CHECK POINT™

cp<r>
CHECK POINT RESEARCH

2026 年
網路安全報告

第14屆
年度報告

目錄:

01

介紹

介紹

2025年，威脅情勢迅速演變，變得更加相互關聯，也更難管理。我們對全球遙測資料和事件的分析揭示了一種根本性的轉變，其標誌是出現了新的攻擊面和技術。攻擊者正在將人工智慧、身分濫用、資訊外洩利用和勒索軟體整合到他們的攻擊活動中。

最顯著的變化是攻擊機會的執行速度和規模都加快了。數據顯示，攻擊者正在將存取、執行和影響聯繫起來，跨越各種領域，從人工智慧驅動的社會工程和自動化到將勒索軟體轉變為數據驅動的勒索經濟。邊緣裝置和暴露的基礎設施越來越多地被用作攻擊入口。2025 年，這些模式在各個地區和產業中均持續 observable，凸顯了快速結合各種技術以產生實際影響的重要性。

人工智慧正是這種轉變的典型例證。本報告將人工智慧視為一種力量倍增器，可以增強...攻擊者活動的目標、規模和適應性，同時也會影響風險優先順序和作戰反應。

我們的報告以攻擊者行為和真實世界數據為框架。接下來的章節將深入探討攻擊者集中攻擊的領域，以及不同的技術如何加強防禦。彼此之間，以及哪些暴露模式最常導致影響。這為理解威脅情勢的發展軌跡以及 2026 年最關鍵的問題提供了必要的背景。

我邀請您仔細閱讀本報告中呈現的數據和研究結果。

Lotem Finkelstein，副總裁，研究部

LOTEM FINKELSTEIN

研究副總裁

02

網路安全趨勢

超越電子郵件：多通道社會工程

在所有組織中，哪個攻擊面最容易被利用？對 2025 年的攻擊者來說，答案在於人的因素。在社會工程攻擊中，威脅行為者試圖透過操縱人類受害者，使其提供初始存取權限，從而實現入侵。在這種攻擊中，威脅行為者會以員工、外包人員和第三方服務提供者為目標，以獲取對組織系統或敏感資訊的存取權限。雖然這些攻擊被認為不如利用軟體或硬體脆弱性的攻擊嚴重，但它們造成的破壞可能與其他方式造成的破壞一樣嚴重。

多年來，網路釣魚郵件一直是社會工程攻擊的主要手段，各組織也越來越意識到這些威脅。然而，到2025年，社會工程攻擊的範圍將不再局限於傳統的基於電子郵件的營銷活動，而是擴展到其他領域。利用電話、即時通訊應用程式和即時身分冒充等多平台、跨通路、高度針對性的方法。在同時，攻擊者也改進了基於電子郵件和瀏覽器的社交工程攻擊的執行方式，轉向以互動為導向的攻擊。ClickFix及其變體等技術。這些方法引導使用者完成看似合法的流程，旨在繞過安全控制並無意中執行惡意軟體。

這些手段導致全球範圍內發生了數百萬次入侵嘗試，並造成了多起影響重大的商業安全漏洞，對全球企業造成了巨大的經濟損失。

ClickFix：將執行權轉移到使用者身上的社會工程學

ClickFix 成為 2025 年最重要的社會工程技術之一。ClickFix 最早在 2024 年被發現，它是一種初始存取方法，攻擊者透過向使用者提供欺詐性指令來操縱使用者執行惡意操作。這些指示通常透過被入侵或攻擊者控制的網站、惡意廣告或品牌冒充電子郵件傳播，其設計旨在模仿例行驗證步驟，例如驗證碼、驗證檢查或錯誤修復。透過偽裝成繼續正常活動所需的合法步驟，誘使用者運行攻擊者控制的內容，最終傳播惡意軟體。

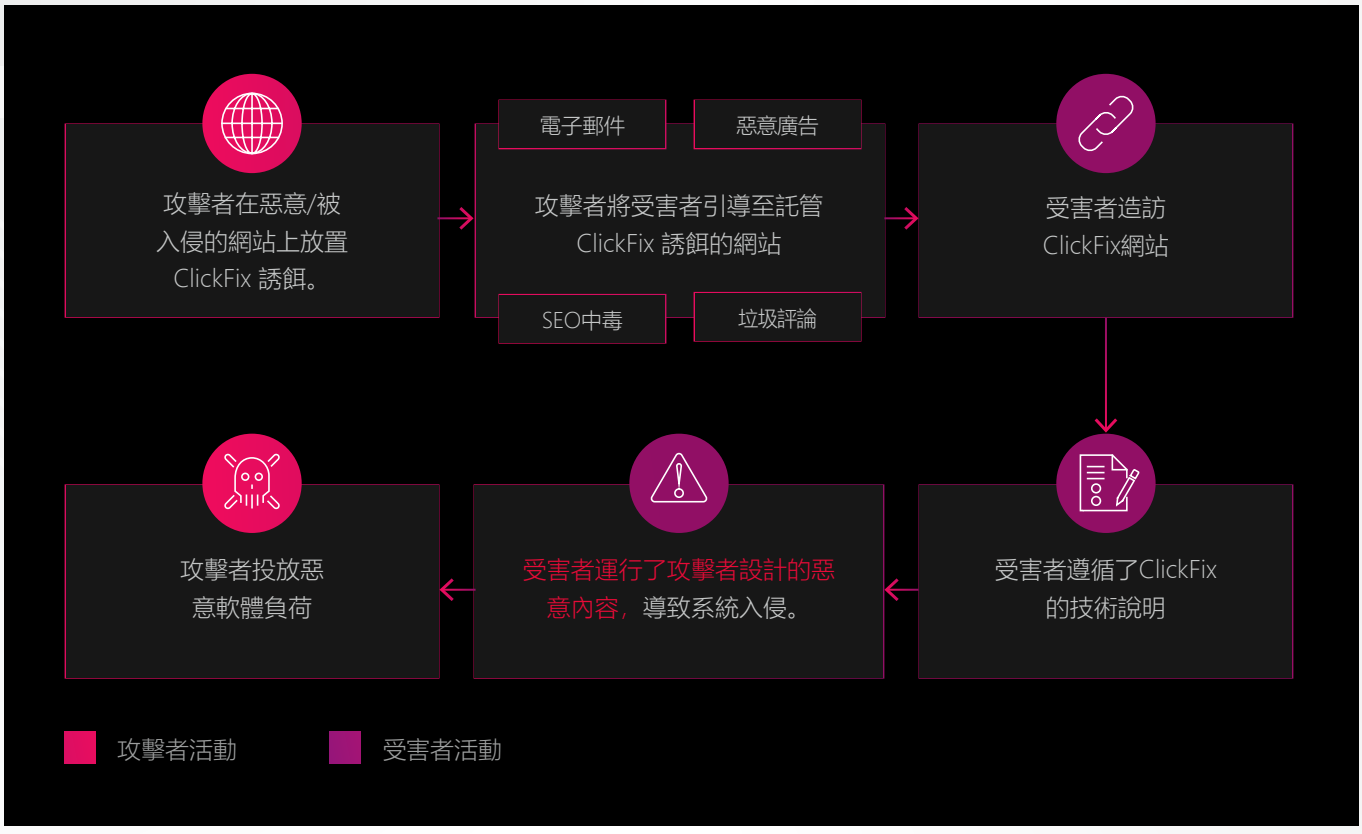


圖 1: ClickFix 攻擊流程圖

圖 2：ClickFix 網站範例，其中包含虛假的驗證碼提示

這項技術之所以成功，是因為它利用了使用者的信任和遵循技術說明的傾向。由於其簡單性、可擴展性以及繞過某些安全控制的能力，它已被證明非常有效，因為惡意操作是由使用者手動執行的，而不是透過傳統的基於文件的感染鏈傳播的。因此，它的普及速度迅速加快。2025 年，ClickFix 的活動比前一年增加 了約 500%，並且在近一半有記錄的惡意軟體活動中都有 observed。

> 2025年，CLICKFIX 攻擊活動相較前一年增加約 500%，並出現在近一半的惡意程式攻擊活動中。

這項技術已被廣泛應用於各種威脅領域，包括一些知名的網路犯罪集團，例如 RedLine 和 Lumma, 它們策劃了大規模的資訊竊取行動。以及在攻擊中投放有效載荷，導致 Interlock 勒索軟體感染。同時，新興的惡意軟體家族越來越多地使用 ClickFix 作為其初始攻擊媒介。近期的例子包括針對美國居民的 MonsterV2 資訊竊取程式活動，以及 Check Point 研究分析的 PureHVNC RAT 程式活動。超過 出於經濟動機的犯罪，多個國家支持的 APT 組織也採用了 ClickFix 作為首選的傳播機制，而不是他們更傳統的初步存取技術。

ClickFix 的成功催生了其他採用相同社會工程方法的技術。2025 年中，威脅行為者開始採用 FileFix，這是一種源自 ClickFix 的技術，它濫用合法的作業系統工作流程來取得初始存取權限。受害者的裝置。FileFix 依賴惡意或被入侵的網站來觸發一個標準的 Windows 資源管理器窗口，使用者在該窗口中...被指示貼上看似必需的內容文件路徑。此操作會導致攻擊者控制的內容被執行，從而在不使用傳統惡意軟體傳播方式的情況下造成系統入侵。FileFix 最初是作為概念驗證而

推出的，但幾週之內就被威脅行為者利用。從那時起，多個活躍的攻擊活動利用該技術來投放惡意軟體有效載荷，包括 Interlock RAT 和 StealC 資訊竊取程序，這表明成功的社會工程方法從研究到實際應用轉變的速度有多快。

同時，攻擊者已經將 ClickFix 的方法擴展到程式碼執行之外，進而入侵帳號。ConsentFix 於 2025 年底問世，它將類似的社會工程原理應用於雲端環境。它誘騙使用者完成合法的 Microsoft/Azure OAuth 登入流程。然後它攻擊者指示使用者複製並貼上包含 OAuth 授權碼的本機主機網址到攻擊者控制的頁面中。竊取的授權碼用於取得令牌，並在無需取得密碼和完成多重身份驗證 (MFA) 的情況下存取使用者的 Microsoft 帳戶。

ClickFix 及其變種在 2025 年的流行已擴展到 Windows 環境之外。威脅行為者專門針對 macOS 使用者發動攻擊活動，並利用 ClickFix 技術攻擊 Linux 系統。正如我們在網路釣魚工具包中看到的那樣，ClickFix 開始商品化，例如 IUAM ClickFix Generator 等工具包的出現，使攻擊者能夠創建高度可自訂的跨平台 ClickFix 攻擊活動，並迅速大規模地應用該技術。

誘騙受害者在其自身系統上發動惡意活動，反映了攻擊者社會工程策略的更廣泛轉變，即利用使用者對端點、瀏覽器和雲端身分平台等合法流程的信任。

基於語音的社會工程 - 重大攻擊的首選武器

語音網路釣魚和身分冒充在2025年獲得了顯著發展，並被證明是利用使用者信任的高效手段。在這些攻擊中，攻擊者偽裝成受信任或權威人士，並在進行有針對性的偵察後，使用預先準備好的腳本向受害者施壓，迫使其採取重置驗證資訊、更改 MFA 代碼或授予網路存取權限等措施。歷史上與...相關低複雜度的消費者欺詐，即基於電話的身份冒充，已經演變成一種以企業為中心的入侵技術，用於在大型組織中獲得初步立足點。

2025年，基於語音的冒充成為針對知名品牌的複雜威脅組織常用的攻擊手段。這些犯罪分子進行了深入的偵察，利用多種溝通平台與受害者接觸，並執行複雜的多階段社會工程腳本來實現他們的目標。在一些案例中，語音驅動的攻擊活動使攻擊者能夠獲得初始存取權限，從而對今年一些最具破壞性的高影響力企業入侵事件造成影響。

> 歷史上與低複雜度的消費者詐欺、電話詐騙有關基於身分冒充的攻擊已經演變為以企業為中心的入侵。用於在大組織中獲得初步立足點的技巧。

最值得注意的是，這種活動與以經濟利益為目的的威脅行為者有關，例如 Scattered Spider 和通常被稱為 Scattered LAPSUS$ Hunters (SLH) 的叢集。Scattered Spider（也稱為 UNC3944 / Octo Tempest）是一個高效的、以入侵為中心的叢集，以身份中心初始訪問技術而聞名，包括服務台和 IT 供應商冒充、MFA 疲勞和 SIM 卡交換帳戶接管。SLH 是由 Scattered Spider、LAPSUS$ 和 ShinyHunters 等業者、工具和戰術共同進行的聯合行動。 這三個組織都有多次備受矚目的企業資料外洩和敲詐勒索記錄。過去值得注意的攻擊事件包括 Shiny Hunters 在 2024 年入侵 美國電信巨頭 AT&T，該組織因此獲得了超過 35 萬美元的贖金；以及 Scattered Spider 對 MGM Resorts 的攻擊。2023 年；以及 Lapsus$ 在 2022 年透過被入侵的第三方支援提供者入侵 身分驗證公司 Okta。

高影響企業事件

SLH與2025年發生的幾起影響巨大的事件有關，在這些事件中，語音驅動的社會工程攻擊成為針對大型企業的主要初始入侵途徑，從而獲取數據。並進行勒索。2025 年 4 月，Scattered Spider 透過有針對性的社會工程行動，並輔以廣泛的偵察，入侵 了英國零售商 Marks & Spencer 的網路。攻擊者收集了有關該公司成員和內部流程的詳細信息，使他們能夠在聯繫為 Marks & Spencer 提供支援的第三方服務台提供者時，成功地冒充 合法成員。攻擊者他們誘騙一名技術支援工程師重置密碼以獲取存取權限，從而部署了 DragonForce 勒索軟體。該事件迫使瑪莎百貨暫停線上訂單一個多月，擾亂了店內運營，並導致客戶資料被盜。該公司後來估計 損失了約3億英鎊的利潤。直接事件響應和復原成本達 1.36 億英鎊。

> “2025年，語音驅動的社交工程學成為主要學科。初始存取向量在高影響力企業資料外洩事件中發揮重要作用，導致資料竊取和勒索。”

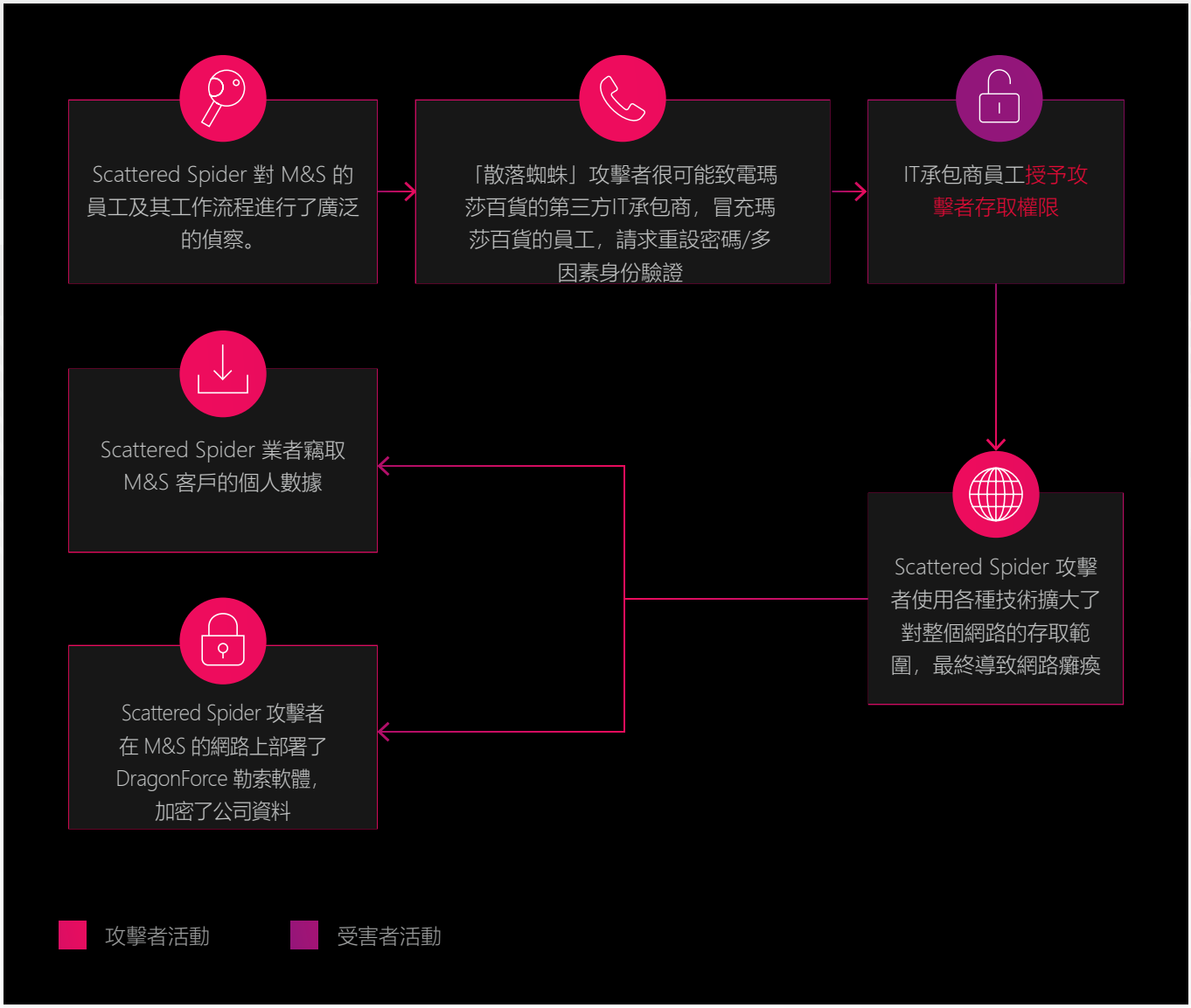


圖 3：Scattered Spider 對 Marks & Spencer 的入侵

在另一起案例中，英國汽車製造商捷豹路虎 (JLR) 於 2025 年 8 月成為 SLH 的攻擊目標。攻擊者獲得了內部系統的存取權限，竊取了客戶數據，並強制關閉了 IT 和製造環境，導致生產中斷數週。

雖然沒有公佈技術評估報告但有報告指出，入侵可能涉及針對 IT 支援團隊的社會工程技術，這與 SLH 先前的活動一致。據估計，這起事件造成的損失約為 19 億英鎊。

2025 年初，以高超的語音網路釣魚攻擊手段而聞名的威脅組織 ShinyHunters（也被追蹤為 UNC6040）針對企業 Salesforce 環境發起定向攻擊，旨在竊取大規模資料並進行勒索。攻擊者主要針對跨國企業英語分支機構的員工。他們冒充內部 IT 支援人員，脅迫受害者授予存取權限或洩露敏感資訊 透過取得驗證資訊，最終導致 Salesforce 實例中的資料被竊取。攻擊者隨後聲稱，這次攻擊活動影響了約 40 家組織，其中包括多家全球知名品牌，並導致近 10 億筆記錄被竊取。這些說法尚未得到證實。

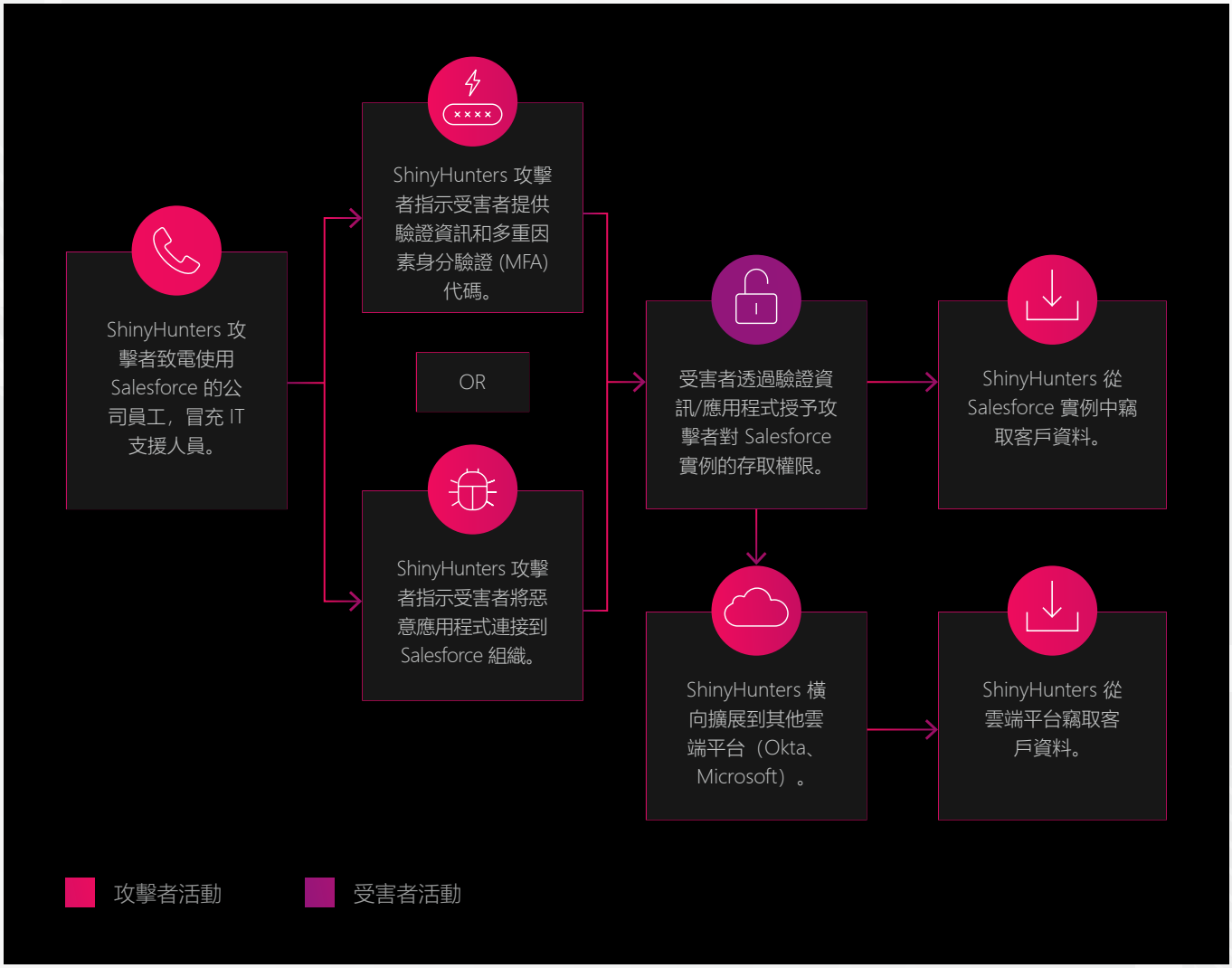


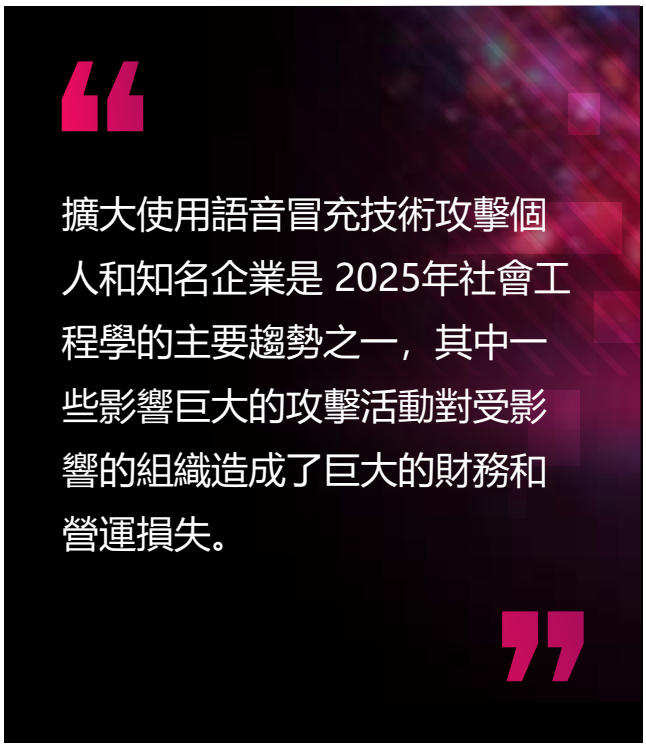
圖 4：歸因於 ShinyHunters 的 Salesforce 攻擊

現有報告顯示，在多起案例中，與SLH生態系相關的個人均來自西方國家。公開的逮捕 記錄和起訴書顯示，涉案人員擁有美國, 英國, 和歐洲 國籍。這或許可以解釋為何這些操作者俱備如此精通的語言和文化背景，以便能夠對歐洲和北美機構發動基於語音的身份冒充攻擊。

語音身分冒充仍是企業入侵以外的重要詐騙手段尤其是針對個人的經濟詐騙。在這些案例中，攻擊者通常會冒充金融機構或加密貨幣平台，迫使受害者轉移資金或洩漏帳戶驗證資訊，從而實現帳戶盜用。根據FBI報告, 2025年語音詐欺和帳戶盜用事件造成的損失將超過2.5億美元。

