2020年
6月
JUNE

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

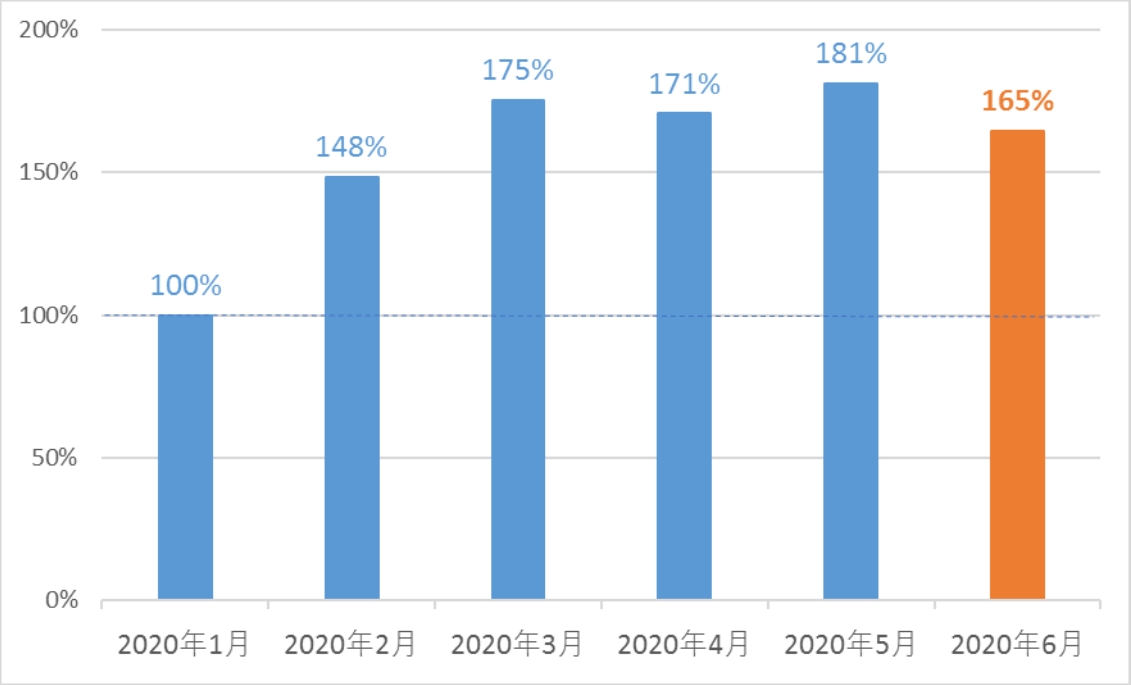
「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

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 6 月マルウェア検出状況」

6 月の概況

2020 年 6 月（6 月 1 日～6 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
(2020 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。

2020 年 6 月の国内マルウェア検出数は、直近 6 か月の中で検出数が最も多かった 5 月と同じくらい多いものとなっています。
検出されたマルウェアの内訳は以下のとおりです。

