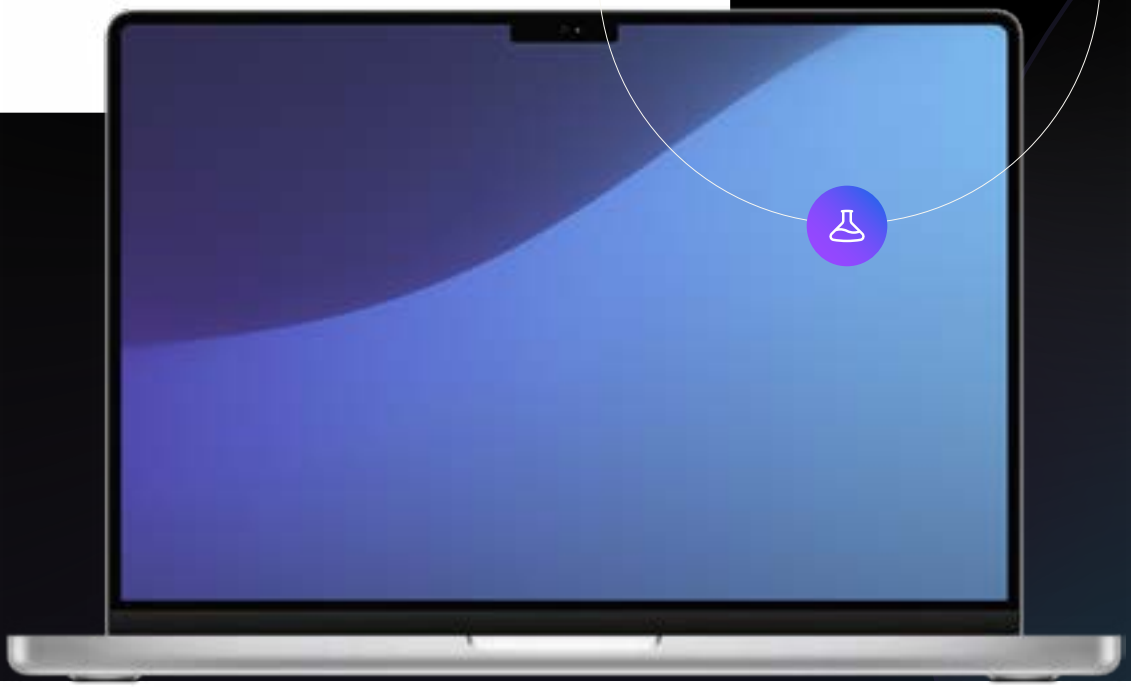
jamf

セキュリティ360：
最新トレンドレポート

Mac



目次

はじめに

Jamfセキュリティ360は、昨年実際に起きたお客様のインシデント、脅威の調査、業界の出来事を分析した結果を基に作成されるレポートです。本レポートでは、組織が直面しているリスクを明らかにするため、現在のMacを標的とした脅威の状況を調査しています。

本書では、攻撃者が被害をもたらす際に用いる、影響力の大きい様々な攻撃ベクトルを検証しました。Macデバイスの普及に伴い、攻撃者にとってMacは格好の標的となっており、デバイスへの侵入やデータ窃盗のために絶えず新たな手口が編み出されています。

さらに、攻撃者がMacを狙う新たな手法の分析結果に加え、Macデバイスの保護責任を負うセキュリティリーダーやIT担当者に向けたJamf CISOからの助言も提供します。

調査方法

本レポートで特定するセキュリティトレンドが現実社会に及ぼす影響を把握、定量化するために、15万台以上のMacで構成されるサンプルグループを匿名で調査しました。分析は2025年末に実施され、過去12ヶ月間のデータを対象としました。マルウェア調査では米国を拠点とするデバイスのみを対象としましたが、脆弱性調査では世界各国のデータを使用しました。

プライバシーを守り、データの収集・取り扱いに関する最高の基準を維持するため、調査で分析されたメタデータは個人情報や組織を特定する情報を含まない集約されたログから得られたものを使用しています。

主な調査結果

44%

悪意のあるネットワークトラフィックが検出された**デバイス**の割合

攻撃者は絶えずデバイスを侵害しようと狙っています。悪意のあるトラフィックを検出して封じ込めるには、継続的な取り組みと適切なツールが必要です。

41%

OSのバージョンが**古く危険な状態**にある**デバイス**

ソフトウェアの最小バージョン要件を徹底することで、デバイスに最新のセキュリティパッチが適用され、悪用可能な既知の脆弱性の数を減らすことができます。

50%

Macを攻撃する**マルウェア**に占める**トロイの木馬**の割合

今年の統計ではトロイの木馬が最も多く検出されたマルウェアとなり、2024年から33%以上増加しました。トロイの木馬はシステムへのバックドアとなり、長期的な被害や他の攻撃に対する脆弱性を残します。

73%

脆弱性のあるアプリがインストールされている**デバイス**の割合

リスクをもたらすソフトウェアはOSだけではありません。アプリにも脆弱なライブラリが含まれていたり、サプライチェーン侵害の被害を受けたり、データの取り扱いに問題があったりする可能性があります。組織全体でインストールされているものを把握することが、リスク管理において極めて重要です。

26%

少なくとも**1台のデバイス**が**クリプトジャッキングの影響を受けている組織**の割合

クリプトジャッキング攻撃は、デバイスの処理能力を悪用して暗号通貨をマイニングします。攻撃者が利益を得る間、デバイスのパフォーマンスや効率が低下します。

企業における主要なセキュリティトレンド

1. 攻撃対象として一般化したMacの現状

あらゆる規模・業種の組織が、これまで以上にMacを活用しています。2024年から2025年にかけてのMacの**市場シェアは16.4%の成長率**を見せ、約10%に達しました。これは他のどのベンダーよりも大きな伸びです。

2025年のMac出荷台数は270万台を超え、あらゆる場所でMacが活用されている現状を裏付けています。こうしたトレンドを攻撃者が見逃すはずはなく、今やMacは格好の標的となりました。堅牢なセキュリティ機能が備わっているものの、『Macはマルウェアに感染しない』という時代はとうに過ぎ去っています。

