的登入伺服器，即可取得帳號登入權限，並且發動進一步的攻擊，竊取用戶存在熱錢包中的加密貨幣。

其次，駭侵者也可透過植入挖礦惡意軟體的方式，在用戶不知不覺的情形下，盜用受害者的計算資源來為駭侵者挖掘加密貨幣，例如門羅幣或 Zcash 這兩種匿名性較高的加密貨幣；這會造成用戶的裝置過度負荷，不但耗能大大提升，組件壽命也會顯著減損。

另外，駭侵者也可能利用夾藏在其他應用軟體中的惡意程式碼，在加密貨幣持有人輸入錢包位址進行轉帳時，將轉帳目標偷換為駭侵者錢包位置；或是假冒名人舉辦空投活動，要求用戶先轉一筆加密貨幣給駭侵者錢包，以換取更大額的回報等等，都是常見的詐騙攻擊手法。

- 資料來源：
  1. Cryptocurrency Attacks To Be Aware Of In 2021
  2. Bitcoin And Alternative Cryptos In The Cybercriminal Underground

4.2.2、微軟發現大量挖礦惡意軟體，鎖定 Kubernetes 運算叢集進行攻擊

微軟公司日前發表研究報告，指出該公司發現一個全新攻擊活動，針對眾多 Kubernetes 運算叢集植入挖礦惡意容器（pod），正在大量蔓延。

微軟公司日前發表研究報告，指出該公司發現一個全新攻擊活動，針對眾多執行 Kubeflow instance 的 Kubernetes 運算叢集植入含有挖礦惡意程式碼的 TensorFlow 容器（pod）；這類攻擊活動正在大量蔓延，系統管理員應特別提高警覺。

Kubeflow 是一種開放源碼的熱門專案，多用以在 Kubernetes 中執行機器學習工作，而 TensorFlow 則是一種端對端的開源機器學習平台。

微軟在 6 月 8 日發表的研究報告中說，該公司的資安團隊自五月底開始觀測到 TensorFlow 容器大量布署於 Kubernetes 叢集的高峰；這些被布署的容器，看似來自 Docker Hub 帳號的正常容器，但仔細研究後發現其目的在於挖掘以太幣（Ethereum）與門羅幣（Monero）等加密貨幣。

微軟資安研究員說，這些容器同時大量布署，顯示駭侵者事前經過縝密調查，掌握所有存有安全設定漏洞的 Kubernetes 運算叢集後，才發動大舉攻擊。

微軟說，這波攻擊活動十分類似去年六月發生過的案例，當時也有攻擊者攻擊設定錯誤的 KubeFlow，透過惡意式碼挖掘門羅幣。

微軟的研究人員在報告中詳細分析了攻擊流程，並且建議所有執行 Kubernetes 運算叢集的系統管理人員，應該立即檢視安全設定，看看是否鎖定其中央控制面板，並確認沒有曝露在外網中供人任意存取；如果該運算叢集必須放在外網，就必須強化登入安全認證機制。

- 資料來源：
  1. New large-scale campaign targets Kubeflow
  2. Misconfigured Kubeflow workloads are a security risk
  3. Microsoft: Big Cryptomining Attacks Hit Kubeflow

4.2.3、PyPI 程式庫，遭植入挖礦惡意程式碼套件

資安專家發現在 Python 中的 PyPI 程式庫，遭人植入多個挖礦惡意程式碼套件；不慎下載安裝的開發者電腦，就會被攻擊者用以挖掘加密貨幣。

資安廠商 Sonatype 旗下的資安專家 Ax Sharma，日前發現在 Python 中的 PyPI 程式庫內，有多個程式套件遭人植入多個含有挖礦惡意程式碼的套件，並以拼錯但極為近似某一常用套件的名字命名；不慎下載安裝的開發者電腦，就會被攻擊者用以挖掘加密貨幣。

據 Ax Sharma 日前的研究報告指出，這些被上傳到 PyPI（Python Package Index）中含有挖礦惡意程式碼的套件，分別如下：

- maratlib
- maratlib1
- matplatlib-plus
- mllearnlib
- mplatlib
- learninglib

這些惡意套件的名稱，故意接近常用的描點用套件 matplotlib，意圖混淆視聽並誘使開發者下載安裝；開發者如果執行這些套件內的程式碼，就會下載並執行一個叫做「Ubqminer」的挖礦惡意軟體，利用開發者電腦的計算資源來挖掘 Ubiq 加密貨幣，並轉帳給攻擊者。

資安專家還發現另一個變種，攻擊原理和手法類似，但改用另一種稱為 T-Rex 的開源挖礦軟體，可利用開發者電腦上的圖形處理器（GPU）來加快

挖礦運算速度。

研究指出，上述這些惡意挖礦套件，都是由同一個帳號「nedog123」上傳的，至今各套件的下載次數，自 300 多次到近 2,400 次不等。

報告也指出，這類藉由攻擊開源開發工具而發動的供應鏈攻擊駭侵活動，近年來案例數量有逐漸增加的趨勢，受害者除了開發者本身外，透過這種惡意程式碼開發出來的軟體產品，也可能含有惡意程式碼，造成更大的危害。開發者在下載安裝各種開源開發工具與套件時，應特別提高警覺。

- 資料來源：
  1. Sonatype Catches New PyPI Cryptomining Malware
  2. Malicious PyPI packages hijack dev devices to mine cryptocurrency

4.2.4、駭侵者郵寄假冒硬體錢包，騙取用戶存入的加密貨幣

近來發生最新的加密貨幣詐騙手法，駭侵者寄送假冒的硬體加密貨幣錢包替換品給受害者，藉以竊取加密貨幣。

近來發生最新的加密貨幣詐騙手法，駭侵者寄送假冒的硬體加密貨幣錢包替換品給受害者，藉以竊取加密貨幣。

遭到駭侵者假冒的硬體加密貨幣錢包，是由 Ledger 公司推出的「Ledger Nano X」；駭侵者透過包裹寄送假冒的 Ledger 硬體錢包給受害者，在內附上文筆拙劣的通知信，假稱「由於資安理由，特別寄送全新加密貨幣錢包硬體」，要求用戶透過說明書的指示來轉移存在原硬體錢包中的加密貨幣到「新錢包」中。

駭侵者取得的受害者名單，是先前遭不明駭侵者自 Ledger 公司取得的，並在 2020 年 12 月遭人張貼於某駭侵相關論壇；名單中一共有 272,853 名 Ledger 硬體錢包的用戶資料。

在 Reddit 論壇上，有收到假冒 Ledger 硬體錢包的用戶，將其收到的假冒硬體錢包拆開，並與真正的 Ledger 錢包硬體電路相互比對，可以發現電路布局與使用的元件略有不同；資安專家分析該照片後指出，該假冒硬體錢包，就電路來看，似乎有一個架構在 Ledger 上的 USB 隨身碟，可能用以在用戶電腦上植入惡意程式碼。

