2019年
3月
MARCH

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

圧縮・展開ソフトウェアの脆弱性を悪用したランサムウェアを確認

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

「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

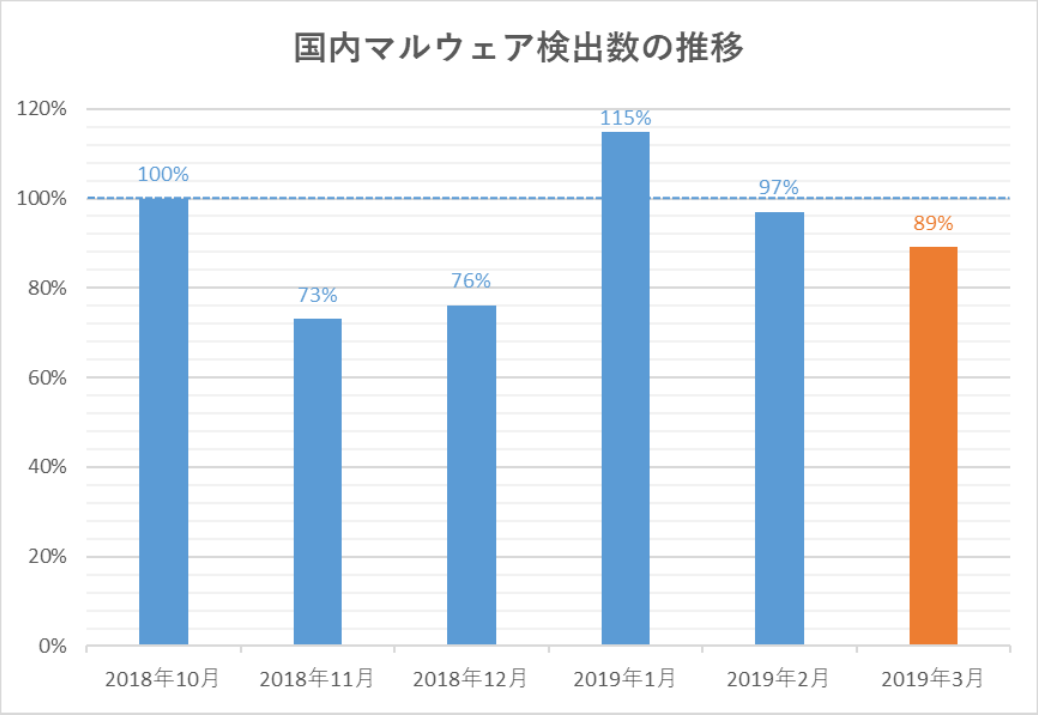
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 3 月マルウェア検出状況」

1. 3 月の概況について
2. 圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

1. 3 月の概況について

2019 年 3 月（3 月 1 日～3 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数は、以下のとおりです。



