2026年
4月
APRIL

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

はじめに

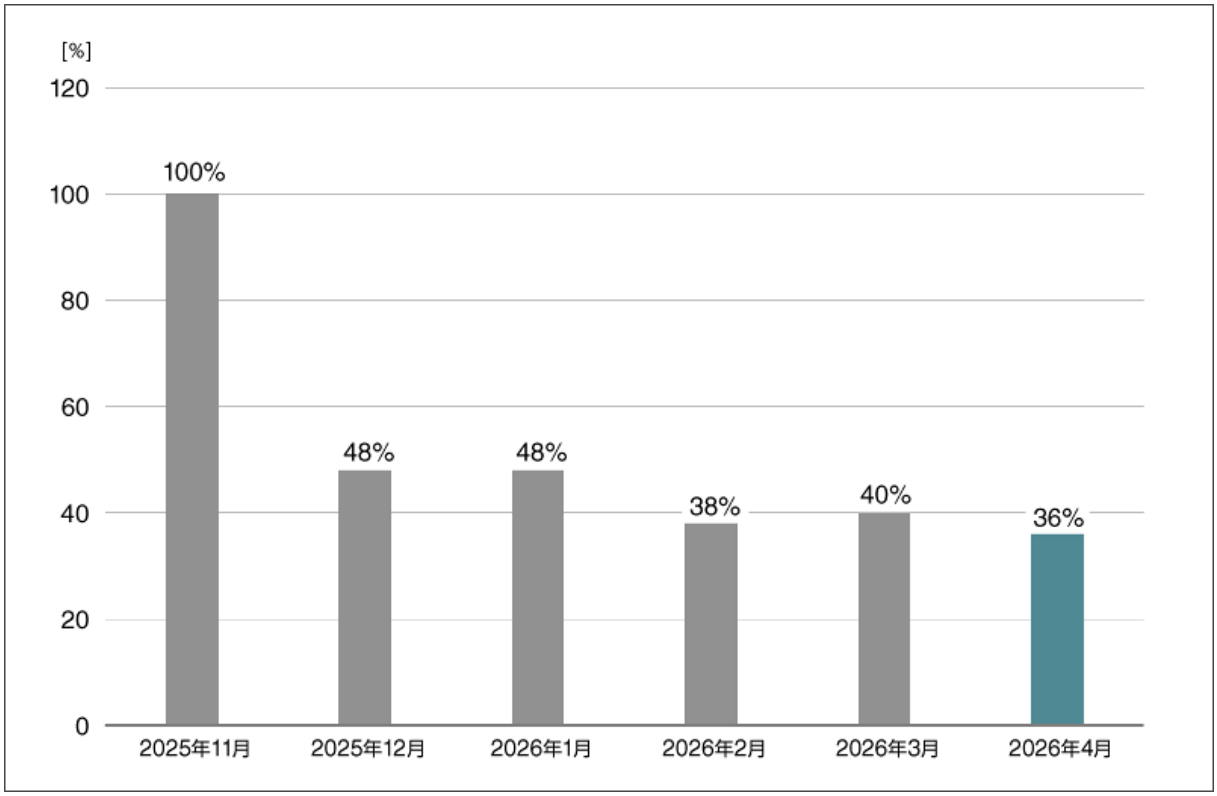
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2026 年 4 月マルウェア検出状況

2026 年 4 月（4 月 1 日～4 月 30 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

(2025 年 11 月の全検出数を 100%として比較)

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2026 年 4 月の国内マルウェア検出数は、2026 年 3 月と比較して微減しました。検出されたマルウェアの内訳は以下のとおりです。

