TWCERT/CC 資安情資電子報

2020 年 2 月份

目錄

第 1 章、 封面故事 1
抖音 App 有多個資安漏洞，惡意軟體可透過簡訊傳遞給用戶、個資有曝光風險. 1
第 2 章、 資安小知識 3
網路攻擊者以武漢肺炎名義散發電子郵件，意圖傳播惡意檔案 3
第 3 章、 國內外重要資安事件 6
3.1、 資安趨勢 6
3.1.1、 日本三菱電機遭多個駭侵團體同時大規模駭侵 6
3.1.2、 美國連鎖超商 Wawa 三千萬顧客個資被竊 8
3.1.3、 近十二億張醫療影像在網路上曝光，而且全無保護 10
3.1.4、 新年伊始，勒贖軟體繼續在全球各地傳出災情 12
3.2、 國際政府組織資安資訊 14
3.2.1、 美伊對立升高，德州每分鐘被駭侵攻擊高達一萬次 14
3.2.2、 美國政府所屬網站遭駭，放置伊朗國旗 16
3.2.3、 賭城拉斯維加斯遭網路攻擊，部分市政服務短暫停擺 18
3.2.4、 奧地利外交部等政府所屬網站遭網路攻擊 20
3.2.5、 聯合國驚傳遭大規模駭侵攻擊 22
3.3、 行動裝置資安訊息 23
3.3.1、 Android 惡意木馬 App 能切斷 Google Play 保護措施，偽造用戶評價 ... 23
3.3.2、 特定型號 Android 手機，遭發現預裝惡意軟體 25
3.4、 軟體系統資安議題 27
3.4.1、 國內網路監視器 DVR 設備存有資安漏洞，建議用戶立即更新版本 27
3.4.2、 2020 年，多種微軟產品即停止提供支援，包括漏洞修補更新在內 28
3.4.3、 雲端服務業者提供使用者帳戶安全保護 30
3.4.4、 超過七萬張交友軟體 Tinder 上相片遭盜並分享至網路犯罪論壇 31
3.4.5、 IoT 設備業者 Wyze 外洩近 240 萬用戶個資 33
3.4.6、 美國連鎖餐廳體系 POS 系統遭惡意軟體攻擊，顧客信用卡資訊遭竊取 35
3.5、 軟硬體漏洞資訊 37
3.5.1、 Firefox 修補可能遭駭侵控制電腦的資安漏洞 37

3.5.2、 Google Chrome 被發現含有可被遠端執行程式碼的一系列漏洞 39
3.5.3、 美國國家安全局發布公告，建議 Windows 相關用戶立即更新修補漏洞 41
3.5.4、 近期多家 VPN 設備資安漏洞，相關單位應立即檢視以降低資安威脅 43
3.5.5、 Ruckus 無線路由器發現多個資安漏洞 44
第 4 章、 資安研討會及活動 46
第 5 章、 2020 年 01 月份資安情資分享概況 50

第 1 章、 封面故事

抖音 App 有多個資安漏洞，惡意軟體可透過簡訊傳遞給用戶、個資有曝光風險

資安廠商發現抖音（TikTok）存有多個資安漏洞，對用戶造成相當嚴重的資安風險。

資安廠商 Check Point 日前針對在全球都席捲年輕用戶，擁有破億使用者的短影音 UGC 服務「抖音」（Tik Tok）的多個資安漏洞發表研究報告；報告指出這個極受歡迎的 App 的資安漏洞，能讓駭侵者簡單地以傳送文字訊息的方式，將惡意軟體傳送給受害對象。

Check Point 指出，這個漏洞稱為「SMS link Spoofing」，可以讓駭侵者假冒 Tik Tok 名義，發送任何簡訊給任何電話號碼。

Check Point 說，在 Tik Tok 的官方主站上有個功能，可以讓用戶傳送簡訊給其他用戶，好讓對方下載 Tik Tok 的 App；駭侵者可透過中介工具攔截該站傳送 SMS 簡訊的 HTTP 請求，竄改其中的下載連結，改為下載惡意軟體的連結，接著再傳送給任意電話號碼。

收到這個詐騙簡訊的受害者，會以為自己下載的是 Tik Tok 的應用程式；如果真的點按了連結，就可能在自己的手機上安裝歹徒指定的任何惡意軟體。

Check Point 的資安專家，同時也在 Tik Tok 的 Android App 中的 Deep Link 功能也可能遭駭侵者竄改，駭侵者同樣可藉此傳送含有惡意連結的 SMS 簡訊給任意受害者，或是詐騙用戶安裝惡意軟體，或是將他們導向到其他釣魚網站。

Check Point 另外也在 Tik Tok 的廣告主機上發現 XSS 漏洞，另外也發現有數個 API 呼叫，可以用來取得特定用戶的個人資訊，包括 Email 地址、支付相關資訊，以及用戶生日等個資。

在 Check Point 向 Tik Tok 回報問題後，目前 Tik Tok 已修復上述漏洞。

- 影響產品：Tik Tok App 與官方網站
- 解決方案：App 更新至最新版本
- 資料來源：
  1. https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/
  2. https://www.computing.co.uk/ctg/news/3084911/tiktok-security-flaws

第 2 章、 資安小知識

網路攻擊者以武漢肺炎名義散發電子郵件，意圖傳播惡意檔案

當疫情感染爆發後，在上週開始，就有網路攻擊者藉此混亂時機，利用武漢肺炎名義的電郵，傳播惡意巨集檔案，主要是 Emotet 類型的惡意巨集。

當疫情感染爆發後，就有網路攻擊者藉此混亂時機，利用武漢肺炎名義的電郵，傳播惡意巨集檔案，主要是 Emotet 類型的惡意巨集。

類似的 Emotet 惡意巨集電郵，採用日文訊息內容，標題多半與「武漢肺炎」的相關文字有關(Corona Virus,或是 China Virus)整封電郵均改用日文撰寫，並在信件中提及其附件為政府相關衛生單位所提供之新型冠狀病毒防疫措施，以此誘使使用者開啟附件。而當使用者開啟該附件後，該檔案內含與惡意程式 Emotet 的連結，造成使用者的相關資料，例如憑證、瀏覽紀錄或其他文件都可能遭到惡意程式竊取。

而駭客之所以在現階段將目標設於日本，主要是由於日本日前武漢肺炎疫情嚴重，因此在民眾對新型冠狀病毒的恐慌下，駭客便容易透過關鍵字促使使用者點擊和受騙上當。這也顯示該電郵是鎖定疫情嚴重地區進行傳播，以達到較高的詐騙率。因此，不僅止於一般民眾，許多日本企業也成為該攻擊的受害者。然而，當各地區疫情也逐漸浮現後，駭客亦有可能針對其他地區進行類似的攻擊。

建議如果有下列情況發生，請勿開啟電郵：

(1)電郵標題為英文 Corona Virus 或是中文、日文的武漢肺炎開頭，並且有附帶附件檔案，為 Office 系列檔案，Word 或 Excel。

(2)電郵標題類似(1)但是沒有電郵附件檔案，而是內含 URL 網址，需要點選該網址，以下載檔案。

以上兩種情況，為目前最為普遍的惡意巨集(假借武漢肺炎相關通知)的攻擊方式，請勿開啟此類電子郵件。

若不慎開啟此類電郵，還不一定會感染 Emotet 惡意巨集，必須再點選附件檔案或是 URL 網址。因此，只要謹慎處理此類電郵，無需太過緊張。

由於 Emotet 惡意巨集，會觸發下載程序(Downloader)並可能進一步引發 APT 後續攻擊，或是安裝 Trojan 或 Ransomware。若不慎點選此類電郵的附件檔案或 URL 網址，請勿驚慌。依據網路封包分析協會的建議，按照下列原則，進行處理。

(A)備份檔案，除了自己建立的 Office 文件與圖片影片檔案之外，其餘檔案均不要備份。

(B)找出異常通訊程序，按照網路封包分析協會的 NSPA 封包技巧，使用各種封包分析工具，檢視電腦主機有無下列異常通訊行為：

(1)沒有開啟網頁瀏覽器、FTP 工具、電郵程式，卻發現有通訊連接到外部 HTTP, HTTPS, FTP, SMTP 網路行為(根據 NSPA 分析技巧，請排除 System Update, App.Update, AV Update)

