TWCERT/CC 資安情資電子報

2020 年 1 月份

目錄

第 1 章、 封面故事

Microsoft PowerPoint 2010、2013、2016 存有遠端執行任意程式碼漏洞

近來被發現的 Microsoft PowerPoint 遠端執行任意程式碼漏洞，嚴重程度被評級為「重要級」；因這些漏洞可能讓成功入侵 Windows 裝置的駭侵者可遠端執行任意程式碼。

漏洞主要的成因，是由於 Power Point 無法正確處理記憶體中的物件；駭侵者可取得與目前登入使用者相同的權限；若登入用戶為系統管理員權限，駭侵者即可控制整個系統。

微軟已在本月（2019 年 12 月）發行的 Microsoft Office 安全更新中修補了這些漏洞，用戶只要盡速更新至最新版本即可。

同一個軟體更新包中，也同時解決了存在於 Office 系列其他軟體的安全漏洞，例如 CVE-2019-1461、CVE-2019-1400、CVE-2019-1463、CVE-2019-1464 等。這些安全漏洞均和服務阻斷攻擊（DoS）有關。

- CVE 編號：CVE-2019-1462
- 影響產品(版本)： Microsoft PowerPoint 2010、2013、2016
- 解決方案：將 Microsoft Office 盡速更新至最新版本。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1462

2. https://www.bleepingcomputer.com/news/microsoft/microsoft-office-december-security-updates-fix-remote-execution-bugs/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、MS Office 是全球最常被駭侵攻擊的應用軟體

資安廠商的統計資料指出，全球所有針對應用軟體漏洞的駭侵攻擊事件中，有超過七成是攻擊 MS Office。

資安廠商 PreciseSecurity.com 指出，在今年第三季全球所有針對應用軟體漏洞發動的攻擊行動，有 72.85%都是鎖定 MS Office。而在 MS Office 中最常被用來發動攻擊的漏洞，則是存在於數學式編輯器應用程式。

其餘常受攻擊的應用軟體與比例如下：

- 瀏覽器：13.47%
- Android 作業系統：9.09%
- Java：2.34%
- Adobe Flash：1.57%
- PDF：0.66%

該公司的統計數字也指出，在 2019 年第三季，網頁中包括惡意軟體的來源國家，排名與比例如下：

美國：79.16%

荷蘭：15.58%

德國：2.35%

法國：1.85%

俄羅斯：1.05%

- 資料來源：

1. https://www.precisesecurity.com/articles/ms-office-represents-73-of-the-most-commonly-exploited-applications-worldwide/

2.1.2、大品牌特別容易在購物狂潮時遭詐騙駭侵冒用

資安專家指出，在「黑色星期五」之類的網路購物熱潮期間，也是駭侵者假冒大品牌名義進行詐騙攻擊的高峰，尤其是知名大品牌特別容易被假冒。

資安廠商 ZeroFOX 指出，在「黑色星期五」與「網購星期一」這類網購熱潮期間，原本就是駭侵攻擊大行其道的高峰；今年他們更觀察到各種詐騙手法的升級，包括透過社群平台散布詐騙釣魚連結，或是透過假冒 Domain 架設釣魚網站，企圖騙取受害者的付款資訊。

用來詐騙用戶上鉤的假網站或假訊息，通常會以大品牌知名商品為餌，以超乎想像的優惠作為招徠；據統計，最常被假冒的品牌排行如下：

Apple：33.8%

Amazon：12.7%

Target：9.9%

Tiffany：6.4%

Sony：6.1%

Samsung：5.3%

Microsoft：5.2%

Hermés：3.9%

Xbox：3.8%

GoPro：2.9%

- 資料來源：

1. https://threatpost.com/black-friday-shoppers-scams-fake-domains/150593/

2.1.3、資安廠商指出，日本是發送 Emotet 勒贖釣魚信最多的國家

資安廠商 Proofpring 發表研究報告指出，近來在全球各地造成嚴重災情的勒贖軟體 Emotet，最多的釣魚信發送來源國是日本。

在 Proofprint 的報告中，列出了 12 大 Emotet 釣魚郵件的發送國 TLD，依序如下：

- 日本
- 德國
- 義大利
- 阿拉伯聯合大公國
- 澳洲
- 英國
- 瑞士
- 歐盟
- 美國
- 奧地利
- 加拿大
- 新加坡

Emotet 曾在 2018 年造成相當嚴重的災情，包括竊取受害者的銀行金融相關資訊、竊取用戶電郵憑證和瀏覽器儲存的密碼，甚至也能用來發動 DDoS 攻擊；今年 Emotet 又再度大舉流行。

- 資料來源：

1. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more
2. https://www.proofpoint.com/us/corporate-blog/post/emotet-wishes-you-merry-christmas-greta-thunberg

3. https://www.bleepingcomputer.com/news/security/emotet-malware-uses-greta-thunberg-demonstration-invites-as-lure/

2.2、國際政府組織資安資訊

2.2.1、全新駭侵行動，意圖竊取各國政府機關重要系統登入資訊

資安廠商 Anomali 的研究人員，日前觀察到一個全新的大規模駭侵攻擊活動，目標鎖定全球各國政府機關與其供應商，透過釣魚郵件騙取重要系統的登入資訊。

Anomali 指出，受到駭侵攻擊的目標至少有 22 個，包括美國、加拿大、中國、澳洲、瑞典等國家的政府與民間企業。釣魚郵件中都包含詐騙連結，意圖騙取受害者登入系統所需的帳號密碼。

