2021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

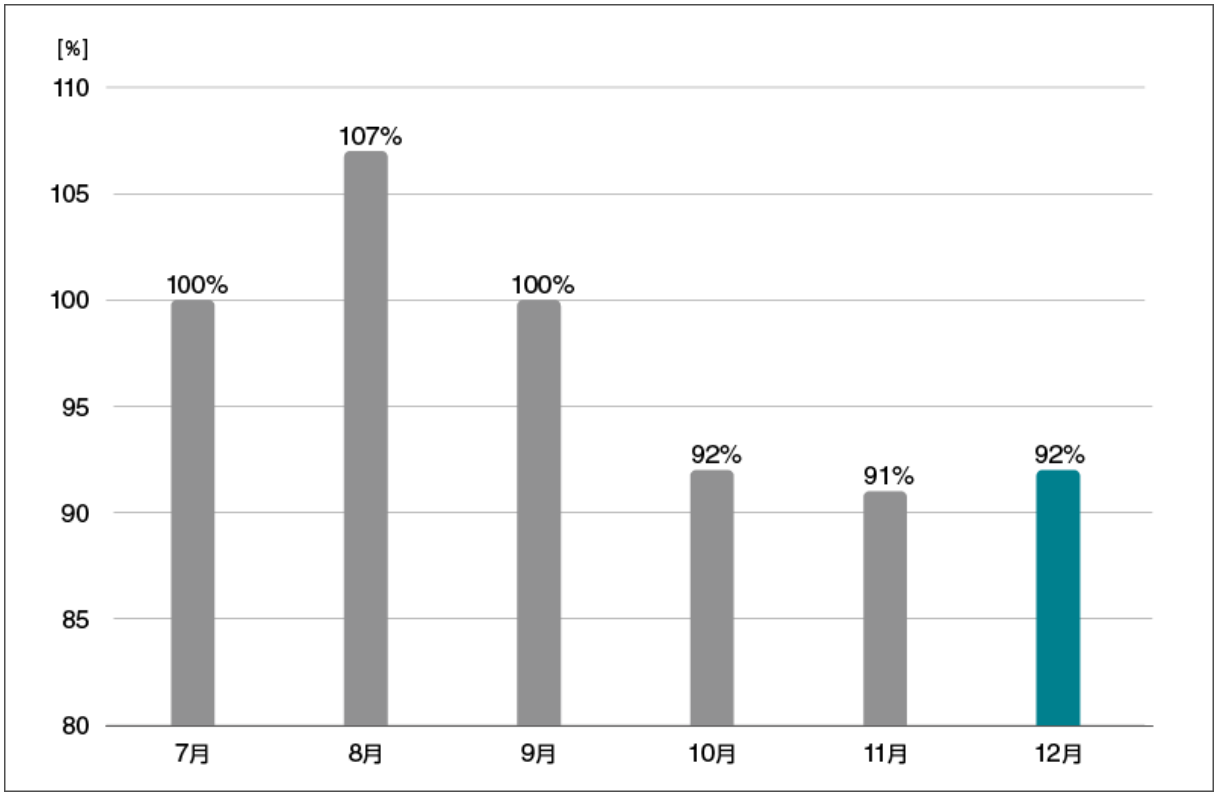
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」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。

