2025年
9月
SEPTEMBER

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

Canon キヤノンマーケティングジャパン株式会社

はじめに

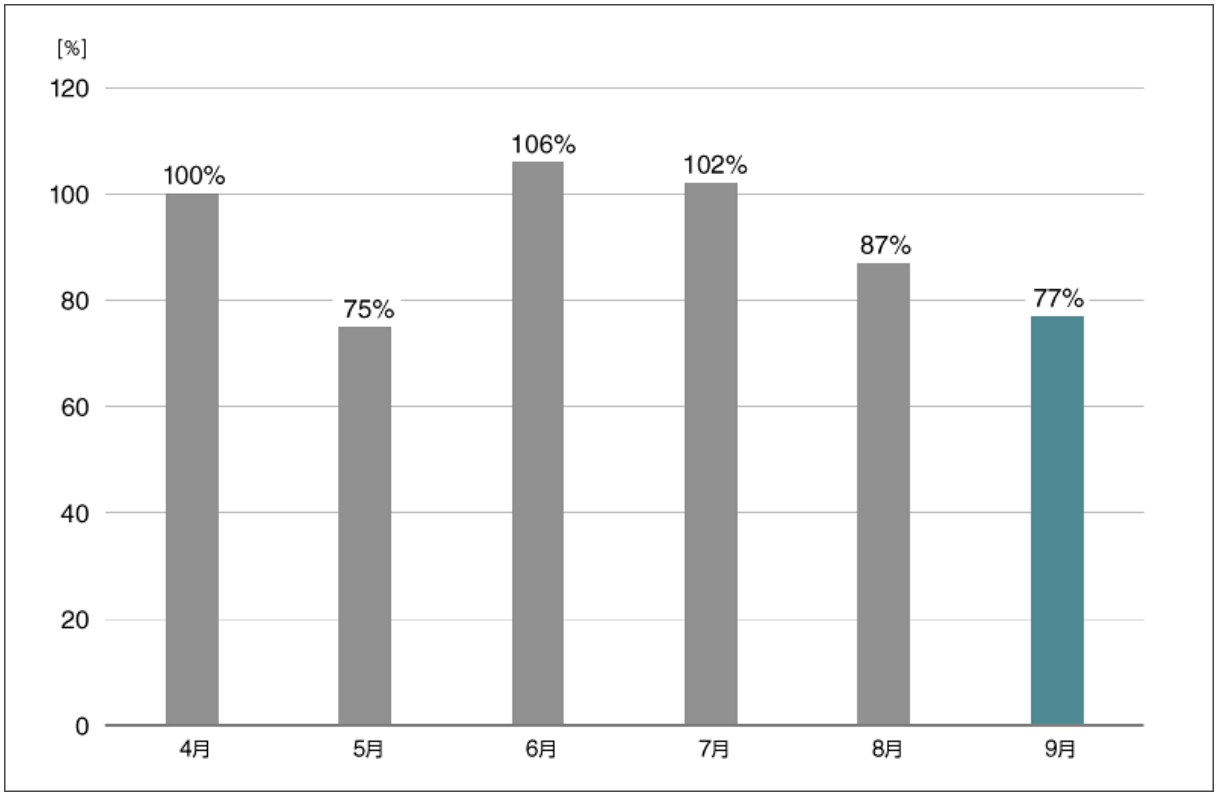
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2025 年 9 月マルウェア検出状況

2025 年 9 月（9 月 1 日～9 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 4 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。

2025 年 9 月の国内マルウェア検出数は、2025 年 8 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

