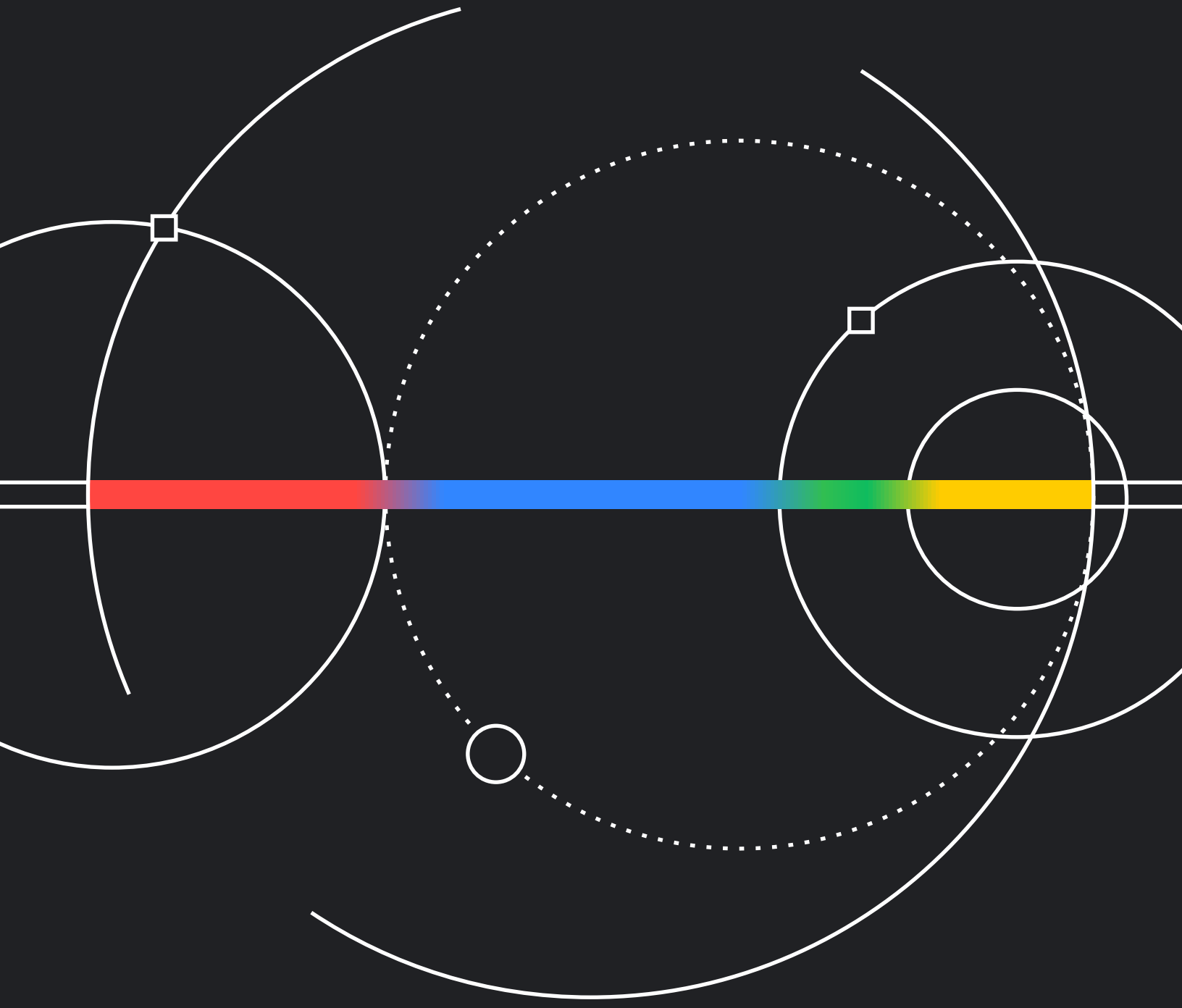
2026 年網路安全預測

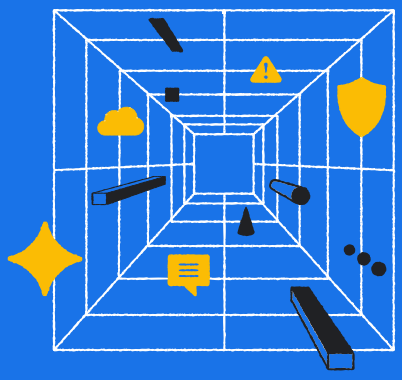
Google Cloud
Security



目錄

簡介

深入分析來年資安情勢時，我們從不憑空臆測，而是根據目前實際觀察到的趨勢和資料，彙整出清晰、符合現況的預測資訊，說明潛在的主要資安趨勢與挑戰。



這份《2026 年網路安全預測》報告著重三大主題：資安攻防雙方如何應用人工智慧、全球最具破壞性的網路犯罪威脅，以及國家級威脅發動者為達成戰略目標而持續採取的行動。

