重要資安情資分享

目錄

一、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

二、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。

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/

三、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：

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

四、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

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

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**https://twcert.pixnet.net/blog**

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

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

Twitter：**@TWCERTCC**