2021年
4月
APRIL

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

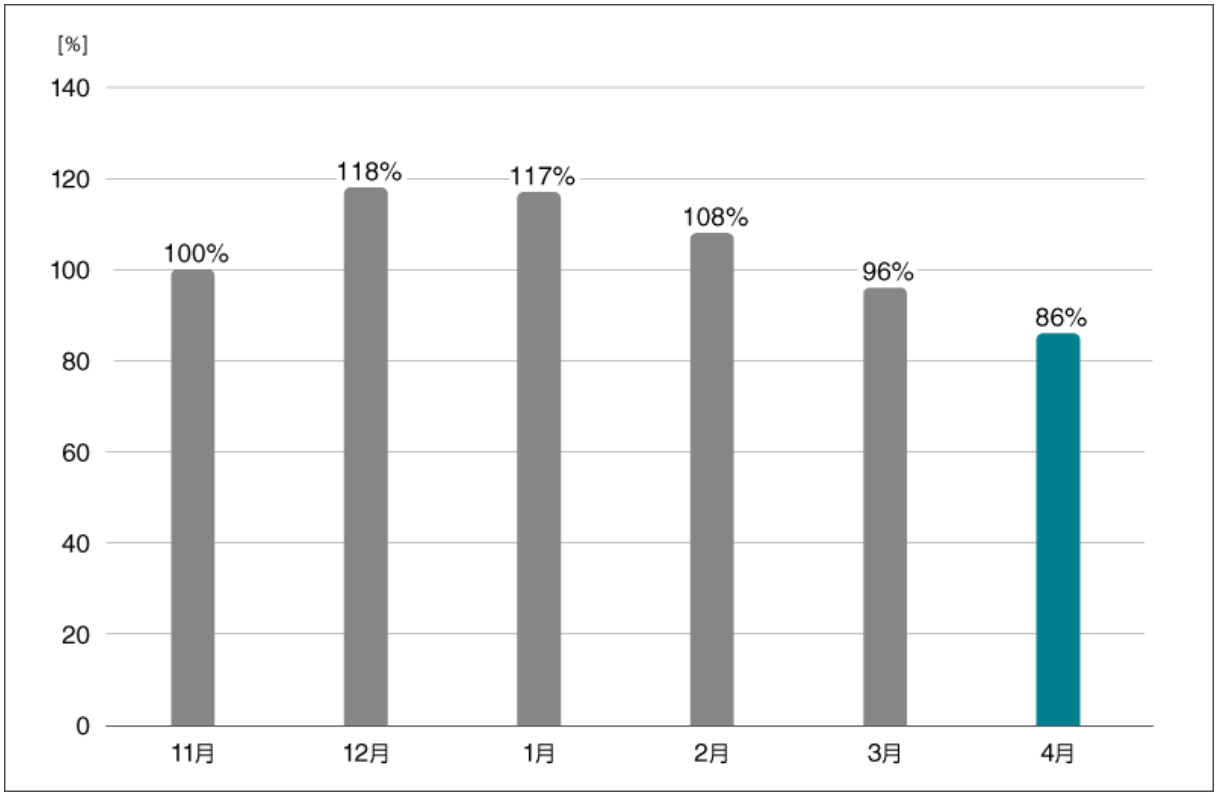
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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「2021 年 4 月マルウェア検出状況」

2021 年 4 月（4 月 1 日～4 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 11 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 4 月の国内マルウェア検出数は、2021 年 3 月に引き続いて減少しています。検出されたマルウェアの内訳は以下のとおりです。