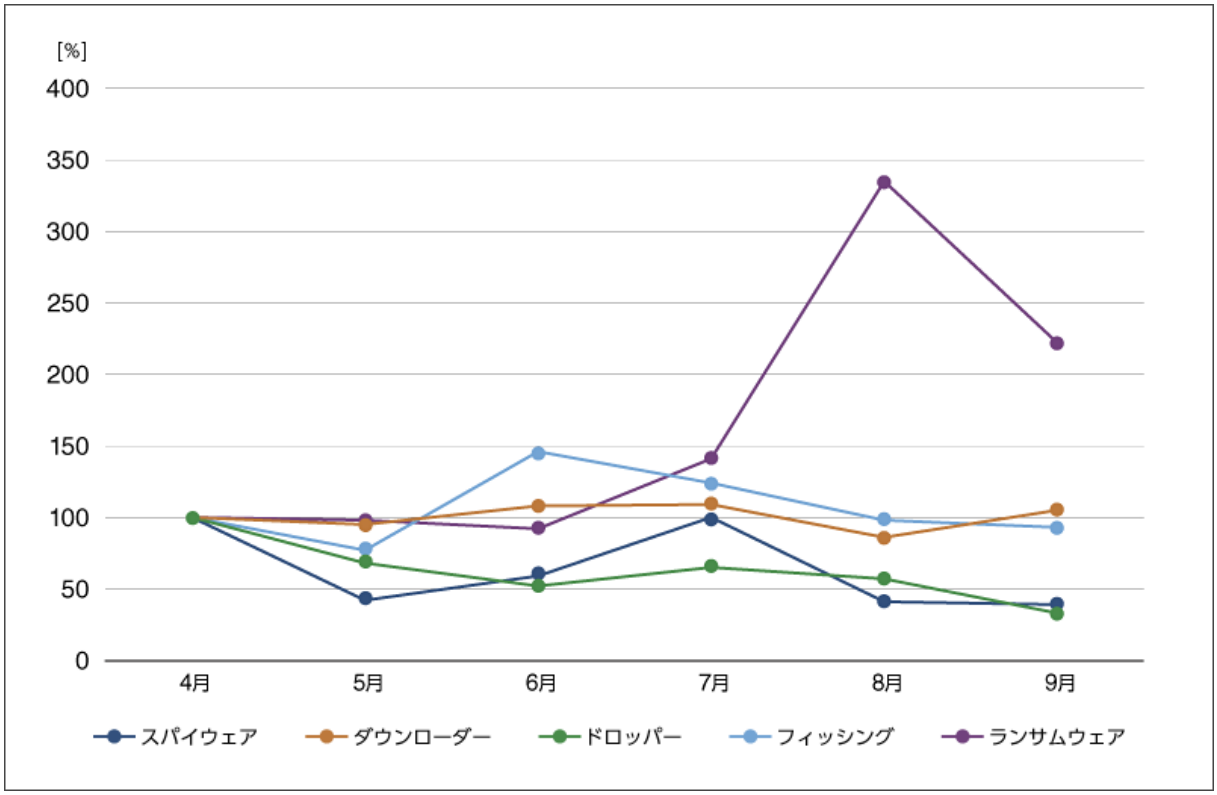
国内マルウェア検出数*2 上位（2025 年 9 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	22.9%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	20.4%	アドウェア
3	DOC/Fraud	14.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Agent	2.3%	不正な JavaScript の汎用検出名
5	HTML/Phishing.Gen	1.8%	フィッシングを目的とした不正な HTML ファイル
6	HTML/Fraud	1.5%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	JS/Adware.Subprop	1.2%	アドウェア
8	Win32/TrojanDownloader.Modi Loader	1.0%	ダウンローダー
9	Win64/Agent	0.9%	不正な実行ファイルの汎用検出名
10	JS/Adware.Sculinst	0.8%	アドウェア