在用戶收到的「轉移指南」中，要求用戶輸入當初設定的復原短詞；一旦用戶照實輸入，這些復原短詞立即會被傳送給駭侵者，即可用以竊取用戶存入的所有加密貨幣。

Ledger 公司表示，已經掌握此類駭侵攻擊的情報；該公司呼籲用戶提高警覺，在任何情況下都不應分享復原短詞給任何人，或是在不明的軟體中輸入這些復原短詞。

- 資料來源：
  1. Ongoing phishing campaigns
  2. Package from Ledger. Is this legit?
  3. Criminals are mailing altered Ledger devices to steal cryptocurrency

4.2.5、駭侵者在盜版遊戲中植入挖礦惡意軟體，不法獲利高達 200 萬美元以上

資安廠商發現一個名為 Crackonosh 的挖礦惡意軟體，由放在論壇上的盜版遊戲夾帶，植入在受害者電腦內挖掘加密貨幣；目前不法獲利已高達 200 萬美元。

資安廠商 Avast 日前接獲用戶的異常反應，深入研究發現一個名為 Crackonosh 的挖礦惡意軟體，由放在論壇上的盜版遊戲夾帶，植入在受害者電腦內，挖掘加密貨幣「門羅幣」（Monero, XMR）；目前不法獲利已高達 200 萬美元。

據 Avast 發表的報告指出，有用戶反應自不明論壇下載盜版遊戲後，其安裝在新購 Windows 筆電中的 Avast 防毒軟體即遭刪除，且 Windows 也出現錯誤訊息。

Avast 深入研究該案例後，發現一個名為 Crackonosh 的挖礦惡意軟體，在這些盜版遊戲中植入惡意挖礦程式碼，並安裝 XMRig 以挖掘門羅幣；目前已知 Crackonosh 已經感染超過 222,000 台電腦，一共挖出 9,000 枚門羅幣，市價高達 200 萬美元。

Avast 的報告中也指出，Crackonosh 的擴散相當快速，自 2020 年 12 月開始感染後，目前有十多個國家的遊戲玩家遭到攻擊，受害最嚴重的是菲律賓，共有 18,448 台電腦遭到感染，其次是巴西（16,584）、印度（13,779）、波蘭（12,727）、美國（11,856）與英國（8.946）。

除了挖礦之外，Crackonosh 還有個特色，就是會停止並移除 Windows 系統上原本安裝的各種防毒防駭軟體，甚至連 Windows 內建的防毒防駭機制 Windows Defender 也無法倖免；Avast 的研究人員指出，這是 Crackonosh 自我保護免被發現的方法，也使得 Crackonosh 難以被偵測並移除。

Avast 的報告中指出，除了 Avast 與 Windows Defender 外，包括 Adaware、Bitdefender、Escan、F-secure、Kaspersky、Mcafee（僅掃瞄功能）、Norton、Panda 等著名常見防毒防駭工具，都會被 Crackonosh 停用並刪除。

- 資料來源：
  1. Crackonosh: A New Malware Distributed in Cracked Software
  2. Hackers Crack Pirated Games with Cryptojacking Malware

4.3、國際政府組織資安資訊

4.3.1、APT 駭侵團體針對東南亞某國政府發動後門監聽攻擊長達三年

資安廠商發現一個 APT 駭侵團體，針對東南亞某國政府單位發動後門監聽攻擊，竊取各種機敏資訊，時間長達三年以上。

資安廠商 Check Point 旗下的資安研究單位 Check Point Research，日前發現一個 APT 駭侵團體，針對東南亞某國政府單位，透過一個過去未知的後門惡意攻擊軟體，發動長期監聽攻擊，竊取各種機敏資訊，且時間長達三年以上。

據 Check Point Research 發表的研究報告指出，該 APT 駭侵團體，針對該國外交部各單位發動有系統的攻擊，假冒該國政府其他單位，寄送內藏惡意軟體的文件，以便在該國外交部使用的 Windows PC 中植入一種前所未見的後門軟體。

Check Point Research 說，攻擊活動寄送的 RTF 格式文件，看起來非常像是正常的公文，但內藏的 Remote template 中有惡意軟體，會利用系統上的三個老舊漏洞 CVE-2017-11882、CVE-2018-0798、CVE-2018-0802，從攻擊者的控制伺服器中，下載進一步的惡意軟體 VictoryDll_x86.dll，可以取得檔案的完整存取權限、取得系統運作中程序與服務的資訊、進行螢幕擷取、竊取電腦上的各種用戶資料等等。

Check Point Research 說，由於該駭侵團體使用的酬載工具，會經常檢查與 baidu.com 網站的連線，工具本身也是過去某些 APT 團體慣常使用的惡意軟體，其控制伺服器在 5 月 1 日至 5 月 5 日該國連假期間均停止運作，因此他們高度懷疑駭侵者與特定 APT 團體有關。

- 資料來源：
  1. Chinese APT group targets Southeast Asian government with previously unknown backdoor
  2. An Overhead View of the Royal Road

4.3.2、國際刑警組織破獲並下架數千個線上偽藥網站

國際刑警組織宣布破獲數千個在網路上販售偽劣藥品的假冒網站，並將其離線。

國際刑警組織（International Criminal Police Organization, INTERPOL）日前宣布，破獲數千個在網路上販售偽劣藥品的假冒網站，並將其離線；這些假網站在網路上販售各種可能危害健康的非法藥品、醫療器材、檢測試劑等，目前均已緝獲並下線。

國際刑警組織是在一個名為「Operation Pangea XIV」的國際聯合查緝行動中，查緝到如此眾多的非法賣藥網站；該行動鎖定網路上販賣各種非法醫藥品的相關賣家及其網站。

該行動一共聯合多達 92 個國家的警政、司法、海關、醫藥衛生主管機管參與，總共下線或移除的網站與賣場連結，多達 113,020 個。

INTERPOL 指出，光在英國就查獲三百多萬種偽藥與假冒醫材，總額高達 1300 萬美元；有 43 個網站、3,100 個偽藥廣告連結遭到下線移除。

INTERPOL 也說，在查緝行動展開的一周期間（自 5 月 18 日至 25 日），一共在全球逮捕 277 人，總共查緝到的偽劣藥品與醫材，總額高達美金 2300 萬元；其中超過半數都是未經核准的偽劣 COVID-19 武漢肺炎檢測組。

在行動期間，INTERPOL 也會同各國海關嚴格查緝自這些偽藥網站送出的包裹，結果發現許多偽劣藥品藏匿在正常貨物如衣物、玩具或罐頭之中；其中一個案例，在一罐豆子罐頭中就裝有 2,800 粒偽劣止痛藥錠。

