113年6月號

公務機密
資訊安全維護

林業及自然保育署
臺東分署 政風室

公務機密 資訊安全維護

目錄

駭客宣稱濫用Dell網站API竊取近5千萬用戶個資

文/林妍溱 | 2024-05-13發表

上周電腦大廠Dell爆發4,900萬筆用戶個資外洩，媒體《Bleeping Computer》報導，駭客是利用Dell合作夥伴的API漏洞，得以竊取到用戶個人及設備資訊。

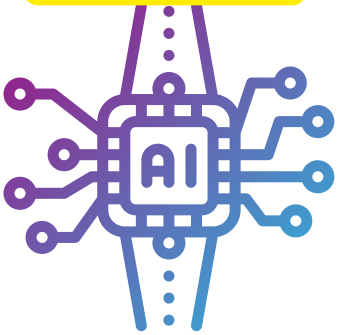
此事是在多名用戶反映接到Dell資料外洩的通知，疑似證實4月底《The Daily Dark Web》的報導。該報導指一名代號為Menelik的駭客在地下論壇上兜售4,900萬筆消費者個人及公司用戶資料，涵括用戶名及客戶號碼、住家地址、獨特的系統7位數服務標籤、出貨日期、監視器序列號碼、Dell訂單號碼等。這些用戶分布美、加、澳、中國、印度等國。

Menelik周五向《Bleeping Computer》透露取得這些資料的方法。他是先找到Dell提供給經銷商、零售商等合作夥伴的入口網站，然後以假公司身分註冊多個帳戶，這些只要到Dell網站上填上申請表即可存取網站，也無需驗證。駭客開發了一支能產生7位數服務標籤的程式，於3月上傳Dell入口網站，並利用該程式下指令查詢，並蒐集網站回傳的用戶資料。此外，由於Dell系統未設定流量限制，因此駭客以每分鐘5,000次呼叫網站長達3周，都沒有遭到Dell網站阻撓。

這名駭客也透露，外洩資料包含來自美、加、澳洲、中國與印度的個人及消費產業公司。他還透露，用戶使用的裝置涵括監視器、Chromebooks、Alienware、Optiplex、Latitude筆電、Inspiron筆電、Inspiron桌機、Poweredge、Precision、Vostro、XPS等品牌。

駭客並說在4月中曾以電子郵件聯繫Dell告知有漏洞，但始終沒有獲得Dell回應。他最後將部分資料上傳駭客論壇並求售。其貼文之後遭論壇版主刪除。
Dell回應媒體，證實有接獲駭客聯繫。Dell以已經報警，執法機關正在調查為由未透露其他細節，也說已經修正了網站問題。但Dell堅稱公司在駭客聯繫前即已偵測到惡意活動。

資安時事案例



資安即國安！勒索軟體攻擊暴增 大廠出招應戰

台北市 / 綜合報導華視
2024年5月14日

AI席捲各界，但像是「雙面刃」，一方面為產業帶來全新契機，不過另一方面，卻也讓透過「深偽技術」進行的詐騙更加猖獗，形成新的資安隱憂。調查顯示，去年全球多重勒索軟體攻擊，年增將近5成；今年第1季也有6家上市櫃公司，發布重大資安事件，像鴻海旗下半導體設備廠京鼎，1月就遭駭客入侵，顯現資安受威脅的嚴重性。今(14)日台灣資安大會登場，許多廠商都秀出自家解決方案，想協助如何面對資安危機。

CNN主播VS.AI深偽影片說：「前總統或他的法律團隊惡意行事。(這是深偽技術的實例，顯示強力電腦編輯能做到的。」AI仿造的CNN主播，看起來完全就是真人，強大深偽技術令人震驚，形成的資安隱憂怎能不擔心，像勒索軟體攻擊能力就大幅升級。

Palo Alto Networks台灣區總經理尤惠生說：「以前是數天內要反應，現在在數分鐘內就要反應了。」層出不窮的勒索舉動變得更快更猛，國際資安大廠Palo Alto Networks祭出解方，過去各種數據來源丟出的警示，可能超過三千多個，只要整合進AI驅動的平台，能先歸納串連成200多個「事件」，系統能做的就「自動化」解決，剩下的再由人類親自手動作業，直接把工作量降到剩60個，盡可能把處理時間縮到最短。

Palo Alto Networks台灣區總經理尤惠生：「過去在資安這三塊(雲.地.端)分別是有30幾種公司組成，所以管理起來非常複雜。現在收斂成我們一家，我們稱為「平台式」的資安。」台廠也積極開闢新路，像宏碁資訊喊出「資安左移新戰略」。

