2021年
9月
SEPTEMBER

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

Canon キヤノンマーケティングジャパン株式会社

はじめに

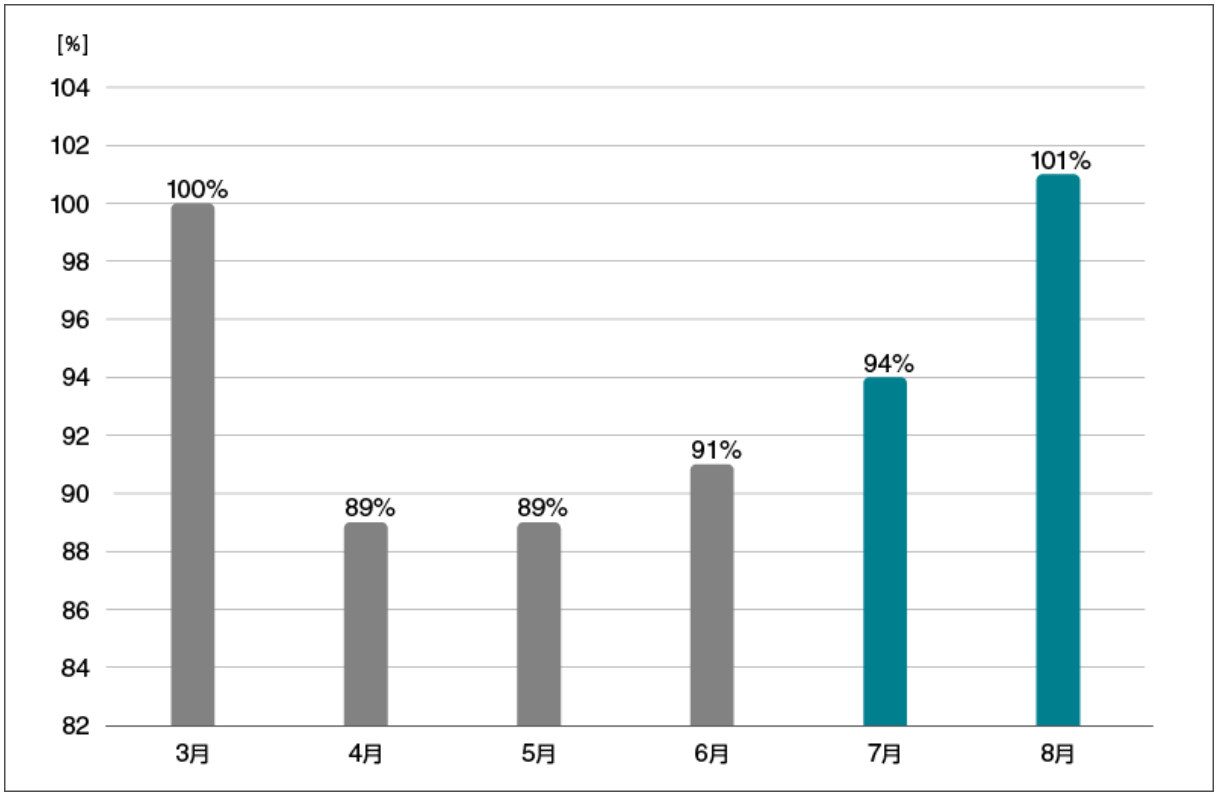
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 9 月マルウェア検出状況

2021 年 9 月（9 月 1 日～9 月 30 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 4 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 9 月の国内マルウェア検出数は、2021 年 8 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