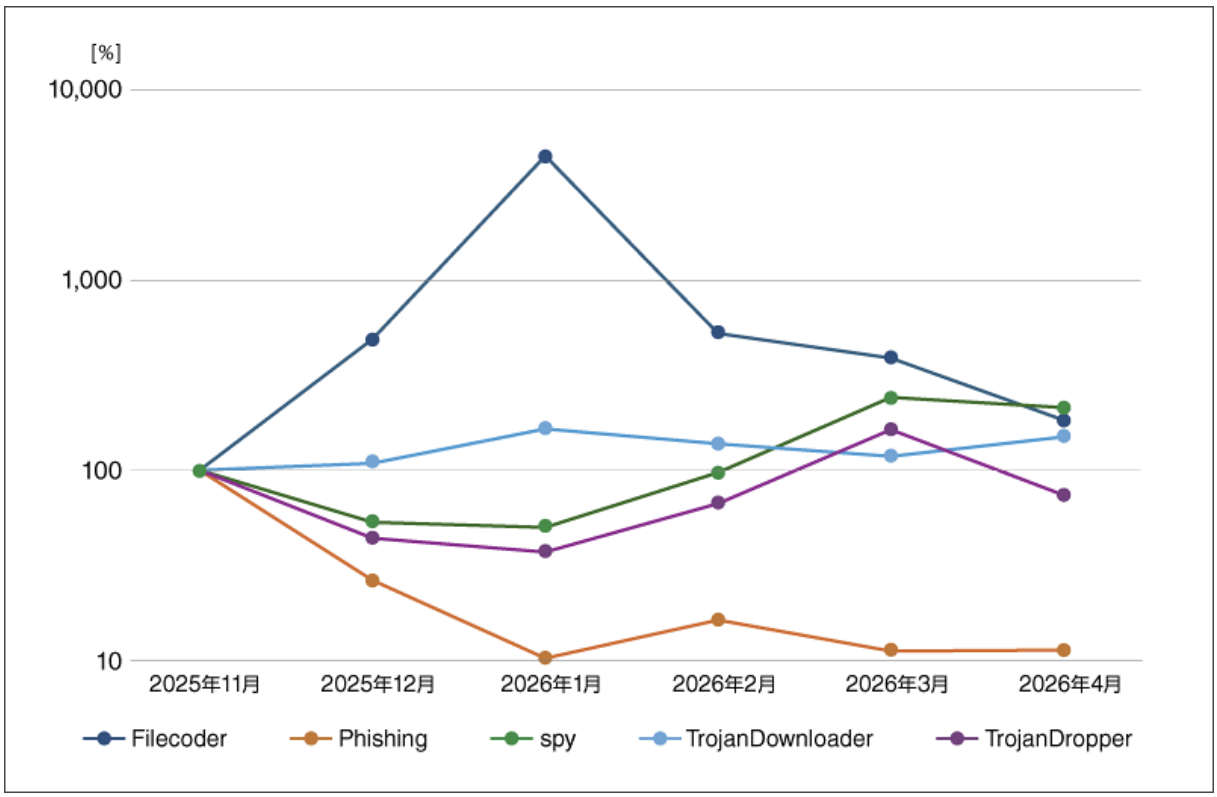
国内マルウェア検出数*2 上位（2026 年 4 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	23.4%	アドウェア
2	HTML/Phishing.Agent	13.8%	メールに添付された不正な HTML ファイル
3	Win64/Agent	7.0%	不正な 64bit プログラムの汎用検出名
4	DOC/Fraud	4.8%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	2.6%	不正な JavaScript の汎用検出名
6	JS/TrojanDownloader.Agent	2.0%	ダウンローダー
7	BAT/Agent	1.9%	不正なバッチファイルの汎用検出名
8	JS/Danger.ScriptAttachment	1.5%	ダウンローダー
9	HTML/Phishing.Gen	1.4%	フィッシングを目的とした不正な HTML ファイル
10	JS/TrojanDropper.Agent	1.0%	ドロッパー

*2 本表には PUA を含めていません。

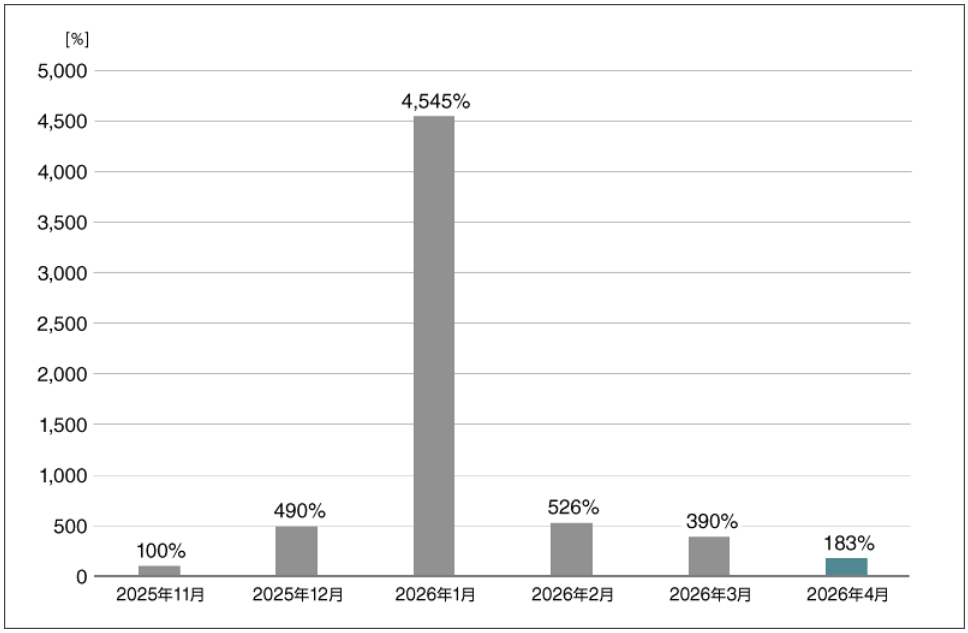
4 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