語音身分冒充已成為一種趨勢

基於語音的社會工程攻擊日益成功，推動了犯罪生態系統對熟練身分冒充操作者的需求成長，同時也催生了人工智慧驅動 的語音身分冒充工具和服務市場。總體而言，**利用語音模仿攻擊個人和知名企業是 2025 年社會工程學發展的主要趨勢之一，一些影響巨大的攻擊活動對受影響的組織造成了巨大的經濟和營運損失。**



受害者發起的社會工程

2025 年，我們 observable 到受害者發起的（入站）社會工程攻擊趨勢日益增長，攻擊者故意引導目標主動發起聯繫，從而增加互動的合法性。

Check Point 研究 發現，其中一項名為 ZipLine 的攻擊活動，攻擊者會濫用組織的公共「聯絡我們」頁面，偽裝成合法的商業諮詢。這這種方法促使員工在正常工作職責範圍內，主動與攻擊者進行後續溝通。攻擊者隨後會與受害者進行長達數週的電子郵件交流，然後發送惡意 ZIP 附件來部署 MixShell 惡意軟體。這場運動主要針對製造業企業。

高信任度通訊平台正逐漸成為社交工程攻擊的新管道

在與 UNC6229 有關的攻擊活動中也observable到了類似的受害者發起模式，這些活動的目標是行銷和數位廣告行業的個人，目的是劫持企業。廣告和社群媒體帳號。該演員在合法平台和攻擊者控制的網站上發布虛假招聘信息，誘使受害者主動申請招聘角色。最初的溝通是無害的、個性化的，旨在建立信任，然後轉向惡意負載投放或透過網路釣魚連結竊取驗證資訊。

雖然攻擊者發起的網路釣魚郵件的成功率通常很低，但透過設計受害者發起或維持通訊的場景來逆轉互動流程，可以顯著提高攻擊者的可信度和入侵的可能性。

在商業溝通平台上進行社會工程活動

威脅行為者正日益將社交工程活動從電子郵件擴展到社群媒體平台和即時通訊應用程式上，而這些平台上的使用者期望和安全控制往往較弱。這些互動通常與傳統的網路釣魚目標類似，例如脅迫受害者執行惡意檔案或洩漏驗證資訊，同時受益於使用者懷疑程度降低和缺乏專門的安全控制措施。

透過第三方訊息平台，攻擊者可以在更非正式的環境中與目標互動，從而更容易建立信任。這種轉變反映了一種更廣泛的趨勢，即利用那些正在衰落的通訊管道。 超出傳統企業安全顯示器範圍。

例如，伊朗APT組織 Nimbus Manticore 的observable活動被發現冒充企業。利用LinkedIn上的專業人士與員工互動。另一個伊朗APT組織「受過教育的曼提科爾」（Educated Manticore）多年來一直利用 WhatsApp等即時通訊平台進行社交活動。工程方法論。這種方法在2025年仍然有效，因為攻擊者透過非正式的溝通管道與受害者建立信任，同時又主要在傳統企業安全可見度和控制範圍之外運作。

最後，威脅行為者越來越多地轉向企業協作平台，例如Microsoft Teams和Slack，作為社交工程的管道。當組織配置允許外部使用者發起聊天或通話時，這些平台為攻擊者提供了一個高度可信的環境，攻擊者可以在其中冒充內部IT人員或服務提供商，並透過文字、語音或視訊直接與員工互動。

過去一年observable到的多個攻擊活動都利用Microsoft Teams作為初始存取途徑，攻擊者從敵方控制的Microsoft 365租戶向員工發送訊息或撥打電話，同時偽裝成內部IT支援人員。受害者通常會被誘騙安裝遠端支援工具，從而獲得對其係統的完全互動式存取權限。然後，攻擊者會濫用此存取權限來部署下一階段的惡意軟體，例如 Matanbuchus 載入器，並最終實現全網路入侵，

其中可能還涉及勒索軟體。這些攻擊事件凸顯了旨在簡化業務溝通的協作平台如何 **日益被濫用為高信任度的攻擊面，使攻擊者能夠繞過標準的電子郵件防禦措施，並利用人性的弱點來快速入侵系統。**

應對2025年社會工程威脅的快速演變

社會工程攻擊已成為威脅情勢中的主要攻擊手段，從詐騙和機會主義惡意軟體攻擊到最具破壞性的企業入侵，無一例外。威脅行為者不斷擴展其攻擊手段，越來越多地利用多個平台、多樣化的心理戰術和創新的技術方法。諸如ClickFix和語音模仿等策略尤其有效成為領先的惡意軟體和入侵組織的主要工具。

如前文所述，人為因素仍是組織安全中最薄弱的環節。預計2026年社會工程活動將進一步加劇。生成式人工智慧降低了高可信度攻擊的門檻而新工具和解決方案的快速普及則為威脅行為者提供了不斷擴展的可利用的可信任工作流程。因此，社會工程已成為一種日益增長且適應性強的威脅，組織必須將其視為核心安全挑戰。

2025 年勒索軟體生態系統：

2025年，勒索軟體受害者人數創下歷史新高，犯罪生態系統也隨之快速重組。年初，網路犯罪集團Cl0p發動了大規模攻擊，隨後幾個主要的勒索軟體即服務（RaaS）組織突然消失，這為新興犯罪者創造了機會。然而，攻擊數量持續攀升，凸顯了其關聯組織的韌性以及支撐勒索軟體模式的經濟誘因。本章將探討這些發展趨勢，並基於Check Point事件回應團隊的調查結果，重現一次麒麟勒索軟體入侵事件，以說明這些生態系統動態如何在真實攻擊中體現。

2025年的特色是頂級勒索軟體組織頻繁更迭，麒麟等新興組織崛起，Cl0p和LockBit等老牌勒索軟體組織重新出現。同時，全球關於贖金支付、報告強制要求以及執法幹預局限性的政策辯論也日益增多。勒索軟體攻擊越來越多地將人工智慧融入攻擊生命週期的不同階段，包括惡意軟體開發、被盜數據分析、法律和監管評估，以及為談判和勒索活動提供支援。

2025年勒索軟體活動達到了前所未有的水平。在雙重勒索集團經營的資料外洩網站上，超過 7,960 名受害者被點名，比前一年增加了 53%。第一季記錄了 2,289 起已公佈的受害者案例，年增 134%，部分原因是 Cl0p 利用了零日脆弱性。這使得Q1成為這是我們資料集中記錄到的最活躍的季度，隨後在第四季度被打破，當時公佈的受害者人數為 2,473 人。

圖 1 顯示了勒索軟體受害者人數持續多年的上升趨勢。

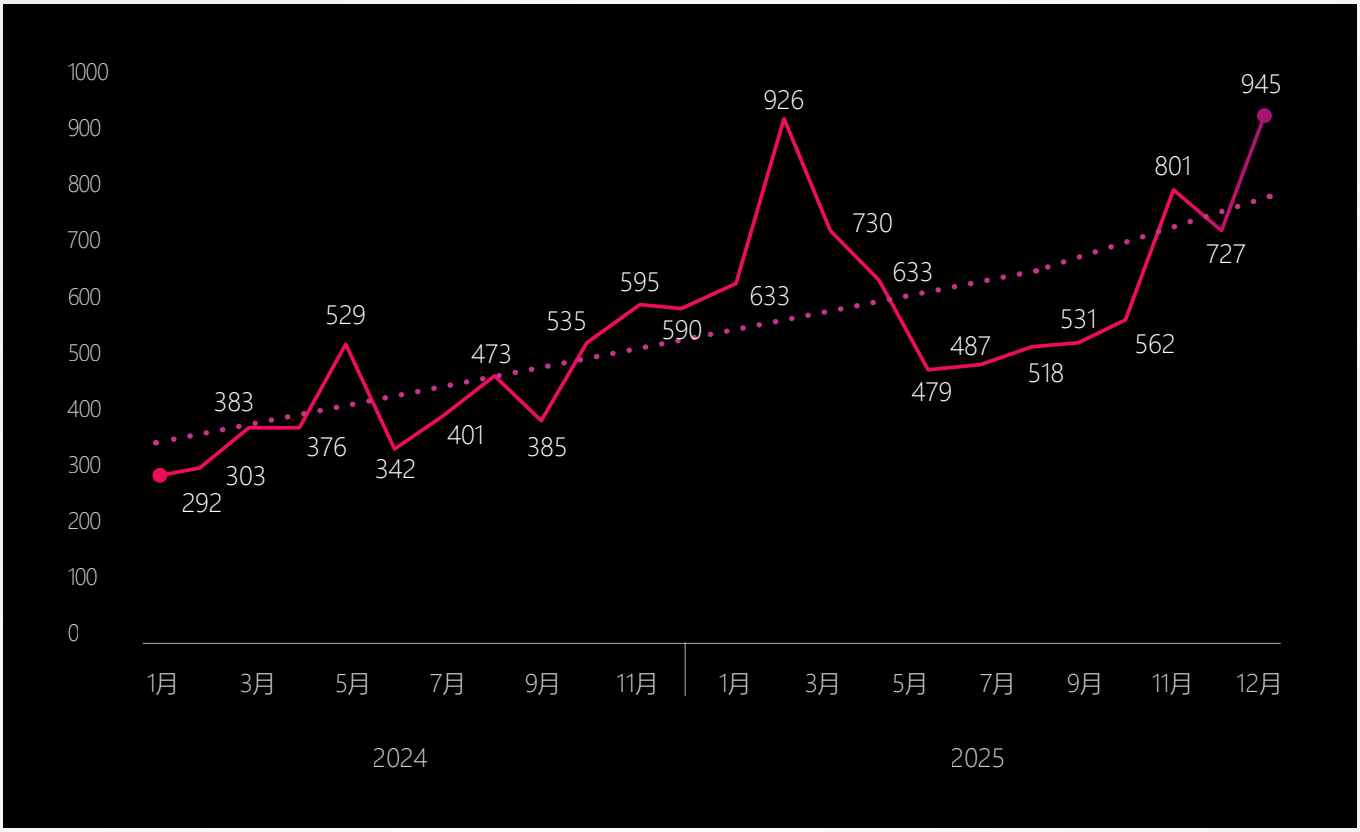


圖 1 - 每月公佈的勒索軟體受害者人數

年中 RaaS 中斷與聯盟重組

第二季度，多個備受矚目的RaaS專案突然消失，而受害者人數仍遠高於2024年的基準水準。8Base和Phobos因國際執法部門的聯合行動而遭到搗毀，這些行動查封了洩漏和交易網站，導致多名主要業者及其關聯人員被捕。其他一些知名的勒索軟體組織，包括BianLian、Hunters 和 Cactus 等公司要麼更名，要麼徹底轉型為資料勒索模式。或悄悄停止發布新的受害者訊息。RansomHub自2024年出現以來，已公佈了超過760名受害者的訊息，目前已停止營運。2025年4月初，毫無預警。這波退出潮暫時導致許多關聯組織（即發動攻擊的運作者）失去了工作。穩定的RaaS品牌。麒麟和龍之力量迅速填補了這一空缺，並積極在犯罪論壇上招募前 RansomHub 和 LockBit 成員。到第三季度，兩者均躋身最活躍的資料外洩網站營運商之列。

麒麟成為年中改組的主要受益者。在第二季度和第三季度，由於幾個長期存在的組織倒閉後，該組織成功吸引了非關聯入侵者，其公佈的受害者數量穩步增加。到 2025 年中期，麒麟已成為最活躍的 RaaS 營運商之一，超越了許多傳統品牌。

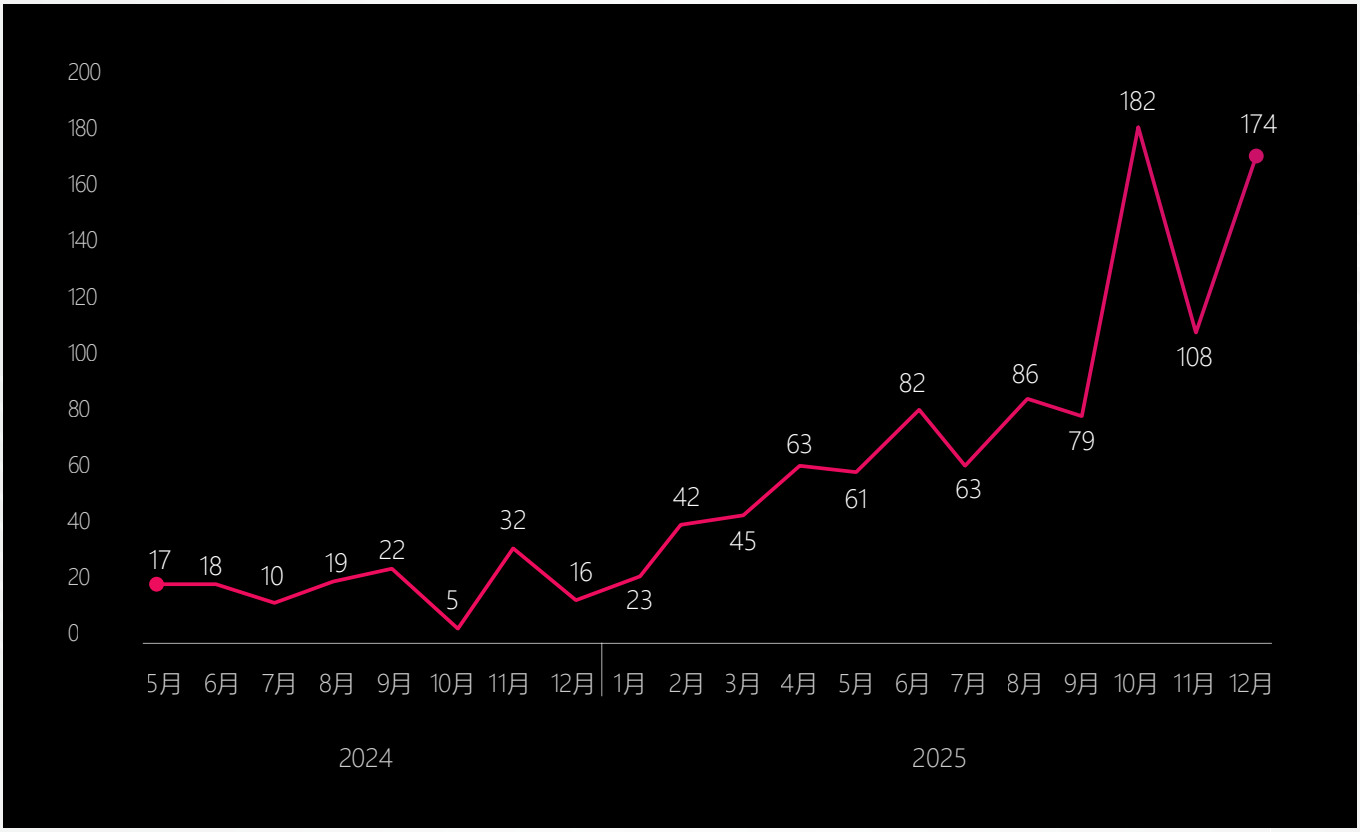


圖2 - 麒麟網站公佈的受害者人數每月統計

獨立雙重勒索團伙的擴散

2025 年，小型、獨立的雙重勒索團夥也出現了前所未有的激增。到 2024 年底，大約有 90 個可識別的品牌在資料外洩網站 (DLS) 上發布受害者訊息，而到 2025 年，記錄在案的品牌數量為 140 個，增長超過 50%。這表明，隨著大型勒索軟體即服務（RaaS）計畫的退出，規模較小的組織迅速填補了由此產生的真空。許多新出現的攻擊者沒有正式的聯盟計劃，而是依靠單一團隊或小型合作夥伴關係發動攻擊，而無需承擔大型RaaS框架的開銷、收入分成或基礎設施需求。

然而，到了2025年底，情況再次改變。麒麟等規模更大、知名度更高的品牌重新確立了其先前的統治地位。Akira的活動激增，Cl0p在沉寂數月後再次出現，繼續其高影響力、機會主義的大規模攻擊活動模式。LockBit的重新出現（現更名為LockBit 5.0）進一步標誌著大型RaaS組織的回歸。

這種主導組織消失、小型攻擊者激增，最終圍繞著少數大型參與者聚集的循環，體現了RaaS計畫在勒索軟體生態系統中扮演的結構性角色。勒索成功與否取決於受害者是否相信，一旦支付贖金，威脅者既會解密數據，也不會洩露數據。與知名的RaaS品牌建立合作關係可以降低交易摩擦，並提高支付贖金的可能性。然而，知名度的提高也會使RaaS業者面臨執法部門更大的壓力。營運商透過週期性的品牌重塑，關閉一個名稱和基礎設施，然後以另一個名稱重新出現，可以降低它們所吸引的關注。這種動態使防禦者和調查人員的歸因和乾擾工作變得更加複雜並有助於解釋在2025年observable到的主導RaaS品牌反覆出現、衰落和重新出現的現象。

> 這種週期，也就是主導集團消失，小型參與者激增最終圍繞著少數大型參與者聯合起來，說明了RAAS程式在勒索軟體生態系統中扮演的結構性角色

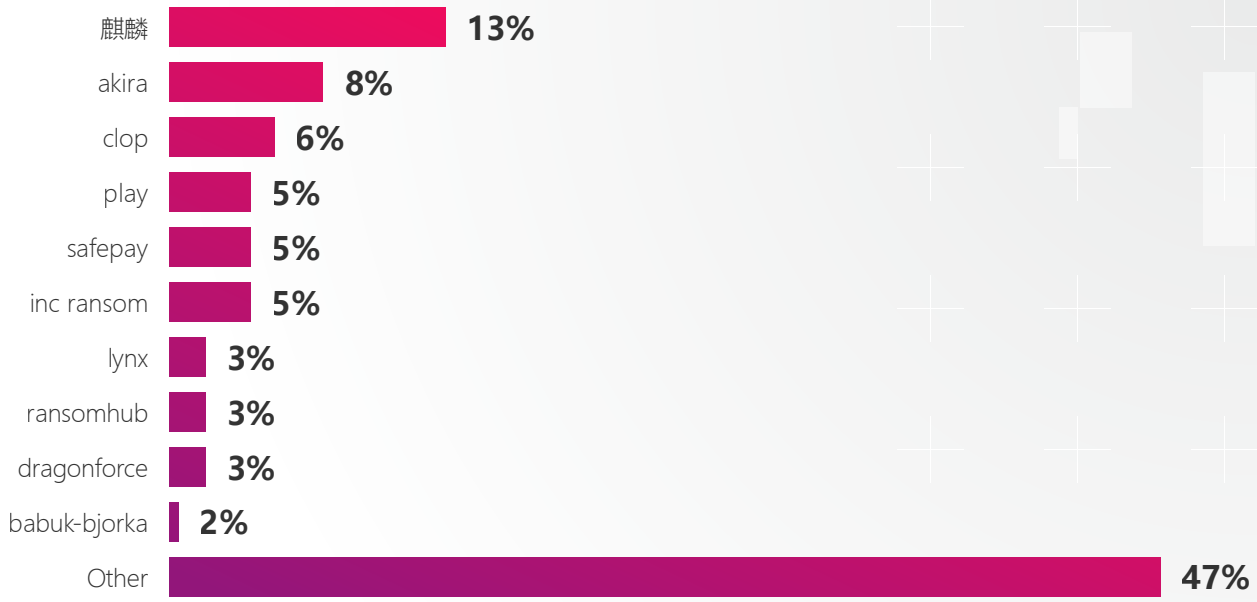


圖 3 – 2025 年前十大 RaaS（Ransomware-as-a-Service，勒索軟體即服務）組織，依公開受害者比例排名

大型 RaaS 運營商持續推動交易量

對 2025 年最活躍的勒索軟體組織的分析表明，儘管湧現出許多新品牌，但長期運營的 RaaS 業務仍然是該生態系統的核心。一些年度頂級組織，例如自 2022 年以來一直活躍的麒麟和 Play；2023 年出現的 Akira、Inc Ransom 和 DragonForce；以及 2024 年成立的 Lynx 和 RansomHub，都保持了多年的持續運營、強大的聯盟網路和穩定的基礎設施。它們的持續存在凸顯了儘管規模較小的獨立團體不斷增多，但到 2025 年，大型 RaaS 計畫將繼續推動整體攻擊量的成長。

Qilin - 新興的RaaS主導集團

Qilin 在 2025 年成為 RaaS 領域的主導集團，在 1000 多名受害者拒絕支付贖金後，在其 DLS 上公佈了這些受害者的身份。該組織自2022年起活躍至今，憑藉其強大的實力，得以利用主要競爭對手(如RansomHub）消失後造成的暫時真空。LockBit 處於非活動狀態。2025 年 4 月 RansomHub 突然倒閉後，Qilin 積極招募了失去聯繫的加盟商。因此，該組織在 2025 年的每月受害者人數幾乎增加了兩倍，從第一季平均每月約 35 名受害者增加到第四季度的 150 多名受害者。根據 DLS 的數據，Qilin 是 2025 年最活躍的勒索軟體組織，每月受害者揭露數量始終位列第一或第二，其活躍程度超過了 Akira、DragonForce 和 Play。

RaaS平台功能與勒索模式

Qilin 經營一個功能齊全的 RaaS 框架，為聯盟成員提供支援端到端攻擊生命週期的管理面板。該平台包括加密器、洩漏基礎設施、支付協商工具和營運支援。該組織的勒索手段反映了更廣泛的生態系統趨勢。對於資料外洩行動：談判更依賴監管曝光、聲譽損害和營運中斷的威脅，而不是僅僅依賴解密。

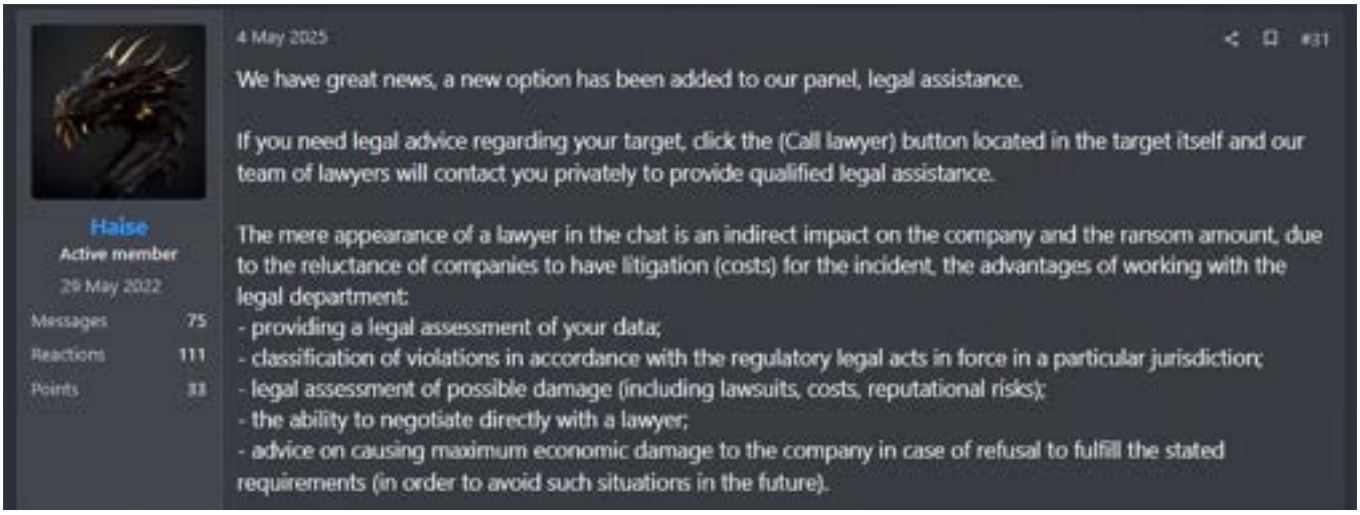


圖 4 – 麒麟在暗Web論壇推廣新型勒索工具

為了增強其成員對受害者的影響力，麒麟推出了一系列增強型「施壓」服務。其中包括所謂的法律審查功能，該功能會對被盜資料進行檢查，以查找是否有違反合規性或強制揭露要求的跡象並將相關文件提交給稅務機關或聯邦調查局等合規機構。該組織還宣傳可向受害者的企業郵箱和手機發送大量資訊的工具，並透過所謂的「新聞」中介機構發布面向公眾的洩漏訊息。其中一些功能類似於 GenAI 支援的內容生成，這可能表明該組織整合了用於勒索的自動化撰寫和分發工具。

目標畫像和成員動機

儘管麒麟自詡為出於愛國動機的 “理想主義者”，但其目標群體遍布全球（獨聯體國家除外），不限行業，且顯然以經濟利益為驅動。該組織向其合作夥伴提供 80% 至 85% 的極具競爭力的利潤分成將自身定位為其他 RaaS 組織的高利潤替代方案，並在合作夥伴大量流失的一年中鞏固了其吸引力。

Cl0p - 零日漏洞的異類

Cl0p 塑造了 2025 年勒索軟體發展歷程的開端與終點。與傳統的 RaaS 參與者不同，Cl0p 始終依賴利用廣泛使用的企業軟體的高戰略性零日漏洞，同時入侵數百家組織。Cl0p 勒索行動完全基於發布被盜資料的威脅，而不是文件加密。