企業における存在感が高まるにつれ、攻撃者はMacに特化した脅威を次々と生み出し、データを盗むための手法を高度化させているのが現状です。

2. インフォスティーラーの進化とデータ被害の深刻化

インフォスティーラーは、いま最も広く拡散されているマルウェアの一つです。マルウェアの開発者は、大規模にデータを収集するための効果的かつ巧妙な手口の構築に余念がありません。インフォスティーラーは、ユーザが異変に気づく前に、認証情報、セッショントークン、ファイルなど、入手可能なあらゆるデータを素早く収集する傾向があります。

多くの場合、情報窃盗は大規模な攻撃を仕掛けるための『足がかり』となります。盗み出したデータを身代金目的で人質にしたり、他のアカウントやシステムに侵入するために悪用したりします。こうした特徴から、インフォスティーラーは攻撃者にとって人気のツールになっており、多くのマルウェア作成者がサービスとして提供しています。最新のインフォスティーラーは、バックドアを作って持続性を確保することで、再起動やログアウトの後も生き残り、攻撃者がC2サーバからコマンドを送信できるようにする場合もあります。

3. macOSを執拗に狙うAPT（持続的標的型攻撃）グループの脅威

Macの脅威状況を調査すると、既知の攻撃グループが暗躍している実態を目にすることになります。北朝鮮（DPRK）関連の脅威に似た高度な脅威は、Contagious Interview、FlexibleFerret、Odyssey infostealerの進化版といった攻撃キャンペーンやマルウェアでmacOSを標的にし続けています。

バックドアやその他の持続化手法の開発も続けられています。Jamf Threat Labsは、ChillyHellのようなマルウェアでこれを確認しました。

本レポートの後半にて、Jamf Threat Labsによる調査内容の詳細をご確認いただけます。

Macを狙うマルウェアと脅威

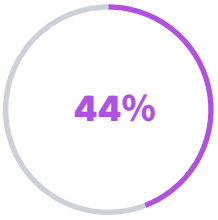
MacとWindowsはコンピュータの仕組みが異なるため、おのずとマルウェアも異なります。Macを狙うマルウェアを作成する攻撃者は、その違いを考慮して、どこを攻撃すべきかを把握しなければなりません。攻撃を成功させるには、次のようなセキュリティ機能を回避することが必要になります。

1. **Gatekeeper：アプリの公証情報や開発者情報/署名**を確認することで、そのアプリが正当で安全なものであるかをチェックする機能

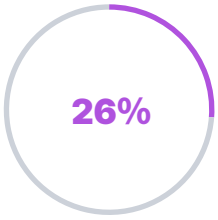
2. **システム整合性保護（SIP）：**重要なシステムファイルへの書き込みを制限する機能

3. **Transparency, Consent and Control（TCC）：**カメラ、マイク、ファイル、その他のコンテンツへのアクセスにユーザの明示的な許可を求める機能

このような壁があるにもかかわらず、**攻撃者は成功を収めています。**



悪意のあるネットワークトラフィックが検出された**デバイス**の割合



クリプトジャッキング攻撃の被害を受けたことのある**組織**の割合

だからこそ、**最新の脅威を理解して明らかにする**ことが極めて重要なのです。
把握すべき事項は多岐にわたります。

26,000件以上

Jamf Threat Labsが2025年にデータベースに追加した**マルウェアサンプル**の数

230件以上

Jamf Threat Labsが2025年に追加した**YARAルール**の数

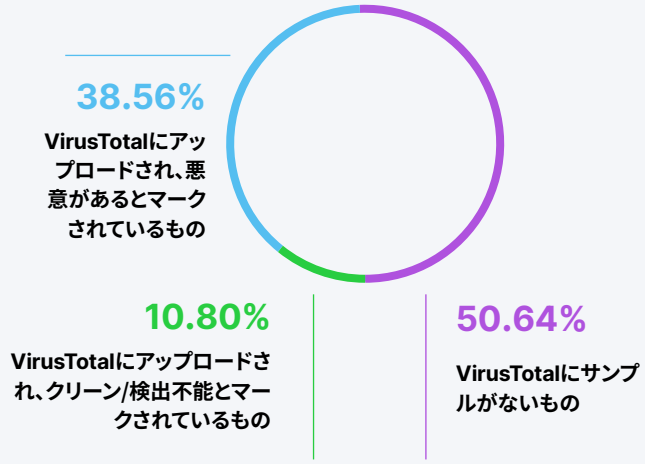
直面している脅威を特定したら、次は『いかに検知するか』が重要になります。この検出に役立つのが**YARAルール**です。調査機関はYARAルールを使ってマルウェアサンプルを特定・分類しています。

しかし、未知の脅威についてはどうでしょうか？攻撃者もまた進化を続けており、未だ発見されていない攻撃が生まれるのは避けられない現実です。

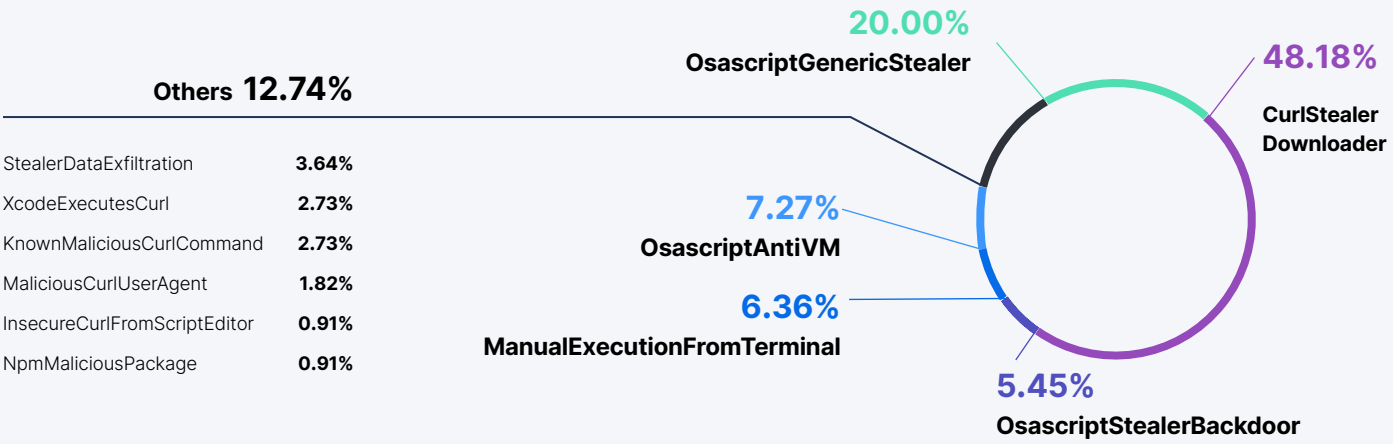
Jamf Threat Labsでは、静的ルールと振る舞い検知型ルールを用いて実環境でサンプルを捕捉し、こうした脅威も検出しています。調査したサンプルの約**50%**はVirusTotalに未登録であり、他の研究者にも発見されていない未知の検体でした。