Anomali 表示，這起駭侵行動是長期的活動，目前尚不清楚駭侵者的背景，也不知其最終目的，但很可能是為了進行間諜監視。

目前已知整起行動中，最大量的攻擊目標是美國能源部、美國商務部與美國退伍軍人事務部等單位。

另外值得注意的是，駭侵者除了會針對不同國家的目標，以其當地語言撰寫詐騙內容外，針對有採購需求的特定目標，還會以量身訂做的採購相關文件進行詐騙。

- 攻擊手法：釣魚郵件
- 關鍵字：Phishing mail, credentials
- 資料來源：

1. https://www.anomali.com/resources/whitepapers/phishing-campaign-targets-login-credentials-of-multiple-us-international-government-procurement-services

2. https://www.zdnet.com/article/cybersecurity-this-password-stealing-hacking-campaign-is-targeting-governments-around-the-world/

2.2.2、「江南工業風」：研究人員發現針對南韓等亞洲國家製造業的駭侵行動

資安廠商 CyberX 的研究團隊，日前發現針對南韓等亞洲國家製造業大廠進行的大規模駭侵攻擊行動，受害廠商有近 60% 都是南韓製造業者；其他的受害者分布在泰國、中國、印尼、土耳其、厄瓜多、德國與英國。

CyberX 指出，這個駭侵行動多以詢價的釣魚郵件為攻擊的起點，受害的廠商會接到在捷克或印尼等國興建電廠的詢價單，但郵件的 PDF 夾檔中藏有惡意軟體。一旦惡意軟體成功侵入系統，便會關閉 Windows 防火牆，並開始收集各種 Email 和瀏覽器密碼，再把這些登入資訊上傳到某個伺服器。

受害廠商中有 52% 屬大型製造業。由於超過一半都是南韓工業廠商，CyberX 便稱此攻擊行動為「江南工業風」（Gangnam Industrial Style）。進行惡意攻擊的目的，據推測是要竊取各大公司的機密，包括產品設計、製程、合約等商業機密或新技術。

據信這個駭侵行動與某個 APT 團體有關，但目前未能具體掌握是哪個 APT 駭侵團體、背後有無國家支持。

- 攻擊手法：利用釣魚郵件植入惡意軟體
- 關鍵字：Phishing, Spear Malware, South Korea, APT

- 資料來源：
  1. https://cyberx-labs.com/blog/gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies/
  2. https://www.bleepingcomputer.com/news/security/industrial-cyber-espionage-campaign-targets-hundreds-of-companies/

2.2.3、北韓駭侵印度核能電廠，目的為竊取放射性釷核能科技

日前位於印度 Tami Nadu 的核能電廠遭到北韓駭侵攻擊；資安專家認為，北韓駭侵核電廠的目的，是為了竊取印度自主開發的放射性釷發電技術。

資安專家指出，攻擊行動來自由北韓支持的 Lazarus 駭侵團體，利用一個稱為「Dtrack」的惡意軟體，透過釣魚郵件植入電廠的 Email 系統之中。

釣魚郵件偽裝成由印度核能監管單位和核能研究中心所發；雖然美國核能委員會認為攻擊行動並未影響電廠的發電控制系統，但印度國家資安中心的專家，認為攻擊者可能已經取得高階目標的存取權限，目的在於竊取由印度自主開發的放射性釷發電技術。

相較於全球核電廠普遍用以發電的放射性鈾，放射性釷不論在安全性、經濟性上，都比鈾更為優越；印度計畫在 2050 年時，透過放射性釷產生的電力，將佔印度全國電力需求的 30%。

全球只有少數以釷發電的核能電廠，資安專家認為這可能是該電廠遭北韓駭侵的主因。

- 資料來源：
  1. https://www.ibtimes.com/north-korea-hackers-breached-indian-nuke-reactor-search-advanced-thorium-technology-2878052

2.2.4、越南駭侵團體 APT32 駭入 BMW、現代車廠

德國媒體報導，世界最大車廠 BMW 與現代，疑似遭到越南支持的駭侵團體 APT32 的駭侵攻擊。

據報導，攻擊發生在今年春季；駭侵者在兩家車廠內網中的弱點電腦內植入稱為「Cobalt Strike」的駭侵用測試工具，以此為後門進入車廠的內部網路。

據指出，BMW 發現駭侵行為後，就開始追蹤駭侵者在內網的一舉一動，直到上周末才完全切斷駭侵者的存取權限。

BMW 和現代汽車都沒有對報導發表任何評論，但 APT32 過去已有多次針對大型汽車製造業者發動攻擊的記錄，過去的受害者包括 Toyota 的澳洲、日本和越南分支機構。

資安專家認為，支持 APT32 的越南政府，想要竊取這些大型汽車公司的特有技術與智慧財產，用以扶植越南國營的本土汽車產業。中國過去也曾運用這種手法支持其航太工業。

- 攻擊手法：駭侵者在兩家車廠內網中的弱點電腦內植入稱為「Cobalt Strike」的駭侵用測試工具，以此為後門進入車廠的內部網路。
- 關鍵字：APT32、BMW、Hyundai、Cobalt Strike
- 資料來源：
  1. https://www.br.de/nachrichten/wirtschaft/fr-autoindustrie-im-visier-von-hackern-bmw-ausgespaeht,RjnLkD4

2. https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

2.2.5、為防惡意軟體攻擊，德國法蘭克福預警性關閉市政系統

為防範惡意軟體 Emotet 肆虐，德國法蘭克福市政當局於上周預警性關閉市政系統，以遏止攻擊的蔓延，造成更大災情。

最近德國法蘭克福市政系統偵測到 Emotet 勒贖軟體的入侵，且有愈演愈烈之勢；為避免災情進一步擴大，法蘭克福市府決定預警性關閉幾乎所有市政系統，以避免災情擴大。

