2021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

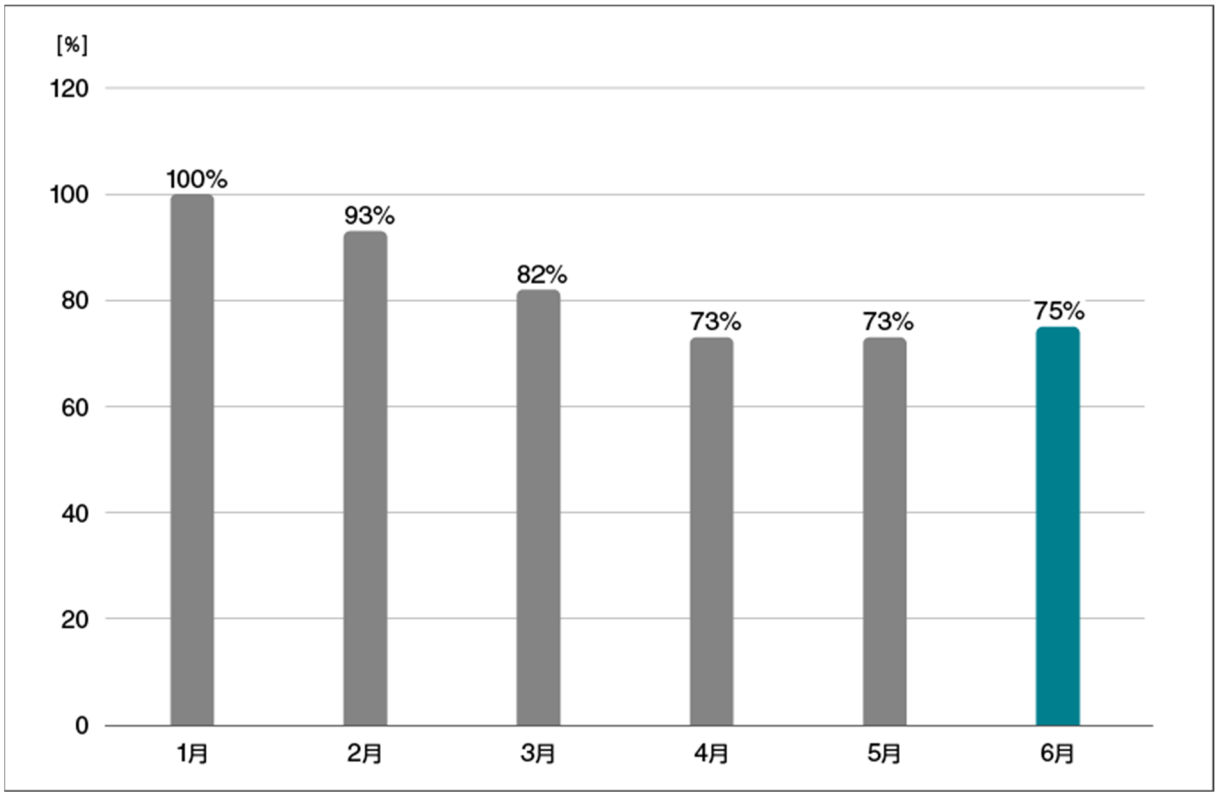
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 6 月マルウェア検出状況」

