2017年
7月
JULY

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

開発コードVBAを悪用したマルウェアが増加

キヤノンITソリューションズ株式会社

はじめに

「マルウェアレポート」は、キヤノンITソリューションズが運営する

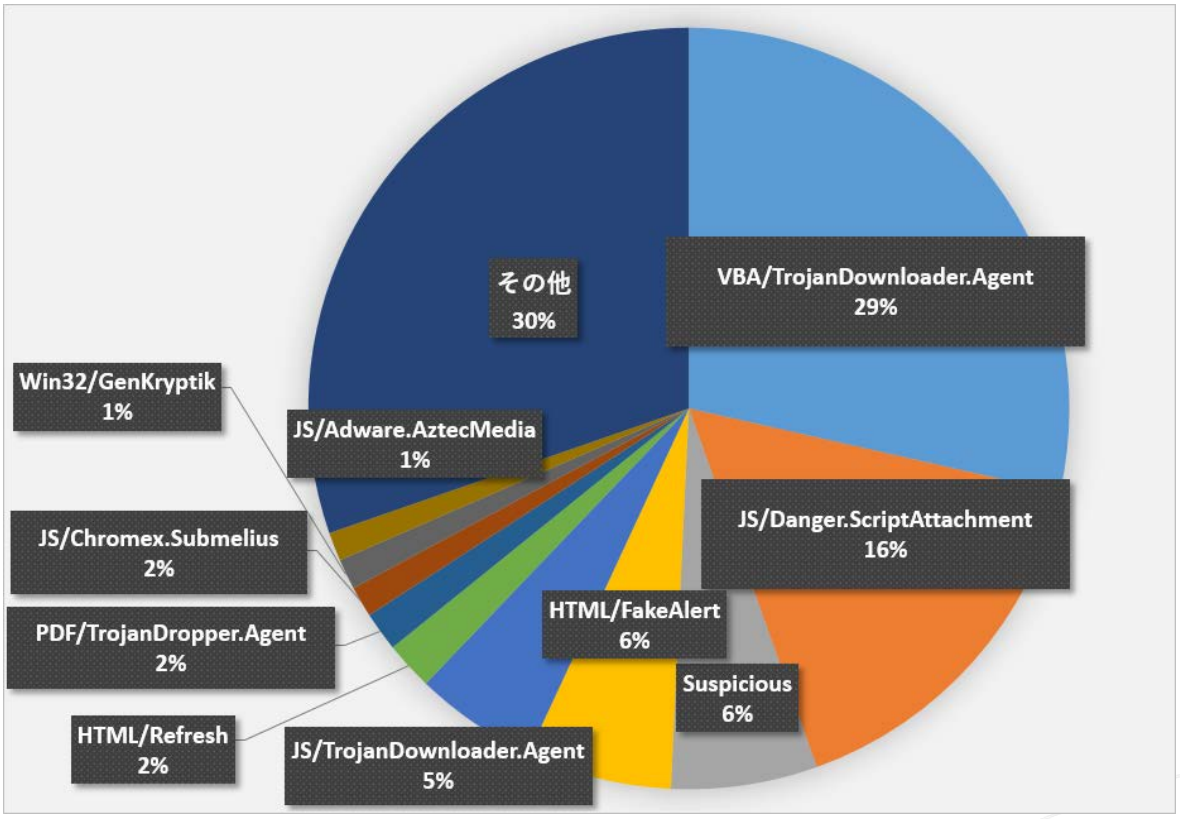
「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2017 年 7 月マルウェア検出状況」

1. 2017 年 7 月の概況

弊社マルウェアラボでは、2017 年 7 月 1 日から 31 日までの ESET 製品国内利用の検出状況について集計しました。6 月と同様に、メール経由のダウンローダー（別のマルウェアをダウンロードするマルウェア）が半数近くを占めていて、中でも VBA（Microsoft Office で利用できるプログラミング言語）を悪用したダウンローダーが急増しています。
また、偽の警告メッセージを表示する Web サイトに埋め込まれたコード（HTML/FakeAlert）が多く検出されています。

