2022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

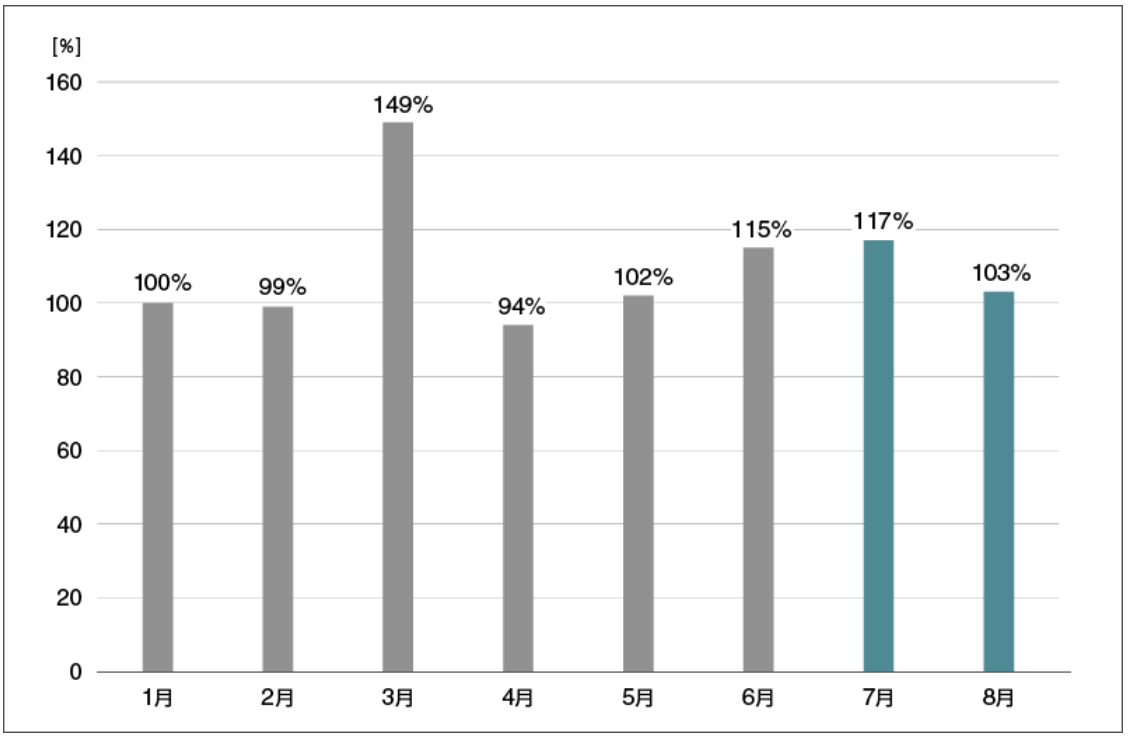
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2022 年 7 月･8 月マルウェア検出状況

2022 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
(2022 年 1 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。

2022 年 7 月と 8 月の国内マルウェア検出数は、2022 年 6 月から 7 月にかけては増加しており、7 月から 8 月にかけては減少しています。Emotet への感染を狙ったばらまきメールの送信停止に伴うダウンローダー検出数の減少や一部のアドウェアの検出数減少などが要因として考えられます。
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（2022 年 7 月·8 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	13.7%	アドウェア
2	JS/Packed.Agent	13.2%	パックされた不正な JavaScript の汎用検出名
3	JS/Adware.Agent	8.9%	アドウェア
4	HTML/Pharmacy	8.6%	違法薬品の販売サイトに関連する HTML ファイル
5	HTML/FakeAlert	4.3%	偽の警告文を表示させる HTML ファイル
6	HTML/Phishing.Agent	4.0%	メールに添付された不正な HTML ファイル
7	DOC/TrojanDownloader.Agent	3.5%	ダウンローダー
8	JS/Adware.Sculinst	3.1%	アドウェア
9	HTML/ScrInject	2.5%	HTML に埋め込まれた不正スクリプト
10	MSIL/Kryptik	1.8%	難読化された MSIL で作成されたファイルの汎用検出名