2021 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

(2021 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。

2021 年 6 月の国内マルウェア検出数は、2021 年 5 月と比較して微増しました。検出されたマルウェアの内訳は以下のとおりです。

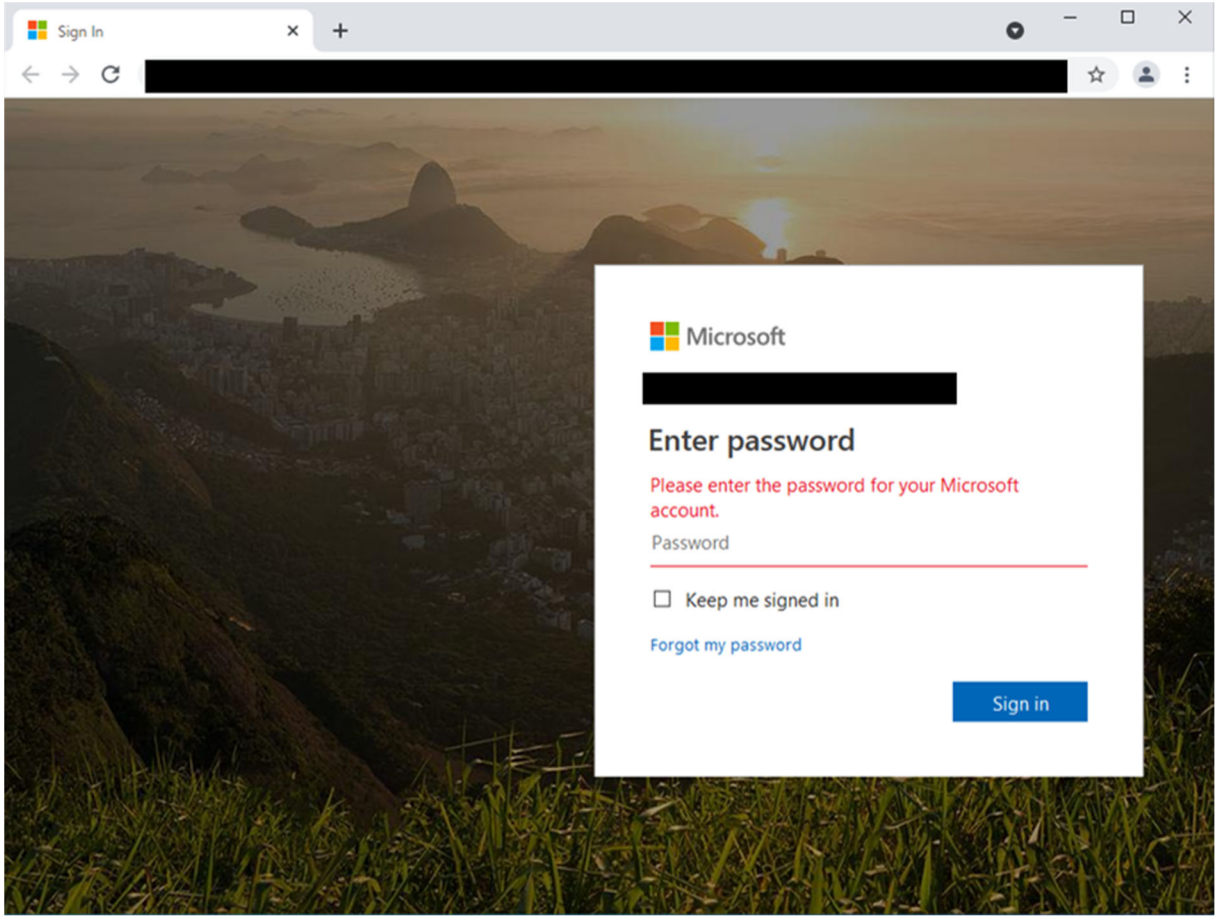
国内マルウェア検出数*2 上位（2021 年 6 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	19.2%	アドウェア
2	JS/Adware.Sculinst	9.7%	アドウェア
3	DOC/Fraud	7.0%	詐欺サイトのリンクが埋め込まれた doc ファイル
4	HTML/Phishing.Agent	5.1%	メールに添付された不正な HTML ファイル
5	JS/Adware.Subprop	4.8%	アドウェア
6	JS/Adware.TerraClicks	4.3%	アドウェア
7	HTML/Refresh	2.7%	別のページに遷移させるスクリプト
8	HTML/ScrInject	2.7%	HTML に埋め込まれた不正スクリプト
9	HTML/Phishing	2.3%	詐欺を目的とした不正な HTML ファイル
10	JS/Adware.PopAds	1.6%	アドウェア