(2)罕見的 DNS 查詢內容，特別有超長網域名稱、Onion.pet 或 Onion.io 的洋蔥橋接域名。

(3)週期性、間歇性的網址連接行為，特別是 RST 封包後，又發生 Retry 的反覆嘗試連線行為，持續進行。

(4)開啟電郵後，產生明顯 HTTP 下載檔案的通訊行為。

(5)Emotet 多半會於惡意巨集開啟時，進行 C&C 通訊行為。因此，檢查內部網路有無類似 C2 通訊行為，亦為重點之一。

也可以錄製網路封包，觀察有無(1) (2) (3)等異常行為。或是將網路封包檔案，郵寄傳送到網路封包分析協會查驗有無異常。

Emotet 惡意巨集，可能會導致內部網路被駭，或是電腦主機被加密勒索。這段期間，請小心謹慎 Corona Virus 或類似中文標題電郵。進一步技術範例，請參考網路封包分析協會網站相關資料，https://www.nspa-cert-tw.org/。

不僅如此，也有詐騙網站藉此機會想賺一筆。該網站聲稱他們是來自澳洲國立大學的團隊，並研發出了首個新型冠狀病毒的疫苗，首頁還使用了美國國家實驗室的照片。根據專家的說法，真正的疫苗還需數個月的研製時間。最近針對武漢肺炎或新型冠狀病毒等電子信件請務必小心因應，避免成為受駭者。

- 資料來源：

1. https://www.hackread.com/cyber-criminals-coronavirus-emergency-spread-malware/
2. https://hackersonlineclub.com/cybercriminals-spreading-coronavirus-malicious-files/
3. https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/?sf116266679=1
4. https://www.bleepingcomputer.com/news/security/emotet-uses-coronavirus-scare-to-infect-japanese-targets/
5. https://twitter.com/briankrebs/status/1223959185764896768
6. https://www.dailycal.org/2018/12/13/lawrence-livermore-national-laboratory-named-one-of-best-places-to-work-in-2019/
7. https://www.nspa-cert-tw.org/

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、日本三菱電機遭多個駭侵團體同時大規模駭侵

日本最大製造業者三菱電機，遭多個駭侵組織共同發動大規模駭侵

日本最大製造業者三菱電機於星期一表示，該公司遭到駭侵團體大規模駭侵。

三菱電機在日本的國防與基礎設施工業領域，佔有非常重要的地位。該公司指出，根據社內進行的事後調查，認為高機密性的各項營業資料，如國防、電力、鐵道等與社會基礎建設相關的資料應無外洩之虞。

目前該公司正在進行事件調查，整個受災情況仍在確認中。

據日本經濟新聞報導指出，該社日本本土和海外分社有多達數十台 PC 和伺服器遭到入侵，被不當存取的資料量約有 200MB。

除了營業秘密資料外，可能外流的資料還包括八千多名該社社員、應徵者和退休人員的各項個資。

三菱電機在日本國內的伺服器，於去年六月底也曾遭到駭侵；外洩的檔案後來在多個國家的某些伺服器上出現。

朝日新聞指出，這次的駭侵團體很可能是稱為「BlackTech」、「Aurora Panda」「emdivi」和「Tick」的駭侵組織共同發動。這些組織過去常以製造業、政府單位、大企業、電力、航空、資通訊等基礎建設設施為攻擊目標，竊取內部機密資訊或製造破壞。

據讀賣新聞報導，由於三菱電機在日本國防與各項基礎建設的重要地位，日本政府已要求三菱電機提出完整調查報告，同時加強日本各政府單位的資安防護措施。

- 資料來源：
  1. https://www.mitsubishielectric.co.jp/notice/2020/0120/0120.pdf
  2. https://www.nikkei.com/article/DGXMZO54586740Q0A120C2MM0000/
  3. https://www.yomiuri.co.jp/economy/20200120-OYT1T50131/
  4. https://www.asahi.com/articles/ASN1P6TGLN1PUTIL02V.html
  5. https://www.asahi.com/articles/ASN1P6V0QN1PUTIL02W.html?iref=pc_extlink

3.1.2、美國連鎖超商 Wawa 三千萬顧客個資被竊

美國連鎖超商與加油站業者 Wawa 去年 12 月遭駭，超過三千萬顧客個資疑遭上網求售。

從美國東部起家，在全美國擁有 850 家分店的大型連鎖超商與加油站的 Wawa 集團，去年 12 月傳出其信用卡支付系統被長期駭侵；駭侵期間據報導長達九個月以上，被駭侵者竊取個資的受害顧客人數，恐怕多達三千萬人以上。

日前在一個著名的個資市集「Joker' s Stash」上，出現了疑似和這起駭侵事件有關的個資販賣案例；賣家稱這包個資來自四十個以上美國各州，超過三千萬人的信用卡資訊。

總部設在賓州的 Wawa 表示，該公司在去年 12 月 10 日發現系統遭駭，旗下的信用卡收銀機疑在 3 月 4 日左右遭植入惡意軟體，時間長達九個月以上；外洩的顧客信用卡資訊包括卡號、到期日、用戶姓名等。Wawa 說信用卡的 PIN 和卡片背面的三位安全碼並未外洩。

該公司表示已得知個資可能遭變賣一事，目前正和相關調查單位密切合作，進行事件調查中。

一家位於紐約的網路詐騙事件調查公司 Gemini Adversary 指出，該批資料目前只被賣家釋出一小部分，這是常見用來抬高資料賣價的手法。目前賣家僅釋出十萬筆資料，其中大多數信用卡資料屬於美國當地用戶在美國所屬銀行申辦的信用卡，但也有少數受害者來自拉丁美洲、歐洲或亞洲國家。

據 Gemini Adversary 估計，每張信用卡個資的售價，會依受害者國籍而有

所不同；美國本土受害者的資料約為一張信用卡 17 美元，但海外受害者則高達每張信用卡 210 美元。

資安專家指出，被植入刷卡機的惡意軟體，目前僅能讀取信用卡磁條上未加密儲存的資訊，還無法存取晶片卡；但由於美國尚有大量信用卡僅具備磁條，許多銷售端點也沒有晶片信用卡的讀取能力，因而造成極大資安風險。

- 資料來源：
  1. https://www.nbcphiladelphia.com/news/local/wawa-investigates-reports-of-attempts-to-sell-customer-info-during-data-breach/2281344/
  2. https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/

3.1.3、近十二億張醫療影像在網路上曝光，而且全無保護

資安廠商發現大量醫療影像在網路上儲存，全無保護，任何人都可以輕易取得，患者隱私遭到極大威脅。

德國資安廠商 Greenbone 在去年九月時就已發現，網路上有七億兩千萬張、屬於二千四百萬次醫學檢查的醫療影像，全無保護措施，可任意下載。

當時該廠商就曾提出警告，呼籲醫療院所應該加強保護這些患者隱私資料，此事且經媒體披露；但 Greenbone 發現未經保護的這些醫療影像不但數量沒有減少，反而還大量增加。

僅僅兩個月內，會洩露病患影像的伺服器數量增加超過 50%，曝險的影像張數來到近 12 億張，分屬三千五百萬次檢驗。

這些曝險的醫療影像，不只含有影像資訊而已，更包括許多病患個人的健康記錄資訊。許多醫療影像內都含有包裝封面的相片，上頭記載了病患的姓名、年齡、生日，以及各種疾病資訊。

Greenbone 表示，外洩的醫療影像數量完全未見減少趨勢，甚至扣除在報導曝光後自動撤下網路的數量外，還是有更多未受保護的醫療影像繼續出現在網路上。

Greenbone 指出，問題顯然出在醫療界缺乏資安防護與用戶隱私保護意識。該公司警告，如果不正視這些問題，外流的醫療個資不但會危及病患的隱私

權，可能讓病患遭到醫療詐騙、影響保險權益，甚至可能危及病患的安全。

Greenbone 曾試圖與多家美國醫療單位連絡，敦促這些院所加強資安防護能力。不少醫療院所十分願意配合，外洩的醫療影像數量也有所降低。

- 資料來源：
  1. https://techcrunch.com/2020/01/10/medical-images-exposed-pacs/
  2. https://www.greenbone.net/en/unprotected-patient-data-on-the-internet-a-massive-global-data-leak/
  3. https://themighty.com/2020/01/unsecured-medical-image-data-threat-to-patients/

