



2025資安威脅趨勢分析與因應策略



Peter Fan – PaloAlto Networks 技術總監

演講大綱

1

2025資安趨勢分析及因應策略

2

AI驅動下應有的資安防禦準備

3

Q & A

重塑威脅格局的 5 大新興趨勢

1

威脅行為者正在通過旨在故意破壞營運的攻擊來增強傳統的勒索軟體和勒索行為。

2

軟體供應鏈和雲端攻擊的頻率和複雜性都在增長。

3

入侵速度的提高 — 自動化和簡化的駭客工具包放大了入侵速度 — 在近20%的案例中，數據洩露發生在入侵後的第1個小時內。

4

組織面臨內部威脅的風險更高，因為北韓等民族國家以竊取資訊和資助國家計劃為目標。

5

對人工智慧輔助攻擊的早期觀察表明，人工智慧如何放大入侵的規模和速度。

86%

對業務產生影響的攻擊
攻擊者越來越創新。



攻擊發生得更快



GenAI 允許攻擊者擴展



攻擊者利用深厚的雲專業
知識

重新定義威脅 5 大攻擊趨勢

1. 駭客正在通過目的在故意破壞或影響營運的攻擊來增強傳統的勒索軟體和勒索行為。
2. 軟體供應鏈和雲端攻擊頻率和複雜性都在增長。
3. 入侵速度的提高 — 自動化和簡化的駭客工具包加快了入侵速度 — 在近期**20%**的案例中，數據洩露發生在入侵後的第**1**個小時內。
4. 組織面臨內部威脅的風險更高，因為北韓等共產國家以竊取資訊和資助國家計劃為目標。
5. 對人工智慧輔助攻擊的早期觀察發現，人工智慧如何擴大入侵的規模和速度。

攻擊技術 不斷演進發展



70%

針對 3 個或更多攻擊面的事件

- 在一些事件中，威脅行為者在多達 8 條戰線進行攻擊。

防禦者應準備訪問和有效處理資訊
來自整個組織的這些不同來源。

攻擊的常見8個方式

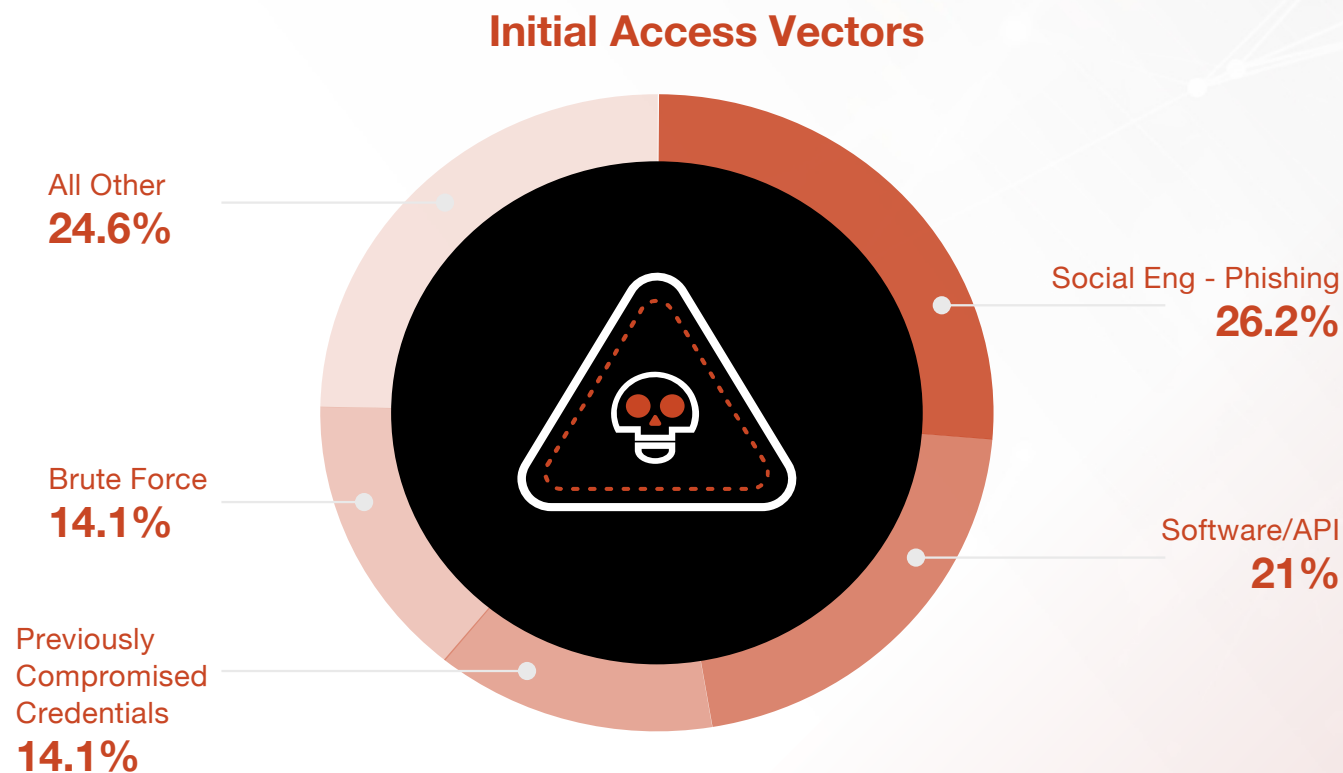
- 1 電子郵件攻擊 (**Email Phishing**) 發送精心設計的釣魚郵件，誘騙使用者點擊惡意連結或下載附件。
- 2 網頁釣魚與水坑攻擊 (**Web / Watering Hole**) 建立仿冒網站或入侵常訪網站，進行惡意腳本植入。
- 3 身分與帳號竊取 (**Credential Harvesting**) 利用網釣或攻擊獲取使用者登入憑證，包括MFA繞過。
- 4 遠端漏洞與暴力破解 (**VPN / RDP / Zero-Day**) 利用未修補的遠端接入設備或服務弱密碼進行入侵。