部分精闢見解來自 Google Cloud 的資安主管，包括 Sandra Joyce (VP, Google Threat Intelligence)、Charles Carmakal (Chief Technology Officer, Mandiant Consulting)，以及 Jon Ramsey (VP & GM, Google Cloud Security)。

這份報告也收錄了來自數十名研究人員、分析師、事件應變人員和專家的專業洞察，他們皆來自 Google Cloud 旗下的資安團隊，像是 Google Threat Intelligence Group、Mandiant Consulting、Google Security Operations 和 Google Cloud 資安長辦公室。從 Mandiant 的事件應變經驗到 Google 的全球威脅情報，這些獨家整合的第一手資訊，讓我們得以全面預測首要威脅和趨勢。

隨著科技推陳出新、威脅日新月異，資安局勢也瞬息萬變，因此資安防護團隊必須隨時調整做法，才能迎頭趕上。Google Cloud 為此推出《2026 年網路安全預測》報告，協助資安產業制定 2026 年的網路攻擊抵禦戰略。

人工智慧

全面運用 AI 的攻擊者

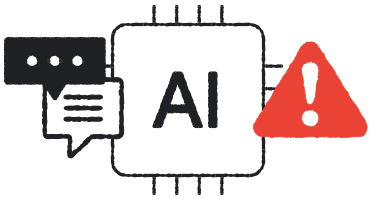
「**組織必須**做好準備，迎戰利用人工智慧的威脅與攻擊。」

Jon Ramsey
VP & GM, Google Cloud Security

邁入 2026 年後，威脅發動者利用 AI 的現象將從特例變成常態，因而大幅改變網路威脅態勢。根據 2025 年觀察到的事件與新型手法，我們預計發動者將全面運用 AI 提升行動速度、規模和效率，應用層面包括社交工程、資訊戰和惡意軟體開發。

此外，我們也預計威脅發動者會擴大採用代理系統，將攻擊生命週期各階段的行動自動化，藉此加速和擴大攻勢。資安研究領域也將更加關注其他類型的 AI 威脅，例如提示詞注入，以及直接鎖定 AI 模型的攻擊手法。

提示詞注入：操控 AI 的攻擊



AI 可望帶來前所未有的成長，但也會催生出更複雜的新型風險，而最主要的威脅之一就是提示詞注入。這類網路攻擊會控制 AI，讓模型繞過安全通訊協定，執行攻擊者暗藏的惡意指令。這不是日後可能出現的潛在威脅，而是已然存在的風險，且預計在 2026 年將大幅加劇。

隨著強大的 AI 模型日益普及，越來越多企業將相關技術導入日常業務，正好成為了這類攻擊的完美溫床。威脅發動者的技術日益精進，加上這類攻擊成本低、報酬高，因此自然成為首選手法。攻擊者將從概念驗證型漏洞攻擊，改為發動大規模的資料竊取和破壞行動，因此 2026 年預計將有更多企業 AI 系統成為首要目標。

Google 持續採取措施抵禦提示詞注入攻擊，包括採用多層次縱深防禦策略強化模型韌性，以及實施系統層級的防護機制。這些防護機制包括：運用機器學習內容分類器，從不受信任的資料中過濾惡意指示；強化模型安全思維，使其專注在使用者意圖；以及針對高風險動作，執行嚴格的輸出內容清理和使用者確認程序。

由 AI 技術支援的社交工程

到了 2026 年，我們預計 ShinyHunters (UNC6240) 等成熟的威脅發動者將加速利用 AI，進行極具說服力的社交工程，構成重大威脅。這類攻擊者在 2025 年能成功得手，關鍵就在於他們不需仰賴技術漏洞，而是專攻人性弱點，尤其是利用語音釣魚。未來的語音釣魚攻擊將利用 AI 聲音複製技術，生成逼真的偽聲冒用他人身分，而高階主管或 IT 人員往往會成為主要目標。