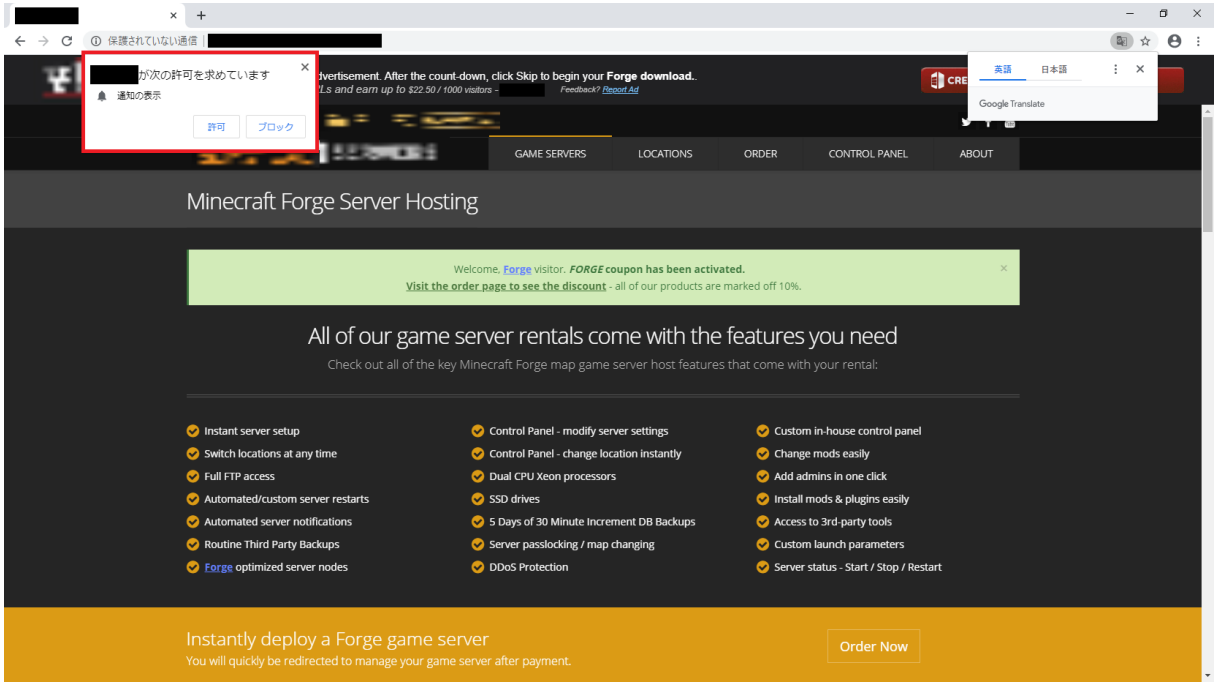
国内マルウェア検出数*2 上位（2020 年 6 月）

順位	マルウェア	割合	種別
1	JS/Adware.Subprop	11.0%	アドウェア
2	JS/Adware.Agent	10.9%	アドウェア
3	JS/Adware.Inpagepush	6.4%	アドウェア
4	HTML/ScrInject	5.9%	HTML に埋め込まれた不正スクリプト
5	JS/Danger.ScriptAttachment	4.9%	ダウンローダー
6	JS/Adware.PopAds	4.2%	アドウェア
