2023年
6月
JUNE

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

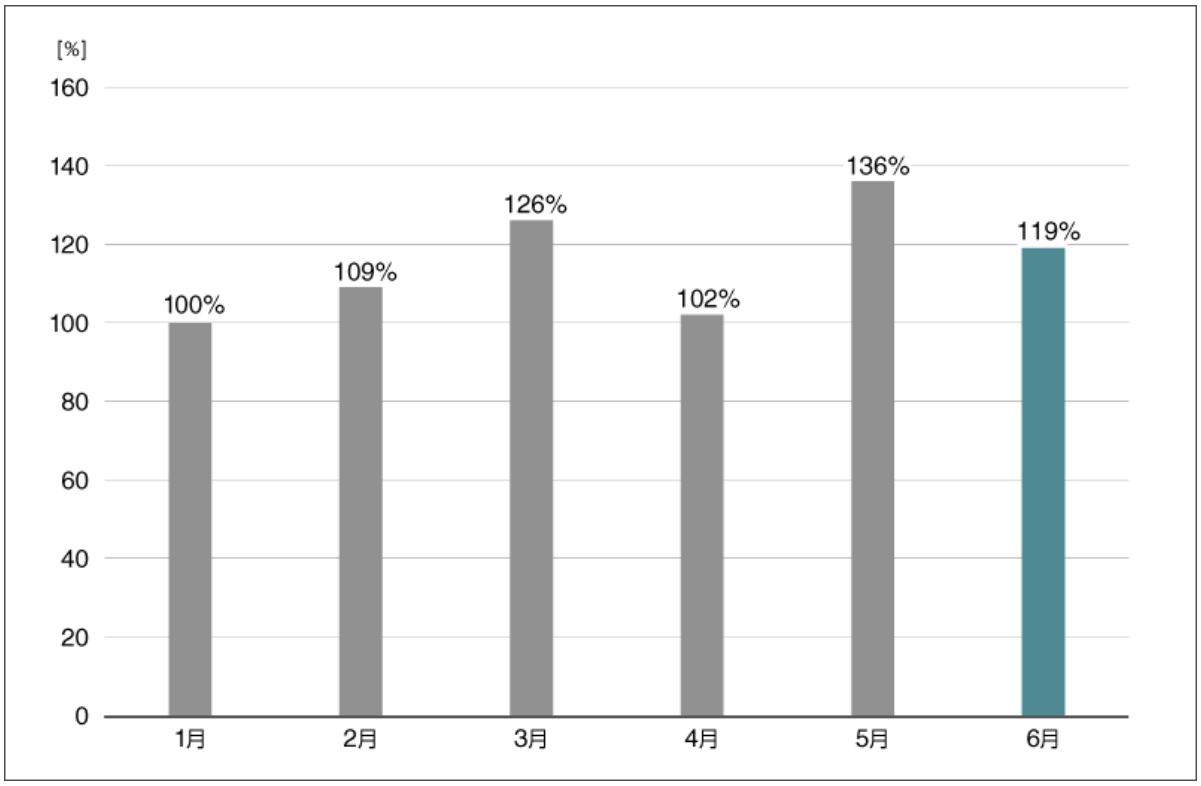
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2023 年 6 月マルウェア検出状況

2023 年 6 月（6 月 1 日～6 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

（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。

2023 年 6 月の国内マルウェア検出数は、2023 年 5 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（2023 年 6 月）