*2 本表には PUA を含めていません。

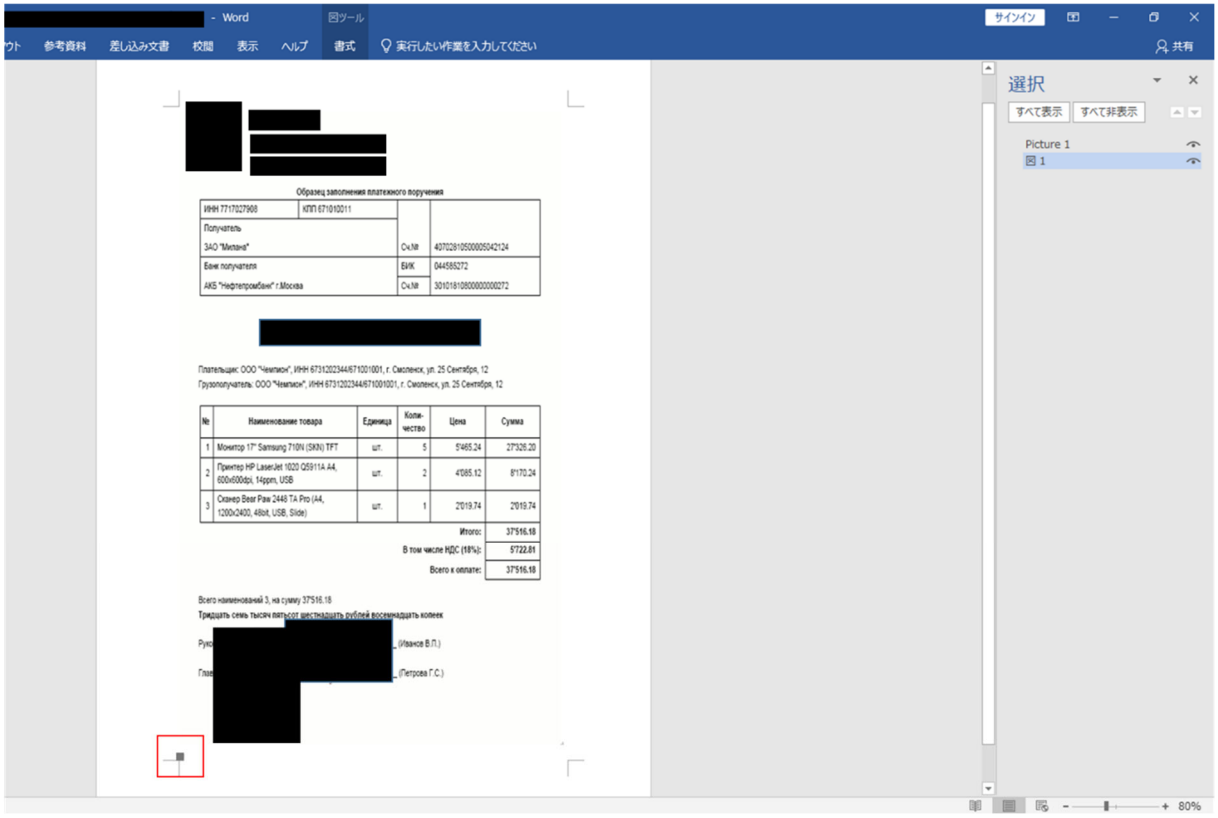
6 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