マルウェアが特定されやすくなると、マルウェアの作者は検出を回避するために大幅な改修を行います。調査機関は、静的なファイル特性ではなく、**振る舞い・挙動**を調べる高度な検出技術を駆使する必要があります。深刻度が「高」と判断された挙動のアラートは、Jamfの高度な脅威制御による注視の対象となり、その後ブロックされます。2025年には次のようなものが多く見られました。

JAMF THREAT LABSで発見されたサンプル



高度な挙動検出



検出されたこれらのマルウェアの挙動の例をいくつか紹介します。

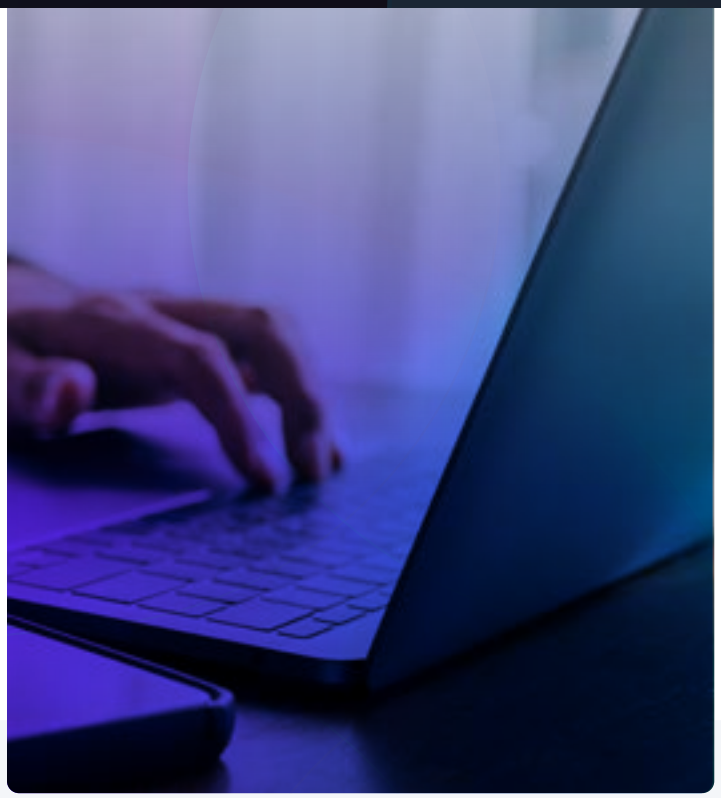
CurlStealerDownloader
curlを悪用してインフォスティーラーのペイロードをダウンロード・実行しようとする不審な動作

OsascriptGenericStealer
AppleScriptの実行によって検出された、macOSを狙った一般的なインフォスティーラー活動

XcodeExecutesCurl
Xcodeビルドプロセス中に実行された不審なcurlコマンド

NpmMaliciousPackage
悪意のある可能性のあるNPMパッケージの実行。インストール時や実行時に不審なスクリプト活動があったことを示している

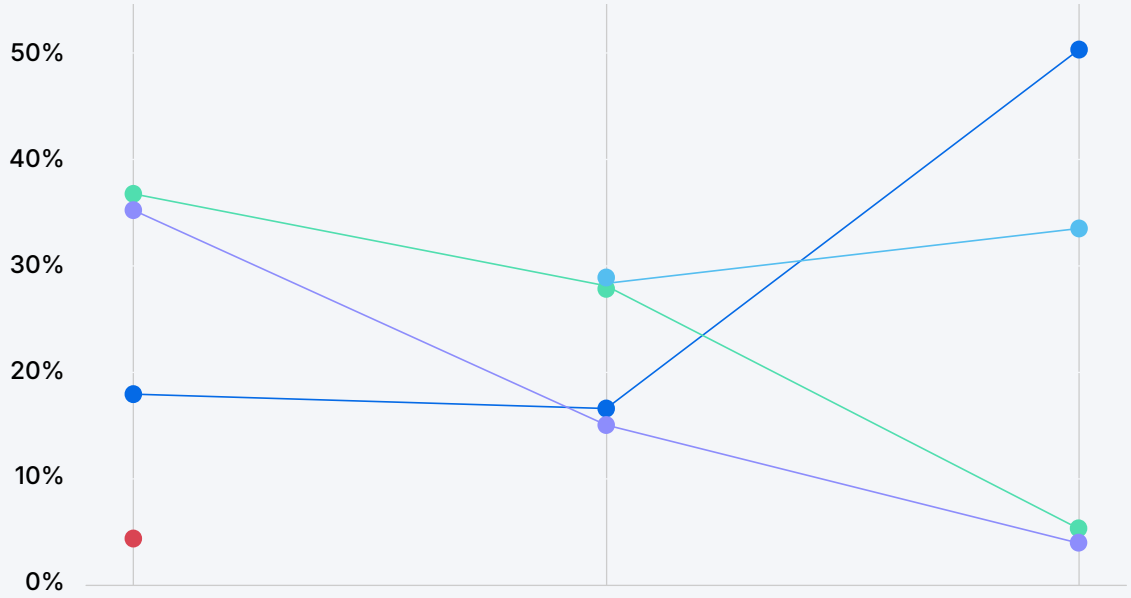
重要なのは、Macを標的とした脅威は広く蔓延しており、しかも多種多様であるという点です。攻撃者は自らの利益のため、最も高い値を付けた者に販売するためにマルウェアを作成しており、その需要はかつてないほど高まっています。守りを固めるための第一歩は、まず戦うべきマルウェアのことを知る必要があります。