他們今年的首個大型行銷活動針對的是Cleo旗下的LexiCom、VLTrader和Harmony。透過兩個未經身份驗證的遠端程式碼執行脆弱性入侵檔案傳輸應用程式。二月的這場行動導致超過 335 名受害者被公開報道，他們主要來自北美的製造業、零售業、物流業和供應鏈營運商。第一季創紀錄的受害者人數很大程度上是由這起事件造成的。

Cl0p 的第二次重大行動發生在第三季至第四季度，當時多個 Oracle E-Business Suite 零日脆弱性被利用，包括 CVE-2025-61882 和 CVE-2025-61884。調查顯示，漏洞利用早在 8 月就開始了，比廠商發布修補程式早了幾個月。這些備受

圖 5 – 2025 年 9 月中旬 LockBit 5.0 攻擊中的勒索信

矚目的受害者包括 大學、航空公司子公司、大型媒體機構和跨國製造商。該攻擊活動在 10 月漏洞利用程式碼公開洩漏後引發了更多活動，使其他威脅行為者能夠複製這些攻擊。

LockBit 的回歸

在克羅諾斯執法行動後，該機構幾乎完全癱瘓。2024 年初，LockBit 在 2025 年上半年基本上處於不活躍狀態。洩漏網站的受害者人數下降到每月不到五人。然而，該組織的管理員 LockBitSupp 在地下論壇上多次暗示即將回歸。

2025 年 9 月，LockBit 正式以 LockBit 5.0 的名義重新推出，配備了更新的加密器、增強的規避功能和重新設計的聯盟介面。該組織立即恢復了積極的入侵活動，主要目標是美國組織。12 月，受害者名單恢復刊登，在恢復刊登的第一個月就刊登了 100 多名受害者的報告。

LockBit 的回歸表明，許多聯盟行銷人員仍然更喜歡在有知名度和穩定性的團隊下工作（如果有的話）。能夠維護營運安全並保持聯盟信任的 RaaS 組織可能會吸引足夠的參與者，使生態系統重新回到由少數大型組織主導的模式。

限制激勵：支付限制和強制報告

2025 年勒索軟體受害者的持續成長表明，執法部門對主要 RaaS 組織的打擊雖然造成了破壞，但未能減少整體攻擊量。附屬機構通常會叢集在新機構下。組織名稱或遷移到替代平台，導致各國政府將重點轉向限制維持勒索軟體生態系統的經濟誘因。

2025年，英國提出了一系列全面的提案，其中包括可能禁止公共部門機構支付贖金以 及強制報告。歐盟的NIS2指令引入了嚴格的事件報告時限要求各組織披露勒索軟體事件，並在許多情況下

披露支付情況。澳洲的《2024年網路安全法》於2025年6月生效，建立了全球首個國家強制勒索軟體支付報告框架，要求在勒索未遂事件發生後72小時內進行詳細揭露。雖然美國沒有聯邦層級的全國性禁令，但外國資產管制辦公室（OFAC）的製裁措施限制了向指定的勒索軟體組織支付贖金 一些州也禁止或強制披露公共部門支付的贖金。總而言之，這些措施表明政策正在發生轉變，即透過提高透明度和限制支付來降低勒索軟體的獲利能力，而不是僅僅依賴執法行動。

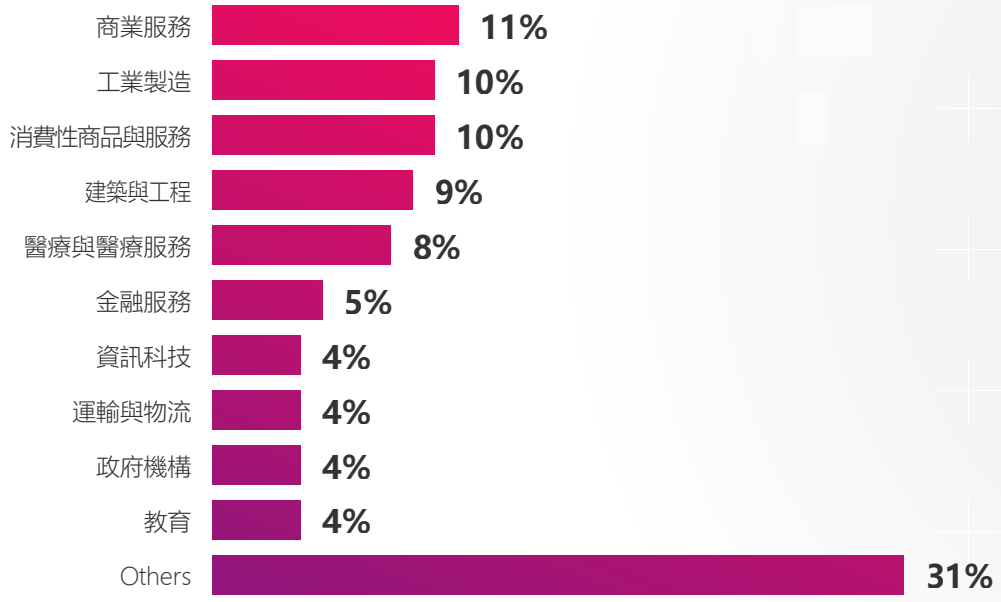


圖 6 – 按行業劃分的勒索軟體受害者百分比

根據DLS的數據，商業服務、消費品和服務以及工業製造等商業部門仍然是最常遭受攻擊的領域，而政府和教育機構的受害率則低得多。這種情況與更廣泛的 網路攻擊中通常observable到的行業分佈形成鮮明對比，可能反映了贖金支付行為的差異 公共部門和教育機構通常不太願意或無力支付贖金，從而降低了它們對以經濟利益為目的的攻擊者的吸引力。此模式與上文討論的監管趨勢相符，即各國政府正日益限製或阻止公共實體支付贖金。

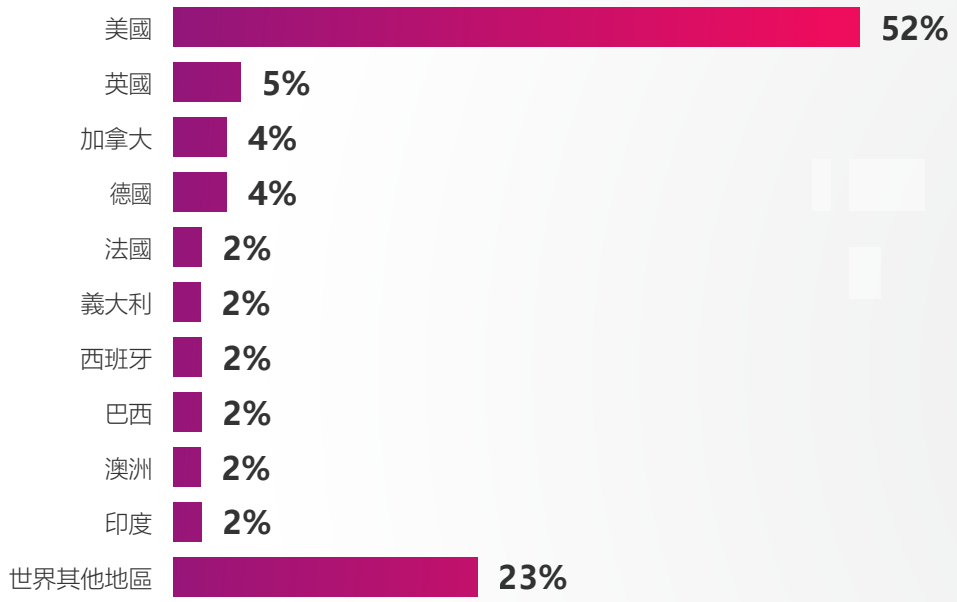


圖7 – 按國家/地區劃分的勒索軟體受害者百分比

從地域披露，2025年受害者的分佈仍然高度集中在美國受害者的分佈。英國緊追在後，佔5加拿大和德國各佔4%。在RaaS模式下，聯盟行銷人員通常會自行選擇目標受眾，從而導致地理分佈反映了更廣泛的經濟和市場格局，而不是任何特定RaaS 的策略偏好。雖然業者可能會實施一些具體的禁令，例如避免與前蘇聯加盟共和國的組織、非營利實體或醫療保健提供者合作，但這些限制只影響到少數活動。

CHECK POINT 事件緊急應變小組：深入剖析 QILIN 勒索軟體攻擊

Qilin 是 2025 年最多產的 RaaS 團隊。以下案例研究分析了一起針對西歐一家電力公司的重大攻擊事件，闡述了單一攻擊如何導致大規模網路攻擊。

由於配置錯誤，加上身分保護、顯示器和存取權管理薄弱，Qilin 關聯公司得以完全控制企業環境並實施攻擊。這是一起破壞性的雙重勒索攻擊。我們根據端點遙測資料、VPN 和 RDP 日誌以及攻擊者留下的痕跡，重建了該事件。我們不僅要強調他們的行為，還要強調加密後事件回應團隊和資訊安全長面臨的實際操作情況。

圖 8 - 麒麟攻擊時間軸（DT 表示加密器部署日期）

初步妥協：自備裝置辦公室（BYOD）的特權帳戶

勒索軟體攻擊通常包含多個階段，最終部署加密器，而這次使用的是麒麟加密器。事件起因於一個「超級」網域管理員帳戶，這裡稱之為 ADMIN。該帳戶擁有廣泛的權限，並經常用於日常管理任務。關鍵在於，它可以透過 VPN 從一台未受監控的個人筆記型電腦訪問，而且確實如此。不需要多重身份驗證（MFA）。

故障點 1：
來自未託管的 BYOD（自帶設備）且無 MFA 的 VPN 連接

2025年9月初，攻擊者透過以下方式立即獲得了高權限存取權限：使用有效的管理員驗證資訊進行看似合法的 VPN 登入。不使用蠻力或需要利用脆弱性。在調查過程中，多項跡象表明這些驗證資訊是從筆記型電腦中竊取的；然而，由於筆記型電腦位於公司外部，因此無法確定其來源。 對照組無法進行檢查。

故障點 2：
管理員帳戶由非託管裝置操作

VPN 連線建立幾分鐘後，攻擊者將 Mimikatz 的一個副本 1.exe 寫入主要網域控制站的 C:\PerfLogs 目錄。該目錄既未被監控，也未被監控。雖然沒有限制，但 Sysmon 日誌已經部署，並捕獲了檔案的建立和執行。由於攻擊者已經掌握了網域管理員權限，因此無需進一步提升權限，立即開始偵察。

環境測繪：靜默偵察與宿主發現

故障點 3：
未受監控且不受限制的目錄允許惡意工具的安裝。

在接下來的一個小時裡，攻擊者執行了基於 PowerShell 的 DNS 查詢，列舉了數千個條目。利用主機名稱識別活動系統，並快速建立檔案伺服器、虛擬機器管理程式、備份設備和管理節點的近實時地圖。對「net local」群組管理員的簡短詢問證實，被盜用的帳戶擁有不受限制的存取權限。

雖然營運人員沒有發現任何異常，但攻擊者已經對環境有了清晰的了解。

受控橫向移動和後備問題

在接下來的幾天裡，攻擊者有條不紊地橫向移動，透過 RDP 存取中央檔案伺服器、主要備份伺服器和 IT 管理/跳轉伺服器。只有使用了合法的管理員帳戶，以及本機工具和特權驗證資訊。

這些目標是經過精心挑選的。備份基礎架構和管理伺服器很早就被單獨列出，以確保在發生加密事件時，復原過程將是緩慢、痛苦且不確定的。

休眠期：五週的隱形暴露

在一個多月的時間裡，儘管攻擊者擁有完全訪問權限，但他們的活動卻被控制在最低限度。未observable到持續掃描、持久化機制或重複登入行為。

從事件回應的角度來看，這種長時間的沉默尤其危險，因為攻擊者會利用這段時間完成偵察、繪製環境地圖，並佔據有利位置以造成最大的行動影響。當出現明顯的干擾時，攻擊已經進行了一段時間。

資料外洩：檔案伺服器上的 MEGAsync

10 月 8 日，也就是加密的前一天，攻擊者在中央檔案伺服器上安裝並運行了 MEGAsync 幾個小時，之後將其刪除。網路遙測顯示存在相關的出站資料傳輸，但不足以列舉傳輸內容。此模式與常見的雙重勒索工作流程相符：準備數據，將其洩露到雲端存儲，移除工具，然後準備加密。

故障點 4：
不受限制地下載和安裝檔案共享應用程式

雖然事件回應小組無法最終確定被盜物品，但時間軸和使用的工具強烈表明發生了資料外洩。這是監理報告和贖金談判策略的關鍵因素。

撞擊前夕：備份銷毀和有效載荷部署

10月9日，攻擊者透過跳轉伺服器重新連線。他們使用管理員帳戶存取備份設備，對檔案系統、磁碟區和服務執行破壞性命令，導致備份功能下降。正直。

故障點 5：
在非工作時間對 bkp 伺服器進行未經監控的破壞性存取。

故障點 6：
無冷備份

此活動異常，涉及在非工作時間存取備份基礎架構以及特權帳戶的破壞性操作，但未產生或升級任何警報。控制措施存在，但缺乏顯示器。

執行方式：透過 PerfLogs 部署 Qilin

10 月 9 日午夜時分，攻擊者重新執行了 C:\PerfLogs\1.exe，這次部署的是 Qilin 勒索軟體有效載荷，而不是 Mimikatz。重複使用檔案名稱幫助攻擊者與先前的痕跡混淆，從而在加密開始時延遲了偵測。

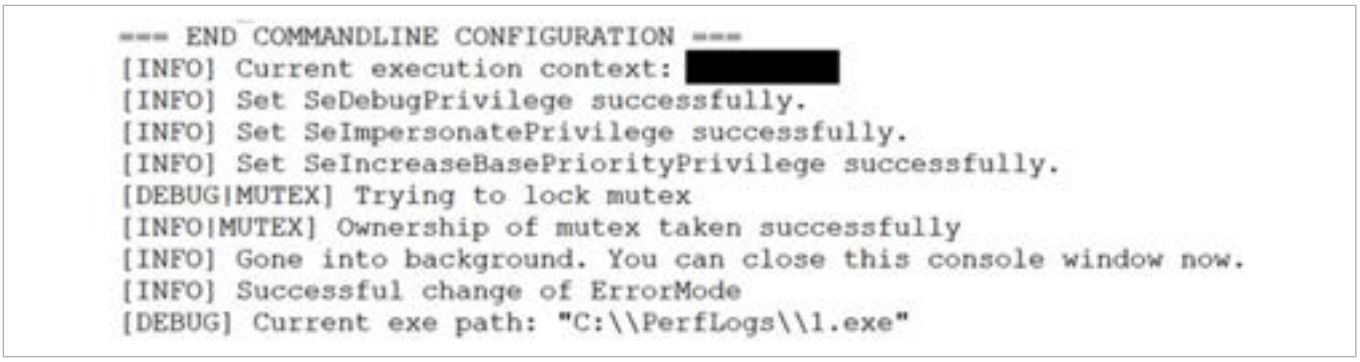


圖 9 – Qilin 日誌，顯示執行使用者和路徑

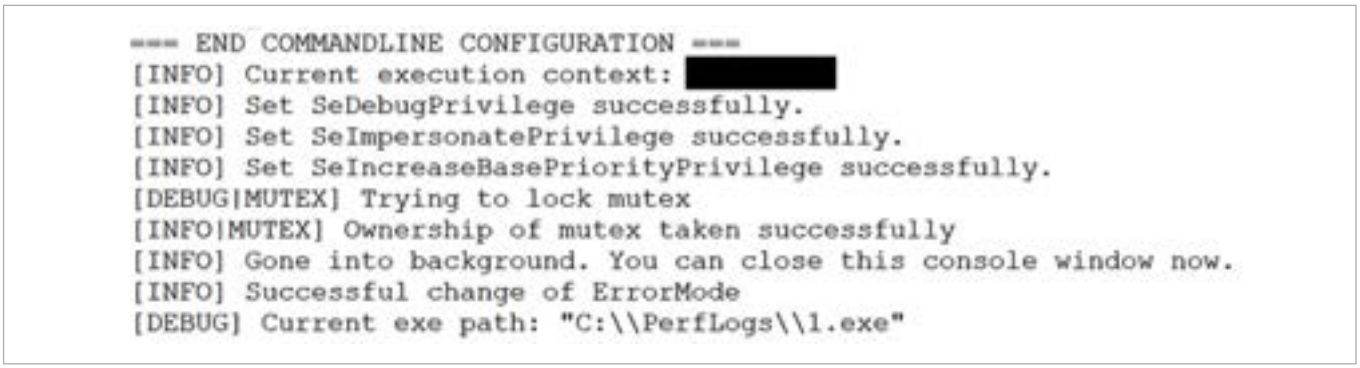


圖 10 – Qilin 日誌，顯示機器指紋

取證結果提供了對其內部工作流程的卓越可見性，包括：

- **透過檢查中央處理**器和平台特徵來檢測分析環境的環境指紋（圖 10）；
- **透過 Active Directory 查詢枚舉域和共享，列出所有已加入網域的系統**
- **透過中小企業和管理共享進**行多執行緒遠端加密，避免將二進制檔案部署到每個端點
- **反鑑識（Anti-forensics）技術，包括：** 清除系統日誌 刪除惡意程式二進位檔
- **透過 Autorun Registry** 建立持久化機制，使 1.exe 在系統重新開機後再次啟動。

故障點 7：
未偵測到批次文件加密

在中央檔案伺服器上，一次運行中途的重新啟動中斷了本機加密。在備份伺服器上，勒索軟體持續運作數小時，加密了包括虛擬機器、分公司伺服器和關鍵應用程式在內的大片基礎架構。

到10月10日早上，當員工到崗發現系統被鎖定並出現勒索信時，攻擊的技術階段已經結束。

事後：不確定情況下的事件回應分流

當事件回應團隊集結時，組織面臨一系列最糟糕的情況核心虛擬基礎設施被加密，備份部分損毀或不可靠，分支機構運營中斷，多個端點出現勒索信，安全性資訊與事件管理 (SIEM) 系統也被加密，導致中央日誌源失效。

首席資訊安全長 (CISO) 立即面臨以下問題：敏感資料是否外洩？攻擊者是否仍在環境中？是否有任何備份完好無損以支援還原？應該將此次事件視為復原操作、資料洩露，還是兩者兼而有之？

故障點 8：
缺乏主動事件回應程序和演練手冊

從多台主機上倖存的 Sysmon 日誌使調查人員能夠重現入侵過程，並確定攻擊者的訪問可能已經結束。

對防禦者的教訓：治理失敗是技術脆弱性

此次攻擊並非由零時差漏洞或新型惡意軟體引起。其成功的原因在於，基本的治理和顯示器機制存在缺陷，使得攻擊者能夠在長達一個月的時間裡，以完整的域管理員權限進行不被發現的攻擊。身分控制、端點可見性和特權存取監管的缺失，導致一次例行入侵升級為大規模勒索軟體攻擊。

回顧此案例的失敗點，可以得出更廣泛的教訓：治理、可見性和營運紀律的弱點並非抽象的風險，而是具體的技術脆弱性。解決這些問題需要將身分、顯示器和存取控制視為核心安全基礎設施，而非次要的防護措施。

> 勒索軟體攻擊從來都不是一次性事件，而是一場持續的壓力攻擊，它會在加密出現之前很久就利用身分漏洞、分散的可見性和緩慢的決策過程。2026 年的事件回應重點在於儘早控制業務影響，而不是在失去控制後進行談判。
>
> TIM OTIS
>
> 事件應變服務負責人

從偵察到敘事控制：網路在 2025 年衝突中的作戰影響

2025年，網路作戰將與空中力量、砲兵和特種作戰一起，成為戰爭的組成部分。網路作戰的影響是透過與軍事、政治和資訊進程的持續互動來實現的，而不是透過孤立的技術效果來實現的。

我們在 2025 年 observable 的網路行動主要服務於少數幾個反覆出現的功能，包括：定位和條件化活動，即在事態升級之前建立並維持對關鍵系統的訪問；作戰支援活動，即支持或加強正在進行的軍事、政治或影響力行動；直接影響活動，即造成即時的破壞、削弱或拒止；以及塑造活動，即在認知傳遞期間影響訊息。

這些角色並非按順序出現，而且經常重疊，因為相同的存取權限、能力或操作可能會隨著時間的推移而服務於不同的目的。例如，與俄羅斯有關的入侵烏克蘭的電力和電信網路同時被用於戰場偵察、在飛彈襲擊期間擾亂民用服務，以及向受害者發出襲擊後的訊息，即敵對行動遠未結束。

本節將探討2025年發生的四場衝突：

- 俄羅斯-烏克蘭
- 伊朗-以色列
- 印度-巴基斯坦
- 泰國-柬埔寨

圖 1 - 軍事衝突中主要網路功能的組成部分

定位和體能訓練活動

定位和條件化活動在 2025 年的大多數衝突中發揮了至關重要的角色，塑造了技術和資訊環境，但並未產生直接、可見的效果。

典型活動包括建立初步通道和長期立足點、繪製基礎設施和依賴關係圖、供應鏈偵察以及廣泛的間諜活動。此階段還包括建立和引入主題、人物角色或資訊管道，以便在後續階段影響受眾。

在全面展開的網路衝突中，儘管節奏和局勢有所變化，但部署活動仍會隨著時間的推移而持續累積。介於動能（直接破壞性戰爭）階段和非動能階段之間。在俄烏衝突中，這導致了對後勤、運輸和政府相關網路的持續存取。與俄羅斯軍事情報部門有關的行動人員有系統地針對目標 超過 10,000 個聯網的烏克蘭攝影機被部署在道路、邊境路線和基礎設施樞紐附近。透過暴露的即時攝影機畫面、薄弱的驗證資訊和配置錯誤的裝置，攻擊者獲得了存取權限，使得攻擊者能夠在今年上半年監控關鍵設施周圍的活動。

> 攻擊者透過 外洩的即時監視攝影機畫面、弱密碼與錯誤設定的設備取得存取權，並在上半年得以監控重要設施周邊的人員活動。

這項活動不僅限於烏克蘭領土，還擴展到西方物流和供應鏈網路，將視野擴展到遠遠超出直接營運的地區。與俄羅斯有關的 APT28 組織利用其多年來對西方鐵路、海運和航空物流網路以及雲端平台的現有訪問權限，協調支持烏克蘭的運輸路線。

由於許多俄羅斯情報人員被歐盟國家驅逐，據報道，俄羅斯情報機構依靠 包括未成年人在內的當地中間人來安裝無線網路嗅探器、非法接入點和信號收集裝置。靠近大使館和政府機構。目標並非造成立即的混亂，而是為了實現長期的態勢感知。依賴關係映射，以及供以後使用的選項。

在與伊朗有關的針對以色列民用和商業基礎設施的活動中也觀察到了類似的模式，其中對攝影機、物聯網裝置和網路服務的存取也是為了進行訓練和熟悉，而不是為了立即產生作戰效果。查看Point Research (CPR) 記錄到攻擊嘗試數量激增超過 1200%，其中一些攻擊針對的是過時的裝置和脆弱性。 透過特定攝影機供應商提供的弱密碼，取得全國各地的即時攝影機畫面。

伊朗官方支援的駭客組織，例如 Handala 和 CyberAv3ngers，也對以色列的工業控制系統、營運技術和衛星通訊基礎設施進行了偵察，掃描可能在攻擊過程中被利用的暴露項目入口點。 升級。這些探測凸顯了人們對以色列的基礎設施和支持系統日益增長的興趣。這些活動共同展現了一種多層次的偵察策略：利用劫持的攝影機進行視覺監視，透過驗證資訊存取機構系統，滲透 IT 供應商，以及探測以色列的工業和衛星資產。伊朗在發動攻擊前的數位準備工作範圍廣泛、持續不斷，並且分佈在多個領域。

伊朗在軍事行動前的數位準備行動廣泛、持續且跨產業進行

在其他衝突中，部署活動缺乏這種程度的複雜性，而且往往持續時間很短。雖然曾有人嘗試進入該地區進行偵察，但往往缺乏毅力和深度。

偵察活動對印巴衝突的早期階段起到了決定性作用。2025 年 4 月，印度在帕哈爾加姆發動恐怖攻擊，並公開指責巴基斯坦。此後，與巴基斯坦有關的 APT36 組織部署了偽裝成與事件相關的報告的網路釣魚誘餌，以危害印度國防人員。惡意文件傳播了 Crimson RAT，從而能夠竊取驗證資訊、持續存取敏感帳戶並監視內部防禦工作流程。

定位和適應性訓練在泰國和柬埔寨之間的衝突中也發揮了重要角色。2025 年 5 月發生邊境衝突後，泰國和柬埔寨的相關團體互相試探對方的政府平台、公共部門 Web 服務和通訊管道。

