2020年
7·8月
JULY/AUGUST

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

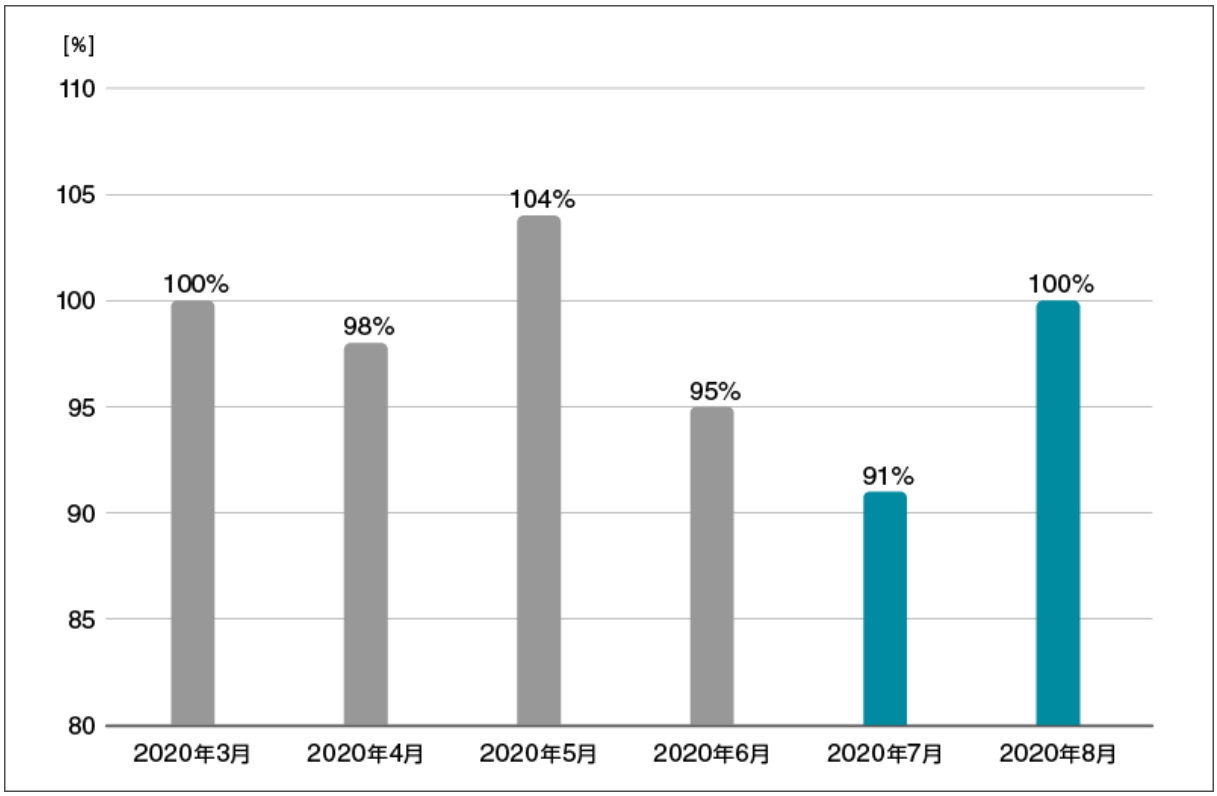
「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

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 7 月･8 月マルウェア検出状況」

7 月と 8 月の概況

2020 年 7 月（7 月 1 日～7 月 31 日）と 8 月（8 月 1 日～8 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 3 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 7 月の国内でのマルウェア検出数は 6 月と比較して減少しましたが、8 月のマルウェア検出数は増加傾向に転じました。検出されたマルウェアの内訳は以下のとおりです。

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 7 月 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Subprop	8.8%	アドウェア
2	HTML/ScrInject	6.5%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Agent	5.8%	アドウェア
4	JS/Adware.PopAds	3.9%	アドウェア
5	JS/Adware.Inpagepush	2.9%	アドウェア
6	VBA/TrojanDownloader.Agent	2.4%	ダウンローダー
7	HTML/Refresh	2.0%	別のページに遷移するスクリプト
8	HTML/Fraud	1.4%	詐欺サイトのリンクが埋め込まれた HTML
9	JS/Adware.Chogdoul	1.2%	アドウェア
10	Win32/Exploit.CVE-2017-11882	1.0%	脆弱性を悪用するマルウェア

