2023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

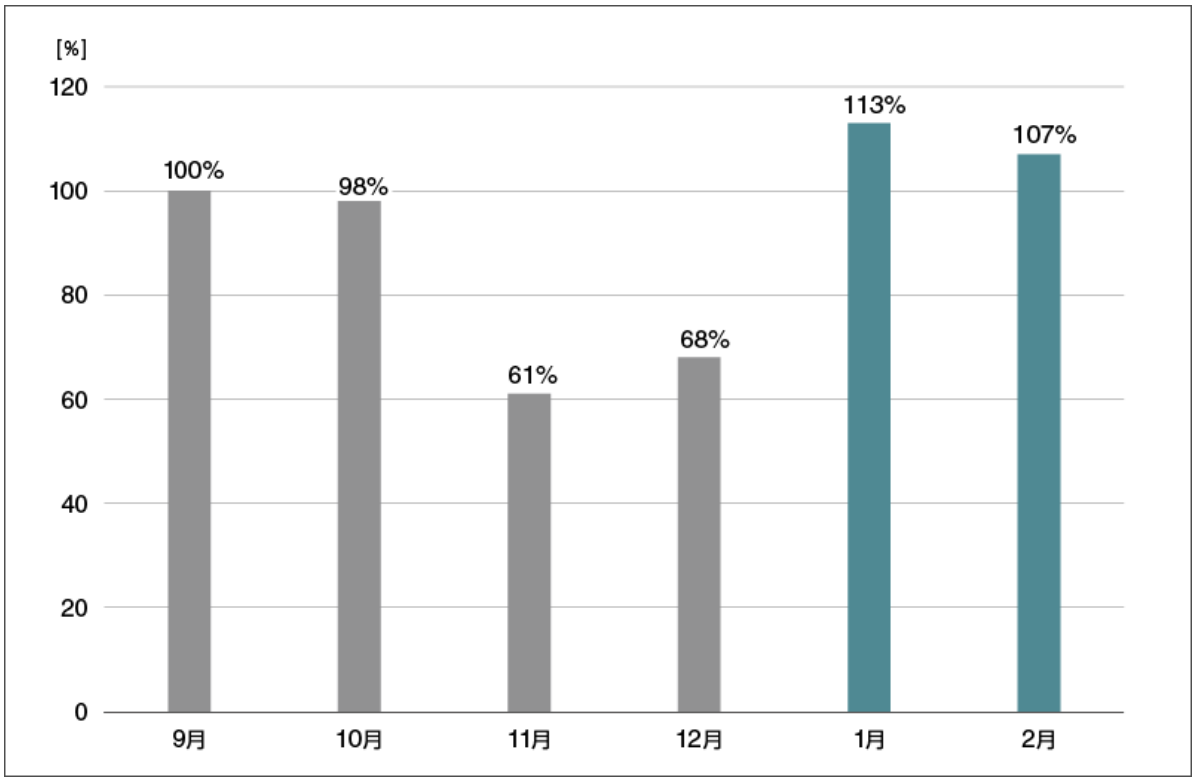
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2023 年 1 月･2 月マルウェア検出状況

2023 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 28 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
(2022 年 9 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 1 月と 2 月の国内マルウェア検出数は、2022 年 12 月と比較して大きく増加しました。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 1 月･2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	14.8%	アドウェア
2	HTML/ScrInject	11.7%	HTML に埋め込まれた不正スクリプト
3	JS/Packed.Agent	8.6%	パックされた不正な JavaScript の汎用検出名
4	DOC/Fraud	5.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Adware.TerraClicks	4.6%	アドウェア
6	HTML/Phishing.Agent	4.4%	メールに添付された不正な HTML ファイル
7	HTML/FakeAlert	3.6%	偽の警告文を表示させる HTML ファイル
8	JS/Adware.Sculinst	2.3%	アドウェア
9	HTML/Pharmacy	2.2%	違法薬品の販売サイトに関連する HTML ファイル
10	MSIL/Kryptik	1.5%	難読化された MSIL で作成されたファイルの汎用検出名

国内マルウェア検出数*2 上位（2023 年 1 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	14.3%	アドウェア
2	HTML/ScrInject	11.9%	HTML に埋め込まれた不正スクリプト
3	JS/Packed.Agent	10.0%	パックされた不正な JavaScript の汎用検出名
4	DOC/Fraud	7.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Adware.TerraClicks	5.1%	アドウェア
6	HTML/Pharmacy	4.2%	違法薬品の販売サイトに関連する HTML ファイル
7	HTML/Phishing.Agent	3.8%	メールに添付された不正な HTML ファイル
8	HTML/FakeAlert	2.4%	偽の警告文を表示させる HTML ファイル
9	JS/Adware.Sculinst	2.3%	アドウェア
10	MSIL/Kryptik	1.1%	難読化された MSIL で作成されたファイルの汎用検出名

