2021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

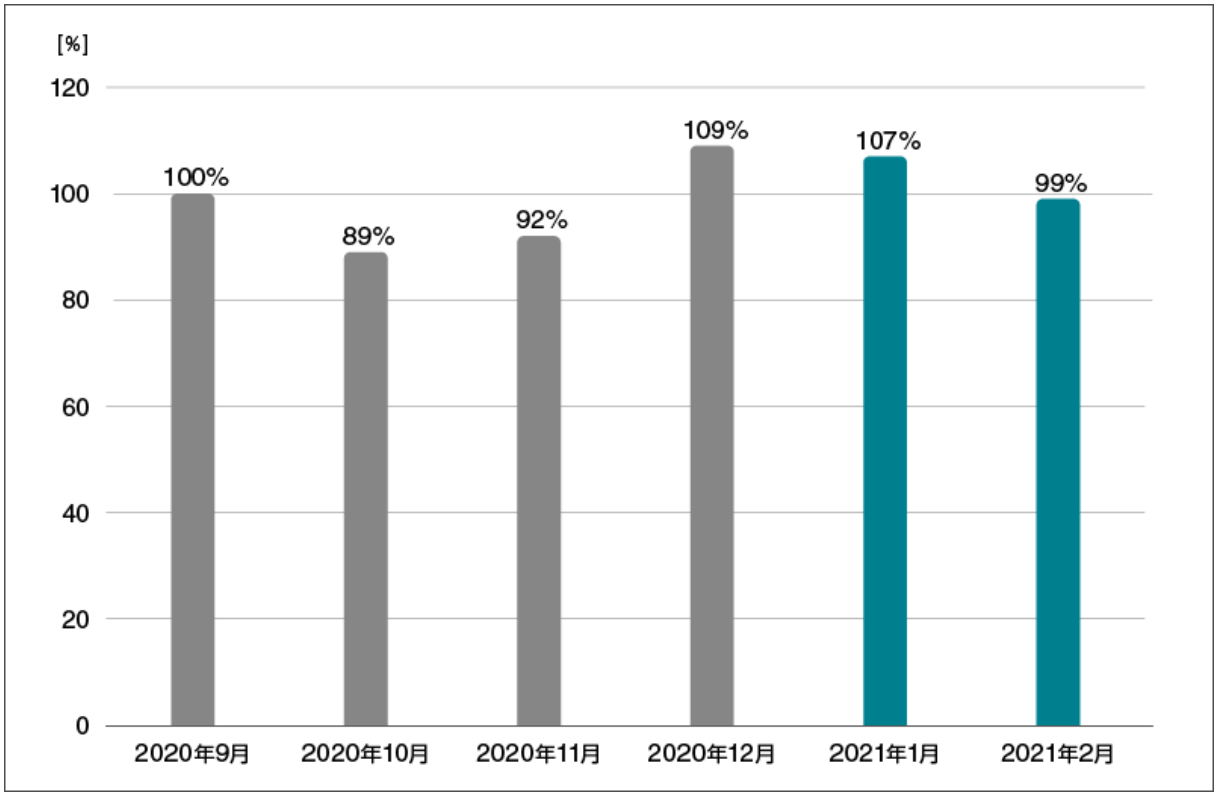
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 1 月･2 月マルウェア検出状況」

2021 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～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

(2020 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。

2021 年 1 月と 2 月の国内マルウェア検出数は、増加傾向にあった 2020 年 12 月から一転して減少しました。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（2020 年 1 月･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/Phishing.Agent	7.2%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	5.4%	アドウェア
4	JS/Adware.Subprop	4.7%	アドウェア
5	HTML/ScrInject	2.9%	HTML に埋め込まれた不正スクリプト
6	JS/Adware.Sculinst	2.2%	アドウェア
7	DOC/Fraud	2.0%	詐欺サイトのリンクが埋め込まれた doc ファイル
8	VBA/TrojanDownloader.Agent	2.0%	ダウンローダー
9	JS/Adware.PopAds	1.7%	アドウェア
10	HTML/Fraud	0.7%	詐欺サイトのリンクが埋め込まれた HTML

国内マルウェア検出数*2 上位（2021 年 1 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	15.3%	アドウェア
2	HTML/Phishing.Agent	7.3%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	5.7%	アドウェア
4	JS/Adware.Subprop	5.0%	アドウェア
5	HTML/ScrInject	2.9%	HTML に埋め込まれた不正スクリプト
6	VBA/TrojanDownloader.Agent	2.7%	ダウンローダー
7	JS/Adware.PopAds	1.7%	アドウェア
8	JS/Adware.Sculinst	1.2%	アドウェア
9	HTML/Fraud	0.8%	詐欺サイトのリンクが埋め込まれた HTML
10	MSIL/GenKryptik	0.5%	難読化された MSIL で作成されたファイルの汎用検出名

