TWCERT/CC 資安情資電子報

2020 年 9 月份

目錄

第 1 章、 封面故事

駭客正透過政府、學術機關網站，植入惡意網址以散布惡意程式

駭客正嘗試攻擊脆弱的政府及學術機關網站，發布貼文來散布虛假的駭客工具，以騙取個資或誘騙下載安裝惡意程式。

根據 BleepingComputer 報導，駭客針對有公信力的政府和學術單位網站，利用網頁後台內容管理系統（CMS，Content Management System）的漏洞，駭入網站並發布貼文，謊稱能提供 Facebook、Instagram、TikTok 等社交平台的駭客工具。一旦使用者開啟貼文中提供的網址並嘗試執行駭客工具，該網站會展示一連串看似進行攻擊的畫面，並在最後要求使用者下載惡意程式，以繼續駭客預設的行為。

這虛假的駭客工具網站通常會進一步要求使用者提供個人資訊、信用卡資訊等，而部分下載的軟體被發現含有 Emotet 惡意程式。

已知的受駭網站中，包含來自美國聯邦政府機構、州政府及高等學術機關，例如美國國家衛生研究院（NIH）、國家癌症研究中心、明尼蘇達州政府網站、科羅納多州政府網站，以及華盛頓大學、愛荷華州立大學、密西根州立大學等多所著名的學術機關，甚至連聯合國教科文組織的官方網站也受駭。

駭客也會利用網站漏洞，上傳虛假的 PDF 文件並謊稱提供類似的駭客工具。而研究人員指出，為了提升惡意貼文或 PDF 文件觸及率，駭客也會使用 SEO 的手法，企圖讓這些貼文或 PDF 文件出現在 Google 搜尋結果的頂部，藉此吸引更多使用者遭受惡意攻擊。

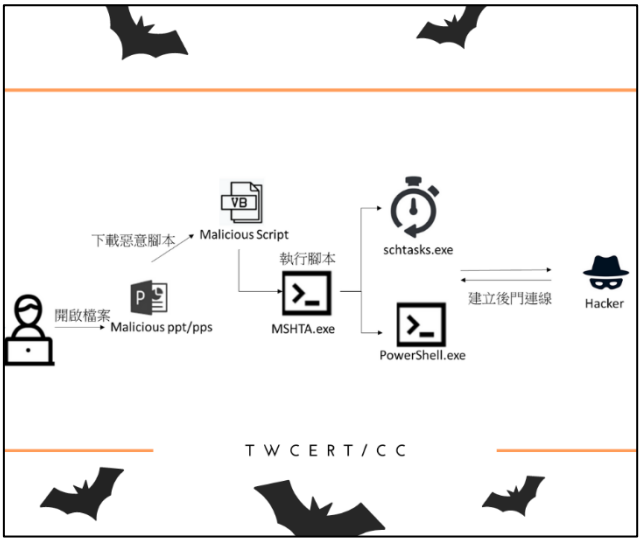
使用者在選擇來自網路的工具或軟體時，需仔細辨別其來源及可信度，並避免使用來路不明或可能從事不法活動的應用程式，以避免受到惡意攻擊或觸犯相關的法律。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/hacked-government-college-sites-push-malware-via-fake-hacking-tools/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、仿冒學校單位寄送釣魚郵件攻擊事件資訊



TWCERT/CC 接獲通報，近日有發現駭客偽冒學術單位的網域名稱發送 mail，博取收信企業之信任，發送要求報價為題的惡意郵件，引誘使用者點擊信件。並於信件中夾帶 2 個含有惡意巨集(Marco)的 PowerPoint 檔案，當使用者開啟該惡意 PowerPoint 檔案，會執行巨集指令下載惡意腳本。該惡意腳本透過 Mshta 執行 schtasks.exe 微軟工作排程，每次開機時會執行惡意腳本建立並維持後門連線。經檢測人員，發現這兩個惡意檔案雖檔名不同，但 Hash 相同。並使用合法網頁如:pastebin 剪貼簿與 j.mp 縮網址躲避防毒軟體偵測。

相關攻擊手法如圖，若需進一步 IOC 資訊請用企業信箱寄信至 twcert@cert.org.tw 索取，謝謝。

2.1.2、台灣半導體製造業遭長期駭侵、多種機密與智財成果遭竊

資安廠商指出，台灣多家半導體製造業者，疑似長期遭到駭侵團體深入，竊取包括各種源碼、軟體工具、晶片設計等機密資料。

台灣資安廠商 CyCraft 八月初在美國舉辦的 BlackHat 資安研討會上發表研究報告，指出台灣多家半導體製造業者，疑似長期遭到駭侵團體深入，竊取包括各種源碼、軟體開發工具、晶片設計等機密資料。

報告說，過去兩年以來，台灣至少有七家晶片製造商遭到來自中國的駭侵團體攻擊，目標在於竊取與晶片製造相關的各種機密資訊；這波長期駭侵攻擊由於使用一種稱為「萬用密碼植入器」（Skeleton Key Injector）的技術，因此被稱為「萬用密碼行動」（Operation Skeleton Key）。

CyCraft 的研究人員指出，在攻擊行動中，駭侵者會仔細選擇駭侵對象，先鎖定市場中居領先地位的廠商，其次再攻擊其分支單位、競爭者、協力廠商和下游供應鏈的業者。

CyCraft 在報告中沒有具體透露是哪些台灣晶片製造業者遭駭，不過他們相信駭侵者位在中國境內，因為這些駭侵者能掌握中文，其攻擊行動在中國的國定假日時都會暫停。

CyCraft 指出，駭侵者係利用植入惡意軟體的 VPN 連線程式，侵入受害企業的內部網路；在該公司提出的研究報告中，詳細列出了兩個具體案例的駭侵路徑分析。

- 資料來源：
  1. https://CyCraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf
  2. https://www.cyberscoop.com/CyCraft-taiwan-semiconductor-espionage-black-hat/
  3. https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
  4. https://www.zdnet.com/article/black-hat-hackers-are-now-using-cobalt-strike-and-skeleton-keys-to-target-semiconductor-firms/

2.1.3、「鸚鵡螺」ATM 遭發現 2 個 0-day 漏洞，駭侵者可竊取用戶資訊、提領存鈔

資安專家發現某款名為「鸚鵡螺」的 ATM 存有兩個 0-day 漏洞，不但能讓駭侵者竊得用戶在銀行的機敏資訊，更能快速將機內存鈔盜領一空。

資安廠商 Red Balloon 旗下的兩名研究人員 Brenda So 和 Trey Keown 指出，由 Hyosung America 製造的 Nautlius「鸚鵡螺」ATM 機台，本身存有兩個 0-day 漏洞；除了可讓駭侵者取得用戶在銀行的往來記錄等機敏資訊，更能快速將 ATM 機身內的存鈔盜領一空。

這兩個漏洞，其中一個存於 Nautlius ATM 處理金融服務的擴充模組，也就是提款使用的軟體程式，駭侵者可以針對這個漏洞加以利用，令 ATM 快速送出所有存鈔。

另一個漏洞則存於 ATM 的遠端控制界面中，駭侵者可藉以遠端執行惡意程式碼；兩名研究人員示範了如何透過這些惡意程式碼，讓 ATM 將用戶的卡號、密碼等機敏資訊傳送到駭侵者架設的控制伺服器。

研究人員說，雖然 Hyosung America 已經針對這兩個漏洞發布修補更新，但由於 Nautlius ATM 使用的作業系統，是十年前發行的 Windows

CE 6.0，在作業系統已經如此老舊的情況下，很難預期不會有其他嚴重資安漏洞出現。

兩位研究人員於今年的 DEF CON 資安大會上示範了入侵 Nautilis ATM 的過程。

- 資料來源：
  1. https://www.cyberscoop.com/atm-vulnerabilities-cash-red-balloon-def-con-2020/
  2. https://techcrunch.com/2020/08/06/hackers-atm-spit-cash/
  3. https://www.youtube.com/watch?v=dJNLBfPo2V8

2.1.4、超過 50,000 個詐騙登入頁面，假冒超過 200 個全球大型品牌

資安廠商指出，2020 上半年共發現超過 50,000 個詐騙登入頁面，冒充 200 個以上的全球大型品牌，意圖騙取用戶的登入資訊，進行進一步的駭侵攻擊。

資安廠商 IRONSCALES 日前發表研究報告指出，該公司的研究團隊，在 2020 上半年進行的觀察研究，共發現超過 50,000 個詐騙登入頁面，冒充 200 個以上的全球大型品牌，意圖騙取用戶的登入資訊，進行進一步的駭侵攻擊。

報告引用 2020 年 Verizon 資料駭侵調查報告指出，65% 的駭侵行動是從 Email 釣魚或 Email 駭侵攻擊開始的；該團隊深入調查各式釣魚攻擊，發現以冒充品牌登入頁面騙取用戶登入資訊，成為十分主流的釣魚攻擊樣態。

報告說，主要被假冒的品牌行業別，依詐騙登入頁面數量排序，分別是金融相關產業、Email 服務提供者、社群網站、電子商務等；排名前五名的被假冒品牌分別是 PayPal（共 11,000 個詐騙登入頁面，在 50,000 個詐騙頁面中佔有達 22%，以下同）、Microsoft（9,500 個、19%）、Facebook （7,500 個，15%）、eBay（3,000 個，6%）、Amazon（1,000 個，3%）。

報告也說，在這 50,000 個詐騙頁面中，至少有 5%，約 2,500 個詐騙頁面，屬於多樣形詐騙登入頁面；以 300 個以上略為不同的登入頁面，冒充同一個品牌。

