2020年
12月
DECEMBER

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

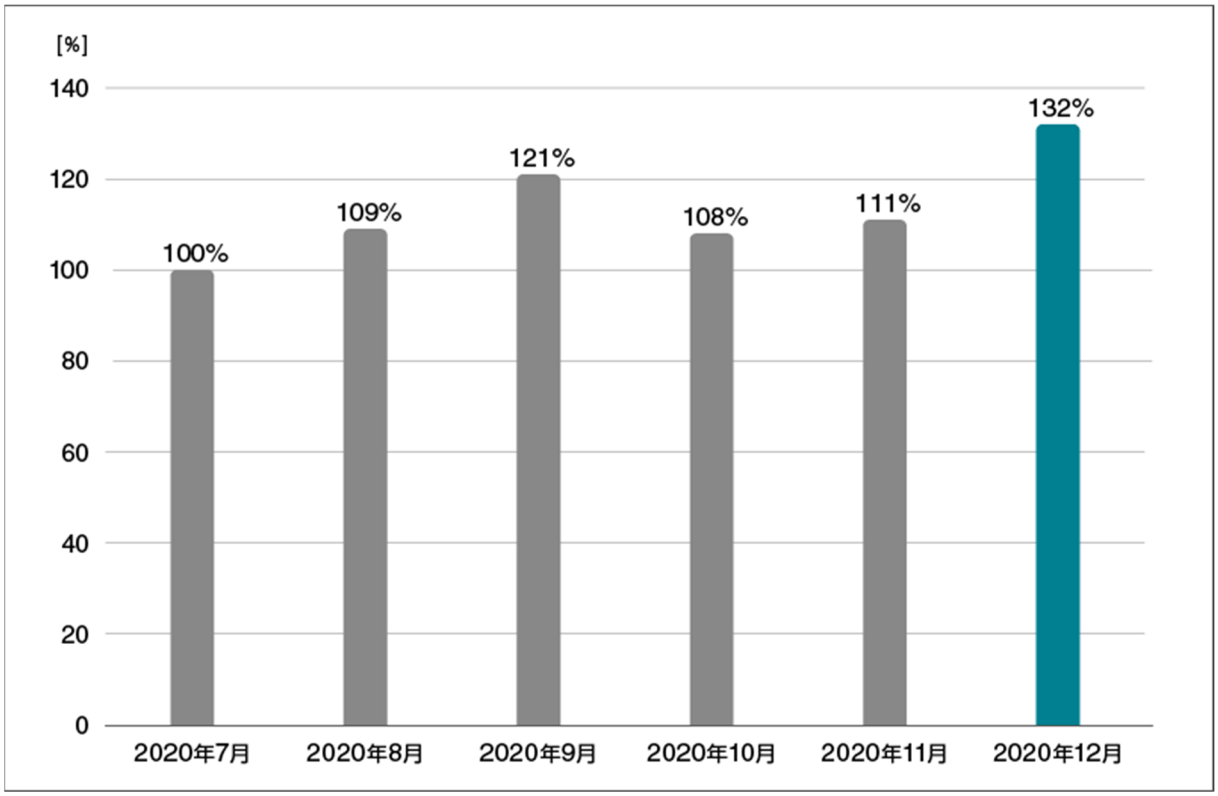
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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「2020 年 12 月マルウェア検出状況」

2020 年 12 月（12 月 1 日～12 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 7 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。