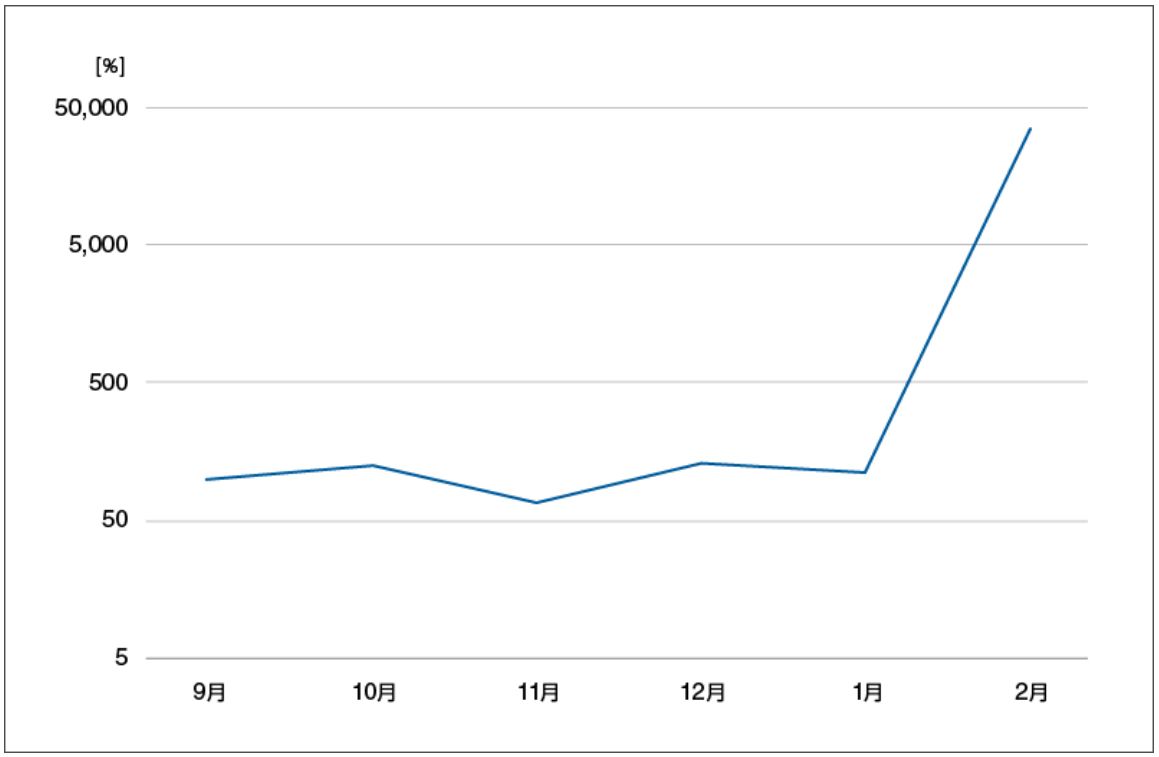
国内マルウェア検出数*2 上位（2023 年 2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	15.4%	アドウェア
2	HTML/ScrInject	11.5%	HTML に埋め込まれた不正スクリプト
3	JS/Packed.Agent	7.1%	パックされた不正な JavaScript の汎用検出名
4	HTML/Phishing.Agent	4.9%	メールに添付された不正な HTML ファイル
5	HTML/FakeAlert	4.8%	偽の警告文を表示させる HTML ファイル
6	JS/Adware.TerraClicks	4.2%	アドウェア
7	DOC/Fraud	4.1%	詐欺サイトのリンクが埋め込まれた DOC ファイル
8	JS/Adware.Sculinst	2.2%	アドウェア

9	MSIL/Kryptik	1.9%	難読化された MSIL で作成されたファイルの汎用検出名
10	JS/TrojanDownloader.Ifram	1.4%	ダウンローダー

*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.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。
1 月と 2 月の特徴として、2 月における JS/TrojanDownloader.Iframe の検出数増加が挙げられます。直近 6 ヶ月の検出状況を見ても、検出数が約 500 倍増加しています。

