駭竊偽冒成挑戰

元宇宙興起催化資安商機

走進元宇宙會議室，你如何確定眼前的同事與主管就是本人，並非駭客假冒？元宇宙不僅延續既有網路資安議題，如駭竊及個資不當運用，更衍生出身分偽冒等多變的犯罪手法。儘管元宇宙看似危機處處，值得慶幸的是，資安科技也在與時俱進，而元宇宙所催化的資安商機，正蓄勢待發。

在元宇宙裡，不僅延續既有網路資安議題，如駭竊及個資不當運用，更衍生出偽冒等更多變的犯罪手法。

撰文／林玉圓

今年1月，臺灣一名彭姓男子入侵虛擬展覽空間，造成提供雲端展覽平台業者數百萬元損失，是國內首宗元宇宙資安事件；2021年12月，一名美國女性登入Horizon Worlds虛擬社群平台，「我上線不到60秒，虛擬分身就被3、4個男性騷擾，甚至還截圖上傳社群，」嚇得她立即脫下VR裝置。Horizon Worlds是由臉書母公司Meta所打造的元宇宙VR平台，消息傳出後，Meta立即為玩家設立「安全專區」，阻斷他人騷擾，僅允許擊掌等有限互動。

真人與演算法並用　遏止違規行為

截至2021年底，擁有近5,000萬每日活躍用戶（DAU）的遊戲平台Roblox，有半數玩家是13歲以下的兒少。Roblox坦言，開發元宇宙的重大挑戰之一，就是建立規則，避免遊戲場域成為「Wild West」（無序的蠻荒之地）。Roblox的解決之道是出動4,000名真人糾察隊，隨時巡邏遊戲平台，確保不會玩家不會遭受不當言語或要暴力對待；另也採用機器學習演算法，24小時檢舉不雅內容，並根據年齡來進行分級篩選。

上述案例突顯了元宇宙發展的幾項安全風險：虛擬資產遭入侵或竊取、虛擬分身的人身安全、兒少保護、甚至延伸到社會、性別議題等。

整合區塊鏈去中心化技術　提高防護門檻

工研院資訊與通訊研究所副所長花凱龍指出，「目前網路世界所存在的犯罪，都會持續發生在元宇宙，手法大致相當，甚至推陳出新，」他進一步說明，元宇宙資安風險主要分為兩大層面：駭客攻擊以及廠商不當使用資料。在駭竊及詐騙方面，傳輸面、人機互動面（駭客讓你的虛擬分身無法動作）、數位資產（NFT等有價資產）都可以是元宇宙不法之徒的攻擊切入點。花凱龍指出，網路駭竊原本已有相當技術門檻，進入元宇宙時代，若能整合區塊鏈等去中心化技術，防護門檻固然提高，但並不代表零風險。

另外還有廠商不當運用個人資料的問題。在元宇宙世界，透過感測器及穿戴裝置等人機介面，可以收集到更詳細多元的個資，例如動作、行為、生物特徵、週遭環境、甚至思考邏輯、移動習慣、社交圈等，一旦資料被不肖人士取得，恐怕將發展出更新穎的犯罪手法。

偽冒頻傳　身分驗證是最大挑戰

「元宇宙因採用虛擬分身，衍生出一個更大也更複雜的問題：身份驗證。」花凱龍以最簡單的遊戲場域為例，「如何得知你是與真人互動還是跟AI對打？未來學習場域進入到元宇宙，老師上課點名時，如何辨認登入者是學生本人，而不是找人頂替？」設想半導體大廠的研發會議中，若有商業間諜假冒身份參與，竊走營業秘密，公司的損失會有多大？近期引發名人圈恐慌的網紅換臉事件，就是採用Deepfake深偽技術，將公眾人物的臉孔嵌入不雅影片。

相較身份盜用更嚴重的，是進一步控制或誤導行為。舉例來說，為了達成高沉浸體驗，已有廠商研發腦波技術，讓嗅覺、味覺更加擬真，此時科技影響人腦的疆界應如何明確規範，才不致讓人腦被操控？或許腦波的控制在短期內無法實現，但眼前更可能的犯罪是：駭客竄改元宇宙的虛擬場景，致使使用者在真實世界跌跤受傷；也可能有駭客隱身登入元宇宙的跨國安全會議，企圖影響決策。

從開發、營運到行動應用　多層次強化資安

元宇宙的興起，使得虛擬與實體世界間，身分切換與驗證頻遭挑戰，相關技術如底層生物辨識、綁定裝置硬體晶片等防偽驗證機制因而更受重視。花凱龍指出，工研院累積多年資安技術開發經驗，在元宇宙時代，從軟體開發開始，導入安全軟體開發流程，主動驗證軟體套件安全；平台營運時，可自動化掃瞄驗證最新資安漏洞，依端點、網路到應用程式行為，套用「零信任白名單」管控機制，確保服務安全可靠；以行動裝置存取服務時，也能應用串流技術提供完整遠端存取，資料不落地，安全再升級。此外，針對元宇宙身分偽冒的新興議題，工研院也密切關注，目前也在發展與身分及裝置ID綁定技術相關的驗證架構。

元宇宙是一個全新的世界，不僅延續了原來的網路安全風險，還會衍生出至今尚未出現的資安議題。然而危機總伴隨著商機，元宇宙資安的威脅有多高，商機就有多大，在與駭客鬥智鬥法的過程中，創新科技將是重要解方。■

元宇宙因採用虛擬分身，衍生出一個更大也更複雜的問題：身份驗證。