自 2024 年以來，威脅發動者便開始將 AI 廣泛應用到其他社交工程環節，隨著應用層面擴大，這類攻擊也會加劇。具體行動包括目標偵察、背景調查，以及生成逼真的網路釣魚訊息。由於這類手法主攻人性弱點，而非技術堆疊，因此發動者能避開傳統安全防護工具的偵測，利用 AI 發動大規模且高度個人化的攻擊。

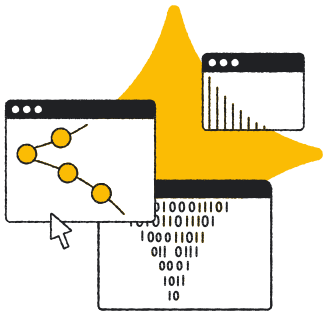
鑑於這類社交工程攻擊成效極佳，加上難以大規模逮捕發動者，達成殺雞儆猴的效果，因此就風險回報比來看，攻擊者將持續得利。由此預計，這類攻擊事件在 2026 年將變得更頻繁。資安防護團隊的當務之急，就是導入具備多重驗證與權限分配機制的程序，讓這類攻擊無機可乘。

AI 代理推動資安典範轉移

我們預計企業將在 2026 年快速導入 AI 代理，用於執行工作流程和制定決策；而傳統的安全架構並非針對 AI 代理設計，因此這項趨勢將引發新的資安挑戰。組織必須開發和導入完善的方法、架構和工具，才能有效管理新的 AI 生態系統，以及評估隨之而來的資安漏洞。

這場資安典範轉移的發展核心，就是身分與存取權管理 (IAM)。身分的概念將出現轉變，將 AI 代理視為自主的數位實體，而每個代理都會擁有獨立的受管理身分。如要順應這波轉型，就必須捨棄傳統的人工驗證和服務帳戶管理方式，改採更靈活、精細的控管機制。我們預計「代理身分管理」將成為新興趨勢，這類機制會採用可彈性調整的 AI 輔助系統，不間斷地評估風險，並隨時依環境變化調整存取權；目標就是盡可能減少權限蔓延的風險，並防止未經授權或不安全的行為。這類身分管理解決方案會遵循最小權限原則，只在有工作需求時，透過及時授予機制提供臨時權限，並透過可靠的委派鏈管理存取權。

資安分析師戰力大幅提升



企業將在 2026 年大規模採用 AI，徹底改變資安分析師的日常工作重心。我們期盼新的工作模式，能讓資安分析師不再被大量警報壓得喘不過氣，而是能主導代理執行工作，實現「代理資安營運中心」。所有第一線情報，都將成為這群 AI 工作夥伴的智慧中樞。事件應變人員收到的警報將附加由 AI 生成的事件摘要、模糊化 PowerShell 指令的解碼版，以及依據 MITRE ATT&CK 框架分析的結果。分析師的任務將從手動分析資料關聯，轉變為驗證 AI 提供的策略，因此核准 SOAR 防堵行動的時間，將能從數小時縮短至幾分鐘。

這套方法也能直接應用到威脅搜索和情報生成等任務。威脅搜索人員可以提出假設，以自然語言直接向 AI 代理下達指令，例如：「掃描整個組織環境，找出與 UNC5221 相關的 TTP (戰術、技術和程序)，並回報異常狀況」，AI 便會接手最繁重的任務，負責收集和比對 PB 規模的資料。情報分析師可以提供惡意軟體樣本和初步分析註記，指示 AI 代理草擬完整的威脅報告，並納入威脅發動者溯源分析及適用的緩解措施。將繁瑣工作交給 AI，分析師就能專注於宏觀分析和做出最終決策。簡單來說，應用 AI 的重點在於輔助人類分析師判斷，而非取代他們的工作。

「影子代理」的風險

我們預計精密的 AI 代理在 2026 年會變得更普及，進而導致目前的「影子 AI」問題升級為更重大的「影子代理」威脅。組織員工將無視公司是否批准，私自部署這類強大的自動化代理執行工作，衍生出不受監管的隱形機密資料管道，引發資料外洩風險、違規事件和 IP 竊取行為。