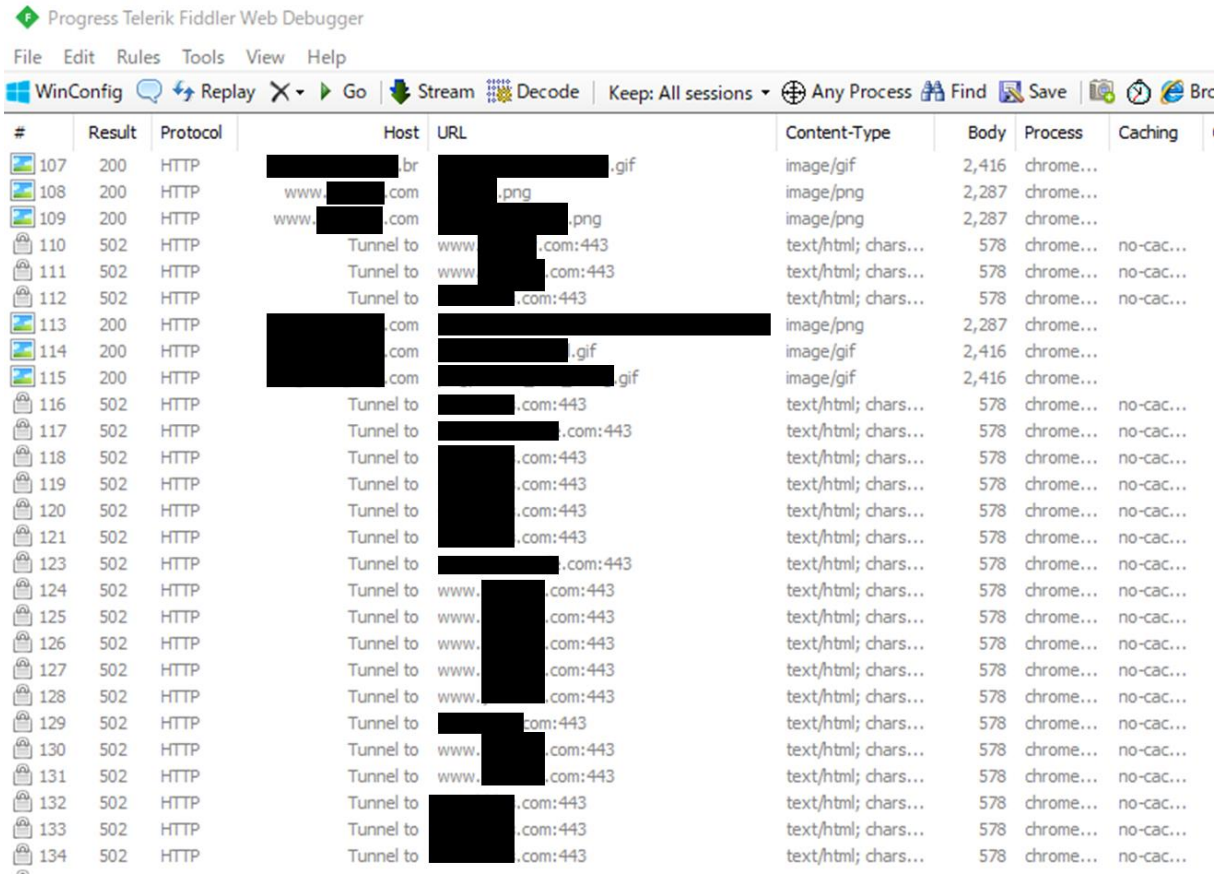


JS/TrojanDownloader.Iframe の検出数月別推移（国内･2022 年 9 月～2023 年 2 月）
（2022 年 9 月の検出数を 100%として比較、縦軸を対数軸として表記）

JS/TrojanDownloader.Iframe は、悪意のあるファイル/スクリプトのダウンロードや悪意のあるランディングページにリダイレクトさせる JavaScript の検出名です。通常、HTML ファイルの iframe が悪用され、悪意のある

コードが埋め込まれています。iframe とは、HTML ページにほかの Web ページを埋め込むことを可能にする HTML の要素の 1 つです。iframe の悪用には、iframe タグに悪意のある URL を直接埋め込む手法があります。iframe タグに URL を直接埋め込む手法は、2022 年の macOS を狙ったマルウェアの配布にも悪用されていました。改ざんされた正規サイトや攻撃者が用意した偽サイトといった Web サイトが感染経路の場合、1 つの Web サイトで不特定多数のユーザーを対象にできるメリットが攻撃者にあると考えられます。

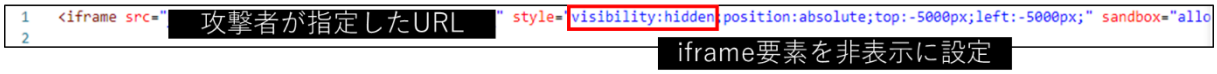
続けて、今回確認した JS/TrojanDownloader.Iframe の動作を紹介します。
検体の 1 つをオフライン環境で読み込むと、Web サイトの表示と同時にさまざまな URL へアクセスを行います。
検体を読み込んだときの通信が、下図です。



検体を読み込んだときの通信

今回の通信先によるマルウェアのダウンロードは確認できませんでしたが、リダイレクト先でスクリプトのダウンロード・実行が行われる可能性が考えられます。

また、別の検体には、以下のコードが書かれていました。



今回確認した検体の 1 つに書かれたコード

iframe タグには、style 属性に visibility:hidden が設定されています。これにより、iframe 要素を非表示にすることができます。これによって、ユーザーに見えない状況で、任意の動作が実行される恐れがあります。
今回紹介した脅威の被害に遭わないためにも、日頃からアクセスする Web サイトはブックマーク登録を行い、ブックマークからアクセスすることが重要です。

2023 年 1 月･2 月では、多数の JS/TrojanDownloader.Iframe 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、セキュリティ製品を正しく利用することや利用しているブラウザーを最新の状態に保つことが重要です。また、管理している Web サイトが悪用されないために、サーバーなどのハードウェアや CMS をはじめとしたコンポーネントの脆弱性に対応することが重要です。ベンダーや機関から公表される脆弱性情報を収集してください。

■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

■クリックジャッキング｜サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00055.html

■Watering hole deploys new macOS malware, DazzleSpy, in Asia | WeliveSecurity
https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

Canon

キヤノンマーケティングジャパン株式会社