攻擊的常見8個方式

- 5 雲端與SaaS環境滲透 (**Cloud/SaaS Access**) 入侵 AWS、Azure、Google Workspace、Box、Salesforce 等服務。
- 6 橫向移動與權限擴張 (**Lateral Movement / Privilege Escalation**) 使用合法工具 (如PsExec、RDP) 在內部網路中快速擴散。
- 7 數據壓縮與竊取 (**Data Collection & Exfiltration**) 壓縮或分批竊取內部文件、資料庫、開發文件等資產。
- 8 勒索與營運破壞 (**Ransomware & Sabotage**) 加密資料並刪除備份，或刻意癱瘓服務造成停機與壓力。

攻擊技術 不斷演進發展

威脅行為者經常在多個方面攻擊組織。



瀏覽器 是威脅的 關鍵管道



44%

通過網路瀏覽器利用人為因素的事件

- 策略包括網路釣魚攻擊、惡意重定向和惡意軟體下載。

組織必須提高瀏覽器級別的可見性和控制，以便在這些威脅傳播之前檢測、阻止和回應它們。

瀏覽器是威脅的關鍵管道

1. 使用者與網路的主要接觸點

幾乎所有日常活動：登入雲端、下載文件、收發信件、觀看內部系統——都經由瀏覽器進行。

2. 攻擊者最常利用的通道

駭客利用瀏覽器進行釣魚攻擊（Phishing）、惡意網站載入、零日漏洞攻擊（Zero-Day Exploits）、Session 劫持、瀏覽器外掛入侵等。

3. 攻擊與防禦的「第一接觸點」

瀏覽器在用戶端與網頁內容之間做中介，是最容易控制與檢測的安全節點之一。

瀏覽器是威脅的關鍵管道

網路瀏覽器 (Web Browser) 是企業與個人存取網際網路的主要入口之一，也是駭客最常攻擊的向量之一。它的重要性往往被低估，但實際上，**瀏覽器就是使用者與惡意網站之間的第一道防線。**

威脅類型	說明
惡意網站 / 釣魚網站	利用域名相似、仿真畫面騙取帳號密碼
零日漏洞攻擊 (Browser 0-day)	利用未修補的漏洞直接取得電腦控制權
不安全插件 / 外掛	插件被植入惡意碼，如竊取密碼、擴充追蹤
會話劫持 (Session Hijacking)	攻擊者偷取 Cookie 或 Token，冒用登入狀態
Drive-by Download	使用者無感點擊後自動下載惡意檔案