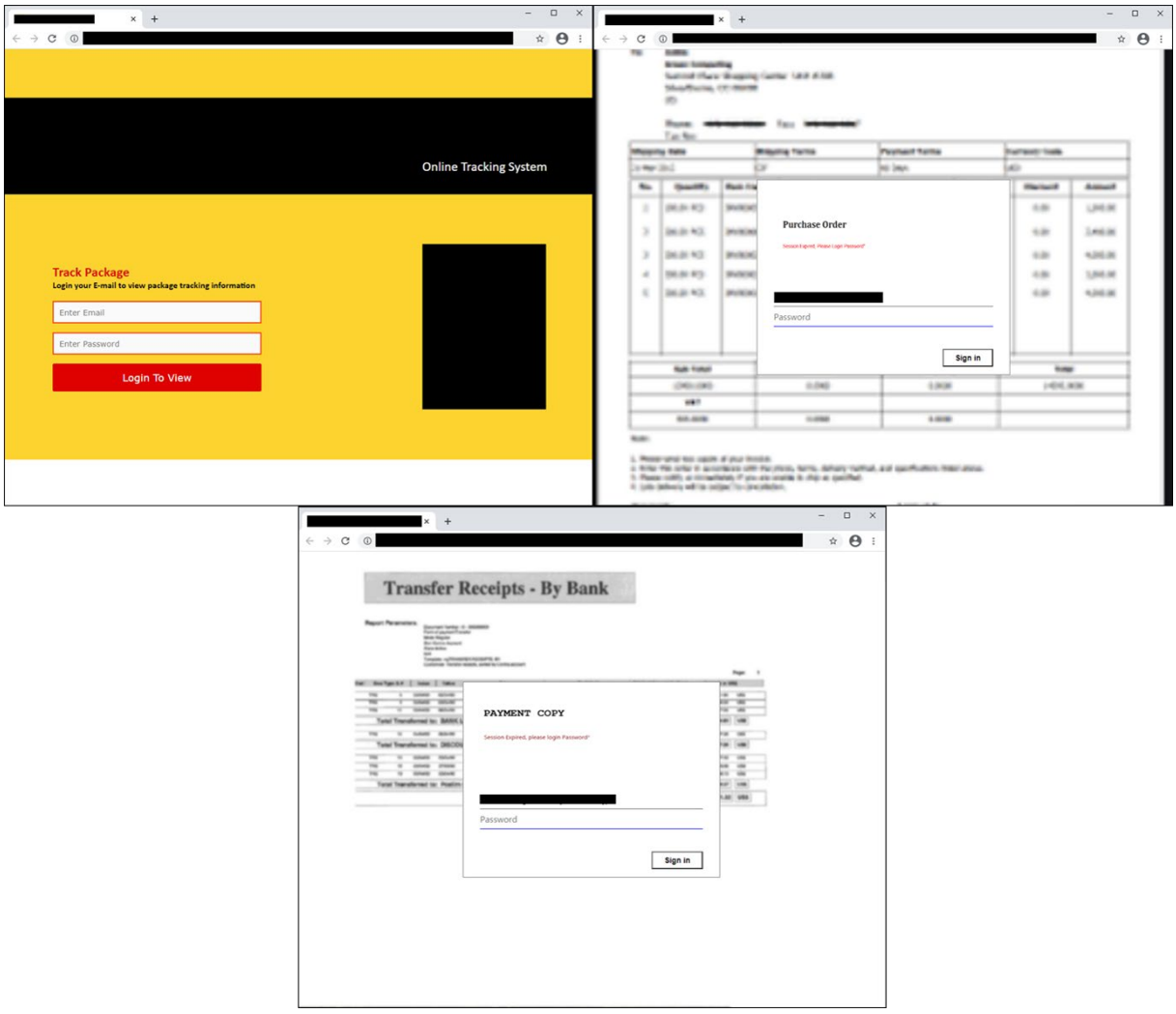
国内マルウェア検出数*2 上位（2021 年 2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	15.5%	アドウェア
2	HTML/Phishing.Agent	7.0%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	5.1%	アドウェア
4	JS/Adware.Subprop	4.3%	アドウェア
5	DOC/Fraud	3.9%	詐欺サイトのリンクが埋め込まれた doc ファイル
6	JS/Adware.Sculinst	3.2%	アドウェア
7	HTML/ScrInject	2.9%	HTML に埋め込まれた不正スクリプト
8	JS/Adware.PopAds	1.6%	アドウェア
9	VBA/TrojanDownloader.Agent	1.3%	ダウンローダー
10	DOC/Phishing.Agent	0.6%	フィッシング目的の doc ファイル