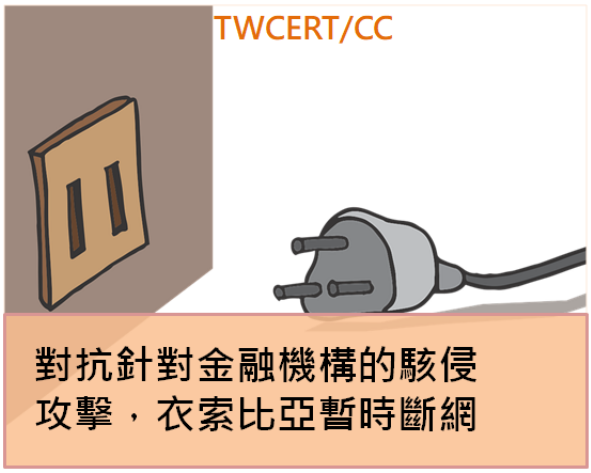
法蘭克福是近來第四個因為 Emotet 而關閉系統的德國機關；之前還有位在基森的尤斯突斯利比克大學、巴特洪堡市、福萊堡天主教大學等三個機關，也因為 Emotet 而關閉系統。

德國中央政府資安主管機關 BSI 指出，雖然關閉市政系統必然造成各種不便與損失，但和 Emotet 可能帶來的災情相比仍屬輕微；該局建議所有可能面臨 Emotet 勒贖攻擊的單位，都要準備採取因應措施，及時關閉可能受損的系統。

法蘭克福是歐洲中央銀行所在地，也是全球主要金融中心之一。

- 資料來源
  1. https://twitter.com/GossiTheDog/status/1207741172812255235
  2. https://www.zdnet.com/article/frankfurt-shuts-down-it-network-following-emotet-infection/

2.2.6、對抗針對金融機構的駭侵攻擊，衣索比亞暫時斷網



依索比亞近來遭到針對該國金融機構的大規模駭侵攻擊；為抵擋該攻擊，衣索比亞祭出斷網手段。

衣索比亞網路安全中心表示，由於斷網措施得宜，該次攻擊行動並未得逞。

根據衣國國營廣播電台的報導，這次斷網為時約 20 分鐘；但報導中並未揭露是哪一家金融機構遭到駭侵攻擊，也未透露具體的攻擊手法與受損情形。

不過根據衣國網路安全緊急應變中心（Ethio-CERT）表示，該攻擊在還沒有造成嚴重破壞之前，便因斷網措施而成功攔阻其攻擊行動。

愈來愈多政府以斷網來應對各種攻擊或政治問題，曾採用斷網手段的國家，主要都是極權統治國，包括委內瑞拉、蘇丹、印尼、斯里蘭卡、衣索比亞，剛果民主共和國等國。剛果民主共和國甚至曾經全國斷網長達 20 天之久。

- 關鍵字：cyberattack, internet shutdown, disconnection
- 資料來源：
  1. https://borkena.com/2019/12/05/ethiopia-briefly-shut-internet-as-a-cyber-attack-hits/
  2. https://www.datacenterdynamics.com/analysis/great-disconnect/

2.3、社群媒體資安近況

藏有惡意程式之 PDFReader，竊取使用者 Facebook 金融及廣告資訊

近日發現有駭客透過含有惡意程式的 PDFReader 應用程式，竊取使用者 Facebook Ads Manager 以及 Amazon 的相關資訊，包含使用者的金融資訊、聯絡資訊、廣告發佈對象等，作為惡意行為之用。

日前，資安團隊 Malware Hunter Team 發佈了一項資訊，指有駭客試圖透過惡意程式竊取使用者社群媒體的資料。首先，駭客製作了一款功能性高的 PDF 軟體「PDFReader」，並透過各種方式讓受害者連入該網站後下載安裝。然而，該軟體卻有木馬程式藏於其中，因此只要使用者進行安裝，該主機便會被木馬程式入侵，與駭客主機連線，接受駭客的指令和操縱。

而駭客在成功透過應用程式入侵後，會竊取使用者瀏覽器中 Facebook 的 Cookie 資料，並透過竊取到的使用者帳號密碼登入，觀察使用者使用 Facebook 中發佈廣告的 Ads Manager 系統的使用狀況。由於該系統主要為使用者付費以發佈相關廣告給特定群體，因此使用者便可透過該系統取得使用者付費時的信用卡資訊、金融資訊，以及發佈的對象、群體等，作為後續獲得不法利益之用。

儘管在這件駭侵行為中，由於駭客開發之惡意 PDFReader 軟體除了功能強大且免付費之外，更因為該惡意程式具有合法的憑證，因此讓使用者

得以信任並下載該軟體，但在經過針對該軟體之.exe 檔案解析後，證實了其中的木馬程式，以及其竊取瀏覽器 Cookie 資訊等行為。然而，該駭侵行為在被發覺後，並未停止其攻擊行為，反而將其網站位址更動，以及將其程式進行版本之更新，企圖避過資安組織及檢測系統的偵測及阻擋，以進行更多的攻擊及獲取更多的資訊。

TWCERT/CC 在收到該資訊後，已立即進行了相關通報作業，希望能藉此提升企業或組織的相關警覺。並且在此提醒使用者請勿隨意點擊下載或執行來源不明的檔案或軟體，必須清楚確認開發單位的正確性及安全性以避免成為駭客惡意程式下之受害者。此外，同時也應使用防毒軟體等進行定期性的掃描，以及作業系統或相關軟體的版本更新，以配合廠商修補可能的資安弱點。並且盡量能在收到與自身可能相關之資安資訊後，立即針對自身主機進行檢查，例如是否有不明檔案存在或是否有異常之連線狀況等，方能將損失降至最低，以及提升資安之防護能量。

