114年11月號

林業及自然保育署
臺東分署

公務機密
資訊安全維護

目錄

資安時事案例

駭客盯上甲骨文軟體　Google：逾百家企業恐已受害

示意圖。（圖取自Pixabay圖庫）

2025/10/10 07:22（10/10 07:32 更新）

（中央社華盛頓9日綜合外電報導）Alphabet旗下的谷歌（Google）今天指出，有100多家企業恐已遭受一項大規模駭客攻擊影響。駭客攻擊以甲骨文（Oracle）企業套裝軟體為目標，初步評估可能造成廣泛損害。

路透社報導，谷歌聲明指出，駭客「竊取了大量客戶資料」，攻擊行動可能3個月前就已展開。

谷歌表示，「這樣的攻擊規模顯示，發動最初侵駭的行為者很可能在攻擊前進行了大量研究與準備。」谷歌除了以搜尋、電子郵件與影音服務聞名外，也擁有規模龐大的網路安全業務。谷歌在部落格發文

指出，據信駭客組織CLOP是這次入侵事件主謀，曾多次對第3方軟體或服務供應商發動大規模攻擊。

谷歌分析師拉森（Austin Larsen）在回覆路透的聲明中表示：「我們目前已確認數十個受害者，但預期實際數量更多。根據CLOP以往攻擊規模來看，受害者可能超過100家。」

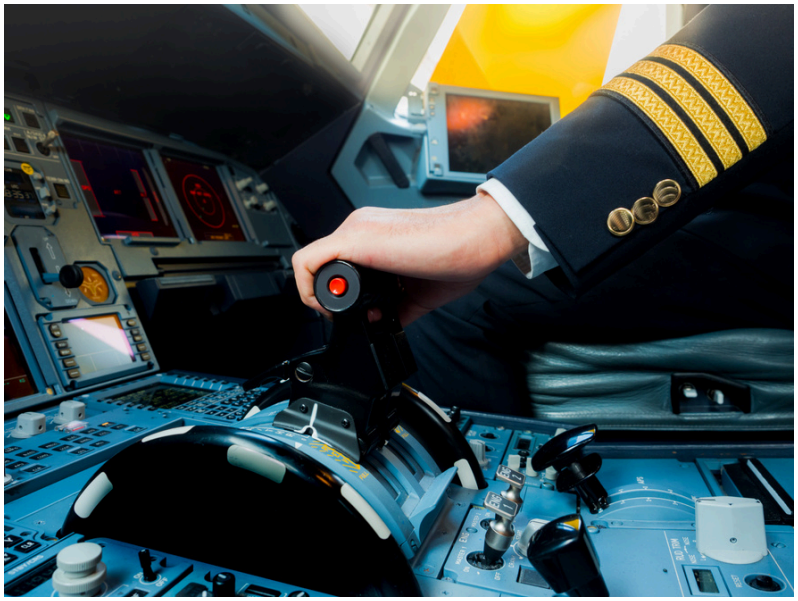
谷歌表示，駭客這次鎖定的是甲骨文E-Business Suite應用程式，這個套裝軟體被企業客戶用來管理客戶關係、供應商、生產、物流及其他業務流程。

甲骨文未立即回覆電郵置評請求，但先前證實發現針對其客戶的勒索行動。

CLOP也未回覆電郵置評請求。CLOP先前聲稱，很快就會證明甲骨文的「核心產品存在重大漏洞」。

（編譯：徐睿承）1141010

澳航：7月遇大型網攻　570萬個資已外洩網路



2025/10/12 13:16

（中央社雪梨12日綜合外電報導）澳洲航空公司今天表示，今年7月發生的大型網路攻擊事件中，遭竊的570萬名顧客資料已被駭客公開洩漏到網路。

法新社報導，澳航在聲明中表示：「澳航是全球眾多遭網路犯罪洩露資料的公司之一。這間公司先前在7月初遇駭，客戶資料透過第三方平台遭竊。」

澳航7月表示，駭客攻擊一個客戶服務中心，並入侵由第三方所使用的電腦系統。
這間澳洲績優公司表示，駭客成功取得客戶姓名、電子郵件地址、電話號碼和生日等敏感資訊的存取權限。

澳航今天表示這批資料已外洩至網路，現正與資安專家合作，調查外流資料的具體內容。
澳航也表示，已向公司總部所在地新南威爾斯最高法院（Supreme Court of New South Wales）取得法律禁制令，「以防任何人（包括第三方）存取、查看、發布、使用、傳輸或公布被盜資料」。（編譯：屈享平）1141012