3.1.4、新年伊始，勒贖軟體繼續在全球各地傳出災情

勒贖軟體繼續在美國各地傳出災情，包括密西根州的學校系統、德州城鎮的市政系統，都因為勒贖軟體攻擊而宣告停擺。

新年伊始，勒贖軟體的危害仍不斷傳出災情。

據美國媒體報導，密西根州所屬的多個學校系統，日前遭到不明勒贖軟體攻擊；歹徒要求高達一萬美元等值的比特幣贖金，若不支付，便不解鎖遭加密的市政相關重要檔案。

密西根州相關官員指出，勒贖攻擊是在耶誕假期將結束時發動，該州學校體系的多個系統都遭到攻擊，包括影印機、電話和教室內的資訊系統均無法運作。

官員指出，雖然和師生相關的個人資料都平安無事，但仍有三所學校因為攻擊事件而被迫關閉；相關資訊人員已開始復原被攻擊的系統，但復原所需時間將會相當漫長。

官員表示，他們不會支付贖款，因為就算付了贖款，也無法保證受到攻擊的系統和檔案就能完全復原。

無獨有偶，德州的英格賽市（City of the Ingleside）近日也遭到勒贖軟體攻擊，造成部份市政系統停止運作。該市正在努力恢復受損的資料和系統。

根據一份 2019 年十二月底由資安公司 Emsisoft 發表的統計，全美在去年一共有 113 個州級和城市等級的政府單位、764 個醫療單位、89 所學校遭到勒贖軟體攻擊，造成的損失難以估計。

Emisoft 也警告，2019 年沒有任何人因為勒贖軟體而傷亡，這純粹只是因為運氣好，；2020 年全球各地因為勒贖攻擊造成的損失，恐將有過之而無不及。

美國聯邦調查局網路犯罪相關官員也表示，去年光是某一支勒贖軟體，其所有變種襲擊範圍，就廣達全美 50 州，不法贖金所得達六百萬美元，造成的損失更高達三千萬美元。他警告人人都應有可能遭到勒贖軟體攻擊的準備。

- 資料來源：
  1. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
  2. https://www.cbsnews.com/news/ransomware-attack-shuts-down-richmond-michigan-school-district/
  3. https://www.kiiitv.com/article/news/local/ransomware-attack-hits-city-of-ingleside/503-46c2ad28-b617-4cab-8991-711c64ffdebc

3.2、國際政府組織資安資訊

3.2.1、美伊對立升高，德州每分鐘被駭侵攻擊高達一萬次

在美伊衝突升高後，來自伊朗，針對美國的駭侵威脅也隨之升高。

美國德州州長葛瑞格．阿柏特（Greg Abbott）日前提出警告，表示面對日益升高的美伊緊張情勢，以及隨之而來的大量駭侵攻擊行動，德州應該特別提高警戒。

阿柏特州長指出，來自伊朗的駭侵攻擊，德州境內每一個人都應該特別提高警覺，做好充分因應準備與對策。

阿柏特州長也說，根據德州政府的資訊單位的 48 小時統計，每分鐘有高達一萬次來自伊朗的駭侵攻擊行為被偵測到。鑑於去年有多個德州城鎮遭到勒贖軟體的攻擊，造成市政嚴重停擺，州長特別呼籲該州的公民營組織，都應該嚴陣以待。

德州資安相關高階官員也指出，這類駭侵攻擊天天都在發生，每天都有超過十億次以上攻擊；但在美伊對立升高之後，德州遭到的攻擊不論在量或攻擊強度上都大大提升。不過官員並未透露哪個州政府單位遭到最嚴重的攻擊。

官員指出，最近這些強力的駭侵攻擊並未得逞。然而本周二德州農業局的網站，曾被一群自稱為伊朗駭客的駭侵團體攻破。

為了預防可能進一步升高的伊朗駭侵攻擊，德州政府在官方網站中列出了公私單位應特別注意的多點建議，特別是針對勒贖軟體攻擊的可行防禦措施。

- 資料來源：

1. https://www.texastribune.org/2020/01/07/greg-abbott-warns-texas-seeing-thousands-cyber-attacks-iran/
2. https://www.dallasnews.com/news/politics/2020/01/07/texas-officials-fear-iranian-cyber-attack-attempts-may-be-increasing/
3. https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=155
4. https://www.vice.com/en_us/article/m7qa83/iranian-hackers-deface-texas-government-website

3.2.2、美國政府所屬網站遭駭，放置伊朗國旗

一個美國聯邦政府所屬網站，近日遭到親伊朗駭客入侵。美國官員警告，伊朗可能發動更大規模的網路攻擊行動。

美國聯邦政府轄下的「聯邦寄存圖書館」（Federal Depository Library）的一個政府出版品免費借閱計畫網站，日前遭親伊朗的駭客駭入。駭客將該站首頁的內容置換成伊朗國旗。

該網站在上周六遭駭後，目前被迫下線；截至發稿為止，該網站仍無法正常運作。

美國國土安全部所屬的網路與基礎架構安全局，已經開始調查整起駭侵事件。不過該局官員表示，目前仍無證據可以證實駭侵者受伊朗官方指使或支持，也有可能是親伊朗分子自行發動的攻擊。

美國官員警告，這起事件很可能只是冰山之一角；伊朗隨時可能發動更大規模的網路攻擊行動。

美國在上周以無人機攻擊行動，致美伊對立情勢再度昇高。網路攻擊將會是實體攻擊之外，伊朗可能採取的報復手段。

資安專家警告，伊朗駭侵團體對美國公私單位的駭侵行動，很可能因而加強。

網路與基礎架構安全局的官員也指出，伊朗網軍有能力針對美國重要的基礎設施，發動強力網路攻擊，使這些重要設施為之癱瘓。

官員重申，美國各公私單位都應該加強資安戒備，強化監控與備份機制，並且提高各系統的安全控管層級，以防來自伊朗的報復攻擊真的發生。

資安專家指出，除了公部門之外，私部門的金融、大型製造業、能源、電力網絡、航空、醫療體系，都可能會是潛在的攻擊目標。

- 資料來源：

1. https://www.usatoday.com/story/news/nation/2020/01/05/iran-hack-homeland-security-website-hacked-image-bloody-trump/2818308001/
2. https://www.forbes.com/sites/kateoflahertyuk/2020/01/03/will-iran-respond-to-general-qassem-soleimani-killing-with-a-cyber-attack/#76f5f4bf122e
3. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/01/06/the-cybersecurity-202-u-s-should-brace-for-iran-to-cross-red-lines-in-cyberspace-experts-warn/5e123521602ff125ce5bbf7b/

3.2.3、賭城拉斯維加斯遭網路攻擊，部分市政服務短暫停擺

位於美國內華達州，全球知名的觀光賭城拉斯維加斯，日前傳出遭駭侵攻擊。

該市官員指出，本周二晚間發生的這起不明網路攻擊事件，造成該市部分市政服務短暫受阻，對居民和大量觀光客造成不便。

拉斯維加斯市官方推特貼文指出，周二凌晨四點三十分左右，該市遭到不明網路攻擊；該市的 IT 團隊在第一時間採取必要行動，以避免市政系統與重要資料進一步的損毀。

拉斯維加斯市的 IT 團隊，目前也正在調查攻擊者來源，以及攻擊造成的損失。據了解，目前並未傳出重大災情。部分受攻擊時停止運作的市政系統也已恢復運作。

拉斯維加斯市官員在隔天表示，所有市政系統與資料均已復原；該市也認為並未發生任何資料遭竊事件。

拉斯維加斯市此次遭駭事件，正好發生在美伊緊張關係升高的這段期間，時機非常敏感；美國已有其他州、城市和各公私單位，在最近遭到比往日更強大的網路攻擊。

當地的資安專家懷疑，這次拉斯維加斯市被駭侵攻擊，可能也和伊朗網軍的軍事報復行動有關。

專家指出，除了伊朗之外，來自俄羅斯、中國等勢力支持的進階長期駭侵團體（APT），也很可能趁機加強駭侵活動。

資安專家也說，除了政府單位之外，金融機構、重要製造業、服務業、醫療體系等重要民生體系，也可能是外國支持駭侵者的目標，應特別加強資安防護層級，並且提高警戒。

- 資料來源：
  1. https://twitter.com/CityOfLasVegas/status/1214699343745126400
  2. https://statescoop.com/las-vegas-reports-experiencing-cyber-compromise/
  3. https://news3lv.com/news/local/las-vegas-data-breach-comes-amid-homeland-security-warning-on-iranian-cyber-threat