- 參考資料：

1. https://twitter.com/malwrhunterteam/status/1201552349715673088
2. https://www.bleepingcomputer.com/news/security/facebook-ads-manager-targeted-by-new-info-stealing-trojan/

2.4、行動裝置資安訊息

2.4.1、美國聯邦調查局提出警訊：在外旅遊時勿使用免費 Wi-Fi 服務

美國聯邦調查局在其官方 Twitter 上發布警訊，建議在接下來的耶誕假期中返鄉團圓的旅人，避免在旅途中使用免費的 Wi-Fi 服務，以避免成為駭侵目標。

美國耶誕假期將至，大量返鄉渡假人潮，會在車站、機場、飯店等各種公共場所使用免費 Wi-Fi 連線；而這可能成為駭侵者的最佳目標。

FBI 指出，若將個人的電腦、手機、平板等裝置連上免費無線網路熱點，就等於開門揖盜；駭侵者很容易通過免費網路，將惡意軟體植入你的裝置，並竊取登入資訊、密碼，甚至遠端遙控你的裝置。

FBI 建議在透過免費無線網路連線時，應該使用安全的 VPN，避免網路封包遭駭客攔截竊聽；FBI 也建議用戶在出外旅行時，關閉裝置上的所在地偵測功能，也不要打卡分享自己的位置，以免讓歹徒知道自己出門在外，甚至預測你的動向。

- 資料來源：
  1. https://twitter.com/FBI/status/1041840500473581568
  2. https://www.bleepingcomputer.com/news/security/fbi-warns-of-risks-behind-using-free-wifi-while-traveling/

2.4.2、紐約時報揭露手機位置資訊販售案，包含 1200 萬支手機用戶座標資訊

紐約時報發表調查報導，揭露以販賣用戶手機所在地座標資料的真實狀況；資料包括 1200 萬名美國手機用戶，於 2016 年到 2017 年間，在 500 億個特定地點之間移動、停留的活動資訊，而這些都成為業者用以牟利的出售標的。

據報導指出，在美國有許多小型業者合法從事用戶手機所在地活動資訊的收集活動，並將這些用戶活動資訊出售給有需要的業者，如公關、行銷、廣告、消費產品、甚至政治團體。

紐約時報說，這些業者透過各種各樣的手機 App，每天 24 小時監控並回傳用戶所在地的資訊；雖然業者強調這些資訊都經去識別化，但專家指出仍然可以拼湊並分析這些資料，找出某個特定用戶經常造訪的地點清單，甚至能以此得出資訊所有人的真實身分。

為破解業者的說法，紐時也成功分析出數名影響力人士的行蹤，包括某軍事將領在沒有維安人員隨行的下班回家動線、某法律高官送小孩上學、某知名大律師與其客戶搭乘私人飛機度假的所有行程等。

最值得注意的是，多數用戶對於自己行蹤被監控是渾然不覺的，而且也不知道是被哪一支 App 所監控。

- 資料來源：
  1. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

2.4.3、專家展示利用 AirDrop 對周遭 iPhone、iPad 進行 DoS 攻擊的方法

資安專家展示利用 iOS Bug，透過 AirDrop 功能，對周遭 iPhone、iPad 進行 DoS 攻擊的方法；被攻擊的手機將暫時無法操作。

獨立資安專家 Kishan Bagaria 發表專文，指出利用 iOS 系統 bug，透過 iOS 內建的 AirDrop 無線檔案傳輸功能，對攻擊者周遭的 iPhone、iPad 等 iOS 裝置發動 DoS 攻擊的方法。

該攻擊法稱為「AirDoS」，只要用一行指令，就能針對周遭數公尺內的 iOS 裝置持續大量發送 AirDrop 連線要求；遭攻擊的用戶，其裝置的介面會持續出現 AirDrop 連線要求的通知視窗，即使同意或拒絕，也會再次出現，這導致用戶將無法使用其裝置。

避免攻擊的方法也很簡單，只要移動到較遠的距離，讓攻擊要求無法透過 AirDrop 連線即可。另外，將 AirDrop 設定為「只限連絡人」而非「所有人」，也可以降低遭到 AirDos 攻擊的風險。

該專家於 2019 年 8 月向 Apple 通報此一問題，Apple 隨即回應即將展開調查，並已於 iOS 13.3 中更正這個錯誤。iPhone 與 iPad 用戶應盡快更新至最新 iOS 版本。

- 資料來源：
  1. https://kishanbagaria.com/airdos/

2.4.4、超過一百種 Android App 內含詐騙廣告，少數仍在 Play Store 架上

資安廠商 White Ops 發表研究報告，指出有超過 100 種以上 Android App 內含詐騙廣告機制，會在用戶手機上顯示各種詐騙廣告，或在背景進行詐騙廣告點擊，以詐取廣告點擊佣金。

White Ops 指出，這一百多個 Android App 都內含兩個分別稱為「Soraka」和「Sogo」的惡意廣告程式庫，以及一個稱為 AppsFlyer 的行銷分析套件；透過這三個元件，惡意廣告將可在用戶不知情的狀況下不斷顯示並製造假點擊。

據指出，這些詐騙廣告 App 的總下載量超過 460 萬次，多半藏身於用戶最喜歡的幾種應用類型，例如算命、戲、美拍或系統最佳化工具等。

這類詐騙廣告點擊，除了讓用戶的手機可能面臨更多資安風險外，也詐取大筆廣告抽佣。今年二月美國司法部門起訴某個廣告詐騙網，指出該詐騙行動於一年之間騙取的廣告佣金高達三千萬美元，受害裝置數多達 170 萬台。

White Ops 的報告中詳述了這些詐騙 App 的運作流程。

- 資料來源：
  1. https://www.whiteops.com/blog/bringing-starchild-down-to-earth-soraka-sdk
  2. https://www.cyberscoop.com/play-store-adware-white-ops/