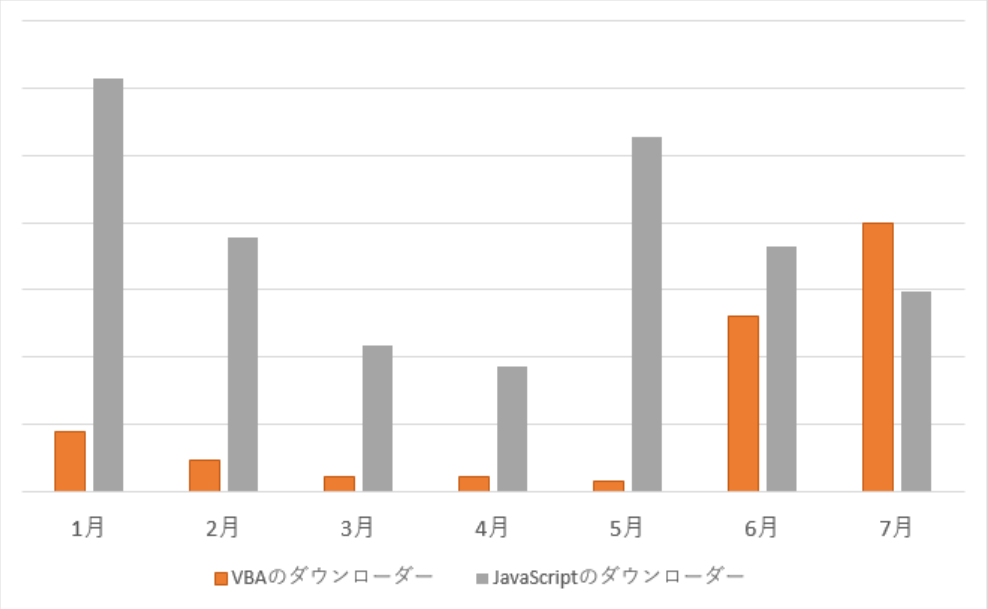


日本国内マルウェア検出状況　上位 10 種の検出比率（2017 年 7 月）
(ESET 社　VIRUS RADAR より)

順位	マルウェア名	種別	割合
1	VBA/TrojanDownloader.Agent	ダウンローダー	29%
2	JS/Danger.ScriptAttachment)	ダウンローダー	16%
3	Suspicious	未知の不審なファイル	6%
4	HTML/FakeAlert	偽の警告メッセージ表示	6%
5	JS/TrojanDownloader.Agent	ダウンローダー	5%
6	HTML/Refresh	別サイト誘導	2%
7	PDF/TrojanDropper.Agent	ドロッパー	2%
8	JS/Chromex.Submelius	偽の警告メッセージ表示	2%
9	Win32/GenKryptik	汎用検出名	1%
10	JS/Adware.AztecMedia	アドウェア	1%