3.2.4、奧地利外交部等政府所屬網站遭網路攻擊

奧地利外交部所屬網站，日前遭網路攻擊；專家懷疑係外國敵對勢力所為。

據奧地利政府表示，這起針對奧國外交部所屬網站與其他網站發動的攻擊，發生於一月四日（周六）夜間；一位奧地利官員指出，這次攻擊造成的後果相當嚴重，而且可能持續數日之久。

奧地利資安單位發表新聞稿指出，該國正在依「網路與資訊系統安全法」的規定，組成特別委員會以因應這波攻擊行動。新聞稿也說，「相關單位很快就掌握狀況，並且迅速採取因應作為。」

但一名奧國國會議員指出，這次攻擊突顯出奧國在資安防護方面準備有多麼不足；這名國會議員也提議，應該增列預算給奧國軍方，以強化資安防護作戰能力，提高該國關鍵基礎設施對抗外國網路攻擊的能力。

奧國資安官員指出，由於攻擊本身十分猛烈，不能排除駭侵者係由外國敵對勢力支持的可能性。

歐盟各國過去也曾遭到外國敵對勢力支持的駭侵攻擊；例如德國外交部、國防部、聯邦監理法院等單位，曾在 2017 年起遭到由俄國支持的 APT28 駭侵團體猛攻。調查報告指出，APT28 滲入德國政府的內部網路系統，時間長達一年以上。

目前資安專家認為由俄國支持的進階持續性駭侵團體 APT28，很可能也是本次攻擊的主要幕後黑手。

這次針對奧地利政府網站的攻擊，正好發生在奧國綠黨於薩爾茲堡舉行集會，決定與奧國保守人民黨結盟的同一天。

攻擊隔天，奧國外交部的官方網站旋即恢復運作如常。

- 資料來源：
  1. https://www.infosecurity-magazine.com/news/austria-foreign-ministry/
  2. https://www.bleepingcomputer.com/news/security/mp-says-austria-unprepared-after-cyberattack-on-foreign-ministry/
  3. https://www.bbc.com/news/world-europe-50997773

3.2.5、聯合國驚傳遭大規模駭侵攻擊

外媒根據其掌握的聯合國內部機密文件指出，聯合國旗下多個組織的伺服器遭嚴重駭侵攻擊，但聯合國並未對外公開此事。

瑞士媒體《新人道主義者》（The New Humanitarian）日前獨家揭露聯合國在去年遭到嚴重駭侵攻擊，但聯合國當局並未對外公開的消息。

該媒體指出，聯合國日內瓦辦公室的 IT 官員在去年 8 月 30 日就提出旗下電腦設備遭駭的報告，指出整個聯合國網域下的電腦系統都遭到駭侵威脅；但聯合國沒有對外公開這些訊息。

報導說遭到攻擊的伺服器有十多台，包括聯合國人權辦公室與其人力資源部門的伺服器都遭到入侵，多個管理用帳號也被駭侵者掌控。

攻擊是從去年七月中開始發動，一位聯合國資深 IT 官員形容這次攻擊的嚴重程度「如同核能電廠發生爐心熔毀事件」；不過只有少數聯合國高階官員知道此事，其他聯合國內部人員僅收到系統維護通知。

這次攻擊事件造成的損害，目前仍無法得知，因為相關的系統記錄已被攻擊者清除；但一位聯合國官員向媒體表示，可能有很多敏感的個人資料在攻擊中被竊取。

資安專家指出，這次攻擊事件明顯是屬於間諜監看類型，因為駭侵攻擊的對象中包括數台 Active Domain 節點，內含所有伺服器的用戶管理功能。

- 資料來源：
  1. https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack
  2. https://apnews.com/0d958e15d7f5081dd612f07482f48b73

3.3、行動裝置資安訊息

3.3.1、Android 惡意木馬 App 能切斷 Google Play 保護措施，偽造用戶評價

資安廠商指出一支 Android 惡意木馬軟體，能切斷 Google Play 的保護措施，並且偽造用戶正面評價。

資安廠商卡巴斯基發表研究報告，指出一支名為 Trojan-Dropper.AndroidOS.Shopper.a 的惡意木馬軟體，不但能夠阻斷 Google Play 應用程式商店的保護機制，偽造虛假的用戶評價，在用戶手機不幸感染後，還會偽裝成系統管理工具、在背景安裝其他惡意軟體、竊取用戶手機中的各項資訊，甚至進行廣告詐騙點擊等。

這支惡意軟體在手機中會以某個系統圖示顯示，名稱也會顯示為 ConfigAPKs，非常類似一支用來進行開機後 App 設定的系統程式。

用戶的 Android 手機一旦感染這支惡意程式，該程式會先下載並解密其酬載程式碼，接著就會立即開始竊取手機中的各項資訊，包括手機所在國名、行動

網路、手機廠牌型號、Email 地址、IMEI 和 IMSI 編號等，並上傳到攻擊者擁有的伺服器中；接著伺服器會發送一系列攻擊用的指令給手機中的惡意軟體。

這支惡意軟體接下來會開始到 Google Play 軟體商店中，針對多個同為惡意軟體的 App 發送評價和虛假用戶評論，企圖拉抬這些惡意 App 的能見度，甚至還會跳過使用者，自行下載更多惡意軟體到手機中。

這支惡意軟體也會同時關閉 Google Play 用以偵測並保護手機免於安裝惡意軟體的服務，同時透過 Android 系統中的輔助使用功能，跳過許多用戶權限許可關卡，因此才能橫行無阻。

卡巴斯基指出，這支 App 在俄羅斯為害最廣，去年十月到十一月間，有近三成（28.46%）的 Android 手機感染此惡意軟體；而在巴西和印度也有 18.7% 和 14.23% 的感染率。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/android-trojan-kills-google-play-protect-spews-fake-app-reviews/
  2. https://in.mashable.com/tech/10433/online-shoppers-in-danger-new-shopper-malware-affects-over-14-indians-kaspersky-report
  3. https://www.android.com/play-protect/

3.3.2、特定型號 Android 手機，遭發現預裝惡意軟體

資安專家發現，由美國政府贊助，提供弱勢民眾使用的 Android 手機，不幸出廠時被預裝了兩款惡意軟體。

資安廠商 Malwarebyte 的專家日前撰文指出，他們發現一款由美國政府出資捐助，提供弱勢階級用戶使用的 Android 手機，不幸出廠時就被預裝了兩款惡意軟體。

被指出預裝惡意軟體的 Android 手機，廠牌型號是 UMX U683CL，透過維京集團旗下電信業者 Assurance Wireless 所出售，由美國政府的生命線計畫資助。

據 Malwarebyte 資安團隊指出，這兩支預裝在手機內的惡意軟體，不但會在用戶毫不知情的情況下，自動安裝用戶不想要的軟體，更會竊取用戶的各種機敏資訊。

這兩支惡意軟體暗藏在手機最重要的系統設定與自動更新程式的框架內；因此根本無法由使用者自行移除。一但強行移除，整支手機就無法使用，形同報廢。

資安專家分析這兩支惡意軟體的程式碼，認定其中一支屬於在 2019 年初就廣為流行的 Adups 變種，目的在收集用戶的資料、開啟手機可被駭侵的後門，並且在用戶不知不覺中安裝任意軟體。

另一支藏在該手機中的惡意軟體，是屬於 Android 特洛伊木馬，會在手機背景執行詐騙廣告點擊，而且也無法由用戶自行移除。

Malwarebyte 在發現該手機被預裝惡意軟體後，在第一時間已通知出售這支手機的 Assurance Wireless 公司。

- 資料來源：
  1. https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/
  2. https://www.forbes.com/sites/thomasbrewster/2020/01/09/us-funds-free-android-phones-for-the-poor---but-with-permanent-chinese-malware/amp/