然而，禁用代理並非解決之道，因為員工會改用公司外部網路，脫離資安部門的監控範圍。最能防患於未然的策略，就是建立新的 AI 資安與治理規範，從一開始就融入安全考量的設計，建置防護措施。公司必須部署 AI 控管機制，才能安全地轉送和監控所有代理流量。成功的組織會創造允許運用 AI 創新的工作環境，同時落實可稽核的安全控管機制。

網路犯罪

勒索軟體和資料竊取型勒索

「**我們預計將出現更多**勒索軟體和網路敲詐事件，到了 2026 年會更加猖獗。」

Sandra Joyce
VP, Google Threat Intelligence

2026 年，勒索軟體、資料竊取和多面向勒索手法的組合，仍會是全球最具財務破壞力的威脅類型。除了事件數量居高不下，更是因為這類威脅會造成連鎖經濟影響，衝擊最初受害者以外的供應商、客戶和社群。舉例來說，2025 年針對零售和食品批發供應鏈關鍵節點發動的攻擊，就造成總共數億美元的損失，並嚴重影響了消費供應鏈。

這類活動的數量正急速攀升。2025 年第一季，資料洩露網站 (DLS) 列出的受害者數量就高達 2,302 名。這是我們自 2020 年開始追蹤這些網站以來，觀察到單季數量最高的紀錄，證實網路勒索生態系統已十分成熟。能達到如此規模，主要是因為主要犯罪團體採用了專業戰術，包括鎖定第三方供應商和利用零時差安全漏洞。光是鎖定代管檔案傳輸 (MFT) 軟體，網路犯罪分子就能同時攻擊數百個目標，從中竊取大量資料。

預計到了 2026 年，網路犯罪分子將繼續利用語音釣魚等初始存取策略，以及其他可鎖定對象的社交工程技術，躲過多重驗證 (MFA) 機制。他們可能會進一步利用零時差漏洞展開大規模的勒索行動，並透過更多新穎手法脅迫受害者支付贖金。

鏈上網路犯罪經濟

隨著金融業逐步採用加密貨幣和代幣化資產，並朝向全球區塊鏈經濟發展，我們預計威脅發動者將利用區塊鏈的不可變性和去中心化等特性，從中牟取龐大的經濟利益。加密貨幣和穩定幣的應用層面越來越廣，不僅使得傳統機構和創新公司的攻擊面迅速擴大，也導致加密貨幣原生解決方案和企業 IT 系統出現新漏洞。

我們預計去中心化金融 (DeFi) 平台和加密貨幣交易所，依舊會是攻擊者鎖定的高價值目標。具體行動包括大規模攻擊，以及結合數位資產竊取的供應鏈攻擊。犯罪者也會繼續攻擊產業規模持續擴大，且監管環境對區塊鏈有利的國家/地區，例如美國、東南亞和中東。

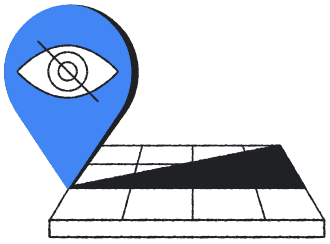
在接下來的幾年內，惡意攻擊者可能會開始將生命週期的核心環節遷移到公共區塊鏈，從傳統的惡意酬載傳送，轉變為使用 EtherHiding 等技術。攻擊者可能會全面利用 Web3 堆疊進行各種活動，包括動態命令與控制 (C2) 攻擊、去中心化資料竊取，以及透過代幣市場變現資產。只要將惡意活動遷移到鏈上，攻擊者就能大幅提升對傳統清除機制的韌性。

因此，防禦方式勢必得跟著調整。到了 2026 年，分析師和調查人員必須精通區塊鏈調查，所以需要培養追蹤交易記錄、解讀惡意智慧型合約的邏輯，以及執行錢包分析等新技能。

組織若疏於培養團隊的 Web3 基礎技能，就會無法及時辨識這類靈活的持續型威脅活動。

然而，區塊鏈的不可變性雖賦予了攻擊者韌性，卻也伴隨著無可避免的運作風險。無論是為錢包加值或部署合約，所有鏈上操作都會留下永久的公開稽核紀錄。這點正好讓資安人員在追溯源頭時能有所突破：透過重複使用的錢包地址或相似的合約位元碼，即使惡意行動相隔多年，也有機會可以找出之間的關聯，將防禦戰略轉向瓦解整個鏈上犯罪組織。