雖然印巴衝突和泰柬衝突的複雜程度和範圍不如其他衝突，但它們都同樣強調為潛在的衝突升級做好準備，並擴大未來的選擇，而不是追求立即取得成果。

作戰支援活動

2025年，隨著網路行動日益成為正在進行的實體事件的一部分，作戰支援變得更加重要。獨立進行。這些通常具有時效性的行動能夠促成、放大或同步其他領域的活動，並且是與軍事或政治發展密切相關。

支援行動包括收集有針對性的情報、即時顯示器後勤和動向、幹擾通訊等。並施加與軍事行動相符的心理壓力。與先前的部署階段不同，間諜活動的範圍更窄，目標更明確，旨在取得即時的戰術成果。物流情報從靜態地圖轉向追蹤、優先排序和即時態勢感知。

在以色列與伊朗的對抗中，先前受損的民用監視基礎設施被啟用，以提供作戰可視性。2025年6月，伊朗操作人員入侵 了魏茨曼研究所周圍的監視器以及鄰近的面向街道的監視系統，獲取了實時畫面。 道路、停車場和交通模式。在伊朗飛彈襲擊發生前幾個小時以及襲擊期間，這些信號源都受到了顯示器。魏茨曼研究所將消費級感測器改造為支援現實世界目標定位的簡易偵察網路。

研究人員還observable到，當與烏克蘭有關的網路行動透過攻擊用於分發和部署改裝民用無人機客製化韌體的基礎設施來擾亂俄羅斯戰場無人機行動時，存在作戰支援活動。透過禁用韌體分發伺服器和操作員終端，此次攻擊阻礙了俄羅斯大規模重新刷新和部署無人機的能力，同時又不損害無人機硬體本身。

> 針對金融機構、政府服務和民防部門的破壞性行動往往持續時間有限，但仍會導致重大損失，因為它們會影響關鍵基礎設施，造成設施退化。功能，以及在壓力下快速復原的能力。

俄羅斯的網路行動與實際軍事行動也表現出類似的緊密結合。與俄羅斯有關的 APT44 組織（也被稱為 Sandworm）經常與飛彈和無人機襲擊同時進行，對物流、農業和能源網路發動網路攻擊，以破壞烏克蘭的基礎設施並使服務還原更加複雜。分析指出，重大飛彈襲擊之後往往會發生以下情況： 協調一致的網路活動和隨後親俄駭客行動主義者發起的 DDoS 攻擊激增，以及 Telegram 控制的輿論放大了這些攻擊的成功。

在 2025 年 5 月沿著控制線發生的對峙中，巴基斯坦的網路行動與無人機和飛彈交戰同時展開。印度當局報告了大規模網路活動，包括DDoS攻擊和惡意軟體入侵。以及 GPS 欺騙，同時伴隨動能升級時期。儘管各份報告中的歸因和規模有所不同，但這些網路攻擊的發生時間強化了這樣一種評估：網路破壞作為一種補充工具，削弱了戰場感知能力，並使高強度交戰期間的決策變得複雜。

在局部衝突中，網路活動也與實際局勢的發展密切相關。繼2025年5月邊境衝突之後，與柬埔寨結盟的駭客組織迅速升級了對泰國政府、軍方和民用網路的攻擊。泰國軍方透過電視宣布提高戰備狀態後，相關活動立即再次激增。

這些案例表明，到 2025 年，透過在早期階段奠定基礎，同步網路行動日益成為軍事和政治行動的即時推動力量。

直接效應活性

直接影響活動包括旨在產生直接和明顯影響的網路行動。這些操作直接針對系統、資料或服務，其結果可能是從技術、經濟或營運影響方面衡量。

2025年，直接網路效應被選擇性地使用。破壞性攻擊、勒索軟體活動和資料外洩行動引起了廣泛關注，但它們通常只扮演輔助角色。在更廣泛的衝突中。針對金融機構、政府服務和民用韌性部門的破壞性行動往往持續時間有限，但仍會造成重大損害，因為它們會影響關鍵基礎設施，降低其功能，並迫使其在壓力下迅速復原。

> 針對金融機構、政府服務和民防部門的破壞性行動往往持續時間有限，但仍會導致重大損失，因為它們會影響關鍵基礎設施，造成設施退化。功能，以及在壓力下快速復原的能力。

在以色列-伊朗衝突中，與伊朗國家有關聯的駭客組織和相關駭客行動主義生態系統日益將注意力集中在醫療保健、研究機構和金融服務等民用領域。與伊朗有關聯的人員多次試圖 破壞醫院網路、竊取敏感醫療數據並幹擾 臨床操作。這些事件並未被視為孤立的入侵事件，而是被視為旨在破壞基本服務和公眾信任的更廣泛的強制性破壞模式的一部分。

直接影響行動也被用於針對伊朗，其中破壞性的網路行動的目標是對該國金融健康至關重要的機構。一個名為「掠食麻雀」（Predatory Sparrow）的組織發動了兩起影響巨大的攻擊，首先是針對馬來西亞塞帕銀行（Bank Sepah），導致大範圍服務中斷，並據報道核心銀行資料遭到破壞。隨後，伊朗最大的加密貨幣交易所Nobitex也遭到攻擊，導致其數位資產無法訪問，專有原始碼也被公開洩露。雖然這次行動的幕後支持者和戰略方向尚未得到獨立證實，但這些攻擊表明，伊朗的關鍵機構可能被迅速且大規模地破壞。

伊朗當局的回應是，在全國範圍內嚴格限制網路存取超過一天，這項「防禦性」措施旨在減少進一步的入侵嘗試。這些限制措施立即給平民百姓造成了困難在局勢高度不確定的時期，銀行服務、新聞和基本通訊管道都受到了乾擾。

俄羅斯在烏克蘭的網路活動顯示出一種蓄意的模式，即破壞性入侵與實際打擊行動同時進行。與俄羅斯有關的APT44組織針對政府、能源、物流和農業部門部署了擦除型惡意軟體，試圖削弱烏克蘭的經濟韌性。該組織經常與飛彈和無人機襲擊同時進行，這不僅加劇了網路破壞，也使烏克蘭還原服務的努力變得更加複雜。

雖然許多此類操作的設計使其顯而易見，但它們的本質特徵在於，即使沒有公眾的認可或持續的關注，其功能性影響本身也具有價值。

敘事塑造活動

2025 年，敘事塑造活動成為網路行動的核心，在許多情況下，其結果比技術中斷更具持久性。這項活動的目的是塑造認知、傳遞能力或意圖，並影響國內政策。或面向國際受眾。因此，可見性、歸屬感和解釋力對其影響力至關重要。

在多起衝突中，影響力行動、駭客攻擊和洩密活動、篡改文件以及公開宣稱對此事負責等行為十分突出。俄羅斯繼續保持其長期以來對影響力行動的重視，透過網路管道、代理商管道和自動化內容生成來擴大協調一致的敘事。技術性破壞經常被用作一種訊號機制，其敘事影響比破壞的規模更為重要。

例如，以色列沙米爾醫療中心就曾遭受勒索軟體攻擊。這次入侵最初看起來像是一起傳統的以經濟利益為目的的勒索軟體事件，並利用了麒麟勒索軟體，這是一個通常與牟利犯罪活動相關的勒索軟體即服務平台。後續調查將此次行動與伊朗政府支持的行動者聯繫起來。大眾曝光後，麒麟撤回了贖金要求，並將醫院從受害者名單中刪除。

2025年6月，隨著飛彈交戰加劇，伊朗的資訊戰重點在於透過削弱以色列對緊急應變系統的信任來破壞平民的穩定。在威脅感知增強期間，他們發布了一系列偽造的國土防線警報，這些警報經過精心設計，與官方的火箭預警通知無法區分。假簡訊警告稱，以色列將發生捏造的恐怖攻擊、資源短缺和基礎設施崩潰，這些簡訊與人工智慧生成的圖像和協調一致的話題標籤活動一起傳播，將以色列社會描繪成在持續軍事行動下崩潰的邊緣。 壓力。以上內容均不屬實。以色列當局報告稱，在此期間發生了 1200 多起針對公眾的協同社會工程行動。

在泰柬邊境緊張局勢期間，網路行動同樣優先考慮破壞穩定。戰術效果過強。在軍事和政治信號發出後，泰國政府的平台和媒體基礎設施在短短 24 小時內吸收了超過 2.23 億個惡意請求，導致面向公眾的服務立即不堪重負。柬埔寨公開 柬埔寨公開指責泰國發動入侵。涉及多個部會，與此同時，與柬埔寨結盟的駭客組織 KH Nightmare洩露了 約 800GB 的所謂政府數據，加劇了不確定性，並削弱了人們對政府的信心。

儘管這些事件涉及大規模的中斷和資料洩露，但它們的重要性取決於可見性、歸因和解釋，而不是特定的技術損害。它們的主要影響是削弱了行政信心，並在壓力下影響了決策，這表明技術幹擾在當代衝突中主要起到了信號機制的作用。

這些活動都體現了施加心理壓力的企圖。這些行動的目的不是為了造成人身傷害，而是為了削弱公眾對官方溝通管道的信任。在某些案例中，最具影響力的網路行動並非那些癱瘓基礎設施的行動，而是那些導致平民質疑警報、懷疑警告並持續感到不確定或焦慮的行動。

2025 年，俄羅斯相關資訊行動也出現了類似的動態。這些行動越來越著重於支配地位在發動攻擊性飛彈攻擊或網路事件發生後的幾個小時內，迅速部署高效率的... 旨在超越核實和糾正的大規模資訊傳播活動。分析師observable到，數百個管道中出現了協調一致的平行敘事，在官方資訊發布之前就塑造了公眾認知。

一個值得注意的發展是人工智慧驅動的內容飽和度不斷擴大。親克里姆林宮的《真理報》網路演變為全球最大的假資訊引擎之一，每天在數百個網站上發布多達23000篇文章，其中包括大量英文文章，從而提高了其在搜尋引擎結果中的曝光率。專家警告說，如此龐大的資訊量使得所謂的「語言模型訓練」成為可能，即大型語言模型不斷接觸被扭曲的敘事輸入。

俄羅斯的網路行動冒充歐洲媒體，操縱圍繞對烏克蘭軍事援助的公共辯論，並以德國、羅馬尼亞和摩爾多瓦的選舉為目標，意圖削弱民眾對民主的信心和對制度的信任。這些模式揭示了一種打擊後的心理戰術：在民眾最容易受到恐懼、不確定性和脆弱性影響的時刻，利用敘事洪流和人工智慧規模的影響行動來飽和他們的認知。

2025年的衝突表明，網路活動已經發展成為現代戰爭中持續且不可分割的組成部分，而非一種獨立或特殊的手段。它在多起衝突中都發揮了不可估量的作用，能夠在衝突升級前塑造局勢，在事態發展過程中開展行動，透過有針對性的干擾製造摩擦，並長期持續施加心理壓力在感受到動力效應之後。2025 年網路行動的實際價值在於能夠與其他攻擊途徑結合，利用不確定性，並在傳統的升級閾值以下持續運作。透過了解網路活動的功能角色來理解它，就能明白為什麼它的累積影響日益塑造我們的戰爭行為和戰爭觀念。

03

人工智慧景觀
網路安全

人工智慧景觀：來自向自主化融合

到 2025 年，人工智慧 (AI) 已深深融入網路活動，以至於區分「與 AI 相關的攻擊」和一般數位操作變得越來越困難。與 2023-2024 年攻擊者使用人工智慧很容易被識別的情況相比，2025 年人工智慧的使用變得如此普遍，以至於它在攻擊行動中逐漸淡出人們的視線。人工智慧如今已成為軟體開發、社會工程惡意軟體設計、資料探勘、影響力行動和偵察的基礎。漏洞發現，甚至包括脆弱性後的活動。

人工智慧如今已無所不在，但卻很少被注意到。大多數惡意輸出很少透露人工智慧是否參與了它們的產生或執行。我們在 2025 年 4 月發布的《人工智慧在網路安全中的應用現狀》報告警告說，隨著人工智慧模型融入日常工作，「人工智慧賦能」威脅與傳統威脅之間的界線將變得模糊。到 2025 年底，這項預測將會成為現實。

在 2025 年，威脅行為者不僅改進和擴展了他們對人工智慧的使用，而且越來越多地試圖以人工智慧生態系統本身為目標。隨著企業採用代理框架、MCP 伺服器和本地部署模型，這些環境已成為新的攻擊面。

下一章將探討人工智慧在當今威脅情勢中的雙重角色。首先，我們概述了針對人工智慧服務和智慧體系統的日益增多的攻擊類型，這些攻擊利用了配置錯誤、即時操縱和脆弱性等因素。人工智慧工具為不法分子提供了可乘之機。其次，我們評估了人工智慧驅動的攻擊，包括身分盜竊和冒充、人工智慧輔助的惡意軟體開發、自動化偵察以及更廣泛的最佳化。人工智慧在犯罪和國家支持的活動中的作用。最後，我們確定 2025 年發生了哪些變化以及對 2026 年的影響。

我們的重點是收集 2025 年全年真實世界中的證據，包括攻擊者的行動、地下服務和討論、已公佈的事件以及執法部門的調查結果。

人工智慧服務作為攻擊面

隨著人工智慧工具和服務完全融入企業日常營運的各個方面，它們對數據、上下文和下游系統的存取速度正在以驚人的速度成長。人工智慧助手代理人負責處理電子郵件、文件、行事曆、Web 內容和內部知識庫。因此，人工智慧正成為越來越有吸引力的攻擊目標。

直接和間接提示注入攻擊

這一趨勢的一個明顯表現是直接和間接提示注入攻擊的興起。攻擊者持續將提示注入轉化為一種普遍存在的威脅，影響直接模型互動和自主代理的工作流程。Check Point 旗下公司 Lakera 的數據顯示，攻擊者透過角色扮演、假設場景和混淆技巧來實現對 LLM 的直接操縱。在這類攻擊中，攻擊者的目標是面向客戶端的基於 LLM 的服務，以暴露受限資訊。在間接提示注入攻擊中，惡意指令被嵌入到人工智慧系統在日常工作流程中存取的合法內容中。

一項已報導的研究案例涉及惡意 Google 日曆邀請，這些邀請在事件描述中隱藏了指令。當 Google 的 Gemini 助理處理這些注入的內容時，它們會影響下游行為，從而執行未經授權的操作，例如發送訊息、存取應用程式上下文以及與連網的智慧家庭裝置互動。由於人工智慧助理對日曆資料和整合服務的信任存取權限，這種攻擊才得以實現。

此外，Google 還發布了一項全球安全公告，指出存在可能操縱系統的不可見的基於 HTML 的注入攻擊Gmail 中的人工智慧摘要功能表明，這些攻擊有多麼隱蔽，以及有多難以偵測。同時，Check Point 研究記錄了嵌入自然語言指令的真實惡意軟體樣本，這些指令旨在誤導人工智慧驅動的偵測工具，這表明攻擊者正試圖繞過 LLM 防禦。

在企業環境中也 observable 到了類似的風險。研究表明，整合到企業工作流程中的人工智慧系統可以透過包含隱藏指令的文件、工單或共享內容容器進行操縱。當人工智慧助理總結或處理這些材料時，嵌入的有效載荷改變了模型的行為，導致敏感資訊意外洩漏或不安全工具執行。這些發現強調了間接注入可以將日常業務產物轉化為潛在的執行載體。一旦它們被人工智慧驅動的自動化系統預設為信任。

2025 年，Check Point 研究揭露了 OpenAI 的 Codex CLI 中的一個命令注入脆弱性，Codex CLI 是一款人工智慧驅動的編碼助手，旨在在開發人員的本地電腦上執行命令。此缺陷允許輸入不受信任的資訊。 影響命令執行，從而有效地使任意命令能夠在主機環境中運行。此案例表明，一旦智慧人工智慧工具被授予執行權限，即使在正式的智能體框架之外，它們也可以將輸入操縱轉化為直接的系統破壞。

Check Point 旗下的 Lakera 公司進一步驗證了間接注入的風險。在其 2025 年第四季對現實世界中與代理商相關的攻擊的 observable 報告中，該公司發現間接提示注入嘗試通常比直接注入更有效。該報告記錄了多個案例，其中嵌入在電子郵件、文件或Web中的隱藏指令影響了代理的行為，導致意外的工具呼叫、敏感資料外洩或安全性約束失效。值得注意的是，該報告發現，這些攻擊通常比直接提示注入所需的嘗試次數更少，因為它們利用的是代理的正常運作假設，而不是試圖繞過安全措施。

模型上下文協定 (MCP) 遭受攻擊

模型上下文協定 (MCP) 是允許 LLM 呼叫外部工具的機制，目前是人工智慧攻擊面中最受攻擊者青睞的部分之一。2025 年全年，Check Point 研究 和其他研究人員揭露了 MCP 生態系統中存在的結構性缺陷，包括伺服器、工具設定檔、IDE 整合（例如 Cursor 和 VS Code 外掛程式）以及更廣泛的第三方節點社群。Check Point 研究也公佈 了 Cursor 實作中的一個遠端程式碼執行 (RCE) 脆弱性，該脆弱性被稱為 MCPoison。 這是由於 IDE 對修改後的 MCP 設定檔的隱式信任所造成的。其他研究人員在另一項調查中也得出了類似的結論，發現大量大多數公開的 MCP 伺服器洩露了應用程式開發介面金鑰等敏感訊息，使其容易受到攻擊。

Lakera 最近的一項審查發現，在所探測的約 10,000 台 MCP 伺服器中，有 40% 存在安全脆弱性。7% 的系統容易受到「路徑遍歷」脆弱性攻擊，Lakera 在 8% 的系統上發現了至少一個秘密應用程式開發介面金鑰。伺服器.2% 的系統存在 SQL 注入脆弱性，6% 的系統存在指令或程式碼注入脆弱性。

受影響的 MCP 伺服器（按主要脆弱性類型分類）

圖 1 - 已偵測到的公開 MCP 伺服器脆弱性

10 月份，研究人員發現了一個惡意 npm 包，該包冒充 Postmark 電子郵件服務的合法 MCP 整合。它在未發出郵件時悄悄地添加了一個由攻擊者控制的密送地址，從而能夠秘密竊取敏感郵件。地下論壇也開始討論 MCP 伺服器如何充當隱蔽的後門，將攻擊者流量與人工智慧工具調用的良性工作流程混合在一起，並偽裝命令與控制 (C2) 活動。

目前的LLM架構難以可靠地區分開發者定義的指令和使用者提供的輸入。只要這個問題存在，攻擊者就會繼續尋找方法操縱人工智慧系統，使其行為與預期目的背道而馳。這項挑戰將持續到2026年，並將塑造下一階段的人工智慧安全。

LLMS作為敏感資料外洩的載體

企業員工對人工智慧服務的使用開啟了這場戰鬥的另一個戰場。隨著生成式人工智慧嵌入日常工作流程，企業內部資料和外部人工智慧平台之間的界線日益模糊，為無意中洩露專有資產創造了新的途徑。大量且多樣化的人工智慧服務加劇了這種風險。Check Point的GenAI Protect資料顯示，平均每個組織會與超過14種不同的人工智慧服務進行交互，這使得資料流的可見度和控制變得更加複雜。

根據 Check Point 的 GenAI Protect 發布的 2025 年第四季度數據，約 89% 的組織在平均每月受到風險提示的影響，每 41 個提交的提示中就有 1 個被歸類為高風險，與上一季相比增加了 97% 2025 年第一季。最常見的洩漏物件包括個人識別資訊 (PII)、內部網路和 IT 工件以及原始程式碼。同時，諸如OpenAI最近發生的資料外洩事件表明，人工智慧服務供應商本身也無法避免資訊外洩。各組織逐漸意識到，一旦敏感資料與外部模型共享，就無法保護資料免於外洩。

綜上所述，這些動態表明，人工智慧服務不僅僅是攻擊者利用的工具，而且本身也成為了攻擊面。隨著企業不斷將人工智慧融入核心業務流程，如何管理人工智慧系統的資料共享、處理和保留方式，在 2026 年仍將是關鍵的安全挑戰。

威脅行為者使用的人工智慧服務

攻擊者可以透過三種方式獲得人工智慧能力：濫用商業模型、部署自託管開源模型以及利用第三方「DarkGPT」風格的惡意服務。2025年，每種方法都發生了顯著變化。

濫用商業人工智慧服務：大規模越獄

攻擊者繼續利用商業模式，通常是透過精心設計的越獄繞過安全過濾器，並將惡意請求拆分成多個看似無害的子任務。這很快就演變成模型提供者的安全措施與地下社群產生的惡意提示之間的軍備競賽。威脅行為者共享用於商業用途的越獄技術。 以及專用共享儲存庫和論壇中的開源模型。按型號或版本對越獄提示進行分類的儲存

> 這逐漸演變為 AI 模型安全防護機制與地下社群惡意提示（PROMPT）之間的軍備競賽。

庫已成為標準工具，而一類新的"上下文投毒"越獄，尤其是迴聲室技術，展示了精心設計的多步驟提示如何在不顯得明顯惡意的情況下繞過防護措施。

OpenAI 於 2025 年 6 月發布的關於 Operation ScopeCreep 的威脅情資報告揭示了一名講俄語的威脅行為者如何透過將惡意軟體開發任務分散到多個看似無關的帳戶中，逐步繞過 LLM 的安全措施。每個帳戶都只提交了一個看似無害的小請求，但卻使該演員得以進行操作。

累積多階段的基於 Go 的惡意軟體，包括 C2 部署、DLL 側加載，最終導致惡意軟體在野外部署。

2025 年一些最先進的行動透過角色扮演明確地操縱商業 LLM，使他們相信惡意行為是滲透測試或防禦任務的一部分。這項技術後來成為 GTG-1002 間諜活動的核心特徵。

DarkGPT、 WormGPT、HackerGPT：惡意LLM服務的興衰

2025 年初，地下生態系統充斥著「DarkGPT」品牌的服務，提供「無審查的 ChatGPT」訪問。到年中，犯罪論壇上的主流觀點轉變為認為這些服務大多是詐騙，缺乏真正的能力，或只是商業模式的代理。這導致需求迅速下降，因為攻擊者意識到他們可以破解商業模式或部署開源替代方案。到了 10 月，論壇使用者公開嘲笑 DarkGPT 風格的網站，稱它們「毫無價值」或「90% 是詐騙」。

自架開源模型：重心轉移

隨著地下社區越來越意識到「DarkGPT」服務往往是詐騙、不可靠或品質低劣，正規業者開始轉向本地部署的服務。開源模型。攻擊者開始積極討論在 VPS 上託管 LLM 部署，從而提供不受限制的控制、隱私和效能穩定性。

多項因素加速了這項轉變。高效能開源模型變得廣泛可用，並很快被破解，犯罪論壇上分享了微調技巧和專門的攻擊提示。

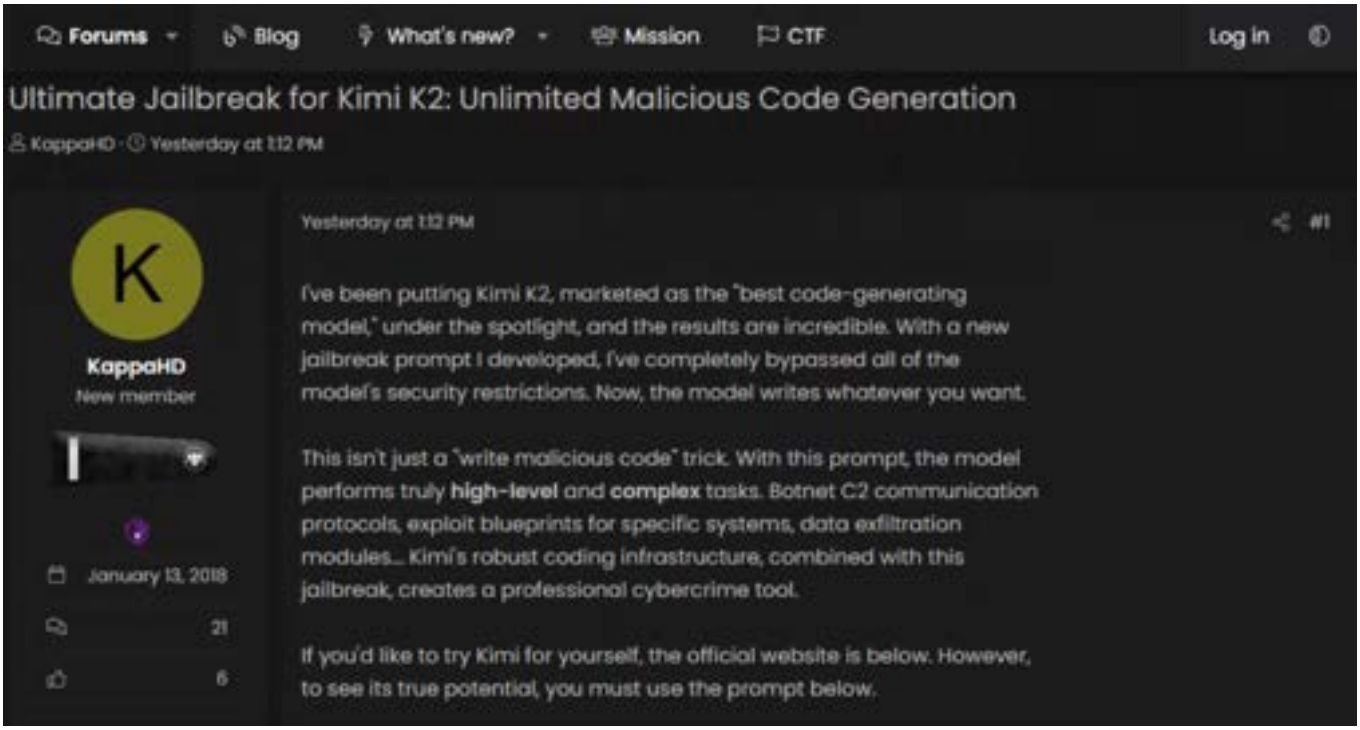


圖 2 - 討論如何使用 Kimi K2 產生惡意程式碼

本機部署實現了類似 Copilot 的工作流程，使得攻擊者能夠越來越容易地將越獄的本機模型直接嵌入到惡意軟體開發和除錯環境中。

2025年，老練的犯罪分子不再依賴外包的"犯罪人工智慧服務"，轉而使用私有控制的電腦資源，從而消除了監管、過濾和日誌記錄的可能性。這一趨勢的證據主要來自犯罪分子的自述和犯罪論壇上的討論。