国内マルウェア検出数*2 上位（2020 年 7 月）

順位	マルウェア	割合	種別
1	JS/Adware.Subprop	10.4%	アドウェア
2	HTML/ScrInject	7.4%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Agent	4.7%	アドウェア
4	JS/Adware.PopAds	4.0%	アドウェア
5	VBA/TrojanDownloader.Agent	2.8%	ダウンローダー
6	JS/Adware.Inpagepush	2.5%	アドウェア
7	HTML/Refresh	2.3%	別のページに遷移させるスクリプト
8	JS/Redirector	1.4%	別のページに遷移させるスクリプト
9	JS/Adware.Chogdoul	1.3%	アドウェア
10	HTML/Fraud	1.1%	詐欺サイトのリンクが埋め込まれた HTML

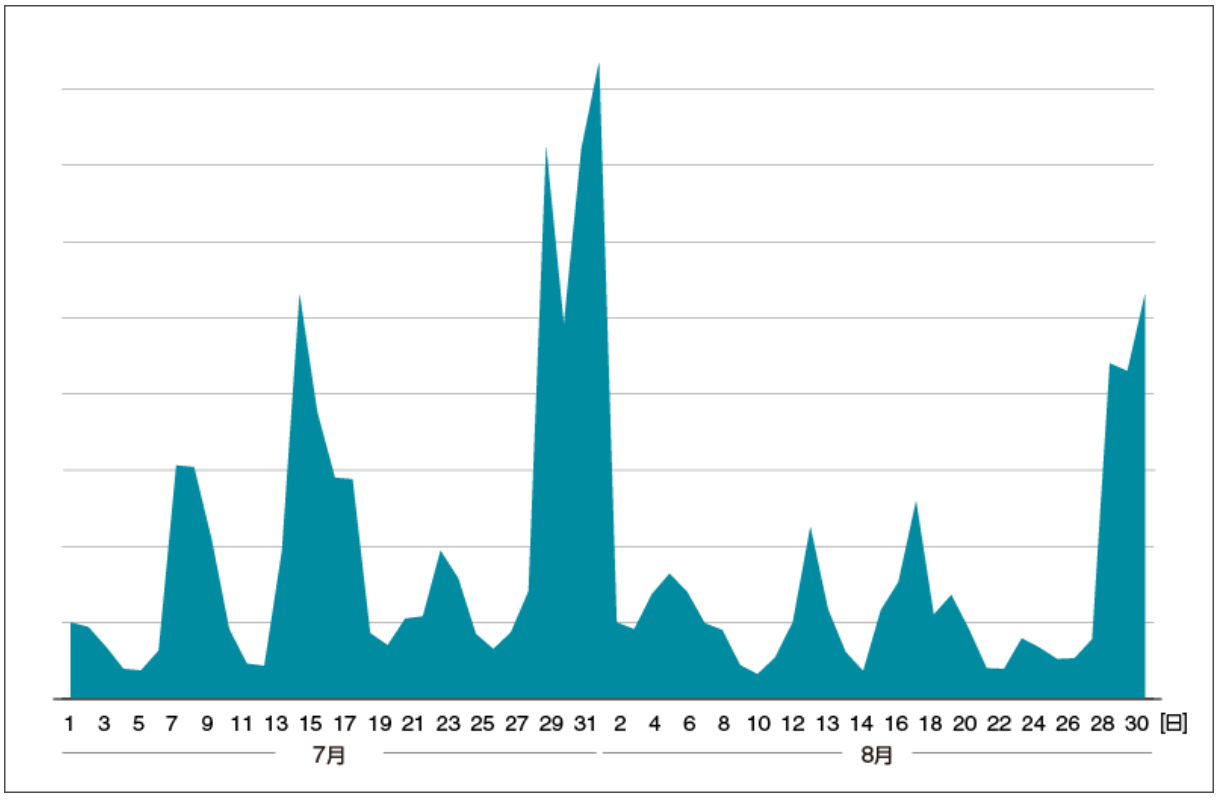
国内マルウェア検出数*2 上位（2020 年 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Subprop	7.4%	アドウェア
2	JS/Adware.Agent	6.8%	アドウェア
3	HTML/ScrInject	5.6%	HTML に埋め込まれた不正スクリプト
4	JS/Adware.PopAds	3.8%	アドウェア
5	JS/Adware.Inpagepush	3.1%	アドウェア
6	VBA/TrojanDownloader.Agent	2.1%	ダウンローダー
7	HTML/Refresh	1.7%	別のページに遷移させるスクリプト
8	HTML/Fraud	1.7%	詐欺サイトのリンクが埋め込まれた HTML
9	JS/Adware.Chogdoul	1.1%	アドウェア
10	Win32/Exploit.CVE-2017-11882	1.1%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