2026 年 4 月に ESET 製品が国内で検出したマルウェアの種類別の推移は、以下のとおりです。以降のグラフには PUA が含まれています。



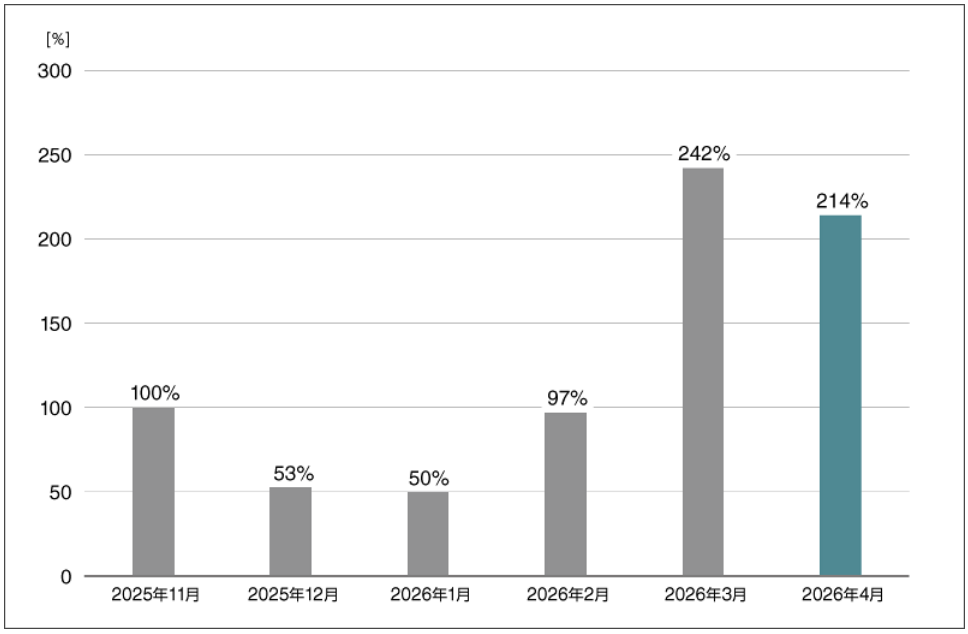
国内マルウェアの種類別検出数の推移
（2025 年 11 月の各検出数を 100%として比較）
※縦軸を対数軸として表記