最も一般的なMacマルウェア

2025年には攻撃戦略に変化が見られました。2024年はインフォスティーラーとアドウェアが主流で、それぞれ攻撃全体の約**28%**を占めていました。しかし2025年はトロイの木馬が首位となり、攻撃全体の約半分を占め、インフォスティーラーは約3分の1を占めて2位になりました。インフォスティーラーがトロイの木馬のバックドアを利用するようになったことが、トロイの木馬の増加の一因となっています。今年のデータを過去のレポートと比較すると、脅威トレンドの変遷が見えてきます。

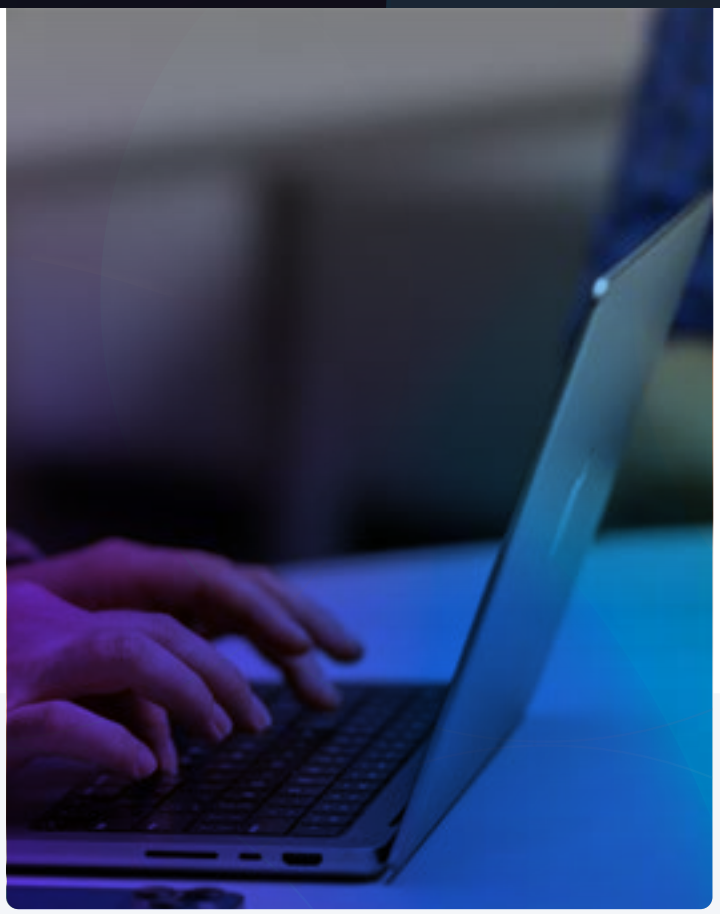
マルウェアの主要なトレンド



Malware Type	2023	2024	2025
Trojan	17.96%	16.61%	50.32%
Infostealer	-	28.36%	33.52%
Adware	36.77%	28.13%	5.06%
PUA	35.24%	15.06%	4.84%
Exploit	4.40%	-	-

上位4種類のマルウェアが
全攻撃の90%以上を占めています。
その4つを表にまとめました。

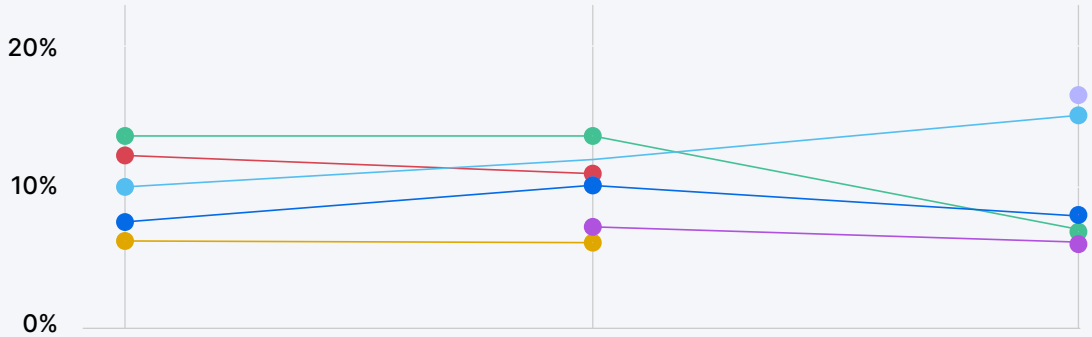
	特性:	狙い:	配布方法:
トロイの木馬 50.40%	正規のアプリケーションを装う	さまざまな形態があり、他の攻撃のためのバックドアとして広く利用される	ソーシャルエンジニアリング、ファイルリポジトリなど
インフォスティーラー 33.52%	感染後すぐにシステムデータを盗み出す	ログイン情報や個人識別情報などの機密データを収集する	サービスとして提供される場合もあり、ソーシャルエンジニアリング、悪意のあるWebサイト、ソフトウェアのダウンロードなどを通じて拡散される
アドウェア 5.06%	広告を表示し、ターゲット広告やスパイウェア目的でユーザーの行動を追跡する場合がある	広告収入を得たり、情報を収集したりする	他のソフトウェアにバンドルされている、悪意のあるWebサイトや添付ファイル内に存在
潜在的に迷惑なアプリケーション（PUA） 4.84%	形態は多岐にわたり、データの収集やデバイスの低速化など業務の妨げとなる場合がある	必ずしも悪意のあるものではないが、ユーザデータを収益化したり他の手段で収益を得たりする可能性がある	他のソフトウェアにバンドルされている、誤解を招く手法でダウンロードされる
その他 6.26%	**2.0% エクスプロイト、1.4% ハッキングツール、0.9% コインマイナー、0.4% ダウンローダー、0.4% キーロガー、0.3% ランサムウェア、0.2% ドロッパー**		



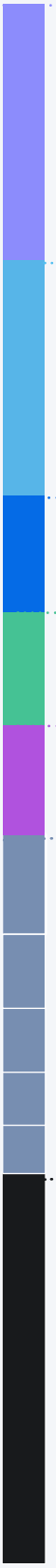
最も一般的なMac マルウェアファミリー

Macを狙うマルウェアは多種多様で、明確な主流は存在しません。2025年にはPuAgentが16.41%で最も多く見られました。2023年と2024年にはGenioアドウェアが13.63%で最も多く見られましたが、2025年には7.19%で4位に後退しました。

