2026 上半年 APT 資安威脅報告

AI 時代下，
APT 組織如何將信任武器化

國家級威脅行為者正將 AI 融入攻擊鏈的每個階段，同時將其基礎設施隱藏於防禦者原本信任的服務之中。本報告解析驅動這些行動背後的地緣政治因素，以及防禦方接下來應優先採取的措施。

TrendAI™ Research

執行摘要

本報告分析 2026 年 1 月至 6 月間，與四大主要地緣政治區域相關的進階持續性威脅（APT）活動。五項要點特別值得關注：

- **AI 應用範圍擴及更多觀察到的攻擊行動。** 2026 年上半年，AI 被觀察到用於入侵行動中更多階段；與中國相關的組織運用生成式 AI 強化漏洞攻擊，並透過反覆的「氛圍編碼」（vibe coding）開發惡意程式。其中一個案例中，AI 代理程式（AI agent）獨立執行了自身的偵察與橫向移動行動。與此同時，與俄羅斯及北韓（DPRK）相關的行為者也被觀察到使用商用 AI 工具。
- **已知漏洞與零日漏洞皆被快速武器化，供應鏈仍是攻擊者偏好的入侵管道。** 與俄羅斯相關的 Pawn Storm 組織在 2026 年上半年初期即利用一個 Office 零日漏洞展開行動。與此同時，Earth Dahu 則因 WinRAR 工具本身不會自動更新，數月來持續利用一項未修補的 WinRAR 漏洞。與伊朗相關的 Earth Vetala 在一項新披露的 Ivanti 漏洞公開後數天內即展開掃描，而與北韓相關的行為者則對一款廣泛使用的軟體套件下毒，藉此滲透下游開發人員。
- **關鍵基礎設施與實體世界目標再度成為焦點。** 與伊朗相關的行為者轉向對暴露於網際網路的營運技術（OT）發動直接攻擊，竄改美國多處據點的油槽量測儀。與此同時，與俄羅斯相關的行動持續向烏克蘭及其在政府、國防與戰時援助領域的合作夥伴施壓。另有偽裝成廣告買家的操作者被觀察到運用廣告情報（ADINT）技術，透過線上廣告競價系統擷取位置與裝置資料，藉此透過受害者所使用的應用程式追蹤其行蹤。
- **指揮與控制（C2）架構及攻擊工具日益仰賴受信任的共用基礎設施。** 威脅行為者被觀察到將指揮與控制（C2）架構部署於企業原本信任的服務之上，例如主要雲端平台、開發人員通道（tunnel）、公開區塊鏈及貼文網站（paste site）。攻擊者偏好使用這些服務，是因為其流量能融入正常活動之中，且不易遭到下架。許多行為者如今更以租用勒索軟體即服務（MaaS）或共用工具的方式行動，這使得歸因調查更加困難。
- **這些行動背後的政治局勢預計將持續存在。** 烏克蘭戰爭已陷入長期消耗戰，而俄羅斯則在 9 月國會選舉前加強資訊管制。與此同時，北韓似乎正持續鞏固其作為擁核國家的地位，並以網路竊盜行動作為資金來源。中國一方面應對與美國的競爭關係，一方面積極推動晶片與 AI 自主化；而與伊朗相關的行動則隨區域緊張情勢升溫而加劇。預期這些趨勢將持續形塑年底前的威脅態勢。

本報告的分析取自一項更廣泛、持續進行中的研究成果：《APT 研究報告》，該報告每兩個月發布一次，可於 TrendAI Vision One™ 威脅情報中心（Threat Intelligence Hub）取得。讀者可於該系列報告中，取得包含入侵指標與技術細節在內的完整研究內容。

目錄

中華人民共和國

與中華人民共和國（PRC）相關的入侵組織持續進行網路間諜活動。政治局勢背景，形塑了我們在 2026 年上半年監測到的網路活動之目標選擇與攻擊手法。

政治趨勢

- **AI 已成為國家優先發展項目，受惠於充沛能源但受限於晶片供應。** 中國已將 AI 定位為國家整體規劃中經濟成長的核心引擎。旨在制定國家經濟與發展藍圖的「十五五」規劃將 AI 列為核心優先項目，並由國家在能源與國產晶片開發方面提供投資支持。截至 2026 年 5 月底，中國已裝置發電容量達 4 太瓦（TW），為運算密集型 AI 提供充足的基礎資源。據報導，西部地區廉價的綠色電力可支持國內運算能力快速擴張。與此同時，中國企業持續開發新技術，以因應影響先進晶片生產的制裁措施。
- **北京已成為高層外交活動的樞紐。** 1 月，中國接待了南韓總統李在明、加拿大總理馬克．卡尼（Mark Carney），以及英國首相基爾．斯塔默（Keir Starmer）。隨後，美國總統唐納．川普（Donald Trump）訪問北京，中美雙方同意成立委員會，推動針對部分非敏感商品的關稅削減。雙方討論也觸及中國可能增加採購美國農產品、波音飛機及能源等議題。儘管在稀土元素（REE）近乎壟斷及技術管制等議題上進展有限，但雙方已建立進一步對話的框架。此次會晤後不久，中國國家主席習近平與俄羅斯總統普丁在北京會面，簽署了約 40 項合作協議。這兩場高峰會的接續舉行，凸顯了中國的雙軌定位策略：一方面管理與美國的貿易關係，一方面深化與俄羅斯的夥伴關係。
- **在中國軍方肅貪行動之際，美中軍事與貿易緊張情勢升溫。** 5 月，前國防部長、曾任中央軍事委員會委員的魏鳳和與李尚福均因貪腐罪名被判處死刑緩期執行。這兩位將領是自 2022 年中國展開反貪腐及肅清軍中不忠誠份子行動以來，公開遭判刑的最高階將領。緊張情勢也蔓延至貿易領域。美國國防部擴大其「中國軍事企業」清單，將阿里巴巴、百度及比亞迪（BYD）納入其中。北京則以將 10 家美國企業列入出口管制清單作為報復，其中包括稀土生產商 MP Materials 與 USA Rare Earth。中國也禁止近 50 家美國國防承包商參與中國政府採購案。