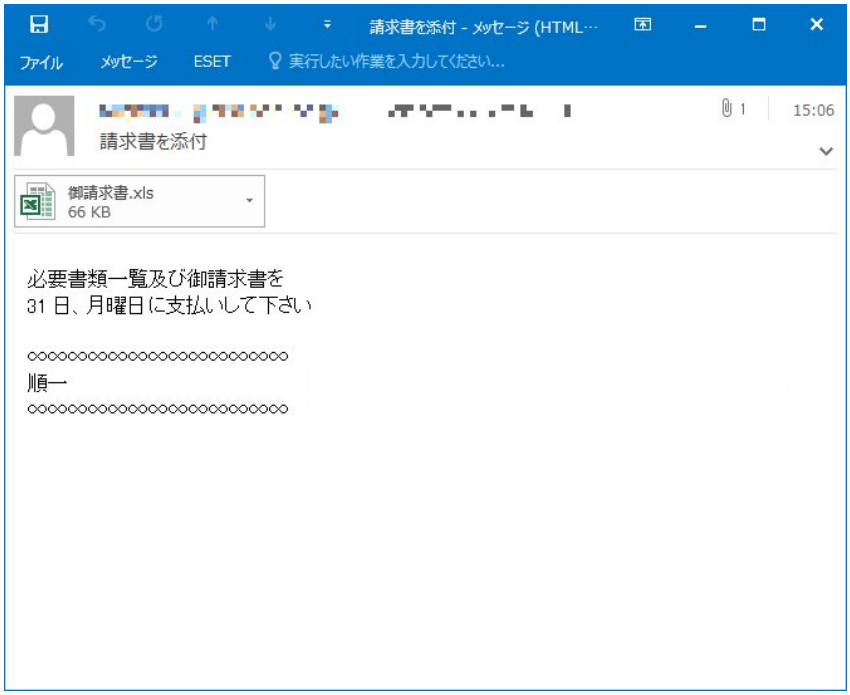
2.「VBA」を悪用したマルウェア

ここ数ヶ月、ダウンローダー型のマルウェアは JavaScript 形式のものが大半を占めていましたが、7 月は「VBA（Visual Basic for Applications）」を悪用した Microsoft Office のドキュメント形式のものが最も多く検出されています。
JavaScript のダウンローダーに対するウイルス対策ソフトウェアの検知率が向上したために、別の手法を試している可能性が考えられます。



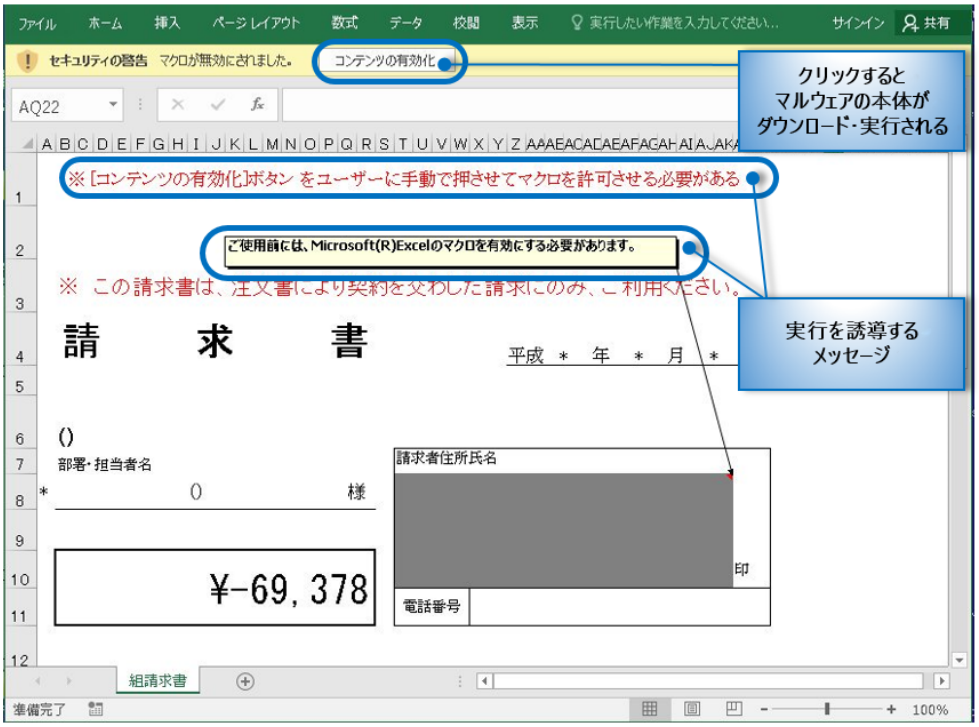
日本国内マルウェア検出状況　上位 10 種の検出比率（2017 年 7 月）
(ESET 社　VIRUS RADAR より)
VBA のダウンローダー：「VBA/TrojanDownloader.Agent」
JavaScript のダウンローダー：「JS/Danger.ScriptAttachment」と「JS/TrojanDownloader.Agent」との合算