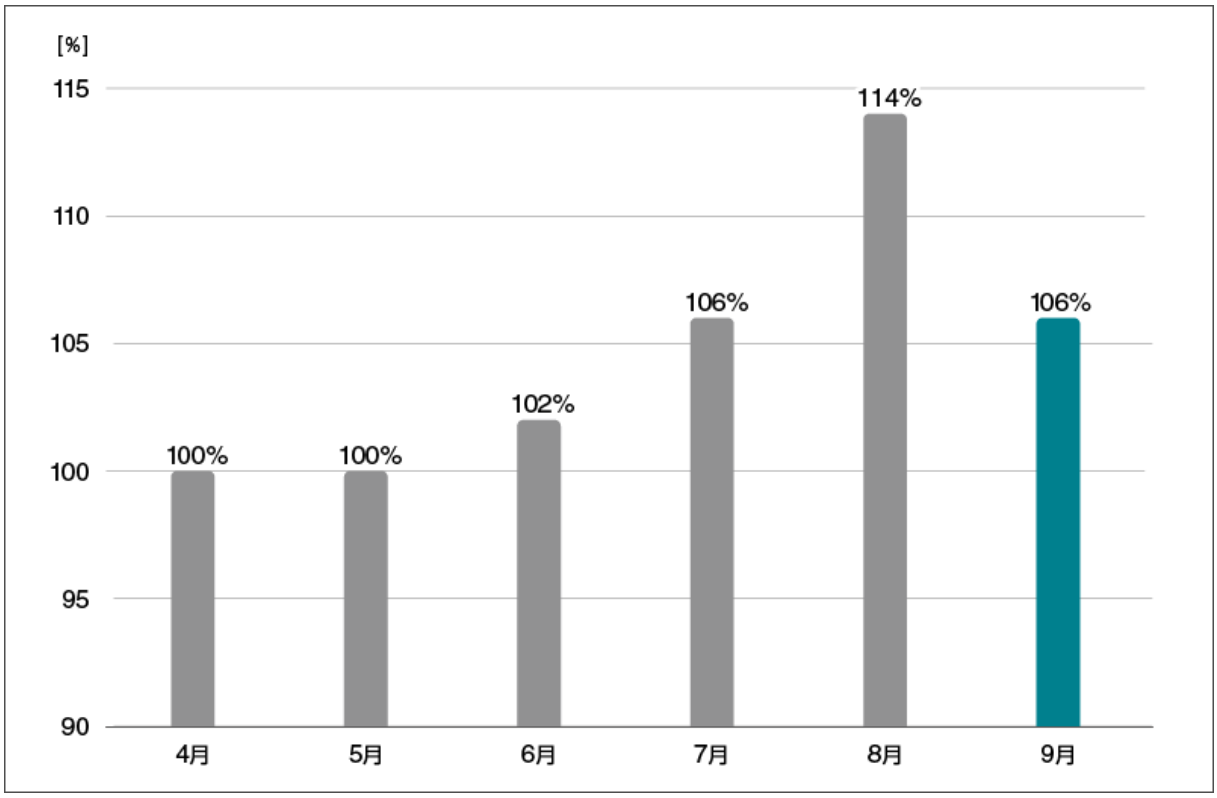
国内マルウェア検出数*2 上位（2021 年 9 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	24.1%	アドウェア
2	HTML/Phishing.Agent	11.4%	メールに添付された不正な HTML ファイル
3	JS/Adware.Sculinst	8.9%	アドウェア
4	JS/Adware.Subprop	4.3%	アドウェア
5	JS/Adware.TerraClicks	4.1%	アドウェア
6	HTML/FakeAlert	1.9%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.PopAds	1.5%	アドウェア
8	Win32/Exploit.CVE-2017-11882	1.1%	脆弱性を悪用するマルウェア
9	HTML/Fraud	1.0%	詐欺サイトのリンクが埋め込まれた HTML ファイル
10	HTML/ScrInject	1.0%	HTML に埋め込まれた不正スクリプト