*2 本表には PUA を含めていません。

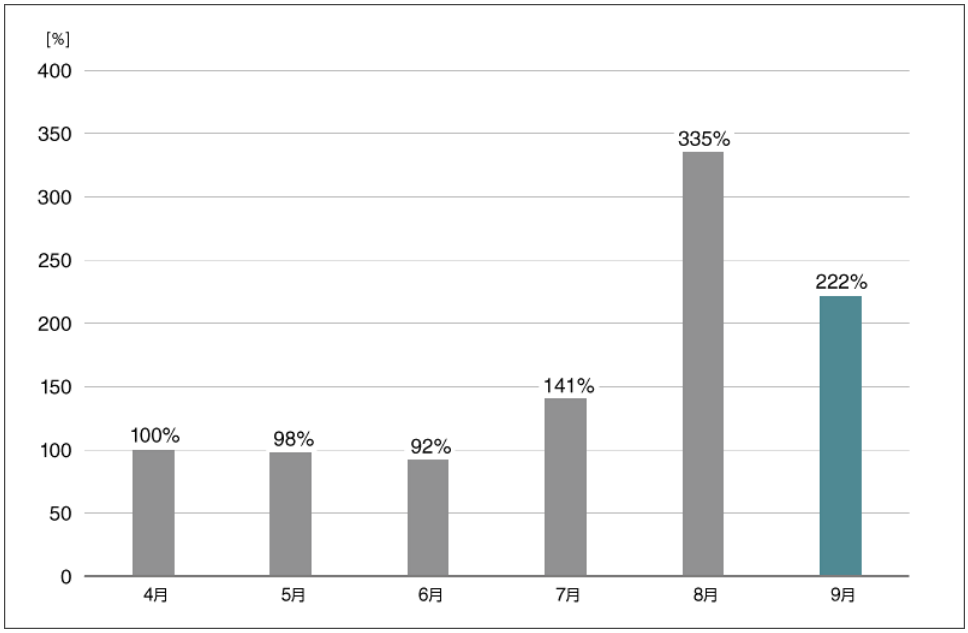
9 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL にアクセスすると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

2025 年 9 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。



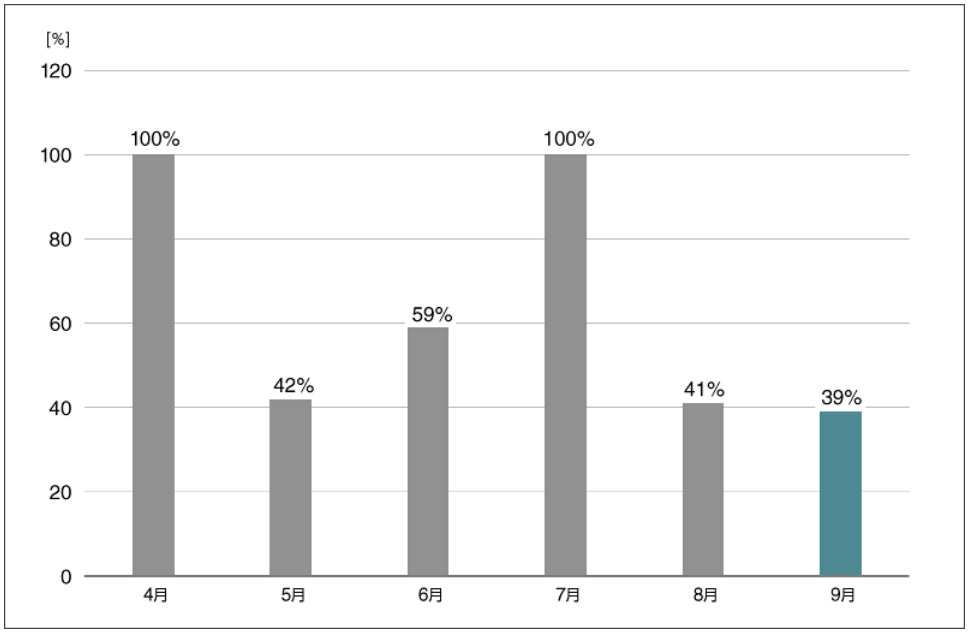
国内マルウェアの種類別検出数の推移
（2025 年 4 月の各検出数を 100%として比較）

ランサムウェアの検出数は 2025 年 8 月から大きく減少しているものの、春頃と比較すると依然高い水準を保っています。ランサムウェア以外では、フィッシングの検出数が 6 月をピークに減少傾向にあります。