3.4、軟體系統資安議題

3.4.1、國內網路監視器 DVR 設備存有資安漏洞，建議用戶立即更新版本

國內網路監視器 DVR 設備廠商，近期被發現產品存有多個資安漏洞，遭駭客入侵導致用戶的 DVR 設備產生異常。

造成 DVR 設備產生異常的原因係產品的特定函式存有漏洞，因此駭客透過網址輸入特定參數，取得密碼或是系統檔案。或是針對特定函式進行緩衝區溢位攻擊，取得系統權限。此外，該 DVR 設備的網路限制也存有漏洞，導致駭客可以竄改網路設定檔，對目標裝置注入惡意的系統指令。

建議 DVR 設備的用戶在發現異常時，應儘速與原廠進行聯繫，或是到廠商官網查詢設備的最新資安漏洞訊息，並立即更新至最新版本。更新完成後，也要修改出廠預設的管理員密碼，提升設備安全性，以避免發生資安事件而造成損失。

3.4.2、2020 年，多種微軟產品即停止提供支援，包括漏洞修補更新在內

2020 年有眾多微軟產品即將停止支援，各軟體用戶應特別注意，採取必要措施。

2020 年將有多種微軟主要軟體產品即將進入產品生命周期結束階段，也就是不再提供各種支援；包括產品使用支援、軟體錯誤或資安漏洞更新等等。

微軟列出所有將在 2020 年停止更新的產品列表如下：

- 2019 年 7 月 9 日：SQL Server 2008 and 2008 R2
- 2020 年 1 月 14 日：Windows Server 2008 and 2008 R2、Exchange Server 2010、Windows 7、Windows 7 Professional for Embedded Systems
- 2020 年 10 月 13 日：Office 2010 client、SharePoint Server 2010、Project Server 2010、Windows Embedded Standard 7

另外，微軟也有大量更早之前的舊軟體產品，在先前進行「延長支援」階段；其中也有一部份產品的延長支援即將在 2020 年到期，因而不再繼續提供支援：

- 2020 年 4 月 14 日：Cloud Platform System
- 2020 年 10 月 13 日：Exchange Server 2010 (all editions)、Exchange Server 2016 (Enterprise, Standard)、Office Home and Business 2016、Office Home and Student 2016、Office Professional 2016、Office Professional Plus 2016、Office Standard 2016、Skype for Business 2016、Visio Professional

2016、Visio Standard 2016、Visual Studio 2015 (all editions)、Visual Studio 2015 Update 3、Windows 10 Enterprise 2015 LTSB、Windows 10 IoT Enterprise 2015 LTSB、Windows Defender Antivirus for Windows 10、Windows Defender Exploit Guard

微軟表示，任何還在使用上述停止支援軟體的用戶，應即昇級到仍提供軟體更新支援的新版本，以取得較完整的資安防護支援。

資安專家指出，不擬昇級的用戶，也應加強自己的資安防護，或改採其他仍提供軟體漏洞更新支援的同類型產品，以防含漏洞的舊版軟體成為遭駭侵攻擊的對象。

完整的微軟產品支援到期日與產品清單，可參考微軟官方網站專頁的說明。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/microsoft/microsoft-products-reaching-end-of-life-in-2020/
  2. https://support.microsoft.com/en-us/help/4470235/products-reaching-end-of-support-for-2020

3.4.3、雲端服務業者提供使用者帳戶安全保護

使用者接收的電子郵件內可能包含惡意檔案、惡意軟體下載連結，或為竊取密碼之釣魚網站連結，均可能造成使用者的損害。

為防止相關威脅，雲端服務業者已開始提供相關保護使用者帳號的措施。其中 Google 更針對使用進階持續性滲透攻擊(Advanced Persistent Threat, APT)的國家組織型駭客進行偵測，並適時提醒使用者注意此類攻擊。相關說明可參考：https://support.google.com/a/answer/9007870?hl=zh-Hant。

APT 是長期且持續性潛伏的網路威脅，用以竊取使用者的重要資料。相關發動攻擊的組織可參考 https://www.fireeye.com/current-threats/apt-groups.html，而我國政府不會資助入侵者攻擊之非法行為。

為保護使用者帳戶不受影響，建議採取以下防護措施：

1.為發現有可疑活動之帳戶重設密碼(http://surl.twcert.org.tw/dGdbi)。

2.新增兩步驟驗證(http://surl.twcert.org.tw/kt5AC)。

3.採取保護帳戶安全的步驟(http://surl.twcert.org.tw/Ri8mV)。

4.使用者電腦/手機需安裝防毒軟體，確實更新病毒碼至最新版本。

5.將可疑檔案上傳至惡意檔案檢測服務 Virus Check 檢測(https://viruscheck.tw/)。

如果使用者需要協助時，可以 email 至 TWCERT/CC (twcert@cert.org.tw)或電洽 0800-885-066 尋求諮詢服務。

- 資料來源：
  1. https://support.google.com/a/answer/9007870?hl=zh-Hant

3.4.4、超過七萬張交友軟體 Tinder 上相片遭盜並分享至網路犯罪論壇

超過七萬張交友軟體 Tinder 上的照片，遭分享至討論網路犯罪相關話題的論壇上，可能對這些人的安全產生威脅。

資安廠商 White Ops 旗下的資安專家，日前發現某個以討論惡意軟體為主的論壇上，出現了一大批交友軟體 Tinder 上的使用者照片，照片張數多達七萬張以上。

除了照片以外，同時被上傳到論壇的資料，還包括這些用戶的 Tinder 用戶 ID，數量達到 16,000 人以上。

除了用戶 ID 等個資外，很多照片的 metadata 中還含有相片拍攝日期和時刻；其中有不少照片是自拍照。

目前尚不清楚這些相片和資料的上傳目的，以及上傳者的背景；但由於上傳的目的地網站是個專門討論惡意軟體駭侵相關技術與資訊的網站，因此不能排除這些相片與個資會被用來進行不法用途的可能性。

資安專家指出，歹徒可能會使用這批相片與資料來製作假身分，用來進行

各種詐騙活動，或是直接針對相片本人進行各種騷擾或其他不法行為。

就算歹徒不間接或直接使用這些相片和資料進行不法活動，有這麼多用戶的相片和個資外洩，對這些交友用戶的隱私權，也是嚴重的破壞；例如可能會有不尊重用戶隱私權的業者，在未經相片主人許可的情形下，把這些相片拿去用以訓練人工智慧程式，或進行其他應用。

這些照片是如何從 Tinder 流出的，目前不得而知；Tinder 表示該公司的 App 對交友對象相片的瀏覽範圍限為 100 英哩內，目前正在調查這起事件的原因。資安專家表示，該公司的 API 過去曾有被濫用的記錄。

- 資料來源：
  1. https://techdator.net/tinder-photos-of-70000-women-are-openly-available-on-cyber-crime-forum/
  2. https://gizmodo.com/70-000-tinder-photos-of-women-just-got-dumped-on-a-cybe-1841043456
  3. https://www.cybersecurity-insiders.com/tinder-cyber-attack-exposes-70k-female-photos-for-catfishing/

3.4.5、IoT 設備業者 Wyze 外洩近 240 萬用戶個資

IoT 廠商 Wyze 一個存有 240 萬名用戶個資的資料庫，被發現未經任何保護，在網路上曝光，嚴重影響用戶隱私。

一家名為 Wyze 的 IoT 設備製造廠商，上個月 4 日遭資安專家發現，有一個內含 240 萬名用戶個資的 Elastic 資料庫放在網路上，未經任何保護，可供任何人存取。

該資料庫的資料欄位，包括用戶名稱、Email 地址、設備共享成員的 Email 地址、設備暱稱、設備型號、韌體版本、無線網路 SSID、內部網路路由結構、攝影機上次上線時間、上次 App 登入與登出時間等。

在這 240 萬筆資料中，有近 1% 的資料還含有用戶透過該公司裝置連上 Alexa 語音助理的 token；另外也有一部分用戶的身高、體重、性別、骨質密度、骨質重量、每日蛋白質攝取量與其他個人健康相關資料。

Wyze 表示，該公司已在 12 月 26 日關閉該料庫；現在也正在調查事件的成因與影響；目前所知是該公司為了方便作業，自原始資料庫中複製了這批資料到更容易進行查詢操作的 Elastic 資料庫中，但由於作業錯誤，於 12 月 4 日誤將資料庫的所有保護機制予以移除。