国内マルウェア検出数*1 の推移

（2018 年 10 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。

2019 年 3 月の国内マルウェア検出数は、検出数が急増した 2019 年 1 月と比較すると減少しました。

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数*2 上位（2019 年 3 月）

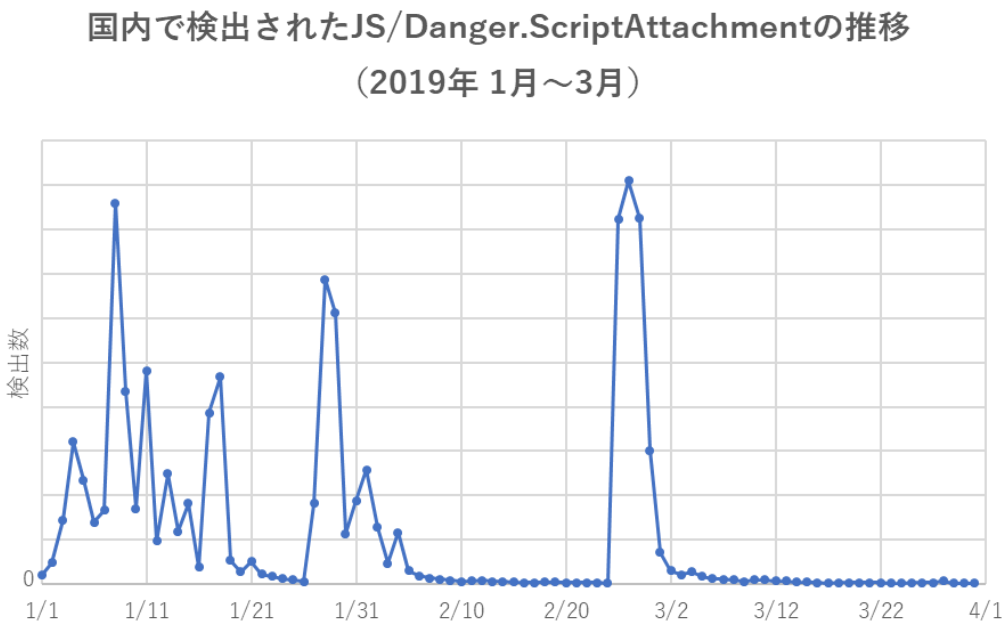
順位	マルウェア名	比率	種別
1	JS/Adware.Agent	11.9%	アドウェア
2	VBA/TrojanDownloader.Agent	10.7%	ダウンローダー
3	HTML/ScrInject	6.8%	HTML に埋め込まれた不正スクリプト
4	HTML/FakeAlert	3.8%	偽の警告文を表示するスクリプト
5	Suspicious	2.4%	未知の不審ファイルの総称
6	JS/Redirector	2.2%	リダイレクター
7	JS/Danger.ScriptAttachment	2.0%	ダウンローダー
8	HTML/Fraud	1.8%	詐欺サイトのリンクが埋め込まれた HTML
9	PDF/Fraud	1.7%	詐欺サイトのリンクが埋め込まれた PDF
10	HTML/Phishing.Amazon	1.5%	Amazon.com の偽サイトのリンクが埋め込まれた HTML

*2 本表には PUA を含めていません。

3 月に国内で最も多く検出されたマルウェアは、JavaScript で記述されたアドウェアである JS/Adware.Agent でした。本マルウェアは、Web 閲覧中に不正な広告を表示させる可能性があります。
2 番目に多く検出されたマルウェアは、VBA(Visual Basic For Applications)で記述されたダウンローダーである VBA/TrojanDownloader.Agent でした。

JS/Adware.Agent と VBA/TrojanDownloader.Agent は、2018 年の年間を通して 非常に多く観測されたマルウェアです。2018 年全体において国内で検出されたマルウェアのうち、それぞれ前者が 2 番目、後者が 1 番目に多く検出されたものです（参考：年間マルウェアレポート）。これらのマルウェアに対しては、引き続き警戒が必要だと考えられます。

2019 年 1 月と 2 月に猛威を振るった JS/Danger.ScriptAttachment（参考：2019 年 1 月・2 月マルウェアレポート）は、検出数が大幅に低下し、第 8 位になりました。
国内で検出された JS/Danger.ScriptAttachment の推移は以下のとおりです。



国内で検出された JS/Danger.ScriptAttachment の推移

2 月後半のピーク以降、目立った活動は確認されませんでした。

2. 圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

多くの圧縮・展開ソフトウェアが利用しているライブラリ UNACEV2.DLL に脆弱性（以降、本脆弱性と記載）が発見されました。さらに、その脆弱性を悪用するマルウェアが確認されています。

■ 脆弱性の概要と影響を受けるソフトウェア

本脆弱性（CVE-2018-20250）はディレクトリトラバーサルの脆弱性です。ディレクトリトラバーサルとは、通常はアクセスできないディレクトリやファイルにアクセスする脆弱性（攻撃手法）のことです。攻撃者によって細工された圧縮ファイルを展開した場合、任意のフォルダーに悪意のあるファイルが展開されるおそれがあります。

WinRAR（バージョン 5.61 以前）のほか、**UNACEV2.DLL を利用しているすべての圧縮・展開ソフトウェア**が本脆弱性の影響を受ける可能性があります。

WinRAR は既に修正版（バージョン 5.70）が公開されています。 以前のバージョンをお使いの場合は速やかにアップデートされることを推奨します。

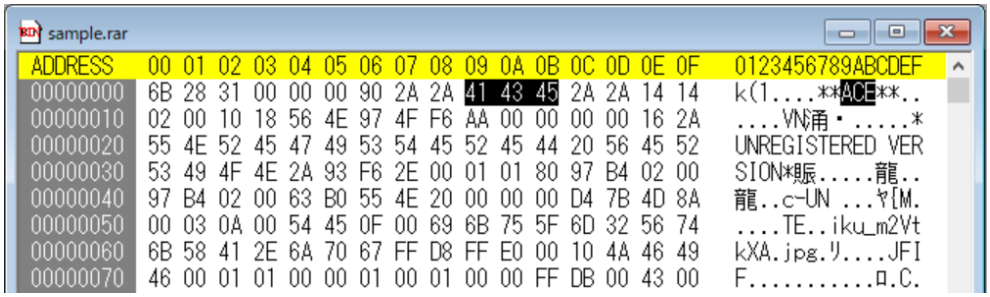
お使いの圧縮・展開ソフトウェアで脆弱性が修正されていない場合は、手動で UNACEV2.DLL を削除するか、脆弱性が修正されるまでの間は脆弱性対応済みの他のソフトウェアを使用されることを推奨します。