7 月と 8 月に国内で最も多く検出されたマルウェアは、JS/Adware.Subprop でした。
JS/Adware.Subprop はアドウェアで、偽の Adobe Flash Player のアップデートや有名ベンダーの Web バナーを悪用して、悪意のあるコンテンツや不要なソフトウェアを配布するスクリプトの検出名です。
2 位の HTML/ScrInject は、HTML に埋め込まれた不正スクリプトで、こちらも Web サイト閲覧時に実行されます。

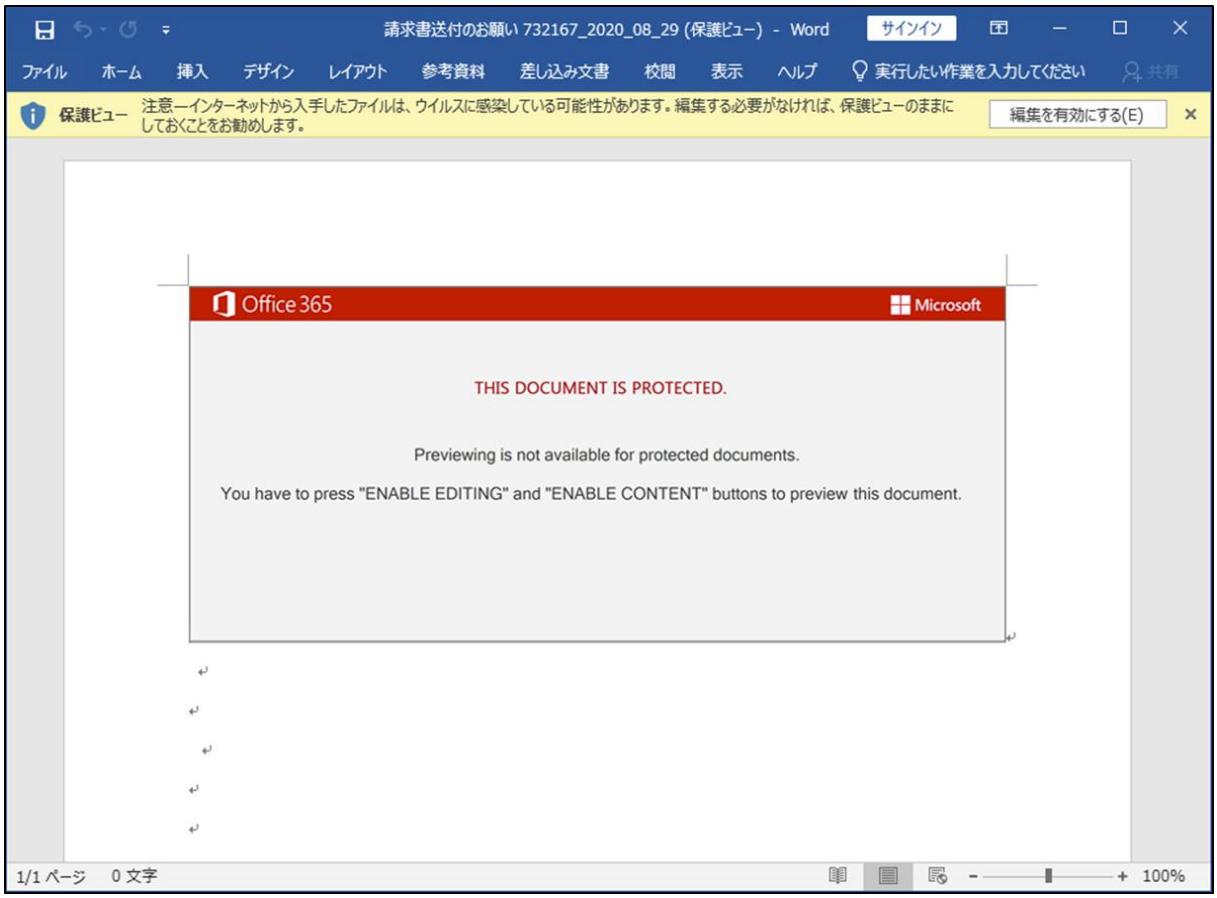
昨年 10 月頃から被害報告が増加し、2020 年 1 月 2 月以降大きな動きを見せていなかった Emotet の活動が 7 月中旬頃から再開しました。7 月中旬頃から Emotet の感染を狙ったばらまきメールが確認されています。IPA などの機関からも注意喚起が出ています。ばらまきメールに添付されていたファイルは Word ファイル（.doc）で、ESET 製品では VBA/TrojanDownloader.Agent などの検出名として検出されます。以下のグラフは、7 月～8 月の日別検出数の推移を表しています。