国内マルウェア検出数*2 上位（2022 年 7 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClick	16.9%	アドウェア
2	JS/Packed.Agent	10.7%	パックされた不正な JavaScript の汎用検出名
3	JS/Adware.Agent	10.3%	アドウェア
4	HTML/Pharmacy	9.0%	違法薬品の販売サイトに関連する HTML ファイル
5	DOC/TrojanDownloader.Agent	6.1%	ダウンローダー
6	HTML/FakeAlert	3.7%	偽の警告文を表示させる HTML ファイル
7	HTML/Phishing.Agent	2.9%	メールに添付された不正な HTML ファイル
8	JS/Adware.Sculinst	2.7%	アドウェア
9	HTML/ScrInject	2.4%	HTML に埋め込まれた不正なスクリプト
10	MSIL/Kryptik	0.8%	難読化された MSIL で作成されたファイルの汎用検出名

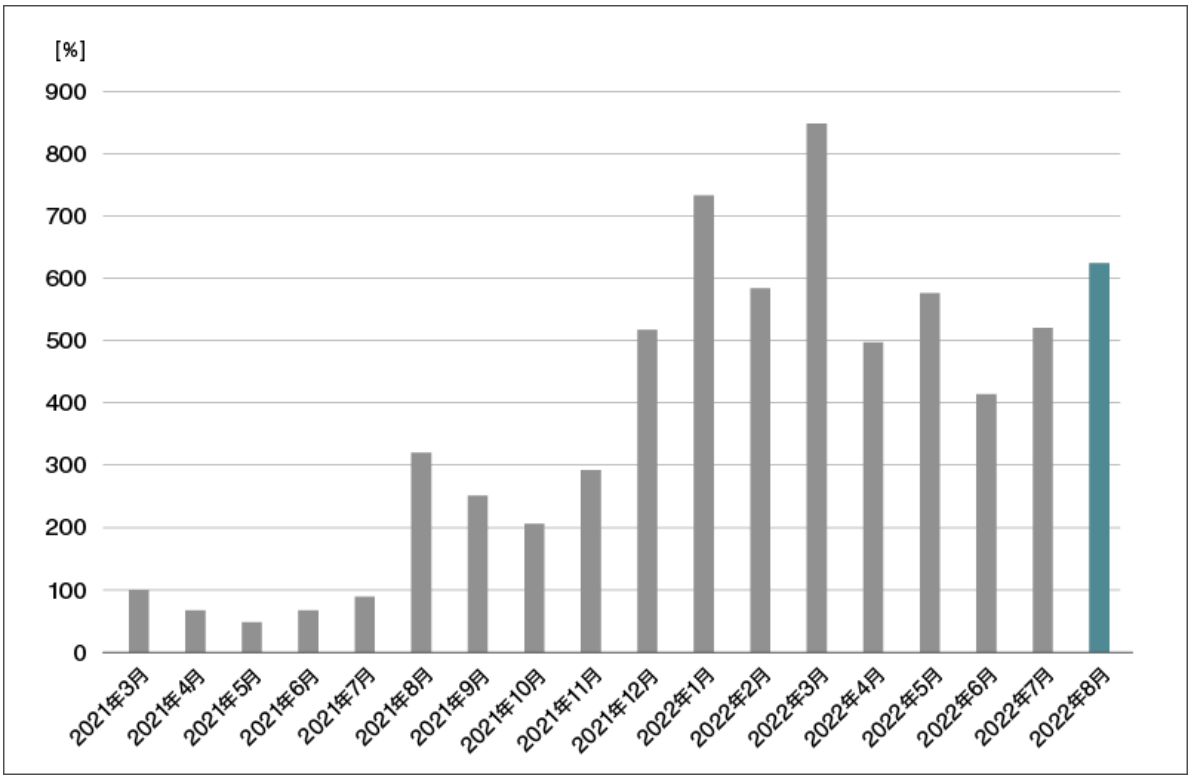
国内マルウェア検出数*2 上位（2022 年 8 月）

順位	マルウェア	割合	種別
1	JS/Packed.Agen	16.6%	パックされた不正な JavaScript の汎用検出名
2	JS/Adware.TerraClicks	10.6%	アドウェア
3	HTML/Pharmacy	8.6%	違法薬品の販売サイトに関連する HTML ファイル
4	JS/Adware.Agent	7.6%	アドウェア
5	HTML/Phishing.Agent	5.4%	メールに添付された不正な HTML ファイル
6	HTML/FakeAlert	5.1%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.Sculinst	3.7%	アドウェア