瀏覽器是威脅的關鍵管道

因此導入企業級瀏覽器(Enterprise Browser)，不僅針對內部員工也可增加對供應商的存取管控。

功能類別	功能說明
安全控制	可限制：下載、上傳、列印、剪貼簿、外掛使用、儲存帳密
零信任瀏覽	強制資安驗證：使用者、裝置、風險態勢都需符合政策才可瀏覽
雲端隔離	敏感網站透過雲端渲染方式呈現，不與本機資料接觸
整合DLP與CASB	監控使用者存取雲端應用（如Box、Google Drive）行為
原生審計與可視性	所有瀏覽與資料行為可記錄並整合至 SIEM/SOC
身份驗證整合	支援 SSO、MFA、端點風險評估、裝置驗證

攻擊發生的速度比組織的回應速度還要快

攻擊正在發生
250%
過去4年更快



在 20% 的事件中，
資料外洩發生在
1 hour

攻擊者 行動速度 越來越快



25%

在案件中，從入侵到滲透的
時間不到 5 個小時。

- 過去 4 年增長 3 倍。
- 20% 的案例少於 1 小時。
- 45% 的案例數據洩露到雲端儲存。

通過集成即時可見性、人工智慧洞察和自動化工作流程，您甚至可以超越行動最快的對手。

攻擊速度愈來愈快的方法

駭客攻擊的速度與自動化程度不斷提升，許多攻擊在1小時內就完成滲透與資料外洩，大幅縮短傳統SOC或防禦系統的反應時間。

加速方式	說明
自動化漏洞掃描與利用	使用工具如 Cobalt Strike、Metasploit 自動探測與攻擊
GenAI生成惡意內容	快速產出多語言釣魚信、假網站、勒索信模板
弱密碼暴力破解自動化	使用botnet對VPN/RDP/雲端服務進行帳密爆破，短時間內試數千筆
自動化橫向移動腳本	一旦取得權限，內部跳板攻擊幾秒內完成
內部跳板 + 駭客即服務（HaaS）	僱用駭客提供內部資料、工具或零日攻擊程式，提高效率
Living-off-the-land 技術	使用合法工具如PowerShell或PsExec隱身作業系統內部，減少偵測跡象

提早偵測、提早阻斷

層級	對策建議
Email/Web 前線	針對釣魚與網頁下載導入 AI 檢測與URL沙箱
雲端與帳號防護	全面啟用MFA，設定API金鑰有效期、最小權限
端點與伺服器	導入EDR/XDR、設定行為型封鎖（如異常PowerShell執行）
SOC	使用 AI-SOC 與自動封鎖反應（SOAR）縮短響應時間
備援	建立 immutable backup（不可改寫備份）以防止同時被刪除或加密

DLP防護策略

DLP 控管層級

✓ 郵件 DLP

- 限制含機敏關鍵字、附件或外部收件人傳送行為
- 建立加密郵件與手動核可流程

說明

避免資料透過釣魚信或遭內部員工外傳

✓ 雲端 DLP (CASB)

- 檢測雲端儲存 (如 Google Drive 、 OneDrive) 中的敏感資料傳送行為
- 阻擋未授權第三方共享

管控資料流向、API 上傳、快照分享等

✓ 端點 DLP

- 禁止 USB 儲存、截圖、複製機敏內容
- 偵測輸出到PDF、列印等異常行為

防止內部人員或駭客於橫向擴張時竊走資料

✓ Data Classification

- 建立資料等級分類機制：機密／內部／公開
- DLP 根據分類自動套用保護策略

提高控管精準度，減少誤報與遺漏

✓ 偵測導出模式 (行為面)