另外，報告也指出，最常被這類假冒品牌釣魚郵件攻擊的對象，依序是金融服務業、醫療產業、科技製造業與政府部門的職員。

- 資料來源：
  1. https://ironscales.com/blog/fake-login-pages-spoof-prominent-brands-phishing-attacks/
  2. https://enterprise.verizon.com/resources/reports/dbir/

2.1.5、FBI 發出警訊，線上購物相關詐騙案例明顯增加

美國聯邦調查局日前發布警訊，指出該單位近來發現線上購物相關的詐騙案件，數量正在快速增加。

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前發布警訊，指出該單位近來發現線上購物相關的詐騙案件，其數量正在快速增加。

FBI 指出，近來該局接獲愈來愈多關於線上購物糾紛案件與檢舉陳情，發現這些案件多半和電子商務的詐騙有關。詐騙者透過社群媒體或搜尋引擎，以超低價吸引受害者點擊進入假冒其他著名線上購物平台的詐騙網站，購買諸如健身器具、小型家電、工具或家具等商品。

FBI 在警訊中說，該局接獲的檢舉陳情，典型的樣態如下：

- 不論訂了什麼商品，都會夾帶來自中國的拋棄式口罩；

- 透過線上轉帳機制而非一般刷卡機制來支付購物款項；

- 這些網站的連絡地址和電話雖然都在美國，但卻都不是廠商真正使用的電話或住址，企圖誤導消費者以為該網站是由美國本土商家經營；

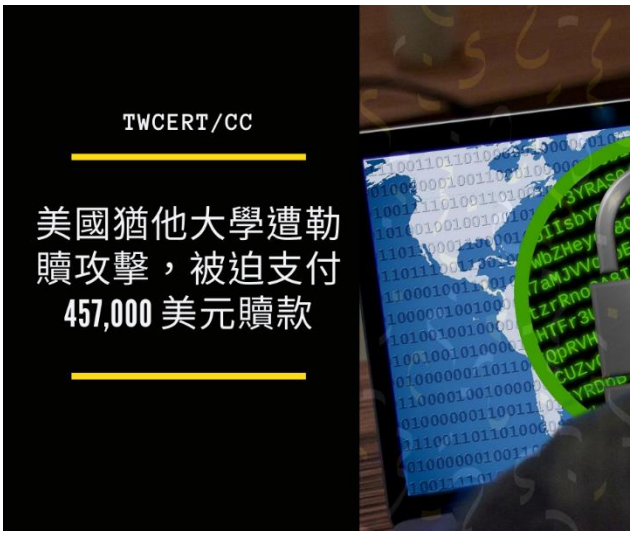
- 許多詐編網站的內容，都是從其他網站複製貼上，因此會有多個不同網站都使用相同電話與地址的情形出現。

當消費者發現收到的貨品品質不如預期，而要求退貨退款時，往往只能得到一部分的退費；詐騙者甚至會告訴消費者，就把隨貨寄到的口罩當做補償。也有些詐騙者會要求受害者將退貨寄到中國，受害者必須負擔高額運費。沒有任何受害消費者能成功取得全額退款。

FBI 呼籲大眾，在網路上購物，除了不要貪小便宜，在價格明顯過低的網站上購買外，也應注意是否可能是詐騙網站；包括其 TLD 網址非常見的 .com 而是 .club 或 .top 等、URL 是否為最近半年內才註冊、是否主要透過社群平台刊登廣告，或是其網域相關資訊被刻意隱藏等。

- 資料來源：
  1. https://www.ic3.gov/media/2020/200803.aspx
  2. https://www.infosecurity-magazine.com/news/fbi-issues-online-shopping-scam/

2.1.6、美國猶他大學遭勒贖攻擊，被迫支付 457,000 美元贖款



美國猶他大學於七月時遭勒贖攻擊，為避免校內重要資料遭駭侵者公開，猶他大學被迫支付高達 457,000 美元的贖款。

美國猶他大學日前發表資安通報，指出該校於今年七月時遭勒贖攻擊；為避免校內重要資料遭駭侵者公開，猶他大學被迫支付高達 457,000 美元的贖款。

遭到攻擊的是猶他大學的社會與行為科學學院（CSBS），該校的資安辦公室發現 CSBS 所屬的伺服器遭到不明駭侵團體攻擊；根據猶他大學的通報指出，約有 0.02% 的伺服器資料遭加密而無法存取。

近年來的勒贖攻擊中，駭侵者在加密受害系統資料前，都會先竊取這些資料；猶他大學這次的案例也不例外。不明駭侵者在攻擊行動成功後，便要脅猶他大學，若不支付贖金，便在網路上公開這批被竊的資料。

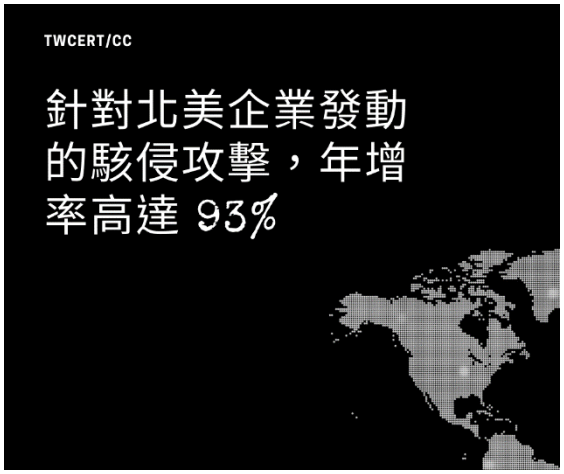
由於被竊資料中含有該校師生與職員的個人資訊，猶他大學決定支付贖款，以解密檔案；該校先前即已投保駭侵險，因此贖款係以保險理賠款項支付。

猶他大學在資安通報中也指出，在支付贖款後，猶他大學 CSBS 伺服器的運作已恢復正常；該校也將會要求所有師生變更密碼，但沒有說明該校是遭到哪一種勒贖軟體的攻擊，也沒有指出駭侵者的身分。

針對高等教育機構發動駭侵攻擊且成功逼迫受害者支付贖款的案例，猶他大學並非今年的首例；在 2020 年六月時加州大學舊金山分校也曾遭到勒贖攻擊，支付的檔案解密贖款高達 114 萬美元。

- 資料來源：
  1. https://attheu.utah.edu/facultystaff/university-of-utah-update-on-data-security-incident/
  2. https://www.bleepingcomputer.com/news/security/university-of-utah-hit-by-ransomware-pays-457k-ransom/

2.1.7、針對北美企業發動的駭侵攻擊，年增率高達 93%



研究報告指出過去一年以來，針對北美各型企業發動的駭侵攻擊事件，數量上暴增了 93%。

VPN 服務廠商 AtlasVPN 發表研究報告指出，過去一年以來，針對北美各型企業發動的駭侵攻擊事件有大幅增加的趨勢，在數量上暴增了 93%。

這份研究是由 VMWare Carbon Black 於 2019 年三月至 2020 年三月之間進行，調查了包括金融業、醫療業、政府機關等 250 家公私單位；其中遭受駭侵攻擊次數增加最多的是金融產業，駭侵攻擊次數較前一年增加達 56%，比各行業的平均值高了 11%。

這份研究同時指出，以特製惡意軟體進行植入攻擊，是駭侵者攻擊這些企業時最常使用的攻擊手法；金融產業遭到特製惡意軟體植入攻擊的比例高達 62%，其他產業被特製惡意軟體攻擊的比例則為 29%。

其他的攻擊手法則包括利用市售惡意軟體（11.5%）、供應鏈攻擊（9%）、勒贖攻擊（7%）等。

報告指出，遭攻擊次數較去年上升 1-25% 的企業，佔全體比例的 23%，攻擊次數增加 26-50% 的企業有 42%；上升 51-100 % 的有 24%，甚至有 4% 的企業，遭攻擊次數年增率高達 100% 到 300%。僅有 7% 的企業遭攻擊次數未較去年為多。

值得注意的是，有高達 88% 的企業認為，惡意攻擊次數的提升，與 Covid-19 疫情大流行高度相關；由於許多企業的員工在家遠距工作，因而提升了遭到駭侵攻擊的可能性。

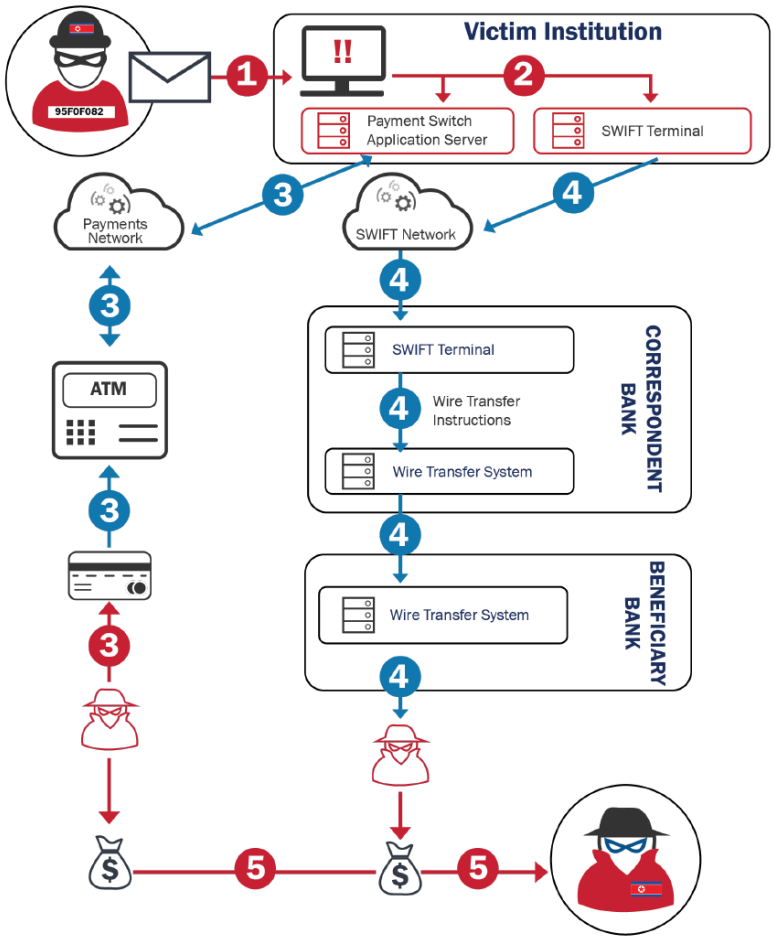
- 資料來源：
  1. https://atlasvpn.com/blog/cyberattacks-on-us-companies-skyrocketed-by-93-in-the-last-12-months
  2. https://trendingng.com/cyberattacks-on-us-companies-skyrocketed-by-93-percent/

