113年1月號

2024
公務機密資訊安全維護

農業部林業及自然保育署臺東分署

公務機密 資訊安全維護

目錄

01

資安時事案例

美媒：逾800個假帳號跟隨台灣時事 操弄2024選舉

LINE母公司遭網攻44萬筆個資外洩、台灣約百筆！數位部要求提補償方案

02

個人資料保護法

查民眾個資、偽造亂丟菸蒂罰單 新北環保局巡查員被起訴

掃描冒牌 QR 碼個資恐遭竊！美國 FTC 公開 3 招防範手法

03

生活中的資安

台灣大推「反詐戰警」APP！AI攔阻可疑電話、揪出惡意簡訊連結

駭客利用AI發起新型態攻擊、資料下毒成新威脅！2024 資安4大預測報告

04

數位學習

網路資料保護－網路不纏身

美媒：逾800個假帳號跟隨台灣時事 操弄2024選舉

示意圖。（中央社）

2023/12/14 11:23

〔中央社〕美國媒體引述社群媒體帳戶分析公司Graphika報告指出，一項試圖操縱2024台灣大選的行動在社群媒體發散。幕後操弄者透過假帳號、搭上台灣新聞脈動，試圖干預台灣選舉。

美國「全國公共電台」（NPR）和華盛頓郵報（The Washington Post）等媒體今天報導，Graphika最新報告揭示，截至上週，這個網絡涉及逾800個Facebook假帳號、13個Facebook頁面、1個TikTok帳戶、1個YouTube頻道。

Graphika報告指出，假帳號常使用中文表情包和影片，並使用不常見的台灣俚語音譯，顯示背後的人並不熟悉這個語言；報告說，這項活動支持並宣傳台灣主要反對黨國民黨，並抨擊包括執政黨民進黨在內的國民黨競爭對手。

Graphika研究人員指出，宣傳行動常跟著台灣新聞動態進行操作，例如缺蛋爭議的話題，試圖將國民黨對手形塑成無能和腐敗的團隊。

報告指出，行動可追溯自2022年5月，TikTok 和 YouTube上開始出現影片，內容來源為一個稱作「搧動台灣」（Agitate Taiwan）的帳號，它的角色如同內容中心，一日可發布多則影片，再由Facebook假帳戶轉發。

Graphika表示， Facebook上的貼文幾乎沒有真實用戶參與，但有些貼文顯示在特定主題標籤的搜尋結果上方，主題與2024台灣選舉的政黨和候選人有關。

Facebook的母公司Meta一名發言人說，公司與Graphika研究人員合作調查這項行動，將持續監測違反公司政策的行為。部分危險信號顯示帳戶並非真實身分，而是從真人那裡竊取來的檔案照，再對某些特徵移花接木，例如替換笑容。

YouTube一名發言人指出，假帳戶違反公司政策已被刪除。YouTube 嚴禁發布垃圾內容，或以詐騙和其他欺騙行為誘騙YouTube使用者的內容。

TikTok上則仍保有「搧動台灣」帳號， TikTok一名發言人表示，該公司正持續調查該帳戶，但尚未發現不真實或屬於操弄行動一環的證據。

Graphika研究人員評估，2024大選前，透過網路操弄台灣政治輿論的行動極有可能升溫。政府官員和科技公司都曾示警，明年全球的選舉將成為中國、俄羅斯和伊朗等國家、以及來自國內團體的干預目標。

LINE母公司遭網攻44萬筆個資外洩、台灣約百筆！數位部要求提補償方案

（圖／彭博社）

2023/11/28 11:12文／記者劉惠琴

即時通訊軟體 LINE 母公司日本雅虎（LY Corporation）發佈公告表示，今年10月外包公司因伺服器遭駭客網路攻擊入侵，導致用戶、合作夥伴、職員、和其他人員在內，共計約有44萬筆的個資與使用行為遭外洩，截至11月27日止，尚未收到流出個資已遭濫用的舉報情事，對此，向用戶致歉並已依法向相關政府部會和機構通報，同時亦將持續調查，以隨時採取必要的應對措施。