- 檢查一次大量複製、上傳、壓縮等動作

利用 UEBA 分析可疑使用者資料操作模式

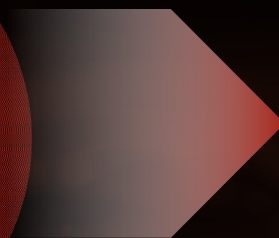
GenAI 正在不斷發展攻擊方法，並將效率提升到新的水準



攻擊生成
開發資源和基礎設施



攻擊加速
提高速度和規模



攻擊效率增
加成功的可能性

攻擊者
行動速度
越來越快



100X 使用 AI 加速攻擊速度

- 人工智慧正在加速從自動網路釣魚到勒索軟體的網路攻擊的每個階段
- 在 Unit 42 的模擬攻擊中，人工智慧將滲透的中位時間從 2 天縮短到僅 25 分鐘

防禦者必須考慮部署 AI 驅動的檢測來發現惡意以機器速度模式，關聯來自多個來源的數據。

AI加速網路攻擊的方式

生成式AI與機器學習模型正被駭客廣泛應用於各階段攻擊流程中，使攻擊**更快、更準、更難防**。

階段	AI 加速方式	說明
 偵察階段 (Recon)	自動搜尋公司、人員、開源弱點	AI工具可自動搜尋OSINT、社群平台資訊，產出針對性目標清單
 社交工程	撰寫自然語言的詐騙信、假訊息	使用 LLM 產出擬真釣魚信、假客服、假語音
 惡意程式開發	自動生成、混淆或加密惡意碼	利用GenAI避開EDR偵測，生成0-day攻擊模組架構
 弱點利用(Exploitation)	快速掃描匹配新漏洞組合	利用模型分析目標環境自動選擇最佳漏洞組合與Exploit套件
 內部橫移	模擬系統行為繞過偵測	AI模擬合法行為 (Living-off-the-land)，降低被SIEM或SOC識破機率

AI網路釣魚威脅

1. APT-C-36：AI撰寫釣魚郵件（2024）

使用 LLM（如 ChatGPT）自動翻譯與生成釣魚郵件內容，結合真實新聞與人名，投遞給目標公司高階主管，點擊率明顯提升。

2. WormGPT 被用於非法市場

黑市上販售的「WormGPT」為未加防護的 GPT 模型，專門用來生成詐騙與勒索信，有駭客利用它創造多語言版本釣魚信，成功騙取公司付款資訊。

3. AI協助生成零日攻擊流程

在「研究攻擊模擬環境」中，有研究者用LLM讓AI構建完整惡意DLL注入流程，包括程式碼、隱藏技巧與反監控方法，時間從2天縮短為25分鐘。

4. AI Voice Deepfake 詐騙

攻擊者利用AI語音技術複製CFO聲音，致電財務部門要求緊急轉帳。企業損失25萬美元。

攻擊技術在 不斷發展



23%

的攻擊始於網路釣魚，因為
GenAI 使活動更難被檢測。

- 與去年相比，漏洞是首要因素。
- 駭客透過自動化工具與技術，快速開發惡意程式，還能讓這些惡意程式自動在攻擊鏈各階段執行下一步操作，例如自動擴散、竊取資料、關閉防毒等，大幅提升攻擊效率與成功率。

安全培訓是幫助員工做好抵禦社會工程攻擊準備的必要條件。培訓應該超越網路釣魚和魚叉式網路釣魚。

AI網路釣魚威脅

駭客運用生成式AI（如 ChatGPT、Claude）快速大量產出高擬真的釣魚郵件、詐騙訊息與假網站內容，避開傳統偵測機制。

攻擊手法	說明
自動撰寫釣魚信（ Email/Message ）	透過AI生成語法正確、語氣自然的詐騙郵件（可模擬老闆/供應商語氣）
多語言釣魚	AI能自動翻譯信件成受害者母語，擴大攻擊範圍
假客服/語音聊天機器人	利用AI語音生成偽裝客服、HR、銀行人員進行詐騙
假網站/假入口頁面生成	AI生成逼真釣魚網站HTML與CSS，幾乎與真頁面無異
結合惡意碼（ Malware-as-a-Service ）	有些攻擊者會讓AI幫忙包裝載入器、隱藏後門連線指令等

AI網路釣魚威脅

1. 2024年某歐洲銀行「CEO詐騙信」
攻擊者使用GenAI模仿CEO語氣，發送緊急請款指令給財務部門。
信件語氣自然、無拼字錯誤，甚至內含真實近期客戶名稱。
2. 針對台灣製造業的WhatsApp詐騙
使用AI生成語音或圖片，假冒供應鏈廠商要求更改付款帳戶。
3. 多語言釣魚攻擊 (Unit 42 觀察)
柬埔寨、越南、印尼、台灣等地區遭同一駭客組織以不同語系釣魚手法攻擊。