網路攻擊行動

AI 輔助開發與代理式橫向移動

- **Earth Krahang 運用 AI 強化漏洞攻擊開發。** Earth Krahang 是一個與中國相關的組織，主要針對全球政府與國防部門，經常利用遭入侵的基礎設施發動攻擊。該組織運用生成式 AI 強化一項公開可取得的概念驗證（PoC）漏洞攻擊程式，鎖定 CVE-2026-0740，此為 WordPress 外掛程式「Ninja Forms – File Uploads」中的一項漏洞。經強化後的攻擊程式能夠進行大規模自動化掃描，以找出存在漏洞的公開伺服器。該組織還在其 C2 伺服器上安裝了由字節跳動（ByteDance）開發的整合開發環境（IDE）AI 程式碼撰寫工具 Trae。AI 生成的程式碼註解以簡體中文撰寫，顯示操作者的來源背景。
- **Earth Naga 運用氛圍編碼（vibe coding）開發惡意程式。** Earth Naga（與 Flax Typhoon 相關）是一個與中國相關的組織，主要鎖定關鍵基礎設施、政府及科技部門，並大量運用高度靈活的「就地取材」（living-off-the-land, LotL）技巧以規避偵測。該組織被觀察到使用反覆的 AI 提示工作流程（即「氛圍編碼」）來開發一款惡意 PowerShell 指令碼。該指令碼會在執行階段編譯並執行 C# 程式碼，以進行處理程序挖空（process hollowing）及後門酬載的反射式

載入。研究人員在其代管伺服器上發現多個版本演進中的指令碼，其中 AI 回應提示的內容以註解形式留存於程式碼內，這些註解無意間洩露了該組織的開發方法。

- **不明行為者（可能為 Earth Lamia）運用自主 AI 代理程式進行橫向移動。** 該組織針對泰國一家機構，部署 Claude Code 命令列介面（CLI）作為自主 AI 代理程式。該行為者透過謊稱此行動為合法的滲透測試，成功繞過該 AI 模型的安全限制。隨後，該 AI 代理程式自主執行了內部網路掃描、漏洞攻擊嘗試（包括 EternalBlue、SMBGhost、PrintNightmare、SMB 中繼攻擊）、憑證擷取（透過 secretsdump、LaZagne 及 Impacket 工具），以及密碼噴灑攻擊。

濫用合法服務作為 C2 通道

- **Earth Baxia 透過 Microsoft 365 電子郵件草稿進行 C2 通訊。** Earth Baxia 是一個高度活躍、與中國相關的組織，主要鎖定東南亞及印太地區的政府機構。該組織的特點在於投入自製工具開發，並致力於維持完全無聲的行動足跡。其自製的 Rust 後門程式 CRAITHNEX，被觀察到完全透過 Microsoft Graph API 的未寄出郵件草稿進行通訊。該後門利用此 API 從草稿主旨列讀取指令，並將執行結果寫回草稿回覆中，同時將檔案傳輸工作交由 OneDrive 處理。由於從未實際寄出任何郵件，其流量能完全融入正常的 Microsoft 365 企業營運活動之中，因此在不干擾企業工作流程的前提下，要偵測或封鎖此活動極為困難。

- **SHADOW-EARTH-067 濫用雲端服務與區塊鏈交易平台。** SHADOW-EARTH-067 是一個與中國相關的組織，鎖定台灣、泰國及馬來西亞，其特點在於具備多層規避技巧及長期持續潛伏能力。該組織的 WHISPERNOTE 後門被觀察到濫用 Microsoft DevTunnel、OneNote 及 OneDrive 進行 C2 通訊。若這些通道遭中斷，該後門會轉而解析隱藏於 Stellar 區塊鏈交易備註中的網路設定資訊。在橫向移動方面，該組織利用使用者資料包通訊協定（UDP）上的 KCP 協定，在受感染主機之間建立點對點網狀網路，並在受限環境下改用伺服器訊息區塊（SMB）具名管道作為備援。

多階段網路釣魚：誘餌文件與社交工程話術

- **Earth Baxia 運用地緣政治誘餌與誘餌 PDF 進行社交工程。** 作為一個主要鎖定印太地區政府機構的活躍組織，Earth Baxia 精心設計以區域領土爭端及政策預測為主題的高度客製化魚叉式網路釣魚郵件。當受害者開啟附件中的惡意指令碼（HTA 或 WSF 檔）後，惡意程式會顯示一份外觀合法的誘餌 PDF 文件以分散使用者注意力，同時在背景悄悄執行 CRAITHNEX 後門程式。

- **APT24 運用多重管道與木馬化軟體。** APT24 以在東亞地區發動廣泛的網路間諜行動著稱，該組織同時運用多條初始入侵管道，將惡意捷徑檔案（LNK 檔）隱藏於 Google 雲端硬碟連結之中。值得注意的是，該組織被觀察到部署 SUESTAG，這是一款偽裝成合法台灣輸入法編輯器（「Going IME」）更新程式的惡意工具。該工具會顯示一個逼真的更新對話框以擷取使用者憑證，並植入 NOMASTEAL 資訊竊取程式。

- **SHADOW-EARTH-068 運用多輪信任建立及水坑式攻擊陷阱。** SHADOW-EARTH-068 主要鎖定海事、半導體及物流產業，該組織採取高耐心策略，以企業身分展開長達數週的電子郵件往來以建立信任，之後才寄送夾帶惡意程式的酬載。該組織也被觀察到透過劫持受信任的網站，並植入以多種語言（繁體中文、英文、德文及印尼文）顯示假冒瀏覽器憑證錯誤訊息的指

令碼，執行水坑式攻擊。這些指令碼會誘騙受害者下載一款名為「CertFixer」的惡意工具。此行動鎖定範圍涵蓋菲律賓、台灣、印尼、秘魯、捷克、德國及美國等地的組織。經確認的受害者涵蓋政府機構、造船公司、半導體晶圓廠、物流業者、非政府組織（NGO）及研究機構。

利用「自帶漏洞驅動程式」（BYOVD）規避 EDR 與防毒偵測

- **SHADOW-EARTH-067 透過 BYOVD 技術使 EDR 與防毒工具失效。** 2026 年上半年，與中國相關的組織日益採用「自帶漏洞驅動程式」（BYOVD）技巧來癱瘓資安防護。這些行為者並非在使用者層級規避防護機制，而是部署能載入受信任、已簽署但存在已知漏洞的第三方驅動程式的 rootkit。這使其能取得核心層（kernel-level）存取權限，從源頭停用 EDR 代理程式。SHADOW-EARTH-067 被觀察到運用此技術永久停用受害者的資安監控，使其在整個行動期間能不被偵測、對全系統維持潛伏。該組織使用自製的 DELEVATE 載入程式部署 VIRIFUSE rootkit，接著武器化一項存在漏洞的驅動程式（ICRTouchIO.sys），藉此深入核心層並操控記憶體、卸除處理程序監控機制，並使 Windows 威脅情報事件追蹤（ETW-TI）遙測失效。一份外部設定檔提供驅動整個攻擊鏈所需的各版本位移值（offset），使該組織能在各種 Windows 版本上穩定執行相同的攻擊。

朝鮮民主主義人民共和國（北韓）

2026 年上半年，與朝鮮民主主義人民共和國（北韓，DPRK）相關的網路行動，仍以財務動機為主，間諜活動則屬於機會性的附帶產物。主要攻擊手法包括供應鏈下毒、加密貨幣竊盜及 IT 員工滲透。不同的行動小組似乎各自獨立運作這些行動，且各自須自行籌措行動資金。