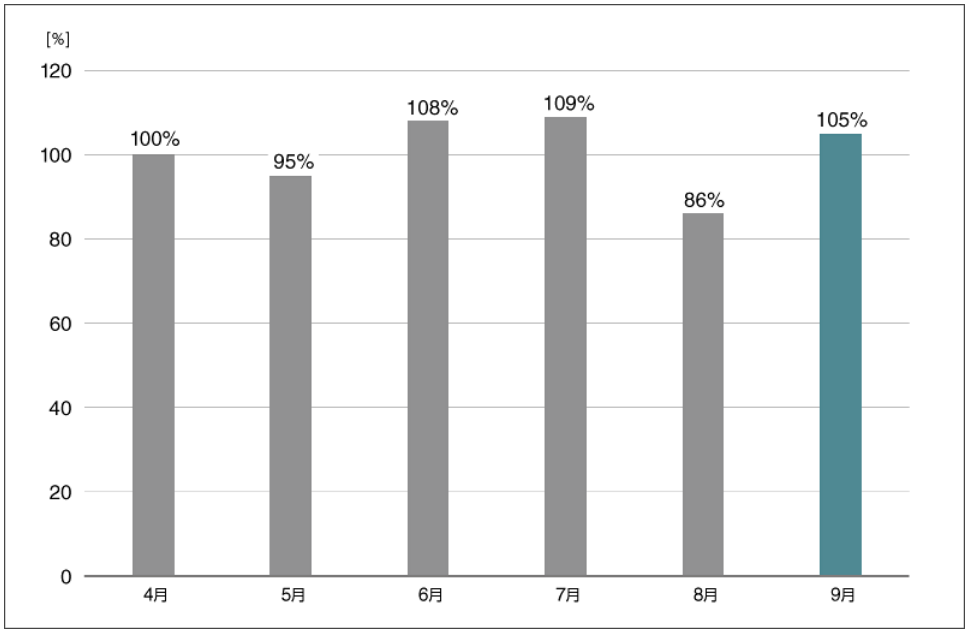
ランサムウェア検出数の推移（国内）

（2025 年 4 月の検出数を 100%として比較）



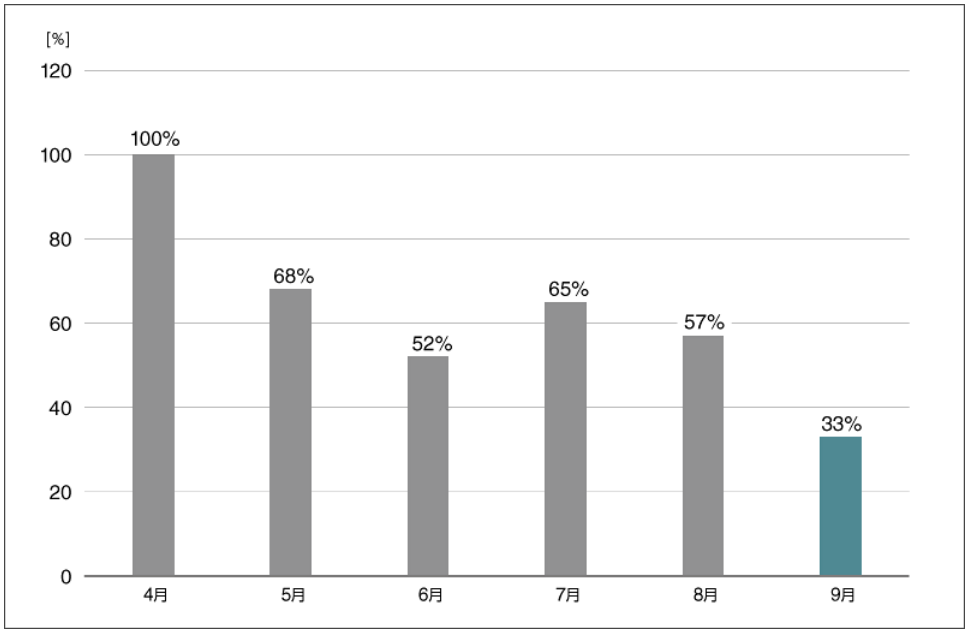
スパイウェア検出数の推移（国内）

（2025 年 4 月の検出数を 100%として比較）



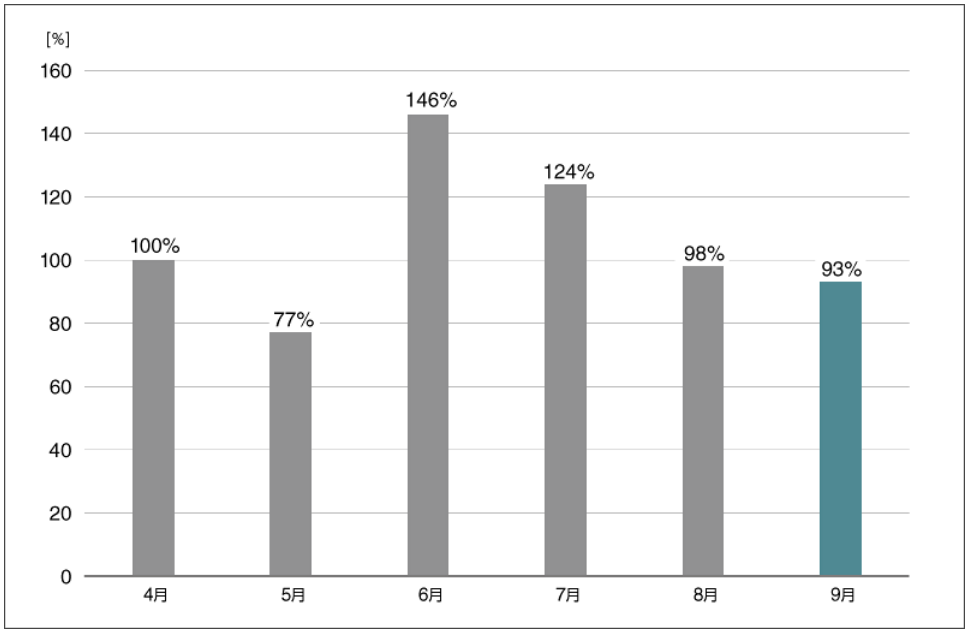
