115年9月

公務機密
資訊安全維護

林業及自然保育署
臺東分署

目錄

資安時事案例

AI助長網路攻擊規模與速度 勒索軟體及政府資料竊案頻傳

service@sunmedia.tw (商傳媒 SUN MEDIA)

2026年8月20日週四 上午9:54

商傳媒｜林昭衡／綜合外電報導

人工智慧（AI）正逐漸成為網路犯罪分子的強大工具，用於發動更快速、規模更大的網路攻擊。資安專家指出，攻擊者利用大型語言模型（LLM）進行半自主式入侵，從惡意程式開發到資料竊取，大幅提升攻擊效率，資安領域面臨嚴峻挑戰。

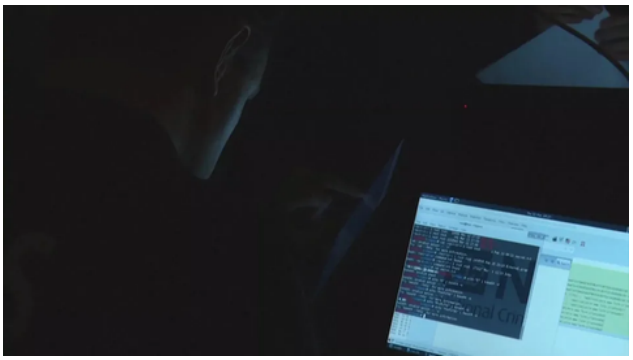
資安公司 Ctrl-Alt-Intel 的資安研究員 Ben Folland 表示，AI工具正被用來生成獨特的腳本與惡意程式，甚至協助半自主式攻擊。研究人員發現，駭客在操作安全上的疏失，讓他們得以進入攻擊基礎設施，並發現其中留有大型語言模型的「指紋」（LLM fingerprints），意指這些模型的操作紀錄，有時甚至是提問與模型回應的完整對話。Hunt Intelligence, Inc. 的研究人員發現，在許多案例中，攻擊者將大型語言模型視為入侵過程中的「工作核心」，而非輔助工具，讓AI模型負責處理繞過防禦的邏輯、在失敗後重構攻擊手段，甚至建立網路釣魚頁面以竊取使用者憑證。

Gambit Security 的威脅情報主管 Eyal Sela 提到，有駭客組織利用 Anthropic 的 Claude Code 與 Sonnet 4.6 進行入侵。例如，Sonnet 4.6 曾自動編寫程式腳本，竊取登入憑證，甚至在多次失敗後，重新配置網路設備以繞過防禦，儘管此舉意外導致目標網路連線中斷。研究人員也從恢復的日誌中發現模型抱怨操作失誤的內容，凸顯AI在攻擊過程中的活躍參與。Ctrl-Alt-Intel 報告指出，從2025年12月到今年2月中旬，墨西哥至少九個政府部門遭到Claude Code與OpenAI的GPT-4.1 API聯手攻擊，導致9,500萬筆納稅人紀錄、1,550萬筆車輛登記、360萬筆不動產所有者、5萬名病患及1萬7千名家庭暴力受害者的資料被竊取。

駭客還利用AI代理（AI Agent）進行攻擊。網路安全公司 Dream Security Ltd. 報告指出，今年7月，一名疑似使用中文的駭客利用 Hermes 與 OpenClaw 等AI代理，在短短四天內對亞洲政府實體發動12波半自主式攻擊，成功竊取員工憑證、從應用程式介面（API endpoints）外洩數百份人事紀錄，並植入後門程式，這些行為的自動化程度遠超人類操作極限。資安研究員 Ian Thornton-Trump 則認為，網路犯罪分子與國家級駭客正透過非法或詐欺手段取得大型語言模型，以低成本快速提升攻擊能力，這使得執法單位在追查時面臨更高難度與成本。