■ 本脆弱性を悪用するランサムウェア

本脆弱性を悪用する事例がいくつか確認されています。

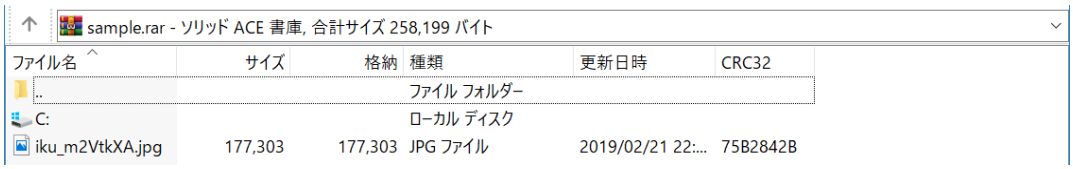
本レポートではランサムウェア JNEC.a をご紹介します。

JNEC.a の拡散には細工が施された圧縮ファイルが使用されています。拡張子は.rar ですが、実体は ACE 形式の圧縮ファイルです。



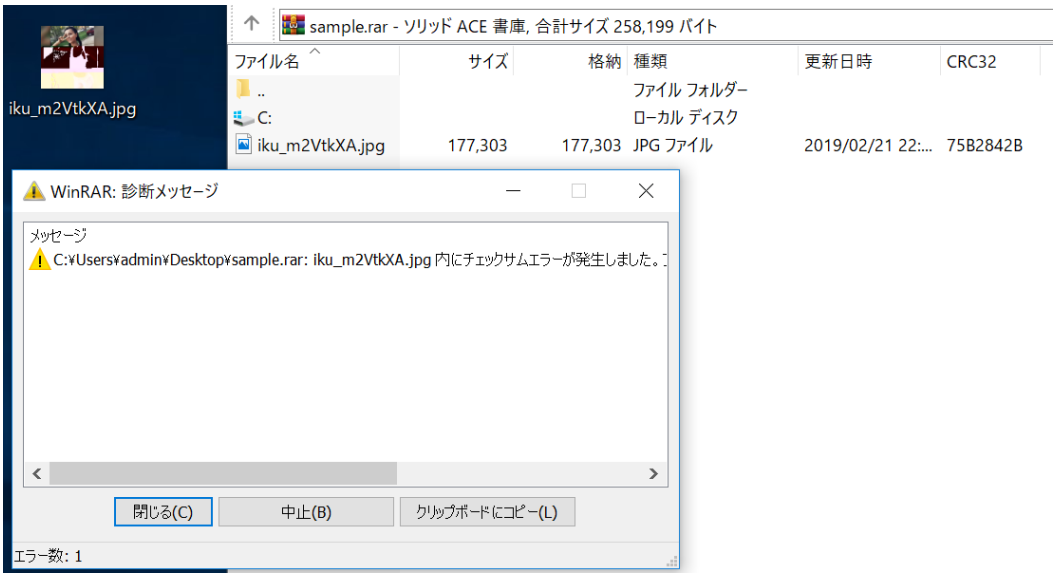
細工が施された圧縮ファイルのヘッダー

JNEC.a の感染プロセスは以下の通りです。
細工された圧縮ファイルを WinRAR などの圧縮・展開ソフトウェアで開くと、画像ファイルと C ドライブへの参照が表示されます。



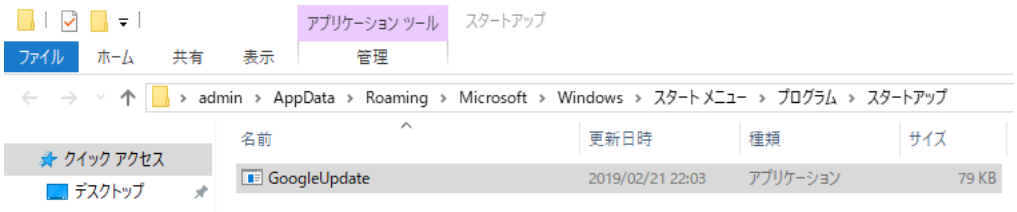
細工された圧縮ファイル

圧縮ファイルを展開すると、ユーザーが指定したフォルダーにデコイ（おとり）ファイルの画像を展開します。
画像は一部の色情報が欠損しており、展開時にはエラーメッセージが表示されます。