ダウンローダー検出数の推移（国内）

（2025 年 4 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）

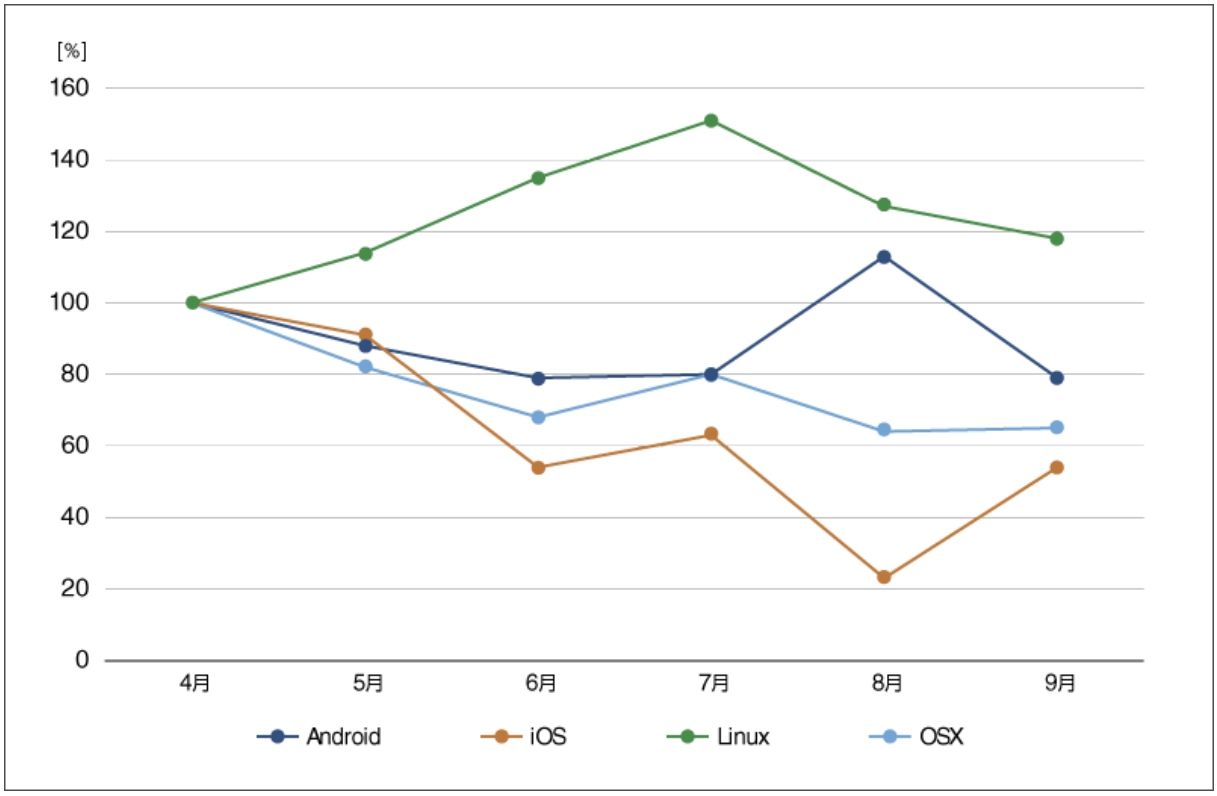
（2025 年 4 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 4 月の検出数を 100%として比較）