2020 年 12 月の国内マルウェア検出数は、増加しました。直近 6 カ月の中で最も多い検出数となっています。検出されたマルウェアの内訳は以下のとおりです。

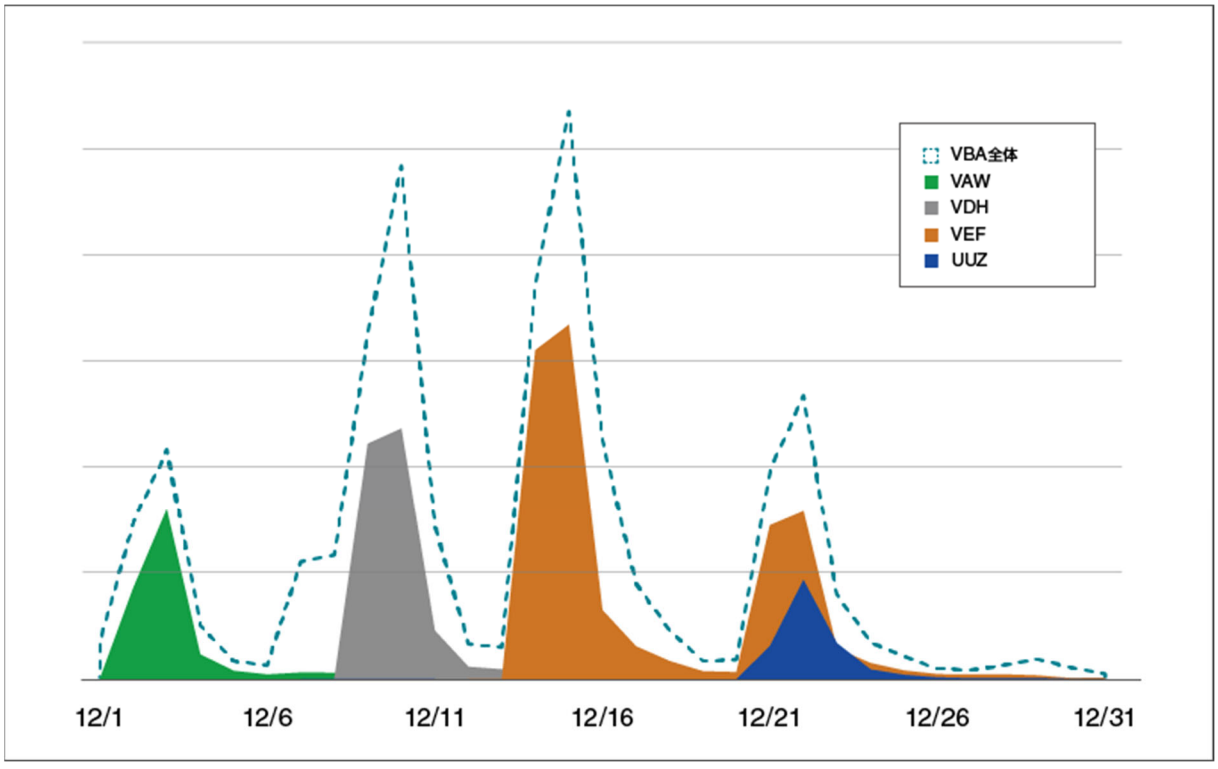
国内マルウェア検出数*2 上位（2020 年 12 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	10.3%	アドウェア
2	JS/Agent.OAY	8.0%	不正な JavaScript の汎用検出名
3	HTML/Phishing.Agent	7.3%	別のページに遷移させるスクリプト
4	JS/Adware.Subprop	4.9%	アドウェア
5	JS/Adware.TerraClicks	4.5%	アドウェア
6	HTML/ScrInject	3.1%	HTML に埋め込まれた不正スクリプト
7	JS/Adware.PopAds	1.7%	アドウェア
8	VBA/TrojanDownloader.Agent	1.7%	ダウンローダー
9	HTML/Fraud	0.6%	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名

*2 本表には PUA を含めていません。

12 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、不正な広告を表示させるアドウェアの汎用検出名です。JS/Adware.Agent は、Web ブラウザー上で実行されます。

今月はメールの添付ファイルによる脅威を多数確認しています。8 位の VBA/TrojanDownloader.Agent は、Office 製品で利用されるプログラミング言語の VBA(Visual Basic for Applications)で作成されたダウンローダーです。VBA/TrojanDownloader.Agent は、主にメールの添付ファイルとして確認されています。VBA/TrojanDownloader.Agent には、多数の亜種が存在しています。12 月に検出数が多く確認された VBA/TrojanDownloader.Agent 亜種の日別検出数の推移は以下のとおりです。4 つの時期において、検出数の増加が確認できます。4 つの期間に多く検出された亜種がダウンロードする主なマルウェアは以下のとおりです。ダウンロードするマルウェアとして、現時点では Dridex や Emotet などを確認しています。