政治趨勢

- **制裁與電網問題使北韓無法在國內開發強大的 AI 模型。** 國際制裁使北韓缺乏先進晶片，而老舊的電力網也可能無法穩定供應大規模 AI 運算所需的持續電力負載。然而，北韓最高領導人金正恩於 2026 年 2 月在朝鮮勞動黨第九次代表大會上的講話中，將 AI 列為當務之急的優先項目，其中最具體的內容提及「各種 AI 無人攻擊系統」。結合 2026 年 5 月已確認的 AI 導引飛彈試射，以及派赴俄羅斯遠東地區的無人機訓練代表團，顯示軍用 AI 發展路線已在執行之中。為了在短期內實現其 AI 野心，北韓勢必得持續採取非對稱手法，包括在境外運行電腦伺服器、濫用西方 AI 模型、使用中國 AI 模型，以及在俄羅斯接受 AI 訓練。

- **北韓持續鞏固其作為永久擁核國家的地位。** 這項核武野心的成本，似乎仍是驅動北韓相關攻勢性網路行動的關鍵因素。2026 年 3 月，有報導指出北韓測試了一款新型固態燃料火箭引擎，據信是為洲際彈道飛彈（ICBM）而研發。同月，北韓修訂憲法，刪除所有有關「民族統一」的內容，正式將南韓重新定位為獨立的敵對國家。此項修憲也明確授予金正恩或其指定代理人對政權核武力量的指揮權。2026 年 6 月，北韓公開了一座新的鈾濃縮設施。同月，北韓也將其首艘 5,000 噸級多功能驅逐艦服役，該艦可能具備發射具核武能力的陸攻巡弋飛彈的能力，惟此點尚未獲得證實。

- **北韓與美國的關係持續處於凍結狀態，北韓幾乎不感受到讓步的壓力。** 金正恩堅持美國必須放棄其無核化框架，並接受北韓作為永久擁核國家的地位。

- **俄羅斯與北韓的關係在 2026 年上半年進一步加深。** 北韓持續支持俄羅斯對烏克蘭的戰爭，作為回報，獲得糧食、現金、軍事技術及創新的戰場經驗。平壤如今公開將傷亡描述為為國家做出的偉大犧牲。一支北韓代表團造訪了俄羅斯位於阿穆爾州的無人機訓練中心，多位俄羅斯高階官員也曾造訪平壤。俄羅斯於 2025 年向北韓公民核發超過 36,000 份簽證，官方說法是用於教育目的，此數字約為 2024 年的四倍，這波人流很可能是為了彌補俄羅斯的勞動力短缺。

- **在一段明顯疏遠期後，中國大幅重新與北韓接觸。** 中國外交部長王毅於 2026 年 4 月造訪平壤，分別與外務相崔善姬及金正恩本人會談。北京似乎意在保留對北韓的影響力，可能將其作為對美博弈的籌碼，同時防止北韓過度靠向俄羅斯。

- **北韓經濟正在成長，但僅嘉惠菁英階層，而非全體人民。** 2023 年與 2024 年，北韓經濟成長率分別估計為 3.1% 及 3.7%，顯示已從疫情後的萎縮中復甦。然而，這波成長主要由國家推動，來源為軍事支出以及向俄羅斯出售武器及派遣部隊。截至 2025 年 10 月，米價達到高峰，以當地貨幣計算幾乎翻漲四倍；但以美元計價則維持穩定，因為同期間北韓幣（won）兌美元大幅貶值。這實質上是一場財富由一般民眾轉移至持有外幣的菁英階層及國家機關的過程。

- **北韓網路行動仰賴中國及俄羅斯的網路基礎設施。** 為了能夠發動網路攻擊，北韓高度依賴中國與俄羅斯提供的網路連線。自俄烏戰爭爆發以來，北韓已越來越常使用俄羅斯境內的靜態 IP 網段。北韓還在全球部署了數百台虛擬私人伺服器（VPS），這些伺服器透過虛擬私人網路（VPN）服務、代理伺服器，有時則直接透過分配給北韓、俄羅斯及其他國家的 IP 位址進行管理。這些 VPS 實例被用於 AI 實驗、架設網站、架設加密貨幣詐騙網站及 C2 伺服器，同時也作為存取 LinkedIn、Upwork、GitHub 及 Dropbox 等服務的出口節點。

網路攻擊行動

供應鏈攻擊鎖定受信任的開發者基礎設施

- **BlueNoroff 入侵 Axios 專案首席維護者的 npm 帳號，並於 2026 年 3 月 31 日發布遭下毒版本的熱門 JavaScript HTTP 用戶端函式庫。** 該受害套件已知每週下載次數超過 1 億次。BlueNoroff（又稱 APT38 或 Sapphire Sleet）是 Lazarus 集團旗下一個財務動機導向的子組織，以鎖定加密貨幣平台及金融機構著稱。該組織植入一個名為 plain-crypto-js 的幽靈相依套件，此套件從未在 Axios 程式碼中實際被使用，其存在的唯一目的是觸發 npm 的安裝後掛鉤（postinstall hook），藉此部署一款跨平台的遠端存取木馬（RAT），鎖定 macOS、Windows 及 Linux 系統。TrendAI™ 遙測資料證實，此事件在 21 個國家共造成超過 100 次偵測，影響政府、金融、科技、醫療等多個產業的組織。
- **Void Dokkaebi 發動一場蠕蟲式行動，誘騙軟體開發人員複製偽裝成求職面試程式測驗的惡意程式碼儲存庫，再將受感染的機器轉變為傳播節點。** 此行動採用兩種感染管道：其一是會在開啟工作區時自動執行的惡意 VS Code .vscode/tasks.json 檔案；其二是主動竄改提交紀錄（commit），將混淆過的 JavaScript 程式碼植入受害者的儲存庫，同時改寫 git 歷史紀錄。所投遞的酬載（DEV#POPPER RAT 變種）利用區塊鏈基礎設施進行酬載暫存，以抵抗下架行動，並藉由劫持 VS Code、Cursor 及 Discord 等開發人員應用程式來維持潛伏。2026 年 3 月，TrendAI™ 辨識出超過 750 個受感染儲存庫、超過 500 個惡意 VS Code 任務設定，以及 101 個提交竄改工具的實例。屬於 DataStax 及 Neutralinojs 等組織的儲存庫也帶有感染痕跡。該組織亦被稱為 Famous Chollima，以透過假求職面試投遞 BeaverTail 及 InvisibleFerret 惡意程式著稱。研究人員也觀察到該組織將社交工程與具供應鏈風險的傳播模式相結合。