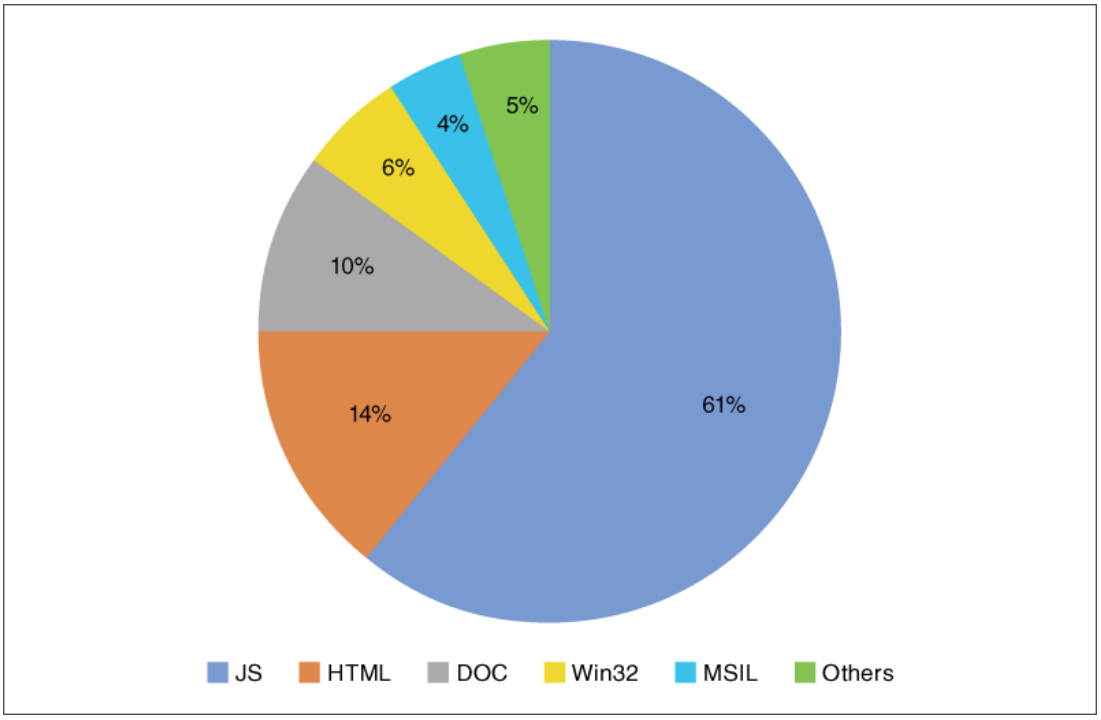
順位	マルウェア	割合	種別
1	JS/Adware.Agent	39.5%	アドウェア
2	HTML/Phishing.Agent	11.0%	メールに添付された不正な HTML ファイル
3	DOC/Fraud	9.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Adware.TerraClicks	7.0%	アドウェア
5	JS/Adware.Sculinst	1.7%	アドウェア
6	JS/Agent	1.5%	不正な JavaScript の汎用検出名
7	Win32/Exploit.CVE-2017-11882	1.4%	脆弱性を悪用するマルウェア
8	HTML/Phishing	1.0%	詐欺を目的とした不正な HTML ファイル
9	PDF/Phishing	1.0%	詐欺を目的とした不正な PDF ファイル
10	HTML/Fraud	0.9%	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。

6 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。

検出数の最も多い JS 形式マルウェア

JS 形式マルウェアは JavaScript で記述されたマルウェアであり、ESET 製品においては「JS/」というプレフィックスから始まる検出名が該当します。
6 月の概況で示したとおり、国内マルウェア検出数上位 10 件のうち、JS 形式マルウェアが 4 件と最も多く確認されました。6 月の検出数全体で見ても JS 形式マルウェアはおよそ 60%を占めており、マルウェアとして最も多いファイル形式であることがわかります。



2023 年 6 月の国内におけるファイル形式別のマルウェア検出数の割合

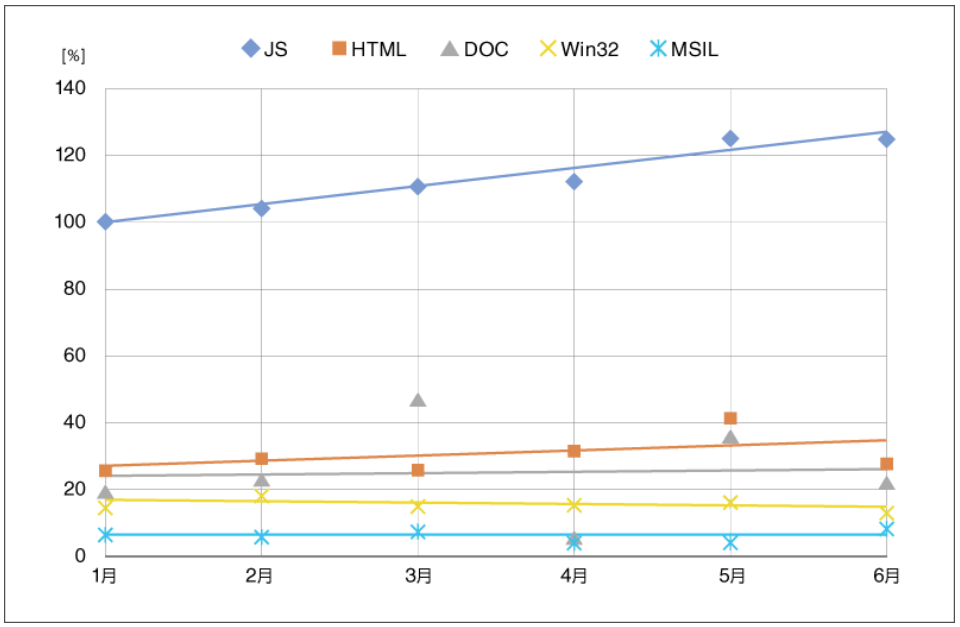
サイバーセキュリティラボが毎年公開している「サイバーセキュリティレポート[*3,4]」の中で上半期および年間におけるファイル形式別の割合を掲載していますが、国内に限定すると 2018 年以降は JS 形式が最も割合の高いマルウェアとして推移し続けています。
2023 年における JS 形式マルウェアの傾向を見てみると、2022 年以前と同様に検出数は最上位を維持し続けています。加えて、検出数の多いファイル形式上位 5 種[*5]のうち、JS 形式は検出数が増加傾向にあるマルウ