マルウェアの主要なトレンド



Malware Type	2023	2024	2025
PuAgent	-	-	16.41%
Generic	10.02%	-	15.09%
Genio	13.63%	13.63%	7.19%
Multiverze	6.84%	9.44%	7.47%
Mackeeper	-	7.19%	7.13%
Imobie	12.25%	10.96%	-
TNT	6.19 %	6.07%	-



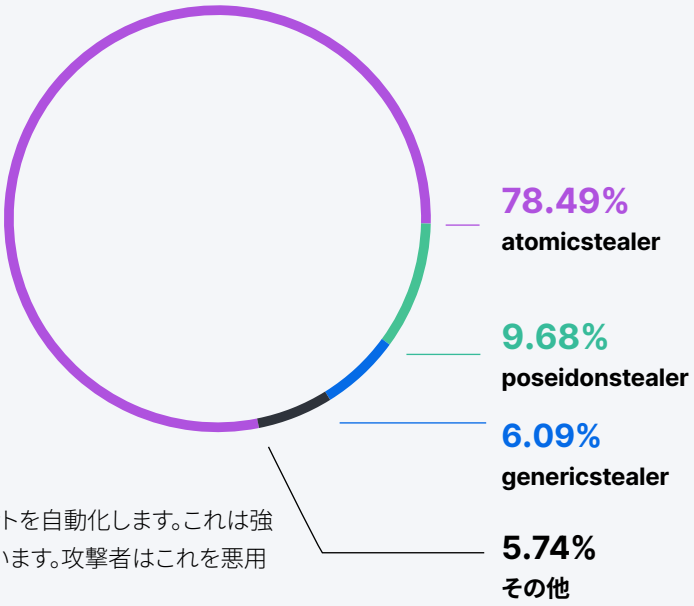
	特性：	配布方法：
PuAgent アドウェア **16.4%**	検索エンジン、ホームページ、設定、拡張機能などを変更してブラウザを改ざんする。広告ポップアップを表示し、ユーザの行動を追跡する。	Eメール添付ファイル、悪意のあるダウンロード/リンク、フリーウェア
汎用マルウェア 各種 **15.1%**	挙動自体はマルウェアの性質を示しているが、特定の既知マルウェアファミリーとして識別できるシグネチャを持たないファイル。	多種多様
Multiverze トロイの木馬 **7.5%**	パスワード、クレジットカード番号、暗号通貨ウォレットなどの個人情報を含むユーザデータを収集する。入力した内容や画面に表示されている内容をすべて記録する場合がある。ユーザには見えないこともある。	フィッシングメール、悪質なWebサイト、マルバタイジング、フリーウェア、SNS
Genio アドウェア **7.2%**	Webブラウザを乗っ取り、ユーザ情報を収集する。検索エンジンを装って広告を表示。アンインストールが困難。	正規のソフトウェアへのバンドル、悪意のあるダウンロード
Mackeeper PUA **7.1%**	正規のアプリケーションを装っているが、宣伝通りの性能を発揮しない可能性がある。広告ポップアップを表示し、デバイスの状態について虚偽の表示をしたり、デバイスのパフォーマンスを低下させたりする場合がある。	マルバタイジング、悪意のあるダウンロード
Imobie **6.3%**		
Revproxy **4.7%**		
atomic_stealer **4.1%**		
Ccleanmac **3.4%**		
Macinformer **3.1%**		
Others **25.1%**		

インフォスティーラー

不正に情報を窃取しようとすれば（もちろん推奨されるものではありません）、侵入から退出までの時間が短いほど、検知される可能性は低くなります。インフォスティーラーは通常、デバイスに感染した直後に素早くデータを盗もうとします。被害を与えた後に自己消去するものもある一方、最新のインフォスティーラーはシステム内に留まる場合もあります。

> インフォスティーラーは、macOSエコシステムにおけるマルウェアの急増に大きく関与しています。AppleScriptは長らくパワーユーザにとって便利なツールでしたが、マルウェアにおいても広く悪用されてきました。
>
> Jaron Bradley、Jamf

主なインフォスティーラー



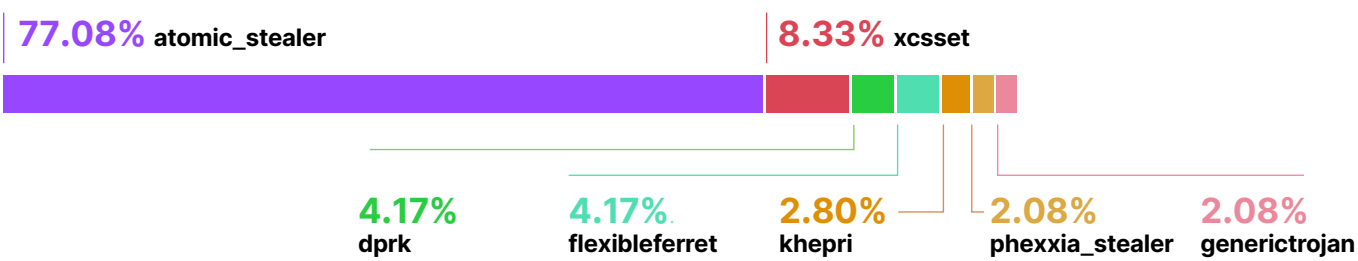
一般の開発者やパワーユーザは、AppleScriptを活用して様々なイベントを自動化します。これは強力なツールであり、良い方向にも悪い方向にも無限の可能性を持っています。攻撃者はこれを悪用してユーザを騙し、情報を盗み出すのです。

インフォスティーラーは、それまでは攻撃全体のわずか**0.25%**を占めるに過ぎませんでしたが、2023年以降はかなり多く見られるようになりました。2024年には**28.36%**へと急増し、**2025年には33.52%**に達しました。インフォスティーラーは広く蔓延している一方で、それよりも多くの攻撃がトロイの木馬などの他の種類のマルウェアで構成されています。具体的には次のとおりです。