*2 本表には PUA を含めていません。

9 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。

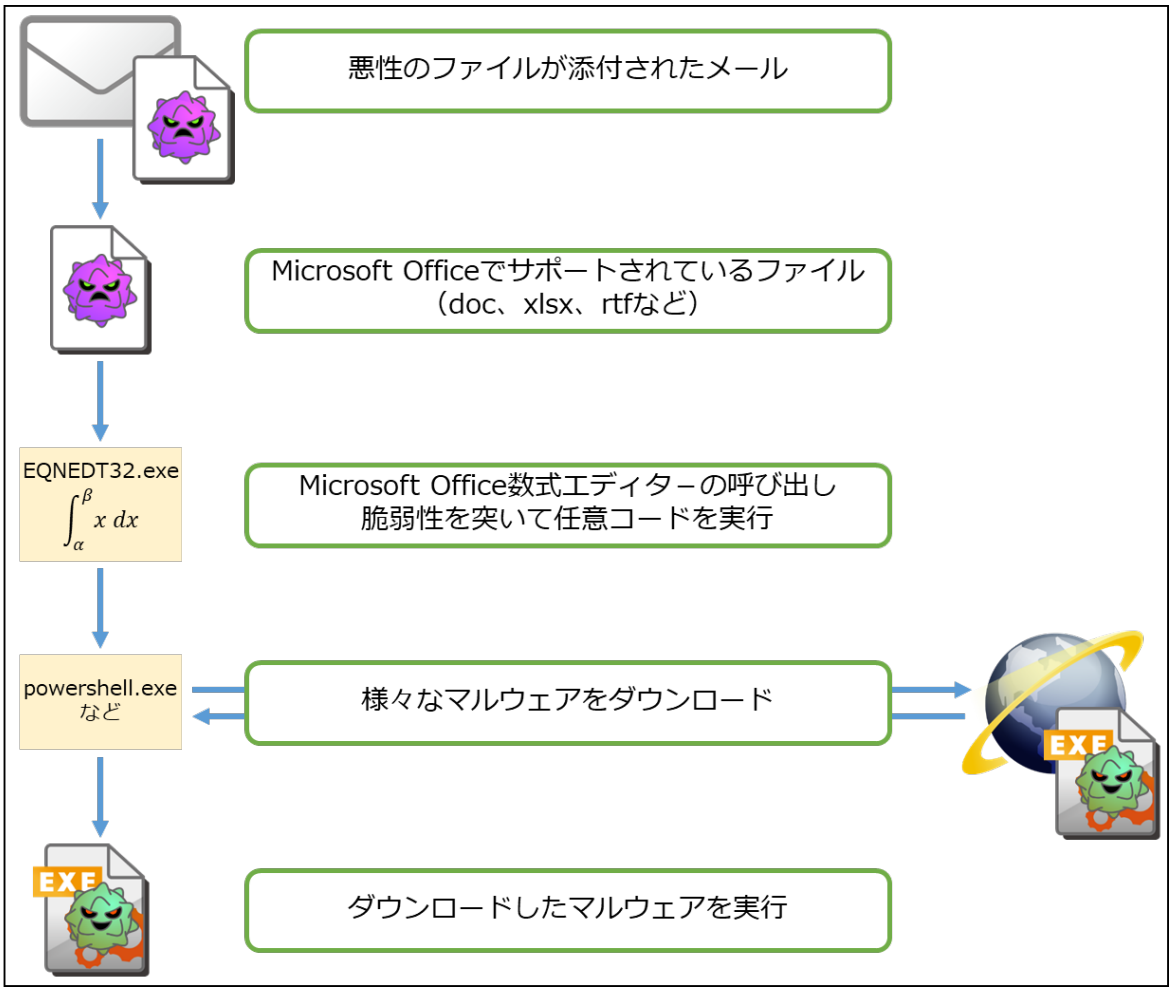
9 月の検出数 8 位の Win32/Exploit.CVE-2017-11882 は Microsoft Office 数式エディターの脆弱性（CVE-2017-11882）[1)] を悪用した脅威です。2017 年 11 月に公表された脆弱性ですが、今年の 8 月から検出数が増加傾向にあります。この脆弱性を悪用した脅威を 2017 年 11 月の定期マルウェアレポートで取り上げましたが、再び脅威が広がっていることから改めて紹介します。