Wyze 也說，目前並未發現用戶透過 iOS 或 Android 裝置連線到 Wyze 設備的 token 有外洩的情形；不過為了確保安全，Wyze 將於近期重置所有第三方連

線用的 token，用戶需重新連結第三方服務並產生新的 token 才能繼續使用。

Wyze 指出這次外洩事件並未洩露用戶的財務相關資訊或密碼；但資安專家 Troy Hunt 認為這是一起相當嚴重的資安事件。

- 資料來源：
  1. https://threatpost.com/iot-company-wyze-leaks-emails-device-data-of-2-4m/151451/
  2. https://blog.12security.com/wyze/
  3. https://forums.wyzecam.com/t/updated-12-30-19-data-leak-12-26-2019/79046

3.4.6、美國連鎖餐廳體系 POS 系統遭惡意軟體攻擊，顧客信用卡資訊遭竊取

美國大型餐飲連鎖體系 Landry’ s 的 POS 系統遭惡意軟體攻擊，大量顧客信用卡資訊恐已遭竊。

擁有超過六百家直營門市，旗下餐飲品牌眾多的美國餐飲連鎖體系 Landry’ s，日前傳出其 POS 系統（銷售點管理系統）遭到惡意軟體攻擊，上門消費用餐的顧客信用卡資訊恐已外洩。

據 Landry’ s 自行發布的資料外洩公告指出，該公司發現一個未經授權的用戶，試圖存取該公司的內部系統；經調查後發現該公司的 POS 系統，可能在 2019 年一月時被惡意軟體入侵，在同年三月到十月之間，這支惡意軟體陸續也出現在多家分店的 POS 系統中。

該公司的聲明中指出，「在很少見的情形之下」，顧客的信用卡資訊可能會遭該惡意軟體竊取。

Landry’ s 表示，該公司已經採取各種可能的行動，包括聘請業界領先的資安公司協助調查整起事件；該公司也說由於該公司的 POS 系統採用點對點加密協定，因此 POS 系統傳送的各種資訊並未外洩；但現場服務人員可能會在點單系統上刷顧客的信用卡，這個部分的資料可能會有外洩疑慮。

該公司也表示，有外洩疑慮的資料，僅限於使用不含顧客姓名資料的信用卡磁條刷卡消費；該公司也列出了可能發生問題的分店。

該公司建議曾在上述期間到該公司旗下餐廳消費的顧客，回頭檢視這段期間的信用卡帳單，是否出現異常消費或盜刷情形。

資安專家指出，由於該公司旗下有數間頂級餐廳，能在這類餐廳消費的顧客，大多屬於財力較雄厚的消費者，因此可能會出現大額盜刷情形；歹徒甚至有可能取得額度相當高的企業配發信用卡的資訊。

- 資料來源：
  1. https://www.landrysinc.com/CreditNotice/CANotice.asp
  2. https://www.bleepingcomputer.com/news/security/popular-us-restaurant-owner-hit-by-credit-card-stealing-malware/

3.5、軟硬體漏洞資訊

3.5.1、Firefox 修補可能遭駭侵控制電腦的資安漏洞

開放源碼瀏覽器 Firefox 日前遭發現一個編號為 CVE-2019-17026 的嚴重 0-day 資安漏洞，該漏洞被評級為 Critical 等級，而且可能已遭到大規模濫用。

被發現這個漏洞的 Firefox 產品除了一般版 Firefox 外，也包括長期支援版本 Firefox ESR。

這個 0-day 資安漏洞屬於 type fusion 類型，可能造成在記憶體禁區中，原本禁止存取的資料遭到不當讀取與寫入。這類的資料越界存取，有可能造成駭侵者跳過某些記憶體保護機制，植入並執行惡意軟體，進而控制受害者的電腦系統。

針對這個 0-day 漏洞可能造成的危害，美國網路與基礎設施安全局官員表示，該局已偵測到大規模利用這個漏洞進行的駭侵攻擊，但攻擊行動相關的細節資訊目前仍未公開。

這個 0-day 漏洞是在日前由中國的奇虎 360 ATA 資安研究團隊所發現，並且即時通報 Firefox 主要開發維護商 Mozilla 知悉。

Firefox 在本周二推出的新版 Firefox 72.0.1，已經修正了這個 0-day 漏洞；這個版本也解決了前一版本中的多個程式錯誤與資安漏洞。

Mozilla 建議所有 Firefox 用戶，應立即更新至最新版本，以儘快補上此一漏洞，避免受到駭侵攻擊影響。Firefox ESR 的用戶也應立即更新。

- CVE 編號：CVE-2019-17026
- 影響版本：Firefox 72.0 之前版本、Firefox ESR 68.4 之前版本
- 解決方案：更新 Firefox 至 72.0.1 之後版本、更新 Firefox ESR 至 68.4.1 之後版本
- 資料來源：
  1. https://www.mozilla.org/en-US/security/advisories/mfsa2020-03
  2. https://www.us-cert.gov/ncas/current-activity/2020/01/08/mozilla-patches-critical-vulnerability
  3. https://arstechnica.com/information-technology/2020/01/firefox-gets-patch-for-critical-zeroday-thats-being-actively-exploited/

3.5.2、Google Chrome 被發現含有可被遠端執行程式碼的一系列漏洞

資安專家近期發現五個 Google Chrome 的資安漏洞，可能遭駭侵者利用，進而在受害系統上遠端執行任意程式碼。

這批漏洞被資安研究人員稱為「麥哲倫 2.0」（Magellan 2.0），主要存在於 Google Chrome 瀏覽器的 SQLite 資料庫管理系統中。

由於 SQLite 資料庫體積小、運作速度快，因此有很多瀏覽器、手機或作業系統都廣泛採用 SQLite。

據 Mitre.org CVE 的報告指出，這五個 SQLite 漏洞，可以透過一個特製的 HTML 加以利用；駭客只要布署含有惡意程式碼的 HTML 檔讓瀏覽器讀取，即可透過這些漏洞遠端執行任意程式碼，並且毫無障礙地存取受害系統的機敏資訊。

據資安專家指出，任何採用 SQLite 的系統，如果沒有更新到最新版本，都可能含有這五個在 Google Chrome 中被發現的漏洞。

這一系列漏洞在 2019 年 11 月 16 日提報給 Google，Google 隨即於 2019 年 12 月 11 日推出修補過後的新版，版本號碼為 79.0.3945.79；任何早於這個版本的 Google Chrome 如果也啟用了內建的 SQLite 資料庫，就存有因為此一系列漏洞而遭攻擊的風險。

資安專家也指出，目前並未觀察到利用此一系列漏洞的大規模攻擊行動。

據 NVD 資料庫的評估，CVE-2019-13751 的嚴重程度為 6.5 分，危險評級為中度。

所有使用 Google Chrome 的用戶，應立即更新到最新版本，以修補這一系列漏洞。

- CVE 編號：CVE-2019-13734, CVE-2019-13750, CVE-2019-13751, CVE-2019-13752,CVE-2019-13753
- 影響產品：Google Chrome 79.0.3945.79 之前版本
- 解決方案：更新至 Google Chrome 79.0.3945.79 起的新版
- 資料來源：
  1. https://threatpost.com/google-chrome-affected-by-magellan-2-0-flaws/151446/
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13751
  3. https://blade.tencent.com/magellan2/index_en.html

3.5.3、美國國家安全局發布公告，建議 Windows 相關用戶立即更新修補漏洞

美國國家安全局（National Security Agency）的資安部門，昨日發表公告，敦促用戶盡速安裝 Microsoft 於 1 月 14 日推出的安全漏洞更新。

微軟在 2020 年首次推出的「周二修補日」（Patch Tuesday）中，針對編號 CVE-2020-0601, CVE-2020-0609, CVE-2020-0610, CVE-2020-0611 等的嚴重資安漏洞進行修補。這些漏洞之所以十分嚴重，必須立刻修補，原因在於 CVE-2020-0601 是關於系統內部的加密程式庫 Windows CryptoAPI (Crypt32.dll)， CVE-2020-0609, CVE-2020-0610 是遠端桌面協定(Remote Desktop Protocol, RDP)伺服器，而 CVE-2020-0611 遠端桌面協定用戶端相關的重大資安漏洞。