トロイの木馬

トロイの木馬は2025年に急速に流行し、最終的に**全マルウェア攻撃の50.3%**を占めて首位になりました。最も一般的なトロイの木馬である**atomic_stealer**は、**攻撃の77.08%**に関与していました。2025年に猛威を振るったインフォスティーラーと酷似していることにお気づきでしょうか。もちろん、これは偶然ではありません。多くのインフォスティーラーは、再侵入を可能にするバックドアを確立するためにトロイの木馬を利用しているのです。

アクティブなトロイの木馬



敵を知れば、半分勝ったも同然。

これまで紹介してきたマルウェアの多くは、既によく知られています。お使いの脅威検出ソフトウェアで特定できる可能性が高いでしょう。しかし、先ほども触れたように、すべてのマルウェアがシグネチャで識別できるわけではありません。サイバーセキュリティコミュニティでまだ分析されていない脅威を発見するには、不審な挙動を特定する高度な検出機能が不可欠です。高度なツールを導入することは、ゼロデイ攻撃から組織を守るうえで大きな効果を発揮します。

構成も重要です。マルウェアは、ユーザがリスクのあるダウンロードを実行する、ソーシャルエンジニアリング攻撃に引っかかるなど、ユーザの行動を悪用することがよくあります。それらへの対抗措置としては、セキュリティポリシーの確立とユーザへのトレーニングが有効です。

脅威の検出は極めて重要ですが、脅威の予防も非常に有効です。これはソフトウェアが出発点になります。サイバー攻撃はソフトウェアの脆弱性、つまり、攻撃の余地を残しているアプリやオペレーティングシステムの設計上の欠陥を悪用します。デバイスとアプリのアップデートを徹底することが、こうした脆弱性を解消し、攻撃者を寄せ付けないための最善策になります。これについて、次のセクションで詳しく説明します。

Jamf CISOからの助言

Appleデバイスの普及が企業で進む今、採用するセキュリティソリューションは、Windows優先のアプローチを流用するのではなく、Appleエコシステム専用に構築されたものであるべきです。組織は、初めからmacOS向けに設計されたセキュリティ製品を優先し、脅威の検出、コンプライアンスの徹底、インシデント対応の機能がAppleプラットフォームの動作に完全に適合するものを選ぶ必要があります。後付けとして扱うべきではありません。

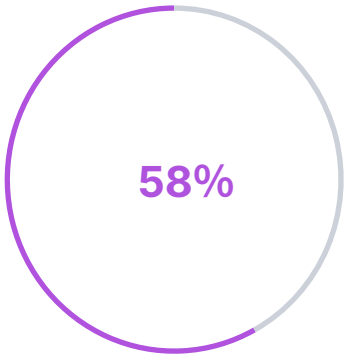
アプリとOSの脆弱性

オペレーティングシステムはデバイスの基盤です。デバイスのツール、サービス、アプリケーション、セキュリティを支えています。攻撃者は侵入するために、常にその防御の穴を探しています。

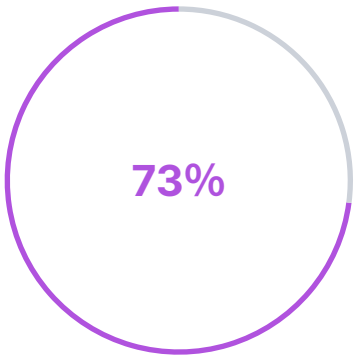
脆弱性は積み上がります。たとえ深刻度の低い脆弱性であっても、攻撃の重要な一歩となりえますが、こうした脆弱性へのパッチ適用が時として後回しにされることがあります。

パッチ適用も、非常に重要な施策です。残念ながら、どれほど安全なオペレーティングシステムであってもどこかに脆弱性が存在します。これは避けられないことではありますが、対処不可能なことではありません。Appleは脆弱性に対処するために、絶えずソフトウェアアップデートをリリースしています。保護された状態を維持するには、組織がこれらのアップデートを強制適用する必要があります。ところが、これは必ずしも実践されていません。

アプリも同様に重要です。アプリごとに独自の脆弱性、データ取り扱いポリシー、開発ライブラリなどがあります。



OSバージョンが古く、危険な状態の**デバイスを1台以上**使用している**組織**の割合



脆弱性のあるアプリが1つ以上確認された**デイバス**の割合

CVEとは

共通脆弱性識別子（CVE）プログラムは、サイバーセキュリティコミュニティが発見した脆弱性をデータベース化したものです。CVE項目それぞれに、影響を受けるソフトウェアやライブラリ、深刻度スコア、考えられる悪用方法が記載されています。

ソフトウェアの更新放置は、驚くほど多く存在します。ユーザは必ずしもアップデートに積極的ではなく、業務に影響が出ると感じる場合はなおさらです。しかし、アップデートの期限を設けたりOSバージョンの最小要件を徹底したりすることは、脆弱性を悪用する攻撃からデバイスを守るなど、デバイスとデータを保護するうえで大きな効果があります。

2025年の注目すべきmacOSの脆弱性

CVE-2025-46287 | 深刻度：9.8（緊急）	CVE-2025-43539 | 深刻度：8.8（高）	CVE-2025-46285 | 深刻度：7.8（高）
説明：		
攻撃者がFaceTimeの発信者IDを偽装できる可能性がある。	ファイルを処理すると、メモリ破損が発生する可能性がある。	アプリがルート権限を取得できる可能性がある。
影響を受けるコンポーネント		
通話フレームワーク	AppleJPEG	カーネル
影響：		
攻撃者が誤解を招く情報を表示してユーザを騙し、不適切な操作に誘導できる。	攻撃者がデータを改ざんして、不正なコードを実行できる。	攻撃者が任意のコードを実行できる。
パッチ適用済みのOS：		
macOS Tahoe 26.2、Sequoia 15.73、Sonoma 14.8.3	macOS Tahoe 26.2、Sequoia 15.73、Sonoma 14.8.3	macOS Tahoe 26.2、Sequoia 15.73、Sonoma 14.8.3