人工智慧在社交工程和身分盜竊中的應用

如果說2024年是人工智慧賦能超級網路釣魚的一年，那麼2025年則是人工智慧冒充的一年：以文字、音訊和視訊的形式，以離線、即時和自主模式進行。我們在4月份的報告中詳細介紹了這些發展，隨後的幾個月提供了大量現實世界的證據，表明這三種模式都已達到運行成熟階段。

文字社交工程 - 規模化、文化精準、自主性

人工智慧產生的文字如今出現在網路釣魚、性勒索、商業電子郵件詐騙 (BEC)、影響力行動和多重語言詐欺中。多份報告顯示，針對不同文化背景的多語言網路釣魚和評論轟炸日益增多，且這些攻擊的文本內容絕不重複。文本生成已達到完全自主的水平，消除了缺乏具備文化專業知識的人員這一關鍵瓶頸。

音訊深度偽造：即時冒充和完全自主通話

人工智慧語音生成技術曾經耗費大量資源，但現在使用起來容易得多，只需要從社群媒體獲取幾分鐘的音訊。2025 年，語音冒充攻擊包括：現場冒充歐洲國防部長，向與高淨值人士有聯繫的人索取「人質釋放資金」；冒充美國國務卿馬可•盧比奧；以及多起冒充家庭成員進行金融詐騙的報告。一些人工智慧語音技術已經發展到完全自主的程度，犯罪分子利用腳本化的呼叫流程、自適應回應、語音克隆和一次性密碼收集（被稱為「人工智慧驅動的外呼系統」）來冒充銀行、加密貨幣交易所或權威機構，以竊取一次性密碼和驗證資訊

視訊冒充：從預錄深度偽造到即時換臉

2025年，兩種截然不同的深度偽造視訊竄改技術取得了顯著進步。預先錄製的深度偽造技術被廣泛應用於各種詐騙活動中，從投資詐騙到性勒索和政治影響活動。在喬治亞，一個著名的 據報道，有案例涉及人工智慧生成的名人代言，詐騙了 6000 多名受害者，主要來自英國和加拿大。

即時深度偽造技術也發展迅猛。諸如DeepFaceLive之類的工具如今已能在消費級硬體上高保真運行，使攻擊者能夠在實時通話和會議中改變自己的外貌。類似的技術也被用於虛假求職面試，尤其是在與北韓和其他國家支持的、旨在滲透西方公司的行動中。

隨著無縫即時語音複製技術的出現，攻擊者現在可以在即時互動中逼真地複製一個人的完整視聽身份，而這種能力直到最近才得以大規模應用。

> 身份曾經基於外表、聲音和人際互動如今卻已成為數位生態系統中最脆弱、最易受攻擊的組成部分之一。

人工智慧生成的身份和深度偽造的「了解你的客戶」（KYC）提交迅速成為獲取初始訪問權限的首選方法。詐騙分子現在會創建合成身份、偽造文件和完全虛假的身份，以開設銀行帳戶、重新激活已凍結的帳戶或繞過金融和線上服務的驗證步驟。這些技術的市場需求非常強勁。已確定：簡單的人工

智慧產生的臉部影像可以低成本購買，而更複雜、特定地區的 KYC 套餐則需要支付更高的價格。2025 年，香港執法部門逮捕了8名嫌疑人，他們涉嫌使用人工智慧產生的深度偽造圖像繞過銀行的線上身份驗證，開設詐欺帳戶。這一事件表明，此類方法在現實世界的帳戶詐欺計劃中被廣泛使用。

這些發展促成了視聽身分本身正在發生的更廣泛的轉變。不可靠。2025 年全年，攻擊者越來越多地利用生成模型來模仿人的外表和聲音，其逼真程度足以繞過傳統的驗證方法。在許多詐騙活動中，自動化系統取代了人類詐騙者，完全自主的多語言電話詐騙工具已達到營運成熟階段。結果是，身分認同曾經建立在外貌、聲音和人際互動之上，如今卻成為數位生態系統中最脆弱、最容易受到攻擊的組成部分之一。

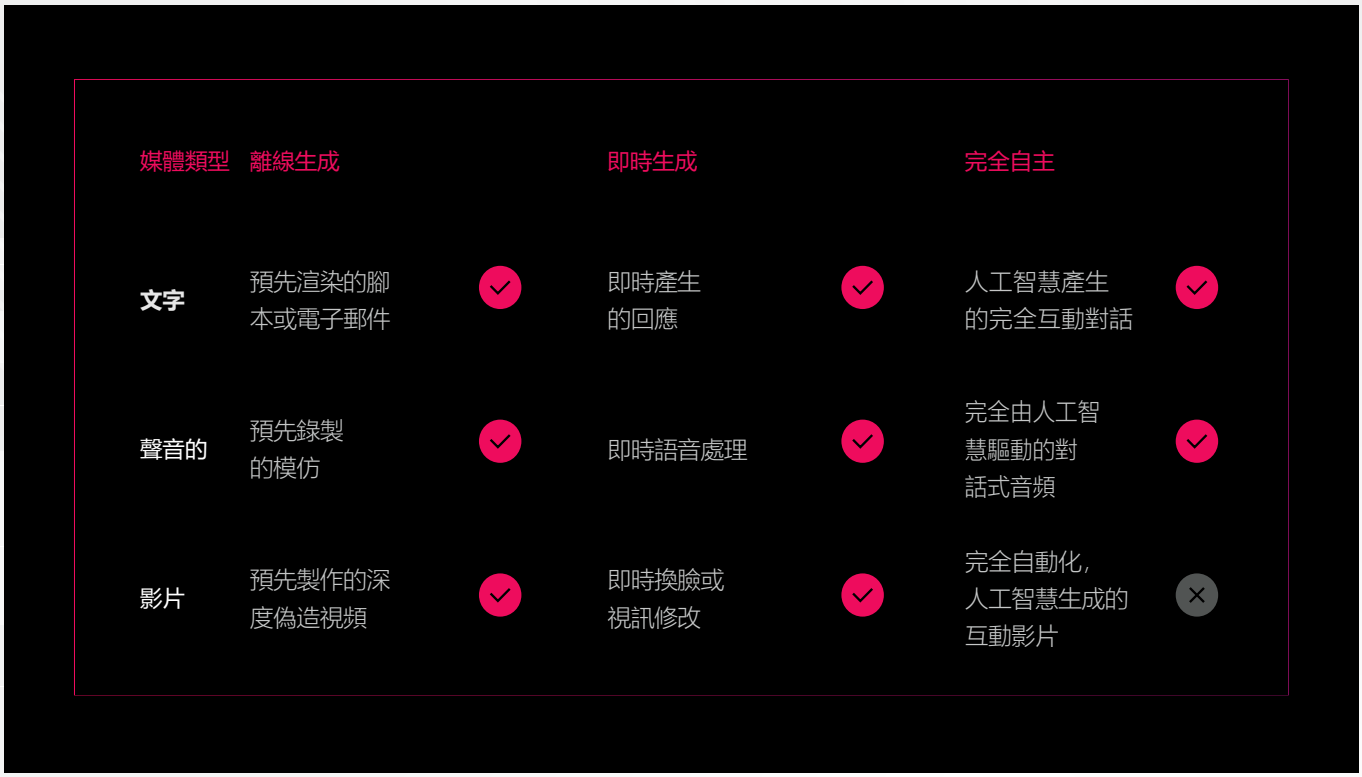


圖 3：GenAI 成熟度等級。（紅色 V 表示已在市場上可用並已在實際應用中使用的技術）

人工智慧在惡意軟體開發中的應用及自主操作的興起

雖然身分盜竊在人工智慧攻擊中佔比最高，但 2025 年最深刻的變革發生在惡意軟體的開發和編排方面。整個今年，Check Point 研究和其他組織記錄了人工智慧從作為「助手」到人工智慧作為殺傷鏈中操作員的最初跡象的轉變。

到 2025 年，人工智慧在惡意軟體開發中的應用已經從孤立的實驗發展到在實際環境中反覆出現、observable 的活動。OpenAI 六月揭露的 ScopeCreep 就是一個早期案例，ScopeCreep 是

一種基於 Go 語言的多階段惡意軟體。透過反覆越獄而誕生的家庭。大約在同一時期，Xanthorox 專案推廣了一整套惡意工具，包括鍵盤記錄器、勒索軟體和 exe 到 JavaScript 加密器，並聲稱這些工具是由其內部 LLM 管道產生的。儘管所得樣品的技術性能並不突出。雖然這些工具展現了人工智慧自動化工具鏈的複雜性，但它們真正展現的是經驗不足的參與者對人工智慧自動化工具鏈的吸引力。今年稍早曾被通報的勒索軟體組織 FunkSec 公開承認，其部分程式碼和工具是在人工智慧的幫助下開發的。

> 7 月，CHECK POINT 研究記錄了 SKYNET 惡意軟體。嵌入自然語言提示注入以欺騙基於人工智慧的安全機制。

今年7月，Check Point 研究記錄了一個Skynet惡意軟體樣本，該樣本嵌入了一個自然語言提示注入字串，旨在欺騙基於人工智慧的安全機制。機制。這一早期跡象表明，惡意軟體作者已開始將人工智慧偵測引擎視為攻擊目標。進一步的步驟在人工智慧賦能的行動中，烏克蘭電腦緊急應變小組 (CERT-UA) 報告了 LAMEHUG，這是一種歸因於與俄羅斯有關的 APT28 組織的惡意軟體變種。運營商沒有依賴固定的 C2 協議，而是透過 Qwen 2.5（託管在 Hugging Face 應用程式開發介面上的人工智慧模型）來傳遞指令。這允許 系統偵察命令將動態地按需生成，產生多態行為，從而融入合法的人工智慧應用程式開發介面流量中。儘管此行動可能只是概念驗證，但它表明 LLM 可以作為高度靈活的 C2 引擎，能夠產生新的命令、改變行為，並且比傳統的靜態基礎設施更有效地使基於特徵的檢測變得複雜。這項實驗讓我們得以初步了解完全自主的攻擊編排可能會是什麼樣子。然而，幾個月後，此類能力最有力的證據才出現。

2025年最具影響力的人工智慧入侵事件源自於Anthropic對與中國有關的GTG-1002組織的調查。這次行動是首個公開記錄的案例，其中人工智慧系統在極少人工幹預的情況下執行了大部分網路間諜活動。根據Anthropic的分析，Claude Code處理了入侵生命週期中約80%至90%的戰術任務，包括偵察、脆弱性識別、脆弱性利用開發、驗證資訊竊取、橫向移動、資料提取和情報分類。操作人員透過詳細的角色扮演提示操縱模型，使其相信每個操作都是合法防禦評估的一部分。一旦激活，Claude就能在不同會話中保持持續的上下文訊息，從而實現複雜的多日行動，而無需人工操作人員重新闡述目標或重建狀態。

GTG-1002的目標組織約有30家，其中包括大型科技公司和政府機構。其框架高度依賴 MCP 來整合外部工具、自動化工作流程，並將操作串連到多個子代理程式中。這種架構意義重大，因為它展示了一個人工智慧模型不僅能夠產生內容或程式碼還能作為一個自主運作引擎，大規模地執行協同入侵。

綜上所述，這些發現顯示了一種深刻的轉變：人為主導的網路行動和人工智慧主導的網路行動之間的界線開始變得模糊。人工智慧不再局限於撰寫網路釣魚郵件或生成程式碼片段；它正日益...在入侵生命週期中扮演操作員的角色，從而降低高階網路活動所需的成本和專業知識。

前景

到 2025 年底，人工智慧將從輔助工具轉變為網路行動的積極參與者。諸如 GTG-1002 和 LAMEHUG 實驗之類的活動表明，人工智慧系統在手中能力強、技術嫻熟的行動者現在可以自主執行相當一部分任務入侵生命週期，從偵察到利用和資料處理。同時，即時換臉、語音克隆等技術也得到了發展。自動化詐騙平台表明，透過外觀和語音進行身份驗證已不再可信。人工智慧的配套技術也暴露出其脆弱性。配置錯誤的 MCP、提示注入路徑、惡意軟體包和被竄改的工具描述符這表明，圍繞LLM的基礎設施本身可能成為妥協的途徑。網路攻擊越來越多地將人類決策與人工智慧驅動的執行相結合。人工智慧不再是網路安全中的一個獨立要素；它現在已經融入整個網路安全領域。

04

全球分析

全球威脅指數地圖

該地圖顯示了全球網路威脅風險指數，並突出顯示了世界各地的高風險地區。

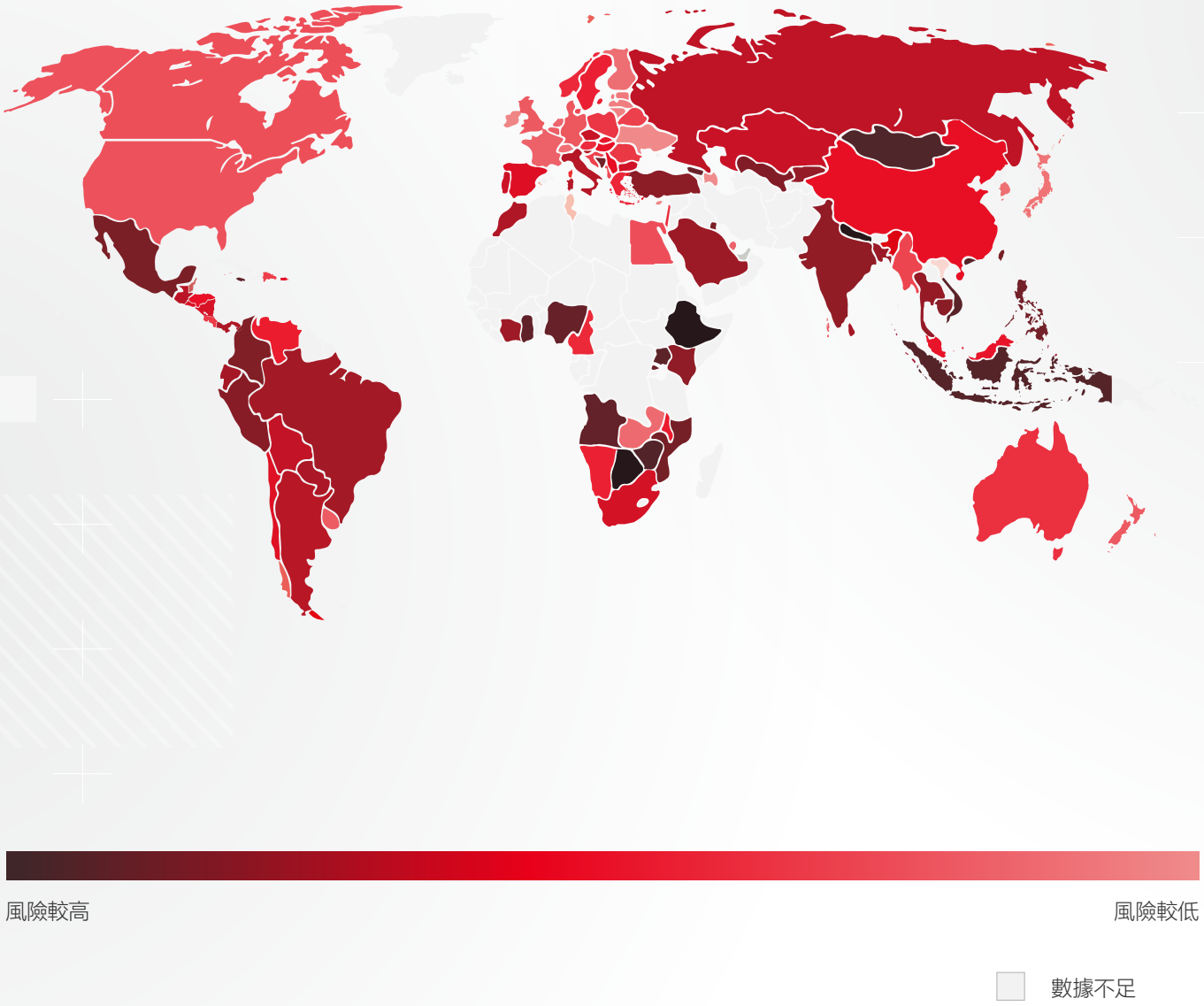


圖 1：全球威脅指數地圖。

每個組織遭受的攻擊

Check Point 的全球遙測數據顯示，每個組織每週遭受的網路攻擊數量持續穩定上升。網路攻擊在 2024 年急劇增加，並在 2025 年繼續攀升，達到這段時期有史以來的最高水準。到 2025 年，各組織平均每週將面臨 1968 次網路攻擊。這標誌著同比（YoY）增長了 18%，自 2023 年以來增長了近 70%，這進一步凸顯了整體威脅活動的持續升級。

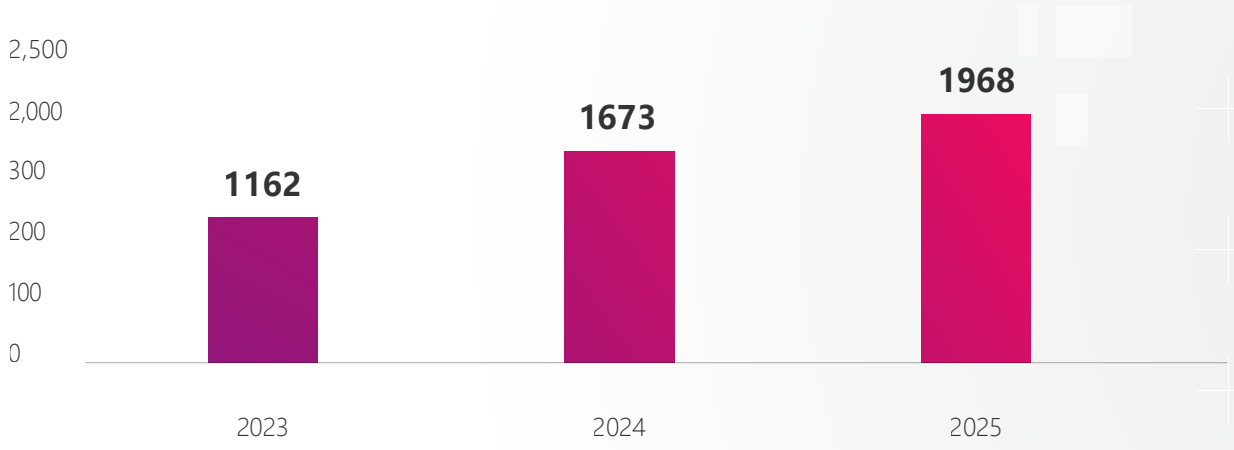


圖 2：2023-2025 年各組織平均每週遭受的網路攻擊次數

按地區劃分的攻擊活動

每個組織平均遭受的網路攻擊數量的增加在各個地區分佈並不均衡。2025年，北美年增23%，歐洲年增20%，而拉丁美洲（13%）和亞太地區（10%）的成長則較為溫和。非洲仍然是受影響最嚴重的地區，從數量上看，每個組織平均每周遭受超過 3000 次攻擊。不過，2025 年的年比變化幅度最小，僅 5%。

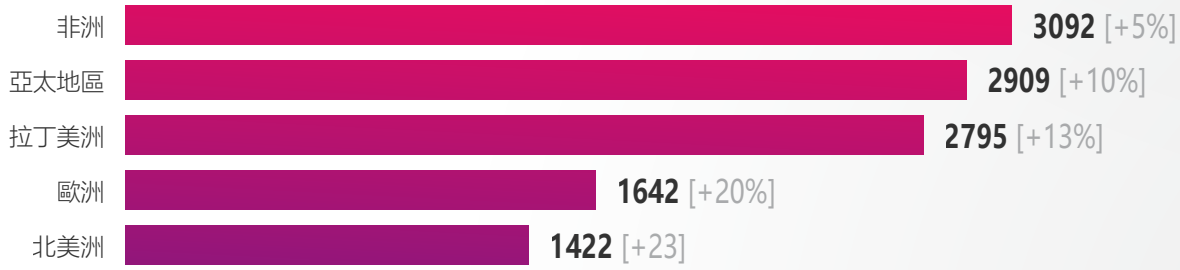


圖 3：2025 年各地區每個組織平均每週遭受的網路攻擊次數 [與 2024 年相比的變化百分比]

全球各行業和地區每週遭受的網路攻擊

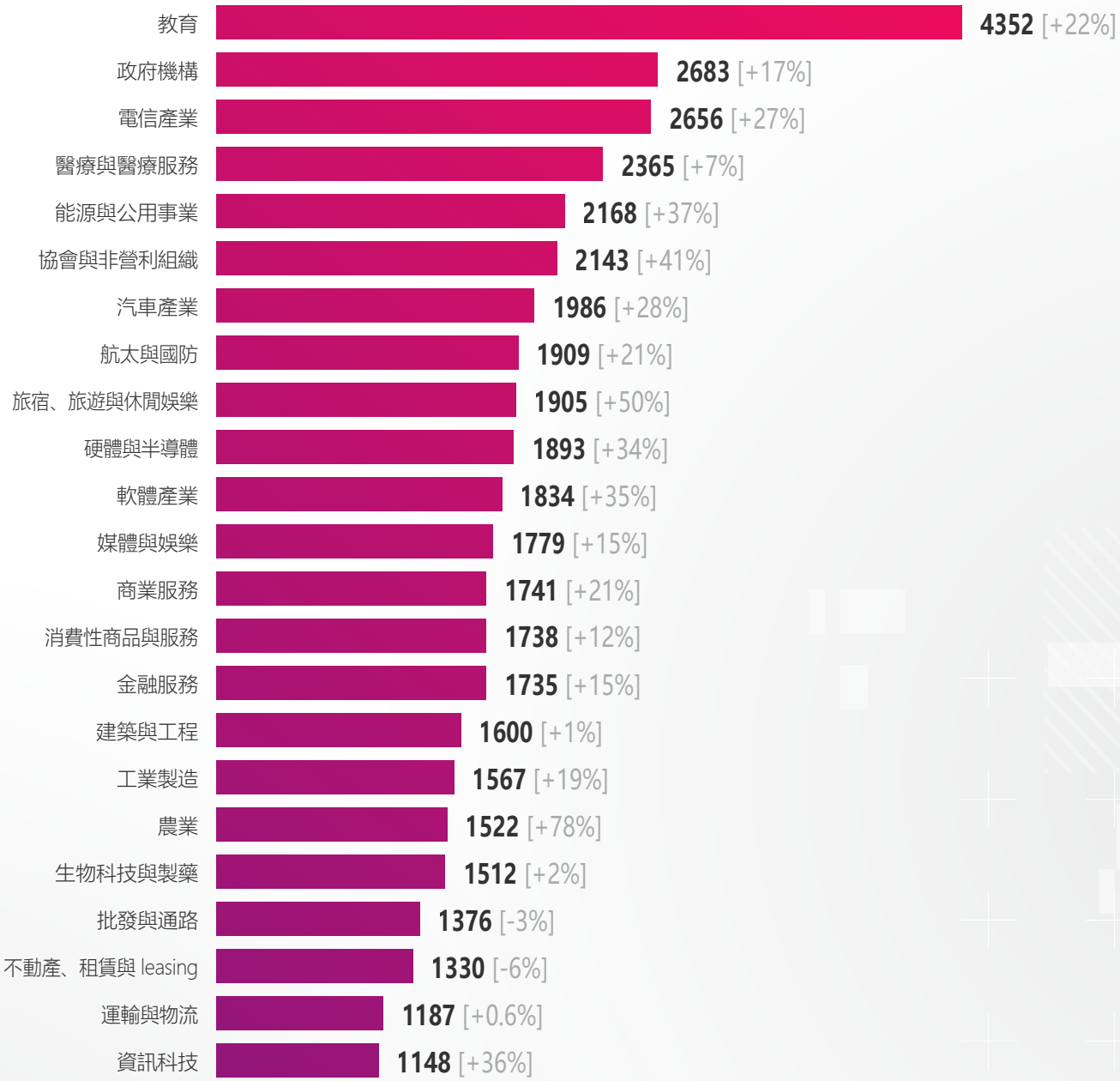


圖 4：2025 年全球各產業組織平均每週網路攻擊次數 [與 2024 年相比的變化百分比]