7	JS/Adware.Chogdoul	3.0%	アドウェア
8	HTML/Refresh	1.9%	別のページに遷移させるスクリプト
9	VBA/TrojanDownloader.Agent	1.5%	ダウンローダー
10	JS/Adware.Velocity	1.4%	アドウェア

*2 本表には PUA を含めていません。

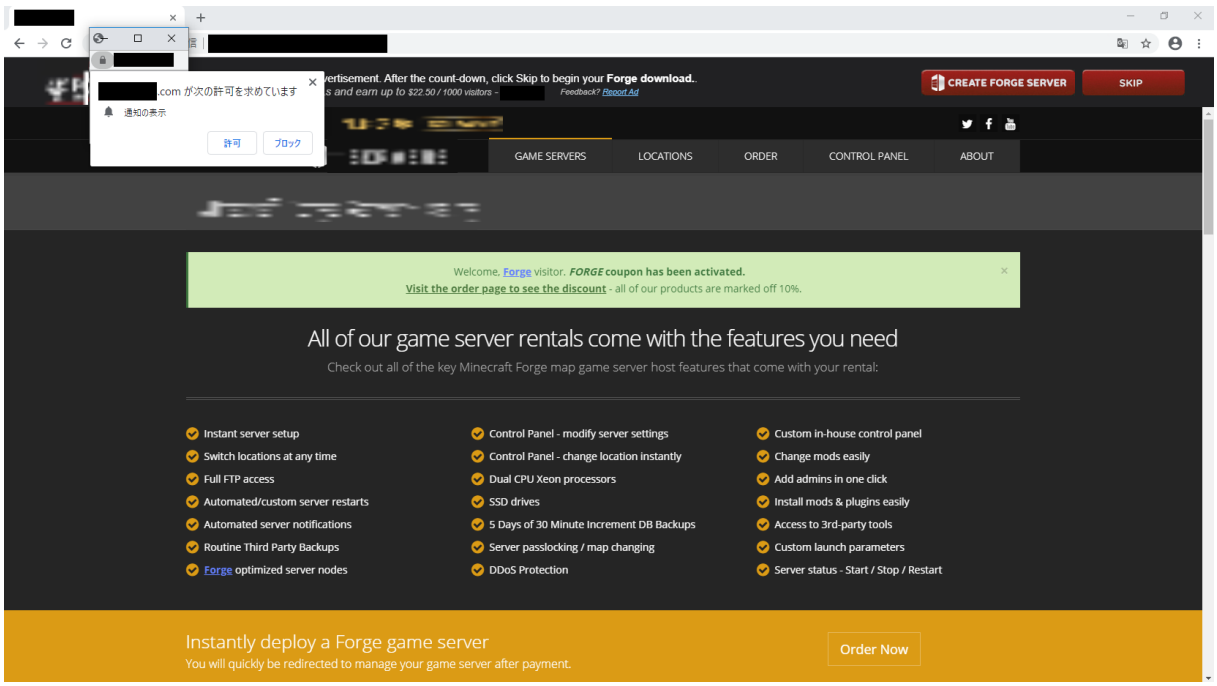
6 月に国内で最も多く検出されたマルウェアは、JS/Adware.Subprop でした。JS/Adware.Subprop は、

