jamf

Beacon by Jamf Threat Labs

macOS 專屬威脅搜捕服務

企業 Mac 的採用率持續成長，攻擊者對 Mac 的 關注 也與日俱增。Mac 專屬的**戰術、技術與程序**（TTP）、惡意軟體變種與傳播手法，正隨著 macOS 資安框架的演進而不斷演化。由於 macOS 資安框架具獨特性，組織在啟動、擴充、常態執行與衡量有效的 Mac 威脅搜捕計畫方面，往往面臨重重困難。

Beacon by Jamf Threat Labs 可解決上述難題。

Beacon 是一項以 Mac 為核心的威脅搜捕服務，由 Jamf Threat Labs 提供。該團隊由資安研究人員、分析師與工程師組成，他們發表 Mac 惡意軟體研究，並開發支撐 Jamf 平台運作的偵測引擎。

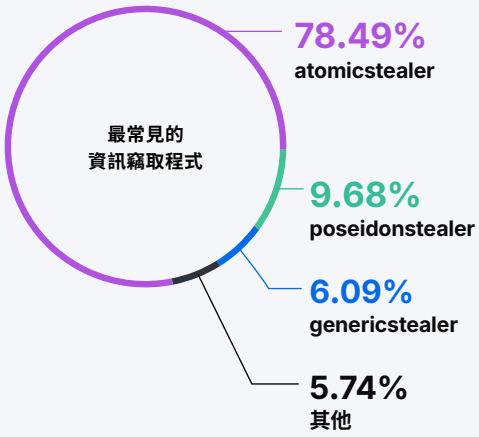
本服務旨在偵測、分析與回報傳統資安工具與團隊未能充分監控的 macOS 威脅。團隊具備完整 Apple 領域專業知識，能深入掌握攻擊者的 TTP、鎖定其試圖利用的漏洞，以及辨識 macOS 配置中的缺口。

☆ 核心優勢

- 以業界領先的 Mac 資安專業知識強化 Mac 威脅搜捕
- 透過逐步處置指引維持營運自主權
- 透過每月客製化報告，掌握新型威脅與 Mac 資安態勢

Beacon 偵測與**回報**的威脅範例：

- 包含木馬化套件的供應鏈攻擊
- 在 VSCode 或 Xcode 專案中執行的惡意程式碼
- ClickFix 社交工程攻擊
- 來自虛假徵才誘餌的北韓後門程式
- 以及其他更多威脅。



Threat Labs

2026 Mac Security 360

藉由 Jamf Threat Labs 專業能量，守護企業 Mac 環境

macOS 專業知識

專屬 Mac 威脅搜捕服務

- 研究人員深入瞭解 macOS 威脅環境、macOS 內部運作機制與攻擊者行為
- 以 Apple 端點資安 API 建構的 Jamf 遙測資料，提供更完整的 macOS 可視性
- 可直接聯繫 Jamf Threat Labs，諮詢 Apple 資安態勢相關問題

深度情資

大規模提供對應場景的 Apple 威脅情資

- 掃描遙測資料，偵測新型 Apple 專屬攻擊手法、入侵指標與隱藏惡意軟體
- 回溯搜捕搜尋長達一年的歷史遙測資料，找出過往未被辨識的威脅指標
- 使用 Jamf Threat Labs 自行撰寫的搜捕規則，提升對新型惡意軟體、可疑行為與 TTP 的偵測警示能力。**服務託管於 Jamf 雲端。**

營運自主權

自主掌控環境——Beacon 強化其資安

- 與 Jamf Threat Labs 協作，針對組織需求實施客製化的處置步驟
- 每月接收資安報告，重點呈現組織資安評分、已封鎖的 Mac 惡意軟體、新型威脅等資訊
- 全程保有完整自主權，同時享有專業團隊的技術指引

Beacon 運作方式：

1. **配置**

   Jamf 設定您的遙測資料配置，讓 Jamf Threat Labs 展開威脅搜捕作業。

2. **搜捕**

   Jamf Threat Labs 運用情資識別 macOS 攻擊、TTP 與入侵指標（IOC）。

3. **報告**

   Jamf Threat Labs 提供可據以行動的指引（工作流程、腳本），供即時威脅回應使用。每月 Jamf Threat Labs 會發送報告，詳細說明您的資安環境與態勢。

4. **威脅處置**

   由企業資安團隊主導隔離、修復與政策調整作業，Jamf Threat Labs 提供分析與專業建議做為處置依據。

Beacon by Jamf Threat Labs。
可量化、可常態執行的威脅搜捕，能隨著您的 Mac 裝置群一同擴展。

jamf

www.jamf.com/zh-tw/

如需更多資訊，請聯繫您指定的經銷商或 Jamf 業務代表。

或立即聯絡我們。