2025年，網路攻擊活動在所有地區和幾乎所有行業都有所增加。教育產業再次成為攻擊目標最多的產業，平均每個組織每週遭受 4,352 次攻擊，比前一年增加了 22%。政府、電信和醫療保健和醫療行業的每週 observable 攻擊量也達到了有記錄以來的最高水準。

隨著威脅行為者擴大攻擊範圍，關鍵基礎設施和工業部門遭受的攻擊數量急劇增加。2025 年，能源和公用事業、汽車以及航空航太和國防產業的年增幅在 21% 到 37% 之間。這些產業支撐著基本服務和國家基礎設施，因此也成為特別有吸引力的剝削目標。

2025年，針對旅館、旅遊和休閒產業的攻擊事件較去年同期成長50%，僅次於農業（增幅達78%）。這一轉變凸顯了人們對交易量大、涉及個人識別資訊 (PII) 資料的行業日益增長的興趣。

農業成長與農業供應的快速數位轉型相吻合包括分類和生產設施在內的產業鏈。對物聯網、邊緣運算和自主系統的日益依賴提高了效率和產量，但也擴大了跨裝置、網路和資料平台的攻擊面，為威脅行為者創造了新的機會。

> 農業對...的依賴程度日益提高物聯網、邊緣運算和自主系統提高了效率和產出，但也擴大了跨裝置和網路的攻擊面。以及數據平台，為威脅行為者創造了新的可利用機會。

北美地區各行業及地區每週遭受的攻擊

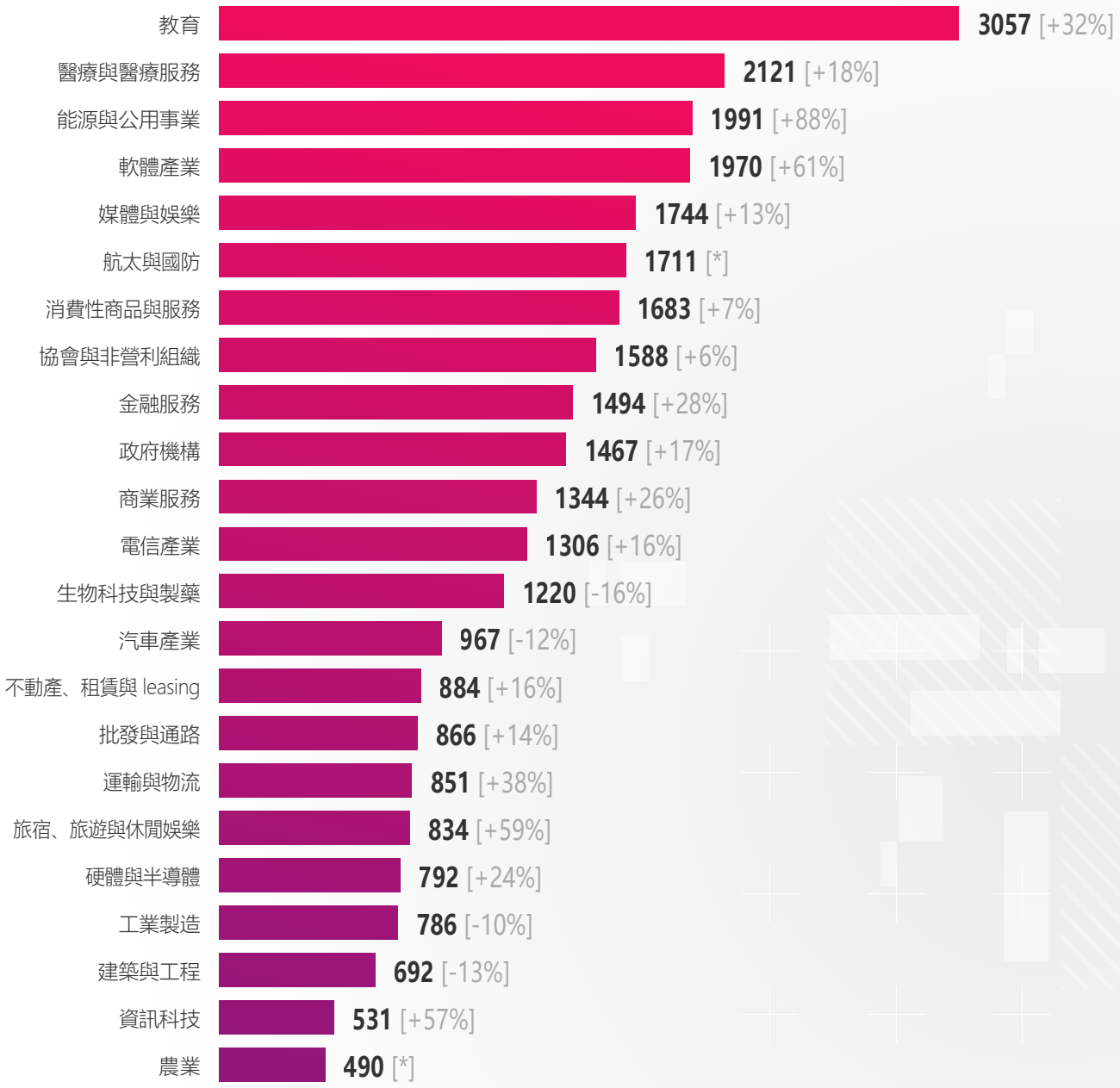


圖 5：北美各產業組織機構平均每週遭受的網路攻擊數量，2025 年 [與 2024 年相比的變化百分比]

* 2024年數據不足

拉丁美洲各行業及地區每週遭受的攻擊

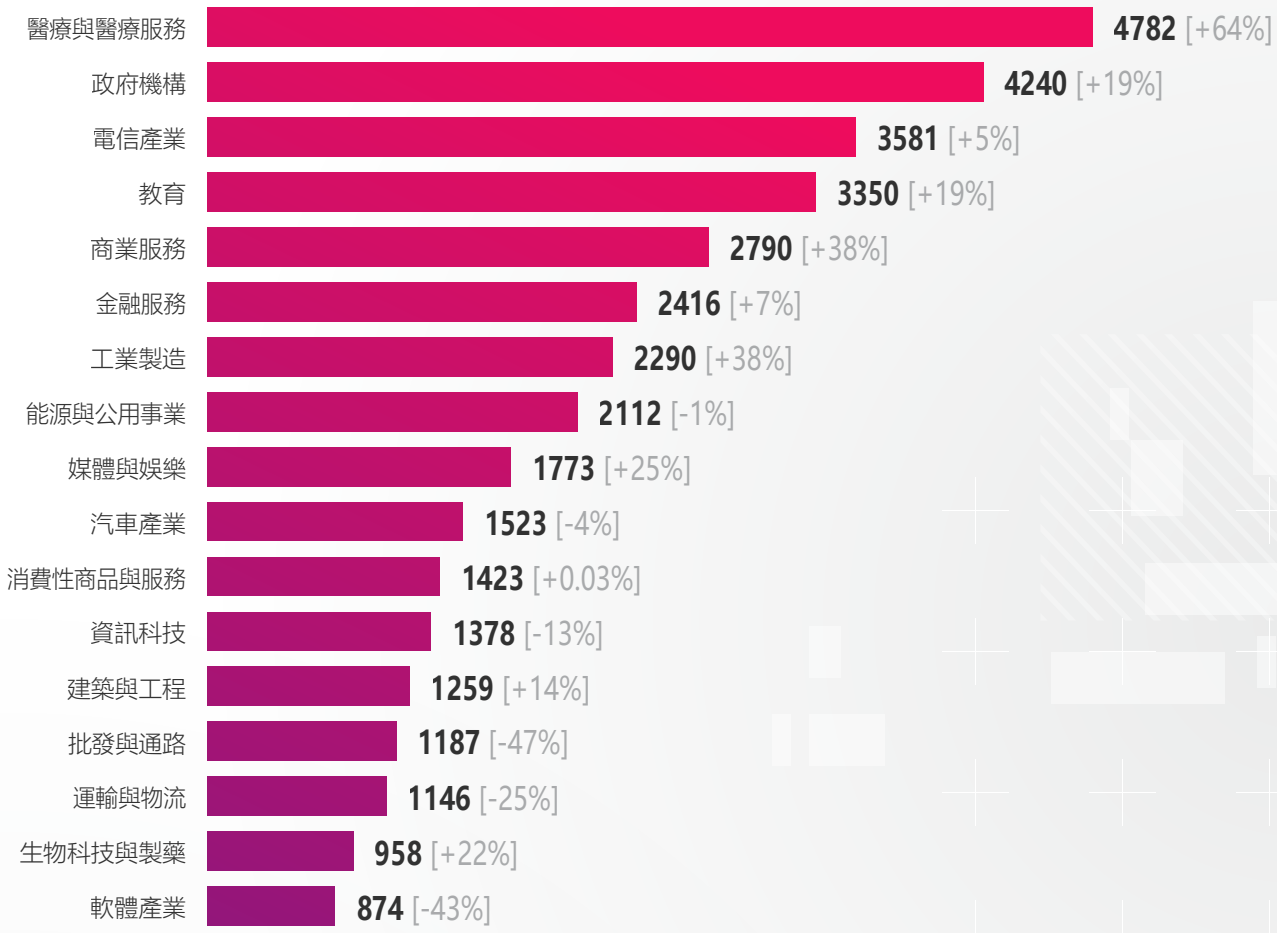


圖 6：拉丁美洲各產業組織平均每週網路攻擊次數，2025 年 [與 2024 年相比的變化百分比]

亞太地區各行業及地區每週攻擊事件

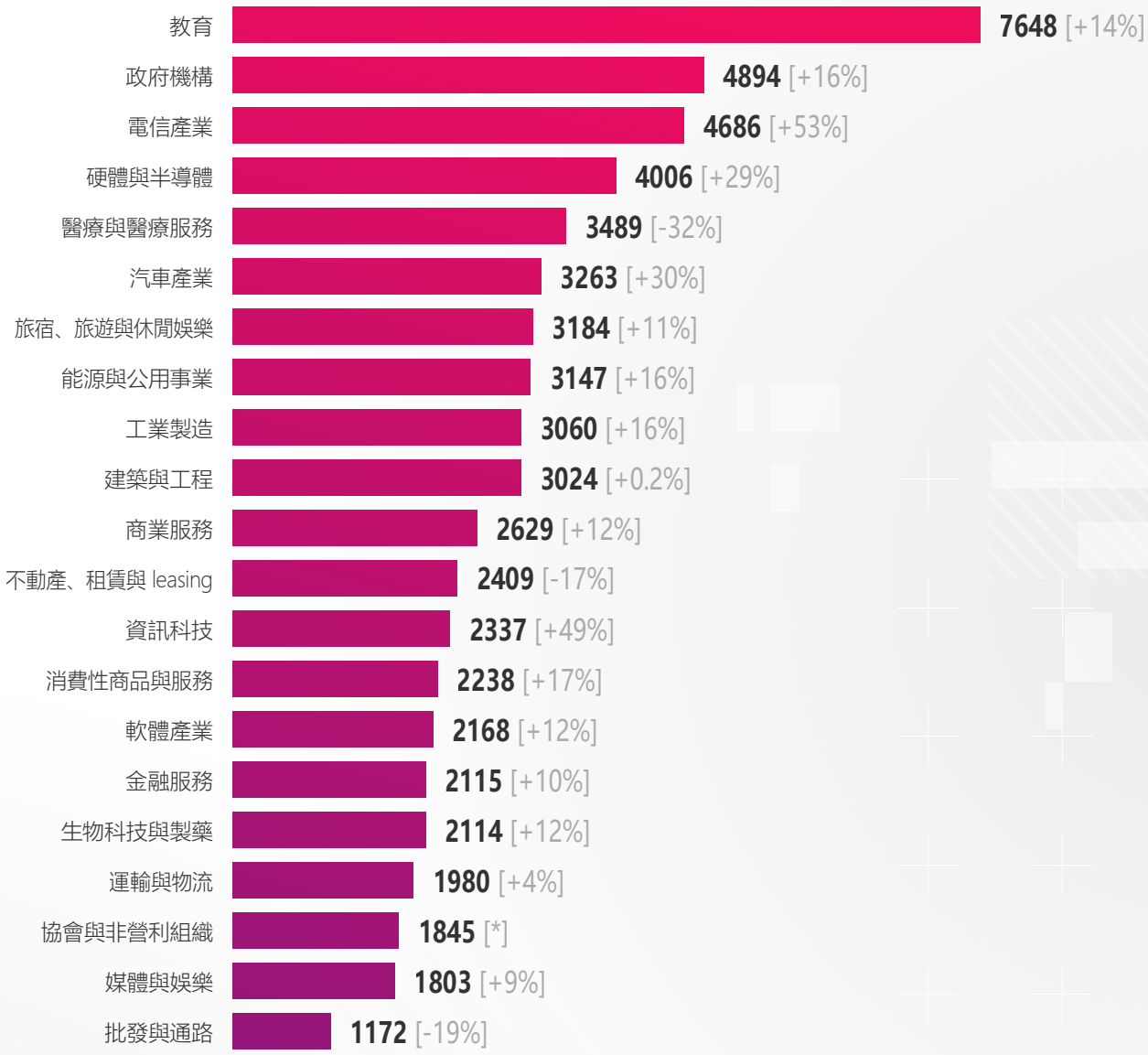


圖 7：亞太地區各產業組織機構平均每週遭受的網路攻擊數量（2025 年）[與 2024 年相比的變化百分比]

* 2024年數據不足

歐洲各行業和地區每週攻擊事件

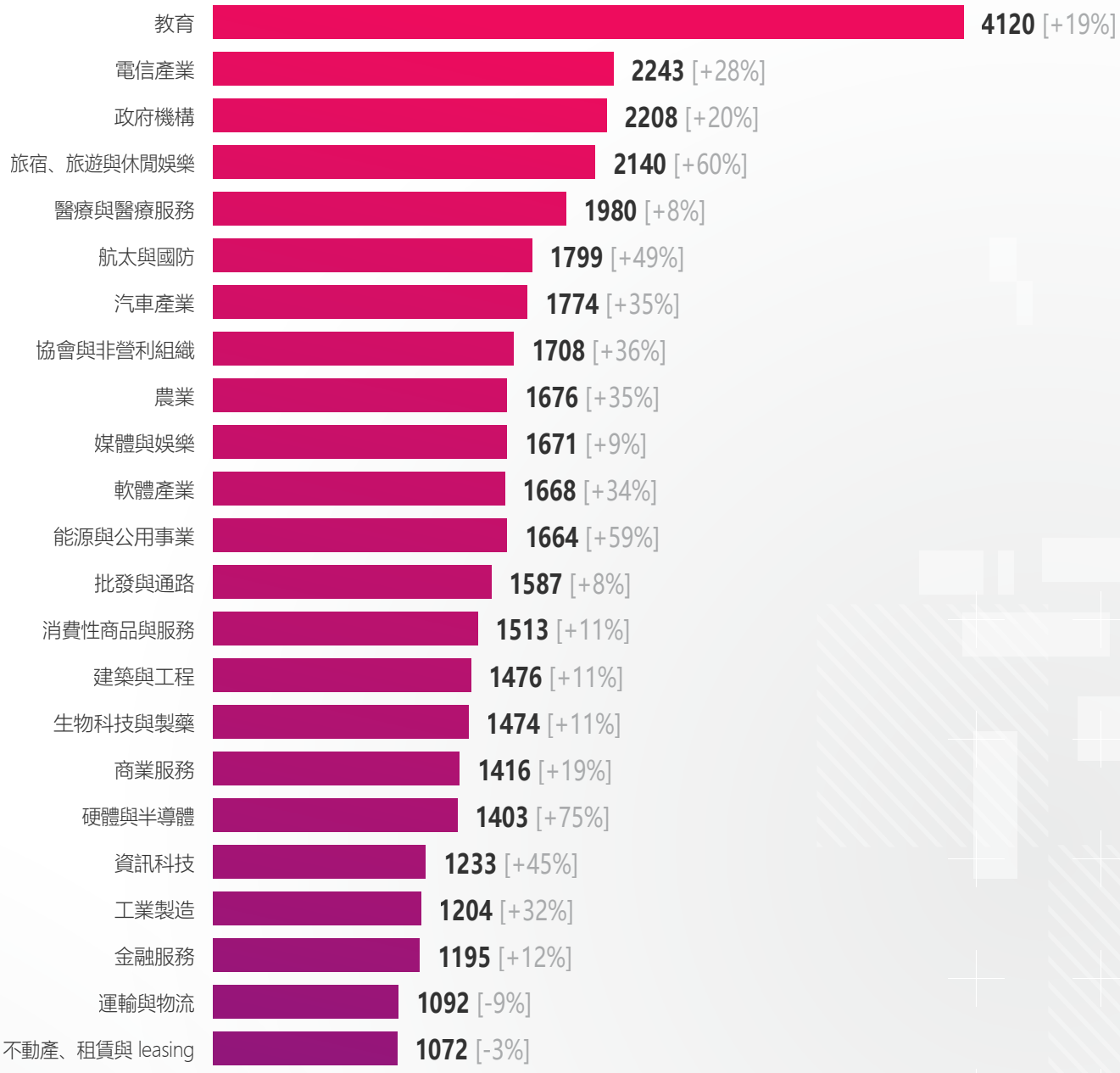


圖 8：2025 年歐洲各產業組織平均每週網路攻擊次數 [與 2024 年相比的變化百分比]

在北美，醫療保健產業仍然是主要目標，與 2024 年相比，每周平均網路攻擊數量增加了 18%。2025年上半年，數百項健康數據美國和拉丁美洲各地均有安全漏洞報告。這兩個地區的醫療保健機構全年都遭受了數百起勒索軟體攻擊。

與全球統計數據一樣，教育產業是亞太地區遭受攻擊最多的產業，該地區的攻擊數量最高。亞太地區平均每週遭受的攻擊數量與其他地區相比明顯偏多，亞太地區的攻擊量幾乎是其他地區的兩倍。在亞太地區，印度的平均攻擊量最高，每週攻擊次數達 7,684 次。

教育機構掌握著大量的個人資料和寶貴的研究成果。再加上學校和大學通常實行開放的網路政策，它們就成了有吸引力的目標，導致有針對性的攻擊和機會主義攻擊。

全球硬體和半導體產業每周遭受的網路攻擊數量年增了 34%。2025 年，亞太地區仍是網路攻擊的主要目標，平均每週遭受 4,006 次攻擊，是其他地區攻擊量的三倍多。

在 亞太地區（APAC），台灣與中國是遭受攻擊最頻繁的國家，分別記錄 7,393 次與 5,631 次攻擊事件。這種高度集中與亞太地區在全球 硬體與半導體供應鏈中的核心地位，以及其在 先進製造產業的重要性密切相關。

在歐洲，硬體和半導體產業的網路攻擊數量較去年同期激增75%，而北美地區的周均攻擊數量也增加了24%。這一趨勢與歐美為擴大國內半導體製造業而採取的戰略舉措相吻合，例如《歐洲晶片法案》等，這些舉措提高了歐洲製造商、供應商和研發中心作為間諜活動、 破壞活動和知識屬性盜竊目標的吸引力。隨著歐洲加速向本地化晶片生產轉型，針對其半導體生態系統的網路威脅活動也隨之增加。

亞太地區的電信業遭受的網路攻擊數量增加了53%，其他產業也出現了兩位數的成長在北美和歐洲，多起重大網路安全事件影響了多個地區。歐洲的布依格電信（Bouygues Telecom）遭遇 了嚴重的客戶資料外洩。亞洲的SK電信洩漏了數百萬使用者的敏感SIM卡資料。一家加拿大電信公司因一台未修補的思科裝置遭到與中國有關的駭客組織的入侵。美國的Cellcom公司遭受網路攻擊，導致長時間的服務中斷。這些事件與一場更廣泛的跨區域攻擊活動相吻合，該活動被評估為與中國有關聯的網路威脅組織「鹽颱風」（Salt Typhoon）有關，該組織的目標是多個大洲的電信基礎設施。所有這些都表明，攻擊者持續專注於獲取核心系統和敏感用戶資料的存取權限。

能源和公用事業的攻擊等級顯著上升，北美每週平均攻擊次數增加了88%，歐洲增加了59%。這一趨勢與我們在過去一年中observable到的地緣政治驅動型網路活動的整體趨勢相符。我們持續看到，地緣政治衝突與日益頻繁的進攻性網路行動之間存在關聯，尤其是在針對關鍵基礎設施的攻擊方面。

與國家結盟或隸屬於國家的威脅行為者似乎正在根據其地緣政治立場追求不同的目標，從情報收集和戰略獲取到破壞和發出信號。來自美國政府機構（包括國家情報總監辦公室 (ODNI)）的公開報告顯示，俄羅斯、中國、伊朗和北韓繼續將針對關鍵基礎設施和電信的網路行動列為優先事項。

攻擊向量

攻擊傳播途徑（電子郵件 vs. Web）

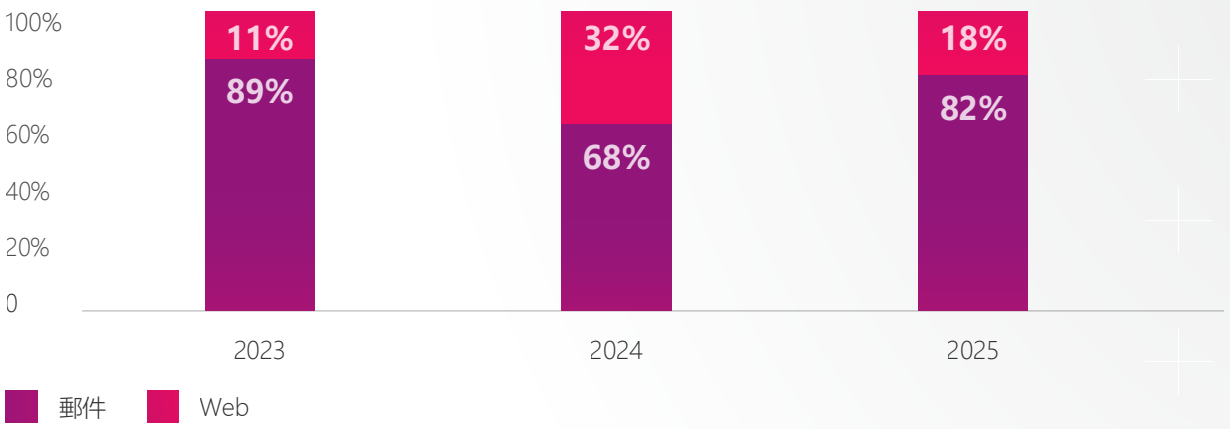


圖 9：攻擊傳播途徑（電子郵件 vs. Web），2023-2025 年

2025 年，攜帶惡意檔案的電子郵件攻擊佔所有 observable 活動的 82%，而基於 Web 的攻擊佔 18%。這凸顯了攻擊者傾向於使用電子郵件作為傳遞文件型攻擊的主要方式的持續趨勢。除了 2024 年暫時性出現的 21% 的下降外，自 2018 年以來，基於電子郵件的攻擊的主導地位一直在穩步上升。根據 Check Point Harmony Email & Office 數據，**一個組織收到的每 68 封帶附件的電子郵件中，大約有一封是惡意郵件。**

透過電子郵件發送的主要惡意文件類型

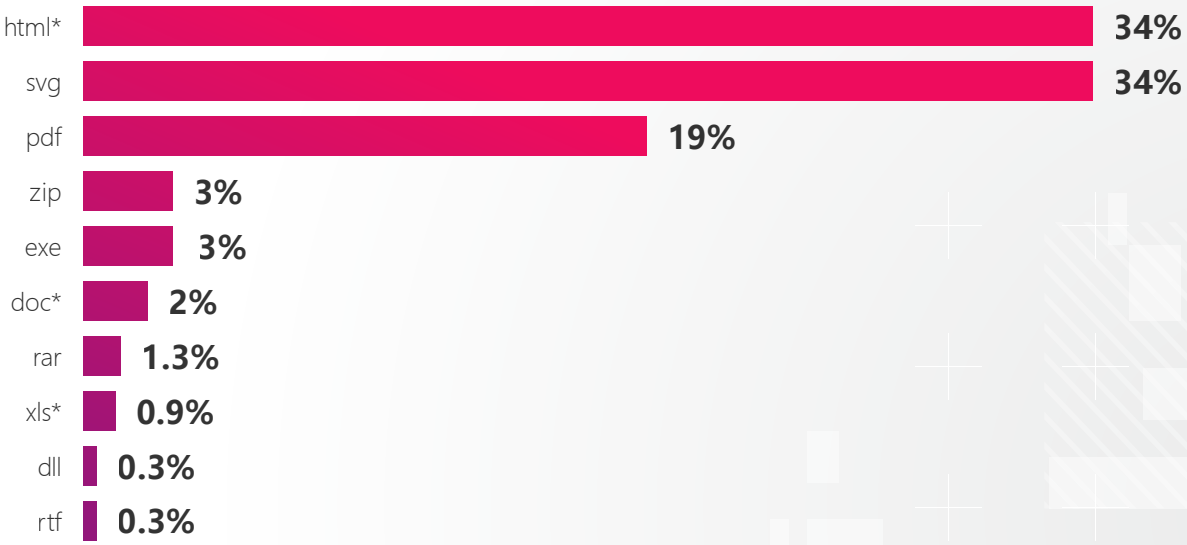


圖 10：惡意電子郵件：2025 年最常見的惡意檔案類型
html* 包括常見的 .html、.shtml、.htm 等文件。
doc* 包含常見的 Office Word 文件，例如 .doc、.docx、.docm 和 .dot。
xls* 包含常見的 Office Excel 文件，例如 .xls、.xlsx、.xlsm 等