不正に広告を表示させるアドウェアで、Web サイト閲覧時に実行されます。
以下に、JS/Adware.Subprop に感染するまでの流れをご紹介します。
下の画像は、アドウェアが仕掛けられた Web サイトです。アクセスすると同時に、画面左上に通知の許可を求めるメッセージが表示されます。表示されたメッセージの[許可]をクリックすると、別の Web サイトがポップアップで表示されます。



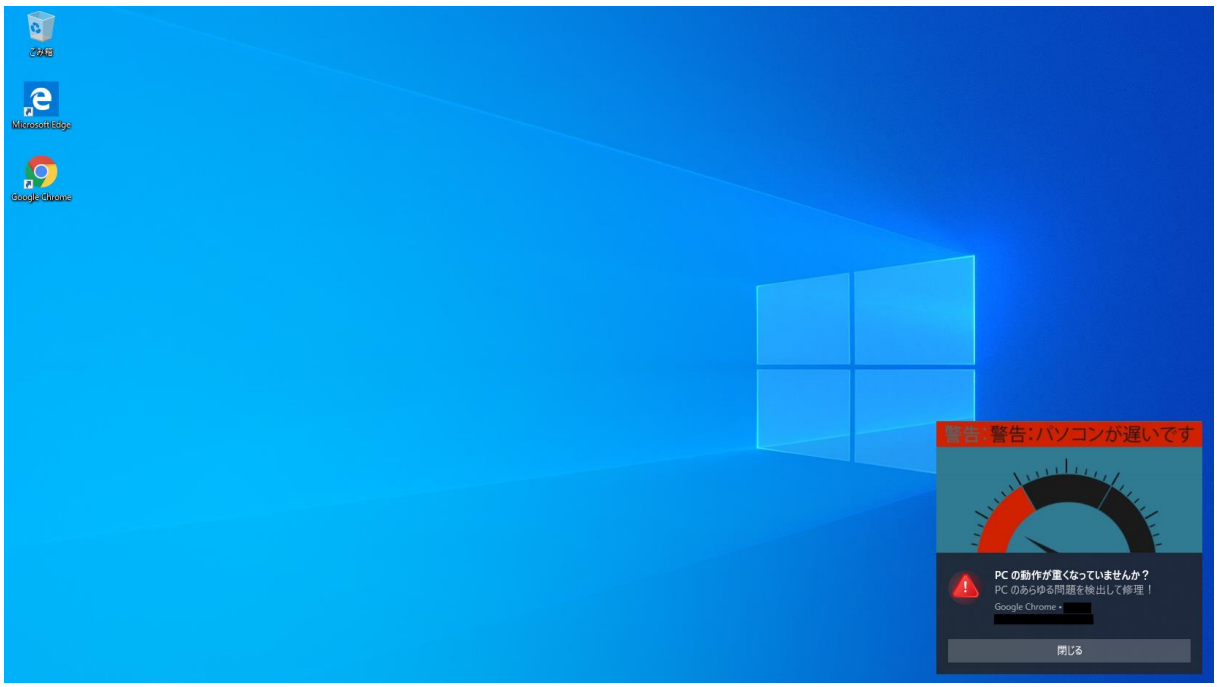
JS/Adware.Subprop が仕掛けられた Web サイト

ポップアップ画面では、画面左上に通知の許可を求めるメッセージがもう一度表示されます。この[許可]をクリックすると JavaScript が実行されます。



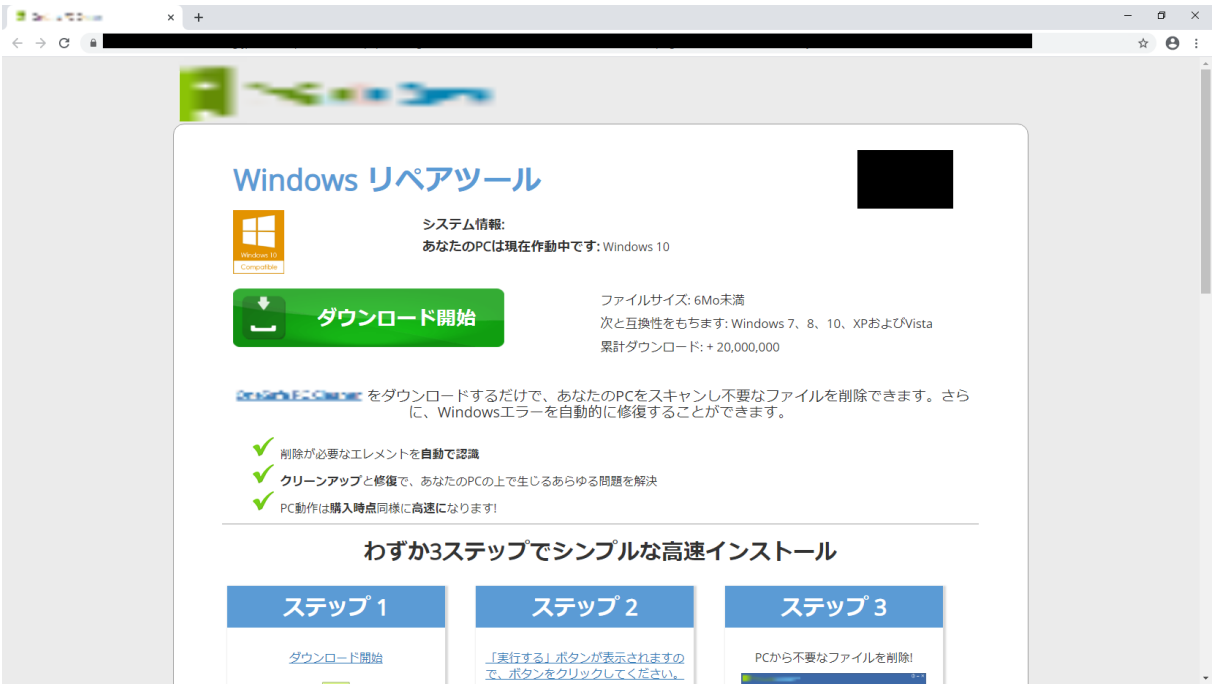
別のサイトへ移動した後に表示される通知の許可を求めるメッセージ

実行後は、下の画像のように PC の動作が遅くなったと偽った広告が表示され続けるようになります。また、表示される広告は、PC の動作の遅さに関するもの以外にも出会い系の広告などがありました。