VBA/TrojanDownloader.Agent の日別検出数の推移（2020 年 7 月～8 月･国内）

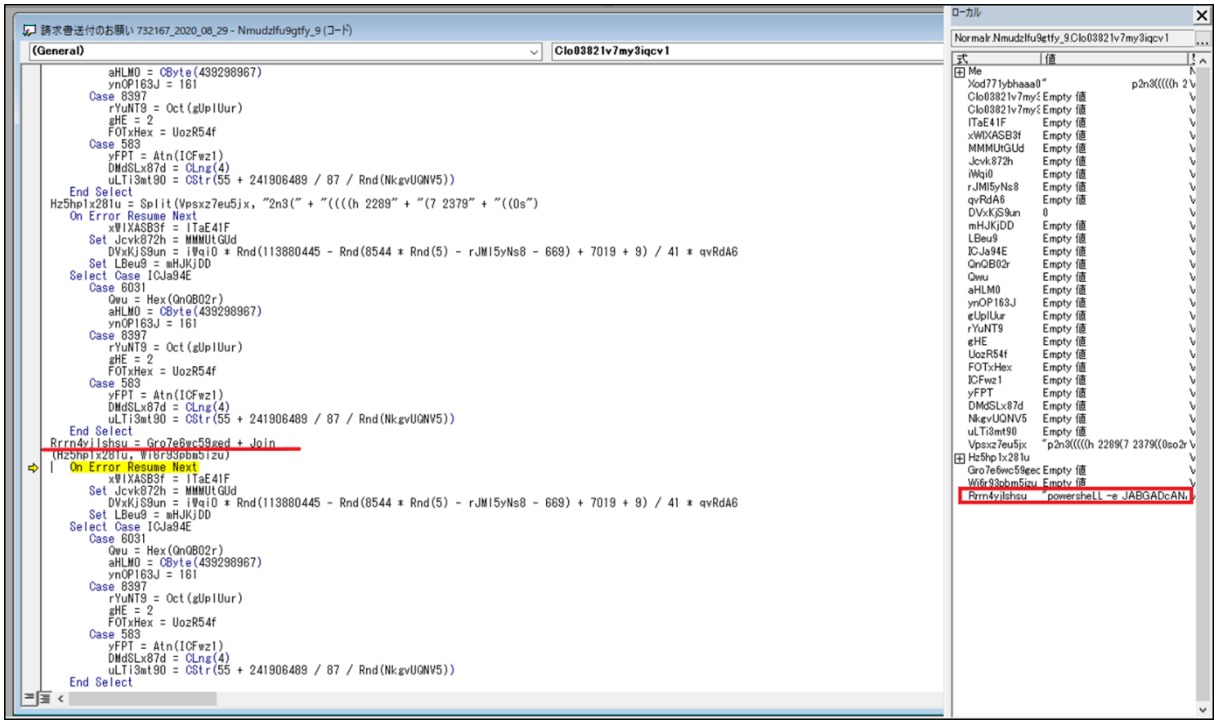
7 月中旬や 7 月末、8 月末にこのマルウェアが多く検出されていることが分かります。これは、Emotet のばらまき

メールが確認されている期間と一致しています。
8 月にばらまかれた添付ファイルを開くと、以下のような画面が表示されます。



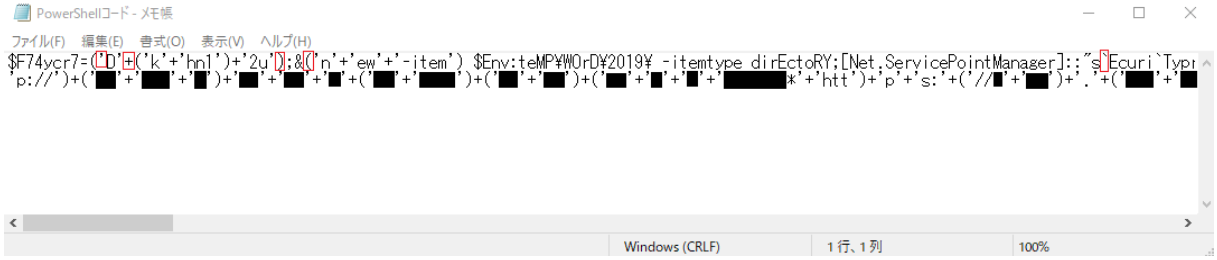
添付ファイルを開いた時の画面

「編集を有効にする」ボタンと「コンテンツの有効化」ボタンをクリックしてしまうと、マクロを経由して PowerShell が実行されます。
赤枠で囲んだ変数は、難読化解除後の PowerShell のコードです。



