2021年
3月
MARCH

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

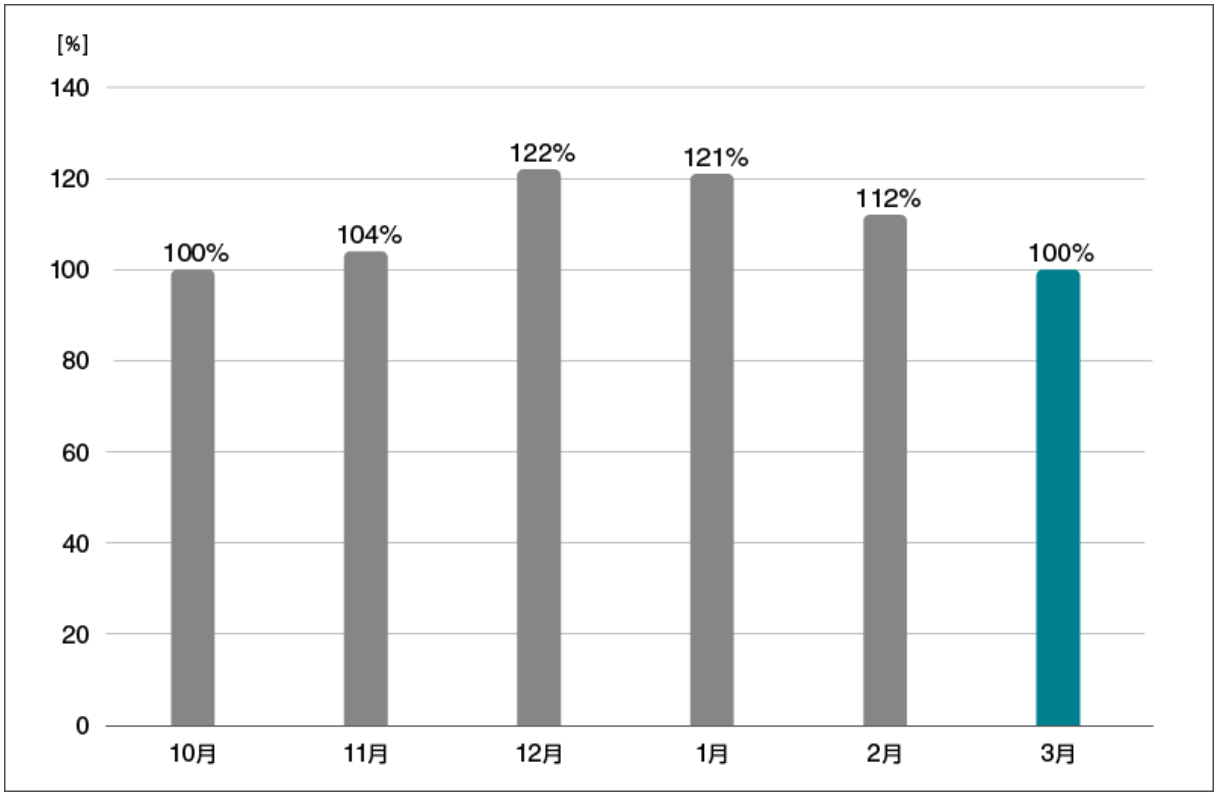
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア 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。