デスクトップ画面に表示され続ける広告

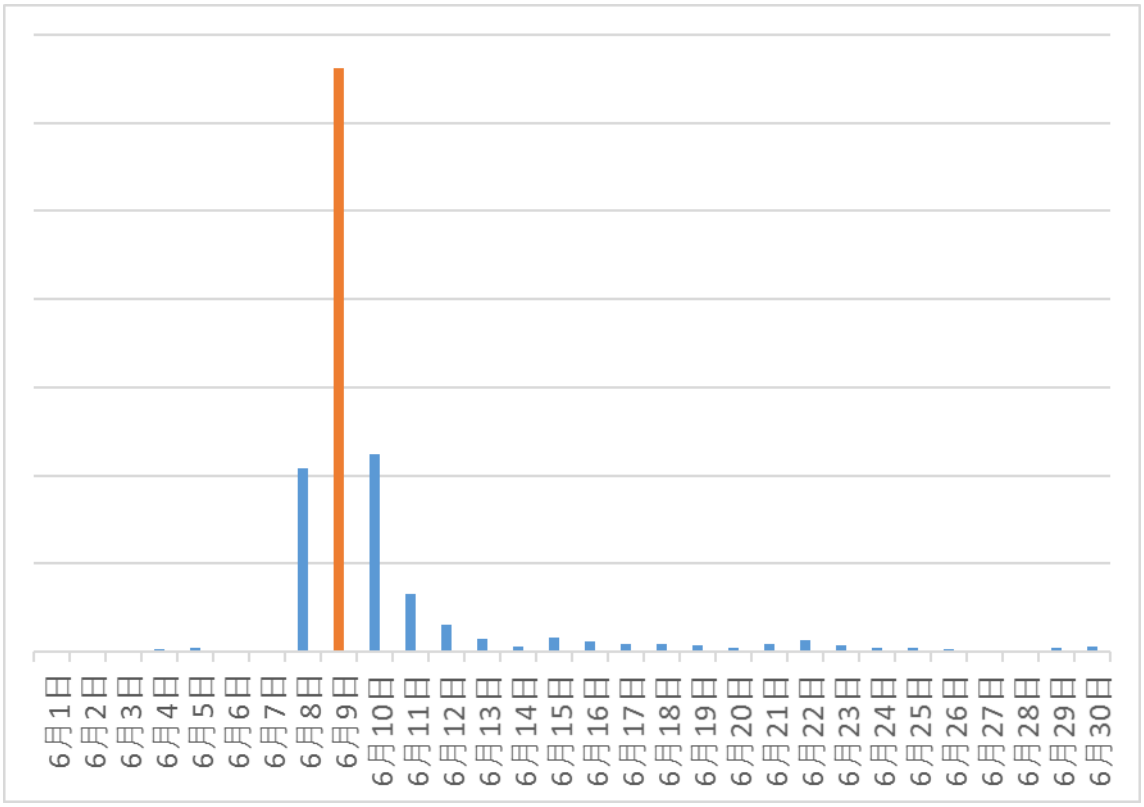
この広告をクリックすると、以下のサイトへアクセスします。
このサイトでは、Windows をリペアするためのツールをインストールさせようとしています。このツールは、PUA として ESET 製品で検出されます。
PUA とは、「必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション」を指しており、注意が必要です。



画面に表示され続ける広告をクリックした際にアクセスする Web サイト

アドウェアの中には、このような不正な広告を表示させるもの以外にも、Web ブラウザーのアクセス履歴を外部へ送信するものもあるので注意が必要です。不用意に許可やインストールを行わないことが重要です。