2026 年 4 月はダウンローダーの検出数が増加しました。一方で、ドロッパーとランサムウェアの検出数は減少しています。



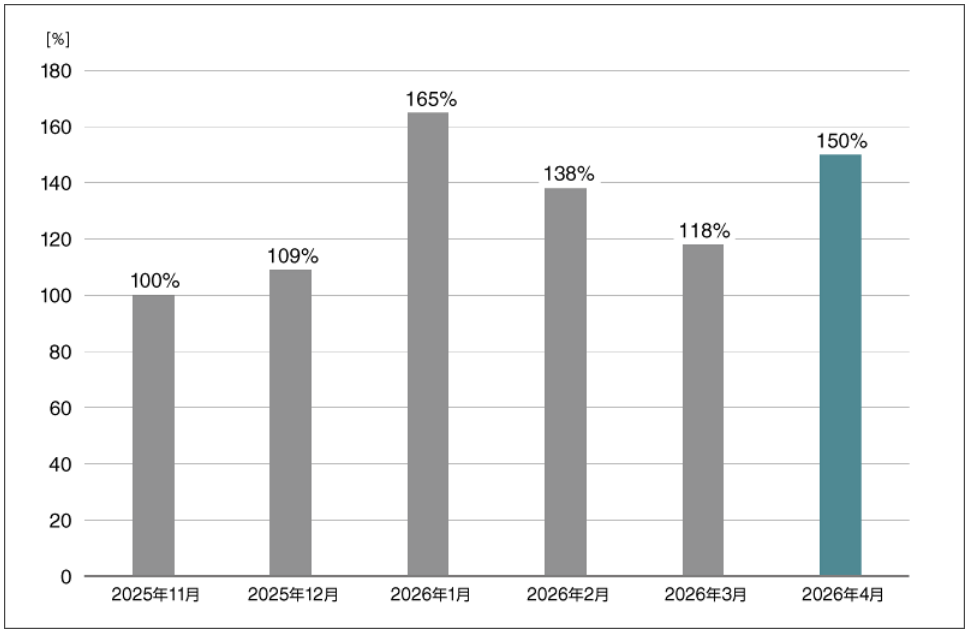
ランサムウェア検出数の推移（国内）

（2025 年 11 月の検出数を 100%として比較）



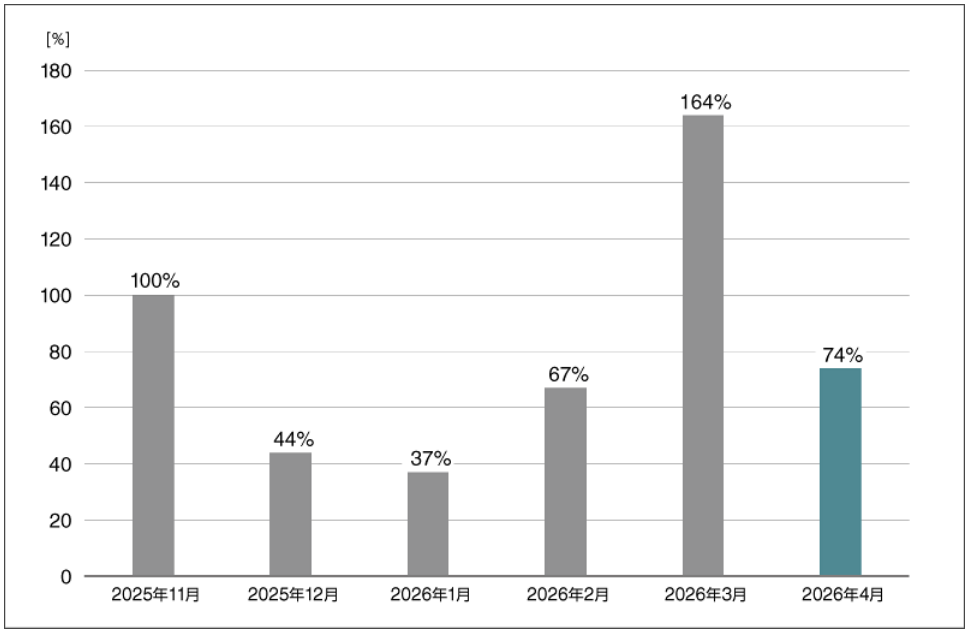
スパイウェア検出数の推移（国内）

（2025 年 11 月の検出数を 100%として比較）