2.2、國際政府組織資安資訊

2.2.1、美國財政部、聯邦調查局、國土安全部、網戰司令部發出聯合警訊，警示北韓政府針對多國金融機關從事駭侵活動

美國財政部、聯邦調查局、國土安全部、網戰司令部發出聯合警訊，自 2020 年 2 月起，朝鮮民主主義人民共和國（以下簡稱北韓）再次針對多國金融機構進行 ATM 駭侵活動，藉由惡意軟體來從事轉帳及現金提款，竊取銀行資金。該組織的駭侵活動於 2019 下半年暫時趨緩後，於今年 2 月重新啟動。

BeagleBoyz 是朝鮮人民軍總參謀部偵察總局旗下駭客組織，自 2015 年起，BeagleBoyz 針對多國銀行的 SWIFT 國際電匯系統、自動櫃員機（ATM）及客戶的銷售系統（POS, Point Of Sale）系統從事駭客活動，進而竊取資金及加密貨幣。近五年間，該團夥已嘗試盜取近 20 億美元，這些不法資金可能用以從事平壤政府的核子武器及飛彈開發。



該組織利用部分銀行在資安防護上的不完善，透過釣魚、水坑攻擊和社交工程等技巧，誘使受害機構的人員開啟惡意網站或啟動惡意程式，藉此入侵內部系統、取得權限並從事駭侵活動。於 2016 年起，該組織更開始攻擊多國金融機構內部的 IBM AIX (Advanced Interactive eXecutive) 伺服器，駭入銀行的支付交易應用程式來發送偽造的交易訊息，藉此於包含美國在內的 30 多個國家之 ATM 上盜領款項，竊取了數千萬美元的不法資金。除此之外，近期也開始偵測到該組織針對銀行間交易系統的活動，顯示其駭侵活動已開始向銀行系統的上層蔓延。

最著名的活動發生在 2016 年，該組織透過 Microsoft Word 巨集攻擊，入侵孟加拉銀行（該國之中央銀行）的內部資訊系統，偽造 SWIFT 轉帳電文，嘗試自該銀行於紐約聯邦儲備的帳戶，竊取近 10 億美元的款項。在其偽造的 35 項轉帳電文中，30 項被紐約聯邦儲備偵測到異常活動而被拒絕交易，而有 5 項被成功執行，總計成功竊取了約 8,100 萬美元（約新台幣 24 億），成為

了史上金額最高的銀行劫案。

北韓政府駭客組織 BeagleBoyz 的駭侵活動可能已涉及全球近 40 個國家，其中包含台灣、日本、南韓、新加坡、西班牙等先進已開發國家。聯合警訊中也提到，BeagleBoyz 可能與 Lazarus 和 APT38 駭客組織在組織和活動範圍上互相重疊。根據美國網路安全公司 FireEye 的報告，Lazarus 和 APT38 為 2017 年竊取遠東商銀 18 億新台幣的主謀，而三者皆為北韓政府所控制的駭客組織。

為避免受到駭客組織攻擊，所有的銀行、金融機構應遵守以下建議措施：

1. 遵照 FFIEC、ISO 等國際標準來部屬交易資訊系統及資訊安全防護系統；
2. 確保所有交易流程遵照 PCI Security 及 SWIFT 等組織的規範；
3. 使用防火牆、存取控制列表，並將機密資訊的資訊系統與其他網際網路服務之系統確實隔離；
4. 使用認證機制來保護所有內、外部的交易活動；
5. 確保內部控制機制，監視並記錄異常交易活動來偵測可疑的駭侵活動；
6. 使用多因子或兩步驟驗證來保護交易應用程式的存取。

對於使用零售支付系統的機構及所有使用者，應遵守以下建議措施：

1. 確保所有交易皆為加密傳輸，並確實受到信用卡發行機構或交易服務提供者的有效回覆；
2. 確保作業系統、防毒軟體、應用程式更新到最新狀態；
3. 禁用檔案分享及印表機分享服務；
4. 使用強密碼並定期更改；

5. 勿開啟來路不明的電子郵件附件，並執行電子郵件掃描；
6. 封鎖含有惡意內容的網站；
7. 謹慎使用卸除式裝置；
8. 掃描自網路網路下載之軟體或檔案；
9. 使用存取控制清單。

- 資料來源：

1. http://www.fisc.com.tw/Upload/80e295db-5cbf-46c2-973c-1a350c9745a9/TC/9606.pdf
2. https://us-cert.cisa.gov/ncas/alerts/TA18-275A
3. https://www.twcert.org.tw/newepaper/cp-65-808-3ad47-3.html
4. https://www.fireeye.com/content/dam/fireeye-www/regional/zh_TW/current%20threats/apt/rpt-apt38.pdf

2.2.2、美國國土安全部與 FBI 公布疑似北韓駭侵活動，以假徵人啟事散布惡意軟體

美國國土安全部與 FBI 發表聯合公告，指出一個北韓政府支持的駭侵團體，假冒美國軍工與能源相關公司的徵人啟事，試圖在這些公司的系統中植入惡意軟體。

美國國土安全部（DHS）與聯邦調查局（FBI）日前發表聯合公告，指出一個北韓政府支持的駭侵團體（代號為 Hidden Cobra），假冒美國軍工與能源相關承包商的徵人啟事，試圖在這些公司的系統中植入惡意軟體，以竊取各種和美國軍事與能源科技相關的機敏情報。

在 FBI 與 DHS 旗下資安主管機關「資安與基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA）的聯合公告中說，Hidden Cobra 駭侵團體運用一個稱為 BLINDINGCAN 的遠端遙控木馬，在目標單位的網路中流竄並試圖竊取資訊。

報告指出，Hidden Cobra 製作的偽造應徵文件中，除了含有惡意程式碼外，還會放置諸如波音公司等軍工承包商的圖誌，試圖以社交工程的手法，吸引目標公司的人資單位等人員誤點；之後再透過分布在多個國家的控制伺服器，一邊竊取機敏資訊，一邊下載更多惡意軟體，並持續擴大感染範圍。

據資安媒體 Cyberscoop 報導指出，北韓駭侵組織透過偽造的徵人啟事，以社交工程的手法來散布惡意軟體，在 2016 年與 2017 年都曾發生過。上周

在以色列也曾發生過類似的案例，北韓駭侵者利用偽造的 LinkedIn 徵人啟事，甚至還假扮成求才公司的高階主管，試圖入侵以色列的國防工業體系。

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a
  2. https://www.cyberscoop.com/north-korean-government-malware-hacking-fake-job-fbi-dhs/
  3. https://www.cyberscoop.com/north-korea-hackers-lazarus-group-israel-defense/

2.2.3、加拿大政府網站遭駭侵攻擊，疫情紓困專款遭盜領

加拿大政府設立的肺炎疫情紓困網站日前遭駭，用以對紓困民眾進行身分認證的登入系統遭到攻擊，駭客成功盜領部分民眾的紓困專款。

由加拿大政府設立，針對肺炎疫情提供移民、稅務服務與紓困專款的網站，日前遭到不明來源的駭侵攻擊；用以對紓困民眾進行身分認證的登入系統遭到攻擊，駭客也成功盜領部分民眾的紓困專款。

加拿大政府的資安相關單位，於上周末發表資安通報，指出管理該國政府各個網站的單一帳號登入系統遭到攻擊；全部 1200 萬個 CGKey 帳號，共有九千餘個被竊走。

加國政府說，駭客係利用自其他地方竊得的用戶登入資訊，以自動化程式嘗試登入該國政府網站；由於許多用戶習慣在不同服務之間使用完全相同的登入帳密，因此這種手法有一定比例的成功機率。

此外，資安專家指出，加拿大政府的身分認證與登入機制，並未導入二階段登入驗證機制，因此也增加了駭客嘗試登入的成功率。

加拿大政府緊急取消了所有可能遭竊的 CGKey 帳號，但也有受害民眾在 Twitter 上抱怨自己應得的紓困救濟金，因為帳號被鎖定而無法順利領取；另外也有人指出駭客盜領了他一萬加幣的紓困救濟金。

據多倫多 CTV 電視台的報導指出，目前遭駭的帳戶數量多達 700 個，但遭駭客竊取的紓困金總額，目前沒有公開。加拿大政府發布的資安通報，要求用戶不要在不同帳號間重覆使用相同密碼。

- 資料來源：
  1. https://www.canada.ca/en/treasury-board-secretariat/news/2020/08/statement-from-the-office-of-the-chief-information-officer-of-the-government-canada-on-recent-credential-stuffing-attacks.html
  2. https://www.bleepingcomputer.com/news/security/canada-suffers-cyberattack-used-to-steal-covid-19-relief-payments/
  3. https://toronto.ctvnews.ca/scammers-are-stealing-identities-to-redirect-cerb-payments-experts-warn-1.5065182