VBA を悪用した Microsoft Office ドキュメントは、多くの場合メール経由で拡散されています。



マルウェアを含む Excel ファイルが添付されたメール

Microsoft Office の標準設定では、VBA コンテンツの実行前に警告が表示されます。しかしながら VBA は業務で利用されることも多いため警告を非表示にしているケースも多く、気付かずに VBA を実行してしまうこともあり得ます。セキュリティの観点から、Microsoft Office のマクロは無効、もしくは警告を表示するよう設定しておくことをおすすめします。
また、VBA コンテンツを有効化させるように、巧みに誘導するものも確認されています。
不用意に実行を許可してしまわないよう注意が必要です。

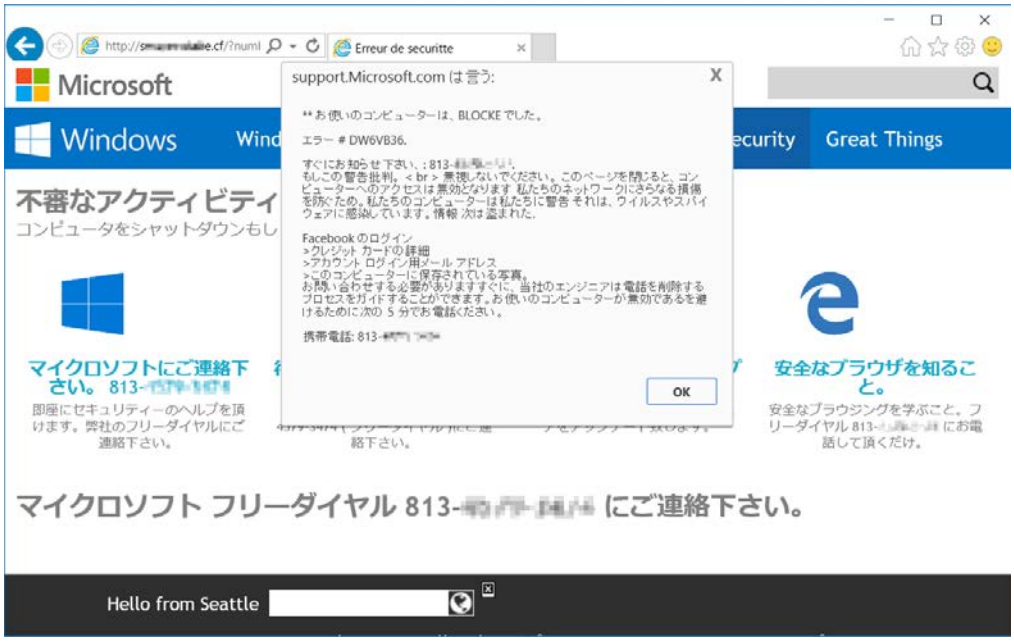


VBA マルウェア付きの Excel ファイル

3. Microsoft の技術サポートを装った詐欺サイト

検出数 4 位の「HTML/FakeAlert」は、偽の警告メッセージを表示する Web サイト（埋め込まれたスクリプト）に対する検出名です。

Microsoft をかたった技術サポートの詐欺サイトが多く確認されています。詐欺サイトへアクセスするとダイアログが表示されます（ダイアログは一度閉じても、再び表示されます）。ダイアログとともに、音声でユーザーに対する警告メッセージが流れます。 詐欺サイトは、「パソコンからマルウェアが検出されました」とユーザーの不安を煽り、偽のサポート窓口に電話をかけるよう促します。この窓口に電話をかけると、架空の有償サポート契約を結ぶよう迫られます。