2025 年 9 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。

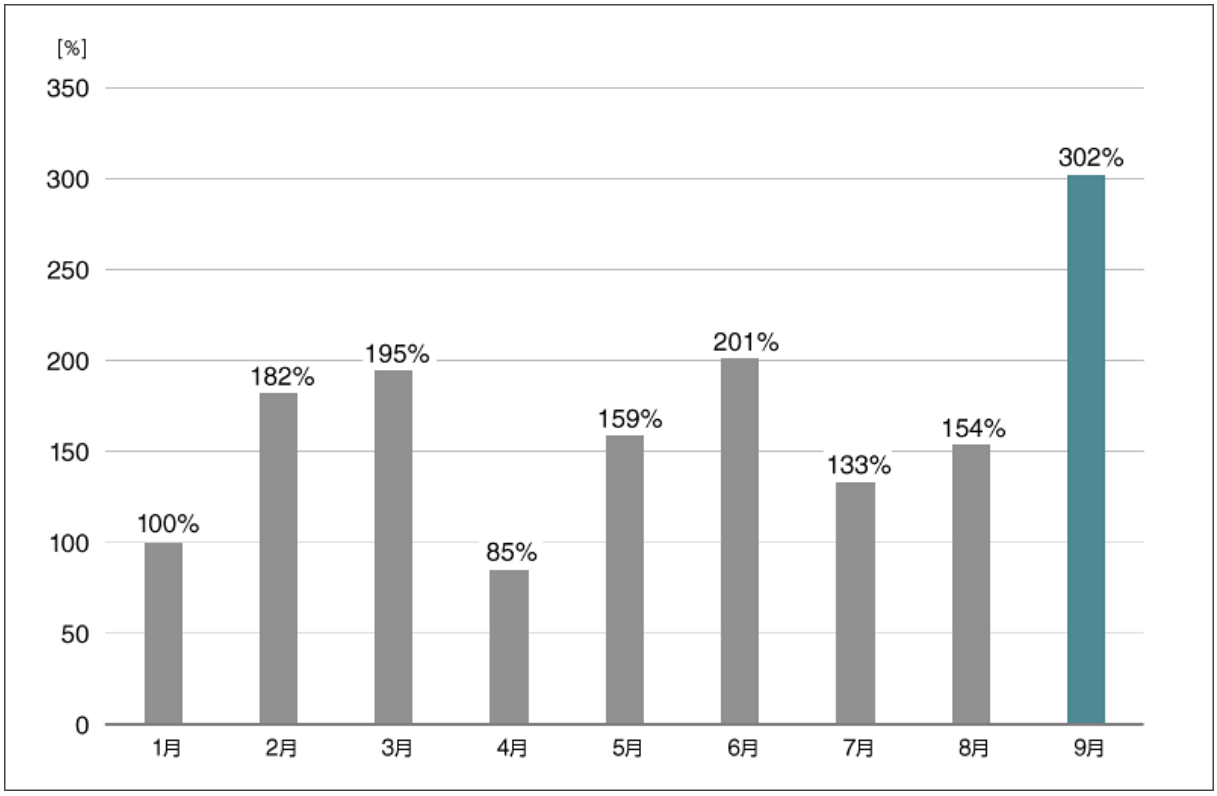


国内マルウェア OS 別の推移（Windows を除く）
（2025 年 4 月の各検出数を 100%として比較）

2025 年 9 月では iOS を狙った脅威が増加していました。一方、Android を狙った脅威は減少しています。

VBScript による脅威について

2025 年 9 月は VBScript を悪用したマルウェアの検出数が増加しており、2025 年の中では最も検出数が多い月でした。



VBScript を悪用したマルウェアの検出数月別推移（2025 年・国内）
（2025 年 1 月の検出数を 100%として比較）