AI網路釣魚威脅

技術面：

Email 安全閘道 (SEG) 啟用自然語意模型偵測：升級傳統關鍵字偵測至 NLP 分析可疑語氣

啟用 SPF / DKIM / DMARC 完整防止寄件人偽造

SPF (Sender Policy Framework)：誰可以發此email

DKIM (DomainKeys Identified Mail)：此email 沒被竄改

DMARC (Domain-based Message Authentication, Reporting, and Conformance)：驗證失敗的處理

導入 UEBA / AI 偵測異常點擊或登入行為

Zero Trust 架構限制釣魚後的 lateral movement (橫向擴散)

使用者教育面：

模擬釣魚演練 + 回報流程教育 (Tabletop / Phishing Simulation)

設立信件回報機制 (Report Suspicious Mail)

建立「不透過Email要求更改匯款資料」政策

雲端服務攻擊正在以驚人的速度、精度和規模發生



Cloud Expertise

Scanning for IAM keys in cloud environment files

Calls to specific cloud APIs

Cloud IAM roles and policies **manipulated**

Cloud instances and infrastructure **created**

Cloud-specific tools **used**

Cloud storage objects **deleted**



Speed of Attack

Some Actions Automated to

< 1 Minute



Scale

Targeted
110K
Domains

Gathered
90K
Env Variables

Across
7K
Cloud Services



攻擊者利用 複雜性、可 見性差距和 過度信任



29%

源自雲端環境的案例

- 21% 的訂單因配置錯誤、憑據被盜和 API 暴露而導致直接營運損失。
- 攻擊者使用已被入侵的雲端資源來滲透或暴力破解其他不相關的目標。

透過持續應用安全管控措施，團隊可及早發現攻擊，限制其影響，並確信雲端資源和軟體管道仍處於控制之下。

雲端服務資安威脅

威脅類型	說明
錯誤設定 (Misconfigurations)	最常見問題之一，例如：S3 bucket未設權限、API未驗證、VM對外暴露
憑證/金鑰洩露	API key、access token、IAM key 被硬編碼或誤上傳至GitHub
身份濫用 (IAM Overprivilege)	權限過大的帳號被駭客利用進行橫向移動與權限提升
雲端資源遭劫持	像是用於密挖 (cryptomining)、中繼C2伺服器等
資料外洩與快照竊取	利用已連結之儲存快照擷取原始資料或備份
供應鏈攻擊	透過第三方SaaS整合、DevOps工具間接入侵

雲端服務資安威脅

1. Snowflake 客戶帳號憑證外洩事件 (2024年中)

- 攻擊者利用無MFA帳號與舊憑證，滲透超過 150 家 Snowflake 客戶。
- 資料包含行銷、電商、金融、醫療等業者之敏感資料。
- 關鍵問題：MFA未啟用 + 憑證重用 + API金鑰存留太久

2. 230M 目標掃描案 (Unit 42 報告)

- 攻擊者嵌入雲端環境後掃描全球超過 2.3 億個目標，尋找API金鑰、開放資源與社群帳號。共挖出 90,000 筆機密變數，其中包含：7,000 筆與 AWS、GCP、Azure 有關；1,500 筆屬於企業社群平台帳號。

3. Muddled Libra 雲端跳板攻擊

- 攻擊者取得某企業 AWS IAM admin 權限後，利用Lambda功能跳板攻擊下游服務。
- 結合“Living off the Land”策略，難以從日誌判斷攻擊異常行為。

Muddled Libra Attack: 從 Helpdesk 到 Domain Admin 在40分鐘內



Muddled Libra Attack 是 Unit 42 在 2023 年命名的一項針對雲端基礎架構的高效率滲透行動，背後攻擊者集團被認為是與金融與勒索攻擊有關的專業威脅行為者（APT）。他們擅長透過合法管道潛入環境，善用 DevOps 工具與「Living-off-the-Land」手法進行隱匿操作。

攻擊者利用 複雜性、可 見性差距和 過度信任



75%

事件在日誌中有證據，但孤島(Silos)阻止了檢測。

- 46% 的人需要將來自 4+ 不同來源的相關數據關聯，以確定根本原因。
- 複雜、脫節的系統，資訊不易訪問或有效作。
- 允許攻擊者在未被發現的情況下利用間隙。