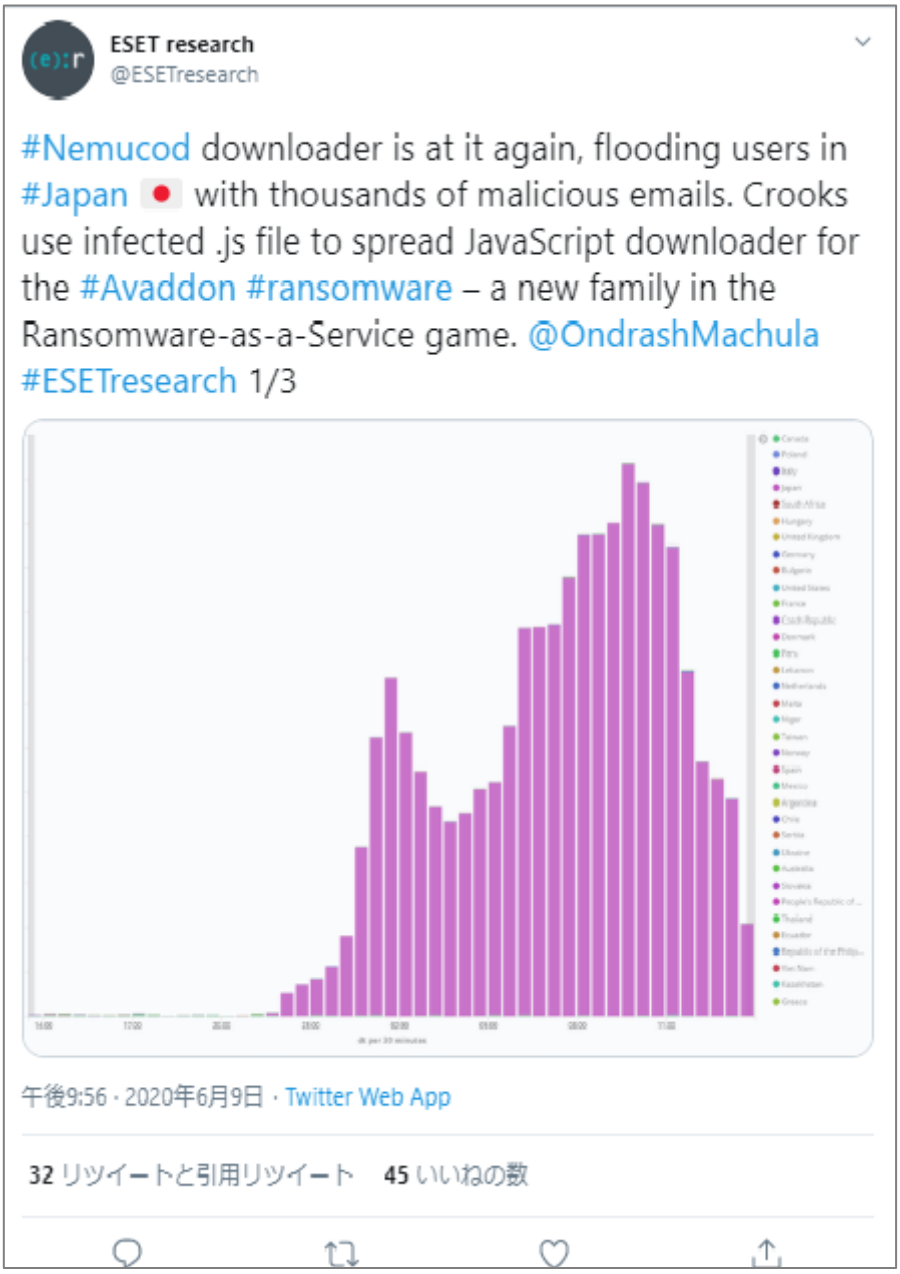
今月は、Web ブラウザー上で実行される脅威以外にも、多数の電子メールによる脅威を確認しました。中でも、検出数 5 位の JS/Danger.ScriptAttachment は、検出数が急増しています。JS/Danger.ScriptAttachment とは、電子メールに添付された悪意のある JavaScript ファイルの汎用検出名です。特定のマルウェアではなく、受信したメールの添付ファイルに悪意があると判断されることで検出されます。
JS/Danger.ScriptAttachment の検出数は、6 月 9 日付近で急増しています。



