2020年
5月
MAY

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

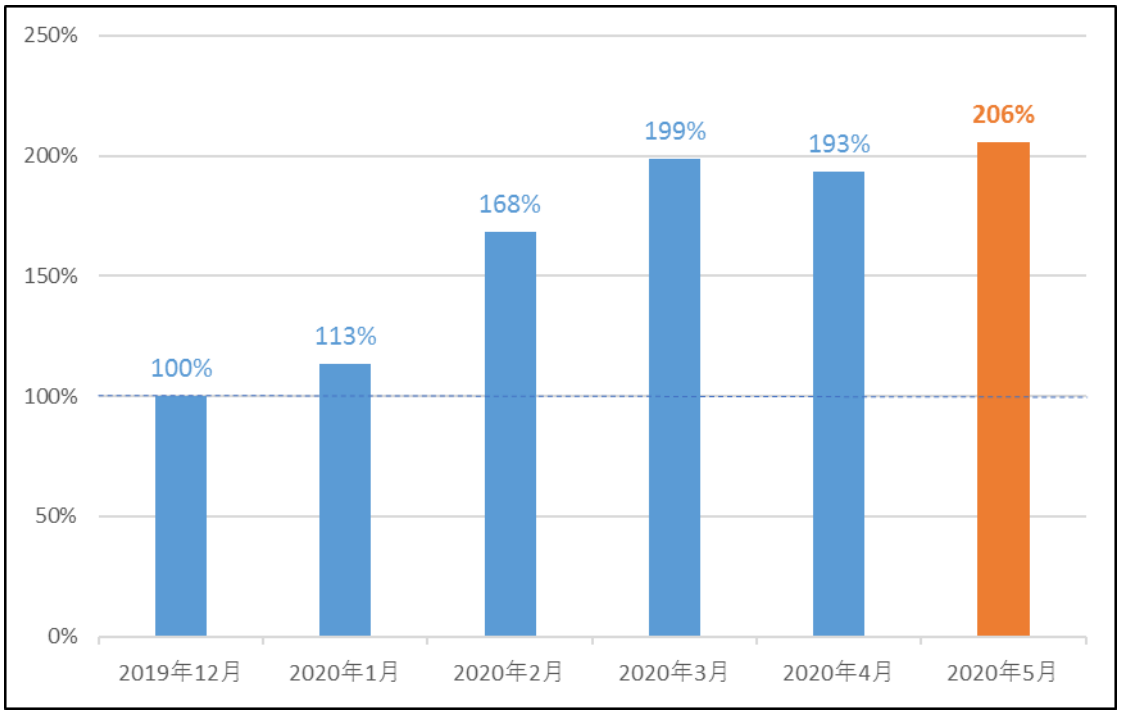
「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

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 5 月マルウェア検出状況」

5 月の概況

2020 年 5 月（5 月 1 日～5 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

(2019 年 12 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 5 月の国内マルウェア検出数は、増加しました。また、直近 6 か月間の中で最も検出数の多い月となっています。

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 5 月）

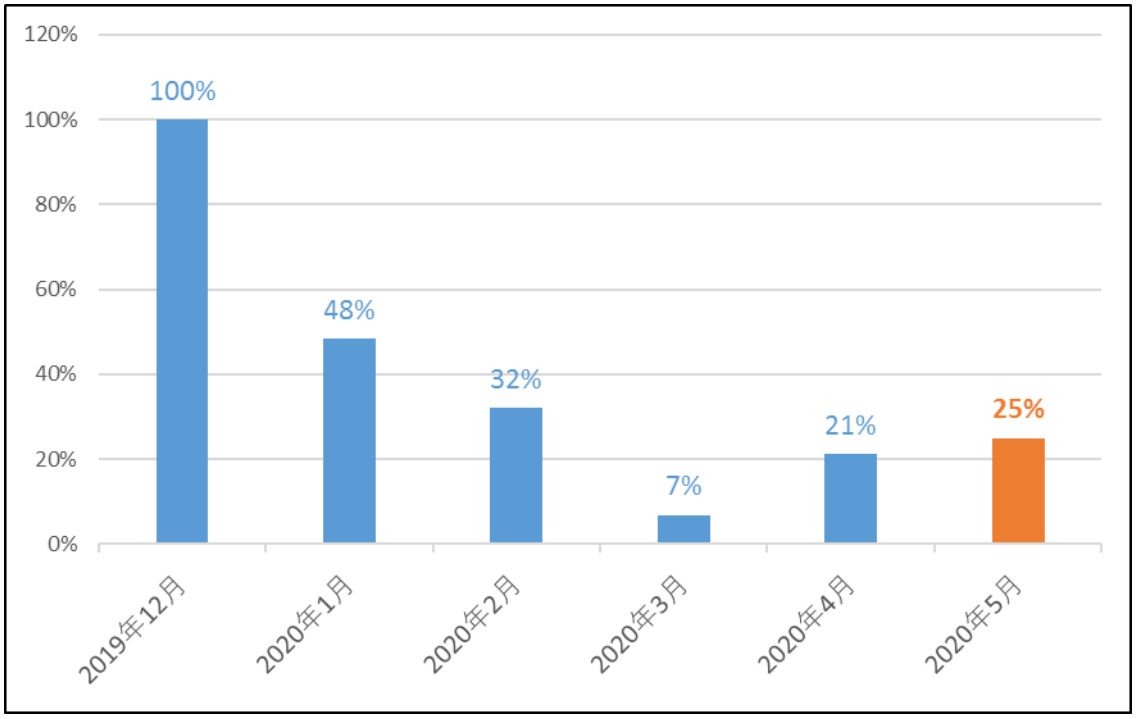
順位	マルウェア	割合	種別
1	JS/Adware.Agent	14.8%	アドウェア
2	JS/Adware.Subprop	7.8%	アドウェア
3	HTML/ScrInject	6.6%	HTML に埋め込まれた不正スクリプト
4	JS/Adware.Chogdoul	6.0%	アドウェア
5	JS/Adware.PopAds	5.9%	アドウェア
6	JS/Adware.Inpagepush	5.0%	アドウェア
7	JS/Adware.Velocity	2.9%	アドウェア
8	HTML/Refresh	2.7%	別のページに遷移させるスクリプト
9	VBA/TrojanDownloader.Agent	1.0%	ダウンローダー
10	JS/Adware.Revmbill	0.7%	別のページに遷移させるスクリプト