個人資料保護法

BBC：開雲集團遭駭　Gucci等品牌恐數百萬客戶個資外洩

圖為法國巴黎一間Gucci門市。（路透社）

2025/9/16 19:07（9/16 19:35 更新）

（中央社巴黎15日綜合外電報導）英國廣播公司（BBC）今天報導，法國精品集團開雲遭駭客入侵，旗下品牌Gucci（古馳）、巴黎世家（Balenciaga）和Alexander McQueen合計恐有數百萬名客戶個資被竊。

路透社報導，開雲（Kering）透過聲明證實系統遭入侵，但未點名受影響的品牌。聲明表示，他們6月發現「某個無權限的第3方能短暫進入我們的系統，並從我們的一些品牌存取有限的顧客資料」。

據BBC報導，遭竊的客戶資料包括姓名、電子郵件地址、電話號碼、住址及在品牌門市消費總額。開雲也說，並無客戶的財務資料被竊，如信用卡號碼或銀行帳號等。

有群自稱「閃亮獵人」（Shiny Hunters）的駭客向BBC聲稱犯案，說他們握有與740萬個獨立電郵地址有關的個人資料。

這起駭客攻擊似乎與今年來精品和零售業者更大規模遇駭現象有關，受害業者包括瑞士歷峰集團（Richemont）的珠寶名錶品牌卡地亞（Cartier）及法國路威酩軒集團（LVMH）的一些品牌。

香港當局7月表示，他們正在調查路威酩軒的時尚品牌路易威登（Louis Vuitton）約41萬9000名客戶個資外洩事件。

開雲表示，受到這起事件影響的品牌，已立即依各地法規通知當局和客戶。至於有哪些國家的客戶受害，開雲則未予回應。（編譯：張正芊）1140916

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

Q19　蒐集個人資料時，要事先告知當事人嗎？

A　新版個人資料保護法增加告知義務，在蒐集個人資料時，必須先告知當事人。

文/iThome

Google與微軟用戶注意！職缺郵件詐騙橫行 駭客鎖定企業帳號竊取憑證


（圖／科技島資料照）

科技島Tech Nice/2025-10-16/記者孫敬／編譯
網路安全公司Sublime Security發布的一份最新報告揭露，電子郵件詐騙持續利用Google的假工作機會，誘騙使用Google Workspace和Microsoft 365並取得用戶登入訊息，其主要仿冒Google Careers的郵件，詳細調查結果已於10月14日發布。

這場詐騙通常以「您有空聊聊嗎？」的電子郵件開場，主要發送到企業的電子郵件地址，因為攻擊者還會過濾掉非商業用戶信箱。研究人員觀察到駭客不斷精進和調整他們的詐騙手法以躲過系統檢測。

詐騙手法越來越多，多國語言、假職稱、假介面、隱藏網頁格式
舉例來說，這些詐騙郵件不僅限於英文，也出現在西班牙文、瑞典文等多種語言版本。寄件人的姓名和電子郵件地址也頻繁更換，有時使用假招募人員名稱或部門，例如GG Careers hire@googleadjobhub.com。

研究人員指出，攻擊者濫用Salesforce和Recruitee等服務來發送這些郵件。惡意連結本身也多變，且通常託管在NiceNIC和Porkbun等網域。

如果收件人點擊「預約通話」的連結，他們將會進入多步驟的陷阱。首先，他們可能會看到一個假冒的Cloudflare Turnstile驗證頁面；接著，他們會被導向一個設計得像Google Careers會議排程器的頁面，要求填寫個人詳細資訊；最後，則進入竊取憑證的階段，這是一個模仿Google登入畫面的假登入頁面。

進一步探測揭露了詐騙者規避電子郵件安全掃描的隱密技巧，他們會隱藏網頁格式，將Google Careers這樣的詞語拆開，例如將每個字母放入單獨的標籤元素中。這種簡單的程式碼技巧使資安程式難以識別完整的惡意短語。

Sublime Security標示了短期註冊的網域
Sublime Security的偵測引擎成功阻止了這些攻擊，將它們標記為使用了在過去30天內註冊的網域上的連結。Netcraft 等網路安全公司最近也警告，以招募為主題的複雜詐騙顯著增加。因此，如果您突然收到一份看似優渥的職位邀約，在點擊任何連結或分享您的私人資訊之前，務必仔細驗證其來源。

資料來源：Hackread