林業及自然保育署
臺東分署

公務機密
資訊安全維護

115年7月

目錄

柯達證實遭駭外洩公司資料，疑兩百多萬筆資料被竊

柯達證實近日遭未授權第三方存取公司資料，勒索組織*ShinyHunters*則宣稱竊得逾*220*萬筆紀錄，包含客戶個資與公司資料，並威脅公開

*iThome*文/林妍溱|*2026-06-18*發表

勒索軟體組織*ShinyHunters*宣稱駭入系統竊取客戶及公司資料後，影像器材大廠柯達（*Eastman Kodak*）昨（*17*）日證實遭駭。

柯達向*Bleeping Computer*證實被駭一事，表示近日發現一個未經授權的第三方人士非法存取了公司小部分資料一小段時間。該公司已立即和外部資安專家合作，調查遭存取與複製的資料範圍，並和執法機關合作。柯達並說有信心此次事件不影響公司系統或營運。

*ShinyHunters*本周稍早在其資料外洩網站公告駭入柯達，不過這群駭客宣稱竊得這家影像巨擘*220*萬筆紀錄，包含客戶個資和其他公司資料。*ShinyHunters*揚言若柯達未在*6*月*18*日前聯繫，將公開資料。

柯達未說明資料何以外洩。若依據*ShinyHunters*所言竊取了客戶資料及公司資料，*ShinyHunters*過去鎖定的攻擊及存取目標，包括*Salesforce*、*Snowflake*以及最新的*PeopleSoft*，都可能是造成柯達資料外洩的原因。*ShinyHunters*曾宣稱駭入上百家*Salesforce*客戶並且取得了*15*億筆紀錄。

*ShinyHunters*兩周來已先後宣稱，駭入了英國諾丁漢大學、歐洲理事會、教育平臺*Infinite Campus*客戶、保全巨人*ADT*、遊輪業者*Carnival*及教育平臺*Canvas*供應商*Instructure*等知名企業及組織。

*Google*控告濫用*Gemini*的中國詐騙集團*Outsider Enterprise*

*Google*控告中國網路犯罪集團*Outsider Enterprise*，指其利用釣魚工具包與包含*Gemini*在內的*AI*平臺，快速打造假網站與詐騙簡訊

*iThome*文/陳曉莉|*2026-06-15*發表

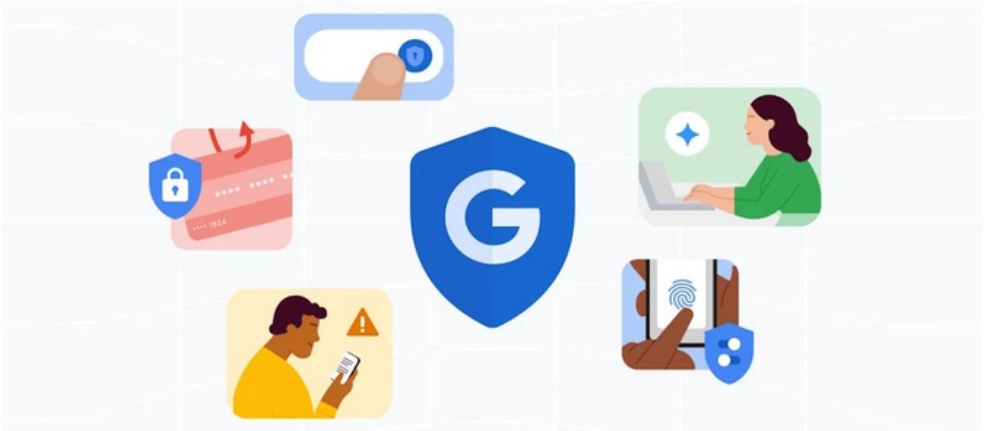
*Google*周五（*6/12*）向紐約南區聯邦地方法院提告，指控中國網路犯罪集團*Outsider Enterprise*透過*AI*工具與釣魚工具包建立大規模詐騙基礎設施，並以詐騙簡訊竊取受害者帳號、密碼與信用卡資料。

*Google*發布的新聞稿並未提及駭客的攻擊手法，而是僅以「*AI*驅動詐騙」（*AI-powered scams*）描述這起案件。然而，根據*TechCrunch*取得的訴狀內容，*Outsider Enterprise*為一網路犯罪集團，開發並維護名為*Outsider*的釣魚工具套件，*Google*將其稱為「傻瓜版釣魚工具」（*phishing-for-dummies*），內建*290*種網站範本，用戶只要每周支付*88*美元，或每月支付*200*美元訂閱費用，就能快速建立冒充電信業者、金融機構、政府機關及零售商的假網站。

*Outsider*還提供如何將*AI*生成程式碼武器化的教學文件，並支援使用*Gemini*等*AI*平臺產生客製化釣魚網站程式碼，再匯入*Outsider*平臺部署成可上線運作的詐騙網站。這些假網站可即時蒐集受害者輸入的帳號密碼、信用卡資料及多因素驗證碼。