*2 本表には PUA を含めていません。

5 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で、Web サイト閲覧時に実行されます。

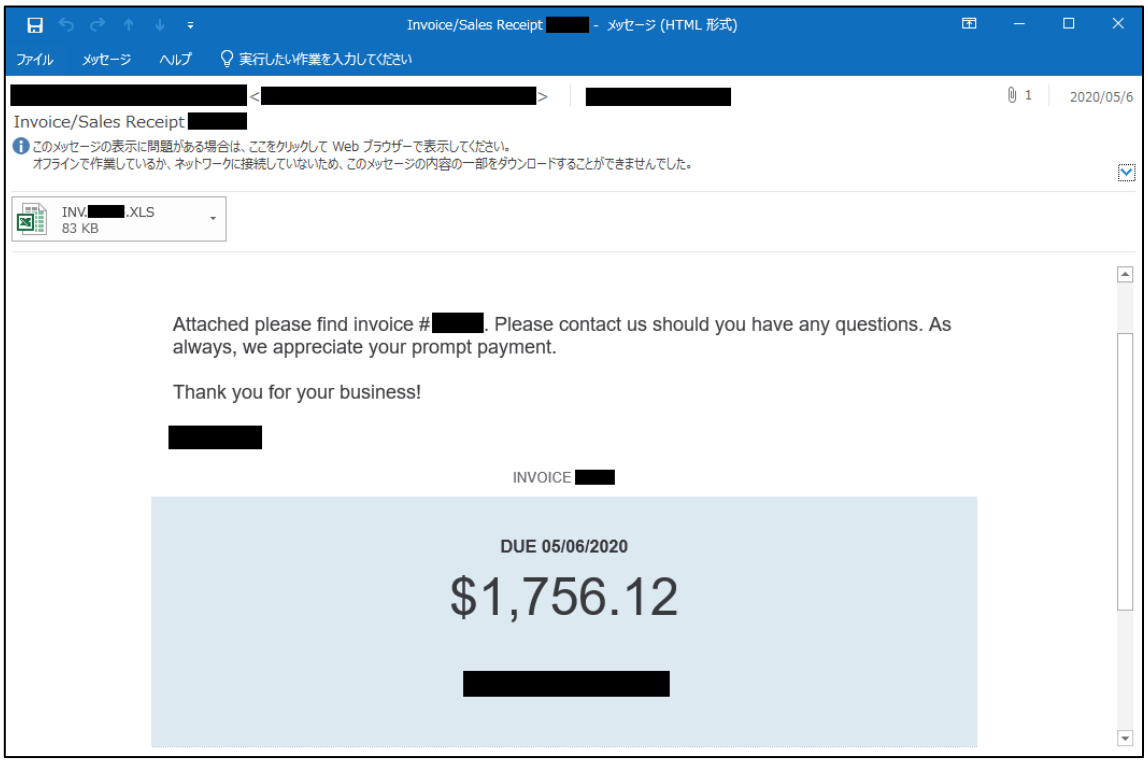
アドウェアの中には、不正な広告を表示させる以外にも、Web ブラウザーのアクセス履歴を外部へ送信するものもあるので注意が必要です。信頼できる Web サイトへアクセスするように心掛けてください。