加密貨幣竊盜仍是主要的資金來源管道

2026 年 4 月，發生兩起被公開歸因於北韓相關行為者組織的大規模加密貨幣竊盜事件。2026 年 4 月 1 日，一項名為「Drift Protocol 駭客攻擊」的行動，從基於 Solana 的去中心化交易所（DEX）Drift 竊取了 2.85 億美元，該行動極可能是由某個此類組織所發動。這起竊案發生前，攻擊者已針對 Drift 安全委員會（Security Council）的簽署人展開數月的社交工程滲透。攻擊者利用 Solana 的持久性隨機數（durable nonce）功能，預先授權提款交易，並在約 12 分鐘內完成執行。

2026 年 4 月 18 日，一個未經歸因的北韓相關行為者組織從 KelpDAO 的跨鏈橋（cross-chain bridge）中提取約 2.92 億美元。該組織入侵內部遠端程序呼叫（RPC）節點，並發動分散式阻斷服務（DDoS）攻擊，迫使橋接系統的單一驗證節點依賴遭污染的資料，進而核准一筆偽造的跨鏈訊息。

除了這些大規模竊案外，北韓相關行為者組織也可能經營規模較小的加密貨幣詐騙網站，鎖定毫無防備的投資人。包括 Void Dokkaebi 在內的多個北韓相關行為者組織，也在其行動中竊取個人的加密貨幣錢包資產。

北韓相關行動似由自籌資金的獨立小組運作

由於戰術、技術與程序（TTP）及基礎設施存在重疊，將特定的網路行動歸因於特定的北韓相關入侵組織，往往極具挑戰性。即便在單一入侵組織內部，也能識別出不同的子集。對此的一種可能解釋是：不同的北韓相關行動小組各自獨立運作，使用相同的惡意程式套件，且必須各自籌措行動資金。

IT 員工滲透手法持續影響全球組織

IT 員工滲透手法在 2026 年北韓相關網路行動中依然十分顯著。根據 TrendAI™ 的電子郵件掃描遙測資料，多個職缺公告吸引了來自北韓相關 IT 員工的多份應徵申請，其中部分人選甚至進入了線上面試階段。這些 IT 員工慣於使用換臉工具、深偽（deepfake）技術及 ChatGPT 等類似工具，用於美化履歷及即時應付面試問題。

根據技術指標，可辨識出多個不同的 IT 員工活動叢集，這顯示可能有多個小組在世界不同地點各自運作此 IT 員工滲透計畫。在一起觀察到的案例中，某個 IT 員工叢集，被連結至一起明顯試圖規避「禁止向北韓出口電腦數值控制（CNC）機械設備」制裁規定的行動。

IT 員工滲透計畫高度仰賴目標國家境內的協助者，這些協助者負責替該行動洗錢及規避制裁。美國已對多個國家（包括寮國及越南）的協助者實施制裁，並於 2026 年 4 月及 5 月分別對一名烏克蘭籍公民及四名美國公民判刑。

間諜行動呈現機會主義特性

這類行動往往帶有機會主義色彩，多半是其他入侵行動的附帶產物。例如 Void Dokkaebi 針對高知名度目標的行動，以及成功取得國防等產業職位的 IT 員工。SHADOW-EARTH-062（Operation Dream Job 相關入侵組織的暫定代號）正於高度針對性的行動中使用 BLINDINGCAN 惡意程式。至少有一起案例中，TrendAI™ 偵測到針對國防產業供應鏈的入侵嘗試。

俄羅斯聯邦

在 2026 年上半年，與俄羅斯相關的網路威脅行動，圍繞著三項發展態勢展開：一場逐漸陷入消耗戰的戰爭、一個在 9 月俄羅斯國會選舉前加強國內管控的國家，以及一場對「主權 AI」的強力推動。在此背景下，俄羅斯相關的入侵組織持續鎖定支撐烏克蘭及其夥伴運作的系統與供應鏈。其所使用的工具，從全新的 Office 零日漏洞攻擊程式，到經改造成殭屍網路的十年前老舊植入程式，種類繁多。

政治趨勢

- **國家主導的「主權 AI」推動計畫，受限於硬體天花板。** 2026 年上半年，俄羅斯致力於將 AI 打造為國家級專案。2 月，總統普丁成立了「總統人工智慧委員會」，成員包括俄羅斯聯邦安全局（FSB）、國防部及俄羅斯儲蓄銀行（Sber）代表。此舉顯示克里姆林宮將 AI 視為安全與管控工具，而非僅是一項產業。3 月隨後推出一項有關「主權、國家與可信 AI」的聯邦法律草案，同月 Sber 也推出了 GigaChat Ultra。目前該國面臨的硬性限制在於運算能力：制裁措施使高階 GPU 持續短缺，迫使俄羅斯須透過第三國以高昂溢價購入相關硬體。公開資訊並未顯示俄羅斯的前沿模型已能與西方領先模型匹敵。俄羅斯的 AI 應用工作也正拓展至無人機領域，據報導已對 Geran-2 機型進行自主目標鎖定測試。
- **俄羅斯正準備打一場長期化的凍結戰爭。** 截至 2026 年上半年，俄羅斯入侵烏克蘭已邁入第五年。儘管傷亡持續攀升，雙方也不斷以有限的戰果作為談判籌碼，前線幾乎毫無變動。有關領土的談判毫無進展，烏克蘭則持續以加強對俄羅斯煉油廠的無人機攻擊維持壓力。這些攻擊旨在削減俄羅斯的煉油產能，迫使莫斯科在 2026 年年中前實施燃油出口限制及區域配給。在烏克蘭與 SpaceX 聯手切斷俄羅斯對 Starlink 的非官方使用後，俄羅斯戰場通訊的脆弱性更加顯著。與此同時，莫斯科持續透過「1440 局」（Bureau 1440）開發自有的衛星網路替代方案，據報導預計於 2027 年投入商業服務。無人機戰事在雙方也日趨成熟，氣象資料、後勤及供應鏈依然是具高價值的攻擊目標。
- **在自入侵爆發以來首次舉行的 9 月國會（杜馬）選舉前，資訊管控正逐步收緊。** 今年上半年最明顯的國內趨勢，是國家依既定步調收緊對資訊空間的掌控。行動網路關閉範圍已從邊境地區擴大至 2025 年底的全國性規模，到 2026 年 3 月，就連莫斯科市中心也曾連續兩週以上失去穩定的網路服務。一項新法律現已強制電信業者配合 FSB 的關閉指令。俄羅斯目前也正在推動一份經核准的「國內服務安全名單」，其中包括本國自製的 Max 通訊軟體，同時限制 Telegram、WhatsApp、YouTube 及 Roblox 等服務。2026 年 2 月 Levada 民調顯示，支持和平談判的比例達到 67%，創下歷史新高。財政狀況則是另一項緩慢累積的風險：石油與天然氣收入佔聯邦預算的比重降至約 23%，創 5 年來新低。中東地區油價短暫飆升一度緩解了此一下滑趨勢，加值稅（VAT）也因應戰爭需求而調升。