Jamfが発見した脆弱性

CVE-2025-43296 | 2025年10月
システム設定のGatekeeperを回避、macOS Tahoe 26でパッチ適用済み。

CVE-2025-43348 | 2025年11月
FinderのGatekeeperを回避、macOS Tahoe 26.1でパッチ適用済み。

2025年に悪用が確認されたその他の脆弱性を以下の表に示します。

CVE ID	コンポーネント	影響
CVE-2025-24113 CVSSスコア：4.3 | 深刻度：中	Safari	悪意のあるウェブサイトにアクセスすると、ユーザインターフェイスを偽装される可能性がある。
CVE-2025-46289 CVSSスコア：5.5 | 深刻度：中	AppSandbox	保護されたユーザデータにアプリからアクセスできる可能性がある。
CVE-2025-43482 CVSSスコア：5.5 | 深刻度：中	オーディオ	アプリがサービス拒否（DoS）攻撃を引き起こす可能性がある。
CVE-2025-43517 CVSSスコア：3.3 | 深刻度：低	通話履歴	ログの問題により、保護されたユーザデータにアプリからアクセスできる可能性がある。
CVE-2025-43542 CVSSスコア：7.5 | 深刻度：高	FaceTime	FaceTime経由でデバイスを遠隔操作しているときに、パスワードフィールドが意図せず表示される可能性がある。
CVE-2025-43532 CVSSスコア：2.8 | 深刻度：低	Foundation	悪意のあるデータを処理すると、メモリ破損によりアプリが予期せず終了する可能性がある。
CVE-2025-43512 CVSSスコア：7.8 | 深刻度：高	カーネル	アプリが権限を昇格できる可能性がある。

脆弱性の管理は絶え間ない戦い — でも決して勝ち目のない戦いではない。

ソフトウェアの脆弱性に対応し続けるには、優れた戦略が必要です。極めてシンプルに言うなら、システムやデバイスに影響を与える脆弱性を継続的に特定し、軽減し、監視し続けることです。

IT部門やセキュリティ部門の規模や能力によっては、脅威を自力で追跡できない場合もあります。幸いにも、サイバーセキュリティコミュニティがサポートしてくれます。脅威調査機関やソフトウェアベンダーは常に最新の攻撃を監視し、潜在的な脆弱性をデータベースに追加することで、組織が自社のどこに脆弱性があるかを把握できるよう支援しています。チームはこれらの情報を参照することで、現在のセキュリティ状態を把握し、それに応じた措置を講じることができます。このプロセスを容易に行えるセキュリティツールも提供されています。

組織には具体的にどのようなツールが必要なのかは、組織の規模、能力、業界などによって異なりますが、一般的には、以下のことを行うツールが必要になります。

- **デバイスを構成し、ポリシーを適用する**
- **ユーザのアカウントとアイデンティティを管理する**
- **デバイスとソフトウェアを最新の状態に維持する**
- **デバイスの健全性を監視する**
- **アクセスポリシーを適用する**

モバイルデバイス管理ツール、エンドポイント保護ツール、アイデンティティ管理ツール、テレメトリツールがこれらのタスクに役立ち、脅威が発生する前に先手を打つことができます。

Jamf CISOからの助言

堅牢なセキュリティ戦略は、可視性、テレメトリ、自動化という核となる原則に基づいて構築されるものであり、脆弱性管理においては、この原則が何よりも重要になります。**セキュリティ部門**が取り組むべき対策：

自社の脆弱性の把握

組織全体の脆弱性を可視化することが、非常に重要な第一歩です。エンドユーザのデバイスやインフラにどのような脆弱性が存在するかを包括的に把握することで、データに基づくセキュリティ状態の基盤を構築できます。そこから、セキュリティチームはアプリケーションの利用状況を分析し、潜在的なリスクを評価し、影響範囲を特定することで、推測ではなく根拠に基づいて脆弱性の優先順位を判断できるようになります。

デバイスアクセスに対するリスクベースのアプローチの実装

要件に準拠していないデバイスが企業リソースにアクセスしようとした場合に、デバイスが要件に準拠するまでアクセスを制限する必要があります。エンドユーザにとってできる限り違和感がなく負担の少ない修復プロセスを設計します。

堅実なパッチ適用プログラムの導入

MDMの話に戻りますが、ソフトウェアやOSを最新バージョンまたはサポート対象のN-Xバージョンに確実に保つためのツールを導入することは、健全で安全な環境を維持するために不可欠です。エンドユーザへの影響をゼロまたは最小限に抑えながらこれを進められれば、社内の協力を得やすくなります。

macOSに関するJamf Threat Labsの最新の調査結果

OpenClaw：便利なAIが、ひそかに最大の内部脅威になりうる

2026年2月

OpenClawは、シェルコマンドの実行、ファイルへのアクセス、アプリケーションの操作を行う自律型AIエージェントを構築するためのオープンソースフレームワークですが、セキュリティ境界が内蔵されていないため、企業に重大なセキュリティリスクをもたらします。このフレームワークは、無制限のシステムアクセス、データ流出の可能性、そして業務データ経由の『間接的なプロンプトインジェクション』への脆弱性により、企業にとって重大な脅威となります。最近公開されたセキュリティ勧告では、攻撃者が様々な欠陥を悪用して永続的なアクセス権を取得できる仕組みが示されています。OpenClawの導入は、高リスクの内部脅威を招くおそれがあり、企業環境で安全に運用するには、包括的な検出・予防・ガバナンス戦略の策定が必要です。

攻撃者がMicrosoft Visual Studio Codeの悪用を拡大

2026年1月

北朝鮮（DPRK）の関与する攻撃が、Contagious Interviewキャンペーンを進化させ、Visual Studio Codeのタスク構成ファイルを悪用するようになっています。被害者が悪意のあるGitリポジトリを開くと、JavaScriptバックドアが仕込まれるという手法です。このバックドアは、持続的なコマンド&コントロール（遠隔操作）通信を確立し、システム情報を収集して、リモートコード実行を可能にします。この手法は、開発者のワークフローにおける信頼の仕組みを悪用しています。ユーザがリポジトリを「信頼済み」としてマークすると、悪意のある設定ファイルが自動的に隠しコマンドを実行します。このことは、正規の開発ツールに攻撃を組み込む戦術を適応させ続ける攻撃者の姿を示す好例です。