*Google*指出，*Outsider Enterprise*並非單一犯罪組織，而是由釣魚工具開發者、受害者名單供應商、垃圾簡訊發送者，以及負責變現與洗錢的成員組成，形成完整的詐騙產業鏈；其成員透過*Telegram*協調運作，迄今已建立*9000*個假網站及超過*100*萬個惡意網域，並在兩周內向*Android*用戶發送*250*萬則詐騙簡訊，已有數十萬人受害。

目前*Google*正與*FBI*，以及*AT&T*、*T-Mobile*、*Verizon*等電信業者合作，試圖瓦解*Outsider Enterprise*的基礎設施，並在詐騙簡訊送達用戶前加以攔截。除了法律行動外，*Google*也呼籲美國國會通過多項反詐騙法案；*Google*表示，隨著*AI*讓詐騙內容變得更逼真、更難辨識，除了技術防禦與執法合作之外，也需要透過立法建立長期防護機制。



個人資料保護法

冒名慈濟醫院稱個資遭外洩！田警戳破「盜領藥物」經典騙局

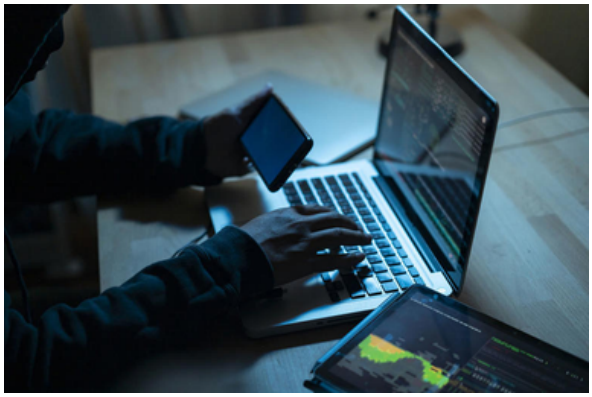
發布單位警察局
發布日期 *2026/06/17*
聯絡資訊 林分局長 *8756901*

田中分局田中派出所副所長張清權、警員黃逸翔及陳渝霈於日前執行巡邏勤務時，接獲一名民眾神色匆忙地走進派出所尋求協助與諮詢。民眾向警方表示，稍早其手機接獲一通顯示為未知號碼的來電，電話接通後，對方語氣嚴肅，自稱是「花蓮慈濟醫院」的行政人員。

該名人員在電話中聲稱，目前醫院櫃檯有一名男子，正持有報案人的身分證及健保卡雙證件「臨櫃申請領取高額藥物」，懷疑報案人的個人資料已遭到嚴重外洩或盜用。民眾聽聞後並未陷入恐慌，反而當機立斷向對方表示：「這件事情太過可疑，我現在要立刻打電話報警處理！」電話另一端的詐騙分子一聽到關鍵字，深怕東窗事發，隨即匆忙掛斷電話。民眾雖然成功嚇退對方，但因擔心自身證件與個資安全是否真的出問題，於是第一時間親自前往派出所向警方報案諮詢。員警聽聞事件經過後，隨即向民眾耐心解釋，明確指出這是詐騙集團的「假冒機構（醫療、健保局、檢警)」詐騙手法，詐騙集團常以「健保卡遭盜刷、身分證遭冒名領藥、申請醫療補助」等藉口恐嚇民眾，隨後便將電話轉接給假冒的「檢察官」或「警官」，以涉嫌洗錢、監管帳戶等連環套路誘騙民眾交付款項。經過員警細心解說民眾終於放下心中大石，感謝警方。

田中分局分局長林鼎超呼籲，醫療機構、健保局及警政單位「絕對不會」在電話中通知民眾身分證、健保卡遭冒用領藥，更不會要求在電話中核對個資或轉接警察局。民眾可至內政部警政署「打詐儀表板」（*https://165dashboard.tw/*）查詢最新詐騙手法與案例。如有任何疑慮，請立即撥打 *165* 反詐騙專線或 *110* 報案電話，由警方為您把關。

24億筆帳密外洩? 史上第二大資料外洩事件曝光 容量超過8.3TB



史上第二大資安漏洞曝光。(圖／VCG)

ETtoday新聞雲

ETtoday 的故事/2026/6/18 記者吳立言／綜合報導

全球資安領域再傳重大警訊。研究人員近日發現一個未受保護的 Elasticsearch 叢集，內部儲存高達 240 億筆資料紀錄，總容量超過 8.3TB，被認為是目前已知規模第二大的資料外洩事件。

規模僅次於「洩露之母」

根據 Cybernews 報導，研究團隊於 6 月 12 日發現這個公開暴露的資料庫。若以資料量計算，本次事件僅次於 2024 年曝光的「Mother of All Breaches（MOAB，洩露之母）」事件，當時整體資料規模約 260 億筆紀錄、容量約 12TB。