8	HTML/ScrInject	2.7%	HTML に埋め込まれた不正なスクリプト
9	MSIL/Kryptik	2.0%	難読化された MSIL で作成されたファイルの汎用検出名
10	DOC/TrojanDownloader.Agent	0.8%	ダウンローダー

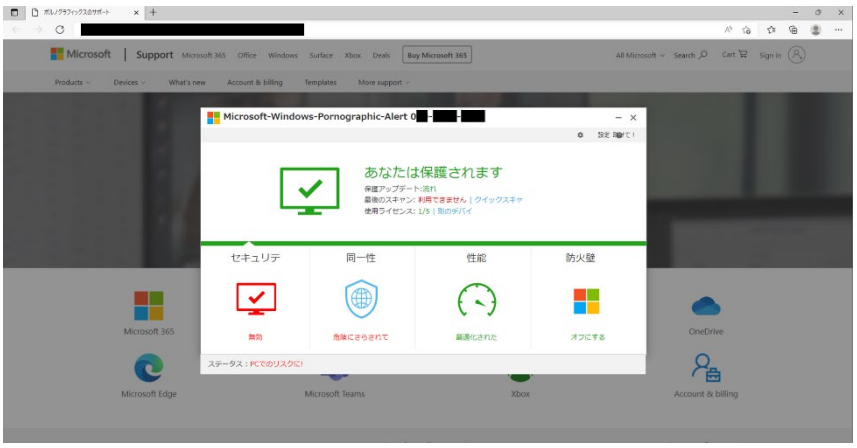
*2 本表には PUA を含めていません。

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.TerraClicks でした。
JS/Adware.TerraClicks は、Web サイト閲覧時に実行されるアドウェアの検出名です。感染すると、アドウェアが仕組まれた Web サイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。
その他にも、アドウェアやダウンローダーをはじめとしたさまざまなマルウェアを確認しています。例えば、2022 年 7 月･8 月の検出数第 10 位の「MSIL/Kryptik」では、Snake Keylogger や Formbook といった情報窃取型のマルウェアが検出されていました。
今回は、2022 年を通して検出され続けており、7 月と 8 月に検出数が増加している「HTML/FakeAlert」について紹介します。
HTML/FakeAlert は、偽の警告文を表示させる HTML ファイルです。Windows のサポートを騙ったものが確認されています。Windows のサポート詐欺については、各種メディアで取り上げられており、Microsoft 社と消費者庁からも注意喚起が行われています。
HTML/FakeAlert は、2021 年 3 月のマルウェアレポートでも紹介しています。2021 年 3 月の検出数と比較すると、約 6 倍となっています。



HTML/FakeAlert の検出数月別推移（国内）
（2021 年 3 月の検出数を 100%として比較）

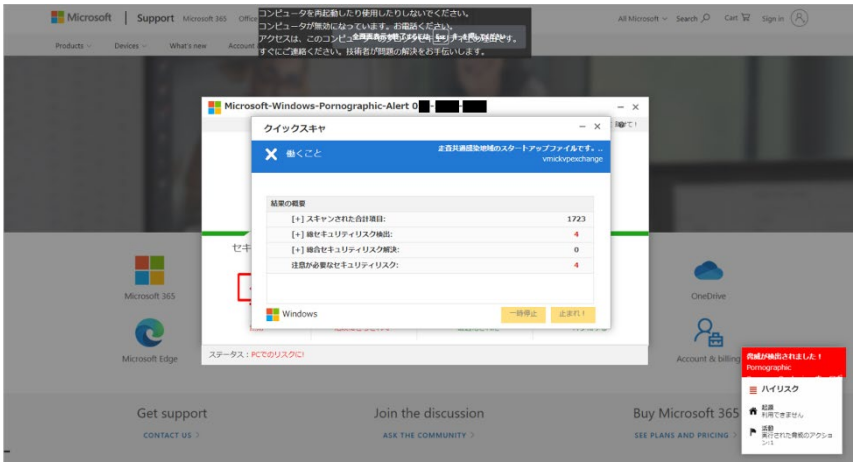
Windows のサポート詐欺を狙った HTML/FakeAlert の 1 つにアクセスすると、Microsoft 社の Web サイトの画像の上から Microsoft Defender によるマルウェア検知を騙った警告文が大きな音とともに表示されます。