因為許多警報都是被攻擊了才發出，這時才想因應早就為時已晚，他們主打「預防勝於治療」，即早監測企業資安設備組態設定，一觀察到不對勁就馬上通報，舉例來說平常都用中文或英文的，突然跑出俄羅斯文，或是異常次數快速從個位數暴增到千位數，就會提早預警。

宏碁資訊總經理周幸蓉說：「不是只有告訴你(警示)喔，還可以給你行動SOP，一二三你應該怎麼做。地緣政治的關係，所以台灣處於非常特殊的地位，所以其實在這段時間也常常遭受到非常非常多的攻擊。」

最新調查發現，勒索軟體要求的贖金過去1年暴增5倍，而企業想恢復數據成本也激增百萬美元，另一份報告則顯示，2023年全球多重勒索軟體攻擊增加將近5成，聚焦台灣，製造業連兩年都是最主要攻擊標的，資安即國安，化解威脅成為顯學，容不得任何妥協。

個人資料保護法所保護的個人資料，是指自然人的姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別該個人的資料。

個資法所指的「個人」，是生存的自然人，因此個資法是保護自然人的個人資料，當自然人死亡後，其個人資料就不受到個資法的規範；另外，公司、法人等非自然人的資料，如公司的電話、地址，當然也不屬於個資法所規範的範疇。

個資法定義的個人資料中，醫療、基因、性生活、健康檢查、犯罪前科等5項屬於特種個人資料，基於特種個資的敏感性，個資法第6條嚴格規定不得蒐集特種個資，但這會導致許多產業的業務無法進行，例如保全業者無法過濾保全員是否有犯罪前科，幼教業者也無法確保工作人員是否有前科，運輸業者亦無法確認駕駛員的健康是否會影響行車安全等等。因此行政院暫緩實施第6條，待修法放寬可使用特種個資。

個資法施行細則對於病歷、醫療、基因、性生活、健康檢查及犯罪前科的個人資料，有進一步的定義，例如性生活的個人資料是指性取向或性慣行，犯罪前科的個人資料是指經緩起訴、職權不起訴或法院判決有罪確定、執行的紀錄。而病歷的個人資料，是指醫療法第67條第2項所列的各款資料，醫療的個人資料則是指病歷及醫師或醫事人員在診察、治療、處方、用藥、施術或處置所產生的個人資料。由於醫療個資的定義包含了病歷，然而醫療個資依第6條規定屬特種個資，但病歷卻未屬於特種個資，因此行政院將提修法，把病歷也納入特種個人資料的範疇。

個人資料除了上述的19項，還包括其他得以直接或間接識別該個人的資料，若有資料可透過與其他資料對照、組合、連結等，而可以識別出特定的個人，也屬於該保護的個人資料。

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

Q2 個人資料保護法何時開始實施？

A 個人資料保護法已於民國99年5月26日正式公告，「個人資料保護法施行細則草案」也於民國100年10月27日公告，但該法正式實施日期，仍待細則確定後，才公告。

文/iThome

8字元密碼超脆弱！專家曝「這長度」破解要100年

（記者周德瑄／綜合報導）網路科技不斷進步，駭客竊取密碼的手法也日益高明。根據美國資訊科技公司Hive Systems最新公布的2024年密碼破解時間表顯示，一組僅由8個數字組成的密碼，駭客只需短短37秒便可破解。然而，若密碼長度增加至16個字元，即使只包含數字，要完全破解也需耗費長達119年的時間。

示意圖／專家指出，駭客破解8字元的密碼只要短短37秒的時間。（擷取自pixabay）

專家指出，雖然現行網站普遍要求密碼至少8個字元，並需包含數字、大小寫字母及符號等不同字元類型，但這樣的要求標準已顯不足。他們建議，即使相對簡單，也應盡量使用較長字元數的密碼，才能大幅增加駭客破解的難度及所需時間，從而提高帳號安全性。

除了密碼長度之外，密碼使用情形也攸關重要。如果該密碼曾遭竊或在多個網站重複使用，甚至是常見單字組合，都會大幅縮短被破解所需時間。因此專家建議，密碼越強大且獨特，在未遭駭客攻破的情況下，即使長期使用也無須頻繁變更。

雖然較長密碼能提供更佳保護，但管理上也是一大挑戰。不過，現代網站皆設有各種防護機制，如限制錯誤嘗試次數、雙重認證等，可有效防範暴力破解攻擊。使用者也可自行至密碼強度評估網站，檢視目前密碼的安全程度。總括而言，創建一組強大且獨特的長密碼，並避免重複使用，比頻繁變更密碼更能有效防範帳號被盜的風險。