2025 年 9 月に検出された VBScript を悪用したマルウェアの中で最も検出数が多かったものは、「VBS/Agent」でした。VBS/Agent は VBScript を悪用したマルウェアに対して使われる汎用的な検出名です。

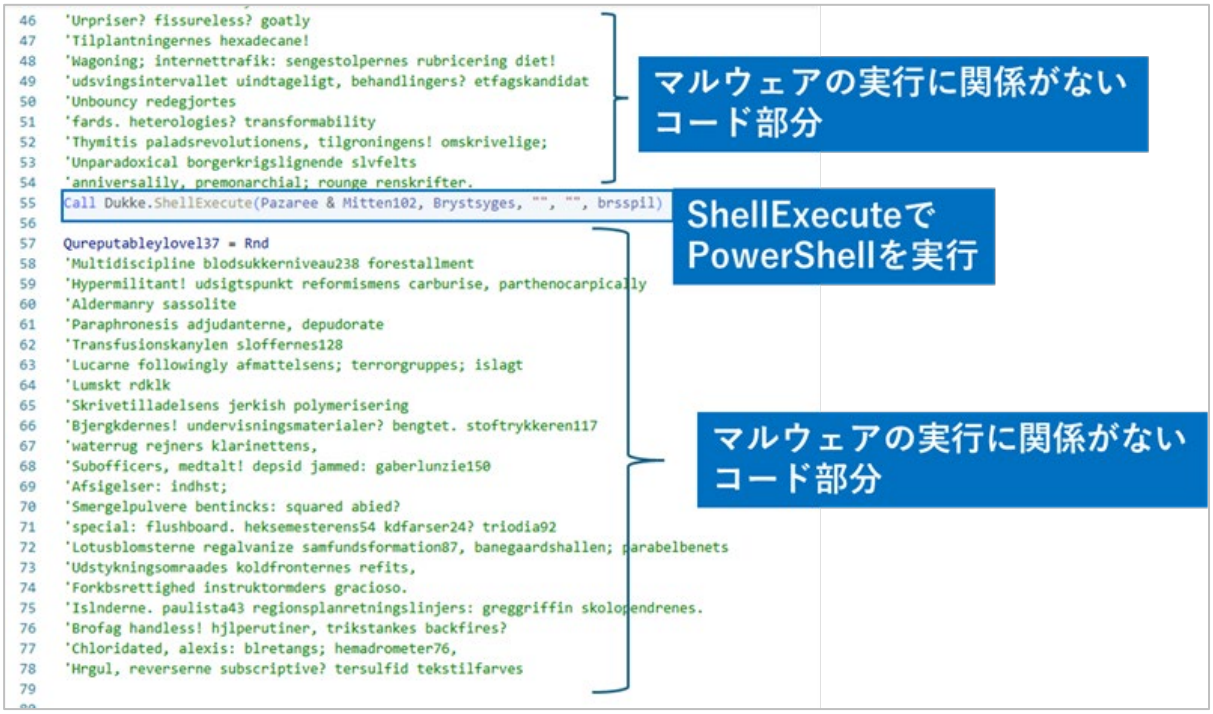
■VBScript とは

上記のように悪用が増加している Visual Basic Scripting Edition（VBScript）とは Microsoft Visual Basic に基づく強力なスクリプト言語であり、タスクの自動化やアプリケーションの制御に活用されてきました。
一方、マルウェアへの悪用も確認されています。具体例としては、攻撃者のサーバーからマルウェアをダウンロードす