*2 本表には PUA を含めていません。

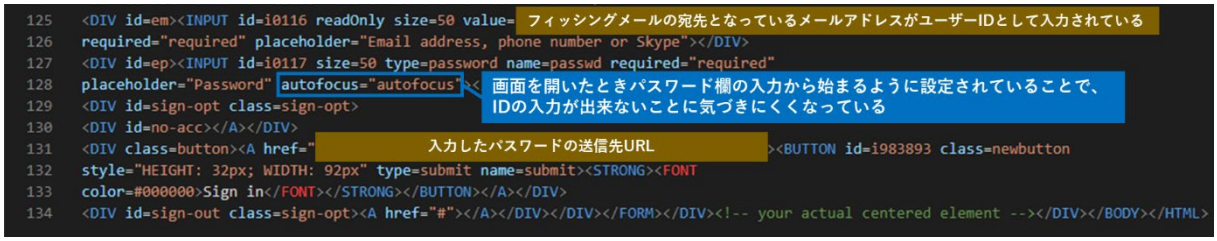
1 月と 2 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

1 月と 2 月は、フィッシング詐欺を狙った脅威が検出されています。中でも、HTML/Phishing.Agent は 1 月と 2 月の両方で検出数第 2 位となっています。HTML/Phishing.Agent は、メールに添付された HTML ファイルです。ファイルを開くと、ローカルでフィッシングサイトの画面が表示されます。表示される画面として、請求書を装ったものや物流会社などのロゴを悪用したものが確認されています。こちらの画面上でパスワードなどの認証情報を入力させることで、情報の窃取を行います。



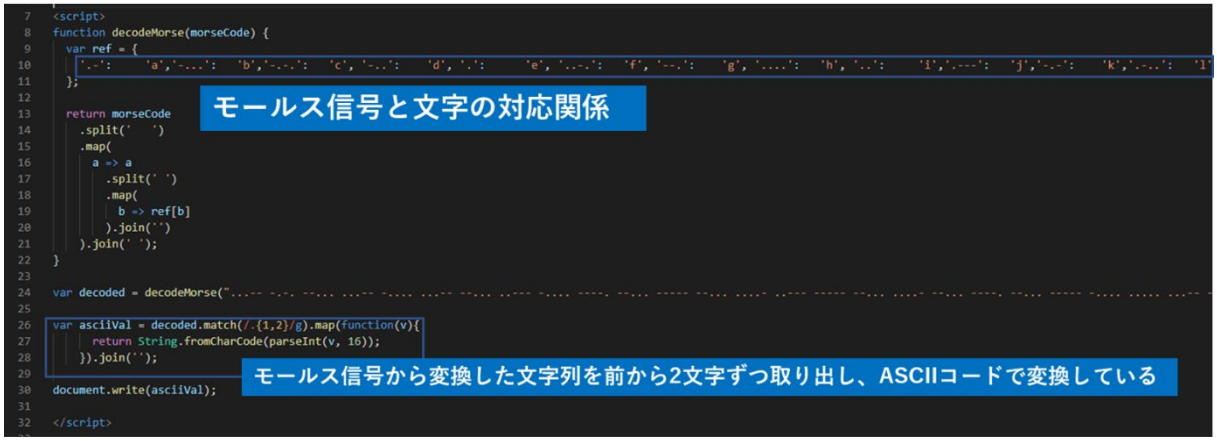
添付ファイルを開いたときに表示される画面の一例

2 月に確認された HTML/Phishing.Agent の中には、フィッシングメールの宛先がユーザーID として事前に設定されているものがありました。普段利用しているサービスだと勘違いさせ、パスワード入力への警戒心を解く狙いがあると考えられます。そして、入力したパスワードは、攻撃者が用意した URL へ送信されます。



HTML/Phishing.Agent サンプルのコードの一部

フィッシング詐欺は、手法の巧妙化や変化が進んでいます。最近では、スミッシングと呼ばれる SMS（ショートメッセージサービス）を利用したフィッシング詐欺など、様々な誘導方法が確認されています。また、金融機関やクレジットカードの認証情報だけでなく様々なオンラインサービスの認証情報を狙っています。他にも、フィッシングサイトへ誘導するためのコードにも変化が出ています。2 月にはモールス信号に変換することでスクリプトの内容を秘匿したファイルが確認されています。スクリプト内で使われているモールス符号は、欧文モールス符号と呼ばれるものです。



モールス信号を悪用したスクリプトの一部

動作としては、モールス符号から 16 進数の文字列へデコードし、その文字列を ASCII コードでもう一度変換します。変換された文字列は、攻撃者が用意した JavaScript がある Web サイトへ誘導するコードになっています。最終的には、Office 365 のパスワード入力を促すフィッシングサイトへアクセスし、パスワードといった認証情報を窃取します。

ご紹介したように、1 月と 2 月はフィッシング詐欺を狙った脅威を検出しています。中でも、フィッシングサイトへ誘導するためのメールに添付された HTML ファイルが多く検出されています。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。また、個別の対策として、メールに添付されたファイルを安易に開かないことや普段利用する 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。

■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 および Office 365 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 キーワード辞典「フィッシング詐欺」

https://eset-info.canon-its.jp/malware_info/term/detail/00128.html

■マルウェア情報局「SMS を利用したスミッシングによるサイバー詐欺の危険性」

https://eset-info.canon-its.jp/malware_info/special/detail/201210.html

Canon

キヤノンマーケティングジャパン株式会社