2.2.4、紐西蘭證交所連續三天遭境外 DDoS 大規模攻擊，導致股市交易暫停

紐西蘭證券交易所近日連續遭到數次來自境外的大規模 DDoS 攻擊；每一次攻擊都造成紐西蘭股市被迫暫停交易達數小時之久。

紐西蘭證券交易所近日連續三天遭到次來自境外的大規模 DDoS 攻擊；每一次攻擊都造成紐西蘭股市被迫暫停交易達數小時之久。

最近一次的攻擊發生在 8 月 27 日，自上午 11：10 起股市就無法進行正常交易。一直到當天休市時間之前，都未恢復正常。

受到攻擊的不只是紐西蘭證交所用以處理交易的相關設備，紐西蘭證交所本身的官方網站也同時遭到阻斷攻擊而無法正常運作。

8 月 26 日發生的第二次攻擊，使得紐西蘭股市交易自上午 11：24 至下午三時，都因系統無法運作而陷入停擺狀態。

據紐西蘭證交所發表的聲明指出，最近的 DDoS（分散式服務阻斷攻擊），和先前發生的攻擊樣態十分類似，都可能來自境外，但到底是誰發動這幾波攻擊，目前仍無從得知。

資安專家指出，紐西蘭股市不算是世界上主要的股票交易市場，過去也鮮少出現股市被駭侵攻擊的案例；但最近有不少企業即將發表財報或配發股息，該國股市最近也屢創新高，可能因此引起駭侵者的注意，因而發動連續攻擊行動。

值得注意的是，紐西蘭資安主管機關 CertNZ 於去年十一月時，曾發表資安通報，指出該單位接獲疑似來自俄羅斯駭侵團體「Fancy Bear」發出的電子郵件，要求若干被鎖定金融業者支付贖款，否則將發動 DDoS 攻擊；不過當時並沒有真的發生攻擊事件。

- 資料來源：
  1. https://www.cnbc.com/2020/08/27/new-zealands-exchange-faced-ddos-attacks-this-week.html
  2. https://securitybrief.co.nz/story/ddos-attack-strikes-nzx-for-third-time-in-as-many-days-43821379-7f0e-4598-8907-0735c9e5254c
  3. https://www.cert.govt.nz/individuals/alerts/financial-sector-targeted-in-blackmail-campaign/

2.3、行動裝置資安訊息

2.3.1、1200 個 iOS App 使用含有廣告詐騙惡意程式碼，且會竊取資料的 SDK

資安廠商發現一個提供 iOS App 行動廣告功能的 SDK，內含惡意程式碼，可用於監看用戶行為、製造詐騙廣告點擊，甚至還會竊取其他廣告平台的分潤。

資安廠商 Snyk 日前發表研究報告指出，該公司的資安研究團隊發現一個名為 Mintegral，可提供 iOS App 行動廣告功能的 SDK，內含惡意程式碼；不但可用於監看用戶行為、製造詐騙廣告點擊，甚至還會竊取其他廣告平台的分潤。

報告指出，該 SDK 內含的惡意程式碼，會從其開發的 App 內收集用戶的使用行為資訊和其他個人可辨識資訊，並上傳到第三方伺服器中。

此外，不少 App 開發者會在其 App 中同時顯示多個行動廣告平台，藉以提高廣告分潤收益；而 Mintegral SDK 中的惡意程式碼，會攔截 App 中所有的廣告點擊，這不但減低了原本應該發生在其他平台的廣告點擊，讓開發者誤以為 Mintegral 的廣告點擊表現更佳，還會製造其他平台的假廣告點擊，私吞應有的廣告分潤。

為了防止這些行為遭揭發，Mintegral SDK 還設有多道防護機制；除了會偵測用戶手機是否有越獄（Jailbreak）外，還會偵測是否有使用任何偵錯工具或 proxy 工具；一旦發現上述情形，SDK 就會停止各種惡意行為。

Snyk 說，就是因為這些防護功能，讓含有此 SDK 惡意程式碼的 App，能夠通過 Apple 的 App 上架審核流程不被發現。

據 Synk 報告的統計，目前 App Store 中有超過 1200 支 App 含有此 SDK 的惡意程式碼，所有 App 的每月下載安裝次數超過三億次。

- 資料來源：
  1. https://snyk.io/research/sour-mint-malicious-sdk/
  2. https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/

2.3.2、部分 APP 潛在資安風險及個資洩漏問題，使用者應謹慎處理

隨著 APP 的普及化，越來越多的 APP 開始成為不論是大人小孩都必不可少的生活樂趣之一，尤其是 TikTok 與 WeChat 等 APP 更是受到全球數十億使用者的歡迎。

然而，這些來自於中國的 APP，卻接連被認為有隱私及個資洩漏的問題，除了會回傳使用者的資訊之外，甚至有審查對於該國不利言論的質疑出現，連他國的使用者都難以倖免。

最為知名也備受爭議的 APP—抖音（TikTok），因其娛樂性及影片的豐富度極高，除了中國版本的抖音 APP 擁有極高的使用者外，連其全球版之 APP，在全球已有逾 20 億的下載量。然而，TikTok APP 卻一直有對於個資洩漏及隱私權的質疑出現，例如在 2019 年，Tiktok 簽署關於兒童線上隱私法的相關條例，不得在未經父母同意的情況下，蒐集 13 歲以下兒童的個資，即便是系統自動運作而蒐集，也應在事後進行刪除。但 TikTok 卻在今年(2020)七月，被指控未遵守該條例，仍然持續蒐集兒童的個人資訊，如此行為將可能導致兒童個資及隱私的不安全，因此美國聯邦貿易委員會重罰 TikTok 570 萬美元。除此之外，該 APP 爆炸性成長的使用者數量，一旦將這些使用者的個資回傳給該廠商、甚至該國，則全球的個資將會掌握在該國手中，因此 TikTok 也被美國情治單位稱為該國的「間諜網路程式」，警告使用者應注意自身個資和隱私的威脅。

除了娛樂性質的 TikTok APP 之外，全球經常使用的通訊 APP—微信

(WeChat)也成為個資和隱私權的質疑對象，但這個來自中國的通訊 APP，卻容易遭他人懷疑其隱私及安全性。在 2020 年五月，多倫多大學安全研究小組公布對於 WeChat APP 的研究，除了該國的使用者之外，即便是以他國電話號碼註冊的帳號，同樣會受到微信公司嚴密的監控。該監控機制主要是針對使用者傳遞的圖片訊息，先透過該圖片的雜湊值(hash)檢測是否已被確認為敏感性內容，一旦認為是敏感信內容則會即時封鎖，如若未被確認為敏感性內容，仍然會持續接受 AI 及人工審查，只要發現該圖片帶有敏感性內容，則會立即將其雜湊值納入黑名單中，拒絕該圖片的傳遞。雖然在多倫多大學的實驗中，他國帳號之間互傳帶有敏感性內容的圖片，並不會遭到嚴格審查及封鎖，但只要他國帳號將該圖片傳遞給該國帳號，則會立即遭到封鎖，代表即便使用者是以他國電話號碼註冊並使用非該國的帳號，其傳遞的內容仍會遭到一定程度的監視。而研究人員在仔細檢閱微信隱私權內容後，不論是中國版本或海外版本，都未有表示會監控他國帳號，微信公司也未正面回應該事件問題，導致其隱私權問題，持續遭到大眾質疑。

在人手一台智慧型手機的時代，APP 是必要的工具及娛樂方式，許多使用者會為了跟隨潮流，選擇受歡迎的 APP 下載，作為主要使用的工具及娛樂模式。但並非擁有大量使用者就代表其擁有足夠的安全性，使用者應在下載安裝時審慎評估，除了檢查其要求的內容、權限、隱私權政策外，相關資安單位或具公信力組織所提出的質疑亦需多方檢閱，避免因該 APP 的熱門程度而盲目下載，造成自身個資及隱私權的問題。

- 資料來源：
  1. https://www.parenting.com.tw/article/5087036-/
  2. https://opinion.udn.com/opinion/story/120611/3973187
  3. https://www.inside.com.tw/article/19740-wechat-users-outside-china-face-surveillance-while-training-censorship-algorithms
  4. https://buzzorange.com/techorange/2020/05/11/wechat-monitor-overseas-users/

2.3.3、中國平價手機遭預裝惡意程式，20 多萬台設備受影響

中國平價手機廠商深圳傳音控股（TRANSSION）遭爆，於旗下品牌 Tecno 系列智慧型手機中安裝惡意程式。

中國平價手機廠商深圳傳音控股（TRANSSION）遭爆，於旗下品牌 Tecno 系列智慧型手機中安裝惡意程式，該惡意程式會在未經使用者允許的狀況下訂閱付費服務，截至目前已有 20 多萬台的設備出現可疑交易。

中國廠商傳音控股所生產的行動裝置傳音手機，靠著價格低廉的政策，以及為族群量身打造的功能，在開發中國家受民眾廣泛支持。根據 IDC 的調查，在東非國家中，傳音控股旗下品牌的市場佔有率高達 6 成以上，而其業務也逐漸遍及中東、南亞等國家。

根據海外科技媒體 TechRadar 報導，行動裝置資安廠商 Upstream，在中國平價手機品牌傳音所生產的設備上，發現被預先安裝的惡意後門軟體 Triada。這個後門軟體會導致使用者一旦啟用裝置並連接網際網路，將會在使用者不知情的情況下訂閱付費服務，用以竊取使用者的預付通話費。