根據 NSA 和微軟的說明，駭侵者可以利用 CVE-2020-0601 這個資安漏洞，製作偽造的數位簽章去加簽執行檔，來騙過系統安全認證機制，造成系統安全威脅。

CVE-2020-0609/CVE-2020-0610 為 Windows Remote Desktop Protocol (RDP) 存有漏洞，導致駭侵者連線到 Windows RDP Gateway Server 後，可遠端執行任意程式碼。CVE-2020-0611 的漏洞則是 Windows Remote Desktop Client，在連線到惡意 Server 後，會受到遠端執行任意程式碼的攻擊。

由於這些漏洞對數位認證機制運作的影響十分重大，為防止駭侵者運用此漏洞，建議應立即安裝微軟提供的安全更新程式，修補系統漏洞。

- CVE 編號：CVE-2020-0601, CVE-2020-0609, CVE-2020-0610, CVE-2020-0611
- 影響產品：
  - CVE-2020-0601-----Windows 10、Windows Server 2016 和 2019
  - CVE-2020-0609/CVE-2020-0610-----Windows Server 2012、2016 和 2019
  - CVE-2020-0611-----Windows 7、Windows 8.1、Windows 10、Windows Server 2008、2012、2016 和 2019
- 解決方案：立即安裝最新 Windows 更新程式
- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
  2. https://www.us-cert.gov/ncas/alerts/aa20-014a
  3. https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2056772/a-very-important-patch-tuesday/
  4. https://www.csa.gov.sg/singcert/advisories/advisory-on-critical-vulnerabilities-in-microsoft-windows-operating-system
  5. https://krebsonsecurity.com/2020/01/cryptic-rumblings-ahead-of-first-2020-patch-tuesday/

3.5.4、近期多家 VPN 設備資安漏洞，相關單位應立即檢視以降低資安威脅

去年(2019)8 月下旬發現 Pulse Secure 公司之 VPN 產品的資安漏洞，並已取得 CVE-2019-11539 之漏洞編號，本中心立即通報國內使用該產品之相關單位，其所涵蓋行業別相當廣泛，顯示出 VPN 系統可能已成為攻擊者的重要目標之一。

近期 Citrix 公司之 VPN 產品也被發現資安漏洞，有心人士可透過該漏洞在不需經身份驗證情況下執行任意程式。也就是攻擊者可透過網際網路，直接入侵單位的內部網路，並透過該漏洞進行相關攻擊行為。該漏洞已取得 CVE 編號 CVE-2019-19781 並公佈，而 Citrix 公司也已針對該漏洞提供即時的緩解方案，並且盡力修補並提出新版本中。

由於此兩次 VPN 設備存在之資安漏洞，均可讓攻擊者不須驗證其身份即可進入單位的內部網路，竊取相關資訊，且影響範圍遍及全球。

因此針對任何有使用 VPN 設備之相關單位，即便自身所使用之設備並非遭通報需處理之廠商或型號，建議都應立即嚴格審視 VPN 系統之安全性並加以防範，以避免未來可能遭受的資安攻擊。

- 資料來源：
  1. https://support.citrix.com/article/CTX267027
  2. https://support.citrix.com/article/CTX267679

3.5.5、Ruckus 無線路由器發現多個資安漏洞

資安專家 Gal Zror 日前發現 Ruckus 品牌的多款無線路由器，存有多個安全漏洞，可能遭駭侵者利用，並駭入路由器中。

TechCrunch 報導指出，存有漏洞的是 Ruckus 的 Unleashed 系列路由器產品的用戶 Web 界面。駭侵者可利用這些漏洞，在無須知悉路由器管理密碼的情形下進入管理界面，藉以自外部網路完全掌控路由器的設定。

資安專家指出，許多小型公司行號或家庭，都使用這種簡單的路由器做為網路連線的闡道，因此很容易遭駭侵者單點突破；以這類事件而言，駭侵者將可輕易監聽攔截用戶的所有網路通訊封包，進而取得用戶的各種資訊，甚至進一步駭入用戶的裝置，竊取更多資料，或將用戶裝置當做發動大規模網路攻擊的節點或跳板。

Zror 表示，這次 Ruckus 的資安漏洞，讓駭侵者只要用一行指令碼就可以成功入侵路由器。Zror 估計受這批資安漏洞影響的路由器，總數恐有數千台之多。

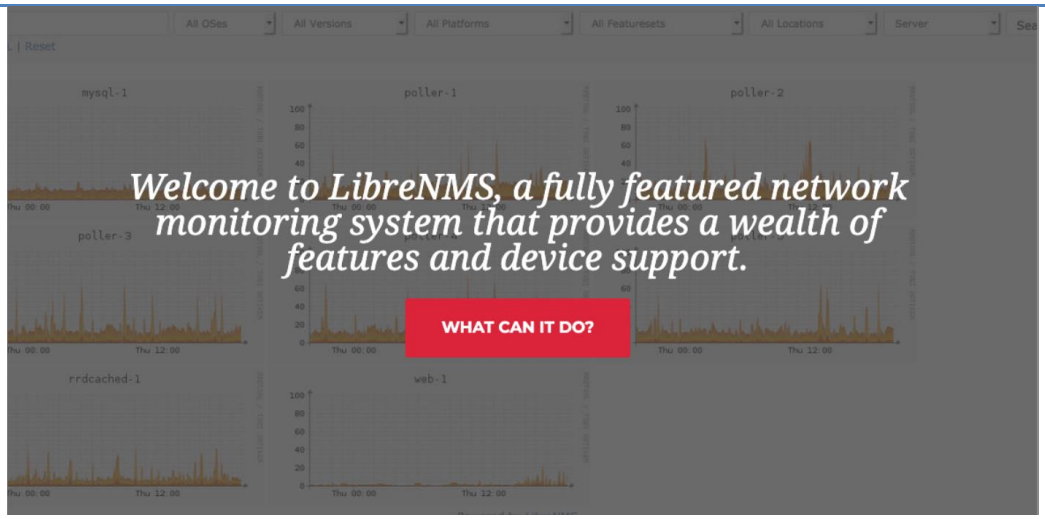
Zror 也在 12 月底舉辦的第 36 屆「混沌通訊會議」（Chaos Commuication Congress）中展示了如何利用 Ruckus 的這批資安漏洞入侵該路由器。

Ruckus 在接獲通報後，很快就發表修補軟體；用戶只要更新到韌體版本 20 0.7.10.202.92，即可將這批安全漏洞修補完成。Ruckus 也呼籲用戶應檢視目前的路由器韌體版本，如果還在使用舊版韌體，應立即更新至最新版本。

Ruckus 官網上提供了關於這一系列資安漏洞的簡要說明，主要的漏洞類型以 RCE（Remote Code Execution，遠端程式碼執行）為主，另外也包括指令注入、存取控制錯誤等等。

- CVE 編號：CVE-2019-19834, CVE-2019-19835, CVE- 2019-19836, CVE-2019-19837, CVE-2019-19838, CVE-2019-19839, CVE-2019-19840, CVE-2019-19841, CVE-2019-19842, CVE-2019-19843
- 影響產品：Ruckus Unleashed 系列路由器
- 解決方案：升級至最新版本韌體
- 資料來源：
  1. https://www.ruckuswireless.com/security/299/view/pdf
  2. https://www.technadu.com/ruckus-wireless-routers-vulnerable-passwordless-takeover-attacks/88805/
  3. https://fahrplan.events.ccc.de/congress/2019/Fahrplan/events/10816.html?=tc
  4. https://techcrunch.com/2019/12/28/ruckus-wireless-routers-flaws/

第 4 章、 資安研討會及活動

LibreNMS 資安應用經驗分享	
活動時間	**02/22(六) 18:30 ~ 20:30**
活動地點	**台中市西區臺灣大道二段 2 號 16F-2**
活動網站	**https://tfc.kktix.cc/events/librenms-infosec-share**
活動概要	 【LibreNMS】 在眾多裝置監視系統套件中，LibreNMS 是一款開源、功能豐富且容易使用的好工具。講者將由過去企業應用經驗中分享，如何以 LibreNMS 為中心，搭配週邊套件來達到多種異常檢測與預警系統建置。 對於有興趣或已經在使用 LibreNMS 的朋友，歡迎前來交流使用心得。