ショートレポート「2021 年 3 月マルウェア検出状況」

2021 年 3 月（3 月 1 日～3 月 31 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

(2020 年 10 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。

2021 年 3 月の国内マルウェア検出数は、2021 年 2 月に引き続いて減少しています。検出されたマルウェアの内訳は以下のとおりです。

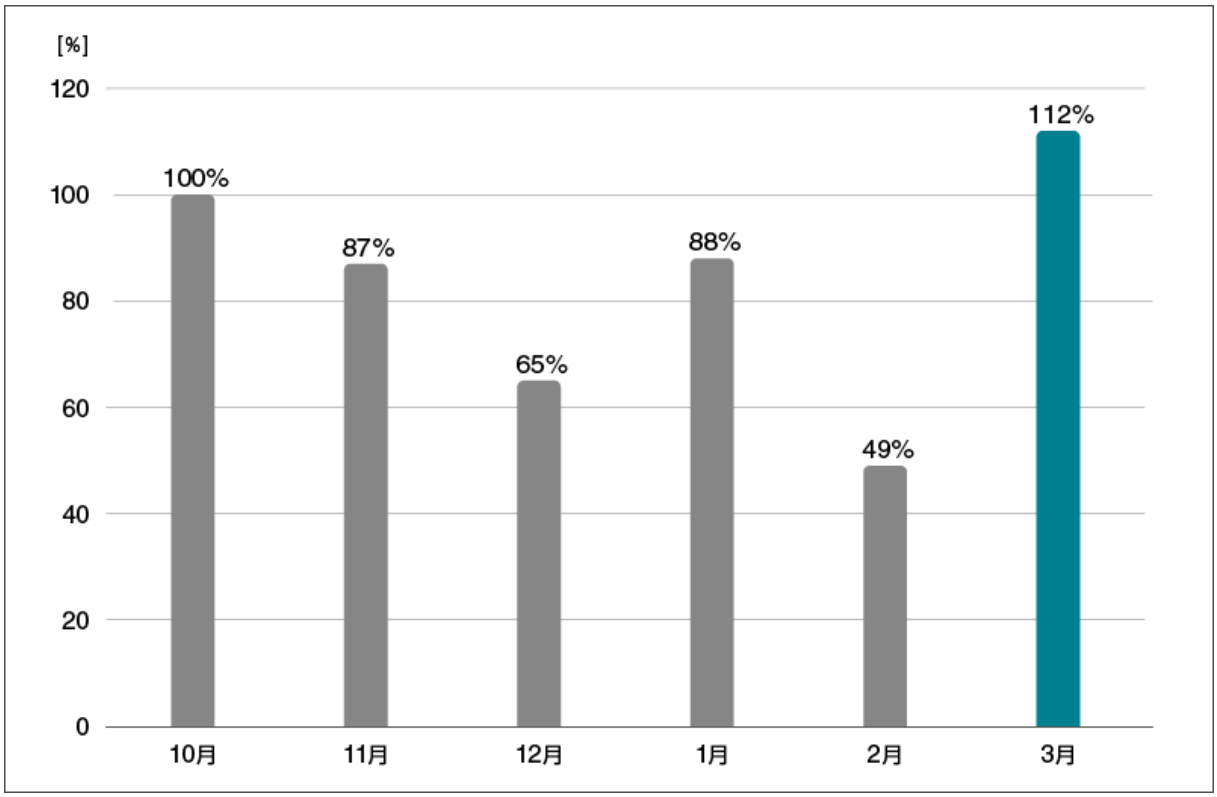
国内マルウェア検出数*2 上位（2020 年 3 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	17.6%	アドウェア
2	JS/Adware.Sculinst	8.6%	アドウェア
3	HTML/Phishing.Agent	8.4%	メールに添付された不正な HTML ファイル
4	JS/Adware.TerraClicks	5.8%	アドウェア
5	JS/Adware.Subprop	4.6%	アドウェア
6	VBA/TrojanDownloader.Agent	2.9%	ダウンローダー
7	HTML/ScrInject	2.9%	HTML に埋め込まれた不正スクリプト
8	JS/Adware.PopAds	1.9%	アドウェア
9	DOC/Fraud	1.1%	詐欺サイトのリンクが埋め込まれた doc ファイル
10	HTML/FakeAlert	0.7%	偽の警告文を表示させる HTML ファイル

