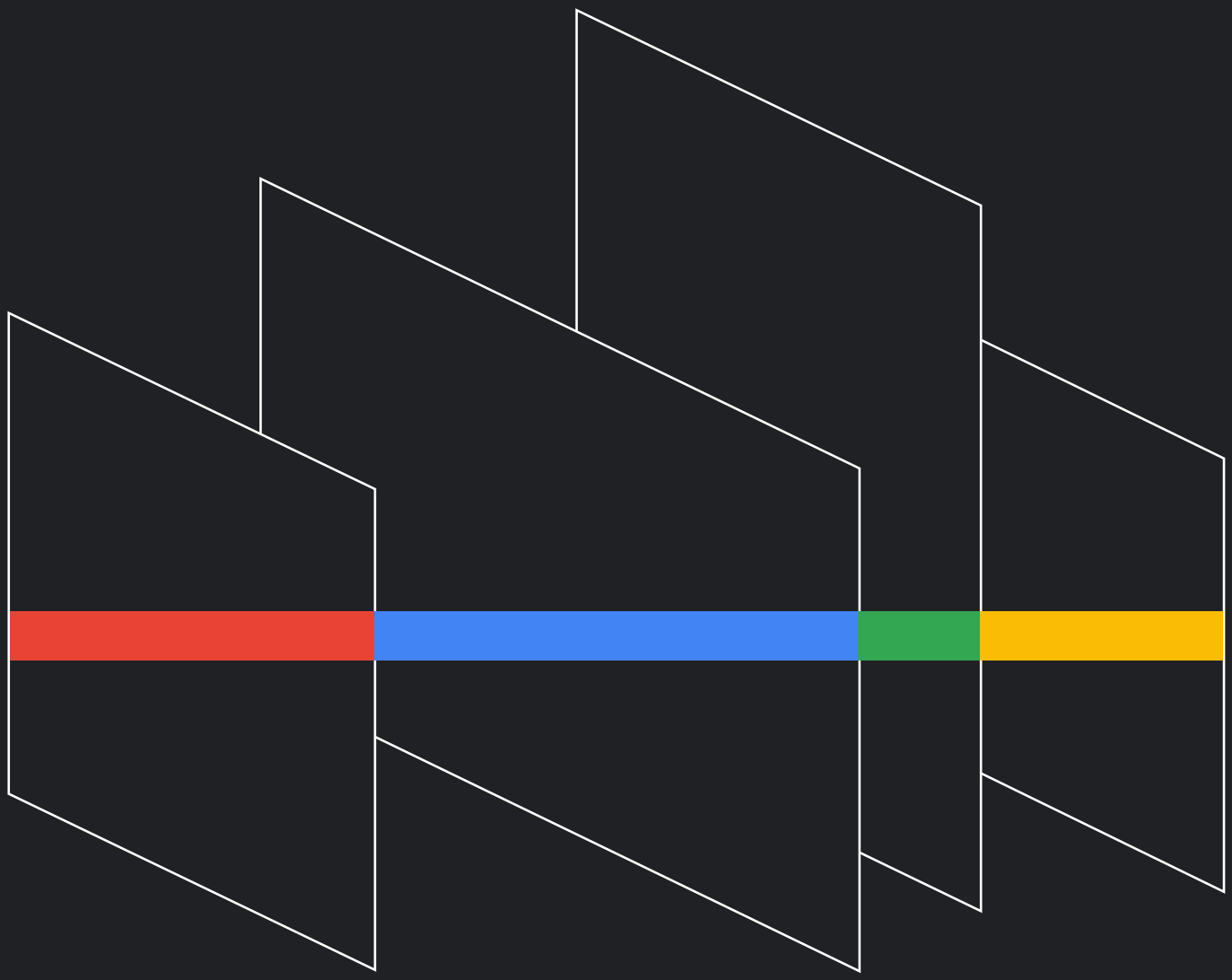
2025 年網路安全預測

Google Cloud
Security



目錄

引言

觀望來年時，我們從不妄自預言，而是會著眼於所見趨勢，實際指出在網路安全這個廣泛領域中，預期會有怎樣的發展。

《2025 年網路安全預測》報告彙整了各種前瞻性深入分析，這些精闢見解來自 Google Cloud Security 主管，包括 Google Cloud Security 團隊的 VP/GM Sunil Potti、Google Cloud 的 Google Threat Intelligence 部門 VP Sandra Joyce、Google Cloud 的 Mandiant CTO Charles Carmakal，以及 TI Security VP 暨 Google Cloud CISOPhil Venables。