アクセスした際の表示画面

警告文には、さまざまな検出名が表示されます。また、攻撃者が用意した電話番号も表示しています。こちらは、Microsoft 社のサポートの電話番号ではありません。この検体では、ポルノコンテンツが含まれた Web サイトにアクセスしたことによるマルウェア検知を装っています。
この検体を 2021 年 3 月マルウェアレポートで紹介した例と比較すると、表示されるポップアップに違いはありましたが、大きな機能の変化はありませんでした。

2021 年 3 月と 2022 年 7 月・8 月の検体の両方で、アクセス中の画面でクリックなどの操作を行うと、ブラウザーが全画面表示に切り替わります



全画面表示に切り替わった Web サイト

全画面表示では、Web ブラウザーのタブやブラウザー本体の「ウィンドウを閉じるボタン」を選ぶことができません。加えて、操作ができなくなった旨が書かれたポップアップも表示されるため、操作ができなくなったユーザーを焦らせます。
全画面表示になってしまった際は、以下の操作のいずれかを試してください。
・F 11 または Esc キーを押す
・Esc キー＋Shift キー＋Ctrl キーを同時に押して、タスクマネージャーを起動し、ブラウザーを終了させる
・右クリックから「全画面表示を終了」を選択（利用ブラウザーが Chrome の場合）
・画面上部にマウスカーソルを移動させると表示される「×ボタン」をクリック

攻撃者の目的としては、用意した電話番号に電話をかけさせることが挙げられます。
通話すると、プリペイドカードを購入し、カードに書かれたシリアルナンバーを電話口で伝えるように指示されます。
他にも、通話先から攻撃者が用意したツールをインストールするように指示されるケースもあります。この場合、攻撃者が用意した RAT などのツールによって、端末をリモートで操作される恐れがあります。

今回ご紹介したとおり、大きな警告音と共に警告文を表示させる HTML ファイルを継続して検出しています。Web サイトの見た目も精巧になっているため、正規サイトかどうかを見た目で判断することは困難です。また、今回ご紹介した例では日本語の文章が怪しい部分がありましたが、今後修正される可能性があるので注意が必要です。
そして、正規 URL に似た URL を使っているケースも考えられます。アクセスする端末によっては、画面に表示される部分が限られることで、正規サイトのように見える場合があります。表示される電話番号や似たケースがないかなどをインターネット検索し、複数の情報から判断することが重要です。また、日ごろからアクセスしている Web サイトは、ブックマークからアクセスすることを推奨します。

■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

■NHK | 詐欺：“パソコン画面のニセ警告”に注意！
https://www.nhk.or.jp/shutoken/net/20211001s.html
■Microsoft 社 | マイクロソフトのサポートを装った詐欺にご注意ください
https://news.microsoft.com/ja-jp/2021/01/29/210129-information/
■消費者庁｜「Microsoft」のロゴを用いて信用させ、パソコンのセキュリティ対策のサポート料などと称して多額の金銭を支払わせる事業者に関する注意喚起
https://www.caa.go.jp/notice/entry/023149/
■サイバーセキュリティ情報局 | 2021 年 3 月マルウェアレポート
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2103.html
■サイバーセキュリティ情報局 | 遠隔操作ソフトとは？インストールするとセキュリティリスクがあるのか？
https://eset-info.canon-its.jp/malware_info/special/detail/220913.html

Canon

キヤノンマーケティングジャパン株式会社