るダウンローダーです。2019 年頃に流行したマルウェア Emotet のダウンローダーにも VBScript が使われていました。
VBScript が悪用されている主な理由として、開発がしやすいこと、Windows 環境であれば実行可能であることやユーザーに気づかれないように正規アプリケーションとして実行できることが挙げられます。

■2025 年 9 月に検出された VBS/Agent.TLM について

脅威となるマルウェアについて組織内で情報共有したり対策を講じたりする上で、マルウェアがどのように動作するかという情報はとても重要です。前述のとおり VBS/Agent は 2025 年 9 月に多数検出されており、この検出名には多数の亜種が存在します。その中でも検出数の多かった亜種の 1 つである VBS/Agent.TLM を例に動作を紹介します。
VBS/Agent.TLM が実行されると、攻撃者が指定した URL からファイルをダウンロードします。実行後にアクセスする URL やマルウェアサンプルデータベースの共有サイトである MalwareBazaar に掲載された情報を考慮すると、この検体はダウンローダーである Guloader の可能性が考えられます。コードには、大量のコメントを挿入する、ランダムな文字列で変数名を構成する、Replace 関数による文字列の置換を組み込んで変数の中身を隠ぺいする、などの難読化が施されています。



VBS/Agent.TLM に書かれたコードの様子

スクリプトが実行されると、Replace 関数などの処理によって難読化が解除されて、最終的に ShellExecute 関数が呼び出されて PowerShell が実行されます。PowerShell 実行後、攻撃者が指定する URL にアクセスします。

```
GET https://[redacted].pt/Tarter.inf HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Host: [redacted].pt
Connection: Keep-Alive
```

PowerShell 実行後にアクセスする通信先の様子

■今後の VBScript について

VBScript は 2027 年に廃止されることが Microsoft 社から公表されています（2024 年）。VBScript が廃止されるまでは 2 年ほど残されており、それまでは VBScript を悪用したマルウェアによる脅威の影響を受ける恐れがあります。Microsoft 社も VBScript からほかのスクリプト言語への移行を推奨しており、組織内で VBScript の実行を無効化する方法も併せて紹介しています。

移行を検討するにあたっては、まず組織内で VBScript が利用されていないかを確認する必要があります。Microsoft 社は Sysmon などのツールを用いて組織内での利用状況を調査する方法を紹介していますので、移行する際にはそちらも参考にしてください。組織内での利用を確認した場合は、JavaScript や PowerShell などのスクリプト言語への移行を推奨します。

まとめ

今月は検出数が増加した VBScript を悪用したマルウェアについて紹介しました。これらはほかのマルウェアへの感染を狙ったダウンローダーとしての悪用も確認されています。また、VBScript は 2027 年での廃止が決定していますが、それまでは VBScript を悪用したマルウェア感染の脅威が続きます。VBScript の全面無効化は効果的な対策になるので、まだ組織内で利用している場合は早めにほかのスクリプト言語に移行することを推奨します。

■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

●VBScript の利用について | Microsoft Learn
https://learn.microsoft.com/ja-jp/office/vba/outlook/how-to/using-visual-basic-to-customize-outlook-forms/about-using-vbscript-in-outlook

●VBScript deprecation: Detection strategies for Windows | Windows IT Pro Blog
https://techcommunity.microsoft.com/blog/windows-itpro-blog/vbscript-deprecation-detection-strategies-for-windows/4414325

Canon

キヤノンマーケティングジャパン株式会社