INTERPOL 秘書長 Jürgen Stock 指出，在肺炎疫情流行期間，許多人的生活被迫轉往線上，讓這類犯罪分子更容易鎖定受害者；大多數受害者在不知情的狀況下，購買這些偽藥，不但破財而且傷身。

- 資料來源：
  1. Thousands of fake online pharmacies shut down in INTERPOL operation
  2. Interpol shuts down thousands of fake online pharmacies

4.4、社群媒體資安近況

駭侵者透過約會軟體 Tinder 用戶個人照片，以手寫網址相片散布惡意網址

資安專家發現在 Tinder 這類的社群約會軟體上，有駭侵者利用在個人檔案照片放上手寫網址相片的方式，一方面避免系統阻擋，一方面誘騙受害者上當。

資安專家發現，近來在 Tinder 這類的社群約會軟體上，有駭侵者利用在個人檔案的照片放上手寫網址相片的方式，一方面避免系統阻擋，一方面誘騙受害者上當。

據資安媒體 BleepingComupter 的調查報導，在 Tinder 上發現多個類似案例；駭侵者在 Tinder 上註冊假帳號，在其個人檔案中先放置來路不明的俊男美女等具吸引力的個人照片，然後再放上一張內有手寫網址的照片。

根據分析，這些手寫的網址，多半都是一些第三方約會網站，或是一些內容不堪入目的色情網站。

此外，這些假帳號也會在自我介紹的文字欄位中，寫上一些鼓勵造訪者在瀏覽器中輸入手寫網址的文句，以便提高受害者上當受騙的機會。

由於多數社群媒體的內容過濾機制，多半僅檢查文字格式的輸入資料，例如用戶以鍵盤輸入的內容、自我介紹文字、即時文字通訊等等，無法檢查照片當中的手寫文字，因此這類釣魚攻擊方式往往可以有效避免各社群平台的自動檢查機制，只能靠人工巡查來進行審核。

另外，也有駭侵者利用發送私訊的方式，在另一個約會社群平台 Grindr 上大量傳送詐騙訊息給受害者；這些受害訊息多半由個人檔案一片空白的假帳號發送，內含惡意網站或詐騙連結。

雖然這類以文字訊息傳送的垃圾與詐騙內容，比手寫照片中的網址容易偵測，但如果社群平台在假帳號註冊的防制上不夠嚴格，駭侵者可以很容易大量註冊各種假帳號的話，用戶就還是有收到各種詐騙訊息或垃圾內容的風險。

- 資料來源：
  1. Spam, Bans…and Our Plans
  2. Tinder spam campaign hides "handwritten" links in profile images

4.5、行動裝置資安訊息

4.5.1、手機遊戲「銀河大戰」爆發用戶資料外洩事件，近 600 萬玩家受害

資安專家發現一台屬於熱門手機遊戲「銀河大戰」的 Elasticsearch 伺服器未經適當保護，600 萬玩家資料可供任何人自由下載。

資安專家 WizCase 日前發現一台屬於熱門手機遊戲「銀河大戰」（Battle for the Galaxy）的 Elasticsearch 伺服器，未經適當保護而在網路上曝露，上有近 600 萬玩家資料，可供任何人自由下載。

這批曝露在網路上的資料，檔案總大小將近 1.5TB ，而且未經任何保護與加密；任何知道該伺服器網址的人，都很容易下載這批用戶資料。

WizCase 表示，這批曝險的資料，確實的檔案大小高達 1.47TB，其中包括 590 萬名玩家的個人檔案、200 萬筆交易資料、587,000 筆客服回覆訊息內容；而在這些客服回覆內容中含有用戶的帳號 ID、Email 地址、遊戲內購資訊、價格與付款方式等；有些甚至含有用戶連線使用的 IP 位址。

WizCase 說，將這些資訊匯集起來，不肖人士即可拼湊出進行釣魚郵件攻擊所需的完整資料，進而假扮為遊戲公司的支援人員，向用戶寄送釣魚攻擊信件。

值得注意的是，WizCase 分析了這批用戶資料中的付款資訊，發現整體玩家中約 0.33% 的付費玩家，貢獻了整個 Battle for the Galaxy 90% 的營收；這些付費玩家也特別容易遭到駭侵者鎖定。

WizCase 也說，在他發現該未受保護的 Elasticsearch 伺服器後，在第一時間與 Battle for the Galaxy 的遊戲開發廠商 AMT 聯絡；截至媒體報導時，AMT 未提出回覆，但已經修復未經保護的 Elasticsearch 伺服器。

- 資料來源：
  1. Data Breach: Millions of Users' Messages, Account IDs, and IP Addresses Exposed in Mobile Game Datab
  2. 'Battle for the Galaxy' Mobile Game Leaks 6M Gamer Profiles

4.5.2、Google 修復 Android 嚴重漏洞，可導致駭侵者遠端執行任意程式碼

Google 在 Android 更新版本中修復多個資安漏洞，包含一個可讓駭侵者遠端執行任意程式碼的嚴重漏洞；Android 裝置用戶應隨時注意並更新系統。

Google 近期在六月初發表的 Android 更新版本中，修復多達 90 個以上資安漏洞，其中包含一個可讓駭侵者遠端執行任意程式碼的嚴重漏洞；廣大 Android 裝置用戶應隨時注意手機原廠公布的作業系統更新訊息，並立即更新系統。

在這批得到修復的漏洞中，最危險的是編號 CVE-2021-0507 的漏洞，存於 Android OS 的系統組件中；駭侵者可利用特製的檔案傳輸來誘發錯誤，並且遠端執行任意程式碼。

另外還有一個屬於嚴重等級的漏洞 CVE-2021-0516，可以讓駭侵者用於提升執行權限；但 Google 沒有說明該漏洞的發生原因。

在這次針對 Android 發布的資安修補新版中，Google 也修復了多個駭侵者可用於提升執行權限的漏洞，包括發生在 Android Runtime 中的 CVE-2021-0511、發生在 Media Framework 中的 CVE-2021-0508、CVE-2021-0509、CVE-2021-0510、CVE-2021-0520、發生在 upstream kernel 的 CVE-2021-14305、CVE-2021-0512。

另有一個高等級 CVE-2021-0521 漏洞，可讓駭侵者在無需額外執行權限的情況下，竊取裝置內的資訊。

由於使用 Android 系統的裝置數量十分龐大，多數第三方廠商製造的手機，必須仰賴原廠推送作業系統更新，無法直接由 Google 推送，因此用戶應特別提高警覺，隨時注意原廠發送的更新訊息，並在可進行系統更新時立即執行，才能降低裝置遭駭侵者攻擊的風險。。