這份報告也收錄了數十位研究人員、分析師、應變人員及專家的真知灼見，他們來自數個 Google Cloud Security 團隊，包括 Google Threat Intelligence、Mandiant Consulting、Google Security Operations、Google Cloud 資安長辦公室和 VirusTotal 等。這些人員經常站在第一線，知道機構和資安團隊應優先考量哪些重點，才能因應來年的挑戰。

隨著科技推陳出新、威脅日新月異，網路安全局勢也瞬息萬變，因此防禦時必須有效調整適應，才能迎頭趕上。Google Cloud 提供《2025 年網路安全預測》報告，協助網路安全產業制定 2025 年對抗網路攻擊的戰略。

人工智慧

「**2025 年**是 AI 在資安領域實際邁入第二階段的**第一年**。」

Sunil Potti. VP/GM, Google Cloud Security

攻擊者如何使用 AI

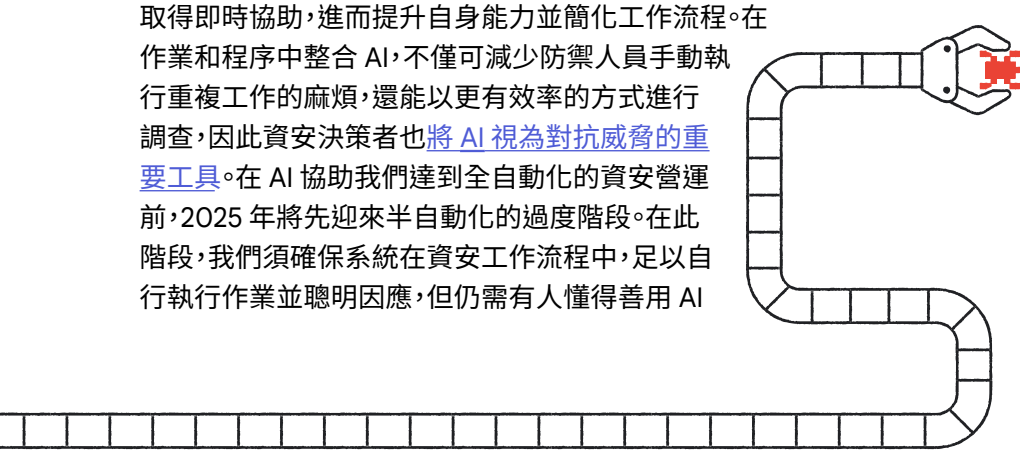
明年，惡意行為人預計會繼續快速採用各種 AI 工具，在攻擊週期的各個階段，強化並輔助線上攻擊行動。我們會看到他們繼續使用 AI 和大型語言模型 (LLM)，研發更逼真的網路釣魚、語音釣魚、簡訊和其他社交工程攻擊手法，規模也會更大。網路間諜和網路犯罪策動者應會繼續利用深偽技術，規避客戶身分驗證 (KYC) 的安全性規範，藉此盜用身分和從事詐欺。預計也會有更多實證，指出惡意行為人嘗試找出 LLM 和深偽技術應用程式的其他用途，包括研究安全漏洞、開發程式碼和偵察等。此外，在地下論壇中，對於缺乏安全防護機制的 LLM 需求預期會增加，讓威脅策動者可以無限制地查詢非法主題。隨著 AI 功能在 2025 年更加普及，這些入侵行為將日趨頻繁且效果顯著，讓企業更防不勝防。

運用 AI 展開資訊戰

為了支援資訊戰，這類威脅策動者會日益仰賴生成式 AI 工具。AI 功能的部署作業已不再只是像早期利用生成式對抗網路 (GAN)，建立假帳號背後的個人資料，而是已擴展至運用 LLM 支援內容創作，在造假的網站上製作並發布看似真實的文章。這使策動者能更大規模地製作這方面的內容，創造更多模糊空間。我們預計此趨勢會持續，這類策動者很可能利用日益普及的生成式 AI 工具達到各種目的，包括大規模建置內容、生成更具說服力的內容和假帳號。