国内における Win32/Exploit.CVE-2017-11882 検出数の推移
（2021 年 4 月の全検出数を 100%として比較）

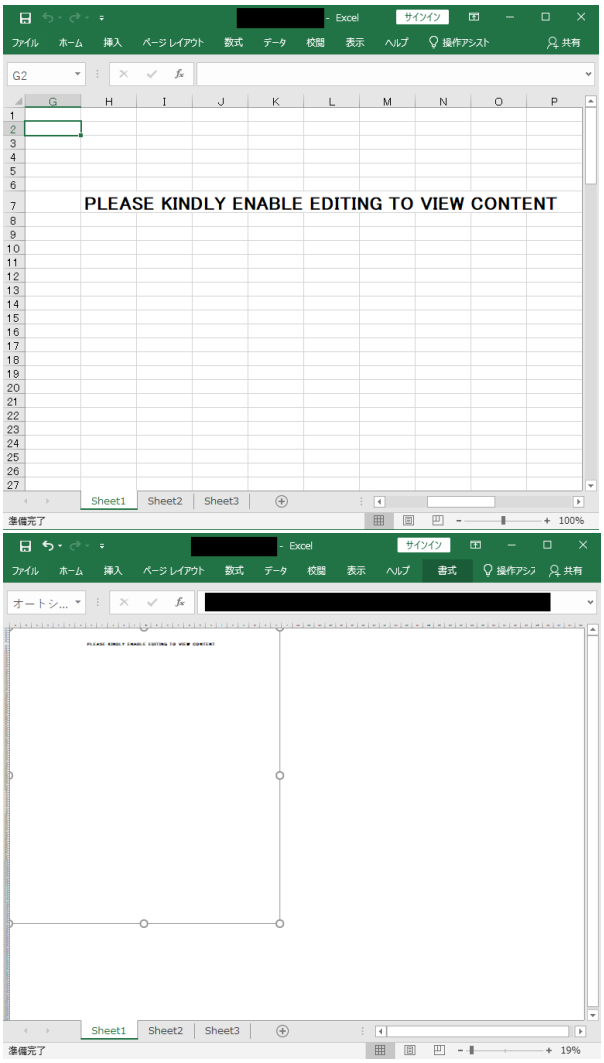
Microsoft Office 数式エディターは、Microsoft Office 2003 以前のバージョンの Microsoft Office において数式を入力するために使用されるソフトウェアです。Microsoft Office 2007 以降の Microsoft Office においては互換性を維持するために搭載されていました。このソフトウェアの脆弱性（CVE-2017-11882）が悪用されると、攻撃者によってリモートで任意のコードが実行される可能性があります。

具体的には、本脆弱性に対する悪意のあるコードを実装した Microsoft Office ファイルが、さまざまなマルウェアのダウンローダーとして利用された事例を確認しています。2017 年 11 月時点ではバンキングマルウェア（バンキングサイトの認証情報などを窃取するマルウェア）である「Ursnif」のダウンローダーとして利用された事例を確認していました。さらに 2021 年 9 月では情報窃取型マルウェアである「AgentTesla」や「FormBook」などのダウンローダーとして利用された事例を確認しています。

