◎資訊安全宣導

—視訊軟體 Zoom 傳資安漏洞、電腦密碼也有遭竊風險—

因為武漢肺炎疫情影響，許多企業改以在家上班避免感染風險，也讓視訊會議軟體 Zoom 短時間內爆紅，但 Zoom 卻不斷傳出資安漏洞，據 Zoom CEO Eric S. Yuan 於部落格揭露，三月每日使用人數達到 2 億人，遠勝於去年 12 月的 1,000 萬。

資安網站 Bleeping Computer 發現，駭客可以透過 Zoom 的系統漏洞，輕易地遠端竊取用戶的 Windows 密碼。由於 Zoom 將 Windows 內部的 UNC（Universal Naming Convention）路徑設置為可以點擊的超連結，也因此若駭客刻意引導用戶，使其按下相關連結，就可以導致帳號、密碼外流，導致電腦門戶大開。專家分析，這項安全漏洞無需複雜的技術就能利用，使用者能暫時修改 Windows 設定避免受害，於 Windows 安全設定內，找到限制 NTLM 的選項，並將其改為全部拒絕即可。真正的關鍵仍是 Zoom 沒有禁止使用 UNC 連結，才導致用戶深陷安全風險。

至今 Zoom 爆發的安全漏洞還不只有一起，像是會將資料共享給臉書；程式存在安全漏洞，會讓駭客輕易獲得麥克風、攝影鏡頭使用權；於 macOS 版本的安裝程序，被批評類似於惡意軟體；視訊通話也被發現，沒有施行端到端加密。儘管官方陸續釋出誠意修補，但隨著 Zoom 爆紅、需求大增，眼下的資安防護自然也被放大檢視。由於線上使用人數大增，Zoom 本身又還沒有做好資安防護，使得成為網路駭客最新的駐紮平台。美國 FBI 建議，使用者最好不要使用公開會議，或是頻繁分享超連結，已經有多起案例，是駭客藉由 Zoom 發起網路攻擊，以搜集用戶個人資料。《路透》報導則指出，SpaceX 與美國國家航空暨太空總署（NASA），都開始基於安全理由，禁止職員使用 Zoom。

【文章擷取-自由時報】

臺中榮民總醫院提醒你!也關心你!