AI 和資安領域的下個階段

2025 年，我們預計會看到 AI 和資安領域進入第二階段的實際運作。過去一年來，從業人員已透過 AI 將資安措施普及化，意即開始運用 AI 工具，自動為複雜的報告產生摘要、輕鬆查詢龐大的資料集，並在從事多種工作時取得即時協助，進而提升自身能力並簡化工作流程。在作業和程序中整合 AI，不僅可減少防禦人員手動執行重複工作的麻煩，還能以更有效率的方式進行調查，因此資安決策者也將 AI 視為對抗威脅的重要工具。在 AI 協助我們達到全自動化的資安營運前，2025 年將先迎來半自動化的過度階段。在此階段，我們須確保系統在資安工作流程中，足以自行執行作業並聰明因應，但仍需有人懂得善用 AI 支援，以收事半功倍之效。這包括要能剖析警告 (即使是誤報情形)，建立最高優先事項清單，讓資安團隊能夠進一步分類並修復最嚴重的風險。



四巨頭

> 「**地緣政治衝突**將繼續在全球各地助長網路威脅活動，讓網路環境日趨複雜。」
>
> Sandra Joyce.
> VP of Google
> Threat Intelligence
> at Google Cloud

俄羅斯

2025 年，烏克蘭衝突可能仍是俄羅斯網路間諜行動、網路攻擊和資訊戰的關鍵所在。2024 年的記錄顯示，鎖定烏克蘭士兵行動裝置的攻擊有所增加，發動者可能試圖取得戰術情報，支援武力作戰和其他常規軍事活動。雖然情況不如 2022 與 2023 年頻繁，但仍能持續觀察到干擾性攻擊，包括針對各種關鍵基礎設施營運業者的攻擊，以及利用 CyberArmyofRussia_Reborn 等駭客人物的身分宣傳威脅活動。我們預計這類攻擊行動會持續到明年。

幾乎可以肯定的是，除了攻擊烏克蘭，俄羅斯的網路間諜也將繼續支援莫斯科取得全球利益，主要鎖定歐洲和北約成員國的政府機關、政治人物、民間團體、記者、媒體管道及技術機構。親俄方的資訊戰也將持續運用各種戰術，使俄羅斯獲得更多利益，並削弱對手力量，同時趁重大活動舉行之際圖謀不軌，正如我們在 2024 年巴黎夏季奧運期間看到的情況。

中國

過去十年，中國有許多機構投資贊助網路威脅策動者，可能會在 2025 年持續助長威脅活動，質與量兩方面都有增長趨勢。我們將繼續觀察親中策動者使用的隱匿戰術，包括運用營運中繼箱 (ORB) 網路掩蓋目標環境中策動者的進出流量；鎖定網路邊緣裝置，藉此利用網際網路暴露的脆弱攻擊面，並減少目標環境中的相關足跡；以及在國家層級以工業化的方式蒐羅軟體安全漏洞，趁機發起零時差安全漏洞攻擊。此外，我們預計中國政府資助的策動者將繼續虎視眈眈，並展現承受高風險的能力。

親中資訊戰則將直接鎖定中國視為首要戰略重點的國家/地區，特別是以台灣和美國的選舉/選民為目標。相關活動包含冒用選民身分、宣傳選票遭操縱的不實資訊，以及主打 AI 生成新聞主播的影片內容。這類資訊戰無法有效促成真實互動，因此僅有少數成功案例。不過，在言語論述和戰術方面仍具侵略性，包括採用人身攻擊和威嚇的方式。

伊朗

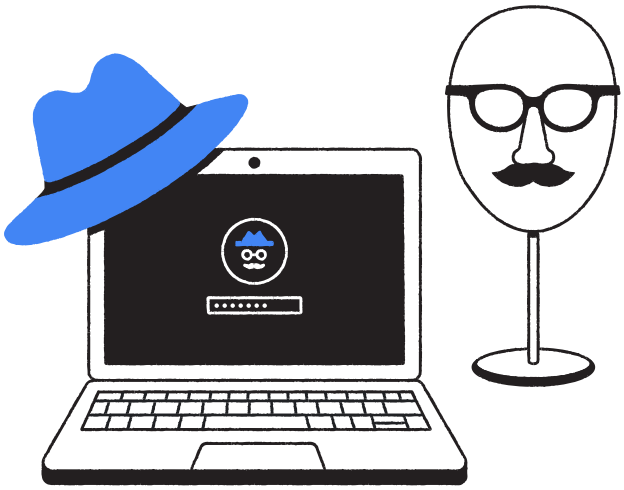
只要哈瑪斯和以色列持續爆發衝突，伊朗政府資助的網路威脅活動就可能會繼續主導局勢，助長網路間諜行動、干擾性和破壞性攻擊，以及資訊戰。然而，這與伊朗威脅策動者長期一貫的攻擊行動不無衝突，他們仍持續鎖定中東與北非地區的政府機關和電信業者，甚或涉足網路犯罪。我們確信，政權穩定、經濟發展和區域影響力等長期以來的目標，將繼續助長監控機制，加強監管異議人士、與伊朗/當地政治密切關聯的重要人士和機構，以及可能支持伊朗軍事力量的技術方。