2.5、軟體系統資安議題

2.5.1、美國新奧爾良市遭勒贖軟體攻擊，市長宣布該市進入緊急狀態

美國新奧爾良市上周遭勒贖軟體大規模攻擊，多項市政運作停擺；市長 LaToya Cantrell 隨即於上周五發布命令，新奧爾良市進入緊急狀態。

該勒贖攻擊係透過釣魚郵件發動，新奧爾良市在上周五上午五點左右偵測到攻擊行動，隨即召開記者會公告周知；上午 11 時左右，該市的資訊部門發現更大規模的攻擊行動，隨即關閉多項市政系統與伺服器，以控制受損範圍與程度。

新奧爾良市表示，雖然偵測到勒贖攻擊，但並未接獲具體的贖金要求；目前也未有政府僱員的個資外洩情形發生。

新奧爾良市政府已會同路易斯安那州、FBI 與各情治單位展開調查。

- 攻擊手法：透過釣魚郵件進行勒贖攻擊
- 關鍵字：New Orleans, Phishing, Ransomware, Louisiana
- 資料來源：
  1. https://twitter.com/nolaready/status/1205611902627397640?s=20
  2. https://edition.cnn.com/2019/12/13/us/new-orleans-cyberattack-state-of-emergency

2.5.2、資安專家發現網頁上的明星圖像資料中暗藏挖礦機器人程式碼

英國資安廠商 Sophos 的資安專家，發現一個稱為 MyKingz 的加密貨幣挖礦機器人的最新散布手法，係將惡意軟體程式碼夾藏到流行歌曲明星 Tylor Swift 的網路相片中。

Sophos 的專家指出，這種透過影像或聲音檔案夾帶惡意程式碼的手法，其實先前早已出現過；透過這種方法「偷渡」，往往能夠有效逃避系統防毒防駭機制的檢查，成功入侵受害者的電腦。

專家也指出，這個 case 的重點並不在於用了誰的相片，而是惡意軟體總會用盡各種手段企圖入侵。特別是近兩年來 MyKingz 對 Windows 系統的為害甚大，特別是沒有定期更新修補漏洞的 Windows 主機。

據估計，MyKingZ 幕後的主使者，每日因為挖礦所得到的不法利益約在 300 美元；自 MyKingZ 開始流行至今的不法利益，高達 300 萬美元以上。

- 資料來源：
  1. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-mykings-report.pdf

2.5.3、數十萬張美國手機用戶帳單曝露在網路上，全無保護

英國資安廠商近期發現 AWS 上的一個未保護檔案庫，內含數十萬張美國各電信服務商的用戶帳單，而且未經任何保護。

據英國資安廠商 Fidus Information Security 指出，該公司發現的手機帳單檔案庫，內含 261,300 個手機帳單文件檔案，帳單日期最早可追溯自 2015 年。

這些帳單內含的個資包括用戶姓名、帳單地址、手機號碼；多數帳單上還包括通聯記錄列表；檔案庫中甚至還有若干更加敏感的個資，例如含有用戶登入資訊、金融密碼的網路銀行頁面擷圖等。

這些帳單是由美國電信業者 Sprint 的外包廠商外洩出去。用戶自其他電信業者轉換至 Sprint 時，會提供過往的帳單給 Sprint，以取得轉換費用的補償。Sprint 說，該公司約聘人員誤將這些檔案放上 AWS。

在 Fidus Information Security 通報 Amazon 後，這個檔案庫立即就下線了；但目前無法得知檔案庫曝露在網路上有多久，也不知道是否已有資料遭人下載利用。

- 資料來源：
  1. https://techcrunch.com/2019/12/04/sprint-contractor-cell-phone-bills-exposed/

2.5.4、近日發現「網路巨砲」，針對香港線上論壇發動 DDoS 攻擊

AT&T 資安研究中心指出，該單位觀察到的「網路巨砲」（Great Cannon）DDoS 攻擊，目標鎖定論壇網站 LIHKG.com。

AT&T 觀察到的攻擊行動，自 8 月 31 日開始，一直持續到 11 月 27 日；而根據 LIHKG.com 的記錄，在八月的攻擊行動中，該站每小時收到超過 15 億次存取要求；而該站在正常情形下的存取要求次數僅為每小時 650 萬次。

據 AT&T 的報告指出，「網路巨砲」是將惡意程式碼植入於眾多中國境內的網站伺服器中，以構成龐大的僵屍網路；發動攻擊時，這些惡意程式碼會攔截用戶正常的網路連線，轉而導向特定目標發動 DDoS 攻擊。

過去中國的「網路巨砲」DDoS 機制也曾多次發動，例如 2015 年時曾用以攻擊 Github.com 和 Greatfire.com、2017 年用以攻擊明鏡新聞。

AT&T 的報告中詳述了他們觀察到的攻擊手法與流程。

- 攻擊手法：於中國境內的多個網頁伺服器中注入僵屍網路惡意程式，攔截用戶流量並導向攻擊目標，進行 DDoS 攻擊。
- 關鍵字：Great Cannon, DDoS
- 資料來源：
  1. https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again
  2. https://www.bleepingcomputer.com/news/security/the-great-cannon-ddos-tool-used-against-hong-kong-protestors-forum/
  3. https://www.zdnet.com/article/china-resurrects-great-cannon-for-ddos-attacks-on-hong-kong-forum/
  4. https://zh.wikipedia.org/wiki/ 大炮_(网络攻击工具)