- 資料來源：
  1. Android 安全公告 - 2021 年 6 月
  2. Google Patches Critical Android RCE Bug

4.6、軟體系統資安議題

4.6.1、台灣記憶體與儲存大廠遭勒贖攻擊

台灣記憶體與儲存媒體大廠，於五月底遭到疑似 Ragnar Locker 勒贖軟體攻擊，導致部分系統無法運作，不過目前已經恢復正常。

台灣記憶體與儲存媒體大廠，於五月底遭到疑似一支名為 Ragnrr Locker 的勒贖軟體發動攻擊，導致部分系統無法運作；不過該公司表示目前已經恢復正常。

據資安科技媒體 BleepingComputer 的報導，該公司表示在今（2021）年 5 月 23 日遭到勒贖軟體攻擊，當時該公司立即將受影響的系統進行斷網，同時向相關主管機管發布資安通報。

在經過系統緊急處置、升級與還原後，該公司表示目前系統已幾近恢復日常運作效率，各種商業運作也已恢復正常作業。

BleepingComputer 指出，該公司並未明確提供該起駭侵攻擊事件的詳細資訊，但一個稱為 Ragnar Locker 的駭侵組織已經表示自己就是攻擊者。

Ragnar Locker 駭侵團體指出，在上一波的攻擊波動中，該組織掌握到的該公司內部機敏資料，檔案大小合計達 1.5TB；該駭侵團體除了貼出部分檔案內容的螢幕擷圖外，也威脅如果拒絕支付贖金，就會公布這些資料。

據 Ragnar Locker 公開的部分螢幕擷圖顯示，該公司這批遭到 Ragnar Locker 竊走的資料，包括各種企業機密資訊與檔案、各種圖表、財務資料、

Gitlab 與 SVN 程式原始碼、法務文件、員工資訊、各種保密條款、工作用檔案等等。

遭勒贖的企業為全球知名的記憶體與儲存媒體相關產品大廠，主要製作高效能 DRAM 模組、NAND 快閃記憶卡、SSD 儲存裝置等產品，相關領域橫跨電腦、行動、遊戲、電動車與各種工業用解決方案等。

- 資料來源：
  1. Computer memory maker ADATA hit by Ragnar Locker ransomware
  2. Computer Memory Maker ADATA Hit By Ragnar Locker Ransomware

4.6.2、台灣記憶體與儲存大廠遭勒贖攻擊資料，再次遭駭侵團體公開釋出

台灣記憶體與儲存裝置大廠，其在五月下旬遭勒贖攻擊竊取而得的部分資料，再次遭到駭侵團體於網路上公布。

台灣記憶體模組與儲存裝置大廠，其在五月下旬遭 Ragnar Locker 勒贖攻擊時被竊取而得的部分資料，再次遭到 Ragnar Locker 駭侵團體於網路上公布，任何人均可下載。

這次是 Ragnar Locker 駭侵團體第二次公開該公司遭竊的資料，一共有 13 批次的壓縮檔，檔案大小合計高達 700GB；這批資料被放在雲端檔案分享服務 MEGA 之上，同時還附有解壓縮專用密碼。

不過，MEGA 在獲悉該批檔案上傳到該公司的檔案分享服務後，隨時關閉這些檔案的存取權限，同時刪除 Ragnar Locker 駭侵團體在該站註冊的帳號；目前這 13 批檔案都已無法存取。

據資安專家分析表示，被短暫放上 MEGA 供人下載的檔案，內容可能為該公司的財務相關資料、保密協議等等。

遭駭之公司是在今（2021）年的 5 月 23 日遭到 Ragnar Locker 的駭侵攻擊，導致該公司部分資訊系統運作受阻；並曾向資安媒體指出，該公司已經自行恢復所有系統運作，也不會支付任何贖金給勒贖攻擊者。

另一方面，釋出竊得資料的 Ragnar Locker 顯然也沒有得到贖款；據該團體發表的「聲明」指出，「我們雖然提供企業修復漏洞並避免檔案被公開的機會，但是該公司顯然不認為自己和合作伙伴、客戶、員工、顧客的機敏

資料很有價值。」

此外，雖然第二批資料已遭雲端檔案分享服務商 MEGA 主動刪除，但據信該資料已在 MEGA 平台曝光一段間；而遭 Ragnar Locker 駭侵團上傳分享的第一批遭竊資料（約有 250MB），目前仍然可供下載。

- 資料來源：
  1. ADATA suffers 700 GB data leak in Ragnar Locker ransomware attack
  2. Ragnar Locker ransomware leaked data stolen from ADATA chipmaker

4.6.3、Google Chrome 緊急修補已遭大規模濫用的 0-day 資安漏洞

Google 緊急推出 Chrome 資安修補新版，修復 14 個資安漏洞；Google Chrome 用戶應立即更新瀏覽器至最新版本。

Google 於 2021 年 6 月 10 日緊急推出 Chrome 資安修補新版，修復 14 個資安漏洞，其中包括一個已遭駭侵者大規模濫用並發動攻擊的 0-day 漏洞；Google Chrome 用戶應立即更新瀏覽器至最新版本。

在 Google Chrome Release 中的最新更新說明中，Google 表示新推出的 91.0.4472.101 更新了一共 14 個資安漏洞，其中有 1 個嚴重等級、7 個高等級、2 個中等等級；而這些漏洞在 Google Chrome for Windows、macOS、Linux 內都存在。

其中屬於 0-day 漏洞的是 CVE-2021-30551 這個漏洞，存於 Chrome V8 引擎中的形別混淆錯誤；雖然 Google 文件中沒有透露駭侵者可以利用此漏洞造成何種錯誤，控制電腦到何種層級，但資安專家認為該漏洞和微軟先前修補的 0-day 漏洞 CVE-2021-33742，很可能都為同一家提供攻擊工具的商業公司所利用，且由駭侵團體用於攻擊某些東歐與中東國家。

Google 也表示該公司已知悉 CVE-2021-30551 遭駭侵團體濫用一事，並表示新版的 91.0.4472.101 即將在數日內正式釋出，供所有用戶下載更新；理論上用戶無需自行安裝，Chrome 會在啟動時自動更新，但用戶也可以手動進行更新。

截至目前為止，Google 已修復 Chrome 多達 6 個 0-day 漏洞。由於 Google Chrome 是目前市佔率最高的網頁瀏覽器，使用人數甚多，強烈建議 Google Chrome 用戶一定要提高警覺，經常檢查 Chrome 版本是否為最新版，以避免遭到駭侵者利用 0-day 漏洞發動攻擊。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. Google fixes sixth Chrome zero-day exploited in the wild this year
  3. Google releases urgent Chrome update to address zero-day bug under active attack