ェアの 1 つであることがわかります。

*3 2020 年以前は「マルウェアレポート」の名称で公開しています。

*4 「定期レポート」に関する記事一覧 | サイバーセキュリティ情報局

*5 2023 年 1 月～6 月における検出数の平均値で算出しました。1 位から順に JS 形式、HTML 形式、DOC 形式、Win32 形式、MSIL 形式の 5 種が該当します。



2023 年の国内におけるファイル形式別の検出数推移
（1 月の JS 形式を 100%として比較）
（図中の直線は各ファイル形式の線形近似直線を表す）

このように、JS 形式マルウェアは国内において長らく脅威が続いているマルウェアであり、2023 年以降は徐々に脅威が拡大しているため警戒が必要です。

JS 形式マルウェアの攻撃対象は広範囲

JS 形式マルウェアの検出数が多い要因として、攻撃者にとって多くのユーザーを標的にできることが考えられます。今回は 3 つの例を紹介します。

1. 悪意のあるインターネット広告

Web ブラウジングは、多くのユーザーにとって仕事やプライベートに関係なくインターネットに触れる代表的な手段の 1 つです。現在は Web ブラウジング中にインターネット広告を見かけることが一般的となっていますが、この広告に悪意のあるコンテンツを含めることによって不特定多数のユーザーを標的にすることが可能です。6 月の国内マルウェア検出数上位に該当する 4 つの JS 形式マルウェアのうち 3 つがアドウェアであることからも、国内の多くのユーザーにとって脅威となっている様子がわかります。