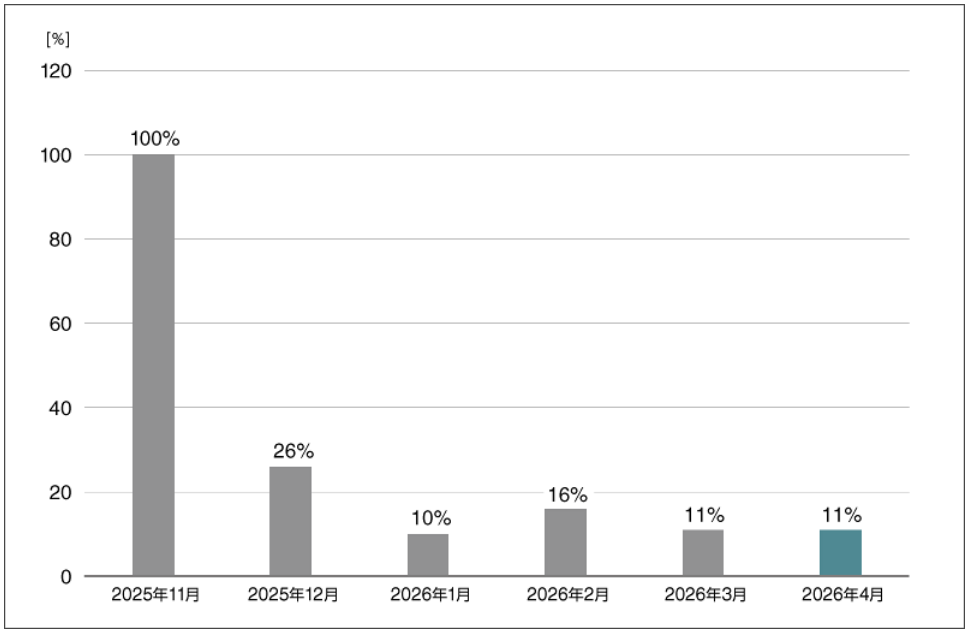
ダウンローダー検出数の推移（国内）

（2025 年 11 月の検出数を 100%として比較）



ドロッパー検出数の推移（国内）

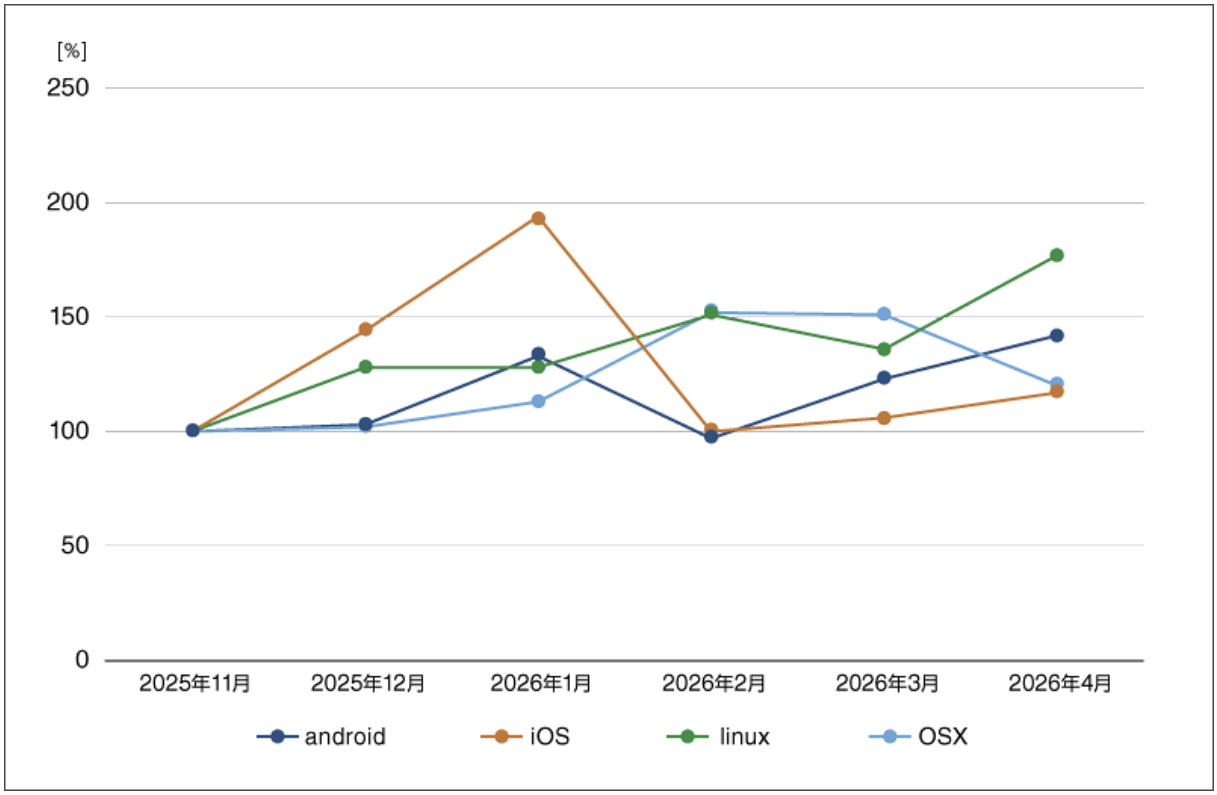
（2025 年 11 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 11 月の検出数を 100%として比較）