4.6.4、富士軟片遭勒贖攻擊，關閉受影響網路與電腦系統運作

日本軟片、光學設備與醫療器材大廠富士軟片，日前遭到駭侵攻擊；該公司隨即關閉部分內部網路運作，以避免資安事件災害擴大，同時啟動資安調查工作。

日本軟片、光學設備與醫療器材大廠富士軟片（Fujifilm），日前遭到不明來源的駭侵攻擊；該公司隨即關閉部分內部網路運作，以避免災害擴大到其他單位，同時也立即啟動事故調查。

富士軟片於 2021 年 6 月 2 日在官方網站上發表簡短新聞稿聲明，指出該公司的東京總部，於 2021 年 6 月 1 日深夜發現遭到來自勒贖軟體的攻擊，並立即將可能遭到影響的伺服器與電腦設備停止運作，並且切斷受影響的內部網路連線。

該公司正在調查整件攻擊事件的來源、受影響範圍與損害程度，不過並未對外提供詳細的攻擊相關資訊，僅向可能因此次攻擊事件產生不便的合作對象與顧客致歉。富士軟片美國分公司也在首頁加上警訊，揭露該公司目前受該勒贖攻擊影響，包括 Email 系統與電話全部不通。

資安廠商 Advanced Intel 執行長 Vitali Kremez 向資安專業媒體 BleepingComputer 表示，根據該公司監測資料顯示，Fujifilm 很可能是受到一種名為 Qbot 的勒贖軟體攻擊，而 Qbot 正是近來惡名昭彰，向多家大型企業發動多起勒贖攻擊的駭侵團體 REvil 慣用的駭侵工具。

Kremez 指出，該公司的偵測系統發現 Qbot 可能是從 2021 年 5 月 21 日起，開始向富士軟片的電腦系統發動攻擊。Kremez 也說，一旦遭到 Qbot 感染，該企業的網路很可能於未來持續遭到更多駭侵攻擊。

- 建議採取資安強化措施

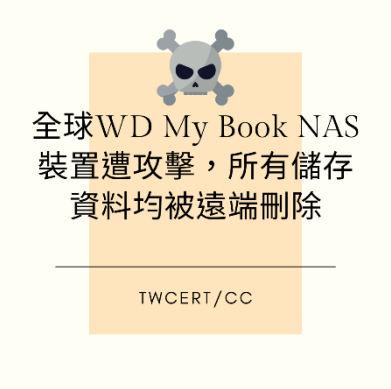
1、發生資安事件時，建議中斷網路連線，將受害與未受到感染的部分進行網路隔離，使駭客無法執行進一步的駭侵行為，以避免造成更嚴重的擴大感染。

2、確認感染範圍、評估受損狀況，並即時向相關單位進行資安通報，TWCERT/CC 亦是企業發生資安事件通報及協助之單位。

- 資料來源：

1. 当社サーバーへの不正アクセスについて
2. Website Notice - June 4, 2021
3. みずほ銀行 藤原頭取当面続投へ 再発防止の徹底になお時間
4. FUJIFILM shuts down network after suspected ransomware attack
5. 中勒索病毒因應之道

4.6.5、全球 WD My Book NAS 裝置遭攻擊，所有儲存資料均被遠端刪除



Western Digital My Book NAS 遭到全球性的駭侵攻擊行動，不但裝置會被重置為出廠設定，儲存在內的資料也被遠端移除。

銷售量相當大的 Western Digital 品牌 My Book NAS 網路儲存裝置，目前正遭到全球性的駭侵攻擊行動，不但裝置會被重置為出廠設定，所有儲存在內的資料，也都被遠端移除。

該裝置是一款體積輕巧的家用、個人用網路儲存設備，立起來時就像一本書一樣；原廠提供的 WD My Book Live app 可以讓用戶在任何地方存取儲存在 NAS 內的檔案，無論 NAS 本身是不是設於防火牆以內。

近來世界各地許多 WD My Book NAS 用戶反應，突然無法透過 app 或瀏覽器存取 NAS 內的資料；用戶透過瀏覽器登入其管理界面後，會因出現「密碼錯誤」而擋於門外；而所有存在 NAS 內的資料也全部遭到刪除。

有用戶找出 WD My Book NAS 的裝置記錄檔，發現在 2021 年 6 月 23 日下午三時許，裝置開始執行一個稱為「My BookLive factoryRestore.sh」的指令檔案，這個指令與後續自動執行的程式碼，即是將 WD My Book NAS 回復原廠設定並刪除所有資料的元兇。

值得注意的是，這波攻擊行動至今沒有受害用戶表示收到勒贖威脅；這表示攻擊者的目的純為造成破壞，而非藉以要求贖款。

製造廠 Western Digital 隨即發表聲明表示，該公司正在調查整個事件；該公司認為是用戶的 WD My Book NAS 裝置遭到惡意軟體攻擊，但否認是該公司的雲端伺服器遭到攻擊。

該公司建議所有尚未遭到攻擊的 WD My Book NAS 用戶，應立即將其裝置離線，避免遭到進一步攻擊；但由於本款機種已經相當老舊，最後一次韌體更新時間早在 2015 年，因此後續是否能繼續更新，目前不得而知。。

- 資料來源：
  1. Help! All data in mybook live gone and owner password unknown
  2. WD My Book NAS devices are being remotely wiped clean worldwide

4.6.6、駭侵團體 Nobelium 入侵並存取微軟客戶支援工具

微軟表示該公司發現其客戶支援工具遭到駭侵團體入侵存取，部分客服人員電腦內的客戶訂購資訊遭到竊取。

微軟公司日前在官方部落格中發文，表示該公司發現其客戶支援工具，遭到一個名為 Nobelium 的駭侵團體入侵存取；部分客服人員電腦內的客戶訂購資訊也遭到竊取。

在微軟的部落格貼文中指出，該公司的資安威脅情報中心，正在調查整起事件的來龍去脈，以及駭侵團體使用的攻擊策略與手法。

貼文中說，該公司發現駭侵者使用「密碼噴灑」與暴力登入試誤等方法，試圖入侵目標電腦設備，但大多數攻擊都未見成功，目前確認有三台電腦設備遭 Nobelium 駭侵團體成功入侵，並遭駭侵者植入木馬惡意程式，以便存取電腦中的客戶資訊。

微軟指出，Nobelium 將可能利用竊得的客戶資訊，對這些客戶發動進一步的釣魚攻擊。微軟已經通知可能因此受到波及的客戶。

另外，由於 Nobelium （又名 Cozy Bear）疑似涉及今年年初爆發的 SolarWinds 大規模長期供應鏈攻擊的要角，因此微軟也循管道向主管單位通報這起可能為國際駭侵攻擊行動的事件。