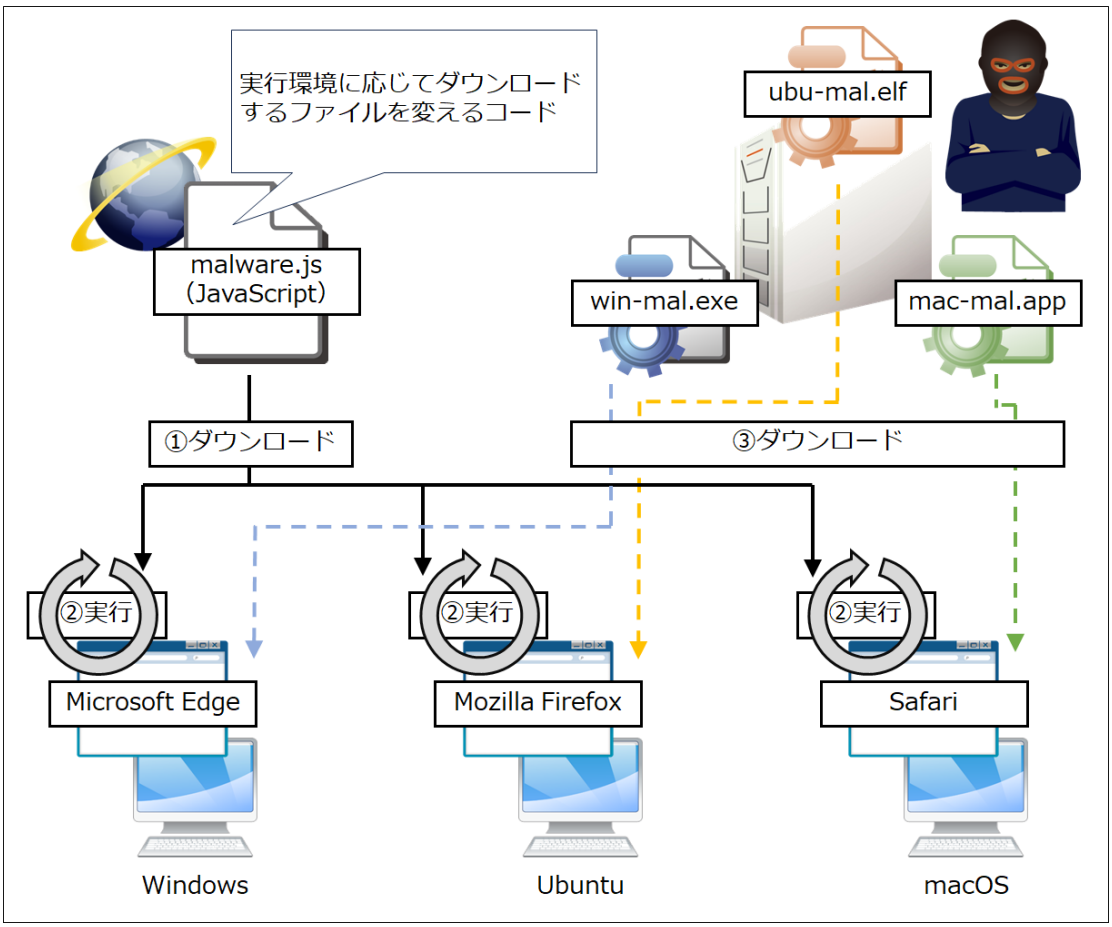
2. 実行環境に応じたマルウェアの配布

JavaScript は ECMAScript として標準化[*6] されており、互換性が高くさまざまな Web ブラウザー上で実行することができます。すなわち、さまざまな OS において Web ブラウザー上で JavaScript を実行できることに他なりません。

JavaScript において、Web ブラウザーや OS などの実行環境に関する情報を取得する方法の 1 つに、Navigator オブジェクト[*7] が挙げられます。このオブジェクトを利用することで、実行環境に適したマルウェアペイロードをダウンロードして実行させることができる可能性があります。

*6 TC39 | Ecma International

*7 Navigator - Web API | Mozilla Foundation



実行環境に応じたマルウェア感染のイメージ

3. JavaScript をマルチプラットフォームで動作させる実行環境の存在

例えば NW.js は、Node.js[*8] に WebKit[*9] の機能を追加した実行環境であり、複数の OS 上で動作するマルチプラットフォームの実行環境でもあります。Ransom32 と呼ばれる JavaScript ベースのランサムウェア[*10] は、この NW.js 上で動作するように設計されているため、NW.js がインストールされた環境であれば OS に関係なく動作します。このように条件が整っている場合、JS 形式マルウェアは複数の OS で動作し得るため標的の範囲が広いマルウェアであると言えます。

*8 クライアントサイドであるブラウザー上で動作する JavaScript を、サーバーサイドで実行できるようにする実行環境です。

*9 Web ページを整形して表示するための HTML レンダリングエンジンです。

*10 Die erste Ransomware in JavaScript: Ransom32 | Emsisoft

まとめ

今回は JS 形式マルウェアについて紹介しました。国内においては最も検出数の多いマルウェアであるため対策は必須です。JS 形式は Web ブラウザー以外の環境でも実行できる場合があります。よって Web ブラウザーを最新の状態に保つこと以外にも、OS のバージョンアップやセキュリティ製品の導入なども実施して、組織の端末を保護するようにしてください。

■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。

引用・出典元

■「定期レポート」に関する記事一覧 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/keyword_topics_list/?tag_id=200
■TC39 | Ecma International
https://www.ecma-international.org/technical-committees/tc39/
■Navigator - Web API | Mozilla Foundation
https://developer.mozilla.org/ja/docs/Web/API/Navigator
■Die erste Ransomware in JavaScript: Ransom32 | Emsisoft
https://www.emsisoft.com/en/blog/21077/meet-ransom32-the-first-javascript-ransomware/

Canon

キヤノンマーケティングジャパン株式会社