Triada 是一種針對 Android 環境開發的木馬程式，一旦被安裝在設備上，將會以 ROOT 的權限來存取系統檔案與更改其設定，而攻擊者可以透過 C&C Server（命令控制伺服器），在受害設備上下載並安裝任意應用程式、存取設備檔案及簡訊，甚至訂閱付費服務。在安裝後，Triada 會修改系統檔案及開機程序，將自身隱藏成系統應用程式，讓使用者無法移除該木馬程式。即使

使用者將設備回復原廠設定，仍無法移除 Triada 木馬。

由於在中國、非洲及南亞等開發中國家，使用者必須預付款項於門號中，才能使用通話、行動網路等電信服務，而門號上的預付款在許多開發中國家也是唯一的電子支付方式。使用者在訂閱電信商或應用程式的付費服務時，通常需要使用簡訊來驗證，而 Trida 木馬程式能自動接收簡訊並傳送至攻擊者端，導致使用者在不知情的情況下，消耗預存通話費訂閱服務。根據報導，至今已經發現了 20 萬支行動設備上，共 1,920 萬筆的可疑交易，受害者遍佈全球 19 個國家。

儘管如此，傳音控股的行為卻未被 Android 系統開發商 Google 所譴責，相反地，Google 在其安全團隊的部落格中表明，認為這些惡意程式的存在是源於上游供應商，而手機生產商只是誤用了含有惡意軟體的第三方元件。

- 資料來源：
  1. https://www.techradar.com/news/chinese-smartphone-maker-selling-devices-with-malware-pre-installed
  2. https://www.kaspersky.com/blog/triada-trojan/11481/
  3. https://security.googleblog.com/2019/06/pha-family-highlights-triada.html
  4. https://www.idc.com/getdoc.jsp?containerId=prMETA46136320&utm_medium=embedd&utm_campaign=idc_embedd&utm_source=referra

2.4、軟體系統資安議題

2.4.1、Cisco 修補完成多個影響交換器、光纖儲存設備的嚴重資安漏洞

Cisco 最近發表資安通報，揭露 8 個嚴重資安漏洞，可能影響該公司旗下多款網路交換器與光纖儲存裝置；所幸這些漏洞均已修補完成。

網通設備大廠 Cisco 最近發表資安通報，揭露多個資安漏洞的修補訊息；其中有 8 個嚴重資安漏洞可能影響該公司旗下多款網路交換器與光纖儲存裝置；所幸這些漏洞均已修補完成。

被發現最多漏洞的是 Cisco NX-OS，共有六個嚴重資安漏洞，會造成 Cisco Nexus 系列的以太網路交換器與 MDS 系列光纖通道儲存裝置遭到攻擊。

其中兩個漏洞 CVE-2020-3397 和 CVE-202-3398 發生在 Cisco NX-OS Border Gateway 通訊協定中的 Multicast VPN，可能造成駭侵者藉以發動 DoS 攻擊。

另一個 CVE-2020-3338 漏洞則存在於 NX-OS IPv6 PIM 的錯誤，駭侵者同樣可利用這個錯誤發動 DoS 攻擊；受影響的機種為 Cisco Nexus 3000 系列、7000 系列 與 9000 系列的交換器。

其他出現在 NS-OS 的嚴重資安漏洞，也包括一個 Call Home 指令注入錯誤，可讓駭侵者以 root 權限遠端執行任意程式碼；受此漏洞影響的 Cicso 網

通設備，則包括 MDS 9000 系列多層交換器，以及 Nexus 9500-R 系列的交換器平台等。

- 資料來源：
  1. https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities
  2. https://threatpost.com/cisco-high-severity-bugs-impact-switches-fibre-storage/158691/

2.4.2、DoH 技術遭駭客組織利用，網路安全技術淪竊密工具

來自伊朗的 APT34（Advanced Persistent Threat，進階持續性威脅）駭客組織，正利用最新的 DNS over HTTPS（DoH）技術，規避既有資安設備的監控。

根據 ZDnet 報導，在網路安全公司 Kaspersky（卡巴斯基）所舉辦的研討會上，資安專家 Vicente Diaz 介紹了這個在網路犯罪活動上的重大技術革新。來自伊朗的駭客組織 Oilrig，開始利用 DoH 技術來從事駭客活動的資料傳輸，該組織利用一種名為 DNSExfiltrator 的工具，將資料偽裝成 DNS 查詢封包，並以 HTTPS 協議在網際網路上傳輸。使用這項至 2018 年才發布的新技術，許多市面上的網路安全產品皆難以偵測其活動，讓受駭者難以發現，藉此規避資安威脅偵測與監控。

DNS over HTTPS（DoH）技術在 2018 年由 IETF（Internet Engineering Task Force，網際網路工程任務組）推出，透過 HTTPS 協定，建立使用者端到 DNS（Domain Name Service，網域名稱系統）伺服器的點到點加密連線，藉此取代傳統上經由 port 53 的 DNS 請求，提升網路傳輸的安全性。

然而，這已經不是該威脅組織第一次利用 DNS 技術來從事駭客活動，自 2018 年底，Oilrig 便已開始利用被稱為 DNSpionage 的客製化工具來從事駭客活動，並向數個 COVID-19 有關的網域傳輸資料，因此令人聯想到近期氾濫的 COVID-19 相關駭客活動與網路釣魚。

根據美國資安公司 FireEye 的資料，來自伊朗的駭客組織 APT34（又稱 Oilrig），主要活動範圍在中東地區，針對政府、能源和金融組織進行攻擊，因此被認為與伊朗政府有所關聯。

- 資料來源：
  1. https://www.zdnet.com/article/iranian-hacker-group-becomes-first-known-apt-to-weaponize-dns-over-https-doh/
  2. https://malpedia.caad.fkie.fraunhofer.de/actor/apt34
  3. https://blog.twnic.tw/2019/06/25/4125/
  4. https://tools.ietf.org/html/rfc8484
  5. https://www.twcert.org.tw/newepaper/cp-65-3588-12d29-3.html。

2.4.3、Intel 內部文件被公開在外網，數量高達 20GB 以上

美國晶片製造商 Intel 有近 20 GB 的內部機密文件，被分享到外部網路上；Intel 目前正展開調查。

美國首屈一指的晶片製造商 Intel，近日有近 20 GB 的內部機密文件，被分享到外部網路上；Intel 目前正展開調查，希望能夠查明如何外洩。

這批高達 20GB 的文件資料，許多都標有「機密」或「限閱」字樣，且被上傳到廣為許多用戶愛用的匿名檔案分享網站 Mega 上。上傳資料的是一名瑞士工程師，他表示這批資料是一名匿名駭客傳給他的，該名駭客自稱曾在今年年初時駭入 Intel，取得這批機密文件檔案。

這名工程師還說，被放上 Mega 分享網站的檔案，不過只是近來 Intel 所有被竊檔檔案的其中一小部分而已。

資安媒體 ZDNet 在相關報導中指出，這批外洩檔案內含多種晶片組的設計資料，包括 2016 年以來的多種產品技術規格、產品指南、處理器使用手冊等等，但未包含任何 Intel 內部員工和顧客相關的機敏資訊。

不過，Intel 在回應採訪時否認這批資料是因遭駭而流出的；Intel 認定是某個可以自 Intel 內部網站「資源與設計中心」存取該批資料的員工，在未經授權的情形下，將這些檔案下載並分享給該瑞士工程師。

ZDNet 說，在該媒體掌握的外洩檔案中，有相當多檔案有標有「資源與設計中心」的字樣，似乎可以印證 Intel 的說法。不過該工程師也提出他和匿名駭客的對話記錄，對方說資料是從一個未加上安全防護的 Akamai CDN 伺服器上下載的，沒有使用任何可以登入 Intel 資源與設計中心主機的帳號。

- 資料來源：
  1. https://www.zdnet.com/article/intel-investigating-breach-after-20gb-of-internal-documents-leak-online/
  2. https://www.anandtech.com/show/15962/intel-data-breach-20gb-of-ip-leaked
  3. https://arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/

2.4.4、LG、Xerox 內部資料遭竊並公開

近來頻繁發動攻擊的勒贖軟體 Maze，其幕後主使者於網路上公開受害者 LG 和 Xerox 的內部資料。

近來頻繁對公私營機關發動駭侵攻擊的勒贖軟體 Maze，其幕後主使者日前於網路上公開受害者 LG 和 Xerox 的公司內部資料。

資安媒體 ZDNet 報導指出，被駭侵者公開的資料，數量相當龐大；LG 的被竊資料大小高達 50.2 GB，而 Xerox 的被竊資料則有 25.8 GB。

據報導指出，LG 是在今年六月時遭到 Maze 勒贖軟體的攻擊，當時 LG 只對媒體簡單發表了一般性的聲明，並未對遭駭事件的細節加以說明。

Maze 幕後的駭侵團體，慣用的攻擊手法，是先竊取企業的各種機敏資訊，然後將之加密，最後再要求被駭者在數週內支付巨額贖款以解密資料；如果企業不從，不願支付贖款，企業自行利用備分檔復原被加密的資訊，Maze 駭侵者就會架設一個網站，威脅被害者若不支付贖款，資料就會遭到公開。

這次 LG 和 Xerox 的案例亦同；自六月起，Maze 駭侵者就開始不斷嘲弄這兩家被駭的公司，也設立了這兩家公司的「資料外洩入口」網站。由於 LG 和 Xerox 堅拒支付贖金，資料遭到公開。

據 ZDNet 取得的部分情資顯示，LG 遭公開的資料，多半和其產品所使用的程式碼相關，例如手機和筆記型電腦使用的充電相關控制軟體等；而 Xerox 遭公開的資料則是和客服相關資料。