2021 年 12 月マルウェア検出状況

2021 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

(2021 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。

2021 年 12 月の国内マルウェア検出数は、2021 年 11 月から微増していました。検出されたマルウェアの内訳は以下のとおりです。

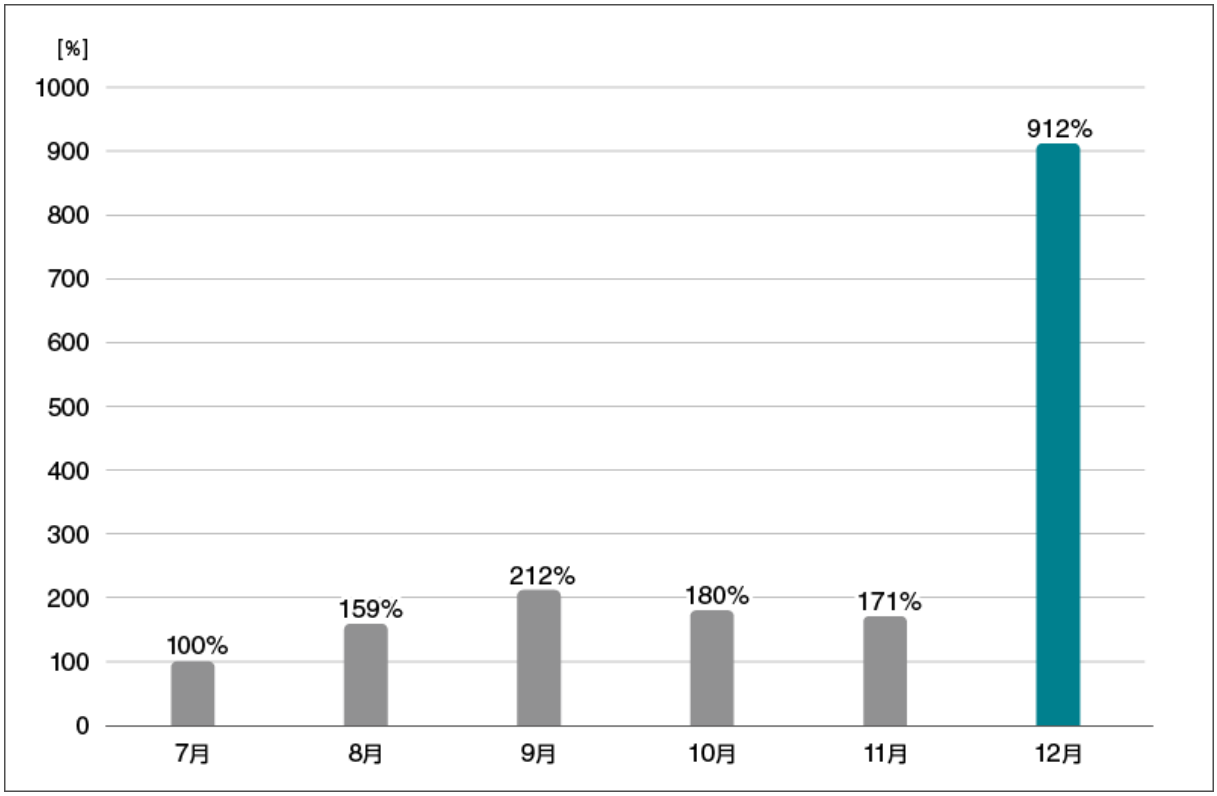
国内マルウェア検出数*2 上位（2021 年 12 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	19.6%	アドウェア
2	HTML/Phishing.Agent	11.0%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	7.8%	アドウェア
4	HTML/ScrInject	5.5%	HTML に埋め込まれた不正スクリプト
5	JS/Adware.TerraClicks	4.2%	アドウェア
6	HTML/FakeAlert	4.2%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.Subprop	2.8%	アドウェア
8	DOC/Fraud	1.6%	詐欺サイトのリンクが埋め込まれた doc ファイル
9	JS/Adware.PopAds	1.3%	アドウェア
10	JS/Redirector	0.9%	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。

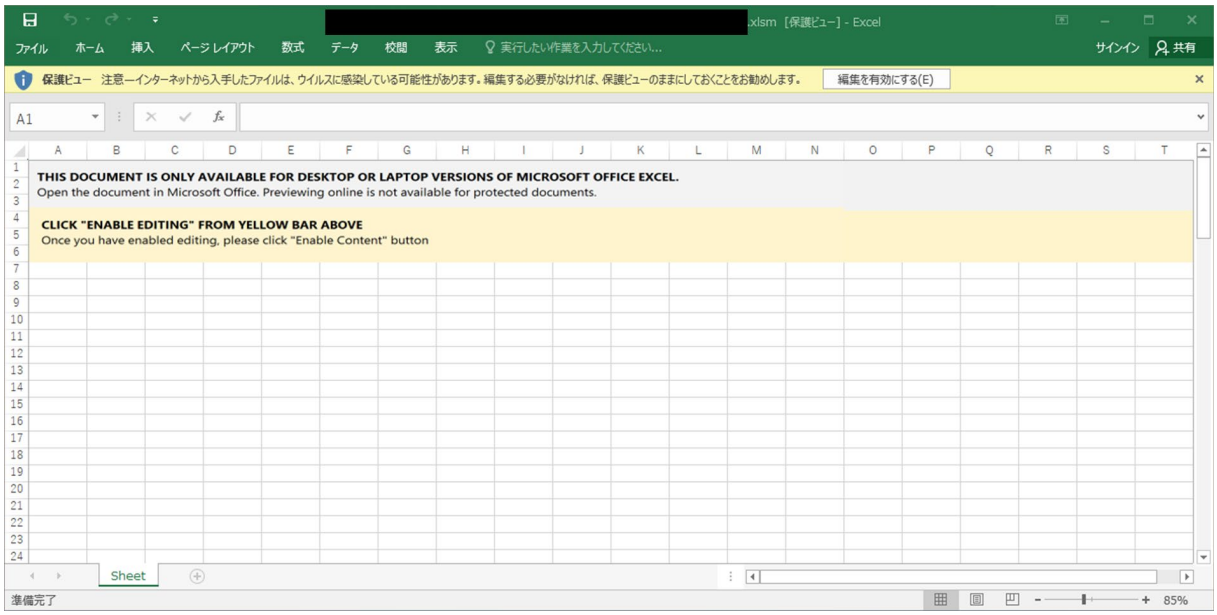
12 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