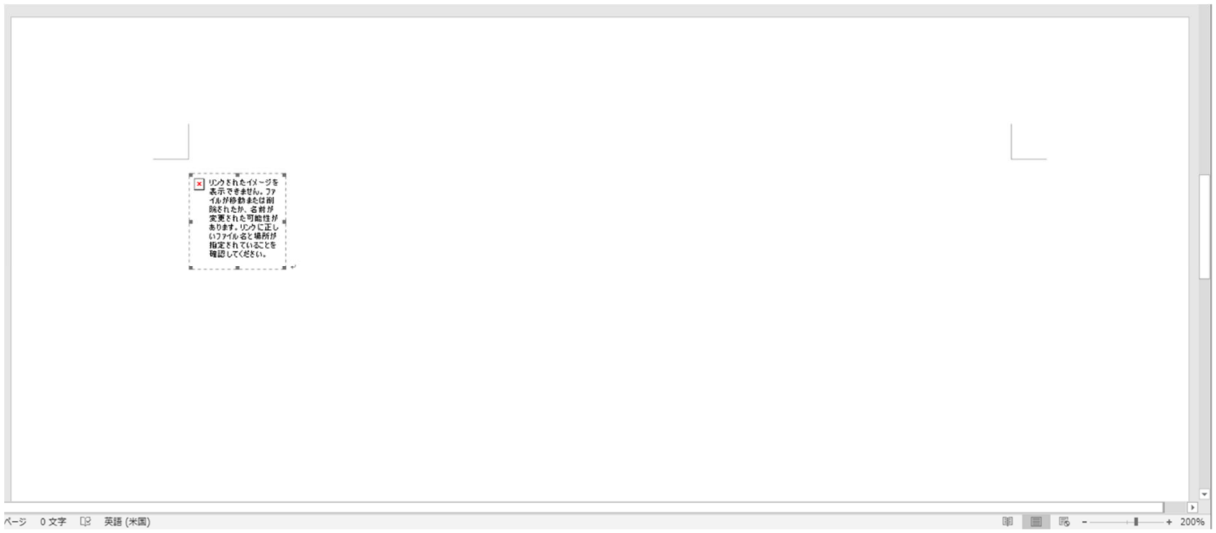
6 月の検出数上位 10 種は、すべて Web ブラウザ上で実行される脅威で構成されています。以下では、アドウェア以外に検出数の多かった HTML/Phishing.Agent と DOC/Fraud について紹介します。
HTML/Phishing.Agent は、正規の Web サイトを装いログイン情報の窃取を行う HTML ファイルです。例えば、Microsoft 社を騙った Web サイトでは、以下の画像のようにログインパスワードを入力させます。入力した情報は、攻撃者が設定した遷移先に送信されます。詳細については、2021 年 1 月・2 月のマルウェアレポートで解説しています。