*2 本表には PUA を含めていません。

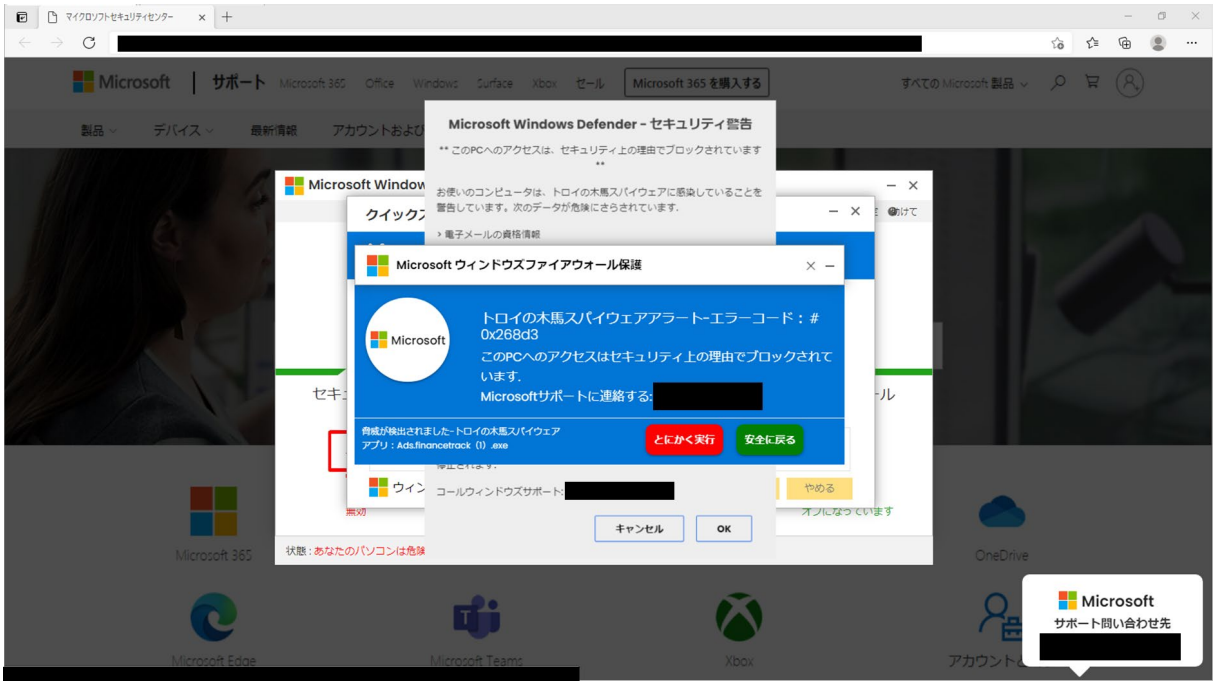
3 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

3 月は、大きな警告音と共に偽の警告文を表示させる偽警告詐欺を目的とした HTML ファイルを検出しています。検出数第 10 位の HTML/FakeAlert は、先月と比較して検出数が増加しています。



直近 6 カ月における HTML/FakeAlert の月別推移（国内）
(2020 年 10 月の検出数を 100%として比較)

HTML/FakeAlert は、偽の警告文を表示させる HTML ファイルです。Web ページにアクセスした際に、大きな警告音と共に偽の警告文を表示させます。偽の警告文は、正規メーカーを騙ったものなどがあります。確認されている警告文の中には、Windows Defender によるマルウェアの検知を騙った警告文があります。偽の警告文について Microsoft 社や消費者庁からも注意喚起が行われています。



HTML/FakeAlert のサンプルの 1 つにアクセスした時の画面

Microsoft サポートの HP を切り取った画像を悪用することで、ユーザーが Microsoft 社の Web サイトへアクセスしていると勘違いさせようとしています。また、画面に表示されている通知や電話番号は Windows Defender や Microsoft サポートによるものではありません。ユーザーは画面に表示されているボタンを操作することができず、攻撃者が用意した電話番号への電話を促されます。このようにユーザーに電話をかけさせることで、サポート料金として金銭の要求や、国際電話による多額の通信料金を発生させるといった目的が考えられます。国際電話については、その国のユーザーを対象としていることやユーザーへの嫌がらせとして多額の通信料金を発生させていることが考えられます。また、「国際ワン切り詐欺」と呼ばれる詐欺のように、国際電話をかけさせることで、攻撃者が利益を得る方法を利用している可能性があります。