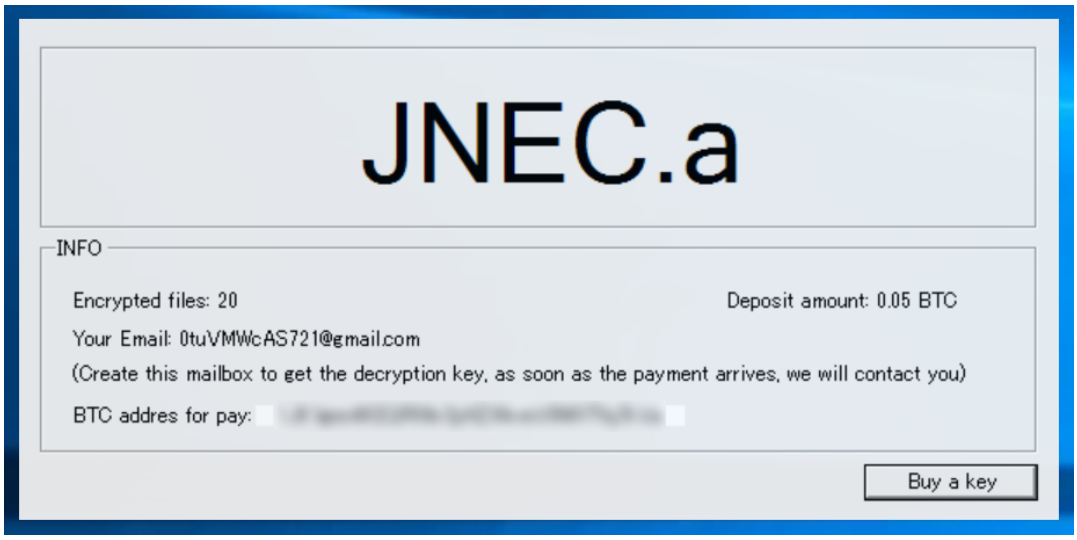
細工された圧縮ファイル展開時のエラーメッセージ

同時に、スタートアップフォルダーにランサムウェアの実行ファイルが展開されます。実行ファイルが展開されたことはユーザーには通知されません。



スタートアップフォルダーに展開されたランサムウェア

ユーザーが PC を再起動すると、ランサムウェア JNEC.a が PC 上のファイルを暗号化します。暗号化が完了すると、ファイルを元に戻すための対価としてビットコインを要求する画面がデスクトップに表示されます。価格は 0.05BTC（2019 年 4 月現在およそ 3 万円）です。
画面上のメッセージには、記載されたメールアドレスで Gmail のアカウントを作成し攻撃者のウォレット宛にビットコインを支払えば、そのメールアドレス宛に復号鍵を送ると書かれていますが、メールアドレスは起動する毎にランダムに変更される上、攻撃者には通知されないため、攻撃者から復号鍵が送られてくることはありません。