網路攻擊行動

利用文件與檔案漏洞取得初始入侵

- **Pawn Storm 以一項 Office 零日漏洞展開 2026 年上半年行動，並搶在公開揭露前將其武器化。** 該組織亦被稱為 APT28 或 Fancy Bear，多年來持續針對政府、軍方及國防產業展開與俄羅斯相關的間諜行動。該組織將微軟 Office 中一項先前未知的漏洞（追蹤代碼為 CVE-2026-21509 的零日漏洞）武器化，使一份預先準備好的文件能在幾乎不需使用者互動的情況下，悄悄擷取並執行攻擊者的程式碼。此漏洞並非記憶體損毀類型的臭蟲，而是利用 Office 判斷內嵌物件是否安全載入的邏輯缺口，這類缺陷極易被忽略，且在傳輸過程中難以被察覺。相關攻擊基礎設施早在漏洞公開揭露約 2 週前便已註冊完成，顯示該組織早已預先備妥此項武器。

- **Earth Dahu 運用一項多數目標未修補的已知 WinRAR 漏洞。** 該組織廣為人知的名稱為 Gamaredon，是一個與俄羅斯相關的組織，針對烏克蘭政府及軍事目標進行高頻率的間諜行動。經過特製的壓縮檔會悄悄植入一個檔案，並在機器下次啟動時執行（對應 CVE-2025-8088）。由於 WinRAR 本身不會自動更新，許多使用者從未修補此漏洞，導致該漏洞維持可用狀態長達數月，也吸引其他組織於同期利用此漏洞。俄羅斯相關的這兩起案例，皆是透過電子郵件夾帶檔案來接觸目標：其一使用全新的零日漏洞，另一則利用已知但未修補的臭蟲。一款從不自動更新的工具，足以讓一項舊漏洞在修補程式問世後仍長期存續。

隱藏惡意程式：混淆技巧、隱寫術與受信任的執行環境

- **Pawn Storm 將其 PRISMEX 工具包隱藏於受信任的處理程序與圖像檔案中，以維持隱蔽性。** 該組織透過劫持一個受信任的 Windows 處理程序來建立持久性，使惡意程式得以在系統已信任的名稱下運行。接著，該組織運用隱寫術（steganography）將下一階段酬載隱藏於一張外觀普通的圖片之中，將隱藏資料分散於整張圖片內以增加偵測難度。最終階段的惡意程式完全在記憶體中運行，在硬碟上幾乎不留下任何痕跡。此工具包是該組織過去曾使用的一系列感染鏈的延伸版本，如今經過調整，能快速利用新披露的漏洞。這使得同一操作者能夠將新發現的高價值漏洞攻擊，快速嵌入其早已信賴的攻擊機制之中。

- **Laundry Bear（Void Blizzard）利用合法、經簽署的執行環境運行其程式碼，使下載內容看似合法。** Laundry Bear 是一個較晚被辨識出的與俄羅斯相關組織，主要針對烏克蘭及其支持者進行間諜活動。受害者透過類似 Signal 的通訊軟體被接觸，並被引導至偽造的慈善機構網站，惡意程式則以多種不同的載入程式變體形式送達。這些載入程式會直接從官方來源下載合法且經簽署的程式設計執行環境，再於其上運行攻擊者自製的程式碼。由於下載內容本身合法，該活動極難被標記為可疑。其 PLUGGYAPE 後門程式在歷經多個版本演進後，混淆程度日益提高，並有跡象顯示該組織正將其擴展至 macOS 平台。

- **Earth Dahu 每隔幾週便重塑其載入程式，以領先偵測技術。** 2026 年上半年，該組織的載入程式被觀察到幾乎以每月為週期改變格式，從一種指令碼格式轉換至另一種，再進一步轉為經編碼的變體。每一次的變化，都與防禦方逐漸能辨識出前一版本的時間點相吻合。到了年中，該組織甚至改用多數電子郵件過濾器幾乎不會檢查的 1990 年代舊式壓縮檔格式，並偽裝成較常見的檔案副檔名。這些變化讀來更像是針對防禦方追上進度所做出的刻意反應，而非例行性的輪替。大量網路釣魚郵件源自真實但遭入侵的政府與市政機關電子郵件信箱，且同一帳號在多起案例中被重複使用，這使得郵件在收件者眼中顯得更加真實可信。

- **SHADOW-EARTH-065 依賴封裝與偽裝技巧，避免其工具遭到識別。** SHADOW-EARTH-065 是 TrendAI™ 為一個與俄羅斯相關、且與 UAC-0099 有所重疊的組織所賦予的暫定代號，據報導該組織已將存取權限轉交給具破壞性的 Sandworm 組織。該組織使用商用封裝程式包裝其 BadPaw 工具，將酬載隱藏於圖片檔案之中，並將檔案偽裝成無害的文件類型。

打造能融入環境、抵抗下架的 C2 架構

- **Turla（Secret Blizzard）將 Kazuar 改造為一個低調難尋、難以下架的殭屍網路。** Turla 是歷史最悠久的與俄羅斯相關間諜組織之一，以對政府及國防網路進行隱蔽的長期入侵著稱。該組織自 2017 年起便持續使用 Kazuar 工具集，自 2024 年初起，TrendAI™ 已觀察到該工具被用

於針對賽普勒斯及烏克蘭政府目標的攻擊。微軟發布的一份分析報告顯示，Kazuar 已被改造為一個殭屍網路，在每個網路中僅由一個被選定的節點代表其他節點對外聯繫，此舉大幅減少了防禦方能察覺的對外流量。該惡意程式主要透過一般網頁流量進行通訊，其他通訊管道則保留作為備援。它從植於遭入侵合法網站上的死投遞點（dead drop）獲取指令，因此不存在固定的攻擊者伺服器可供封鎖，且各受害群組能被彼此隔離管理。TrendAI™ 自 2024 年起，便持續追蹤這款具備三個模組的 Kazuar 新版本。

其他組織則將 C2 架構部署於受信任的服務之上，使其難以直接遭到封鎖：

- Pawn Storm 將 PRISMEX 透過一項合法的加密雲端儲存服務進行傳輸，使其 C2 流量能融入一般的加密網頁使用活動之中。
- Laundry Bear 將其位址存放於 Pastebin、rentry.co 及 Ghostbin 等公開貼文網站上。操作者只需編輯網頁，即可變更惡意程式回報的位址，無需觸碰惡意程式本身。
- Earth Dahu 以 Cloudflare Workers 及 TryCloudflare 通道作為其 C2 的前端，快速輪替基礎設施，並為每個版本加註標籤，以便操作者辨識該版本所屬的目標群組。
- SHADOW-EARTH-065 將其流量隱藏於外觀正常的網頁回應內容之中。