據微軟表示，疑似遭駭侵者存取的資料，主要都和美國的國家利益有關，約佔 45%；其餘受影響客戶的所屬國家分別為英國（10%）、德國與加拿大（小批）；總共受影的國家有 36 個。

在微軟公開這次攻擊行動前，路透社曾發表一則新聞，指出該社收到一封由微軟寄給受影響客戶的郵件；郵件內容指出「有一個被微軟辨識為 NOBELLIUM，且有國家力量支持的強大駭侵團體，最近存取了微軟的客戶支援工具，並且獲悉和貴客戶的微軟服務訂購相關資訊。」。

- 資料來源：
  1. New Nobelium activity
  2. Microsoft says new breach discovered in probe of suspected SolarWinds hackers
  3. Nobelium hackers accessed Microsoft customer support tools

4.7、軟硬體漏洞資訊

4.7.1、微軟六月資安修補包，更新 50 個資安漏洞，其中含 6 個 0-day 漏洞

微軟發布的 2021 年 6 月資安修補包，共修復微軟各項產品中多達 50 個資安漏洞，其中有 6 個 0-day 漏洞，微軟用戶應立即套用更新。

微軟在 6 月 8 日推出例行性的「Patch Tuesday」每月軟體資安更新修補包，針對旗下各款產品，一共修復多達 50 個資安漏洞，其中更含有 6 個 0-day 漏洞；微軟用戶應立即下載執行最新更新，以降低遭駭侵者利用這些漏洞發動攻擊的風險。

在這 50 個得到修復的漏洞中，歸類為「嚴重」等級漏洞者有 5 個，其餘 45 個漏洞的分級均為「重要」。

而這批更新中修復的 6 個 0-day 漏洞，過去都曾有遭到駭侵者利用於攻擊活動的記錄，其 CVE 編號與漏洞發生原因如下：

- CVE-2021-31955：發生於 Windows 核心資訊洩露的錯誤；
- CVE-2021-31956：發生於 Windows NTFS 檔案系統，可用以提升執行權限；
- CVE-2021-33739：發生於 Windows DWN 核心程式庫，可用以提升執行權限；
- CVE-2021-33742：發生於 Windows MSHTML 平台的錯誤，可用以遠端執行任意程式碼；
- CVE-2021-31199：發生於 Microsoft Enhanced Cryptographic Provider，可用

以提升執行權限；

- CVE-2021-31201：發生於 Microsoft Enhanced Cryptographic Provider，可用以提升執行權限。

據資安廠商卡巴斯基的研究報告指出，CVE-2021-31955 和 CVE-2021-31956 這兩個 0-day 漏洞，已遭一個名為 PuzzleMaker 的駭侵團體用於攻擊活動之中。

微軟各種產品用戶與系統管理者，應立即按照微軟發布的更新指南，立即套用本月的資安修補包，以降低系統遭駭侵者攻擊的風險。

- CVE 編號：CVE-2021-31955、CVE-2021-31956、CVE-2021-33739、CVE-2021-33742、CVE-2021-31199、CVE-2021-31201 等
- 解決方案：立即依微軟發布的更新指南進行更新修補

- 資料來源：
  1. Security Update Guide
  2. PuzzleMaker attacks with Chrome zero-day exploit chain
  3. Microsoft June 2021 Patch Tuesday fixes 6 exploited zero-days, 50 flaws
  4. Microsoft June 2021 Patch Tuesday: 50 vulnerabilities patched, six zero-days exploited in the wild

4.7.2、WordPress 熱門外掛 Fancy Product Designer 遭發現嚴重 0-day 漏洞

WordPress熱門外掛Fancy Product Designer遭發現嚴重0-day漏洞

資安廠商發現 WordPress 熱門外掛程式 Fancy Product Designer 存有可讓駭侵者遠端執行任意程式碼的 0-day 嚴重漏洞。

資安廠商 WordFence 日前發表研究報告，指出該公司發現 WordPress 一支熱門外掛程式 Fancy Product Designer，存有一個可讓駭侵者遠端執行任意程式碼的 0-day 嚴重漏洞。目前已觀測到大量使用該漏洞進行的攻擊事件，WordPress 有安裝該外掛的用戶，應特別提高警覺。

Fancy Product Designer 是一個讓 WordPress、WooCommerce 與 Shopify 用戶以視覺方式設計商品頁面版面配置的外掛程式，據估計有超過 17,000 個網站都安裝了 Fancy Product Designer。

被發現的 0-day 漏洞，其 CVE 編號為 CVE-2021-24370，CVSS 嚴重程度評分高達 9.8 分（滿分為 10 分），屬於最高的嚴重等級；該漏洞存於 Fancy Product Designer 在處理上傳 PDF 或影像檔案時的安全掃瞄能力不足，駭侵者可以輕易跳過安全檢查流程，並且上傳惡意的 php 程式檔案到裝有 Fancy Product Designer 的網站，不但可以執行任意程式碼，更能讓駭侵者奪取網站的控制權。

WordFence 說，安裝了 Fancy Product Designer 的 WordPress 和 WooCommerce 網站，會受到這個 0-day 漏洞的影響，但安裝此外掛的 Shopify 網站，得益於其較嚴格的資安控制，並不會受此漏洞波及。

WordFence 自 5 月 16 日起觀測到大量使用該漏洞進行的攻擊事件，也在第一時間通報 Fancy Product Designer 的開發者，但由於這個漏洞屬於 0-day 漏洞，因此目前尚無新版的 Fancy Product Designer 可供下載；現階段的暫時處理方式，就是徹底移除 Fancy Product Designer，直到資安修補版本推出為止。

- CVE 編號：CVE-2021-24370
- 影響產品/版本：Fancy Product Designer 4.6.8 及之前所有版本
- 解決方案：在更新版本推出前，應徹底移除 Fancy Product Designer

- 資料來源：
  1. Critical 0-day in Fancy Product Designer Under Active Attack
  2. CVE-2021-24370
  3. Critical WordPress plugin zero-day under active exploitation

4.7.3、VMware 修復 Carbon Black App Control 中的身分驗證繞過資安漏洞

VMware 修復存於 Carbon Black App Control 中的資安漏洞，該漏洞可導致駭侵者跳過身分驗證程序，直接存取伺服器。

虛擬解決方案大廠 VMware 近日修復存於其 Carbon Black App Control 中的一個嚴重資安漏洞；該漏洞可導致駭侵者跳過身分驗證程序，直接存取伺服器。

Carbon Black App Control 是 VMware 推出的企業用資安強化軟體，可以保護系統免於未經授權的修改，特別是由惡意軟體或 0-day 漏洞造成的系統設定篡改。