面臨威脅的企業虛擬化架構



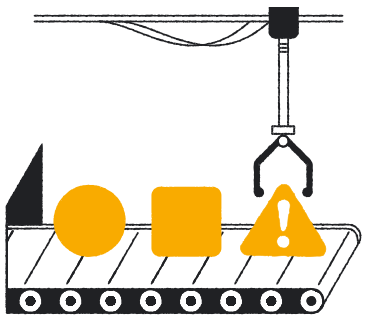
隨著客體作業系統的安全控管機制日益成熟，我們預測威脅發動者會將目標徹底轉移至底層的虛擬化基礎架構，主要藉此牟取經濟利益。這個基礎架構層長久以來都被視為可靠的屏障，如今卻成了防禦盲點，原因在於這類系統存在以下幾種漏洞：缺乏端點偵測與應變 (EDR) 解決方案的能見度、軟體版本過舊，以及套用不安全的預設設定。儘管資安團隊加強了使用者端點和客體內部系統的防禦，託管所有企業應用程式的核心虛擬化架構多半仍未受監控。如果管理程序與傳統的核心身分管理服務深度整合，這個基礎架構元件就成了防禦薄弱的進入點，一旦遭到攻陷，攻擊者就能掌控所有數位資產。

這項策略性轉變並非推測，而是實際在發生的現象。攻擊者正將目標轉向可最輕鬆攻破，同時帶來最大利益的系統。鎖定管理程序的攻擊意圖造成系統中斷，透過規避客體系統內部的 EDR，對基礎虛擬機器磁碟執行大規模加密，藉此癱瘓控制層，讓企業的營運系統全面停擺。這個攻擊面的最大特點在於執行速度：攻擊者在短短幾小時內，就能癱瘓數百個系統。相較之下，傳統的端點勒索軟體攻擊行動往往需要數天甚至數週，才能影響整個網路。

這個層級一旦遭到入侵，將造成嚴重的後果，除了影響規模更廣，偵測與應變時間也會大幅受到壓縮。因此，如果要保護往往遭到忽視的基礎架構層，組織就必須改變資安策略，不再以客體作業系統為營運中心，而是開發新的技術，直接在基礎設施層級抵禦這類不斷加劇的威脅。

Google 持續採取相關措施防範這類威脅，如 Google Cloud VMware Engine (GCVE) 會運用代管服務，並限制 ESXi 等底層元件的直接存取能力，進而強化安全性。這項服務可以將資安責任交給 Google，由我們持續監控漏洞，比起自行管理的解決方案更能有效縮小攻擊面。

首當其衝的 ICS 和 OT



2026 年，網路犯罪預計仍會是對工業控制系統 (ICS) 和營運技術 (OT) 最具破壞性的威脅。未來的勒索軟體攻擊可能會專門針對重要企業軟體 (例如 ERP 系統)，嚴重破壞對 OT 營運至關重要的資料供應鏈。這類攻擊之所以有效，是因為只要攻陷業務系統就能癱瘓整個工業環境，迫使受害者迅速支付贖金。此外，遠端存取等不安全的使用習慣，將讓常見的 Windows 惡意軟體得以繼續入侵 OT 網路。對特定目標發動的國家級攻擊雖然較少見，但若發生，依舊會涉及極度複雜的技術及特定地緣政治衝突。

資安防護人員的優先要務就是實施網路區隔，嚴格隔離 OT 和 IT 網路，防堵勒索軟體從企業端網路入侵。所有遠端存取行為都應採用多重驗證 (MFA) 機制和最小權限原則，阻擋攻擊者以盜用的憑證侵入系統。為確保復原能力，團隊應部署不可變更的離線備份系統，保存工業系統設定和重要企業資料 (例如 ERP 記錄)，並對重要的 IT/OT 路徑進行網路監控。

國家級威脅

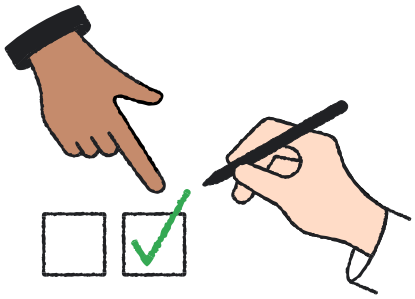
俄羅斯

「**國家級攻擊者**將繼續滲透組織，並長期潛伏在受害者的環境。」

Charles Carmakal
Chief Technology Officer,
Mandiant Consulting

邁入 2026 年後，俄羅斯的網路攻擊活動預計將會出現戰略性轉變，不再僅限於對烏克蘭衝突提供短期戰術支援，而是會優先考量長期的全球戰略目標。網路間諜活動不會停止，並會繼續優先鎖定烏克蘭政府和國防部門，藉此取得軍事行動或政治發展 (例如和平談判) 所需的關鍵情報，但攻擊的戰略目標預計將會擴大。

