115年6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

資安警報升級! Google證實：AI參與「零日攻擊」即時攔截

（示意圖／達志影像Shutterstock）

蘇憶歡 的故事/2026/5/13

Google最近公布最新一份AI威脅報告，指出已成功攔截一起高風險網路攻擊，並首次觀察到威脅行為者疑似利用「AI」協助開發「零日漏洞」攻擊工具。所謂零日漏洞，是指軟體尚未修補就已被利用的安全缺口，一旦遭到攻擊，往往具備極高破壞力，因此這也讓Google提高警戒！

攻擊流程曝！Google疑：AI參與其中

Google指出，這起攻擊事件鎖定一款廣泛使用的開源系統管理工具，並在之中發現「雙重驗證（2FA）」的邏輯設計缺陷，而問題核心在於系統存在信任假設，因此才會讓攻擊者在取得帳號憑證後，有機會繞過驗證機制。Google進一步分析，攻擊者已撰寫 Python腳本製作漏洞利用程式，並計畫進行大規模攻擊，但在擴散前就被 Google的主動偵測與反制機制攔截，同時完成漏洞通報與修補。

另外，Google之所以懷疑這起攻擊可能涉及AI，主要是因為攻擊程式碼呈現出多項異常特徵，包括：出現類似AI幻覺的評分內容、過於完整且教學式的註解風格、整體結構過於工整，甚至還包含一般工程師不會刻意加入的多餘說明。雖然目前還無法確認使用哪種AI模型，但這些特徵都讓研究人員認為AI可能參與其中。

資安戰升級 AI進入攻防加速時代

這起事件也顯示，AI已經不只是輔助開發工具，而是可能進入攻擊鏈的重要加速器。過去需要大量時間與專業能力才能完成的漏洞分析與開發，如今可能被大幅壓縮，讓攻擊者能更快在修補前出手。除了Google之外，Microsoft、OpenAI、Anthropic也正在強化AI安全機制，以防止技術遭到反向利用。

資安研究人員則認為，AI雖然可能還無法完全自主發現高階漏洞，但已經能縮短分析、測試、攻擊腳本生成時間。這也代表未來資安攻防的關鍵不再只是技術深度，而是反應速度，誰能更快發現、修補、攔截漏洞，誰就能在這場AI驅動的攻防中佔據優勢。

台灣企業臨「盲目導入*AI*」風險！*AI*催化駭客身份偽造升級三大威脅

駭客示意圖。路透社資料照片

陳俐妏*2026*年*5*月*4*日

企業透過*AI*驅動創新的同時，駭客也正利用*AI*技術讓網路犯罪從過往仰賴人工作業的模式，走向低成本、低門檻且可大規模複製的新模式。趨勢科技旗下全球企業*AI*資安領導品牌*TrendAI*指出，當今駭客結合內容生成、身分偽造與系統濫用的複合式*AI*威脅，讓企業既有的防護邏輯與管理模式面臨著前所未有的考驗。

企業追求導入*AI*的速度，卻容易忽略風險控管能力。根據*TrendAI*調查，*74%*的台灣受訪企業決策者坦言過去曾在高層要求或市場競爭壓力下，被迫核准在企業導入可能帶來資安風險的*AI*方案註一，卻只有不到一半的企業認為內部團隊能辨識惡意或異常的*AI*行為註二，顯示台灣企業正面臨「盲目導入*AI*」的高度風險。

***TrendAI*統整當代隨*AI* 演進的三大威脅，呼籲企業亟需提高關注：**

威脅升級一、內容生成武器化，假資訊與詐騙內容大規模量產

*AI*提供駭客以極低成本及大規模製造威脅的能力，讓今日的網路攻擊者不需親手撰寫程式碼，而是透過大型語言模型、*AI*代理將詐騙攻擊鏈自動化。*TrendAI*發現，網路攻擊者能以不到*10*美元的成本，自動生成大量看似可信的文字、影像與敘事內容，進一步用於釣魚詐騙、變臉詐騙*(BEC)*，甚至影響特定事件的輿論走向。