- 建議採取資安強化措施

1、 定期將系統、資料進行異地備份，並將備援主機採取離線、網路隔離的模式。

2、 企業應落實對員工的資安宣導與教育訓練，以降低員工受到網路釣魚、社交工程等資安攻擊的可能性。

3、 配合廠商推出的安全性更新，即時更新軟體和系統漏洞，防止駭客透過漏洞進行駭侵攻擊或是執行其他未經授權的行為。

- 資料來源：

1. https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/
2. https://securityaffairs.co/wordpress/106749/cyber-crime/maze-ransomware-lg-xerox.html
3. https://www.kaspersky.com/blog/ransomware-data-disclosure/32410/
4. https://www.acw.org.tw/Events/Detail.aspx?id=1050

2.4.5、Microsoft Teams 先前針對駭客以假冒更新檔進行離地攻擊的修補方式，被證實無法奏效

Microsoft Teams 再度被資安廠商發現離地攻擊漏洞，駭侵者可假冒安裝更新，進行遠端植入並執行惡意程式碼。

新加坡電信旗下的資安團隊 Trustwave 日前發表研究報告，指出 Microsoft Teams 再次被發現離地攻擊漏洞；駭侵者可假冒安裝更新，進行遠端植入並執行惡意程式碼。

報告指出，去年 Microsoft Teams 就被發現存有離地攻擊漏洞；駭侵者可假藉安裝更新程式名義，透過傳訊方式要求用戶輸入更新指令，伺機安裝惡意程式碼；Microsoft 當時提出的解決方式，是限制系統不可透過 URL 下載更新檔，但允許用戶從本機或內部網路共享路徑下載並安裝更新程式。

報告說，這樣的修補方式並無法徹底解決 Microsoft Teams 遭離地攻擊的風險；駭侵者仍可以先設法將假冒為更新檔案的惡意程式檔案，事先置於內網共享資料夾內，或是使用遠端 SMB 分享，再拐騙內部用戶使用假檔案更新 Microsoft Teams，同樣能夠達成植入並執行惡意軟體的作業。

報告指出，Microsoft Teams 透過開源軟體 Squirrel 其中的 NuGet 套件來處理檔案下載與更新，因此假扮成更新包的惡意程式碼，只要命名為 Squirell.exe 並置於特定位置，同時提供假的 metadata，即可成功安裝。

撰寫報告的資安專家將其發現回報給微軟，但微軟回應指出，由於許多客戶頻繁使用 SMB 檔案分享功能，因此從產品設計的角度上，無法禁用 SMB 更新。

- 資料來源：
  1. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/microsoft-teams-updater-living-off-the-land/
  2. https://www.bleepingcomputer.com/news/security/hackers-can-abuse-microsoft-teams-updater-to-install-malware/

2.4.6、微軟八月資安修補包，修復多個漏洞，包括兩個遭駭侵者利用的 0-day 漏洞

微軟於八月推出的例行資安修補包已於日前釋出，其中包括兩個已遭駭侵者廣泛利用的 0-day 嚴重漏洞，也已獲得修補。

微軟於八月推出的例行資安修補包「Patch Tuesday」已於日前釋出，總共修復 120 個大小資安漏洞；值得注意的是，其中包括兩個已遭駭侵者廣泛利用的 0-day 嚴重漏洞修補。

其中一個已得到修補的 0-day 漏洞，是編號 CVE-2020-1464 的漏洞；這個漏洞源於 Windows 系統處理檔案數位簽章時的錯誤；駭侵者可藉以偽造檔案的安全數位簽章，騙過系統檢查。幾乎所有 WIndows 版本，從 Windows 7 到 Windows 10 的各平台版本均存有此一漏洞。

這個漏洞的 CVSS 危險程度評分為 5.5 分，危險程度評級為中等。

另一個得到修補的 0-day 漏洞 CVE-2020-1380 發生於 Internet Explorer 在處理 script 程式碼時發生的記憶體崩潰錯誤；駭侵者可藉由此一漏洞提升執行權限，並且遠端執行任意程式碼。這個錯誤發生在各 Windows 版本上的 Internet Explorer 11。

這個漏洞的 CVSS 危險程度評分為 7.8 分，危險程度評級為高等。

這次微軟推出的八月資安修補包一共修復多達 120 個資安漏洞，其中有 17 個漏洞的危險程度評級達到嚴重等級，其餘 103 個為重要等級；建議微軟

產品用戶盡快透過系統更新程式下載安裝每個月的資安修補包，降低遭到駭侵的風險。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1464
  2. https://nvd.nist.gov/vuln/detail/CVE-2019-1464
  3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380
  4. https://nvd.nist.gov/vuln/detail/CVE-2019-1380

2.4.7、挖礦惡意程式藉由假防毒防駭軟體大肆散布

資安廠商發現，有不明駭侵者在網路上散布假的惡意軟體掃瞄移除程式，其中藏有挖礦惡意程式碼。

資安廠商 Avast 近日發表研究報告，該公司發現有不明駭侵者在網路上散布假的惡意軟體掃瞄移除程式 Malwarebyte，其中藏有挖礦惡意程式碼，會潛藏於受害者的電腦系統上進行挖礦。

Avast 說，該公司在八月下旬起開始偵測到一些假冒的 Malwarebyte 安裝程式，內含會載入 XMRig 惡意軟體的後門；用戶如果安裝了，就會被植入 XMRig 惡意軟體，電腦系統資源將遭盜用進行 Monero 加密貨幣挖礦。

這些假冒的 Malwarebyte 安裝程式，係將惡意程式碼藏在 MBSetup2.exe 以及 Qt5Help.dll、Qt5WinExtras.dll 檔案中，安裝完成後會利用 MBAMSvc 服務下載惡意軟體程式碼的酬載，內含挖礦用的 Bitminer 程式。

目前的受害者多分布於俄羅斯、烏克蘭和東歐諸國。

Avast 說，真正的 Malwarebyte 軟體並不含上述的 .dll 檔，下列檔案也可能會被安裝在 PC 中：

- %ProgramData%\VMware\VMware Tools\vmtoolsd.exe
- %ProgramData%\VMware\VMware Tools\vmmem.exe
- %ProgramData%\VMware\VMware Tools\vm3dservice.exe

- %ProgramData%\VMware\VMware Tools\vmwarehostopen.exe

一旦用戶發現自己電腦上有上述檔案，應該立即移除；同時也應移除「%ProgramFiles(x86)%\Malwarebytes」資料夾中的所有檔案，以策安全。

- 資料來源：
  1. https://blog.avast.com/fake-malwarebytes-installation-files-distributing-coinminer
  2. https://securityboulevard.com/2020/08/fake-malwarebytes-installation-files-distributing-coinminer-avast/

2.4.8、駭侵者可利用 Zoom 資安漏洞，以暴力試誤法破解私人視訊會議密碼

資安專家發現 Zoom 存有一個資安漏洞，可讓駭侵者透過暴力試誤法，猜到私人會議使用的密碼，進而加入會議。

獨立資安專家 Tom Anthony 於日前發現 Zoom 一個嚴重資安漏洞，可讓駭侵者以暴力試誤法重覆嘗試，快速找出私密視訊會議的密碼並登入會議。

這個漏洞出在 Zoom web 版本；web 版本的 Zoom 連線程式不但存有 CSRF 錯誤，甚至完全不限制密碼錯誤重試次數。由於 Zoom 的會議室密碼僅為六位數字，因此理論上最多只要猜測一百萬次，最終能猜到密碼。

Tom Anthony 說，3 月 31 日時英國首相 Boris Johnson 透過 Zoom 進行英國史上首次遠距內閣會議，在其 Twitter 推文的螢幕截圖上顯示了其 Zoom 會議室的編號，引發他的興趣，開始研究 Zoom 會議的登入機制，因而發現這個漏洞。

Tom Anthony 指出，透過自動化程式猜測密碼，要破解這麼短、組合這麼少的會議密碼，根據其測試結果，不到半小時就猜出了正確的密碼；這還是使用單線執行的結果，如果以多台主機分散執行密碼猜測工作，猜到正確密碼的速度還能大幅加快。

該專家於今年四月一日時，將其發現結果通報給 Zoom 公司，Zoom 很快就在四月九日時更新其 Web 會議連線程式；除了修正 CSRF 錯誤、新增密碼

試誤次數限制外，也將密碼格式由原本易破解的六位數字，改成更長的非數字格式，完全修復這個漏洞。

- 資料來源：
  1. https://www.tomanthony.co.uk/blog/zoom-security-exploit-crack-private-meeting-passwords/
  2. https://threatpost.com/zoom-flaw-could-have-allowed-hackers-to-crack-meeting-passcodes/157883/
  3. https://www.securityweek.com/vulnerability-allowed-brute-forcing-passwords-private-zoom-meetings

2.4.9、資安研究人員發現新版挖礦僵屍網路，會竊取 AWS 登入資訊

資安研究人員發表研究報告，指出近期有個挖礦僵屍網路，除了會盜用受害者的計算資源挖礦外，還會竊取 AWS 伺服器的登入資訊。

資安廠商 Cado Secutiry 旗下的研究人員，日前發表研究報告，指出近期發現有個挖礦僵屍網路，除了會盜用受害者的計算資源挖礦外，還會竊取 AWS 伺服器的登入資訊。

這個僵屍網路過去曾被趨勢科技資安團隊截獲，當時命名為 Team TNT，Cado Security 發現 Team TNT 最近增加了新功能，不但專門鎖定使用 Docker 或 Kubernates 的容器平台進行駭侵攻擊，而且還會竊取 host 所在 AWS 伺服器的登入資訊。

除了竊取 AWS 登入資訊外，新版 Team TNT 僵屍網路還會掃瞄本機端的各種登入資訊，並且掃瞄 internet 上配置不當的其他 Docker 和 Kubernates 平台。