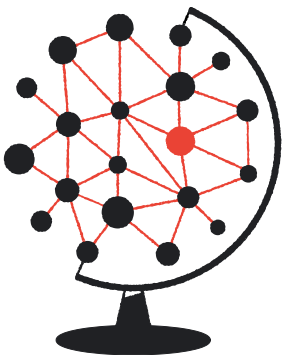
俄羅斯 2025 年持續在歐洲和北美進行網路間諜活動，且採用了新穎又有創意的戰術、技巧和程序，說明該國正將目標轉向長期發展先進的網路技術、收集有利於俄國全球政治與經濟利益的情報，並在國際重要基礎架構中取得戰略立足點。儘管自 2022 年以來，干擾性和破壞性網路攻擊事件的頻率有所下降，組織在 2026 年仍須對這項威脅保持警惕。



親俄攻擊者很可能會加強對美國和西方國家的資訊戰，並繼續鎖定俄羅斯的鄰近國家/地區。選舉仍會是攻擊的主要目標，波蘭、德國、加拿大和摩爾多瓦 2025 年選舉期間的行動就是具體例子。此外，攻擊者會透過這類資訊戰積極操縱新聞敘事，例如在羅馬尼亞宣布 2024 年總統投票結果無效後，散布西方國家涉嫌干預的說法。

親俄的駭客組織將繼續對 OT 環境構成無法預測的重大威脅，挪威 2025 年 4 月的水壩入侵事件就是一例。

中國



2026 年，與中國相關的網路行動數量預計將超越其他國家/地區。這種持續且頻繁的威脅活動，將繼續推動中國長期的戰略目標，包括維持內部穩定及擴大全球政經影響力。接下來一年，中國的網路威脅組織不僅會保持高度活躍，還會優先提升隱匿行動能力及部署創新技術。

我們預計與中國相關的網路間諜戰術、技巧和程序，仍會以提升行動規模和成功率為主要目標，且部分攻擊者還會試圖躲避防禦偵測。中國相關威脅發動者將持續積極鎖定邊緣裝置 (因為通常缺乏端點偵測和應變解決方案)，並利用零時差漏洞。第三方供應商也將成為首要目標，因為只要入侵一家受信任的合作夥伴，就有機會存取多家下游組織的系統，而且如果利用正當的合作夥伴連線，防禦方便無從偵測惡意存取行為。

這類行動會特別鎖定半導體產業：無論是競爭壓力、美國出口限制，或 AI 採用需求增加，都可能引發間諜活動，因此採分層網路防禦措施格外重要。

同時，親中的資訊戰行動預計會繼續操縱全球輿論，維護中國的戰略利益，尤其是以正面角度描繪中國，並貶抑美國、台灣、日本、韓國、越南、菲律賓和批評中國者。

伊朗

2026 年，伊朗預計會繼續發動網路威脅活動，藉此維持政權穩定，以及在持續不斷的地緣政治衝突中保持區域影響力。區域局勢因加薩衝突和 2025 年伊朗、以色列和美國交火持續升溫，這將助長針對以色列及其盟友的網路威脅活動、干擾性攻擊和資訊戰。

我們預計伊朗的網路行動將極具彈性、多面向且難以溯源，且會刻意模糊間諜活動、破壞行動、駭客攻擊和謀財型活動之間的界線。透過這種混合式戰略，相同的攻擊者和網路存取途徑就能用於不同任務，使防禦方難以抵禦和追溯攻擊源頭。另外，我們預計威脅發動者會延續自 2023 年 10 月以來的激進戰略，因此資料刪除程式風險將持續升溫。

在煽動中東衝突、分裂目標國家/地區，以及干預選舉方面，親伊朗的資訊戰行動將繼續扮演要角。這類行動會大舉利用假新聞網站，傳播支持德黑蘭政權的政治內容。利用 AI 生成內容，以及在社群媒體 (尤其是 Telegram 等平台) 大量假冒身分散布特定言論的行動，預計也將增加。在 2025 年 4 月的巴哈甘恐攻事