ブラウザの言語設定の取得

```
<script language="JavaScript" type="text/javascript">
    var lang = window.navigator.language || navigator.userLanguage;
    lang = lang.substr(0, 2).toLowerCase();
```

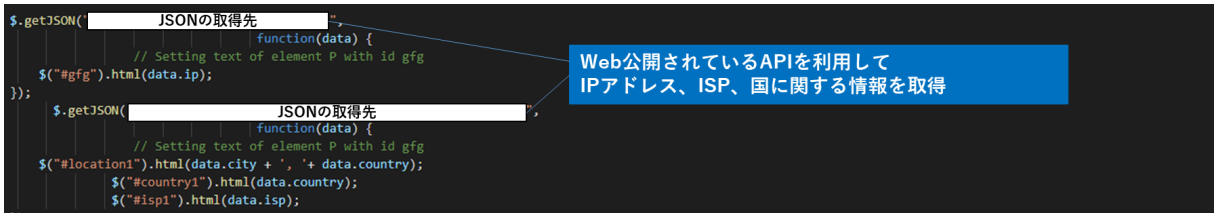
ブラウザの言語設定が日本語の場合に表示される内容

```
if (lang == "ja") {
    document.getElementById("menu").innerHTML = "製品とサービス     [redacted] ブログ     サポート     無料体験版";
    document.getElementById("menu_b").innerHTML = "日本 | 利用規約 | 使用許諾契約 | プライバシーポリシー | 採用情報 | クッキー | サイトマップ | システムの状態";
    document.getElementById("head1").innerHTML = "[redacted]";
    document.getElementById("head2").innerHTML =
        "[redacted]
}
```

指定したHTML内の要素を書き換えている

HTML/FakeAlert のサンプルの 1 つに書かれているコード

HTML ファイル内には、画面上に表示させる内容が書かれています。また、上記のサンプルでは動作していませんでしたが、Web ブラウザーの言語設定を読み取ることで表示する内容を変えるコードも書かれていました。表示する言語やメッセージを変更することで、ユーザーにより本物のページと思わせられることや 1 つの HTML ファイルで多くのユーザーを対象にできるメリットがあると考えられます。



HTML/FakeAlert の別のサンプルに書かれていたコード

他のサンプルでは、アクセスしたユーザーの IP アドレス、ISP や国の情報を画面上に表示させるために情報を取得するコードが書かれているものもありました。取得には、Web 上に公開されている既存の API などを利用しています。情報を表示させることでユーザーをパニックにさせ、冷静な判断をさせないためだと考えられます。

ご紹介したように、3 月は偽警告詐欺を目的とした HTML ファイルを検出しています。大きい警告音や偽の警告文によって不安を煽る Web サイトが多数確認されています。これらの被害に遭わないためにも、セキュリティ製品を正しく利用することが重要です。併せて、普段利用する Web サイトはブックマークからアクセスするなどの対策も重要です。
また、インターネットに書かれている電話番号へ電話をかける際は、正しい電話番号かどうかを事前に検索することも重要です。

■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. ESET 製品の検出エンジン（ウイルス定義データベース）を最新にアップデートする
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おります。
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）を最新にアップデートしてください。

2. OS のアップデートを行い、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い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する

マルウェアの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく

万が一マルウェアに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。
念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る

「知らない人」よりも「知っている人」の方がマルウェアに感染するリスクは低いと考えられます。マルウェアという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

※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

■マルウェア情報局『「Windows セキュリティシステムが破損」というアラートにご用心』
https://eset-info.canon-its.jp/malware_info/special/detail/200609.html

Canon

キヤノンマーケティングジャパン株式会社