ClickFixからコード署名へ：MacSync Stealerマルウェアの静かな進化

2025年12月

MacSync Stealerは、「ターミナルへのドラッグ&ドロップ」手法から進化を遂げ、コード署名と公証を受けたSwiftアプリケーションを通じて展開されるようになりました。このアプリケーションは、ユーザによるターミナル操作を必要とせずにペイロードをひそかに取得・実行します。偽のインストーラを介して配布されるこの亜種は、高度なドロッパーを使用して、実行前に接続性のチェック、レート制限の適用、ペイロードの検証、quarantine属性の削除を行います。署名と公証を受けた配布への移行は、攻撃者が検出を回避し、macOSのセキュリティ対策を迂回するために、悪意のあるコードを正規のアプリケーションに偽装するという広く見られるトレンドを反映しています。

FlexibleFerretマルウェアの攻撃が継続中

2025年11月

北朝鮮（DPRK）と連携するマルウェアファミリーであるFlexibleFerretは、巧妙な偽の求人を通じてmacOSユーザを狙います。このマルウェアは、採用試験を装った悪意のあるターミナルコマンドをユーザに実行するように仕向けます。多段階攻撃で、まず偽の求人サイトにJavaScriptを仕込み、ファイル流出やコマンド実行など幅広い機能を持つバックドアを設置します。そして、偽のChromeプロンプトで認証情報を収集し、攻撃者が管理するDropboxアカウントにデータを送信します。進化を続けるこの脅威は、ユーザにコマンドを手動で実行させることでGatekeeperを回避します。そのため、心当たりのない「採用面接」やターミナル操作を促す指示に対する警戒心を高めることが、防御の鍵となります。

DigitStealer：痕跡をほとんど残さないJXAベースのインフォスティーラー

2025年11月

DigitStealerは、高度な分析対策手法を採用し、VirusTotalでもまったく検出されずにいた、巧妙なmacOSインフォスティーラーです。分析の回避には、実行をApple シリコンM2チップ以降に制限するハードウェア機能検出などが用いられました。このマルウェアは、ブラウザデータ、暗号通貨ウォレット、認証情報を盗む4つのメモリ常駐型ペイロードを展開します。さらに、Ledger Liveに3つのコンポーネントを統合することでトロイの木馬化して検出を回避し、動的なバックドアを通じて持続性を確保します。ペイロードのホスティングに正規のCloudflareサービスを利用し、多段階の難読化を実施していることから、macOSの内部構造を深く理解していることがうかがえます。実行の大部分がメモリ内で完結するため、振る舞い・挙動検出が極めて重要となります。

ChillyHell：モジュール型macOSバックドアの徹底調査

2025年9月

ChillyHellは、2021年以来、公証を受けて検出されずに潜伏し続けていた巧妙なmacOSバックドアです。当初はウクライナ政府関係者を標的とした攻撃に関連していました。このモジュール型C++マルウェアは、複数の持続化メカニズムを確立し、DNSやHTTPを介して通信を行い、リバースシェル、自己アップデート、ペイロード配信、パスワードブルートフォース攻撃などの機能を展開します。その高度な回避手法は、署名・公証されたアプリであっても必ずしも安全ではないことを示しています。

署名と窃盗：Odysseyインフォスティーラー関する新たな知見

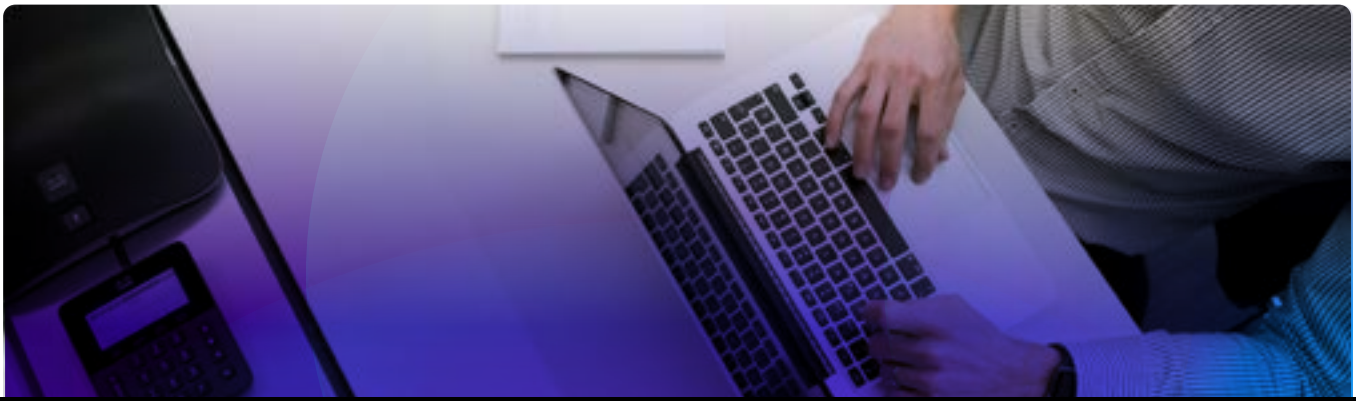
2025年7月

このマルウェアは、偽りのSwiftUIインターフェイスを用いてパスワードを収集し、難読化されたペイロードを動的にダウンロードして、リモートコード実行のための継続的なコマンド&コントロールを確立します。このマルウェアは、偽りのSwiftUIインターフェースを用いてパスワードを収集し、難読化されたペイロードを動的にダウンロードして、リモートコード実行のための継続的なコマンド&コントロールを確立します。最も懸念されるのは、分析環境の詳細を積極的に識別し、検出回避のために調査システムをブラックリストに登録する点です。これは国家レベルの高度な技術力があることを示唆しています。

偽装されたPython：macOS上のPyInstallerマルウェアの解明

2025年5月

攻撃者はPyInstallerを悪用して、悪意のあるPythonコードをmacOSネイティブの実行ファイルに偽装していました。macOSを狙ったインフォスティーラーでこのような手法が確認されたのは、この事例が初めてです。このマルウェアの実行にはPythonのインストールが必要なく、偽りのパスワード入力画面から認証情報を盗み取って、キーチェーンデータや暗号通貨ウォレット情報を収集します。検出回避には複数の難読化レイヤーが用いられています。このような手法はmacOSマルウェアの配布における大きな進化を象徴しており、攻撃者は高度なインフォスティーラーを展開しながら従来のセキュリティメカニズムを回避できる可能性を示しています。



jamf

Macを狙う脅威について詳しく知りたい方は、
Jamfへお問い合わせください。