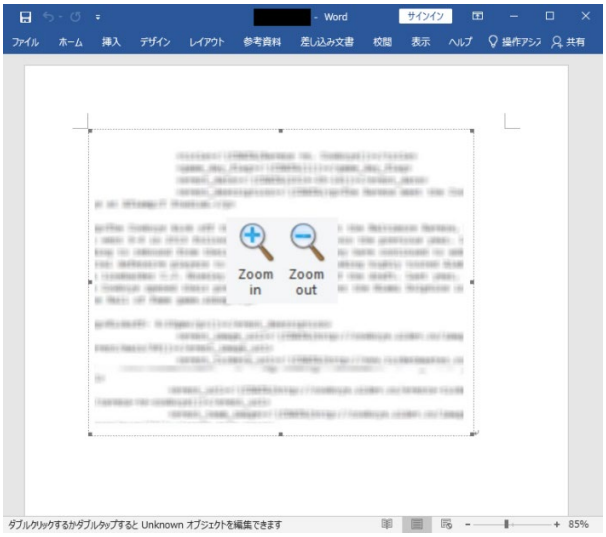


Microsoft Office 数式エディターの脆弱性を悪用した攻撃の事例

Microsoft Office ファイルで悪用されることが多いマクロマルウェアでは、マクロが有効化されない限り脅威にさらされる危険性はありません。しかし本脆弱性を悪用した Microsoft Office ファイルの場合、実装方法によってはファイルを開くだけで悪意のあるコードが実行されてマルウェア感染する恐れがあります。このような悪意のあるコードは、Windows のアプリケーション間で連携または共有されるデータである OLE（Object Linking & Embedding）オブジェクトとして Microsoft Office ファイル内に埋め込まれています。この OLE オブジェクトはユーザーがその存在に気づかないよう視認性が悪い状態で配置されたり、ユーザーのクリックを促すような画像と併用して配置されたりすることがあります。



本脆弱性を悪用するコードが埋め込まれたファイルの例①
上図は表示倍率が 100%の状態、下図は 19%の状態
透明な背景の巨大な OLE オブジェクトにコードが埋め込まれている



本脆弱性を悪用するコードが埋め込まれたファイルの例②
画像ファイルをクリックすることでコードが実行される

2021 年 7 月に米国、イギリス、オーストラリアのセキュリティ機関が、悪用の多い脆弱性 30 件を公表[2)]しました。この 30 件のうち最も古い脆弱性として本脆弱性である CVE-2017-11882 が挙げられています。公表によると、既知の脆弱性を利用することは攻撃者グループの特定を困難にし、ゼロデイ攻撃に利用するエクスプロイトキットを新規開発するよりもコストを抑えることができるとのことです。また Microsoft Office は世界中で利用されており、段階的な攻撃キャンペーンを展開しやすい点やリモートで任意のコードを実行できる点で攻撃者にとって有用であることから、今後も本脆弱性を悪用し続ける可能性が高いと言及しています。
本脆弱性に関する対策として、2017 年 11 月の更新プログラム[1)]や Microsoft Office 数式エディターの無効化方法[3)]、2018 年 1 月の更新プログラム[4) 5) 6) 7)]を Microsoft 社が順次公開しました。特に 2018 年 1 月の更新プログラムでは、Microsoft Office 数式エディターが Windows から削除されるため本脆弱性による影響は受けなくなります。しかしこれらの対策が公開された後も本脆弱性を狙った攻撃は継続して観測されています。

上述のとおり Microsoft Office 数式エディターは Microsoft Office 2007 以降の Microsoft Office における互換性維持のために搭載されていたソフトウェアです。脆弱性が存在するソフトウェアを使用し続けることは危険です。Microsoft Office 数式エディターを使用して数式が記述された Microsoft Office ファイルを開く必要がなければ、早急に更新プログラムの適用を検討してください。また本脆弱性を悪用した Microsoft Office ファイルは、電子メール経由で送付されることを確認しているため、電子メールの添付ファイルを不用意に開かないよう注意してください。

■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．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

1) CVE-2017-11882 - セキュリティ更新プログラム ガイド - Microsoft - Microsoft Office のメモリ破損の脆弱性
2) Top Routinely Exploited Vulnerabilities | CISA
3) How to disable Equation Editor 3.0
4) 2007 Microsoft Office スイート セキュリティ更新プログラムについて 2018 年 1 月 9 日
5) Office 2010 用のセキュリティ更新プログラムについて 2018 年 1 月 10 日
6) Office 2013 用のセキュリティ更新プログラムについて 2018 年 1 月 10 日
7) Office 2016 用のセキュリティ更新プログラムについて: 2018 年 1 月 10 日

Canon

キヤノンマーケティングジャパン株式会社