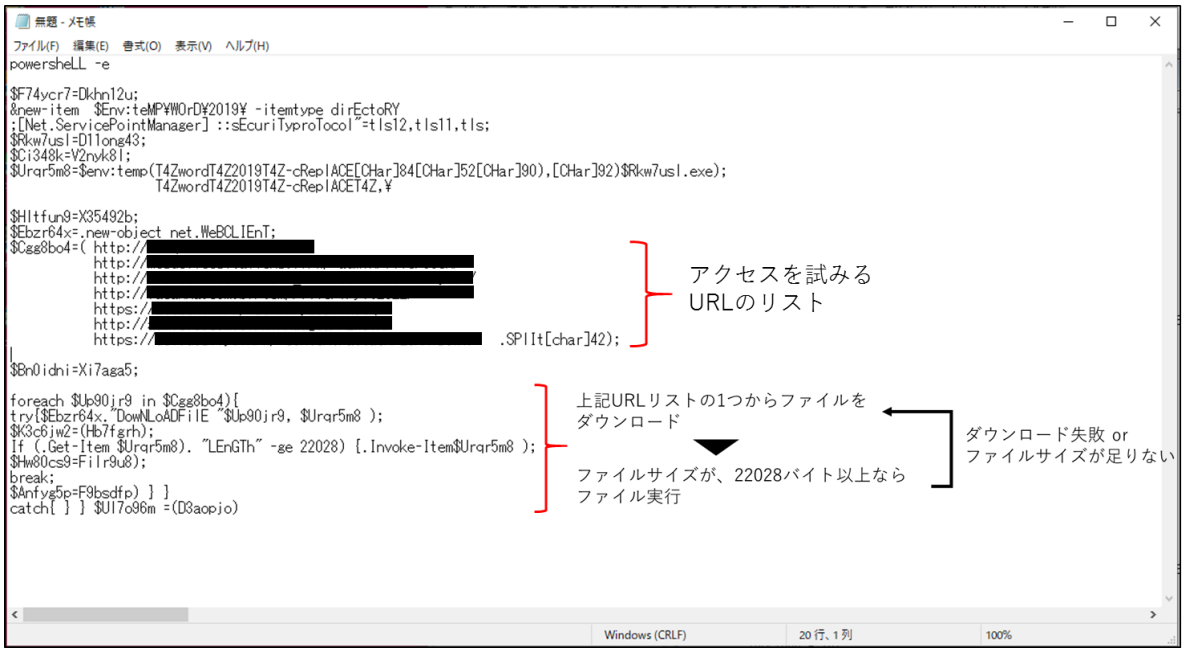
マクロ内に書かれた PowerShell のコード

PowerShell のコード部分は、BASE64 でエンコードされており、デコードすると以下のコードが現れます。



復号した PowerShell のコード

コードの文字部分は「'」「（）」「＋」で区切られており、URL 部分は「＊」で区切られています。区切りの文字を消し、改行を行ったものが以下の画像です。



整形した PowerShell コード

URL のリストから 1 つずつアクセスし、ファイルのダウンロードを行います。その際に、ファイルサイズが 22,028 バイト以上だった場合、ファイルを実行します。ダウンロードに失敗した場合やファイルサイズが条件より小さい場合は、次の URL へアクセスします。

このダウンロードされるファイルが Emotet です。Emotet がダウンロード・実行された場合、情報の窃取や他のマルウェアへの感染などの被害に遭う可能性があります。感染する他のマルウェアは、Trickbot など様々なものが確認されています。さらに、Trickbot からランサムウェア Ryuk をダウンロードされたケースが過去に海外で確認されています。

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導入やシグネチャを最新の状態に保つといった基本的な対策が必要です。加えて、Office 製品でのマクロの設定を無効にすること、添付ファイルを安易に開かないことやランサムウェアの被害軽減策としてのオフラインバックアップ取得といった個別の対策も重要です。

ご紹介したように、7 月と 8 月は Web ブラウザー上で実行される脅威に加えて、Emotet の活動が再開し、多数のダウンローダーが検出されています。セキュリティ製品の導入などの基本的な対策やマクロの設定を無効にするといった個別の対策が重要です。

■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。

Canon

キヤノンマーケティングジャパン株式会社