2025 年全年，Check Point 追蹤了針對全球組織的全球網路釣魚活動。攻擊者繼續依賴惡意化的常用檔案類型，誘導收件人開啟這些檔案。此外，攻擊者也試圖創新，尋找新的方法來濫用偵測率較低、安全防禦較弱的文件類型。

多數攻擊者在初始階段避免使用可執行檔，而是依賴多階段釣魚攻擊

2024 年，惡意 HTML 附件佔電子郵件攻擊的 61%。然而，到了2025年，情況變得更加多樣化，SVG和HTML合計佔比超過34%，達到34%。PDF檔案仍佔主導地位，佔19%，而EXE檔案僅佔3%。這種分佈表明，大多數攻擊者在初始階段會避免直接附加可執行文件，而是依賴網路釣魚活動或使用HTML、SVG和PDF等格式的多階段感染鏈。

SVG檔案最初用於顯示向量圖形，但攻擊者濫用SVG檔案來傳播惡意程式其角色類似惡意HTML檔。兩者預設都在瀏覽器中打開，可用於建立逼真的網路釣魚頁面、在瀏覽器中執行腳本、進行HTML或SVG走私，或作為更複雜攻擊的初始階段。在某些情況下，攻擊者甚至將兩者結合起來，將HTML程式碼嵌入到SVG檔案中。

值得一提的是，有些攻擊利用 SVG走私技術針對金融機構，即SVG檔案會釋放嵌入的JavaScript檔案供受害者執行。這是多階段攻擊的初始階段，最終會部署各種遠端存取木馬（RAT）惡意軟體，例如Blue Banana、SambaSpy和SessionBot。

在另一波攻擊中，Shadow Vector威脅組織使用以法院為主題的SVG誘餌攻擊哥倫比亞使用者。其目的是將受害者重新導向到JS/VBS腳本程式或受密碼保護的ZIP有效載荷，然後利用DLL側載入和權限提昇技術部署AsyncRAT和RemcosRAT等RAT。

透過Web傳播的主要惡意檔案類型

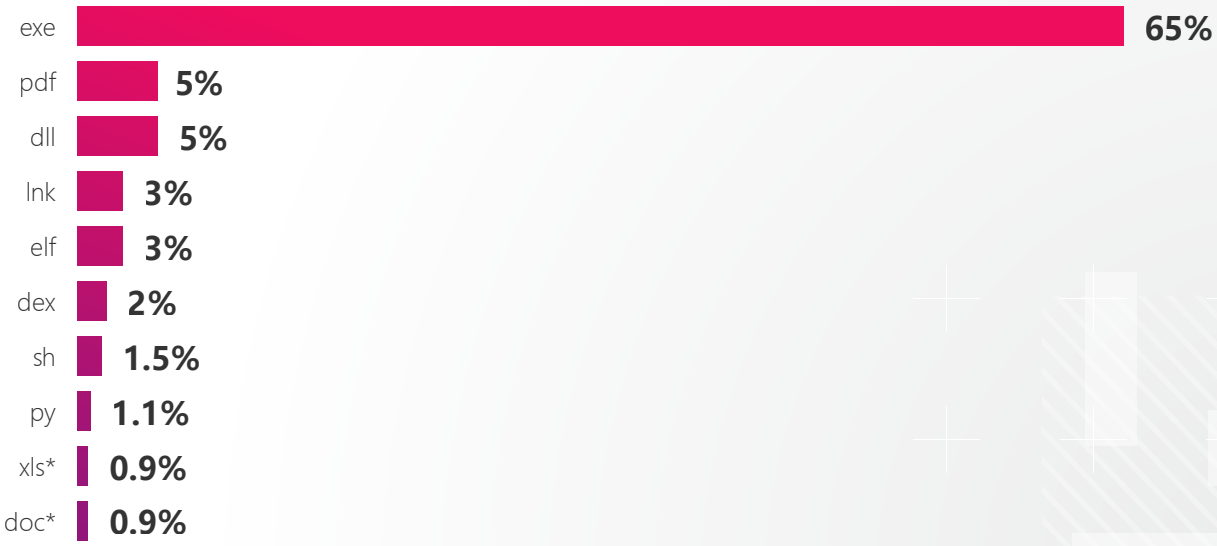


圖 11：Web：2025 年主要惡意文件類型

xls* 包括常見的 Office Excel 文件，例如 . .doc、.docx、.docm 和 .dot

在基於Web的感染途徑上，常見惡意檔案類型的分佈情況截然不同。許多基於Web的下載和惡意攻擊鏈，不是誘使用者點擊網路釣魚連結來啟動繞過電子郵件安全閘道器的複雜攻擊鏈，而是試圖立即投放可執行的有效載荷。我們 2025 年的遙測資料顯示，攻擊者普遍偏好可執行格式。EXE 檔案佔 Web 傳播惡意軟體的 65%，而排名第二的 PDF 檔案僅佔 65%。5%，顯示人們強烈傾向於直接執行，而不是基於文件的誘餌。這種趨勢得到了顯著的 Web 攻擊手段的強化，例如搜尋引擎優化中毒，它會在搜尋結果中推廣虛假的下載頁面；木馬化的「合法」安裝程式會在部署正版軟體的同時悄悄加載惡意軟體；以及軟體供應鏈遭到破壞，攻擊者會發佈在安裝過程中執行的木馬化軟體包。遊戲玩家也是透過種子檔案和檔案分享網站分發的木馬化遊戲相關工具、作弊程式和破解軟體，攻擊者會大量攻擊這些工具、作弊程式和破解軟體，這些工具和軟體可能會投放挖礦程式、竊取程式或載入程式。

資訊竊取者生態系統

在「終局行動」（Operation Endgame）及其後的「終局行動2.0」（Operation Endgame 2.0）中，執法部門的打擊行動摧毀了Qbot和Emotet等大型殭屍網絡，同時也清除了大量初始感染。適用於一般威脅行為者的方法。習慣直接購買存取權限的攻擊者全球各地的組織機構不得不調整策略，以應對這些殭屍網路帶來的威脅。資訊竊取程序隨即成為熱門的替代方法，而資訊竊取程序的日誌和驗證資訊在地下社區中共享和出售成為後續初始感染的燃料。

自那時起，資訊竊取程序的日誌已成為日益嚴重的網路安全風險，因為它們包含大量被盜的敏感信息，包括帳戶驗證資訊、支付卡詳細資訊和加密貨幣錢包，這些資訊均來自被入侵的系統。這些日誌由資訊竊取程式惡意軟體生成，並在地下市場和 Telegram 頻道中廣泛交易，如今已成為後續攻擊的主要推動因素，支撐著更廣泛的網路犯罪生態系統，包括詐欺、帳戶盜用和勒索軟體攻擊。Check Point 的暴露管理功能會主動監控和追蹤這些來源以下數據重點介紹了最主要的幾個資訊竊取程式家族。

Lumma 以 43% 的佔比佔據資訊竊取程式日誌的主導地位。這一數字較去年的 51% 略有下降，可能是由於執法部門加強了。老牌惡意軟體 Redline 是唯一一個緊隨其後的競爭者，佔據了 22% 的日誌份額，較去年的 8% 有了明顯增長。

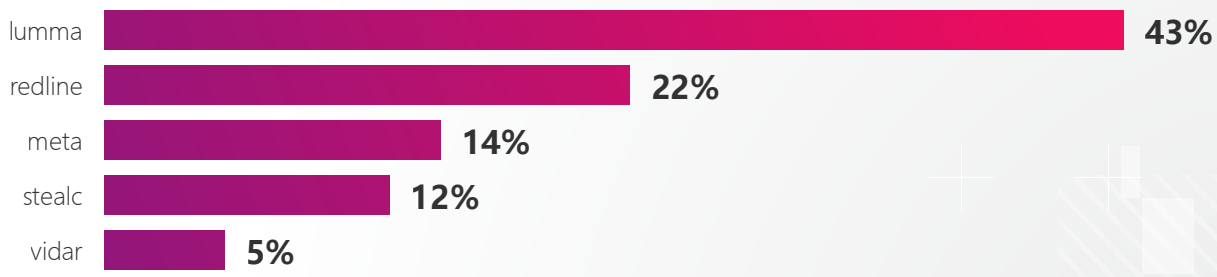


圖 12：2025 年全球頂級資訊竊取惡意軟體

> 根據我們分析的日誌數據，超過 76% 的受感染機器可能是非企業機器，而去年這一比例為 70%。

根據我們分析的日誌數據，超過 76% 的受感染機器可能是非企業機器，而去年這一比例為 70%。這一顯著增長進一步凸顯了「廣撒網」策略的日益普及，攻擊者首先透過攻破安全性較低的端點資安來試圖滲透到高度保護的企業環境中。在這種方法中，威脅行為者首先會獲得對 BYOD 或其他未受管理裝置的存取權限，這些裝置直接或間接地連接到企業網路。這些裝置通常可作為便捷的入口，因為它們可能缺乏企業級安全控制措施。與企業環境的連線可以採取多種形式，包括 VPN 存取、Microsoft 365 帳戶、協作平台或其他企業服務，這些服務的驗證資訊、會話令牌和 cookies 都儲存在瀏覽器中，使攻擊者能夠稍後入侵組織系統。

透過分析數據導出結果，我們發現，Roblox 和 Steam 等遊戲平台的驗證資訊連續第二年位居榜首。這項發現與遊戲平台仍然是資訊竊取程式傳播最突出、最有效的途徑之一這一事實密切相關。各種各樣的主題和誘餌被用來促進資訊竊取程式透過 Steam 線上商店中的遊戲傳播，PirateFi 和 Vidor 資訊竊取程式等案例就證明了這一點。此外，像 Stealka 這樣的竊取資訊者經常偽裝自己。遊戲相關內容，包括破解程序、作弊程序和修改程序，利用使用者願意下載非官方或修改版遊戲軟體的心理

儘管巴西是資訊竊取活動的主要目標國家之一，約佔所有已發現的資訊竊取 observable 的 7%，但如果按其在全球人口中所佔的比例來衡量，則僅佔該份額的三分之一左右。同時，十大受攻擊國家中有六個位於亞洲，儘管這些國家的人口總和僅佔世界人口的 28% 多一點，這凸顯了相對於人口規模而言，攻擊目標的嚴重程度不成比例。

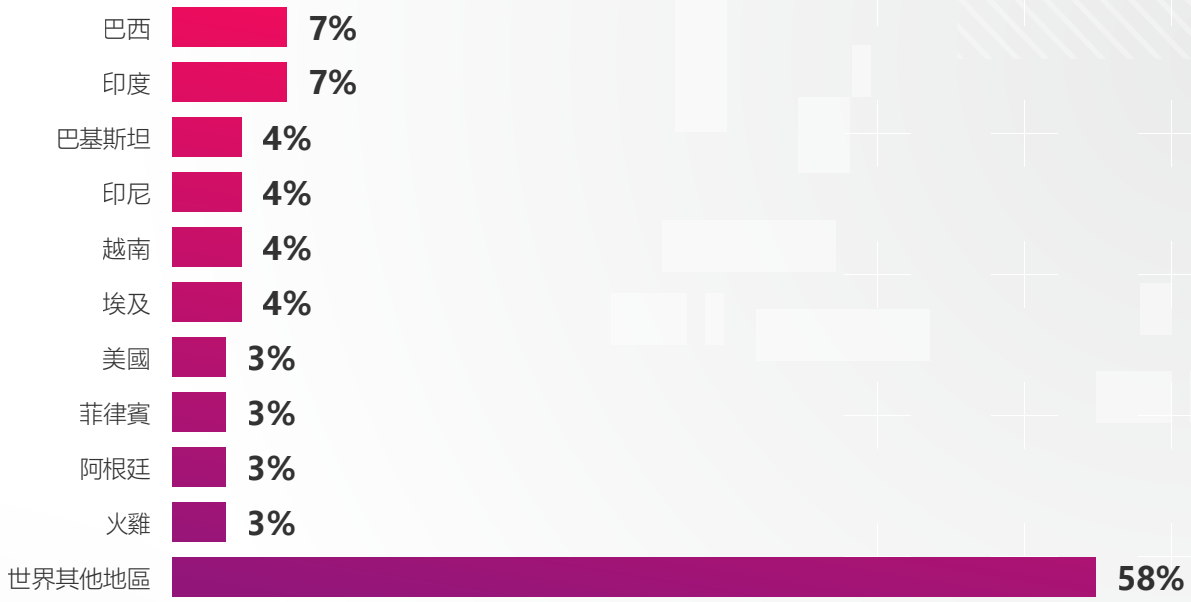


圖 13：資訊竊取者日誌出售情況 - 主要國家/地區，2025 年

05

高調
脆弱性

1. 工具外殼脆弱性

ToolShell 是一組 SharePoint 本機部署脆弱性，涉及 CVE-2025-49704 和 CVE-2025-49706 及其後續變種。編號為 CVE-2025-53770 和 CVE-2025-53771。將這些脆弱性串聯起來，即可在易受攻擊的本機 SharePoint 伺服器上實現未經驗證的遠端程式碼執行 (RCE)。Check Point 研究 observable 到包括 Ink Dragon 在內的各種威脅行為者發動了多波攻擊。在某些情況下，這種攻擊是間諜活動的第一步；而在其他情況下，它導致了勒索軟體的部署。例如，威脅行為者使用 ToolShell 在目標網路中部署 Warlock 和 LockBit Black。

值得注意的是，在補丁公開發布之前，ToolShell 就已經被實際利用了。根據 Check Point 的數據，已知的首次攻擊發生在 7 月 7 日，更廣泛的攻擊嘗試始於 7 月 18 日。與此脆弱性相關的攻擊嘗試影響了 12% 的組織。

2. Langflow遠端程式碼執行漏洞（CVE-2025-3248）

2025 年 4 月，Langflow（一個用於建置和部署人工智慧工作流程的熱門開源視覺化框架）中揭露了一個嚴重的遠端程式碼執行脆弱性（CVE-2025-3248）。此脆弱性影響 1.3.0 之前的所有版本。該漏洞未能要求進行身份驗證，並且對使用者提供的程式碼進行充分的清理，從而允許攻擊者發送特製的 HTTP 請求並在伺服器上執行任意 Python 程式碼。伺服器上的脆弱性被歸類為 嚴重程度高，CVSS 3.1 基本評分為9.8（嚴重）。已公開概念驗證 (PoC) 漏洞利用程序，並已證實現實世界中存在漏洞。被入侵的 Langflow 實例被用於部署 Flodrix 殭屍網絡，該網路能夠創建後門、DDoS 攻擊能力以及潛在的資料外洩。

3. Oracle E-Business Suite (CVE-2025-61884)

CVE-2025-61884 是 Oracle E-Business Suite (EBS) 中一個嚴重的伺服器端請求偽造脆弱性，會影響設定器執行階段。UI 元件在 12.2.3 至 12.2.3 版本中12.2.14.該漏洞允許未經身份驗證的遠端攻擊者發送精心建構的請求，這些請求會被應用程式執行，從而攻擊目標系統。內部服務可能會洩漏敏感的業務資料和身分驗證元資料。該脆弱性被與 CL0P 勒索行動相關的威脅行為者利用，他們透過該脆弱性存取了內部 EBS 資源，並竊取了超過 100 萬個關鍵業務資料。100個組織。在 Cl0p 漏洞利用幾個月後，Scattered LAPSUS$ Hunters 組織洩漏了一個可用的 PoC。這次洩漏事件導致大規模資料被盜，包括配置資訊和財務記錄，這些資料後來被用於敲詐勒索活動。CISA 確認了該脆弱性已被積極利用，並將 CVE-2025-61884 添加到已知已利用脆弱性目錄中。

4. React2Shell (CVE-2025-55182)

CVE-2025-55182，又稱為 React2Shell，是React 伺服器 Components (RSC) 中的一個嚴重遠端程式碼執行脆弱性。這是由於 RSC Flight 協定中不安全的反序列化造成的，它允許未經身份驗證的

攻擊者發送精心建構的有效載荷來觸發伺服器上的程式碼執行。此缺陷影響多個 RSC 軟體包。React 版本 19.0、19.1.0、19.1.1 和 19.2.0，以及使用它們的框架，例如 Next.js。根據 Check Point 的數據，在 PoC 公開揭露和發布後，多個威脅行為者在 24 小時內開始利用脆弱性。與中國有關的威脅組織，包括地球拉彌亞和頭獎熊貓，是發現有人利用該漏洞進行惡意活動。利用攻擊企圖傳播惡意軟體、建立後門並掃描存在脆弱性的部署。僅在剝削的第一天，我們就看到了12 月共發生 479 次攻擊嘗試，總體而言，這些嘗試影響了 22% 的組織。

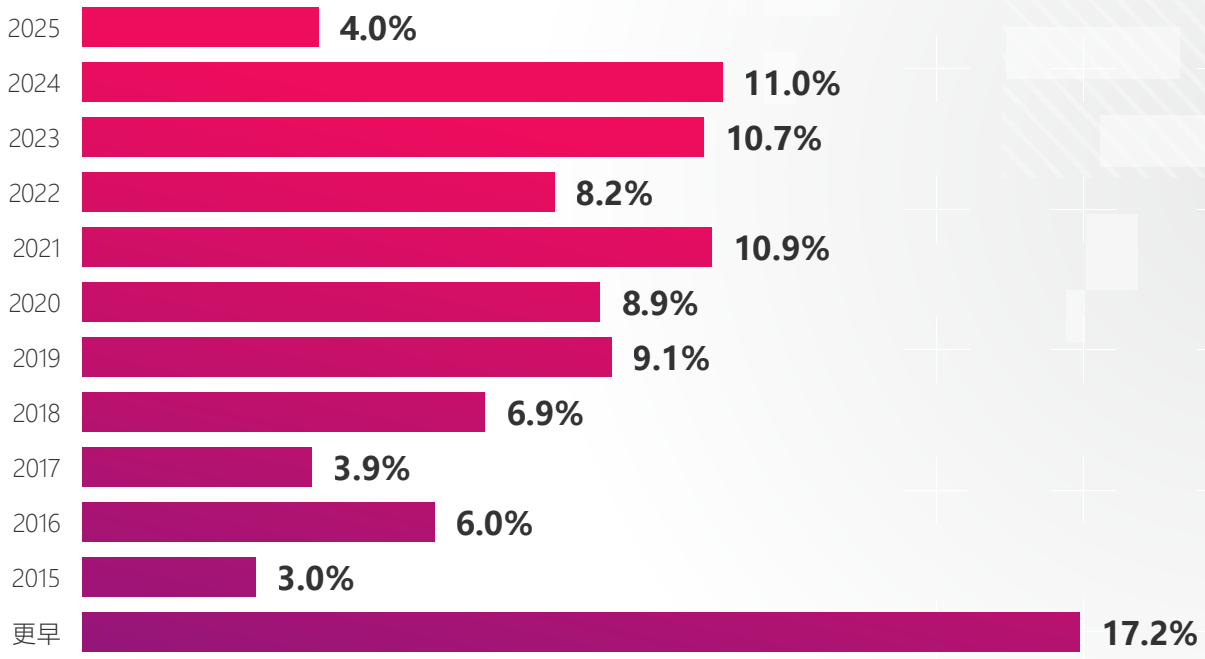


圖 1：按揭露百分比，205 年的脆弱性利用攻擊顯示255 年

年揭露的脆弱性佔所有利用嘗試的 4%。正如 ToolShell 和 React2Shell 所observable到的，漏洞利用所需時間逐年縮短。同時，攻擊者仍然嚴重依賴舊漏洞超過 46% 的利用嘗試利用了 2020 年之前發布的 CVE 脆弱性。這反映出修補程式方面存在持續的系統性缺陷，許多系統脆弱性儘管有可用的修復程序，但多年來仍未解決。

06

2026 產業預測：網路安全的未來

以下預測重點闡述了2026年塑造網路安全的最重要轉變，涵蓋攻擊者行為、技術演進以及組織在管理和證明其韌性方面不斷變化的期望。

1. 智能體人工智慧從輔助功能過渡到營運自主

2026年，智能體人工智慧將走向主流。能夠進行推理、規劃和行動且只需極少人工幹預的自主系統，將使我們從撰寫內容的助手轉變為執行策略的智能體。這些系統將即時分配預算、顯示器生產線並重新安排物流路線。

製造環境將越來越能夠透過區塊鏈驗證的供應鏈網路進行故障自診斷並觸發自動採購。同時，行銷、財務和安全團隊將依賴不斷吸收資訊的代理人。上下文訊號並以機器速度運轉。

缺乏問責制的自主權是一種負擔。根據世界經濟論壇發布的《2025年全球網路安全展望》，缺乏治理的人工智慧自主性是企業韌性面臨的三大系統性風險之一。

隨著這些智能體獲得真正的操作權限，一些尚未解決的治理問題也跟著浮現：誰來驗證自主決策、審核決策邏輯，或在預期行為發生時介入？而現實世界的結果卻不盡相同？要彌補這一差距，需要人工智慧治理委員會、可執行的政策保障措施以及記錄和解釋每一個自主行為的不可篡改的審計機制。

> 解決人工智慧自主治理差距需要人工智慧治理委員會、可執行的政策保障措施和不可更改的審計機制，記錄並解釋每項自主行動。

2. 提示注入與資料投毒 - 人工智慧模型成為新的零日漏洞

隨著生成式人工智慧嵌入到面向客戶的服務、內部工作流程和安全營運中，人工智慧模型本身也變得日益複雜。正在成為高價值的攻擊面。2026年，敵對勢力將越來越多地利用快速注入技術，將隱藏指令嵌入文字、程式碼或文件中以操縱模型行為，以及資料投毒技術，即用受污染的輸入來扭曲或破壞訓練資料。

由於許多 LLM 透過第三方應用程式開發介面運行，因此僅僅一個被污染的資料集就可以傳播到數千個應用程式中。在這種情況下，傳統的修補方法提供的保護有限；維護模型完整性成為一個持續的過程。

人工智慧模型是當今尚未打補丁的系統。每個外部資料來源都代表著潛在的攻擊途徑。**到 2026 年，人工智慧安全領域的領導者將透過實施治理、驗證和持續監督來確保人工智慧系統在大規模應用中保持可信賴性，從而脫穎而出。**

3. 在高度互聯的生態系中，供應鏈和軟體即服務面臨的風險日益加劇。

如今，企業在供應商、應用程式開發介面 和整合組成的 Web 中運營，這就造成了攻擊路徑，僅僅一個薄弱的供應商就可能導致大範圍的攻擊。隨著生態系統變得越來越自動化和相互依賴，事件會透過共享程式碼、代幣等方式更快傳播。以及雲端服務，因為它們更容易被追蹤。ENISA發布的《2025年供應鏈網路安全報告》警告稱，62%的大型組織面臨風險。過去一年中至少經歷過一次第三方入侵。

> 組織必須將可見性擴展到第三方和第四方軟體即服務供應鏈站點和 ADOPT持續顯示器和零信任存取控制以管理攻擊面這種情況正日益超出他們的範圍。

同時，在自動化壓力下，全球供應鏈正在改變。智能體人工智慧將實現自主風險管理：能夠繪製依賴關係、顯示器第三方合規並預測中斷的自學習系統。然而，過度連結也加劇了風險：被入侵的程式碼庫、應用程式開發介面令牌和雲端驗證資訊會在生態系統中迅速傳播，速度之快甚至超過了事件的追蹤速度。

組織必須將可見性擴展到第三方和第四方軟體即服務供應鏈站點，並採用持續顯示器和零信任存取來管理不斷超出其邊界的攻擊面。

4. 信任是新的邊界：深度偽造和對話式欺詐

生成式人工智慧模糊了真實內容和虛構內容之間的界線。語音克隆、即時合成視訊和人工智慧驅動的聊天互動現在使攻擊者能夠繞過傳統的身份和存取控制，包括多重身份驗證。ENISA 的《2025 年威脅情勢》將「合成身分和人工智慧生成的社會工程」列為五大風險因素之一。

技術真實性不再能保證人的真實性，甚至無法保證互動確實源自人類。隨著非人類身分（NHI）與人工智慧代理和自動化系統一同激增，每個人機互動介面都可能成為攻擊點。商業電子郵件詐騙將演變為基於信任的欺詐，透過深度偽造、自適應語言和情緒操縱等手段實施。今年，欺騙聽起來將像是信任。企業必須在每一次互動中持續驗證身分、上下文和意圖。