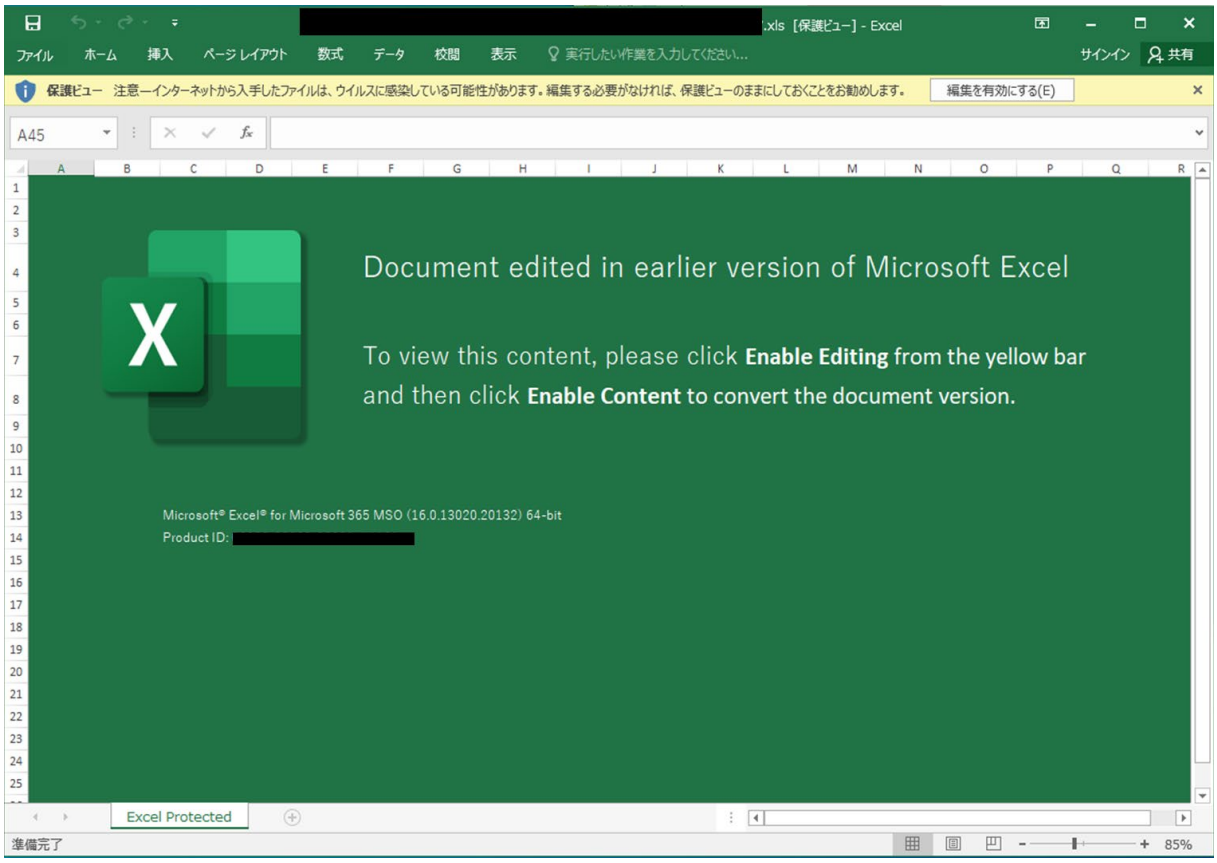
12 月は、Emotet への感染を狙ったメールを引き続き観測しています。中でも Emotet のダウンローダーの 1 つである DOC/TrojanDownloader.Agent の検出数が増加しています。



DOC/TrojanDownloader.Agent の検出数の月別推移（2021 年･国内）
(2021 年 7 月の検出数を 100%として比較)