2026 年 4 月に ESET 製品が国内で検出したマルウェアの OS 別推移は、以下のとおりです。

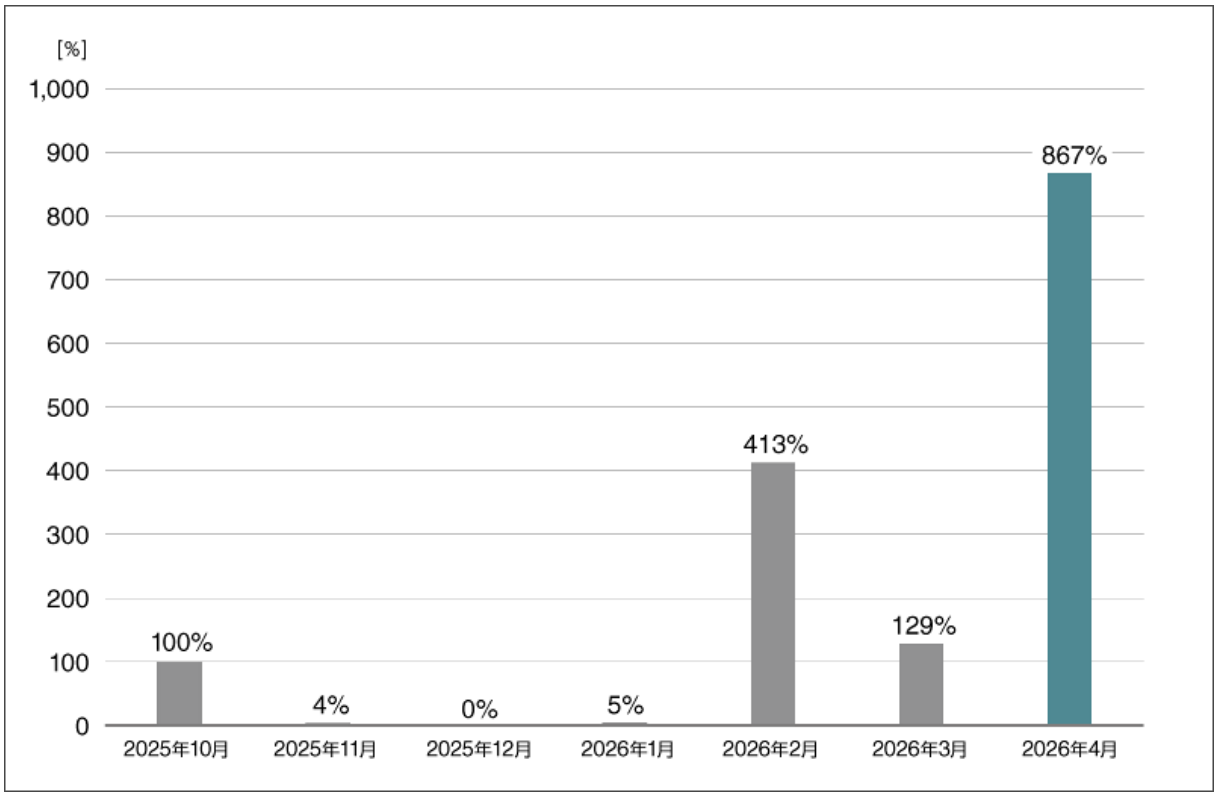


国内マルウェアの OS 別検出数の推移（Windows を除く）
（2025 年 11 月の各検出数を 100%として比較）

2026 年 4 月は Android や iOS、Linux を狙ったマルウェアが増加しました。一方で、OS X を狙ったマルウェアは減少しました。

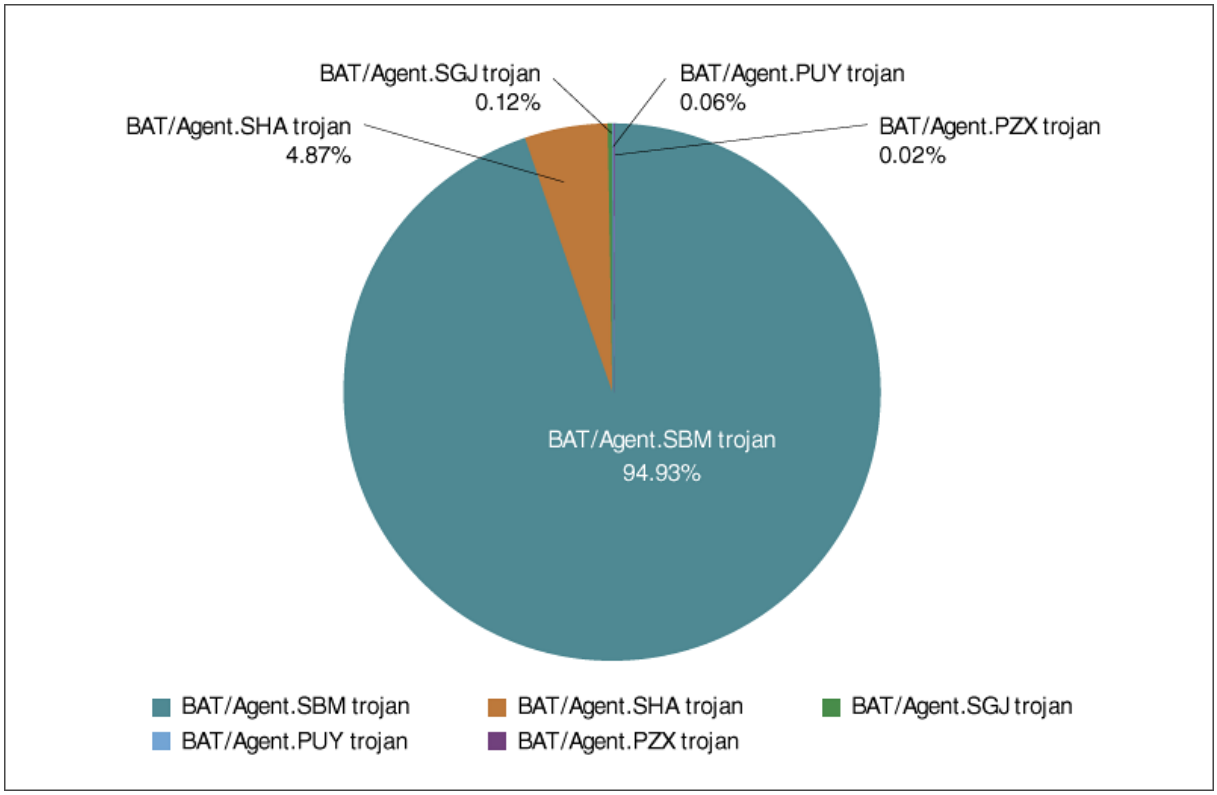
2026 年 4 月に検出数が増加した BAT/Agent について

2026 年 4 月のマルウェア検出統計では、国内における BAT/Agent の検出数増加が確認されました。直近 6 か月の推移を見ると、4 月の検出数は前月比で約 8 倍となり、期間中で最大の検出数を記録しています。このマルウェアは 2026 年 4 月の国内検出数上位 10 種に含まれ、検出数は第 7 位でした。



国内における BAT/Agent の検出数月別推移（2026 年、国内）
※2025 年 10 月の検出数を 100%として比較

BAT/Agent は不正なバッチファイルに対する汎用検出名です。亜種によって対応するマルウェアは異なります。同月に検出された BAT/Agent 亜種の内訳を見ると、BAT/Agent.SBM が全体の 9 割以上を占めていました。



BAT/Agent の亜種別検出数割合（2026 年 4 月、国内）

BAT/Agent.SBM は、難読化されたバッチファイルです。この BAT/Agent.SBM を解析すると、難読化されたスクリプトから悪意のあるコードを復号・実行する挙動を確認しました。

難読化された BAT/Agent.SBM の動作について

2026 年 4 月に検出された BAT/Agent.SBM の動作を紹介します。以下は、BAT/Agent.SBM を実行した際のプロセスツリーを示した図です。