JS/Danger.ScriptAttachment の日別検出数の推移（国内）

検出数の急増は、JavaScript ファイルによってランサムウェアの感染を狙ったばらまきメールが多数送信されたことによるものです。

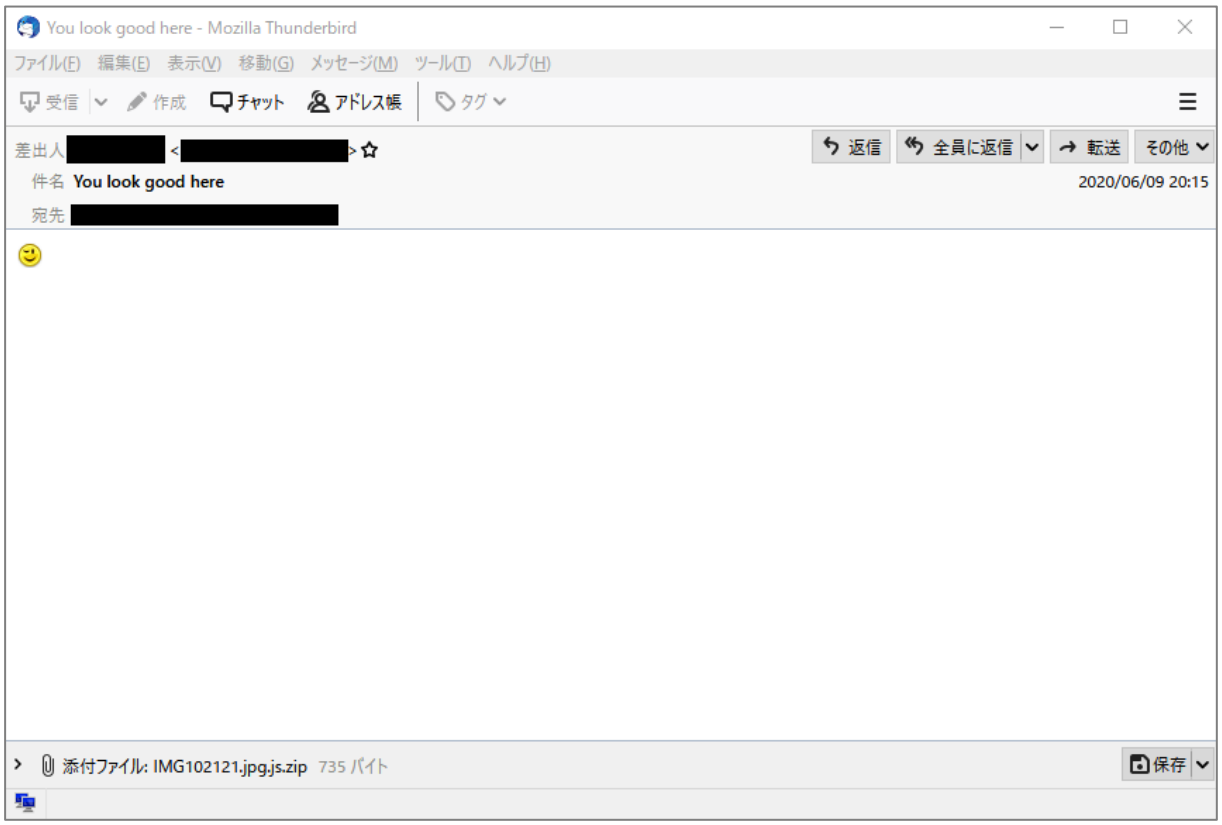
ESET 社も、SNS でこのばらまきメールについて注意喚起を行っています。



ESET 社のばらまきメールについての注意喚起のツイート
（引用元：ESET Research 公式 Twitter）

そのばらまきメールの 1 つが下の画像です。件名は「You look like good」と書かれています。本文の内容は、顔文字が 1 つ書かれているだけです。

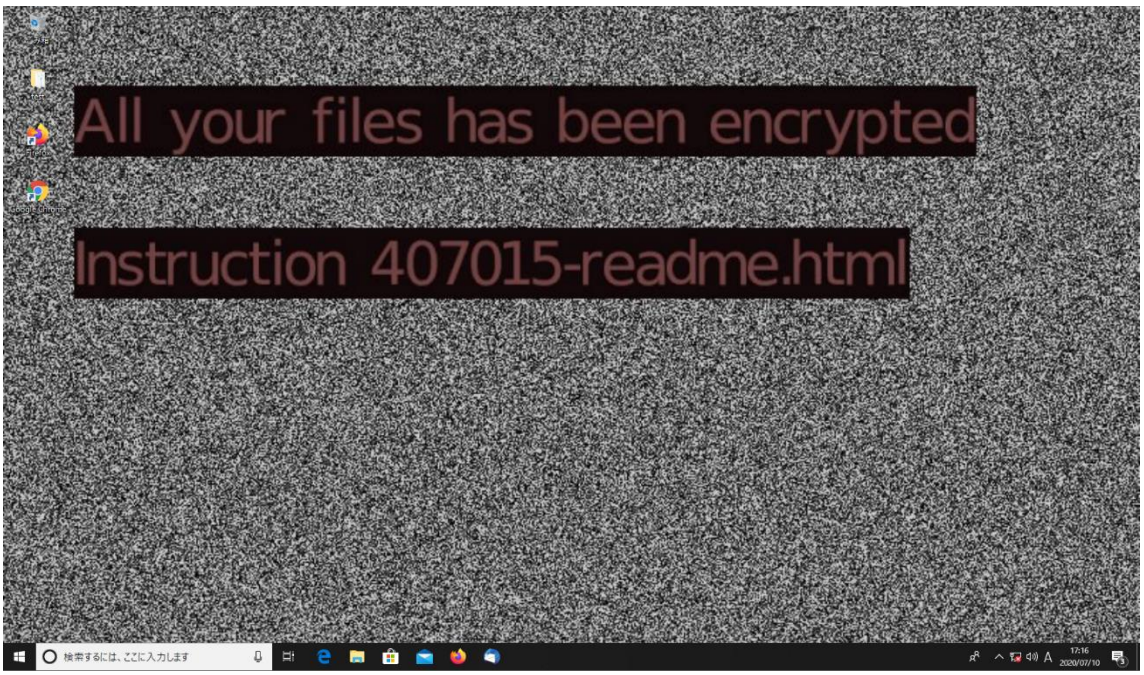
メールの件名は他にも、「Your new photo?」「Is this your photo」などが確認されています。



ばらまきメールのサンプル

これらのメールに添付されているファイルの名前は、どれも「IMG＋ランダムな数字＋.jpg.js.zip」となっています。Zip ファイルの中身は、画像ファイルに偽装した JavaScript ファイルとなっています。あたかも受信者の写真が添付されているかのように見せかける件名を使い、画像ファイルを開かせようとしています。
この JavaScript ファイルを実行してしまうと、PowerShell が起動し、最終的に Avaddon というマルウェアに感染します。

この Avaddon とは、ランサムウェアの 1 つで、最近確認された新しいランサムウェアファミリーです。6 月時点での感染後の動作は、ファイルの拡張子を「avdn」に変更し、ファイルの暗号化を行うことが確認されています。暗号化が終わると、以下のようにデスクトップを変更します。



暗号化が終わった後のデスクトップの画面