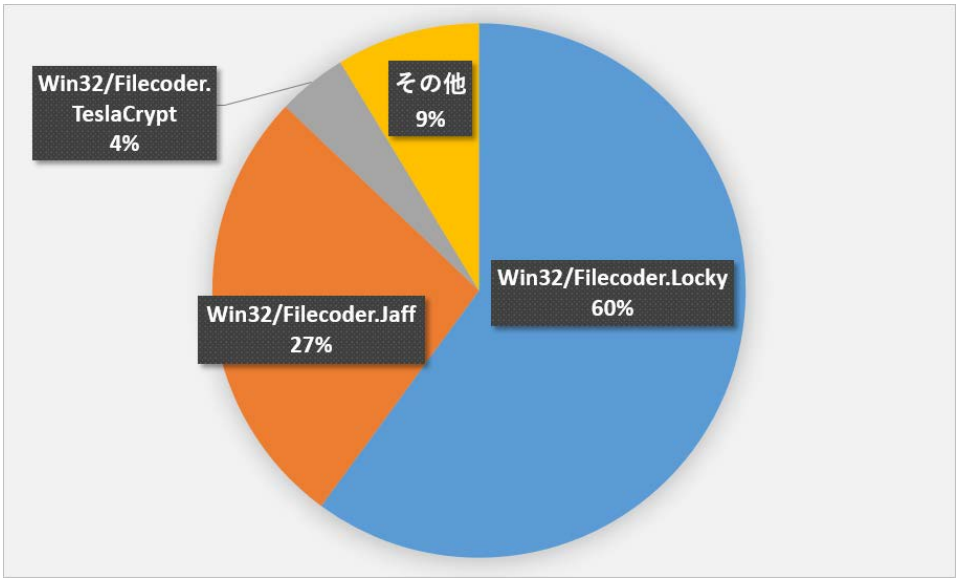


Microsoft を騙った技術サポートの詐欺サイト

現在のところ、これらのサイトにアクセスして実際にウイルスに感染することはまれですが、念のためウイルス対策ソフトウェアで感染していないかを確認（ESET 製品では、「スマート検査」を実行）することをお勧めします。

4．ランサムウェア「Locky」の脅威

ダウンローダーがダウンロードするマルウェアとして、ランサムウェアが多く確認されました。7 月に最も多く検出されたランサムウェアは「Locky（Win32/Filecoder.Locky）」です。

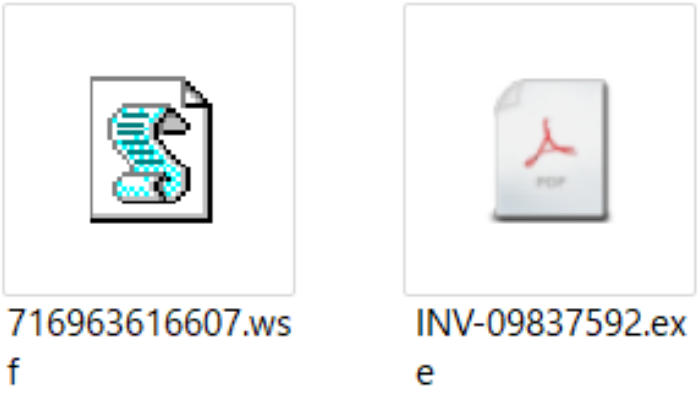


日本国内のランサムウェア　検体種類別の検出数比率（2017 年 7 月）

2016 年 2 月に初めて確認された Locky ですが、プログラムコードを改良しながら、今なお活動を続けています。

Locky は、特定の拡張子を持つファイルのみを暗号化します。暗号化の対象となった拡張子は、2016 年 2 月に確認された検体のおよそ 150 種類から、2017 年 7 月に確認された検体ではおよそ 450 種類に増加しています。また、従来のドキュメントファイルやマルチメディア（画像・音声・動画）ファイルに加えて、データベースファイルやゲームのセーブデータファイルなど、様々なファイルが暗号化の対象となっています。このことから、個人法人問わずあらゆるユーザーが Locky の標的とされていることがうかがえます。

主な感染経路はメールによるもので、ダウンローダー（ユーザーによる実行後、Locky をダウンロード及び実行するマルウェア）を送付する手口と、Locky 本体を直接（ZIP 等で圧縮した上で）送付する手口が確認されています。



左：Locky のダウンローダー（Windows スクリプト形式）
右：PDF ファイルのアイコンに偽装した Locky 本体の実行ファイル

ご紹介したように、マルウェアの仕組みと拡散手法は日々巧妙化しています。最新の脅威について、常に情報をキャッチアップすることが大切です。

■ 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 製品プログラムの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、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
ウイルスの多くは、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
ウイルスの多くが狙う「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
万が一ウイルスに感染した場合、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」の方がウイルスに感染するリスクは低いと考えられます。ウイルス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 ITソリューションズ株式会社

eset-info.canon-its.jp/