這些組織的共同目標，是讓與操作者之間的連線成為入侵行動中最不顯眼、最可拋棄的一環——而這正是防禦方過去用以偵測入侵的關鍵環節。

鎖定與戰爭相關的實體，並伴隨駭客行動主義（hacktivist）施壓

- **Pawn Storm 的目標範圍涵蓋眾多與戰爭相關的機構，而非單一產業。** 該組織鎖定了國防部、邊境警察、國會、國防大學及國家氣象單位，範圍不僅限於烏克蘭，也涵蓋該區域的盟友。其對氣象單位的興趣值得留意，因為氣象資料可用於支援無人機及火砲行動規劃，觀察到的訊息內容也指向烏克蘭軍方無人機部隊。
- **Laundry Bear 冒充戰時慈善機構，藉此接觸相同的供應鏈。** 該組織偽裝成提供發電機及冬季暖氣設備的慈善機構，並選在寒冷月份展開行動。其誘餌內容提及烏克蘭及鄰國的無人機部署位置及倉庫存貨資訊。受害者會看到一份看似合法的文件如預期般開啟，而惡意程式碼則在背景中運行。結合其對供應地點的興趣來看，此行動讀來與其說是純粹的情報蒐集，不如說更像是為實體攻擊行動預作準備。其影響範圍並不僅限於烏克蘭，其他地區與援助行動相關的組織也捲入同一波行動之中。2025 年年底，一名俄羅斯籍人士應美國要求在境外遭到拘捕，被控涉入該組織的活動。
- **SHADOW-EARTH-065 鎖定烏克蘭政府及國防人員。** 該組織偽裝成邊境守衛單位，隨後部署其 BadPaw 及 MeowMeow 工具。如前一節所述，該組織也曾被觀察到與一個具破壞性的組織有所關聯。
- **NoName057(16) 持續發動由志願者驅動的 DDoS 攻擊，其行動與戰爭的政治情勢緊密相關。** NoName057(16) 是一個親俄羅斯的駭客行動主義（hacktivist）集團，發動 DDoS 攻擊以支持莫斯科的政治目標。該組織對數十個國家（範圍已超出北約成員國）的政府、交通、金融及能源目標發動攻擊，尤其是在某國政府宣布支持烏克蘭或對俄羅斯實施制裁之後。該組織運行一套自製工具，並交由志願者使用，志願者則依貢獻程度獲得加密貨幣報酬，使得一支小型核

心團隊得以按莫斯科的工作時段節奏維持行動步調。2025 年年中，歐洲一項執法行動查扣了該組織的基礎設施並逮捕了相關人員，然而該組織在數天內便恢復運作。這正是一個仰賴志願者、而非固定組織所會呈現的行為模式。其嚴重程度低於間諜行動，但已成為這場衝突中持續不斷的背景噪音。

其他地區

除前述內容外，2026 年上半年最值得關注的活動，是與伊朗相關的行動。
這些行動沿著三條防禦方應一併檢視的主軸展開：

- 對暴露於網際網路的營運技術（OT）發動直接攻擊
- 轉向租用犯罪工具及濫用受信任軟體，而非自行開發
- 在監控生態系統中進行大規模追蹤，且無需部署任何惡意程式

貫穿其中的共同脈絡是：過去僅限頂尖國家級行為者才具備的能力，如今已能直接購入現成方案，這使得判斷入侵行動背後真正主使者變得更加困難。

網路攻擊行動

針對暴露於網際網路的營運技術（OT）發動攻擊

- **暴露於網際網路的油槽量測儀，在 2026 年上半年成為活躍的攻擊目標。** 這些設置於加油站及儲存設施的量測儀，原始設計是在不驗證請求來源身分的情況下即回應網路指令。許多量測儀透過老舊的轉接器連上網際網路，使攻擊者能以簡單指令讀取或竄改油槽資料。TrendAI™ 早於 2015 年便透過誘捕系統（honeypot）研究首次記錄此暴露問題，當時已有攻擊者在掃描此類系統、下達有效的量測儀指令，並曾有一起案例將油槽名稱更改為竄改性訊息。該訊息被認為是由親伊朗駭客行動主義組織「伊朗黑暗程式設計師團隊」（Iranian Dark Coders Team，IDC-TEAM）所留下，該組織以網站塗改及低階竄改行為著稱。這種起初屬於機會主義式的竄改行為，如今已升級為對真實燃油基礎設施的攻擊，而只要工業讀數設備為求方便而連上網路，同樣的問題便可能發生於任何場域。
- **美國聯合公告將 CyberAv3ngers 與 IOCONTROL 惡意程式建立關聯。** CyberAv3ngers 是一個與伊朗相關、專注於攻擊關鍵基礎設施及營運技術的組織。IOCONTROL 能在多種以 Linux 為基礎的營運及連網裝置上運行，從攝影機、路由器到控制器及燃油管理系統皆可涵蓋，使其成為一套可重複使用的通用平台，而非單一用途的工具。同一時期，另有一波僅被歸因於疑似與伊朗相關行為者的全國性攻擊行動，入侵了美國多處燃油量測儀，其中包括在田納西州確認發生的攻擊事件。當地一家便利商店連鎖業者共有 15 座油槽受到影響，部分案例中油槽及感測器資料遭到刪除。暴露數量統計顯示，儘管多次示警，暴露於網際網路的量測儀數量多年來幾乎沒有變化，直到這些經確認的攻擊事件及相關媒體報導出現後才急遽下降。除了網路暴露問題外，多款廣泛使用的量測儀（例如 Dover 機型的 CVE-2024-45066，以及 Veeder-Root TLS4B 機型的 CVE-2025-58428）中存在的最高風險等級指令注入漏洞，也持續使軟體層面的風險維持在高檔。

租用攻擊工具及濫用受信任軟體

Earth Vetala（MuddyWater）將自製工具與租用及受信任軟體能力相結合，DinDoor 被評估為其後門程式之一。這個與伊朗相關的間諜組織多年來持續活躍於中東地區。2026 年上半年，該組織大量依賴向犯罪平台租用的能力，藉此降低成本並增加歸因難度。針對一台極可能由該組織操作、且暴露於網際網路的伺服器所進行的傾印資料分析，清楚顯示了這一點：在該組織以波斯語撰寫的自製工具旁，存在一款名為 ChainShell 的租用後門程式，是向一個俄語系犯罪平台以服務形式購入。

該組織同時也能迅速將新披露的漏洞武器化，在一項新披露的 Ivanti 漏洞（CVE-2026-1281）公開後數天內即展開掃描，並曾針對目標利用一項 FortiOS 漏洞（CVE-2024-55591）。這顯示緩慢的修補週期如今幾乎不留任何喘息空間。