Cado Security 的研究人員將試驗用的登入資訊傳送給 Team TNT 的控制伺服器，從而證實了目前 Team TNT 還沒有開始針對收集來的配置不良 Docker 與 Kubernates 容器進行攻擊。

Team TNT 借用了另一個名為 Kinsing 的惡意軟體部分程式，這支惡意軟體除了會挖礦之外，也會針對 Docker 平台進行攻擊。

資安專家指出，絕對不要在系統內儲存 AWS 或任何其他系統的未加密登入資訊，也應針對 Docker 平台加上強化的防火牆保護，禁止任何不必要的網路存取。

- 資料來源：
  1. https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
  2. https://www.trendmicro.com/vinfo/hk-en/security/news/virtualization-and-cloud/coinminer-ddos-bot-attack-docker-daemon-ports
  3. https://securityaffairs.co/wordpress/107248/malware/teamtnt-botnet-steals-aws-credentials.html?utm_source=rss&utm_medium=rss&utm_campaign=teamtnt-botnet-steals-aws-credentials

2.5、軟硬體漏洞資訊

2.5.1、以 Chromium 為基礎的瀏覽器，存有可跳過內容安全原則的嚴重 0-day 漏洞

資安廠商發現以 Chromium 為基礎的瀏覽器，均存有可輕易跳過內容安全原則的嚴重 0-day 漏洞。

資安廠商 PerimeterX 的研究人員，近日發表研究報告，指出市面上以 Chromium 為基礎的各種瀏覽器，存有一個可讓駭侵者跳過網站內容安全原則（Content Security Policies，CSP）的嚴重 0-day 資安漏洞。

這個 0-day 漏洞駭侵者只要將原本會被瀏覽器的內容安全原則（CSP）阻擋的惡意 javascript 程式碼，包入 iframe 當中，即可輕易繞過 CSP 機制。

以 Chromium 為基礎的瀏覽器，包括 Google Chrome、Opera、Microsoft Edge 等的 Windows、Mac、Android 版本，從 2019 年三月發行的版本 73，到今年七月發行的版本 83，全部存有這個漏洞。

光是 Google Chrome 瀏覽器的市場佔有率就高達 65% 以上，使用者多達 20 億人；再加上許多知名熱門網站，包括 Facebook、Gmail、Zoom、TikTok、Instagram、WhatsApp、Blogger、Quora 等，都無法避免駭侵者利用此 0-day 漏洞執行惡意程式碼，因此這個漏洞影響層面極廣，若遭有心人士惡意利用，可能帶來的衝擊也不容忽視。

但也有一些知名熱門網站，例如 Twitter、Github、LinkedIn、Google Play Store、Yahoo 登入頁面、PayPal 等，其 CSP 以 nonce 或 hash 機制加強保護，因此不受本漏洞的影響。

這個漏洞編號為 CVE-2020-6519，其 cvss 影響嚴重程度評分為 6.5 分，屬中等嚴重程度。Chromium 瀏覽器用戶應盡速升級至 84 以上版本，始可避免受此漏洞影響；網站管理者應使用 nonce 或 hash 功能，以加強 CSP 的防護能力。

- CVE 編號：CVE-2020-6519
- 影響產品/版本：以 Chromium 為基礎的瀏覽器，包括 Google Chrome、Micrisift Edge、Opera 等，版本 73 至 83，Windows、Mac、Android 平台。
- 解決方案：用戶應升級至版本 84 以上，網站管理者應加強 CSP 防護能力。

- 資料來源：
  1. https://www.perimeterx.com/resources/blog/2020/vulnerability-discovered-in-google-chrome-csp-enforcement/
  2. https://www.perimeterx.com/tech-blog/2020/csp-bypass-vuln-disclosure/
  3. https://nvd.nist.gov/vuln/detail/CVE-2020-6519

2.5.2、Google 修復可造成遠端執行任意程式碼的嚴重 Chrome 漏洞

目前全球使用率最高的網頁瀏覽器 Google Chrome，遭 Cisco Talos 的資安研究人員於五月時發現一個嚴重的資安漏洞，可能導致駭侵者用以進行遠端任行程式碼執行攻擊。

這個嚴重漏洞的編號為 CVE-2020-6492，問題源於 Chrome 瀏覽器中的 WebGL 繪圖子系統中的「使用已釋放記憶體」（Use-after-free）錯誤；駭侵者可利用這個錯誤來執行任意程式碼。

CVE-2020-6492 的危險程度評分高達 8.3 分，嚴重程度等級為「高」。

Cicso Talos 發現存有這個漏洞的 Google Chrome 版本為 81.0.4044.138（Stable）、84.0.4136.5（Dev）以及 84.0.4143.7（Canary）；其他研究者則指出從 Chrome 版本 73 到 84 都存有此漏洞，而且其他以 Chromium 為核心的相容瀏覽器，也可能受到這個漏洞的影響；而且不論是 Windows、Mac、Linux 或 Android 版本，都存有此漏洞。

Google 已於 8/24 發布的新版 Chrome 85 版中解決了這個漏洞，Chrome 或 Chromium 相容瀏覽器如 Edge、Brave、Opera 等的用戶，應儘速將瀏覽器升級至最新版本，以降低受此漏洞影響的資安風險。

- CVE 編號：CVE-2020-6492
- 影響產品/版本：各平台 Google Chrome 或 Chromium 相容瀏覽器，版本 73~84。
- 解決方案：升級至 Chrome 85 以上版本。

- 資料來源：
  1. https://blog.talosintelligence.com/2020/08/vuln-spotlight-chrome-use-free-aug-2020.html
  2. https://threatpost.com/google-fixes-high-severity-chrome-browser-code-execution-bug/158600/
  3. https://www.chromestatus.com/features/schedule

2.5.3、微軟緊急推出資安修補更新，修復兩個可提升執行權限的資安漏洞

微軟 8/20 緊急推出修復兩個嚴重資安漏洞的更新，分別修復 CVE-2020-1530 和 CVE-2020-1537 漏洞。

微軟發布例行性的 Patch Tuesday 每月資安修補包，修復了 120 個大小漏洞後，8/20 又緊急推出修復兩個嚴重資安漏洞的更新，分別修復 CVE-2020-1530 和 CVE-2020-1537 漏洞。

CVE-2020-1530 這個漏洞存於 Windows Remote Access 服務的記憶體管理錯誤，可讓已經入侵的駭侵者提升系統權限，以便進行更進一步的攻擊行動。受到此漏洞影響的 Windows 版本相當多，自 Windows 7 SR1、Windows 8.1 到 Windows 10 各版本，以及 Windows Server 2008 到現行版本，皆含有此一漏洞。

這個漏洞的 CVSS 危險程度評分高達 7.8 分。

CVE-2020-1537 這個漏洞造成的問題和 CVE-2020-1530 類似，同樣能讓駭侵者提升自己的系統執行權限，但問題的根源是來自檔案處理的錯誤。受影響的 Windows 版本也相當多，從 Windows 7、8.1 到 Windows 10 的各平台版本，以及 Windows Server 自 2008 到現行版本，也都存有此一漏洞。

這個漏洞的 CVSS 危險程度評分，與 CVE-2020-1530 相同，同樣高達 7.8 分。

微軟指出，用戶應立即下載更新檔案，以修補這兩個漏洞，減少遭駭侵者利用這兩個漏洞強化攻擊的風險。

- CVE 編號：CVE-2020-1530、CVE-2020-1537
- 影響產品/版本：Microsoft Windows 7、8.1、10 各平台版本、Windows Server 2008 到現行各平台版本
- 解決方案：自後方連結下載更新檔案即可修復；https://www.catalog.update.microsoft.com/Search.aspx?q=KB4578013

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1530
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1537
  3. https://www.computing.co.uk/news/4019202/microsoft-flaw-windows-remote-access

2.5.4、資安專家發現 Windows 印表機服務存有 0-day 資安漏洞

資安廠商 SafeBreach Labs 的兩名資安研究人員 Peleg Hadar 與 Tomer Bar，發現曾被修補過的 Windows Print Spooler（印表機服務程式）的執行權限提升漏洞（CVE-2020-1048），可以透過某種方式跳過而再度形成資安威脅。

Print Spooler 是用以管理列印行程的程式，兩名資安專家指出 Windows 中的 Print Spooler 程式碼至少有二十年的歷史，因此很容易出現各種資安漏洞，例如 CVE-2010-2729 就是十年前發現的另一個權限提升漏洞。

研究報告指出，CVE-2020-1337 可以提升任何本機程式在作業系統中的執行權限，受到影響的 Windows 版本極廣，從 Windows 7 到 Windows 10 以來的所有 32 位元、64 位元版本，均存有這個漏洞。

成功利用這個漏洞的駭侵者，除了可以取得系統執行權限外，也能夠自我藏身在系統中，每次重啟時都能自動背景執行惡意程式碼。

這個漏洞是由 Peleg Hadar 和 Tomer Bar 於美國舉行的 Black Hat USA 2020 資安研討會上發表的，其 CVSS 危險程度評分是 8.1 分；雖然目前還沒有解決方法，但微軟已表示將在八月發行的 Patch Tuesday 中加以修補。

- CVE 編號：CVE-2020-1337
- 影響產品/版本：自 Windows 7 至 Windows 10 所有版本（含 32 位元、64 位元）
- 解決方案：微軟於 2020 年八月例行更新中修補此漏洞

- 資料來源：

1. https://i.blackhat.com/USA-20/Thursday/us-20-Hadar-A-Decade-After-Stuxnet-Printer-Vulnerability-Printing-Is-Still-The-Stairway-To-Heaven-wp.pdf
2. https://www.helpnetsecurity.com/2020/08/07/zero-days-windows-print-spooler/
3. https://www.cybersecurity-help.cz/vdb/SB2020080804
4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=ALAS-2020-1337