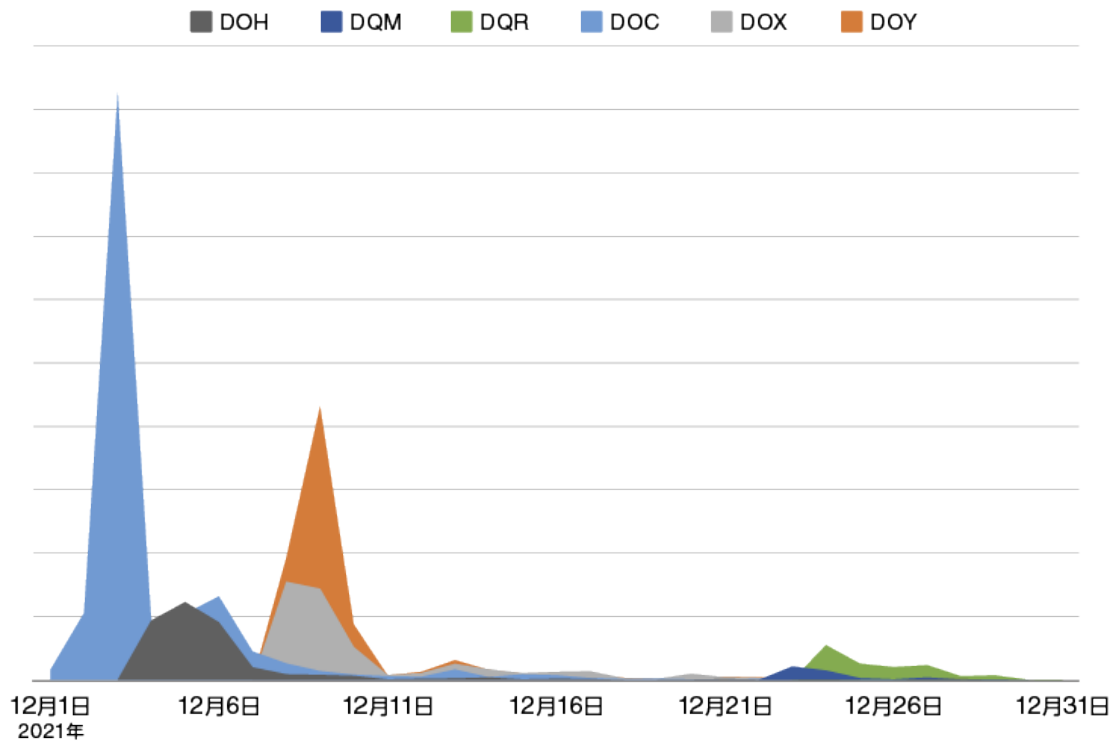
12 月に検出された DOC/TrojanDownloader.Agent の亜種は、マクロ付き Excel ファイルとして検出していました。これらのマクロ付き Excel ファイルを実行した際の画面として、以下のものを確認しています。





添付ファイルを実行した際の表示画面（上：① 下：②）

以前から確認されているダウンローダーと同様に、「編集を有効にする」「コンテンツの有効化」を続けてクリックすると、最終的に Emotet をダウンロードします。
DOC/TrojanDownloader.Agent の亜種の中で検出数上位だった Emotet ダウンローダーの検出状況は以下のとおりです。



Emotet をダウンローダーする DOC/TrojanDownloader.Agent 亜種の日別検出数推移（2021 年・国内） *3 *4

*3 DOC/TrojanDownloader.Agent 亜種のうち、検出数上位のみを掲載しています。

*4 グラフ上の凡例は、亜種ごとに割り振られた文字列を表示しています。

12 月 3 日～9 日にかけて、多数検出されていることが分かります。これらの検体では添付ファイルを実行すると、表示画面①が表示されていました。また、12 月 21 日～12 月 31 日の間にかけてもダウンローダーの検出があります。12 月上旬の検出数と比較すると多くはありませんが、今回ご紹介した表示画面②のダウンローダーを検出したものです。

ご紹介したもの以外にも、Adobe 製品のインストーラーを装ったダウンローダーが確認されています。これは、WindowsAppX インストーラーのなりすましの脆弱性（CVE-2021-43890）を悪用しており、添付ファイルではなくメール本文内の URL からダウンロードされていました。2021 年 12 月 15 日の Microsoft 社のアップデートによって修正された後は、URL からマクロ付きの Word ファイルや Excel ファイルをダウンロードするメールが確認されています。今後もダウンローダーの変化に注意する必要があります。

ご紹介したとおり、2021 年 12 月は Emotet への感染を狙ったダウンローダーが増加しています。このような脅威の被害に遭わないためにも、添付ファイルを不用意に開かないことやメール本文に書かれた URL に不用意にアクセスしないことが重要です。また、添付ファイルを実行してしまった場合も、「コンテンツの有効化」をクリックしないようにしてください。そして、Emotet に感染した場合の影響や被害範囲を把握しておくことも対策として重要です。

■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．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

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います。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）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

2．脆弱性への対応

2-1. 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ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1．脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2．インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1．情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2．情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

引用・出典元

Microsoft Security Response Center「2021 年 12 月のセキュリティ更新プログラム（月例）」
https://msrc-blog.microsoft.com/2021/12/14/202112-security-updates/

Canon

キヤノンマーケティングジャパン株式会社