研究人員指出，資料庫內大部分內容來自資訊竊取惡意程式（Infostealer）蒐集的紀錄，其中包含電子郵件地址、使用者名稱、密碼，以及對應的登入網址等資訊。部分資料甚至以明文形式保存，增加遭不法利用的風險。

資料來自 36 個不同來源

調查顯示，這批資料整合自 36 個不同來源。其中，來自 Telegram 頻道的資料超過 17 億筆，另有約 2600 萬筆紀錄與名稱含有「Darkside」的頻道有關。

規模最大的資料區塊則被標記為「Collections」，包含約 22.6 億筆紀錄。研究團隊表示，目前無法確認這些資料究竟來自過往外洩事件整合，或是依照不同服務分類整理而成的帳密資料庫。

此外，資料庫中還出現約 1.5 億筆標示為「本地資料庫匯出（Local Database Dumps）」的內容，推測可能直接來自遭入侵伺服器的資料轉儲檔案。

受害規模仍難確認

由於研究人員尚未取得完整存取權限，因此無法確認資料中是否存在大量重複紀錄，也無法統計實際受影響的獨立使用者數量。同時，部分資料可能來自多年以前的外洩事件，因此其時效性仍有待進一步驗證。

截至目前為止，研究團隊仍未能確認資料庫擁有者身分，無法排除其為企業內部資料庫誤設公開權限，也可能是駭客組織或其他威脅行為者建立的資料集合。

使用者應提高警覺

雖然此次事件尚未確認有多少帳號受到直接影響，但資安專家建議民眾定期更換重要帳號密碼，避免在不同服務使用相同密碼，並盡可能啟用雙重驗證（2FA），降低帳號遭盜用風險。

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

Q27　可以任意使用所蒐集的個人資料嗎？

A　不行，僅能就蒐集個資的特定目的範圍內使用個人資料。例如在贈獎活動中蒐集到的個人資料，就僅能用於贈獎活動，不能做為其他用途。

文/iThome

韓國爆*ChatGPT*大規模盜刷 官方出手了

▲韓國近期接連傳出生成式*AI*服務*ChatGPT*高額訂閱費遭盜刷事。（圖／達志影像／美聯社）

*NOWNEWS*今日新聞/國際中心徐筱晴／綜合報導 的故事

韓國近期接連傳出生成式*AI*服務*ChatGPT*高額訂閱費遭盜刷事件，多名民眾在毫不知情的情況下，發現信用卡或金融卡被扣除*29.9*萬韓元（約新台幣*7000*元），而且皆為*ChatGPT*最高級別的*Pro*方案費用。根據統計，目前已確認超過*800*起疑似不法交易案例，涉及金額約*2.5*億韓元（約台幣*590*萬元），引發外界對信用卡資訊外洩與線上支付安全的憂慮。

根據韓媒*SBS NEWS*報導，韓國一名上班族本月*3*日突然收到金融卡扣款通知，顯示被收取*29.9*萬韓元的*ChatGPT Pro*月費，但他表示自己從未使用過*ChatGPT*付費服務，也從未在相關平台輸入過卡片資料。

受害者表示，當下感到相當害怕，不僅擔心個人金融資料已遭外流，也擔憂其他名下信用卡可能再次發生類似事件。

統計顯示，本月以來韓國境內共出現*1368*筆*ChatGPT Pro*方案交易，總金額約*4*億韓元，其中有*858*筆、約*2.5*億韓元被列為疑似盜刷案件。相關交易涉及包括樂天卡、*NH*農協卡、*KB*國民卡等*9*家主要信用卡公司。

專家指出，若掌握信用卡卡號、有效期限、持卡人出生日期以及密碼前兩碼等資訊，即有可能完成部分線上支付程序，因此推測不法人士可能透過外洩資料進行盜刷。

韓國東國大學國際資訊保護研究所教授黃碩鎮表示，駭客可能利用遭竊取的卡片資訊測試卡號是否有效，甚至在完成付款後，將取得的帳號或服務資格打包轉售，藉此牟利。

針對事件，*OpenAI*表示，經調查後確認並非*ChatGPT*在未獲用戶同意下自行扣款，而是遭竊的信用卡資訊被第三方非法使用，官方目前已緊急將受影響的支付管道進行封鎖。與此同時，*OpenAI*在韓國的電子支付代理商*NICE*資訊通信也積極展開應變，證實已對其中*700*多筆異常交易完成刷退退款，其餘爭議款項仍在持續調查中。該公司同時宣布，已暫時停止新增信用卡綁定及部分付款功能，未來將導入手機身分驗證程序，以提高交易安全性。

此外，韓國金融監督院也已要求各信用卡公司加強異常交易監控機制，防範類似事件進一步擴大。分析認為，此次大規模盜刷事件凸顯*AI*訂閱服務快速普及後所衍生的支付安全問題，也反映信用卡資料外洩風險依然存在。建議民眾定期檢查帳單紀錄，並開啟即時交易通知功能，若發現不明扣款應立即向發卡銀行申請停卡與爭議款項調查，以降低損失。