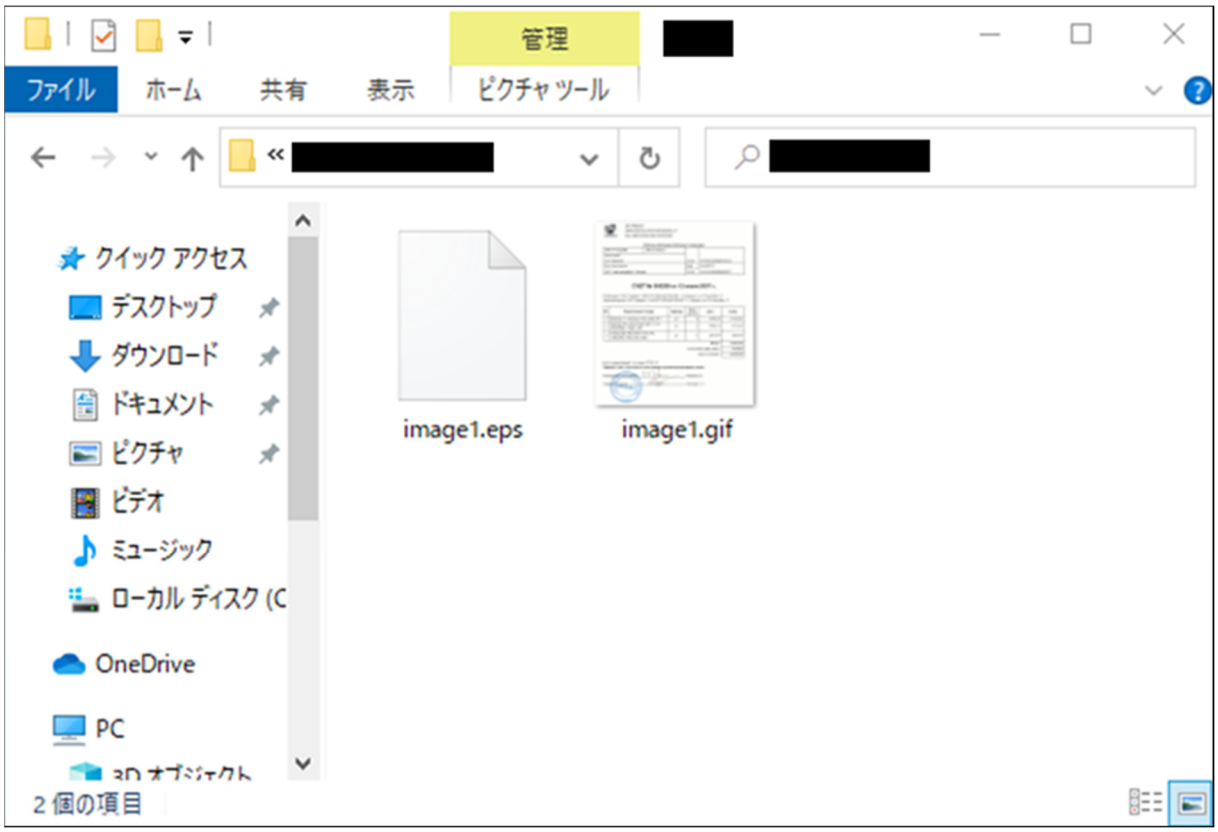


Microsoft 社を騙った Web サイトのサンプル

DOC/Fraud は、ファイルを開いた際に埋め込まれた URL リンクから不正な Web サイトへアクセスを行うことがある Word 形式のファイルです。DOC/Fraud のサンプルの中には、CVE-2015-2545 を悪用したものもあります。CVE-2015-2545 は、Office 2016、Office 2013、Office 2013 RT、Office 2010、Office 2007 に存在する不正な EPS ファイルの脆弱性です[1)]。2015 年のセキュリティアップデートにより修正されています。EPS ファイルは、「Encapsulated PostScript」の略称で PostScript を基にした Adobe 社が開発した画像ファイルです。Photoshop や Illustrator で利用可能なファイル形式です。攻撃者は Word ファイルの中に細工した EPS ファイルを埋め込むことでこの脆弱性を悪用します。







1 枚目：Word ファイルを開いたときの表示画面（赤枠部分が EPS ファイル）

2 枚目：1 枚目の画像の赤枠部分を拡大した画像

3 枚目：Word ファイルから取り出した EPS ファイル

2017 年 4 月の定例アップデート[2) 3) 4) 5)] で、Office 2016、Office 2013、Office 2010 では、EPS ファイルを Office ドキュメントに挿入する機能が既定でオフになるようになっています。2018 年 5 月以降のアップデートで、Office 2019 と Office 365 では、この機能がなくなっています。アップデートを行っていない製品では、この脆弱性を悪用される恐れがあります。脆弱性が残った古いバージョンの Office 製品を利用しているユーザーを狙ったものだと考えられます。脆弱性があるバージョンの製品を利用し続けることは危険です。早急にアップデートなどを検討することが重要です。

ご紹介したように、6 月は Web ブラウザ上で実行される脅威を多数検出しています。普段利用するサイトへのアクセスはブックマークから行い、Web サイトの URL やドメインに注意しながらアクセスすることが重要です。また、メールに記載された URL や添付された Word ファイルなどを不用意に開かないように心がけることも重要です。フィッシング対策協議会といった機関の Web サイトやセキュリティベンダーの HP（例：サイバーセキュリティ情報局のフィッシング情報など）を利用してフィッシング情報の収集を行ってください。知らないことへの対策は難しいですが、知ることで被害を未然に防げるケースもあります。

■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. 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。

引用・出典元

1) マイクロソフト セキュリティ情報 MS15-099 - 緊急
Microsoft Office の脆弱性により、リモートでコードが実行される (3089664)
2) Office 2016 用のセキュリティ更新プログラムについて 2017 年 4 月 12 日
3) Office 2013 用のセキュリティ更新プログラムについて 2017 年 4 月 12 日
4) Office 2010 用のセキュリティ更新プログラムについて 2017 年 4 月 12 日
5) 2007 Microsoft Office スイート用のセキュリティ更新プログラムについて: 2017 年 4 月 12 日

Canon

キヤノンマーケティングジャパン株式会社