2.5.5、資安專家發現中國電商公司 1.3TB 顧客資料庫外洩

資安廠商 vpnMentor 的研究人員發現中國電商公司蘭亭集勢的一個顧客資料庫發生資料外洩事件，受外洩影響的顧客遍及全球。

研究人員指出，這個外洩的資料庫，檔案大小高達 1.3TB，內含超過 15 億筆資料，其中包括部分顧客個資，包括用戶的 IP 位址、所在國家、Email 地址、用戶在該網站上的使用記錄等等。

vpnMentor 也指出，這個外洩的資料庫屬於 Elasticsearch 資料庫，並沒有加上任何加密或密碼保護，任何人只要知道存取方法，皆可取得內部的資料。

資安專家指出，這些資料的外洩，可能導致受害者收到假冒蘭亭集勢的釣魚信件，進一步提高資安風險。

vpnMentor 於今年十一月下旬發現這起事件後，隨即通報蘭亭集勢；蘭亭集勢沒有任何回應或說明，但於通報當天就關閉了該資料庫。

- 資料來源：
  1. https://www.vpnmentor.com/blog/report-lightinthebox-leak/

2.5.6、勒贖軟體 Emotet 假借瑞典環保女孩或耶誕節之名散布釣魚郵件

資安廠商 Proofprint 發表駭侵觀測報告，指出全球目前正遭到 Emotet 勒贖軟體的全面襲擊；目前的攻擊手法，係透過假冒瑞典知名環保運動女孩 Greta Thunberg 或是耶誕節祝賀信名義發送的釣魚郵件。

在假冒 Greta Thunberg 的釣魚郵件中，內文希望收件者能參加由她發起的全球抗議遊行活動，時間和地點放在郵件夾檔的 .docx 檔案；但此檔案就夾藏有 Emotet 勒贖軟體。

Emotet 是最近為害甚大的勒贖軟體，在 Proofprint 的統計中，2019 年第三季的全球釣魚郵件攻擊中，Emote t 就佔了 12%。

這波假冒 Greta Thunberg 的釣魚信，目前發現會以英文、西班牙文、法文、波蘭文和義大利文等國語言發送。

- 攻擊手法：假冒名人或賀電，於夾檔中發送惡意軟體
- 關鍵字：Emotet, Malware, Phising Mail
- 資料來源：
  1. https://www.proofpoint.com/us/corporate-blog/post/emotet-wishes-you-merry-christmas-greta-thunberg
  2. https://www.bleepingcomputer.com/news/security/emotet-malware-uses-greta-thunberg-demonstration-invites-as-lure/

2.5.7、 Cisco 指控 Zoom Connector for Cisco 會造成嚴重資安漏洞

網通大廠 Cisco 發布公告指出，使用率相當高的視訊會議廠商 Zoom 推出的 Zoom Connector for Cisco，可能讓任何人透過 Internet 存取 Cisco 網通產品的 web 管理界面，甚至可以跳過身分認證關卡。

資安專家在分析 Zoom Connector for Cisco 後指出，Zoom 為了讓建置 Cisco 視訊會議裝置的用戶，也能透過這些裝置來快速撥入 Zoom 的視訊會議服務，因而透過安裝在企業內網 Windows Server 上的 Zoom Connector for Cisco 擔任中界者，透過這台伺服器設定 Cisco 裝置的 Web 界面，接通會議連線要求。

然而由於 Zoom 視訊會議的連結並不做任何身分認證即可連線，因此造成駭侵者可以透過 Zoom Connector for Cisco 連入 Cisco 裝置的 Web 界面，進一步控制 Cisco 裝置，甚至進行駭侵攻擊。

同樣會被 Zoom Connector for Cisco 漏洞控制的網通廠商還包括 Poly 和 Lifesize。Cisco 在聲明中表示 Zoom Connector for Cisco 並非 Cisco 官方支援的解決方案；Cisco 呼籲有使用 Zoom Connector for Cisco 的用戶，務必檢查連線 log 是否有異常。

- 資料來源：
  1. https://blogs.cisco.com/collaboration/our-focus-on-security-in-an-open-collaboration-world
  2. https://www.nojitter.com/video-collaboration-av/zoom-gives-way-video-device-security-breach-again

第 3 章、 資安研討會及活動

資安所 2020 研發策略分享會	
活動時間	**2020-01-13(一) 9:00~16:00**
活動地點	**科技服務大樓 14 樓創新廳 台北市松山區民生東路四段 133 號**
活動網站	http://surl.twcert.org.tw/frbaB
活動概要	CSTI 資安科技研究所 CyberSecurity Technology Institute 資策會資安所致力成為台灣資安產業的 Virtual R&D 資安共創(Cybersecurity Foundry)團隊，深化核心技術，推動產業發展，本次活動針對 2020 年資安所研發計畫: AI、5G、物聯網、工控、資安人培等進行公開報告，並邀請產學研專家共同交流，為計畫合作提供媒合平台，達到佈局科專研發，升級產業資安，創造新創事業，試煉實際場域，爭取國際標案，一同攜手推進台灣資安產業。

Kali 讀書會 資安小聚	
活動時間	**2020/01/17(五) 19:00 ~ 21:00**
活動地點	**天瓏 CodingSpace / 台北市中正區重慶南路一段 105 號**
活動網站	**https://kaliworkshop.kktix.cc/events/c0dd5249**
活動概要	 資策會資安所致力成為台灣資安產業的 Virtual R&D 資安共創(Cybersecurity Foundry)團隊，深化核心技術，推動產業發展，本次活動針對 2020 年資安所研發計畫: AI、5G、物聯網、工控、資安人培等進行公開報告，並邀請產學研專家共同交流，為計畫合作提供媒合平台，達到佈局科專研發，升級產業資安，創造新創事業，試煉實際場域，爭取國際標案，一同攜手推進台灣資安產業。