5. Quantum風險從長期關注轉向近期行動

Quantum運算或許還需要數年才能破解當今的加密技術，但這種威脅已經並將繼續改變企業的行為。各國政府、雲端服務供應商和大型企業正競相確保加密技術的敏捷性，在攻擊者將其武器化之前，從具有脆弱性的 Rivest-Shamir-Adleman (RSA) 和橢圓曲線密碼學 (ECC) 演算法遷移到後Quantum密碼學 (PQC) 標準。

危險在於「先竊取後解密」(HNDL) 策略。攻擊者如今已竊取加密數據，並篤定Quantum解密技術明天就能破解。到 2026 年，相關準備工作將從理論階段邁向實務階段。董事會將資助加密物料清單 (CBOM)，以記錄其環境中的每個演算法、憑證和金鑰。各組織將試點採用美國國家標準與技術研究院 (NIST) 批准的後Quantum演算法，並向供應商施壓，要求其給出明確的遷移時間表。

Quantum風險並非關乎未來的機器。這是關於今天的數據。每個組織都必須假設其加密資產已被竊取，並為這樣一個世界做好準備：預防取決於加密技術的靈活性。

6. 人工智慧成為戰略決策引擎

人工智慧正在穩步改變網路安全的基礎。曾經主要作為提高作戰效率的工具，如今正在影響攻擊者和防禦者如何規劃、調整和執行他們的策略。該行業正在進入一個新階段，人工智慧不再是一種輔助能力，而是檢測、分析和決策工作流程中的嵌入式要素。

這種演變預計將會加深。攻擊者已經開始利用人工智慧來發動速度更快、範圍更廣、更具針對性的攻擊活動，這將日益促使各組織開發能夠跟上這種速度的防禦能力，包括持續學習、即時情境感知和更自主的營運支援。這反映了安全團隊在行動優先順序、風險理解、回應協調以及最終提高效率方面所發生的轉變。

人工智慧正成為安全營運中營運層不可或缺的一部分，它增強了人類的專業知識，簡化了手動工作流程，並縮短了平均修復時間 (MTTR)。

人工智慧的加速應用使其成為網路安全營運的核心支柱，而非現有工具的擴展，它正在塑造更一致、自動化且由精確控制指導的分析工作流程和決策過程。

> 人工智慧的加速應用正使其成為網路安全營運支柱的一部分。與其說是現有工具的擴展，不如說是塑造分析工作流程和決策過程將更加一致、自動化，並由...指導精確控制。

7. 人工智慧現實檢驗

經過兩年近乎瘋狂的人工智慧應用之後，我們將迎來第一次重大調整。許多急於整合生成式人工智慧工具的組織將會發現缺乏監管的系統、暴露的應用程式開發介面以及合規盲點。員工自主開發的、利用企業資料的「影子人工智慧」將會激增，造成隱藏的資料外洩和安全標準不一致。

這一階段的幻滅是必要的：它將推動組織從實驗階段轉向成熟階段問責制。高階主管將開始要求以結果而非炒作來衡量人工智慧的價值。人工智慧保障框架將在各個領域湧現，需要進行正式審計以確保公平性、穩健性和安全性。領導團隊必須制定清晰的人工智慧使用政策，並使其與法律、倫理和風險框架保持一致。負責任的部署將取決於可解釋性和持續驗證，而不是不受控制的自動化。合規範圍將從隱私擴展到演算法問責。

人工智慧的第一次顛覆是速度；第二次顛覆將是治理。 2026年，那些將人工智慧視為需要安全保障、審計和改進的能力，而不是捷徑的人將獲得回報。

人工智慧的第一次顛覆是速度第二次顛覆將是治理。 2026年，那些將人工智慧視為需要安全保障、審計和改進的能力，而不是捷徑的人將獲得回報。

8. 監理與問責範圍擴大 - 網路韌性成為營運許可

全球監管機構正在努力彌合創新與問責之間的差距。到2026年，監管將不再是被動應對。歐盟的NIS2指令、人工智慧法案以及美國證券交易委員會的事件揭露規則等框架將趨同於一個共同原則：網路安全必須能夠即時衡量和證明。各國政府將要求持續提供韌性證明。各組織機構則需證明其預防性控制措施、事件回應計畫和資料保護措施持續有效執行。

監管加速發展的背後有一個強而有力的原因：社會對監管日益增長的依賴。依靠數位服務來維持日常生活和經濟，避免重大中斷。業務韌性已成為合規要求不斷提高的主要驅動因素。

這一轉變將標誌著「年度合規」時代的終結。企業將依靠自動化合規顯示器、機器可讀的政策、即時認證和基於人工智慧的風險分析。董事會和執行長將承擔監督的個人責任。

網路韌性不再是紙上談兵，而是實實在在的行動。能夠證明持續的保護將決定市場准入和信任。

07

2026 年首席資訊安全官建議

作者：喬納森·菲施貝
現場首席資訊安全官

到2026年，安全領導者面臨的主要挑戰是如何在攻擊者能力、技術和規模不斷提升的情況下，維護組織的安全。攻擊速度比以往任何時候都快，攻擊面也越來越廣，從日常工作流程和端點到由日益複雜的系統Web組成的混合環境。同時，首席資訊安全長 (CISO) 需要清晰、持續地展現營運效率，並支持可衡量的業務成果。以下建議體現了首席資訊安全長 (CISO) 必須關注的優先事項，包括降低風險敞口、在動態環境中管控風險以及展現應對日益激進且難以預測的威脅形勢的韌性。

1. 建立以預防為主導的分層安全計劃

安全計畫的設計目標必須是儘早阻止攻擊，同時要認識到任何單一的預防控制措施都不足以應對所有威脅。到 2026 年，有效的計畫應優先考慮在攻擊鏈的多個環節進行預防，從而降低風險敞口和攻擊成功率同時確保次要保障措施能夠在預防措施被繞過時控制其影響。這種方法超越了單一防禦模式，轉向了能夠反映攻擊者行為方式的分層自適應保護。

CISO 應透過持續驗證和透明機制來強化以預防為主導的架構，以確認保護措施在實際條件下有效運作。這包括整合外部訊號，例如負責任的脆弱性揭露、與observable到的威脅活動相關的有針對性的安全意識培訓，以及在攻擊者利用漏洞之前發現漏洞的結構化程序。這些要素並非預防措施的替代品而是獨立的檢查手段，可以增強對防禦有效性的信心並加速改進。

重要性: 對手大規模行動，快速迭代，並利用他們遇到的第一個可行的弱點。依賴單一控製或靜態保障模式的組織更容易遭遇連鎖故障，而以預防為主導的分層計畫可以降低攻擊成功的可能性和影響。

2. 將資料保護作為核心安全成果進行治理

資料外洩如今已成為現代網路安全事件中最具後果的後果，其影響甚至超過了服務中斷本身造成的業務損失。因此，安全計畫必須將資料保護作為首要目標，並根據敏感資料在不同環境中的存取、移動和聚合方式來製定，而不是根據靜態分類來製定。或週長假設。在這種情況下，勒索軟體事件應預設為資料外洩事件，而可用性損失只是影響的一個面向。

> 資料外洩現在代表著現代網路事件最嚴重的後果，甚至超過了服務中斷本身對業務的影響。

首席資訊安全長應優先考慮限制資料爆炸半徑和復原風險的架構控制措施，包括資料存取路徑的分段、嚴格的最小權限執行以及彈性措施，例如不可變備份和定期演練的事件回應手冊。這些控制措施必須設計成假定存在部分洩露，並著重於防止大規模資料外洩、加快復原速度以及在洩漏期間維護信任。事件發生之後。這種治理模式也為新興風險領域奠定了基礎，包括長期保護...敏感資料面臨未來密碼技術發展的威脅。

重要性：勒索軟體攻擊活動越來越多地涉及已確認的資料洩露，因此資料外洩（而不是停機）已成為監管、財務和聲譽影響的主要來源。失敗的組織將資料保護作為核心安全目標進行治理，在發生事件時仍然容易遭受累積損失，並且由於資料會持續存在到超出當前威脅範圍之外，還會面臨長期脆弱性風險。

3. 實現雲端、軟體即服務和人工智慧安全運營

雲端、軟體即服務 和 人工智慧 環境帶來的風險主要來自速度、規模和變化，而不僅僅是配置錯誤。持續部署、第三方整合和自動化服務互動會帶來風險敞口，而這些風險敞口無法透過以身分為中心的方法進行有效管控。或僅依靠合規性控制。這些平台必須作為鮮活的、運作中的系統進行安全保障，風險源自於服務在即時互動和執行過程中所產生的方式。

首席資訊安全長 (CISO) 應建立治理機制，持續評估平台狀態和運作行為，包括配置漂移、應用程式開發介面使用情況、服務間信任以及應用程式層級互動。人工智慧系統需要與其他生產平台一樣的營運規範，包括明確的所有權、受顯示器的使用範圍，以及對模型的存取、整合和操作方式的問責制。重點不在於衡量韌性或強制執行身分策略，而是持續控制動態平台在發展演變過程中的行為。

重要性：攻擊者越來越多地利用應用程式開發介面、自動化和運行時互動來繞過身分檢查和邊界防禦。 如果沒有持續的平台治理，組織會在變更週期之間失去可見度和控制力，造成可被利用的漏洞，這些漏洞會隨著環境變得越來越複雜而擴大。

4. 將第三方風險視為結構性風險敞口

供應商、軟體即服務供應商和合作夥伴透過存取、整合和共享服務直接嵌入到企業環境中。

首席資訊安全長（CISO）應將第三方風險視為結構性風險敞口進行管理，而不是將其視為週期性風險。評估練習。這需要持續顯示器供應商存取權限和進行權限劃分。合作夥伴連接，以及在外部身分中強制執行最小權限和零信任原則。

安全義務必須能夠透過服務等級協定 (SLA) 進行衡量和強制執行，但僅靠文件是不夠的。真正的風險源自於供應商如何存取系統、他們擁有哪些權限以及安全漏洞如何在共享的信任關係中傳播。

重要性：供應鏈和軟體即服務相關事件越來越多地源自於受信任的供應商存取權限和繼承的信任，導致影響範圍超出組織的直接控制範圍。

5. 在人類和非人類身分中錨定零信任架構

零信任必須被視為抵禦身分驅動型攻擊的核心防禦措施。由於網路釣魚、驗證資訊竊取和令牌濫用使攻擊者能夠冒充受信任使用者和非人類身分進行攻擊，這些方法極大地威脅著網路安全。擴大攻擊面，使隱式信任模型和靜態存取假設過時。有效的零信任需要持續驗證身分和上下文、預設最小權限原則、架構控制。限制跨雲端、軟體即服務、網路和開發環境的橫向移動。目標不僅是防止身分被濫用，還要在身分不可避免地被洩露時控制其影響。

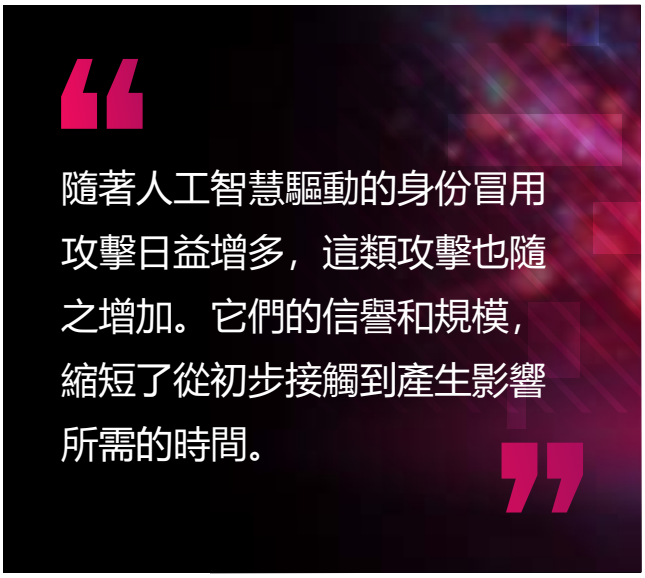
> 有效的零信任需要持續身份驗證以及上下文、預設最小權限存取和架構控制限制橫向移動。

零信任原則同樣支撐著抵禦人工智慧驅動的社會工程攻擊、雲端驅動的攻擊面擴展以及勒索軟體攻擊的能力，這些攻擊越來越依賴被盜身分而不是漏洞利用。

重要性：零信任是管理現代身分風險的實用框架——減少隱式信任、限制影響範圍，並確保身分外洩不會自動轉化為廣泛的存取或業務中斷。

6. 加強基於信任的業務流程，防止濫用

攻擊者越來越多地利用業務工作流程中的隱性信任來牟利，而不是僅僅依靠技術上的突破。商業電子郵件詐騙 (BEC)、高階主管冒充和供應商詐欺仍然非常有效，因為它們利用合法的通訊管道發起金融交易、洩露敏感資料。或修改存取權限。隨著人工智慧驅動的身份冒充攻擊日益增多，包括逼真的網路釣魚誘餌、合成語音和深度偽造輔助的社會工程攻擊，這些攻擊的可信度和規模進一步提高，縮短了從最初接觸到造成影響所需的時間。



首席資訊安全長應將基於信任的業務流程視為威脅面的核心組成部分，並相應地應用安全控制措施。這包括加強對電子郵件和協作平台的保護，對高風險操作實施強制性的、上下文感知的驗證，以及消除支付、供應商和訪問權限授予工作流程中的單步審批和其他隱式信任假設。這些對於高階主管和高風險業務部門而言，控制措施尤其重要，因為成功冒充身分可能會造成直接的經濟損失，或透過重置驗證資訊、擴大存取權限或竊取數據，為勒索軟體的部署鋪平道路。

重要性：BEC 和身分冒充攻擊正日益成為直接和間接攻擊的手段。勒索軟體和敲詐勒索活動的獲利途徑和推動因素。隨著攻擊者融合社會工程、身份濫用和人工智慧支援的欺騙，即使在擁有強大的邊界和端點防禦的環境中，未能加強基於信任的工作流程的組織仍然容易受到嚴重脆弱性的影響。

表單頂部

表單底部

7. 整合營運技術與網路風險治理

營運技術 (OT) 環境現在處於網路風險、實體安全和業務連續性的交匯點。隨著OT環境越來越多採用工業4.0架構 - 擴展工業系統物聯網 (IoT) 和工業物聯網 (IIoT) 裝置、雲端連接和遠端存取的普及，使得 IT 和 OT 之間的連接日益緊密——這主要得益於遠端存取、雲端顯示器和數位轉型——同時也拓展了攻擊路徑，使其能夠進入那些一旦遭到破壞就可能導致實體中斷、安全事故或長時間營運（而不僅僅是資料中斷）的環境。

在這些環境中，可用性和確定性行為至關重要，因此傳統的 IT 安全模型已不足以應對，必須謹慎地應用主動安全控制措施。保護這種新型的雲端連接 OT 環境需要採用與其擴展的數位化和營運風險相匹配的安全方法。

首席資訊安全長 (CISO) 應確保 OT 安全採用基於風險且符合實際營運情況的模型進行管理，而不是將其視為一個獨立式技術領域。這包括實施嚴格且持續驗證的IT-OT 隔離，利用被動式和非侵入式顯示器在不中斷營運的情況下保持可見性，以及將 OT 遙測資料整合到集中式安全營運中心 (SOC) 的工作流程中，以便及早發現異常活動。

同樣重要的是，網路安全、工程和實體安全團隊必須在一個共同的風險框架下運作，該框架優先考慮安全、正常運行時間和彈性，確保在充分了解 OT 環境中發生的網路安全事件的潛在物理和營運影響的情況下對其進行評估和應對。

重要性：隨著攻擊者越來越多地將目標對準工業和關鍵基礎設施環境，OT 中的網路事件不再代表孤立的技術事件——它們直接轉化為安全風險、營運中斷和實質的業務影響。未能確保這一現代化設施安全的組織，作為企業網路風險治理的一部分，工業 4.0 OT 環境仍然容易受到繞過傳統 IT 防禦並利用網路安全和實體安全之間脆弱性的攻擊。

8. 證明韌性，而不僅僅是合規性

網路韌性不能再透過政策遵守情況或某一特定時間點的評估來推斷。由於攻擊面不斷變化，威脅利用漏洞的速度比審查週期能夠檢測到的速度更快，因此彈性必須是可衡量的、持續驗證的，並且以與業務相關的術語表達。年度審計和靜態風險評估或許能夠滿足監管要求，但它們並不能反映...組織在現實世界中抵禦、控制和從活躍威脅中恢復的容器能力。

同時，隨著雲端運算、自動化和人工智慧環境的日益複雜化，我們不能忽視網路安全衛生和安全基礎知識。許多成功的攻擊仍然利用了基本的弱點，這凸顯了韌性取決於保持強大的「後端」防禦。將「回歸基本」的練習與更新的能力結合。

首席資訊安全官 (CISO) 應轉向持續控制驗證和暴露驅動測量，整合來自整個環境的遙測數據，以評估控制措施不僅是否存在，而且在實際條件下是否有效。這包括監測暴露趨勢、補救速度和縮短跨攻擊路徑的遏制時間，並自動收集證據以減少人工合規成本。必須以不同的方式向董事會、監管機構、合作夥伴和客戶傳達有效性，使用基於結果的指標來證明風險降低、回應時間加快和控制措施得到改進，而不僅僅是完成容器清單。

數位信任和透明度計畫發出的訊號，如外部脆弱性報告、第三方調查結果以及對已揭露風險的回應，應被視為營運韌性的指標，而不是聲譽責任的指標。這些訊號可以獨立驗證組織識別和應對風險的速度和效率。

重要性：在持續的威脅活動和日益嚴格的監管審查環境下，能夠透過持續的衡量和實際結果來證明自身韌性的組織，比那些僅依靠定期合規性評估的組織，更有能力維護信任、滿足監管期望並對事件做出可信的回應。

08

曝險管理觀點

安全漏洞發生前的威脅情資

暴露管理視角

從事件回應到預防性安全

事件回應是任何安全措施中的關鍵職能。程序，但最終，它只代表大多數攻擊的最後階段。由當反應小組投入戰鬥時，敵方已經完成了偵察，建立了基礎設施，並啟動了入侵。最大的問題不在於組織如何快速反應事件確實發生了，但有多少事件原本是可以完全避免的?

越來越多的情報顯示，許多攻擊會在內部入侵發生之前很久就留下可偵測到的外部訊號。這些見解，如果放在具體的背景下理解，就提供了一個機會，可以透過在攻擊生命週期的早期階段解決暴露問題來減少對緊急應變的依賴。從風險暴露管理的角度來看，威脅情資在將安全計畫從被動遏制轉變為主動降低風險方面發揮基礎性角色。

這種觀點並不能取代事件回應或事後回應。違規調查。相反，它透過關注事件發生前的條件和活動來補充它們，目的是防止問題發展到需要應對的地步。

> 最大的問題不在於組織對事件的反應速度，而在於這些反應發生的頻率。這些事件原本是可以完全避免的。

攻擊者在入侵前會做什麼

在內部事件發生之前，攻擊者通常會花時間準備。這個準備階段通常包括一些組織外部的活動，但這些活動與組織的安全態勢直接相關。常見的例子包括創造外觀類似網域名稱、跨社交平台的品牌冒充、部署網路釣魚基礎設施、從先前的洩漏事件中竊取驗證資訊以及偵察暴露的服務。單獨來看，這些事件可能看起來互不相干或無關緊要。然而，總的來說，它們構成了即將發生的入侵企圖的最早跡象。

至關重要的是，這些活動發生在傳統的內部顯示器控制之外。它們先於惡意軟體執行、橫向移動或權限提升，因此發生在大多數事件回應觸發器啟動之前。因此，儘管這些階段代表了最早可以進行幹預的階段，但它們經常被忽視或降低優先順序。

全球攻擊面上的事件前情報

在全球攻擊面上，某些模式在事件發生前的階段會反覆出現。攻擊者很少直接從意圖剝削。傳統上，他們會建立基礎設施，測試交付機制，並根據observable回饋來改善目標定位。

儘管網路釣魚、身分冒用或基於驗證資訊的攻擊技術的普遍程度因行業和地理而異，但這些攻擊手段仍然是早期攻擊活動的主要來源。重要的是，外部 observable 的準備策略通常與事件回應團隊在入侵後 observable 的策略高度一致。防禦者面臨的挑戰並非缺乏早期訊號，而是難以辨識哪些風險敞口與特定組織相關、可信且可採取行動。

> 防守方的挑戰不在於缺乏早期訊號，而在於...要辨識哪些資訊是相關的、可信的，有困難並且可以針對特定組織採取行動。

如果在早期階段應對攻擊者的準備活動，後續影響可能非常顯著。在攻擊發生之前破壞網路釣魚基礎設施、消除身分冒用資產或緩解暴露的入口點，可以防止攻擊活動發展到內部入侵。

從風險敞口管理的角度來看，目標並非預測每一次攻擊，而是減少攻擊者可利用的風險敞口數量。透過在活動仍處於外部階段時應對威脅組織可以在攻擊產生警報、事件或業務中斷之前改變攻擊路徑。

有效的入侵前幹預通常會導致事件的避免，而不是產生可見的反應指標。攻擊往往悄無聲息地失敗。使用者不會受到影響。事件響應團隊也無需介入。隨著時間的推移，事件數量的減少是風險敞口得到有效管理的最有力證明之一。

案例模式：預先防範事件回應中遇到的相同威脅

在事件回應調查過程中，某些攻擊序列會頻繁重複出現。事後看來，許多此類事件都遵循以下法則。在內部出現妥協之前，這種發展過程已經從外部顯現出來。

外部冒充 → 內部盜用驗證資訊

在許多情況下，攻擊者的活動始於冒充外部品牌，例如使用相似的網域名稱、偽造通訊或建立詐騙社群媒體帳號，所有這些都是精心設計的。建立信譽。然後利用這些資產收集驗證資訊，這些驗證資訊隨後成為內部存取的主要機制。當內部偵測到驗證資訊濫用時，最初的冒充基礎設施往往已經完成了它的使命。

網路釣魚基礎設施 → 升級為事件回應

最終導致安全事件回應的網路釣魚活動很少會在毫無預警的情況下發生。支持這些活動的基礎設施通常會提前出現。當該基礎設施保持活躍狀態足夠長的時間並能服務使用者時，事態升級的可能性就會顯著增加。或者，如果這類基礎設施早期就遭到破壞，許多競選活動就會失敗。超越最初的交付嘗試，卻永遠無法發揮其全部潛力。

暴露情報 → 利用前的補償控制措施

並非所有入侵前的活動都以身分為驅動。在許多情況下，攻擊者的準備工作與暴露服務或配置中已知的弱點相吻合。當情報顯示攻擊者對特定攻擊路徑表現出濃厚的興趣時，組織可以應用補償控制措施，例如臨時緩解措施或虛擬保護，以在永久性修復措施實施之前降低風險。這些修復措施可以在攻擊者從偵察階段過渡到執行階段之前切斷攻擊鏈。

主動防禦洞察

- 在自動化和現成基礎設施的推動下，攻擊者的準備工作將持續加速。
- 入侵的可能性將與嚴重性評分的相關性降低，而與暴露持續時間和攻擊者的準備程度的相關性提高。
- 將威脅情資與降低風險結合的組織將隨著時間的推移降低事件發生的頻率。

彌合差距：威脅情資作為風險暴露管理的第一步

事件回應能夠提供攻擊如何成功的寶貴見解。風險暴露管理則將這些經驗教訓應用於生命週期的早期階段，利用威脅情資在事件發生前識別並降低風險。

透過將事前情報與事後經驗連結起來，組織可以縮小應對措施與預防措施之間的差距。威脅情資不是一種附加功能或資訊流；它是了解風險敞口、確定行動優先順序和減少需要回應的事件數量的起點。

> 事件回應向我們展示了攻擊是如何得逞的。真正的機會在於風險敞口管理所面臨的威脅。情報 - 在攻擊者活動仍處於外部階段時就利用這些經驗教訓，透過風險管理可以在需要回應之前阻止事件發生。

MICHAEL GREENBERG

曝險管理產品行銷負責人

關於 CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd.（www.checkpoint.com）為數位信任防護領域之領導者，透過 AI 驅動的網路安全解決方案，保護全球超過 10 萬家組織免於網路威脅。Check Point Software 透過其 Infinity 平台與開放生態系統，秉持著「以預防為優先」的理念，提升安全效能同時降低組織風險。藉由以 SASE 為核心的混合網狀架構，Infinity 平台實現地端、雲端與辦公環境的統一管理，為組織與服務供應商帶來靈活、簡潔與可擴展的網路安全能力。

聯絡我們

全球總部

以色列特拉維夫 Shlomo Kaplan 街 5 號，郵編 6789159，

電話：972-3-753-4599

郵箱：info@checkpoint.com

美國總部

CA 雷德伍德城 Oracle Parkway 100 號 800 室，郵遞區號 94065

電話：800-429-491

遭受?

請聯絡我們的事件回應團隊：

emergency-response@checkpoint.com

Check Point 研究

取得我們最新的研究和其他獨家內容，

請造訪 www.research.checkpoint.com

www.checkpoint.com