根據官方公告，此次因遭駭客網路攻擊，導致資料外洩內容主要受影響範圍為系統紀錄檔及部分員工資料，以及用戶年齡、性別、貼圖購買紀錄，並沒有信用卡帳戶、銀行帳戶與財務有關等敏感內容，也沒有聊天室對話內容。而在約44萬筆的個資外洩之中，與LINE台灣用戶有關資料約百筆（非人數），均為經過雜湊的手機號碼、電子郵件或 LINE 帳號。

經 LINE 台灣連線公司向數位部數位產業署通報後，數產署立即要求台灣連線公司提供說明改善作為，LY Corporation 已強制重設員工內部系統密碼及二階段認證機制（Two-Factor Authentication），並透過用戶註冊的電子郵件或官方LINE帳號發出訊息通知相關當事人。此外，數位產業署並已要求台灣連線公司配合行政檢查，持續強化資訊安全防護，並要求台灣連線公司就台灣用戶受損之權益提出方案，除包含個資法在內的相關法規規定外，也需有其他方式落實保障消費者個資權益。

查民眾個資、偽造亂丟菸蒂罰單 新北環保局巡查員被起訴

2023/12/14 15:31

〔記者王定傳／新北報導〕新北市政府環保局蘆洲區清潔隊林姓巡查員，因與詹姓男子有私人糾紛，竟請不知情同事查詢詹男車藉資料，取得他的身分字號後，偽造不實亂丟菸蒂舉發單，再以此查得詹男戶籍資料，新北地檢署調查後依行使公務員登載不實文書、偽造私文書及違反個人資料保護法「公務員假借職務上機會非法蒐集、利用個人資料」等罪嫌，起訴林男。

檢方調查，林男是新北環保局蘆洲區清潔隊的巡查員，對於違反廢棄物清理法的違規行為，有稽查、勸導及告發的權限，怎料，他因為與詹男有私人糾紛，為查明詹男個資，自2020年起指示不知情同事協助查詢車藉資料，因該名同事無查詢車藉權限，因而轉由不知情新北環保局專責人員查詢。

檢方調查，林男以此方式取得詹男身分證字號，隨即在新北環保局違反環保法令案件舉發通知書上偽造詹男亂丟菸蒂，甚至自己在被舉發人簽章欄偽造詹男簽名，表示舉發通知書已由詹男簽名收受，再交由同事查詢詹男戶籍資料，取得對方個資後，為了掩飾犯行，隨即把舉發通知書上的姓名塗改。

檢方偵辦時，林男坦承犯行，檢方調查後依行使公務員登載不實文書、偽造私文書，以及違反個人資料保護法「公務員假借職務上機會非法蒐集、利用個人資料」等罪嫌，將林男起訴。

新北地檢署。（資料照）

掃描冒牌 QR 碼個資恐遭竊！美國 FTC 公開 3 招防範手法

2023/12/11 11:30文／記者黃肇祥

無論是餐廳點餐、繳停車費或是分享資訊，小心日常隨處可見的QR 碼藏有詐騙陷阱！近期美國聯邦貿易委員會（FTC）發出警告，指出詐騙集團開始利用 QR 碼竊取民眾個資，提出 3 個防範手法，讓你避開危險。

根據 FTC 指出，詐騙集團會透過冒牌的 QR 碼去替換停車場的收費 QR 碼，或是在電子郵件、簡訊中，謊稱包裹無法正常運送，需要重新安排收件時間，還有佯裝客服聲稱帳號有問題，需要更改密碼或是確認資訊，要求用戶進一步聯繫，並且隨信附上 QR 碼作為連結。