威脅升級二、身分偽造進化，企業招募與信任機制面臨新挑戰

在*AI*的助長下，身分冒用變得防不勝防，*TrendAI*預測深偽技術將越趨成熟且成本下降，未來將形成更難辨識、更容易被大規模濫用的局面。如今已有北韓駭客組織利用竊取而來的*LinkedIn*、*GitHub*等公開資料，搭配大型語言模型與深偽技術，偽裝成遠距*IT*工作者應聘，成功受聘後再進一步進行橫向移動、竊取機敏資訊，甚至發動勒索攻擊。駭客甚至會設立「假公司」進行反向釣魚，藉由發布假職缺面試真實求職者，並誘騙其下載惡意軟體，藉此竊取個資，甚至劫持真實帳號，以作為下一波假求職真攻擊的完美掩護。

個人資料保護法

數發部國家資安院淪陷! 內鬼植蠕蟲狂吸保密文件 二把手20萬元交保

（圖／翻攝畫面）

三立新聞網 的故事/2026/5/19 社會中心／莊芷榆報導
國家資通安全研究院爆發內鬼駭客案。前瞻研究籌獲中心副主任許世璋涉嫌指示下屬，於主機植入蠕蟲程式，越權撈取各類保密檔案，並上傳至雲端「許願池」供內部隨意取閱。檢調繼3月首波搜索後，於5月12日發動第二波偵查，約談許世璋等6人到案。台北地檢署漏夜複訊後，依涉犯妨害電腦使用及個人資料保護法等罪嫌，諭令許世璋以20萬元交保。

隸屬數發部的國家資安院於2023年掛牌成立，堪稱國家級資安專業技術單位，如今卻傳出自家主機遭「內鬼」攻破的難堪醜聞。據調查局追查，資安院內部原本設有嚴格的權限分級，但前瞻研發組經理彭敏君在2025年間，接獲建置行政系統的任務後，竟以前長官、現任副主任許世璋的指令為由，要求研究員丁柏楓等人動手腳。這群資安高手利用系統漏洞大舉「翻牆」，植入自製的蠕蟲與爬蟲程式，無差別狂吸各單位機密文件，並全數丟包到俗稱「許願池」的雲端空間，開放給其他同事隨意閱覽。

這起監守自盜案之所以曝光，起因於資安院進行內部稽核時，抓包彭敏君下屬的筆電出現異常數位軌跡。檢調指出，專案小組在今年3月率先發動首波搜索，將彭敏君與丁柏楓等人帶回，訊後分別以10萬至50萬元不等金額交保。原本外界以為彭敏君就是主謀，但檢方過濾扣案物證後，案情瞬間炸鍋，所有線索紛紛指向中心「二把手」許世璋才是幕後藏鏡人。

為釐清案情，新北市調查處在5月12日展開第二波收網行動，約談許世璋及其他涉嫌越級查閱文件的員工共6人到案。據了解，許世璋在偵訊時堅詞否認教唆部屬駭入系統，但檢調掌握的人證與物證已讓他百口莫辯。台北地檢署漏夜偵訊後，諭令許世璋20萬元交保，全案持續擴大偵辦中。

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

Q26　受委託蒐集資料，也要受個資法的規範嗎？

A　受委託者依然要遵守個資法的規定，若委託者是公務機關，則必須遵守個資法對公務機關的規定；若委託者是非公務機關，則適用對非公務機關的規定。

文/iThome

5月報稅季小心駭客！假冒免稅通知發動攻擊　資安院教你4招防範

（示意圖／PIXABAY）

SETN三立新聞網

2026/05/15 16:15

5月報稅季，資安院表示，有機關接獲以「免稅原則」等稅務議題為名的郵件，因人員誤信內容，導致設備遭植入後門程式，並出現連線中繼站行為。資安院提醒，涉及稅務、付款或附件下載的郵件，應提高警覺，避免開啟不明檔案或執行相關程式。

資安院近期資安週報示警，適逢報稅期間，駭客常利用免稅、退稅、稅務申報或補件通知等主題寄送社交工程郵件，藉此降低收件人警覺並提高點擊或下載意願。

資安院建議，針對潛在風險，機關可採4大措施因應，首先是強化郵件過濾與惡意附件偵測機制，降低社交工程郵件進入風險；其次為導入端點偵測與回應機制，即時發現後門程式與異常連線行為；再者，建立異常連線監控機制，阻斷設備作為中繼站對外通訊行為；最後也須加強人員資安意識宣導，提升對稅務主題郵件的辨識能力。

資安院提醒，涉及稅務、付款或附件下載的郵件，民眾應提高警覺，避免開啟不明檔案或執行相關程式，以降低受駭風險。