北韓

我們預計地緣政治和經濟需求，將推動北韓的網路攻擊行動到 2025 年以後。

北韓的網路間諜行動將繼續支持該國的地緣政治目標，包括主要鎖定南韓和美國的政府、國防、教育和智庫，同時對英國、德國、澳洲、中國和俄羅斯也有一定的關注。2023 和 2024 年，北韓策動者的重點是供應鏈入侵，通常鎖定軟體開發人員，在社交工程攻擊行動中使用含木馬程式的開放原始碼軟體套件，這類手法應會持續到明年。

北韓的策動者也將繼續利用 IT 工作人員牟利及竊取加密貨幣。IT 工作人員會運用盜取和偽造的身分，應徵高薪軟體開發工作。值得注意的是，這些 IT 人員還會利用特殊權限存取雇主的系統，展開惡意網路入侵，此趨勢亦將持續至明年。



全球預測資訊

中國的策動者將繼續部署自訂惡意軟體生態系統，入侵嵌入式系統

端點偵測與回應 (EDR) 平台一向是機構資安架構的重中之重，有助公司掌握端點活動情形，是有效執行安全監控的重要工具。為了規避偵測機制，中國的間諜行動策動者往往會開發可高度自訂的惡意軟體生態系統，以利入侵嵌入式系統，因為這類系統通常尚未部署 EDR 解決方案，且不利傳統數位鑑識與事件應變。我們發現，他們在來年仍持續展現此傾向，且依舊駕輕就熟。相關例子包括防火牆和 VPN 閘道等邊緣裝置，或交換器和路由器等內部網路裝置。中國策動者設計的這類惡意軟體生態系統，不僅具備目標平台/作業系統限定的附加功能，同時也還運用基礎作業系統的原生功能。這些生態系統可含多種不同元件，彼此間會共同作業，提供所需功能。

2025 年，中國的策動者仍會依此策略部署自訂惡意軟體，進而利用隱蔽的後門程式存取各種環境，例如在合法的服務中植入木馬程式，靜候攻擊者順利連線。此外，他們還會利用 rootkit 等低階惡意軟體，隱藏攻擊活動的證據並阻礙調查工作。

威脅不會消失：勒索軟體和多面向勒索

2025 年，勒索軟體、資料竊取勒索和多面向勒索仍將是全球最具干擾性的網路犯罪類型，原因在於事件量和各事件的潛在破壞範圍有增無減。此外，勒索軟體和勒索行動帶來的影響也會持續擴大，不僅止於最初受害者。醫療照護產業在 2024 年發生了重大勒索軟體事件，對醫院病患的照護品質產生負面影響，患者無法繼續領取重要處方，同時也妨礙醫師執行關鍵的實驗室檢測，或向保險公司申請費用。

現有證據顯示，截至 2024 年，勒索軟體和勒索行動已影響超過 100 個國家/地區和各個產業別。2024 年新發現的資料外洩網站 (DLS) 數量比 2023 年多一倍，而多項新的勒索軟體即服務 (RaaS) 產品出現，說明了勒索軟體和勒索威脅環境正蓬勃發展且日益猖獗。

> 「**無庸置疑**，多面向勒索攻擊和勒索軟體會在 2025 年持續肆虐，且美國境外的案例可能有所增加。」
>
> Charles Carmakal.
> Mandiant CTO,
> Google Cloud

美國大選後的威脅活動

2024 年，各種以美國總統大選為目標的攻擊活動陸續展開，這些行動在大選結束後也不會立即停止。從今年下半年到 2025 年，中國、俄羅斯和伊朗都將繼續鎖定美國政府，可能利用新總統上任之際，企圖爭取決策優勢。我們預計將繼續看到政府資助的網路間諜行動，以及在社群媒體和其他平台上推廣政治分化內容的資訊戰。而生成式 AI 工具，更讓策動者擴大這類行動的規模和效果，因此這些攻擊行動在現今選舉中可能比以往更為普遍。

發掘過去幾年的攻擊行動

我們預計在 2025 年找出並協助修復一些已持續一段時間的入侵問題，特別是要找出更多最初發生在 2024 年，甚或更早前的中國相關入侵行動和間諜攻擊活動。我們發現與中國關聯的間諜組織非常擅長隱藏行蹤，且會長時間潛伏於網路環境中，我們的團隊有時會在威脅策動者入侵機構多年後，才碰巧發現他們存在。