また、Avaddon は、ダークウェブ上で RaaS（Ransomware as a Service）として提供されていることも確認されています。RaaS とは、ランサムウェアのプログラムや C&C サーバなどのインフラを提供するサービスを指します。RaaS については、過去のマルウェアレポートでも解説を行っています。攻撃者が攻撃を行う上での技術的なハードルが下がり、誰でも攻撃者になることができるため、攻撃の増加が懸念されます。攻撃者がプログラムの更新などのサービスに力を入れているマルウェアは、攻撃によく利用されています。Avaddon の作成者も、プログラムの更新を行っているようですので、今後の動向に注意する必要があります。

今回ご紹介したような複数の脅威の被害に遭わないためにも、セキュリティ製品の適切な利用、最新のセキュリティパッチを適用するといった総合的な対策が重要になります。
また、添付ファイルを安易に開かないことやランサムウェアによる被害軽減のためのオフラインバックアップの取得など、脅威に対して個別の対策をとることも心掛けて下さい。

ご紹介したように、6 月は Web ブラウザー上で実行される脅威に加えて、多数のばらまきメールを確認しました。セキュリティ製品の適切な利用や最新のセキュリティパッチを適用することが重要です。また、添付ファイルを安易に開かないことやオフラインバックアップの取得も重要になります。

■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. 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。

［引用・出典元］

・ESET Research 公式 Twitter

https://twitter.com/ESETresearch/status/1270339046645141507

Canon

キヤノンマーケティングジャパン株式会社