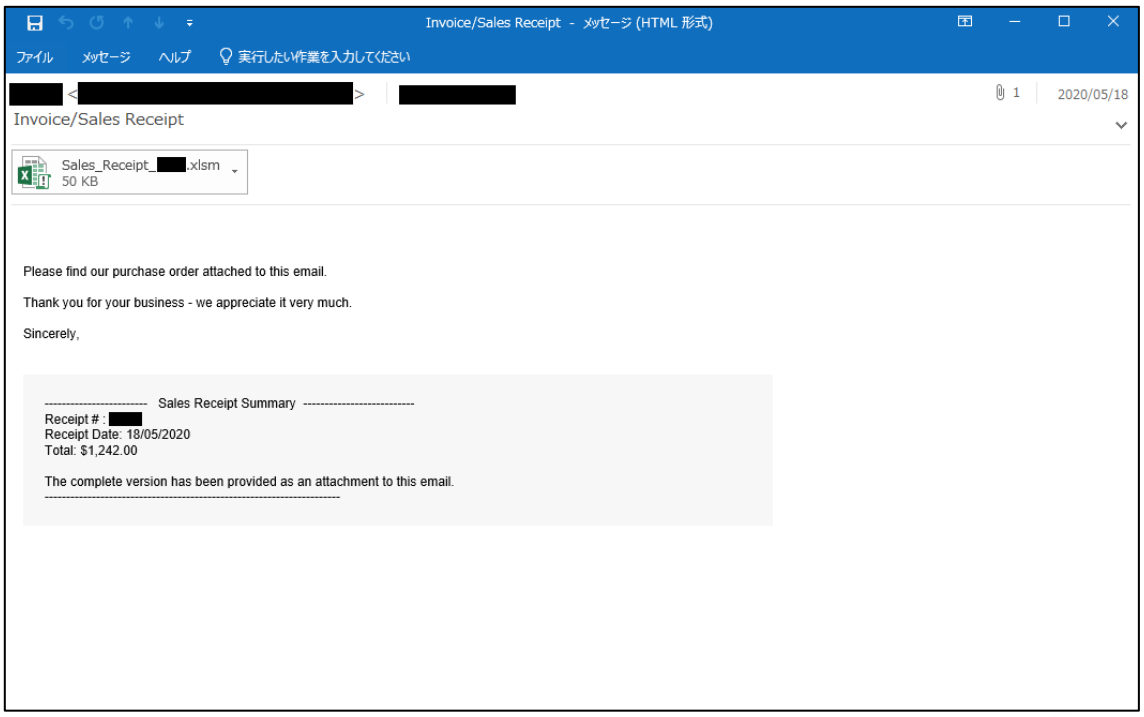
メールの添付ファイルによる脅威は、今月も引き続いて多く検出されています。
VBA/TrojanDownloader.Agent は、Office 製品で利用されるプログラミング言語の VBA で作成されたダウンローダーです。感染経路は、主にメールの添付ファイルです。感染後に他のマルウェアをダウンロードします。



VBA/TrojanDownloader.Agent の月別検出数の推移（国内）
（2019 年 12 月の検出数を 100%として比較）

VBA/TrojanDownloader.Agent の検出数は、12 月以降減少傾向にありましたが、4 月頃から検出数が、増加し始めています。
5 月にばらまかれた VBA/TrojanDownloader.Agent を添付していたメールの一部が以下のものです。





VBA/TrojanDownloader.Agent が添付されていたメールの本文

これらのメールは、請求書の送付を装っています。
また、1 つ目の画像のように実在するソフトウェア会社を装ったメールも確認されています。これらのメールに添付されているファイルは、Excel ファイルでした。Excel ファイルを開いてコンテンツの有効化をクリックすることで、マクロが実行され最終的に Dridex へ感染します。検出された VBA/TrojanDownloader.Agent の中では、Dridex をダウンロードするものが 4 月、5 月と多く確認されています。
Dridex は、バンキングマルウェアの 1 つであり、ボットネットを形成することでも知られています。Dridex の詳細については、4 月マルウェアレポートでご紹介していますので是非参照してください。

これらのようなメールに添付されるファイルによる脅威の被害に遭わないためにも、セキュリティ製品の利用、Office 製品のマクロが無効になっていることの確認や添付ファイルを安易に開かないといった対策が重要です。

ご紹介したように、5 月は Web ブラウザー上で実行される脅威に加えて、
VBA/TrojanDownloader.Agent の検出数の増加傾向が続いています。メールの添付ファイルは安易に開かないことが重要です。また、お使いの Office 製品のマクロが無効になっていることを確認してください。

■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. 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］

Canon

キヤノンマーケティングジャパン株式会社