若用戶掃描詐騙集團提供的 QR 碼，可能會被誘導至假網站輸入個人資料，有些還會直接在設備上安裝惡意軟體。至於該如何防範呢？FTC 提供了 3 大手法。

首先是在掃描 QR 碼後，檢查連結網址是否有拼寫錯誤或是可疑之處。第二，避免直接掃描可疑 QR 碼，改用電話或是真實的網址與該公司聯繫。最後，則是可以強化自己帳戶安全的性，使用更強的密碼或是多重要素驗證（MFA），降低遭竊的可能。

事實上，類似手法在台灣也曾出現。疫情期間就有不肖人士擅自替換店家的簡訊實聯制 QR 碼，原本會傳送至 1922 的簡訊，改為高額的付費號碼，讓荷包大失血。

（圖／彭博社）

台灣大推「反詐戰警」APP！AI攔阻可疑電話、揪出惡意簡訊連結

2023/11/28 15:11文／記者劉惠琴

電話、各式話術包裝的簡訊內容，是詐騙份子引誘民眾上鉤的主要管道。當前AI技術的快速發展與廣泛應用，為生活帶來更多便利性，同時也成為詐騙份子利用的工具，導致更多新型態的詐騙手法案件持續層出不窮。

據電信業者台灣大哥大表示，針對旗下用戶門號所做的大數據統計，手機平均每月接收騷擾或詐騙來電高達750萬通，不僅令人不堪其擾，此外，約超過1成的用戶，手機每月都會收到各式各樣的詐騙簡訊內容。

為協助民眾手機防堵遭詐的資安風險，台灣大哥大於今宣佈（11/28）推出支援Android、iOS雙系統平台的「反詐戰警」個人版App，訴求重視用戶隱私與無廣告干擾的使用體驗，無須上傳通訊錄與通話紀錄等機敏資料，並具備即時自動更新資料庫的功能，幫用戶辨識陌生來電與掃描惡意可疑簡訊內容。

「反詐戰警」個人版App，首波提供台灣大哥大用戶自即日起免費下載使用，預計明年2024年第一季將服務擴及全台民眾，全面擴大資安防護網。

手機免費下載「反詐戰警個人版APP」，無須上傳通訊錄與通話紀錄等機敏資料，可揪出可疑詐騙或廣告騷擾來電、以及掃描辨識惡意簡訊連結。（圖翻攝台灣大哥大官網）

台灣大表示，為擴大化防詐效益，集結技術開發專家、AI工程師，橫跨各單位組成「反詐專案小組」，繼先前推出可偵測偽冒網站的「反詐戰警」、與隱碼服務「安心Call」兩大反詐利器後，此次再度領先業界，推出台灣電信業的第一個「反詐戰警」個人版APP」，運用電信數據AI模型，並整合海量大數據資料庫，串接台灣大反詐戰警全民通報平台、內政部警政署165 全民防騙網等多面向資料源，透過即時數據更新，快速辨識疑似詐騙電話及騷擾電話，提供個人化的電話警示、自動封鎖號碼服務，並可掃描帶有惡意連結的高風險簡訊，避免用戶瀏覽釣魚網站。

手機免費下載「反詐戰警個人版APP」，無須上傳通訊錄與通話紀錄等機敏資料，可揪出可疑詐騙或廣告騷擾來電、以及掃描辨識惡意簡訊連結。（圖翻攝台灣大哥大官網）

駭客利用AI發起新型態攻擊、資料下毒成新威脅！2024 資安4大預測報告

生成式AI的崛起，為各產業帶來推動轉型動能的突破性技術，然而，也成為駭客攻擊的新型武器，尤其是結合傳統攻擊與新型態攻擊的態勢，讓2024年資安環境的風險與壓力都將隨之增強。

資安業者趨勢科技於今發佈2024年的資安預測報告，並特別盤點出四大值得密切關注的資安趨勢，包括有：會自我繁殖的蠕蟲自動化攻擊加劇雲端安全風險、鎖定大型語言模型LLM的資料下毒成新興威脅、鎖定供應鏈發起的攻擊活動更顯著、以及試圖搜刮金鑰篡改私有區塊鏈資料進而勒索贖金的網路敲詐手法。