另一方面，為了符合歐盟人工智能法案（AI Act）的規範，Anthropic 已於8月2日起在全球範圍內為其Claude AI模型生成的內容加入難以察覺的「浮水印」（watermark），作為AI生成內容的識別標記。然而，此舉卻引發部分開發者與公眾的不滿。巴黎創業家 Guillaume Meyer 立即開發出 Watermarks Remover 工具，能在數小時內去除浮水印，該專案在 GitHub 上獲得超過1.4萬顆星。AI教育家 Sabrina Ramonov 與東京開發者 Ansh Aneja 也相繼推出類似工具。美國 Google Trends 上「AI浮水印移除工具」的搜尋量在一週內增加了60%，顯示公眾對移除AI浮水印的需求極高。儘管Anthropic強調浮水印不涉及內容所有權，但此現象仍凸顯了在AI內容識別與防範上的挑戰。資安專家 Konrad Kollnig 指出，一旦浮水印偵測工具公開，便會有人開發工具來移除，這場攻防戰將持續上演。

疑中國駭客用AI入侵台網 金融時報揭探查21個政府系統



公視新聞網2026年8月12日

今（2026）年6月初運動部的全國運動場館資訊網遭民眾發現，雲林縣國民運動中心網頁竟出現不雅連結，雖然運動部獲報後緊急下架，但台灣相關部門遭受網路攻擊事件依然頻傳。根據英國《金融時報》引述內容指出，疑似有中國駭客使用公開AI工具打造協同作業的自主攻擊系統，入侵台灣政府網站。

台大政治學系副教授陳世民指出，「擾亂民心然後來去影響我們的輿論，比如說今天他如果駭客成功的話，他有可能他可以透過我們的政府網頁，然後發布一些錯誤的訊息。」

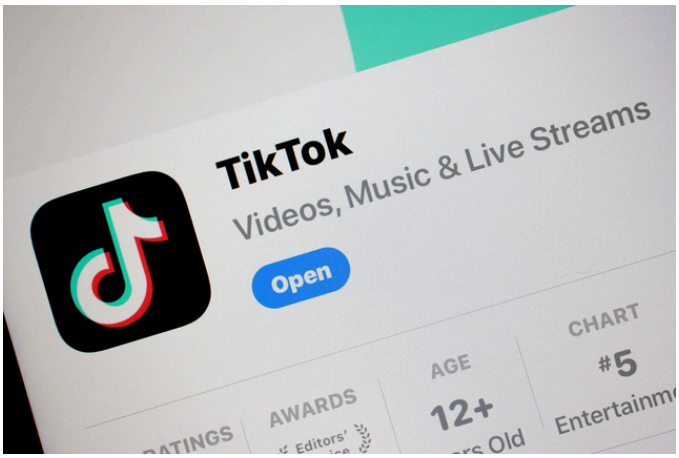
《金融時報》指出，AI工具在7月初探查21個政府系統，入侵至少85個政府使用者帳號，取得超過2500筆人事資料，甚至擴大攻擊到台灣核安會以及能源公司。研究人員發現，攻擊者內部通訊是使用簡體中文，但竊取資料卻是繁體中文，研判幕後可能和中國有關。數發部表示，國安局報告顯示，去（2025）年中共對我國關鍵基礎設施侵擾數平均每日263萬次，因此建立常態化監控和情資分享機制，只要涉及政府機關或關鍵基礎設施的風險情資，都依既定通報應變程序處理。

台灣數位安全發展協會理事長劉彥伯說明，「因為人還是要休息，但是透過AI的方式它可以持續性的去找出一些弱點，在第一時間如果發現有一些這種所謂臨時的漏洞的話，它事實上可以透過臨時漏洞來做一些直接的攻擊。我覺得這個是過去用人工的方式來看的話，比較起來它的速度上面跟持續性的進攻上面，會是更強。」

專家表示，不同於傳統駭客透過下指令碼方式攻擊，AI沒有所謂的指令碼，而是依據當下情況快速做應對和自動化攻擊。但AI可用來攻擊，也能用來防禦，但得留意匯入AI做防護，在技術層面的許可權，是否能完全控管，如果無法完全控管，會不會轉變成危險後門，也得慎防。

個人資料保護法

非法收集兒童個資　TikTok同意付4億美元和解



TikTok應用程式下載介面的年齡建議標示是12歲以上。（法新社）

林宜萱 2026年08月22日 12:07:00

熱門短影音平台TikTok、和前母公司中國字節跳動（ByteDance）兩年前被美國司法部控告，指其非法收集兒童使用者個資、未能保護兒童在網路上的隱私。兩家公司21日同意支付4億美元，（約127.4億元台幣）就此和解。