全球網路的分裂危機： 解讀 2019 IGF	
活動時間	**2 月 25 日（二） 下午 14:00-16:00**
活動地點	**IEAT 會議中心 8F 綜合教室（ 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/ihub2020-01**
活動概要	 在迎接 2020 新年度的前一週，俄羅斯通訊部副部長於對外宣布完成一系列測試，以確保該國網路及電信服務在全球斷網或受敵對勢力網攻時仍能獨立運作。而就在該測試前一個月，聯合國的網路治理論壇（Internet Governance Forum，IGF）才以「一個世界，一個網路，一個願景」（One World. One Net. One Vision）為主題進行為期 4 日的探討，包括聯合國秘書長 Antόnio Guterres、德國總理 Angela Merkel 都在 IGF 開幕致詞中提到全球網路世界的地緣政治分裂現況，強調在分裂下國家政府所築起的網路高牆、日益嚴重的網路監控與審查，以及網路自由與人權不斷被剝奪，已成為當今與未來全球共同面對的網路發展挑戰。 本座談邀請到國內熟稔網路基礎建設歷史脈絡與現況的政策專家，分別從技術、政策與法律等不同觀點，就 2019 年 11 月在德國柏林召開的 IGF 會議中針對網路分裂議題的探討，進行評析，期能從中找出台灣在該趨勢下的可能影響與因應。

第二屆 ICANN APAC-TWNIC Engagement Forum 與第 34 屆 TWNIC IP 政策資源管理會議	
活動時間	**4 月 16-17 日**
活動地點	**台北市大安區仁愛路三段 160 號**
活動網站	**https://forum.twnic.tw/2020/index.htm**
活動概要	 本次論壇邀請喬治亞科技大學公共政策學院的 Milton Mueller 教授擔任專題演講主講人，他的主要研究領域為網路的政經發展，主題涵蓋網路所有權、運作機制及資通訊產業的全球治理。他是網路治理計畫的創立者之一，在 ICANN 及 OECD 的公民社群中具有領導地位。曾經參與建立非商業使用者選舉人並當選兩次主席、擔任 GNSO 議會委員；並於多個 ICANN 工作小組中服務，曾擔任 PIR(.org)之諮詢議會委員。參與網路治理經驗豐富，演講內容精彩可期。 ICANN 及 TWNIC 建立論壇平台，讓地區內之網路相關利害關係人，可以藉由合作交流論壇從區域及台灣的角度探索政策、科技與協作等不同面向中各方利害關係人的觀點。

CYBERSEC 2020 臺灣資安大會	
活動時間	**8/12(二) – 8/14(四) 08:30 ~ 17:00**
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://cyber.ithome.com.tw/**
活動概要	 國際級資安大會 X 超規格資安大展【CYBERSEC 2020 臺灣資安大會】，即將在 8/12-8/14 於南港展覽二館盛大登場！ 匯聚世界級資安大神、國內資安頂尖高手，從提供超過 200 堂資安面向的議程、量身打造最扎實的 CyberLab 實戰演練課程，探討國際最新、最熱門且最全面的資安議題與技術，讓您全方面迎戰資安風險。即刻提升實戰能力。 現場網羅超過 250 家以上全球與國內知名標竿資安品牌，展示 1000+業界最新、最適切的資安產品與服務。平日難以跟進的所有資安產品資訊、市場與發展，都可以在此一次獲得！ 邀請您與我們一同參與這年度資安盛會，與來自臺灣與亞太地區超過 8,000 位菁英進行交流，從技術層面與策略層面，探討資安百種面向、交流技術與知識，讓資安戰場更加壯大，得以更快速地反應、更快速地處理，形成足以跟攻擊者匹敵的更強力防禦。

第 5 章、 2020 年 01 月份資安情資分享概況

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

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

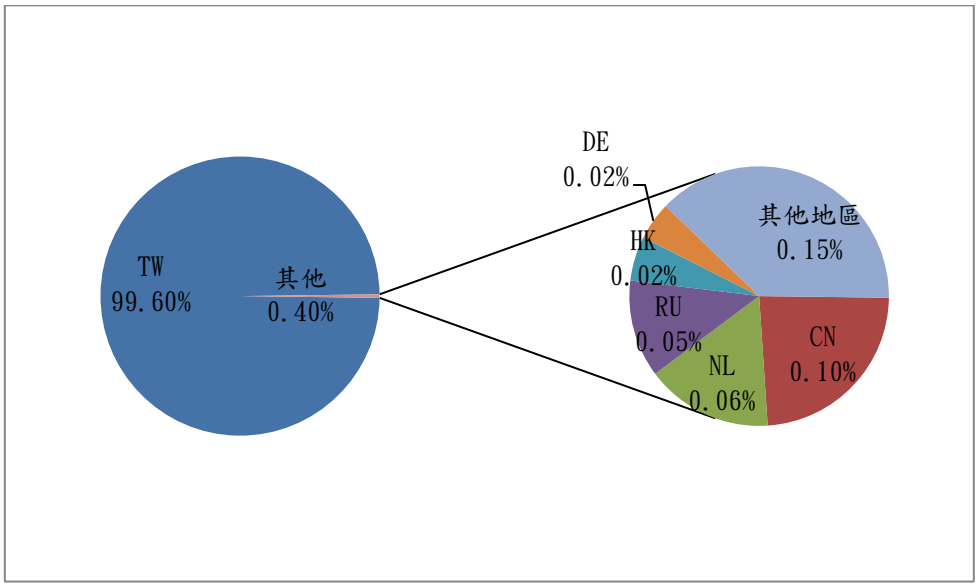


圖 1、分享地區統計圖

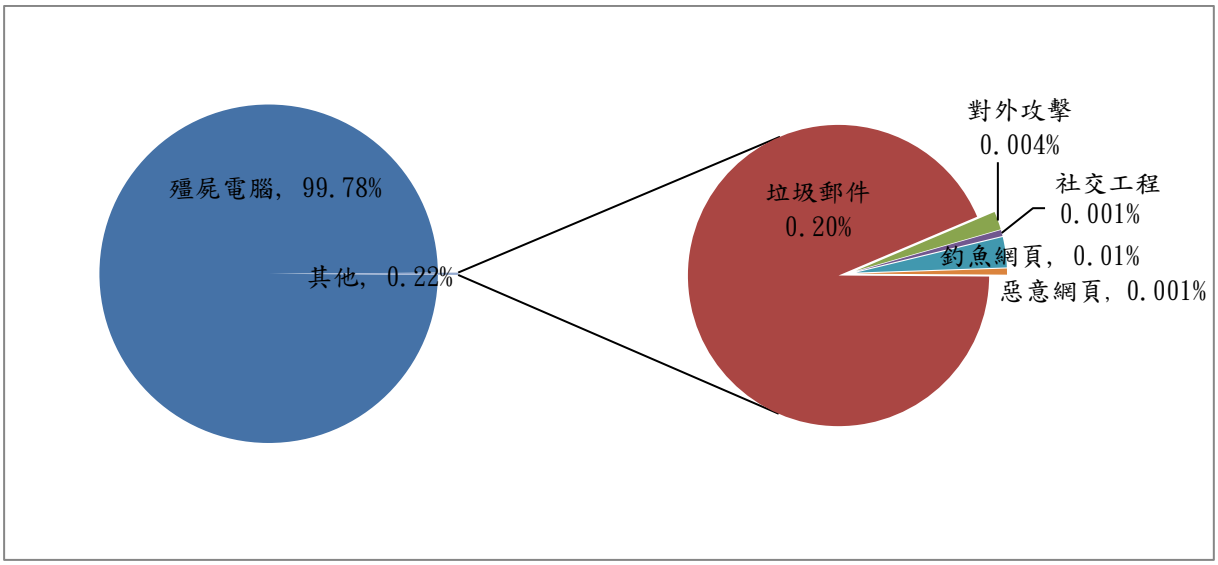

殭屍電腦，99.78%
其他，0.22%
垃圾郵件
0.20%
對外攻擊
0.004%
社交工程
0.001%
釣魚網頁，0.01%
惡意網頁，0.001%

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 2 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**