第 3 章、 資安研討會及活動

【台灣網路講堂】善用數位科技承先啟後，攜手全球公眾共創未來	
活動時間	**2020 年 9 月 17 日（四）14:00-16:00**
活動地點	**IEAT 會議中心 8F 國貿講堂** **（臺北市中山區松江路 350 號,台北市進出口商業同業公會）**
活動網站	**https://www.ihub.tw/Calendar/ihub2020-09**
活動概要	 **主辦單位：TWNIC、TWIGF、NII** 本場講堂活動邀請國內多方利害關係人，從網際網路在技術發展、應用創新、公共政策可著力之觀點，一同探討在 25 年後，亦即聯合國成立 100 年之際，數位科技與網路如何成就我們的未來？是否由於網路科技發展使下一代擁有更多的機會？使所有人都受平等對待？公眾與政府之間的信任因此增強或減弱？網路犯罪有可能停止嗎？國與國之間會不會更劍拔弩張？聯合國或類似組織，在現階段的優先著力點應該是？台灣作為全球公民，又可以扮演的角色？ 活動議程 13:30 - 14:00 活動報到 14:00 - 14:10 主持人開場與介紹與談人 14:10 – 15:50 焦點座談 15:50 - 16:00 現場 QA

遠程辦公一樣可以兼顧安全與工作效率	
活動時間	**2020 年 9 月 23 日（三）14:00**
活動地點	**線上講堂**
活動網站	**http://surl.twcert.org.tw/wPS4s**
活動概要	 **主辦單位：VMware** 為幫助企業迎頭趕上，透過最正確的實施做法、最有效率的部署方式、建立最完善的遠程辦公環境，VMware 將在 9/23、10/7 舉行兩場「週三線上講堂 - 遠程辦公系列」網路研討會。 趕緊為新型態的工作環境做好準備；讓遠程辦公不再是阻礙公司業務發展的藉口，反倒能抓住絕佳機遇，順勢開啟更高效、更經濟的創新協作模式！ 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 9/23 14:00 遠程辦公一樣可以兼顧安全與工作效率 ● 如何讓員工就算不在辦公室，也能輕鬆的使用工作桌面環境辦公 ● 遠程辦公如何協同作業 ● 遠程辦公如何克服資安問題

IoT Sandbox 2020 智慧物聯網資安競賽	
活動時間	**2020 年 9 月 26 日、29 日，2020 年 12 月 11、12 日（五-六）**
活動地點	**台中、台北、台南**
活動網站	**https://nchc-cdx.kktix.cc/events/iotsandbox2020**
活動概要	 **主辦單位：財團法人國家實驗研究院國家高速網路與計算中心** 延續 2019 年科技部指導辦理之「IoT 資安挑戰賽」，於今年規劃的「IoT Sandbox 2020 智慧物聯網資安競賽」將以物聯網居家裝置為主軸作為測試標的，期能邀集國內 IoT 廠商提供設備測試，並邀請國內資安組織或產業擔任評審團，以競賽的型式進行設備的弱點發掘。將物聯網路相關裝置與設備，透過競賽平台搭配情境設計，由參賽者進行解題，所匯集之技術能量將形成一股推動學研與產業發展的助力，形成正向的循環力量，讓技術的能量可以幫助產業獲利，同時讓產業得以回饋至技術社群，讓技術支援產業。 競賽流程：本次競賽分為初賽及決賽，初賽分為中區及北區共兩場，限擇一場次報名參加，晉級後的參賽隊伍獲得參與決賽之資格。 競賽獎項：決賽總獎金 新臺幣 50 萬元 競賽時程： 【 初賽 - 台中 】日期：2020 年 09 月 26 日（六）地點：集思新烏日會議中心 【 初賽 - 台北 】日期：2020 年 09 月 29 日（二）地點：中華電信學院板橋院本部 CB1001 樓 【 決賽 - 台南 】日期：2020 年 12 月 11-12 日（五-六）

第 4 章、 2020 年 08 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。

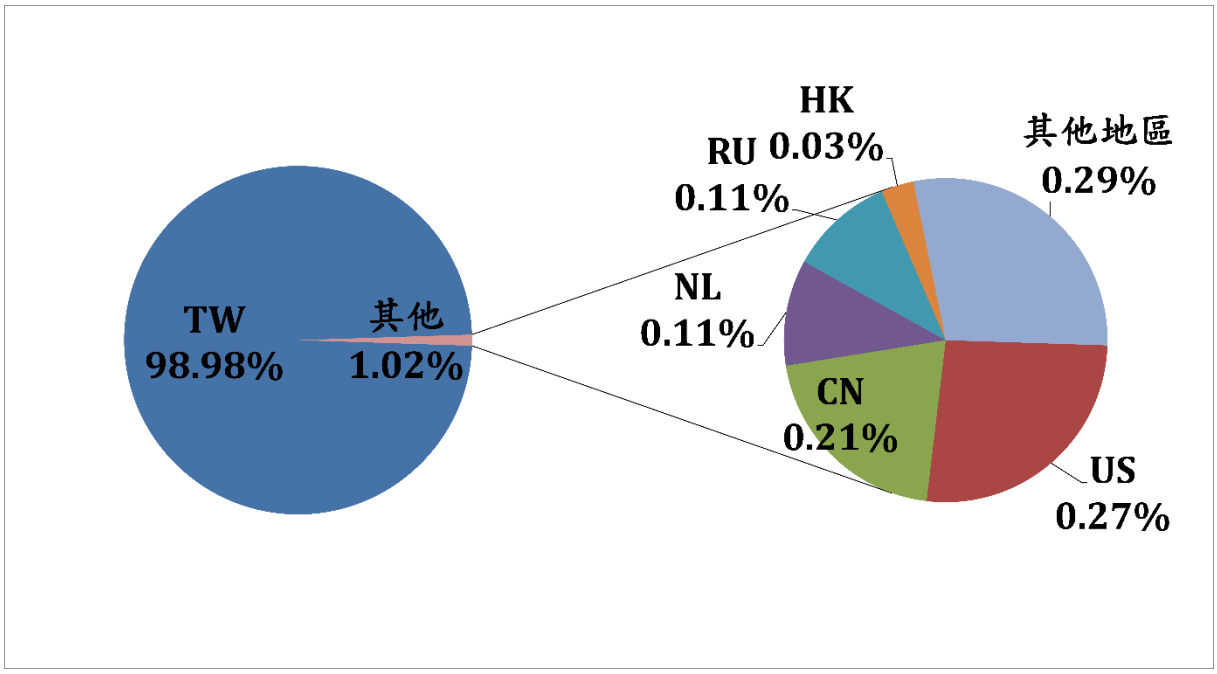


圖 1、分享地區統計圖

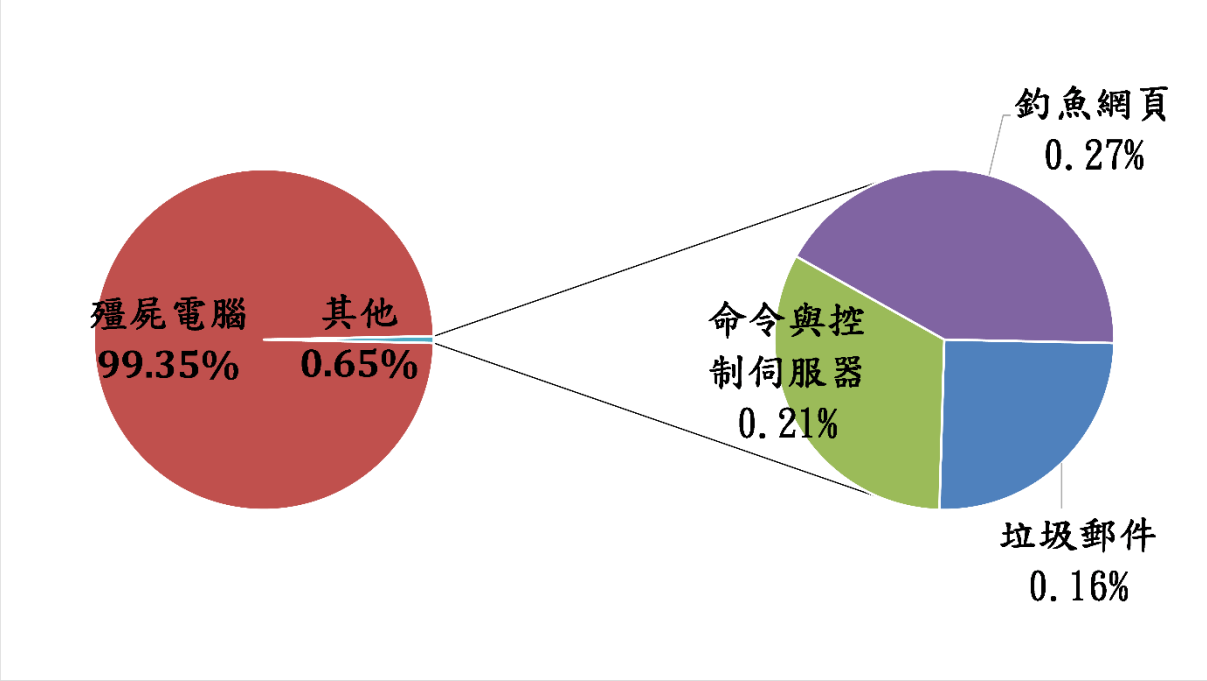


圖 2、分享類型統計圖

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：**2020 年 9 月 10 日**

編輯：**林克容、江奕昉、洪彩馨**

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**