對此，趨勢科技台灣區總經理洪偉淦指出，駭客集團借力AI新技術來優化自身營運模式，提升攻擊速度與力道，擴大資安事件衝擊，將讓資安態勢更加複雜詭譎。無論個人或企業，都需要具備並強化資安意識和審慎評估對應方法。

針對2024年須嚴陣以待的資安趨勢預測，重點列述如下：

一、蠕蟲自動化攻擊為雲端環境首要威脅

蠕蟲具備自動化大量攻擊漏洞的能力，將很可能成為2024駭客集團的首選武器，用以執行各式各樣的任務！

駭客集團只需成功攻擊一個漏洞，就能在雲端環境內迅速蔓延，並利用已感染的雲端原生工具攻擊更多受害者，造成的危害包括：自動化收集企業機敏資料、建立龐大的幕後操縱(C&C)伺服器通訊，甚至發動大規模分散式阻斷服務(DDos)攻擊。

建議資安團隊需加速漏洞修補速度，除了即時掃描惡意程式與漏洞外，還必須嚴格檢視自己的資安政策與雲端環境以避免組態設定錯誤問題。

生成式AI、區塊鏈在商業利益與資安威脅間形成雙面刃。趨勢科技核心技術部資深協理張裕敏指出大型語言模型遭遇「資料下毒」也將成為新興威脅。 （圖／趨勢科技）

二、大型語言模型LLM 遭資料下毒

生成式AI提升個人與企業營運生產力，卻也為駭客帶來助力。駭客使用生成式AI精進社交工程詐騙(例如：變臉詐騙、魚叉式網路釣魚、網路捕鯨等)、生成更具吸引力的釣餌，提高得手機會。

預期2024年駭客將透過結合不同的AI工具(如聊天機器人和偽造語音)製造出如虛擬綁架此類多重面向的威脅。根據FBI報告指出，運用社交工程技巧的網路犯罪是受害者數量最多的犯罪、也是最賺錢的手法之一。未來，此類犯罪手法將不以量取勝，而以更逼真的手法進行勒索。

同時，大型語言模型(LLM)遭遇「資料下毒(data poisoning)」也將成為新興威脅，駭客集團除了透過竄改學習資料操弄機器學習(ML)的表現與行為之外，還可以入侵模型的資料儲存或流程架構之中，可能導致自然語言處理模型洩漏機密資料，系統受污染無法正常偵測非法活動。

三、鎖定軟體供應鏈 追求攻擊效益極大化

順應現代商業營運模式：企業移轉至雲端原生開發工具、採用DevOps流程、使用持續整合/持續交付(CI/CD)、大量使用第三方應用程式，駭客將主力發展「攻擊單一軟體，全供應鏈受害」的攻擊情境。

2024年，供應鏈攻擊即服務(supply chain attacks as aservice)將持續成為駭客集團獲利的主要方式之一，國家級駭客也可能透過攻擊供應鏈來收集情資，駭客將更積極鎖定源頭展開行動，針對IT基礎架構的底層程式碼，瞄準第三方元件，如：函式庫、流程與容器發動攻擊。

四、私有區塊鏈攻擊增加 駭客攻擊複雜化

隨著全世界越來越多企業運用區塊鏈來降低營運成本，區塊鏈上的珍貴資料也引來攻擊者的覬覦。駭客集團除了瞄準公有區塊鏈之外，也將攻擊私有區塊鏈網路，試圖搜刮金鑰篡改區塊鏈資料、寫入惡意資料再勒索贖金等。

如果駭客掌控了足夠的關鍵節點，就能將整個區塊鏈加密，讓區塊鏈完全無法動彈，進而勒索鉅額贖金。因此，企業在推出一些仰賴許可制區塊鏈網路來運作的服務時，務必確保其網路節點要足夠分散，以抵禦潛在的網路攻擊和中斷。

（圖／趨勢科技）