惡意軟體竊取資料的威脅與日俱增：為重大資料侵害事件大開方便之門

利用惡意軟體竊取資料雖然不是新興的威脅手法，但在複雜性和效果方面都令人更加憂心。2024 年，威脅策動者發動大規模的資料竊取行動後，利用得手的憑證滲透了大量重要機構，導致多起影響深遠的入侵事件。令人擔憂的是，甚至是初階的威脅策動者都能透過這些工具取得憑證，更有可能造成大規模影響。

我們預期，使用遭竊憑證入侵的情況將持續到 2025 年，而資料竊取工具仍會是取得這些憑證的主要媒介，特別是在尚未強制執行雙重驗證的環境中更是如此。一旦缺少這層額外的安全防護機制，機構就容易受到不同程度的資料侵害影響。此外，近年來反防毒技術日新月異，繞過端點偵測與回應 (EDR) 的功能推陳出新，資料竊取的惡意軟體也日趨複雜，成為我們面對網路威脅局勢時，更棘手的挑戰。

在混合式環境中盜用身分的影響日益加劇

隨著現今整合地端和多雲端架構的身分管理方式發展，身分遭盜的整體影響將加劇，導致機構面臨更大風險。2025 年，機構勢必要整併資安程序、安全控管機制和驗證工作，盡可能降低單一身分盜用事件後續帶來的整體影響，同時也得制定更有效的高強度驗證策略。

在過去，驗證程序通常是由密碼和單一驗證機制組成，會以單次處理的方式，對已建立的身分進行驗證。現在，有鑑於攻擊行動的分散性，機構在驗證處理期間，必須從單一驗證改用含多個驗證標準的機制。需強化的部分不僅應聚焦在執行驗證要求的身分 (使用者) 方面，還可能需針對與該身分相關聯的裝置，採取更嚴謹的防範網路釣魚多重驗證 (MFA) 機制。此外，縮短存取敏感資源或應用程式時的工作階段週期 (重新驗證)，以及執行身分風險審查和驗證也不可或缺。

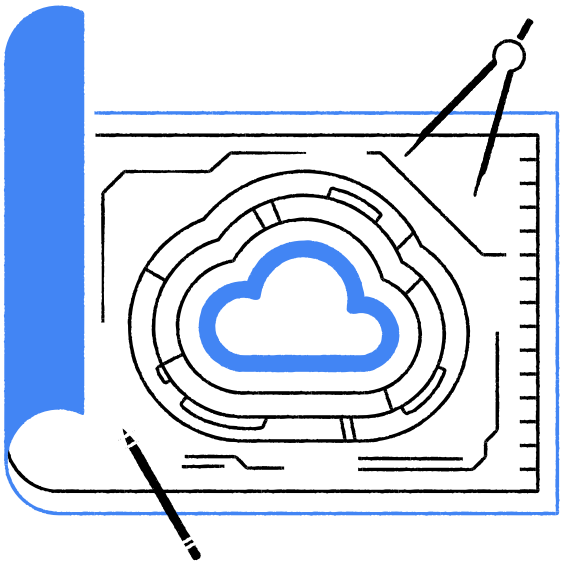
機構在遵循這個模式後，除能適當加強防護機制並降低影響，在處理與授權活動相關的驗證程序時，也能更加放心。

網路能力普及化，將持續使新手發動威脅的技術門檻降低

2025 年，對於技術較不純熟的網路犯罪者和政府支持的策動者來說，會有越來越多技術門檻逐漸降低，機構將繼續面臨此局勢帶來的挑戰。隨著越多工具、網路釣魚套件和「即服務」資源整合先進功能，縱使是技能不足的威脅發動者和新犯罪者，當他們參與惡意網路活動後，也有機會強化技能，高效展開攻擊行動。而網路側錄攻擊、規避多重驗證等服務走向專業化，也使防禦者面臨更多威脅策動者。此外，這些策動者會在攻擊週期的各個階段，使用生成式 AI 不斷實驗，這也讓攻擊者在資安作戰中占盡優勢，發揮更大效用。