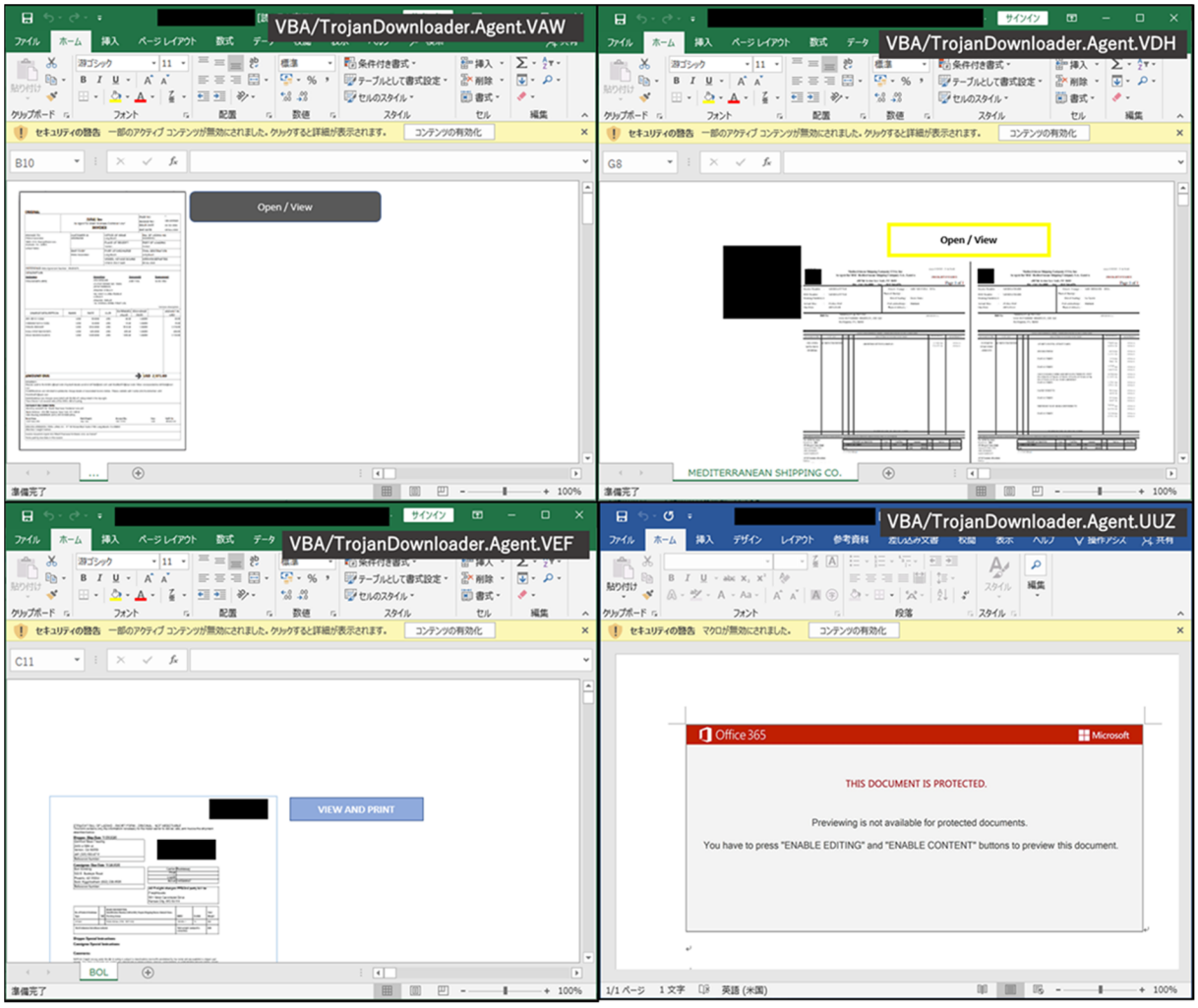
VBA/TrojanDownloader.Agent 亜種の日別検出数推移

※グラフ内の亜種名は一部省略しています。

亜種名	ダウンロードする主なマルウェア
VBA/TrojanDownloader.Agent.VAW	Dridex
VBA/TrojanDownloader.Agent.VDH	Dridex
VBA/TrojanDownloader.Agent.VEF	Dridex
VBA/TrojanDownloader.Agent.UUZ	Emotet

VBA/TrojanDownloader.Agent の亜種とダウンロードする主なマルウェア

VBA/TrojanDownloader.Agent の亜種である添付ファイルを開くと以下の画面が表示されます。今回確認したサンプルでは、Excel ファイルと Word ファイルを確認しています。



VBA/TrojanDownloader.Agent のサンプルを開いた時の表示画面

Excel ファイルは、請求書を装ってコンテンツの有効化をクリックさせようとしています。Word ファイルも、コンテンツの有効化をクリックさせようと誘導しています。
そのコンテンツの有効化をクリックすることで、マクロが実行されます。最終的に他のマルウェアをダウンロードします。
ダウンロードされるマルウェアとして、今回のような Dridex や Emotet などが挙げられます。
また、Dridex や Emotet はモジュール式のマルウェアです。それぞれで追加するモジュールは異なりますが、様々な機能の追加が可能です。追加される機能によって、被害も様々想定されます。また、他のマルウェアをダウンロードする恐れがあります。

今回ご紹介したように、12 月はメールの添付ファイルによる脅威を多数検出しています。
VBA/TrojanDownloader.Agent はマクロを有効化することで他のマルウェアをダウンロードします。また、様々なマルウェアをダウンロードすることが確認されています。
このような脅威の被害に遭わないためにも、セキュリティ製品の正しい運用やマクロが無効になっているかを確認することが重要です。他にも、ダウンロードされるマルウェアに対しての個別の対策も必要です。

■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。

引用・出典元

■マルウェア情報局「フィッシングメールによって拡散された Dridex ダウンローダーの解析レポートを公開」
https://eset-info.canon-its.jp/malware_info/trend/detail/201120.html

Canon

キヤノンマーケティングジャパン株式会社