BAT/Agent.SBM 実行時のプロセスツリー

本検体は、複数の段階を経て悪意のある動作を実行させる構成になっています。バッチファイルは、複数のプロセスを起動します。中でも、PowerShell は、難読化されたコードの復号や、正規アプリケーション上で悪意のある動作を実行させる役割を担っています。さらに、子プロセスとして起動された csc.exe と cvtres.exe は、.NET Framework のコンポーネントであり、コードの動的コンパイルや実行に悪用されることがあります。本検体では、正規アプリケーションの Explorer.exe に悪意のあるコードを実行させるためのコードが C#言語で書かれており、このコードを動的にコンパイルして実行するために csc.exe と cvtres.exe が起動しています。この手法はファイルレスマルウェアで用いられることがあり、ディスク上に痕跡を残しにくいことから、セキュリティ製品による検知の回避やフォレンジックを困難にする目的で悪用される場合があります。

本検体では、Explorer.exe が Telegram に対して PC 名や IP アドレス・国コードを送信する挙動を確認しています。URL 内に感染端末に関するメッセージが含まれていたことから、この通信は攻撃者の bot に感染を通知する目的で行われている可能性があります。

本検体の実行の流れは、大きく 3 つに分けられます。

第一段階：バッチファイルによる PowerShell の実行

第二段階：PowerShell による難読化解除とコードの実行

第三段階：Explorer.exe で悪意のあるコードの実行

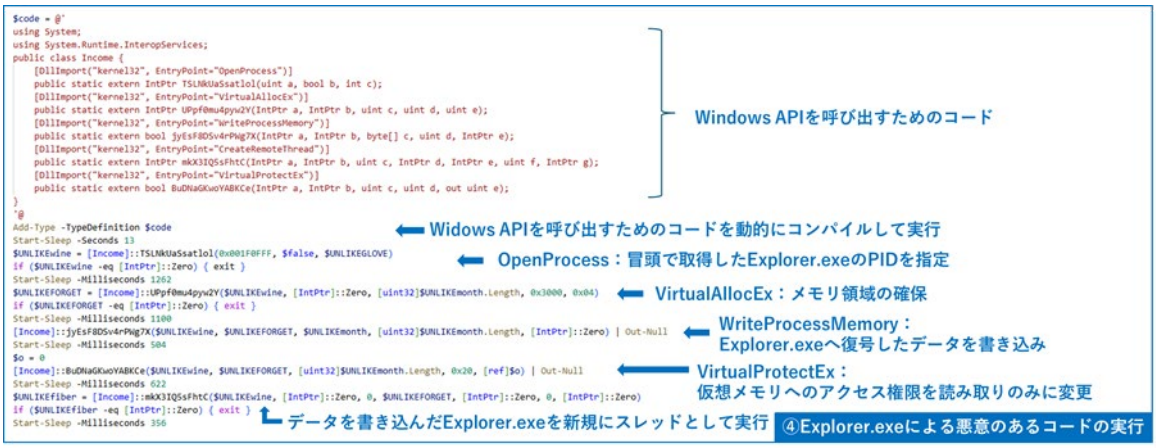
本検体の実行において、担う役割が大きい第二段階のコードを解説します。第二段階では、符号化・暗号化されたデータの復号と、Explorer.exe に悪意のあるコードを実行させる処理が行われます。以下が、第二段階で実行されるコードです。