防禦者應該尋求人工智慧驅動的自動化，將響應時間從幾小時縮短到幾分鐘。自動分析安全日誌，以更快地發現高優先順序威脅。

資安孤島-Silos

部門、系統或工具之間資訊無法互通，形成各自獨立、封閉的狀態。

- **工具孤島 (tool silos)**

每個資安工具都有自己的儀表板、日誌格式，彼此無法整合，導致事件難以統一追蹤。

- **資料孤島 (data silos)**

不同系統產生的資料存放在分離的平台上，**SOC**無法取得完整視角，造成可視性缺口。

- **部門孤島 (organizational silos)**

資安、IT、開發等團隊之間缺乏協作或資訊共享，事件回應延遲，甚至錯失攻擊跡象。

解決Silos問題：

- 提升 事件偵測效率
- 加快 攻擊關聯分析
- 降低 誤判與漏判率
- 實現 整體性可視化與自動化防禦

常見解法：

- 建立 統一日誌格式與集中存取機制
- 導入 **SIEM / SOAR** 平台 整合多來源資料
- 推動 跨部門資安聯防合作機制

內部風險 (Insider) 的問題不斷上升



Privileged Access Abuse

- IP Theft
- Data Exfil
- Sabotage
- Espionage
- Shadow IT
- Exposures



Nation-State Involvement

3X increase in nation-state influenced insider threats*



Devastating Impact

\$4.99M Average cost per insider threat incident**

* 2025 Unit 42 Global Incident Response Report
** IBM Cost of a Data Breach 2024 Report

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

攻擊技術在 不斷發展



內部威脅的崛起 北韓的內部威脅行動浪潮

- 利用由詳細技術組合支援的被盜或合成身份的傳統招聘流程。
- 使用基於合同的技術角色（如人力資源公司）的組織在不知不覺中成為促進者

防禦這種威脅需要改變組織處理工作力管理和安全的方式。

北韓駭客採用的策略

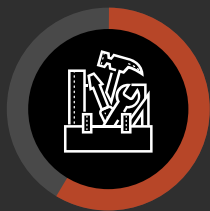
這類行動由北韓的國家級駭客組織（如：Lazarus Group）主導，目標是：

1.賺取外匯以支持政權 2.竊取技術與機密資料 3.建立日後攻擊據點

- 使用偽造或竄改過的履歷與身分證明
- 應徵遠端開發職位，取得企業電腦與存取權限
- 安裝 **KVM-over-IP**、**Remote Access** 工具以保留後門通道

- 收集敏感資料（原始碼、帳號、文件）並轉交給北韓政府
- 引薦其他「假工程師」，擴大滲透網絡
- 通過威脅發佈敏感信息來勒索僱主

這些促成因素有助於攻擊者成功



1.

Too much **complexity**

75% had evidence in logs

But silos and complexity prevented detection



2.

Not enough **visibility**

70%

happened on **three or more**
attack surfaces



3.

Too much **trust**

99% of cloud accounts

over permissioned

解決這些問題可以降低攻擊的可能性或影響。

2025-資安防禦對策

- **加速零信任的採用**：消除隱式信任，強制實施最低許可權訪問，並持續驗證用戶和設備。
- **增強雲端和身份安全**：實施 MFA、即時訪問和持續監控，以減少攻擊面。
- **內部威脅監控**：加強對 IT 承包商的審查，監控特權訪問，並關聯身份、網路和行為數據。
- **加強檢測和自動回應**：使用 AI 驅動的自動化將響應時間從幾小時縮短到幾分鐘。自動分析安全日誌，以更快地發現高優先順序威脅。
- **增強安全運營能力**：為您的SOC提供整個企業的全面可見性，以及識別雜訊中信號的技術。



Proactive Services



Managed Services



Incident Response

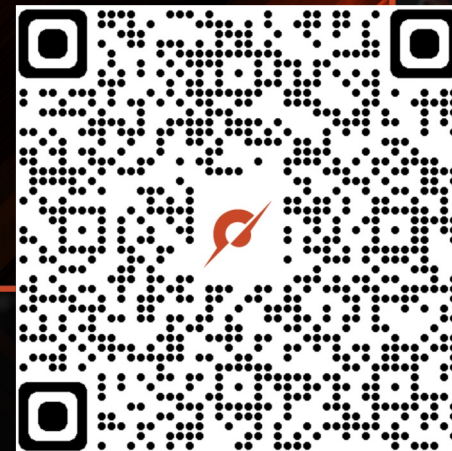


Leading Threat Intelligence

Global Incident Response Report 2025



THREAT VECTOR



Thank You

paloaltonetworks.com