得到 VMware 修補的資安漏洞，其 CVE 編號為 CVE-2021-21198，發生在 Black Carbon App Control 的 8.1、8.1、8.5.8 之前的 8.5 版、8.6.2 之前的 8.6 版。駭侵者只要先取得 Black Carbon App Control 伺服器的存取權限，即可利用這個漏洞，進一步取得系統管理權限，而不需要通過身分驗證程序。

由於 Black Carbon App Control 是企業資安防護系統的一環，因此一旦駭侵者利用此漏洞取得 Black Carbon App Control 伺服器的控制權，就更容易針對企業內部的關鍵設施發動進一步的駭侵攻擊，包括 POS 系統、工業製造控制系統等等，都可是潛在的攻擊對象。

這個漏洞的 CVSS 危險程度評分高達 9.4 分，危險程度分級為最高等級的「嚴重」（Critial）等級；採用 VMware Black Carbon App Control 的系統管理員應立即採取行動。

據 VMware 針對此漏洞發表的資安通報指出，目前並未針對此漏洞推出暫時處理方式建議，而是依使用的版本應升級到對應最新版本：8.0 或 8.1 版本應升級到 hotfix 版本，8.5 應升級至 8.5.8，8.6 應升級至 8.6.2。

- CVE 編號：CVE-2021-21198
- 影響產品/版本：VMware Black Carbon App Control 的 8.1、8.1、8.5.8 之前的 8.5 版、8.6.2 之前的 8.6 版。
- 解決方案：8.0 或 8.1 版本應升級到 hotfix 版本，8.5 應升級至 8.5.8，8.6 應升級至 8.6.2。

- 資料來源：
  1. CVE-2021-21998
  2. Advisory ID: VMSA-2021-0012
  3. VMware fixes authentication bypass in Carbon Black App Control

第 5 章、 資安研討會及活動

WFH 之下的網路與資安	
活動時間	**2021/7/14 ~ 2021/7/15**
活動地點	**線上研討會**
活動網站	**https://www.digitimes.com.tw/seminar/DWebinar_20210714/**
活動概要	 **主辦單位：DIGITIMES** 詳細活動議程及報名資訊，請參閱活動網站。 響應防駭新生活　行動辦公不駭怕 COVID-19 讓全台進入 3 級警戒 學生們開始遠距學習、遠距醫療上路、企業採分流、居家工作... 這讓各式通訊軟體、線上會議、郵件等遠端協作軟體活絡了起來 但少了公司內網的金鐘罩、鐵布衫 又該如何鞏固企業資訊安全，阻絕對抗黑帽駭客的攻擊? 7 月 14-15 日 WFH 下的網路與資安 疫起防駭不中斷 擁抱遠距新生活

歐美中建構數位主權，臺灣如何接招？	
活動時間	**2021 年 7 月 14 日（三）14:00-16:00**
活動地點	**線上視訊直播**
活動網站	**https://www.twsig.tw/20210714/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 詳細活動議程及報名方式，請參閱活動網站。 活動背景 從 2020 年 2 月的《塑造歐洲數位未來》（Shaping Europe’ s Digital Future）戰略，到 2021 年 3 月的數位羅盤計畫（Digital Compass），歐盟提出了建構未來數位十年政策治理框架，新政策不只是要推動企業數位轉型，還強調要強化科技主權並減少對美國和中國的依賴。 中國則早在 2000 年的《中國互聯網狀況》白皮書中提到，中國境內的互聯網屬於中國主權管轄範圍；2015 年的烏鎮互聯網大會中更再次強調「尊重網路主權」，並試圖將此概念拓展成為國際準則。去（2020）年 8 月美國前任總統川普執政團隊則透過公布「淨網計畫」（Clean Network Program），從軟硬體到服務商，都要實施淨化，也被喻為是美國版的數位主權。 當全球三大經濟體都在建構自己的數位主權，近期全球爭奪半導體更讓各國領導者將取回「數位主權」或「科技主權」列為重大國家戰略，臺灣該如何接招?臺灣與三大經濟體間存在著科技戰略夥伴關係與貿易往來關係，也存在著地緣政治複雜性。歐美中積極建構數位主權之時，臺灣該如何應對？

Hack The Box Business CTF 2021	
活動時間	**Friday, July 23rd, 12:00 UTC - Sunday, July 25th, 18:00 UTC**
活動地點	**請見活動官網**
活動網站	**https://www.hackthebox.eu/htb-business-ctf-2021**
活動概要	 **主辦單位：Hack The Box** 詳細活動資訊及報名方式，請參閱活動網站。 Companies Around The World, Assemble! The first Hack The Box Business CTF competition is coming: latest vulnerabilities, state-of-the-art attack techniques, challenges for every skill level based on real-world attack scenarios! Ready, Set, PWN! 54 Hours Of Hacking Training Friday, July 23rd, 12:00 UTC - Sunday, July 25th, 18:00 UTC 22 JULY 2021 **Pre-Event Talks Agenda** Watch live on our Youtube channel. All talks are at UTC time. Make sure to set up a reminder for the event.

【數位同步】資安事件偵查技術解密班	
活動時間	7/24、7/25 (六)、(日)共 14 小時
活動地點	工研院光復院區 1 館(詳細地點請以上課通知為準)及數位直播同步
活動網站	**https://college.itri.org.tw/course/all-events/92ABA661-D427-4076-BD9F-480ED04D69C4.html**
活動概要	【數位同步】資安事件偵查技術解密班 **主辦單位：工研院產業學院** 詳細課程資訊及報名方式，請參閱課程網站。 聯絡資訊：溫小姐/03-5743864 報名截止日：2021-07-16 課程介紹 1.資安事件的正確處理因應。2.強化受駭電腦的鑑識能力。 3.強化惡意程式分析的能力。4.解除資安事故發生的原因。 課程大綱 ● 資安事件處理流程概說 ● 鑑識受駭電腦：此部分將搭配實作解說如何利用 Windows 鑑識工具找出電腦中的惡意程式及連線中繼站。 ● 惡意程式行為分析：藉由找出惡意程式之後，進一步對惡意程式進行行為分析，釐清受駭主機的感染範圍(包含惡意檔案之建立及註冊表之竄改)，並進行惡意檔案的移除及系統修復。 ● 常見後門介紹：除惡意程式外，駭客也會使用多種網頁或 VPN 後門對政府企業進行滲透，本課程也將針對實案中駭客常見使用之後門搭配實例進行解說。 ● 實際案例介紹：從我國近期油品事業遭勒索病毒案、政府機關遭入侵滲透案中研析資安事件發生之原因，提供學員進行反思。