雲端的資安營運做法日趨成熟

2025 年，會有越來越多機構採用雲端原生的安全資訊與事件管理 (SIEM) 解決方案。擴充性和成本效益是幕後功臣，即使是還在猶豫是否淘汰地端部署作業的機構也會選用。我們預期 SIEM 會再度成為資安營運中心 (SOC) 的中樞神經系統，負責擷取從雲端記錄到端點遙測的所有資料。資安調度管理、自動化與應變 (SOAR) 往往是 SIEM 的一環，也可能會執行基礎應對以外的作業，處理更複雜的事件應變事宜，包括自動分析惡意軟體、移除網路釣魚內容，甚至是在遭到攻擊前修補漏洞。此外，身分與存取權管理 (IAM) 的設定錯誤、無伺服器的安全漏洞，以及容器跳脫等雲端特有威脅，將隨專門設計的工具和策略出現而迎刃而解。



安全防護事關重大，雲端服務供應商須遵守更多法規

隨著改用超大規模雲端服務的重大基礎設施增加，越來越多監管機構會直接鎖定全球雲端服務供應商 (而非僅針對客戶)，要求他們的雲端服務須符合特定控管規定與韌性標準。2025 年，雲端服務供應商將面臨更多規範，也更加備受期望。由於這些供應商的角色愈發重要，加上移至超大規模雲端 (包括 Google Cloud) 的服務普遍增加，呈此趨勢不無道理。

Web3 和加密貨幣更常淪為竊盜目標

隨著 Web3 和加密貨幣組織在 2025 年後持續增加，攻擊者應會繼續鎖定智慧型合約的安全漏洞，竊取並盜轉私密金鑰。Web3 組織對攻擊者來說是高價值目標，自 2020 年以來，報導指出已發生數百起 Web3 盜轉事件，導致 120 億美元的數位資產遭盜。

我們預計，朝鮮民主主義人民共和國 (DPRK) 的威脅策動者在鎖定 Web3 組織及供應鏈時，將會繼續利用社交工程戰術，建立初步立足點。Web3 公司必須在強化安全控管措施及全天候監控方面投注心力，力求及早偵測攻擊，防範盜轉事件。

更快發動漏洞攻擊，更多供應商成為目標

2024 年，我們對 2023 年揭露的安全漏洞攻擊進行分析，發現在出現安全漏洞與遇到攻擊間平均會有五天，我們將此定義為平均漏洞攻擊時間 (TTE)，相較於先前分析的平均 32 天大幅降低。預計 2025 年以後仍會維持這樣的攻擊速度，甚至還會加快。N 日和零時差安全漏洞會持續影響平均攻擊時間，因為這兩者對威脅策動者來說還是頗具吸引力。單就 N 日漏洞攻擊的時程來看，我們發現 2021 至 2022 期間，在六個月後才首次遭到攻擊的漏洞有 23 個，到了 2023 年卻降為 2 個，再再顯示攻擊速度有加快的趨勢。

此外，遭到攻擊的供應商無論在數量還是類型方面，2025 年後都會持續成長，因為自 2018 年以來，這類供應商數量幾乎年年上升。攻擊數量在 2023 年達到 56 家，創下歷史新高，比 2018 年觀察到的 25 家增加超過一倍。我們預計，此數據將持續攀升，超越過往記錄，因此必須對攻擊面和相關要素有更進一步的瞭解。

為後量子密碼編譯時代做好準備

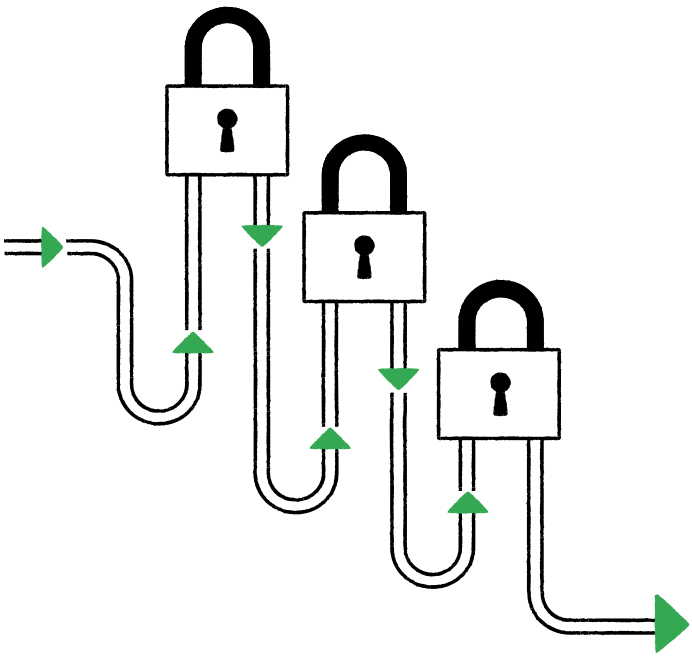
2025 年，許多機構將開始採用美國國家標準暨技術研究院 (NIST) 於 2024 年定案的全新後量子密碼編譯標準。這是 NIST 就量子安全加密/金鑰傳輸，以及加密簽署領域提供的最新指引，有助緩解運用大規模量子電腦的攻擊威脅，避免這些攻擊破壞加密機制，最終導致機密資料遭駭。