件爆發後，攻擊者改變宣傳論述，證實伊朗能迅速利用預先建立的基礎影響力架構，在全球出現新的緊張局勢之際靈活發動攻勢。

伊朗的核心目標預計將維持不變：持續監控反政權者、收集與伊朗或區域政治相關的實體和個人情報，以及鎖定有機會用於軍事方面的技術。

北韓

北韓網路威脅組織 2026 年的目標，預計仍會聚焦在獲取資金，以及針對美國和韓國等敵對國家/地區發動傳統網路間諜活動。

北韓的網路威脅發動者將針對加密貨幣組織和使用者，擴大發動十分有效且利潤可觀的行動。他們在 2025 年竊取了價值高達 15 億美元的加密貨幣，創下史上最高紀錄；這類戰術說明北韓將重點放在高報酬的網路經濟攻擊。我們預計北韓攻擊者將加速技術創新，包括誘導目標執行惡意程式碼，以及對雲端環境執行大規模內部偵察，藉此找出並竊取高價值資產。

這類行動將進一步利用進階社交工程，例如使用假的求職者評估網頁誘騙目標。此外，利用深偽影片建立信任並欺騙高價值人士的現象，也會更加普遍。

北韓 IT 人員的活動預計將繼續在全球 (尤其是歐洲) 擴張，且會調整策略規避日益嚴峻的法規要求，以及躲避美國不斷強化的偵測網。先前，北韓在美國利用「筆電農場」遠端存取資訊並隱匿位置，最終遭美國成功破獲；這項全球多點布局策略，正是對此事的回應。

此外，北韓 IT 人員的活動目標依舊不會僅限於賺取薪資，他們的目標還有濫用雇主的網路存取權並從中牟利，特別是從加密貨幣相關組織竊取加密貨幣。這類 IT 人員也會利用受僱人員的存取權進行戰略性間諜活動，例如透過開發 AI 技術的國防承包商竊取機密資料。

結論

無論是攻擊者或防禦方，都將在 2026 年跨入 AI 和網路安全的新時代。威脅發動者將利用 AI 提升攻擊速度、規模和效率，而資安防護團隊也會運用 AI 代理強化資安營運並輔助分析師。然而，這項變革也將引發「影子代理」風險等新挑戰，以及升級身分與存取權管理機制的需求。

為謀財而發動的行動仍會是主要的破壞來源，特別是勒索軟體和資料竊取型勒索。地緣政治方面，俄羅斯、中國、伊朗和北韓等國家將基於各自的戰略利益，運用多種網路戰術發動攻擊，帶來不斷演變的重大威脅。

組織要在複雜且瞬息萬變的網路環境有效應對威脅，就必須採取主動式多層防禦策略，落實 AI 治理，並根據新出現的威脅持續調整安全防護機制，確保營運韌性。

《2026 年網路安全預測》報告提供了重要的洞察和資訊，協助組織迎戰明年複雜的威脅環境。我們清楚闡明不斷發展的趨勢和潛在威脅，可做為領導者的行動方針，從被動防禦升級至更具韌性及遠見的安全防護策略。

貢獻者

《2026 年網路安全預測》報告收錄了以下 Google Cloud 資安主管的分析洞見：

Sandra Joyce
VP, Google Threat Intelligence

Charles Carmakal
Chief Technology Officer, Mandiant Consulting

Jon Ramsey
VP & GM, Google Cloud Security

本報告的貢獻者包括數十名來自不同 Google Cloud Security 團隊的研究員、分析師、事件應變人員及專家：

Josh Atkins
Bhavana Bhinder
Doug Bienstock
Sarah Bock
Pierre-Marc Bureau
Michelle Cantos
Stuart Carrera
Anton Chuvakin
Tom Curry
Odun Fadahunsi
David Grout
Adrian Hernandez
Jose Hernandez
Scott Henderson
Joshua Kim
Martin Lawther
Steve Ledzian
Yihao Lim
Keith Lunden
Mark Magee
David Mainor
Stuart McKenzie
Thiébaut Meyer
Jordan Nuce
Josh Palatucci
Christiane Peters
Fred Plan
Alice Revelli
Gabby Roncone
Cameron Sabel
James Sadowski
Nick Schroeder
Chris Sistrunk
Genevieve Stark
Kelli Vanderlee
Alden Wahlstrom
Jess Xia

Google Cloud

如需更多資訊，請前往 cloud.google.com