【數位同步】網頁安全開發深入解析	
活動時間	2021-08-07
活動地點	工研院光復院區 1 館(新竹市東區光復路二段 321 號，詳細地點請見課前通知) 同步數位線上課程
活動網站	**https://college.itri.org.tw/course/all-events/E8B394A7-160C-4CB2-A408-4BAE609C8EB7.html**
活動概要	【數位同步】網頁安全開發深入解析 **主辦單位：工研院產業學院** 詳細課程資訊及報名方式，請參閱課程網站。 聯絡資訊：溫郁佳/03-5743864 報名截止日：2021-08-03 課程簡介 ● 了解網站應用程式常見的弱點 ● 撰寫安全的網站程式碼 ● 建立與設置具加密通道的網站伺服器 ● 學會使用檢測工具驗證網站的安全性 1.常見網站弱點介紹 2.安全程式碼撰寫基礎 3.SSL/TLS 介紹 4.常見網站程式弱點檢測工具

第 6 章、 2021 年 6 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。

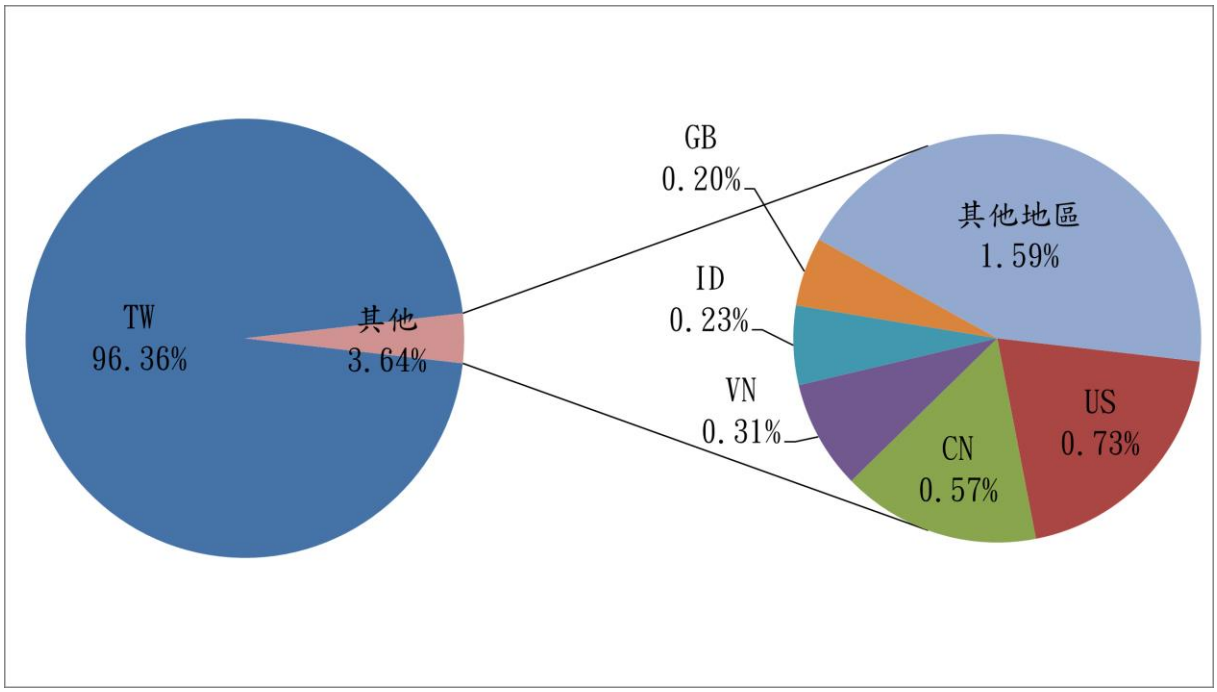


圖 1、分享地區統計圖

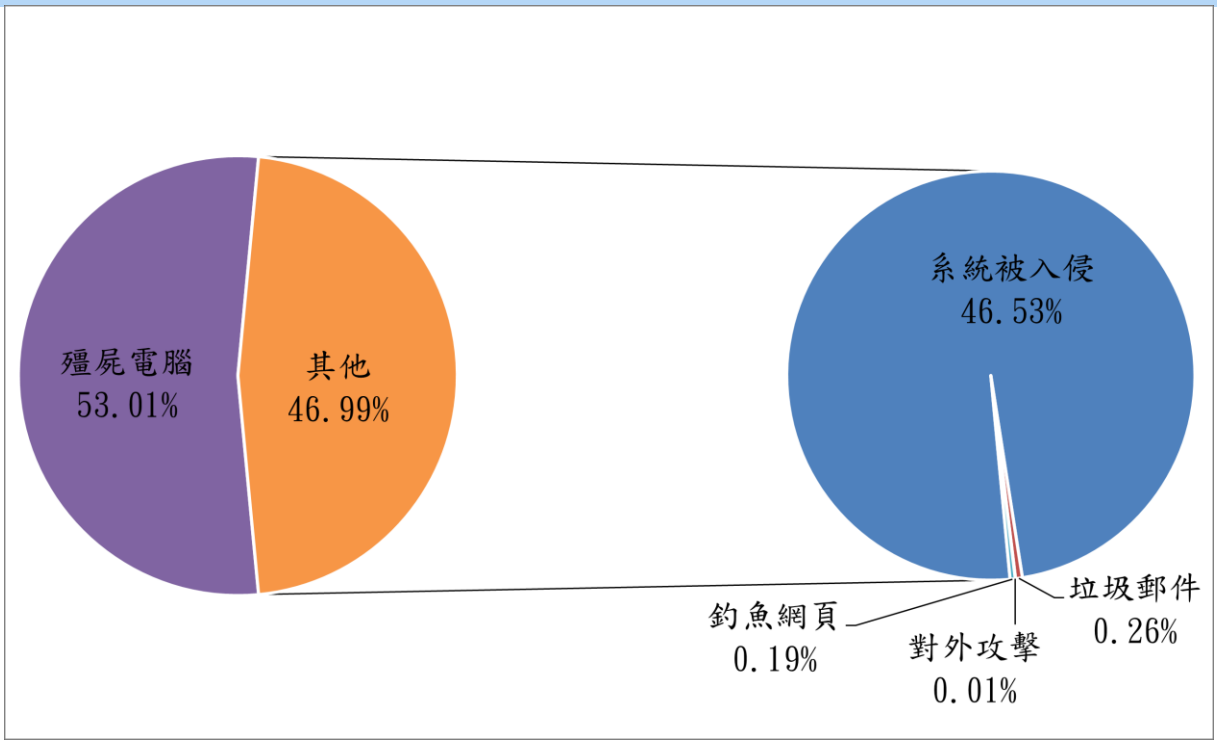


圖 2、分享類型統計圖

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 7 月 9 日**

編輯：**TWCERT/CC 團隊**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**