另一款後門程式 DinDoor 則展現了濫用受信任軟體的手法：該程式在 Deno（一款合法且經簽署的程式設計執行環境）之上運行攻擊者的程式碼，由於防禦系統通常不會預期一款受信任的開發者工具具有惡意性質，此舉能降低遭懷疑的可能性。DinDoor 指向一項由多名客戶共用的服務，其他研究人員也曾將同一套基礎設施與一起勒索軟體行動建立關聯。根據共用的程式碼簽署憑證及中東地區受害者輪廓，該工具被以中等信心程度評估為 Earth Vetala 的工具之一，惟需留意憑證存在

遭竊取或重複使用的可能性。當同一套工具同時服務於間諜活動及勒索軟體集團時，單憑惡意程式本身，已不足以判斷防禦方所面對的究竟是哪一方。

將 C2 隱藏於區塊鏈之上

Earth Vetala 透過公開區塊鏈解析其 C2 位址，使其難以遭到封鎖或下架。其租用的 ChainShell 後門程式並未帶有固定位址，而是透過讀取公開區塊鏈上的資訊來判斷回報位置。這類查詢行為能融入一般區塊鏈活動之中，因此難以被封鎖。此外，一旦位址公開發布，相較於傳統寫死於程式碼中的網域名稱或 IP 位址，該位址更難以被移除，且操作者無需重建惡意程式即可變更該位址。

此惡意程式還會檢查系統地區設定，並避免在設定為多種後蘇聯獨立國協（CIS）語言的機器上運行，這是俄語系犯罪工具中常見的手法。由於這項具韌性的技巧如今已內建於多個行為者皆可購得的工具之中，其出現本身，已無法透露太多關於入侵行動背後主使者的資訊，這也促使偵測工作的重心，須從網路目的地轉向端點行為分析。

ADINT：無需惡意程式即可實現大規模監控

在另一起未經歸因的行動中，廣告情報（ADINT）技術透過濫用線上廣告生態系統，在大多不需部署任何惡意程式的情況下，追蹤並去匿名化目標對象。每當手機顯示一則廣告時，該裝置及其位置的相關細節，便會被廣播給競標該廣告版位的各家公司。任何以競標方身分註冊的一方，皆可在完全不購買廣告、也不觸碰目標裝置或網路的情況下，蒐集這些資訊。透過廣告投遞惡意程式的情況雖確實存在，但僅屬高度針對性的次要手法。其監控價值主要來自競價流（bidstream）資料本身，而標準資安工具無法標記出這類在技術上完全合法的廣告交易行為。

TrendAI™ 進行了一項長達數月的調查，發現有兩個操作者從事此類行為。其一是一家美國公司，同時經營廣告業務與位置情報業務。另一個則與商用間諜軟體業界有所關聯，在超過一年的時間內，於 155 個以上的國家追蹤了超過 184,000 人。其追蹤焦點曾在西班牙一場地區選舉及荷姆茲海峽危機發生後數小時內隨即轉移，此舉讀來更像是情報蒐集行為，而非廣告投放行為。此風險並非僅止於假設：2026 年 5 月，美國中央司令部（U.S. Central Command）曾報告指出，對手曾利用商業可得的位置資料，鎖定執行任務中的美軍人員，包括在荷姆茲海峽區域的人員。由於此類行為發生於合法的廣告系統之內，並無惡意程式可供偵測，其風險暴露源自於一般應用程式所外洩的資料。實務上可行的防禦措施，在於強化治理機制，並從源頭限制員工手機所允許外洩的裝置及位置識別資訊種類。

結論

這些攻擊行動集中發生於防禦方早已知曉的幾個關鍵領域：受信任的服務、軟體供應鏈，以及未修補的網際網路暴露軟體，如今更加入了 AI 這項變數。重點並非追逐單一的新興工具，而是持續將偵測與管控能力，推向這些關鍵領域。以下依大致優先順序列出建議：

將偵測重心轉向身分識別、雲端與端點行為。

由於 C2 架構經常隱藏於主要雲端平台、開發人員通道、區塊鏈及貼文網站之中，僅僅封鎖已知的惡意伺服器並不足夠。應留意異常的雲端及身分識別活動，強制實施能抵禦網路釣魚的多因子驗證，並著重追查處理程序在主機上的實際行為，而非僅關注其連線對象。負責單位：資安維運（SecOps）及身分識別團隊。

將軟體供應鏈及開發人員本身，視為攻擊面的一部分。

如同 npm 套件遭入侵事件所顯示，單一遭下毒的相依套件或維護者帳號，即可一次觸及大量受害者。應對相依套件進行釘選及驗證，針對安裝時期執行的指令碼啟用警示機制，並讓維護者及開發人員帳號享有與正式環境系統同等的保護層級。負責單位：治理團隊及資安維運。

縮短邊緣及非受管軟體的修補與暴露時間窗。

攻擊者不僅將零日漏洞武器化，也持續利用長期已知的漏洞，而不會自動更新的工具，更讓舊有漏洞得以長期存續。應優先處理暴露於網際網路的系統，追蹤修補速度較慢的軟體（例如壓縮工具及管理設備），並假設具備高度能力的行為者可能早在修補程式發布前，便已掌握該漏洞的攻擊方式。負責單位：風險管理團隊。

將營運技術及關鍵基礎設施裝置從公開網際網路上下線。

本次半年期間，暴露於網際網路的油槽量測儀及序列埠轉 IP 轉換器均遭到直接攻擊。應將這些裝置從公開可及的範圍中移除，對控制網路進行區隔並加以監控，並修補燃油系統中最高風險等級的漏洞。暴露數量僅在確認發生攻擊事件並經媒體報導後才出現下降，此模式並不應作為可依賴的防禦策略。負責單位：風險管理團隊及資安維運。

為 AI 加速的對手預作準備，包括環境中已存在的 AI 工具。

應預期漏洞攻擊及誘餌內容的產出速度將加快，也將更早出現 AI 代理程式的運用。同時也應留意，行為者可能將環境中已存在的 AI 工具（例如程式碼協作助理及代理程式框架）轉化為在主機上採取行動的手段。應預期同一套工具將同時服務於間諜活動與犯罪行為，因此在判斷入侵行動背後的主使者時，應綜合權衡行為模式與意圖，而非僅依賴單一指標。負責單位：資安維運及治理團隊。

參考資料

以下參考資料清單為原始文獻之引用出處，為利讀者查證來源，保留原文（英文）呈現：

1. National Energy Administration of China. (June 25, 2026). "National Energy Administration Releases National Electricity Statistics for January–May 2026."

2. National Energy Administration of China. (June 30, 2026). "National Energy Administration Releases May 2026 Data on National Renewable Energy Green Power Certificate Issuance and Trading."

3. Che Pan, Eduardo Baptista, and Casey Hall. (May 25, 2026). Reuters. "Huawei Proposes New Path for Chip Development Amid US Sanctions."