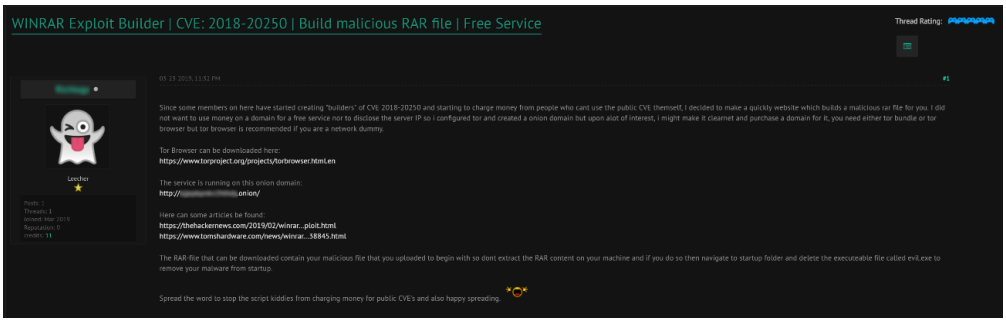


ビットコインの支払いを要求するメッセージ

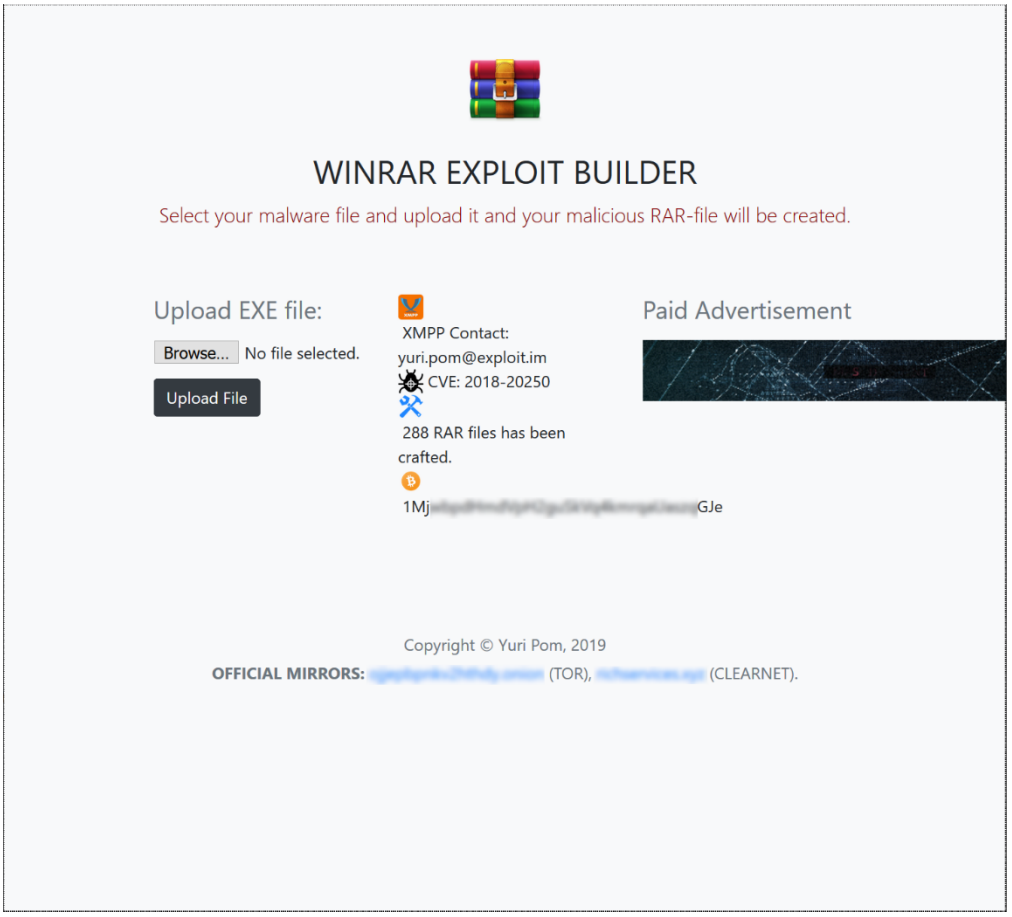
2018 年 11 月以降攻撃者ウォレットに対する入金がないことや、サンプルの観測数が少ないことから、本マルウェアの拡散は限定的とみています。

ESET 製品では、本脆弱性を悪用した圧縮ファイルを「ACE/Exploit.CVE-2018-20250 トロイの木馬」、JNEC.a ランサムウェアを「MSIL/Filecoder.SC トロイの木馬」としてそれぞれ検出・駆除します。

■ 「WinRAR」の脆弱性を悪用するツールキット（exploit builder）
今回発見された脆弱性を悪用するマルウェアを作成するためのツールキットがハッキングフォーラム等で公開されています。2019 年 4 月 5 日時点で既に 288 個のマルウェア（の可能性があるファイル）が作成されたことを示す記載もあります。



マルウェア作成ツールキットを公開していることを伝えるフォーラム上の書き込み



脆弱性悪用ツールを公開している Web サイト

このようなサイトが存在することから、今後も本脆弱性を悪用した攻撃が発生することが予想されます。お使いの圧縮・展開ソフトウェアが本脆弱性の影響を受けるかどうか確認し、速やかに対応されることを推奨します。
またランサムウェアへの感染に備えて、定期的にバックアップを取得し、バックアップをネットワークから隔離した環境に保管されることを推奨します。

ご紹介したように、3 月は圧縮・展開ソフトウェアの脆弱性を悪用した攻撃が確認されました。常に最新の脅威情報をキャッチアップすることが重要です。

■ 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

キヤノンマーケティングジャパン株式会社