COMPTIA SECURITY+ 國際網路資安認證班	
活動時間	**2/8(六)、2/9(日)、2/15 (六)、2/16(日)，每日 9:00～12:30、13:30～17:30**
活動地點	**資策會 數位教育研究所**
活動網站	**https://www.twcert.org.tw/tw/cp-105-3200-9f58f-1.html**
活動概要	 CompTIA Security+已連續 3 年列為 CertCities.com 公佈 IT 業 10 大熱門證照排行榜的前 10 名，是目前國際上最為普及與非廠商導向之資訊安全證照。本課程將學習資訊安全中之基礎技術及核心概念，讓學員在資安領域下對於廠商的解決方案有更詳盡的認知。 CompTIA Security+ 考試已於 2017 年底全面改版為最新的「SY0-501」版本，本課程亦已針對新版的考試內容做調整，將考試內容彙整至上課教材中，目標是協助學員考取最新版的 CompTIA Security+ 國際認證。

容器安全實作坊	
活動時間	**2020/2/16 (日) 9:30~12:30 / 13:30~16:30**
活動地點	**台北市中山區松江路 131 號(2 樓教室)**
活動網站	**https://broadmission.kktix.cc/events/container-security0216**
活動概要	 Container 容器技術成為開發與運行雲端應用服務的主流方式，而 Security 這一塊從去年開始逐漸受到重視，不管是在官方本身或是第三方廠商都開始投入越來越多的資源來積極搶佔這塊市場；而要如何讓 Security 像是基因一般嵌合在運行的雲端服務當中？這就是此次實戰工作坊希望達成的目標，講師將分享從開發到營運各個階段可能會遇到的問題，以及如何運用各種解決方案來排除，試圖從藍隊 Blue Team 的角度來確保使用 Container 應用服務的安全性，並動手實作，高手傾囊相授、內容精彩。

2 月例會_連網設備的資安風險與信任管理策略	
活動時間	**2020/2/25(二)，下午 2:00～5:00**
活動地點	**新竹市光復中學-國中部東側教學大樓推廣中心 第一演講廳**
活動網站	**https://www.caa.org.tw/coursedetail-3272.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 演講大綱： 1.當今環境的資安風險與挑戰 2.傳統資安工具 vs 內稽內控的挑戰 3.業界公認資安指南與資安框架建議的做法 主講講師： 姓名：張恩綾 機構：美商 Forescout Technology 職稱：台灣區總經理 證照：ITIL Foundation、Cybersecurity and Its ten Domain 適合對象：本協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：本會會員(含團體會員公司同仁)免費，非會員 500 元

2 月例會_以 ISO 27701 標準為框架建立在既有資訊安全管理系統中架構之個人隱私管理系統	
活動時間	**2020/2/27(四)，下午 2:00～5:00**
活動地點	**台北市信義區基隆路一段 143 號 3 樓**
活動網站	**https://www.caa.org.tw/coursedetail-3279.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 演講大綱： 1.ISO/ IEC 27701 隱私資訊管理系統標準緣由 2.與 ISO/ IEC 27001 相關的 PIMS 特定要求介紹 3.與 ISO/ IEC 27002 相關的 PIMS 特定指引簡介 4.控制者與處理者的隱私管理強制要求說明 主講講師： 姓名：章鈺 機構：BSI 英國標準協會台灣分公司 單位：驗證部門 職稱：產品經理 證照：CISA、CISM、CGEIT、CRISC 專長：資訊安全檢測、滲透測試、數位鑑識、個資保護 適合對象：本協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：本會會員(含團體會員公司同仁)免費，非會員 500 元

CYBERSEC 2020 臺灣資安大會	
活動時間	**2020 / 3 / 17 – 2020 / 3/ 19　10:00 – 17:30**
活動地點	**台北市南港區經貿二路 2 號 (南港展覽二館)**
活動網站	**https://signupcybersec.ithome.com.tw/attendee**
活動概要	 CYBERSEC 2020 臺灣資安大會為臺灣規模最大、議程面向最完整的資訊安全專業會議。三整天近 200 場研討會與論壇，涵蓋最新技術與產品發表、企業日常實 務操作、特定產業的資安挑戰，以及資安長圓桌會議等內容。 以「MAKE IT SAFER 持續改善 · 全面強化」為主題 鼓舞您我合力建構更有保障的未來。當資安威脅已成常態，我們被迫要習慣 ─ 今日的異常，便是明天的日常。唯有正視資安危機，共同捲起袖子，持續改善，全面強化，終有扳回優勢的一天。

人工智慧拼資安升級實作班	
活動時間	**2020 年 5/4 (一)、5/5(二)，每日 9:30-16:30**
活動地點	**資策會 數位教育研究所**
活動網站	**https://www.iiiedu.org.tw/aiis/**
活動概要	 為了滿足業界需求，本單位特規劃「人工智慧拼資安升級實作班」課程，期盼透過講師的精闢解說或經驗分享，協助學員提升對人工智慧資訊安全的專業知識與能力。另外，搭配人工智慧在應用上之個案分析或討論 (包含物聯網、自動駕駛、以及機器人與智慧製造)，讓學員可以練習或實作人工智慧資訊安全的策略或因應措施。期盼學員在完成課程後，未來具備適當的能力可以協助組織落實相關資訊安全措施，有效改善組織營運績效，增加資訊部門價值，並進而提升學員在職場上的競爭力。 課程大綱： 1.人工智慧 (Artificial Intelligence；AI) 的概述 2.人工智慧資訊安全的風險、威脅與挑戰 3.人工智慧的資訊安全與資料保護 4.人工智慧在雲端運算服務的資訊安全措施與指引 5.人工智慧在物聯網應用的資訊安全 6.人工智慧的應用：自動駕駛的資訊安全 7.人工智慧的應用：機器人與智慧製造的資訊安全