4. Chang Siying. (May 16, 2026). BBC News 中文. "Trump's Visit to China Concludes."

5. Ministry of Foreign Affairs of the People's Republic of China. (May 21, 2026). Joint Statement Between the PRC and the Russian Federation.

6. Steven Jiang. (May 7, 2026). CNN. "China Gives Suspended Death Sentences to Two Former Defense Ministers."

7. U.S. Department of Defense. (June 8, 2026). "Entities Identified as Chinese Military Companies."

8. Ministry of Commerce of the People's Republic of China. (June 22, 2026). MOFCOM Announcement No. 23 of 2026.

9. Wordfence. (April 7, 2026). NVD, NIST. "CVE-2026-0740 Detail."

10. KCNA. (Feb. 26, 2026). Report on Ninth Congress of Workers' Party of Korea.

11. Jack Kim and Joyce Lee. (May 27, 2026). Reuters. "North Korea Tests Mix of Enhanced Ballistic, Cruise Missiles and Artillery Rockets."

12. Vann H. Van Diepen. (April 2, 2026). 38 North. "A New Rocket Motor Further Muddles North Korea's Solid-Propellant ICBM Outlook."

13. Chung Yeong-gyo and Michael Lee. (May 6, 2026). Korea JoongAng Daily.

14. The Associated Press. (June 4, 2026). NPR. "North Korea Unveils a New Plant to Produce Fuel for Nuclear Weapons."

15. Kim Tong-Hyung. (June 24, 2026). Military.com.

16. Park Hee-soo. (June 26, 2026). Daily NK.

17. NK News. (May 19, 2026). The Korea Times.

18. NK News. (April 8, 2026). The Korea Times.

19. Bank of Korea. (Aug. 29, 2025). GDP Estimates for North Korea in 2024.

20. Kim Young-Hoon. (June 19, 2026). Korea Development Institute (KDI).

21. Feike Hacquebord and Stephen Hilt. (April 23, 2025). Trend Micro. "Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations."

22. Peter Girnus and Jacob Santos. (March 31, 2026). Trend Micro. "Axios NPM Package Compromised."

23. Lucas Silva. (April 21, 2026). Trend Micro. "Void Dokkaebi Uses Fake Job Interview Lure."

24. TRM Team. (April 2, 2026). TRM Labs. "North Korean Hackers Attack Drift Protocol."

25. Chainalysis Team. (April 23, 2026). "Inside the KelpDAO Bridge Exploit."

26. U.S. Department of the Treasury. (March 12, 2026). "Treasury Sanctions Facilitators of DPRK IT Worker Fraud."

27. U.S. Attorney's Office, District of Columbia. (Feb. 19, 2026). DOJ.

28. U.S. DOJ, Office of Public Affairs. (April 15, 2026).

29. U.S. DOJ, Office of Public Affairs. (May 6, 2026).

30. President of Russia. (Feb. 26, 2026). Presidential Commission on AI.

31. Skye Lucas. (Feb. 23, 2026). FRONTLINE, PBS.

32. The Associated Press. (July 1, 2026). U.S. News & World Report.

33. CNN. (Feb. 5, 2026).

34. Bloomberg News. (March 24, 2026).

35. Human Rights Watch. (March 31, 2026).

36. Bloomberg News. (March 4, 2026).

37. Bloomberg News. (Jan. 15, 2026).

38. Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). Trend Micro. “Pawn Storm Campaign Deploys PRISMEX.”

39. Microsoft Corporation. (Jan. 26, 2026). “CVE-2026-21509 Detail.”

40. Feike Hacquebord and Hiroyuki Kakara. (June 8, 2026). Trend Micro. “Old WinRAR Flaw Fuels Attacks on Ukraine.”

41. Anton Cherepanov, Peter Košinár, and Peter Strýček. (Aug. 8, 2025). “CVE-2025-8088 Detail.”

42. Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). Trend Micro.

43. CERT-UA. (Jan. 14, 2026). “PLUGGYAPE Backdoor Deployed Against Ukrainian Defense Forces.”

44. HarfangLab Cyber Threat Research Team. (May 13, 2026).

45. ESET Research. (n.d.). “APT Activity Report: Russia-Aligned APTs.”

46. ClearSky Research Team. (March 3, 2026). “Exposing a Russian Campaign Targeting Ukraine.”

47. Microsoft Threat Intelligence. (May 14, 2026). “Kazuar: Anatomy of a Nation-State Botnet.”

48. Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). Trend Micro.

49. Kyle Wilhoit and Stephen Hilt. (2015). TrendLabs. “The GasPot Experiment.”

50. Team82. (Dec. 10, 2024). Claroty. “Inside a New OT/IoT Cyberweapon: IOCONTROL.”

51. CISA, FBI, NSA, DOE, EPA, TSA, DOT, and USDA. (June 2, 2026). “CISA and Partners Urge Hardening Automatic Tank Gauge Systems.”

52. Sean Lyngaas. (May 15, 2026). CNN. “Exclusive: Hackers Have Breached Tank Readers at US Gas Stations.”

53. ICS-CERT. (Sept. 24, 2024). “CVE-2024-45066 Detail.”

54. CISA. (Oct. 23, 2025). “CVE-2025-58428 Detail.”

55. Sean Moran. (April 7, 2026). JUMPSEC. “ChainShell: MuddyWater’s Russian MaaS Link.”

56. Ivanti. (Jan. 29, 2026). “CVE-2026-1281 Detail.”

57. Fortinet, Inc. (Jan. 14, 2025). “CVE-2024-55591 Detail.”

58. Joseph Keyes and Daxton Wirth. (March 17, 2026). ReliaQuest.

59. Check Point Research. (March 10, 2026). “Iranian MOIS Actors & the Cyber Crime Connection.”

60. Ctrl-Alt-Intel. (March 4, 2026). “MuddyWater Exposed: Inside an Iranian APT Operation.”

61. Lisandro Ubiedo. (Nov. 20, 2025). Securelist (Kaspersky).

62. Brian Krebs. (Oct. 23, 2024). Krebs on Security. “The Global Surveillance Free-for-All in Mobile Ad Data.”

63. Raphael Satter. (May 28, 2026). Reuters. “Exclusive: Pentagon Says US Military Personnel Are Reportedly Being Targeted Using Location Data.”

想獲取更多類似的深度洞察？

TrendAI | 資源與洞察（Resources and Insights）

TrendAI™ 是全球 AI 資安領導品牌，也是趨勢科技（Trend Micro）旗下的企業事業群，致力於為組織提供全方位的 AI 能見度及整合式資安防護，藉此建立信心、驅動創新並消弭風險。

TrendAI™ 深受全球 185 個國家中規模最大的企業及政府機構信賴，能全面守護企業的身分識別、基礎設施及數據資產安全。

AI Fearlessly.

了解更多：trendaisecurity.com