jamf

Beacon by Jamf Threat Labs

macOS向け脅威ハンティングサービス

企業でのMac導入の拡大に伴い、このデバイスへの攻撃が活発化しています。macOSセキュリティフレームワークの進化と足並みを揃えるように、Macに特化した**戦術・技術・手順**（TTP）やマルウェアの亜種、配布手法が開拓されています。しかし、macOSには固有の性質が存在するため、組織におけるMac向けの脅威ハンティングプログラムの策定、拡張、運用、評価は容易ではありません。

この課題を解決するのがBeacon by Jamf Threat Labsです。

BeaconはMac特化の脅威ハンティングサービスであり、セキュリティ研究者、アナリスト、エンジニアで編成されたJamf Threat Labsが運営を担当しています。同チームには、Macマルウェアの研究・公開およびJamfプラットフォーム用の検出エンジン開発などの実績があります。

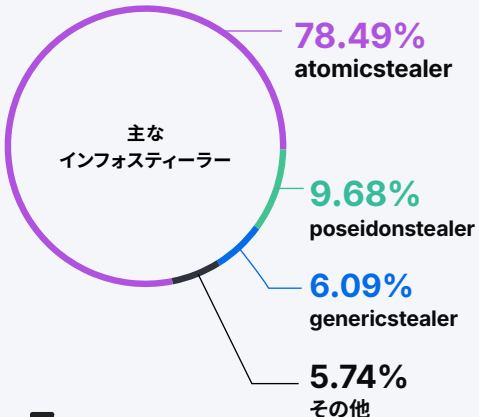
このサービスの目的は、従来のセキュリティツールやセキュリティ担当者の目が届かないmacOS狙いの脅威を検出、分析、報告することにあります。Jamf Threat Labsならではの Appleの専門知識を活かし、脅威アクターのTTP、狙われている脆弱性、macOS構成の欠陥の特定方法に関する知見を提供します。

☆ 主なメリット

- 業界最先端のMacセキュリティの知識で Macの脅威ハンティングを拡充
- 修復に関する詳しい助言を受けながら、お客様主体で環境を管理
- お客様ごとに合わせた月次レポートで脅威の動向やMacセキュリティの状態を把握

Beaconで検出・報告される脅威の例：

- トロイの木馬のパッケージが含まれるサプライチェーン攻撃
- VSCodeまたはXcodeのプロジェクトでの悪意のあるコードの実行
- ClickFixによるソーシャルエンジニアリング
- 北朝鮮による偽求人のバックドア
- 他多数



Threat Labs

2026年版Macセキュリティ360

MacセキュリティにJamf Threat Labsを活用するメリット

macOSの専門知識

Mac専門の脅威ハンティングサービス

- macOS狙いの脅威の動向、macOSの内部構造、攻撃者の行動を熟知した研究者が対応
- AppleのEndpoint Security APIをベースにしたJamf独自のテレメトリでmacOSを詳細に可視化
- Appleデバイスのセキュリティ状態についてJamf Threat Labsに直接質問可能

高度なインテリジェンス

状況に応じたAppleの脅威インテリジェンスを一括提供

- テレメトリ横断調査でApple狙いの新しい攻撃手法、侵害インジケータ（IOC）、潜伏中のマルウェアを検出
- レトロハンティングで最大1年前までのテレメトリを調査し、当時は知られていなかった脅威インジケータを検出
- Jamf Threat Labs作成のハンティングルールで検出アラートを拡充し、新規マルウェア、不審な挙動、TTPに対応（Jamf Cloudでホスト）

環境管理

環境の運用はお客様が担当し、Beaconはセキュリティ面をサポート

- Jamf Threat Labsの助言の下、お客様の組織要件に応じた修復手順を実施
- 月次セキュリティレポートで組織のセキュリティスコアやブロックしたMacマルウェア、新しい脅威などを確認
- 専門家の助言を受けながら、お客様主体で環境を管理

Beaconの仕組み：

1. 2. 3. 4.

構成

JamfがJamf Threat Labsの脅威ハンティング用にお客様のテレメトリを構成します。

ハンティング

Jamf Threat Labsがインテリジェンスを活用してmacOS狙いの攻撃、TTP、IOCを特定します。

レポート

Jamf Threat Labsが、脅威への対応に役立つ実用的なアドバイス（ワークフロー、スクリプト）を提供します。

毎月、Jamf Threat Labsがお客様のセキュリティ環境および状態に関するレポートを提供します。

対応

Jamf Threat Labsの分析および助言を利用して、お客様のセキュリティ部門が封じ込め、修復、ポリシーの変更などの対応を実施します。

Beacon by Jamf Threat Labs。
Mac運用環境にあわせて拡張でき、再現性に優れ効果を測定可能な脅威ハンティングサービス。

jamf

www.jamf.com/ja/

詳細については、お近くの販売代理店またはJamf担当者にお問い合わせいただくか、こちらからお問い合わせください。