第二段階のコードの前半部分

第二段階のコードは、4 つの工程に細分化できます。

① 二重感染を防ぐためのミューテックスの確認
② Explorer.exe の取得と存在の確認
③ 符号化および暗号化された文字列の復号
④ Explorer.exe による悪意のあるコードの実行

1 つ目の工程では、二重感染を防ぐためにミューテックスを確認します。ミューテックスがすでに作成されている場合、コードの実行は終了します。2 つ目の工程は、悪意のあるコードを実行させる Explorer.exe のプロセス ID（以降は PID と表記）を取得して存在を確認します。ここで取得する PID は、悪意のあるコードを実行するアプリケーションを指定するために使います。3 つ目の工程では、Base64 で符号化された文字列を復号し、先頭 1 バイトを鍵とした XOR 演算を実行します。続いて、XOR 演算後の文字列からデータを抽出し、AES で復号します。ここで復号したデータは悪意のある動作に使われます。



第二段階のコードの後半部分

4 つ目の工程では、C#言語で書かれたコードを動的にコンパイルして、実行します。工程②で取得した PID によって Explorer.exe を指定し、工程③で復号した悪意のあるコードを実行させています。ここでは、Explorer.exe に悪意のある動作を実行させるために、メモリ領域に悪意のあるコードを書き込んでいます。

ファイルレスマルウェアへの対策

2026 年 4 月に増加した BAT/Agent.SBM は、ファイルレスマルウェアを実行するバッチファイルでした。ファイルレスマルウェアは、主にメモリ上で動作し、ディスク上に実行ファイルを保存しない特徴を持っており、正規機能を悪用することが多いマルウェアです。そのため、従来のシグネチャベースの検知や、フォレンジックは難しくなる傾向があります。
以下、ファイルレスマルウェアへの対策を紹介します。

■EDR による監視

- メモリに対する不審な操作の監視
- 正規アプリケーション（PowerShell や WMI など）の挙動監視
- Windows マルウェア対策スキャンインターフェイス（AMSI）[1] や Windows LockDownPolicy（WLDP）[2] などのセキュリティ機構に対する回避・無効化の検知および稼働状況の監視

1 AMSI は、アプリケーションとサービスが端末内のマルウェア対策製品と統合することを提供するセキュリティ機能です。

2 WLDP は、実行されるスクリプトが組織内のポリシーで許可されているかを確認し、スクリプトの実行可否を管理します。

ファイルレスマルウェアはシグネチャベースの検知が困難であるため、振る舞い検知が前提となります。特に、PowerShell や Explorer.exe などの悪用される傾向にある正規アプリケーションの挙動監視を継続的に実施する必要があります。加えて、AMSI や WLDP といったスクリプト実行に関するセキュリティ機能が無効化される可能性があるため、これらの稼働状況を監視することが重要です。

■PowerShell 実行ポリシー管理およびファイアウォール制御

- グループポリシーによる PowerShell 実行ポリシーの管理（制限付きや署名必須など）
- PowerShell 経由の通信に対するファイアウォール制御
- PowerShell 実行ログの取得

ファイルレスマルウェアで悪用される PowerShell については、グループポリシーにより実行を制御することで、不正なスクリプト実行の抑止が可能です。また、PowerShell によるインターネット通信が業務上不要な場合は、ファイアウォールで通信を制限することで、マルウェアの追加ダウンロードを防止できます。
さらに、マルウェアによって意図せず PowerShell が実行されてしまった場合に備えて、実行ログを記録しておくことはインシデント対応において有用です。

まとめ

2026 年 4 月マルウェアレポートでは、悪意のあるバッチファイルである BAT/Agent の増加を紹介しました。特に検出数が増加した BAT/Agent.SBM では、正規アプリケーションを悪用してファイルレスで実行する挙動を確認しています。従来のマルウェアと比較して、検知やフォレンジックが難しい傾向にあるため、紹介した対策の導入を推奨します。

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

１．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

２．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1. 脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2. インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1. 情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2. 情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

引用・出典元

●マルウェア対策スキャンインターフェイス（AMSI）| Microsoft 社
https://learn.microsoft.com/ja-jp/windows/win32/amsi/antimalware-scan-interface-portal
●wldp.h ヘッダー | Microsoft 社
https://learn.microsoft.com/ja-jp/windows/win32/api/wldp/

Canon

キヤノンマーケティングジャパン株式会社