儘管量子威脅在 2025 年不太可能會造成大規模影響，但機構必須從明年開始瞭解量子運算帶來的風險，例如規劃改用能防範量子威脅的解決方案、列出使用加密機制的區塊、定期輪替加密金鑰，並透過威脅情報和其他指引，隨時關注量子威脅的發展。

歐洲、中東和非洲地區預測資訊

法規遵循的關鍵之年

新版網路與資訊系統安全指令 (NIS2) 推出後，歐洲、中東和非洲地區 2025 年的網路安全做法將大幅調整。除了導入更嚴格的安全規範，適用範圍也會納入更多產業及機構，包括關鍵和重要的實體。也就是說，會有越來越多的企業需要採行嚴謹的安全措施、執行風險評估，並及時回報突發事件。NIS2 的重點在於風險管理、事件應變及供應鏈安全，促使機構採取更積極且全面的做法。不論是加強監督還是強制執行上述做法，都能讓機構更有效地處理網路安全問題。機構須在員工培訓、資安技術及事件應變規劃方面投注心力，才能達到 NIS2 的要求。藉由這項指令，協作與資訊分享將更加普遍，進而在歐洲、中東和非洲地區打造更強大的網路安全生態系統。NIS2 的目的在於協調會員國的網路安全標準，強化防禦網路威脅的整體韌性，透過制定更高標準的安全防護做法，大幅增強整個歐洲、中東和非洲地區的網路安全防護機制。



地緣政治衝突會助長威脅活動

2025 年，地緣政治衝突仍會是助長歐洲、中東和非洲地區威脅活動的主因，對該區的不同實體造成全面影響。烏克蘭衝突未歇，中東局勢持續緊張，是促成此趨勢的關鍵，除非這些情況在明年告終，否則該區的機構及相關國家都將直接或間接受到影響。

雖然私人實體和個人對地緣政治問題的直接影響有限，但在衝突期間與任一方結盟的國家/地區，都可能面臨遇襲的後果。我們發現，鎖定數位服務和基礎架構攻擊，是其中一種方式。對這些技術的依賴程度越高，就越有可能成為敵方目標，因此也更容易遇襲。

目前未有證據指出這會在 2025 年趨緩。我們預計這股對立的愛國力量，例如駭客或政府資助的攻擊活動，更可能以數位服務為目標，破壞或入侵數位基礎架構。因此，機構必須優先瞭解並隨時關注在網路安全領域中發生的地緣政治事件。

更重視雲端安全

2025 年，雲端安全是歐洲、中東和非洲地區企業要面對的首要課題。雖然這也是全球關注的問題，但 Mandiant 事件應變團隊觀察到，此區的調查行動有大幅增加之勢，主因是在未受管理的雲端環境中，設定有誤、監控不足、憑證重複使用，以及資安做法薄弱所致。這個趨勢預計會持續到明年。歐洲、中東和非洲地區的機構正迅速採用雲端技術，而業務團隊 DevOps 和 SecOps 職責劃分不清，則會加劇這些問題和挑戰。這些機構必須優先考量雲端安全，才能保護機密資料並維持客戶信賴。此外，還必須投注資源強化資安解決方案，採行更嚴格的存取控管機制，並提升監控能力。

日本及亞太地區預測資訊

北韓威脅策動者將日本及亞太地區列為目標

隨著日本及亞太地區的加密貨幣投資日益普遍，我們預計鎖定加密貨幣交易的攻擊將會增加，特別是來自北韓威脅策動者的攻擊。北韓在 2024 年持續對加密貨幣交易發動攻擊，同年 9 月美國聯邦調查局 (FBI) 已針對此問題發出警告。日本及亞太地區是加密貨幣採用率和增長率最高的區域，在過去一年中，報導指出該區發生多起重大加密貨幣入侵事件，包括價值數千萬至數億美元的數位資產遭竊。