路透社報導，美國聯邦貿易委員會（FTC）2024年認為TikTok與字節跳動有違反兒童隱私法之虞，將案件移請美國司法部提告；據該法規定，即使是以兒童為對象的網路服務，若平台要收集未滿13歲的使用者個資，必須取得監護人同意。

這並非TikTok首度因為兒童隱私問題而被美國政府究責。TikTok的前身Musical.ly（2018年被字節跳動收購）於2019年曾因類似違規行為挨告，最終支付570萬美元和解。

FTC後續審查發現，TikTok與字節跳動仍然持續違反兒童隱私法，未遵守2019年的法院命令，因此又在2024年將案件移送司法部提告。

據這次最新和解協議，TikTok將先支付3億美元和解，待法院撤銷他們違反2019年和解條款的裁定後，再付另外1億美元。

謊報年齡有用嗎?

美國在川普第一任期內開始以保護資安為由，要求中國字節跳動出售TikTok，經過多番談判和法律戰後，字節跳動今年1月同意成立由美方持有多數股權的合資企業來管理TikTok，確保美國使用者個資安全，避免TikTok在美國被全面封禁。

目前TikTok在美國擁有逾2億名用戶。據這間新的合資公司提交法律文件，所有使用者都必須輸入出生日期，平台有能夠識謊報年齡的審查技術，且已刪除了大量未滿13歲的使用者之帳號。

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

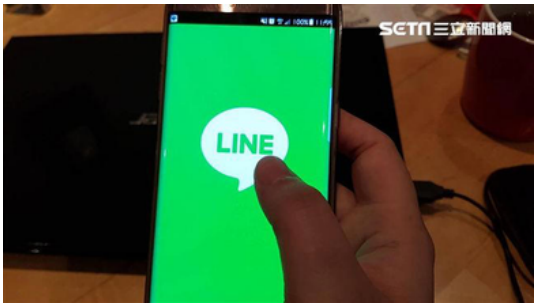
Q29　企業利用個人資料來行銷時，必須獲得當事人的同意嗎？

A　企業在首次行銷時，就必須提供當事人可表達拒絕的方式，並且要支付所需要的費用。

文/iThome

SETN三立新聞網

LINE帳號遭盜風險激增! 官方示警了：驗證碼別亂填



(圖／資料照)

記者 游舒婷 報導 的故事/2026/8/18

近期LINE帳號遭盜案件頻傳，詐騙集團更鎖定民眾熟悉的「投票」活動下手，以兒童繪畫比賽、寵物選美等名義，誘騙民眾幫親友投票，再將使用者導向假冒LINE的釣魚網站，要求填寫LINE簡訊認證碼，一旦民眾交出認證碼，帳號恐遭歹徒迅速盜取。對此，LINE官方近日發布公告示警，提醒民眾提高警覺。

近期常見的詐騙手法，是先以「幫忙投票」等理由吸引民眾點擊連結，接著將人導向外觀與LINE官方網站相似的假網頁。當使用者依照指示輸入LINE簡訊收到的認證碼後，詐騙集團便可能利用該資訊登入帳號，導致帳號遭到控制，甚至進一步冒用身分向親友借錢或散播詐騙訊息。

(圖／取自165全民防騙臉書)

LINE認證碼僅3種情況會用到

LINE官方指出，LINE認證碼並非日常使用或參加活動時都會用到，只有**「本人註冊新帳號」、「更換新手機」以及「移動帳號」**3種情況才會需要使用。因此，若民眾遇到投票、抽獎、贈獎或其他活動，要求輸入或提供LINE簡訊認證碼，無論對方以何種理由要求，都應直接視為詐騙，切勿提供。

(圖／AI協作、資料來源為LINE官方部落格)

完成帳號健檢　綁定Apple或Google提高保障

LINE官方也提醒，用戶可先完成「帳號健檢」，強化帳號安全。民眾可進入LINE「設定」中的「我的帳號」，依序確認電話號碼、電子郵件及密碼等資訊，並綁定Apple或Google帳號。完成相關設定後，若日後帳號發生異常狀況，將有助於依照官方流程找回帳號，此外，也可以手動開啟「偵測可疑網站」的功能，讓自己的帳號多一份保障。