第 4 章、 2019 年 12 月份資安情資分享概況

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

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

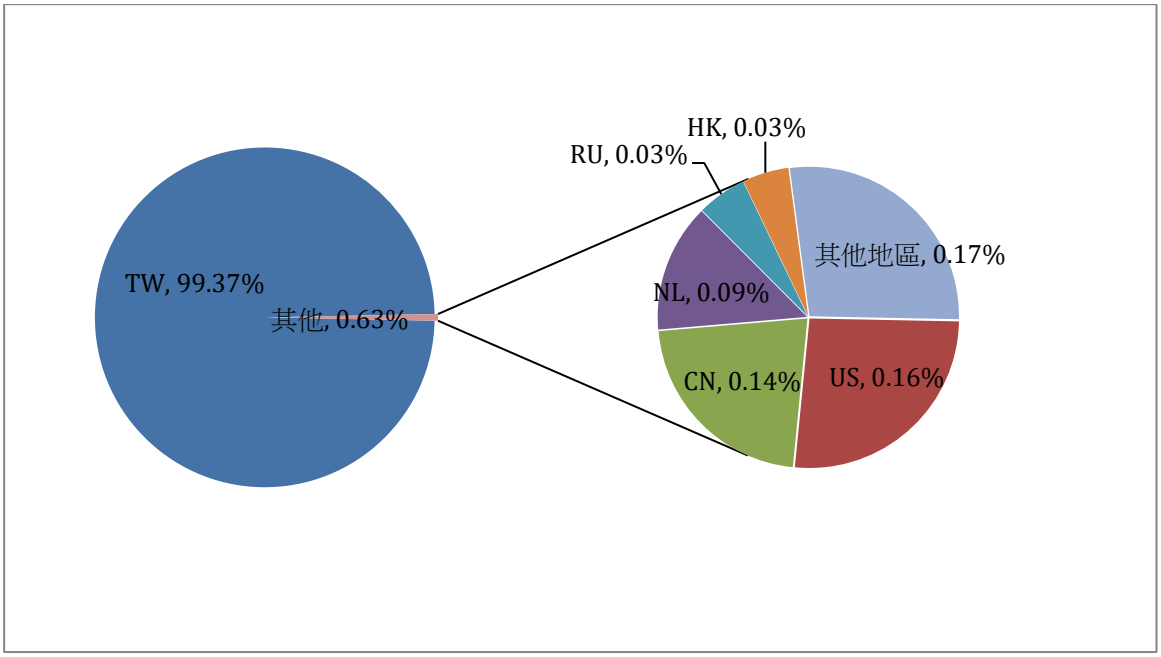


圖 1、分享地區統計圖

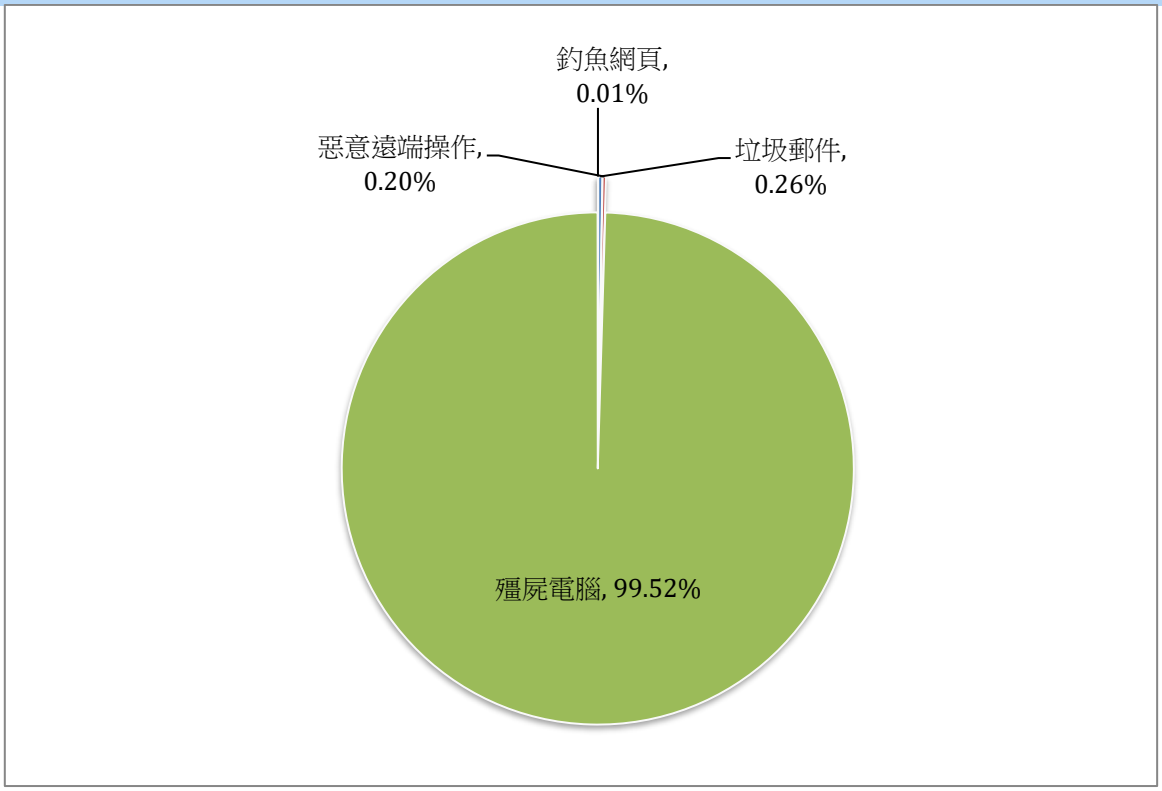


圖 2、分享類型統計圖

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 1 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**