北韓鎖定日本及亞太地區各地攻擊，採用的方式之一是冒用遠端 IT 工作人員的身分。對此，美國司法部和其他機構發布警示提到：「朝鮮民主主義人民共和國 (即北韓) 的資訊技術 (IT) 工作人員，會試圖冒用非北韓國民的身分，藉此取得工作機會。」在這些攻擊行動中，部分偽裝的 IT 工作人員就任職於日本及亞太地區各地機構。

中國政府控制的網站偽裝成當地新聞媒體，向全球受眾放送親北京內容

我們在 2022 年揭露了 HaiEnergy 攻擊行動，其中涉及 72 個疑似假新聞網站，以及若干可能造假的社群媒體資產，內容以 11 種語言發布，目的是傳播戰略上符合中國政治利益的內容。隨後至今，我們發現至少還有另外兩起行動，攻擊者會聘請第三方公司或公關公司，透過假的「地方新聞」管道宣傳政府言論。

這類威脅的風險不容小覷，因為不論是其他地方媒體未盡職調查，還是讀者偶然接觸到這些假的「地方新聞」媒體管道，都會無意間加深威脅影響。儘管這些攻擊活動在 2024 年並未實際改變全球對中國的看法，但我們相信這類活動將持續到 2025 年，所以必須繼續揭露及追蹤這些假新聞媒體，提供全球讀者正確的資訊。相對地，機構也須優先瞭解並隨時關注在網路安全領域中發生的地緣政治事件。

東南亞的網路犯罪手法不斷翻新

2025 年，東南亞的網路犯罪手法預計也將持續翻新。聯合國毒品和犯罪問題辦公室的一份新報告指出，亞洲犯越來越多亞洲犯罪集團將服務型的新商業模式和相關技術 (包括惡意軟體、生成式 AI 和深偽技術)，整併至攻擊行動中，同時建立新的地下市場和加密貨幣解決方案，滿足洗錢需求。報告顯示，該區域的組織型網路犯罪正迅速發展，此趨勢可能導致日本及亞太地區的犯罪活動加劇。因此，政府和企業必須正式定期分享情報，深入瞭解這些活動的戰術、技術和程序，才有辦法追蹤非法的資金流動。

結論

「**2025** 將是 AI 自前測計畫和實驗原型邁向大規模採用的一年。」

Phil Venables.
VP, TI Security & CISO,
Google Cloud

2025 年，網路安全產業將持續創新，而機構面臨威脅環伺的茫茫局勢，也將迎來不斷變化的挑戰。

科技的迅速發展，特別是人工智慧領域，正在重塑防禦者和惡意分子的戰略布局。多虧 AI，新的威脅偵測與因應工具在短時間內問世，但這也為惡意行為人提供強大後盾，得以發動社交工程、不實資訊和其他攻擊。

我們會繼續看到「四巨頭」(俄羅斯、中國、伊朗和北韓) 展開攻擊活動，這些國家將透過網路間諜、干擾及影響行動，達到各自的地緣政治目標。此外，勒索軟體和多面向勒索，以及資料竊取惡意軟體的蓬勃發展，也為全球各地的機構帶來巨大風險。

2025 年，機構必須優先採取積極且全面的網路安全做法，包括採用雲端原生資安解決方案、採行強大的身分與存取權管理措施，以及透過持續監控和威脅情報，預先防範新興威脅。這也意味著須為後量子密碼編譯時代做好準備，並符合不斷變化的法規要求。

《2025 年網路安全預測》報告旨在提供機構所需的洞見與知識，有效應對這個複雜局勢。只要懂得掌握瞬息萬變的趨勢與潛在威脅，機構就能強化防禦機制，打造韌性更高的系統迎接未來。

貢獻者

《2025 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：

Charles Carmakal
Mandiant CTO, Google Cloud

Sandra Joyce
VP of Google Threat Intelligence
at Google Cloud

Sunil Potti
VP/GM, Google Cloud Security

Phil Venables
VP, TI Security & CISO, Google Cloud

多位資安專家也貢獻己力，協助我們完成這份報告：

Tufail Ahmed

Dan Black

Sarah Bock

Michelle Cantos

Casey Charrier

Anton Chuvakin

Jamie Collier

Jennifer Fernick

Felix Gröbert

David Grout

Adrian Hernandez

Cris Brafman Kittner

Steve Ledzian

Yihao Lim

Keith Lunden

David Mainor

John McGuiness

Luke McNamara

Matthew McWhirt

Jens Monrad

Mathew Potaczek

Mike Raggi

Kelli Vanderlee

Alden Wahlstrom

Robert Wallace

Jess Xia

Google Cloud

如需更多資訊，請前往 cloud.google.com