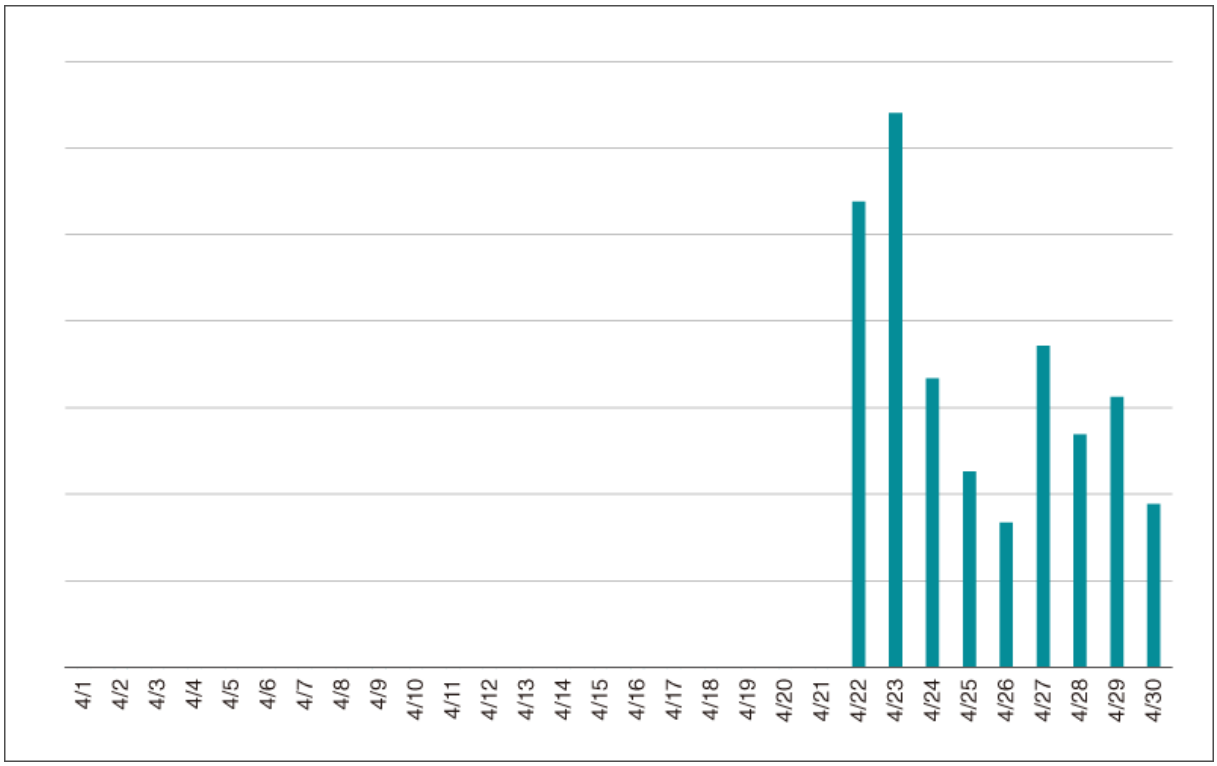
国内マルウェア検出数*2 上位（2021 年 4 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	18.9%	アドウェア
2	JS/Adware.Sculinst	10.6%	アドウェア
3	HTML/Phishing.Agent	6.2%	メールに添付された不正な HTML ファイル
4	JS/Adware.TerraClicks	5.7%	アドウェア
5	JS/Adware.Subprop	4.4%	アドウェア
6	HTML/ScrInject	3.1%	HTML に埋め込まれた不正スクリプト
7	JS/Adware.PopAds	2.0%	アドウェア
8	JS/Agent.OAY	1.7%	不正な JavaScript の汎用検出名
9	VBA/TrojanDownloader.Agent	1.2%	ダウンローダー
10	DOC/Fraud	0.6%	詐欺サイトのリンクが埋め込まれた doc ファイル

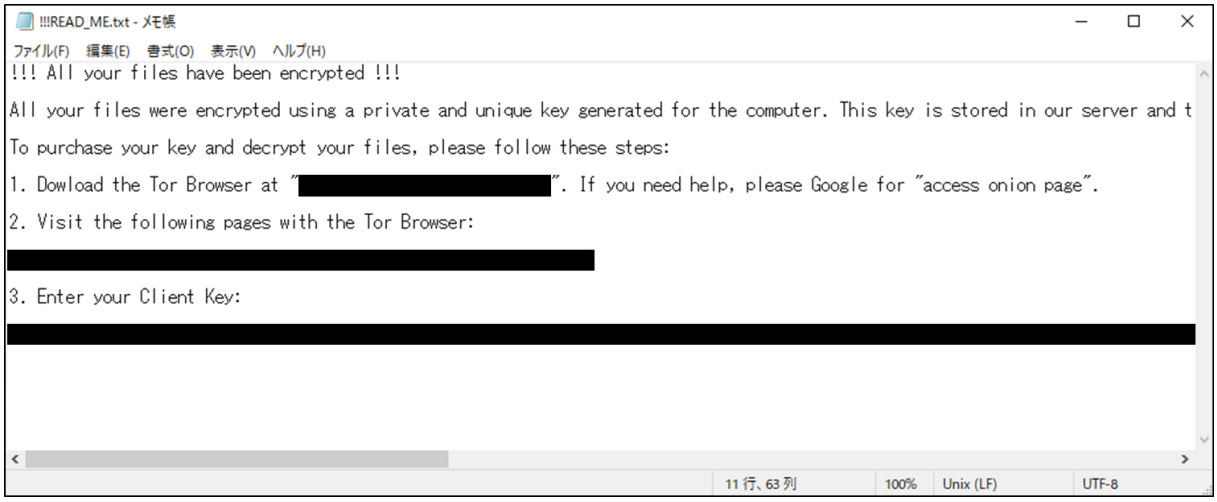
*2 本表には PUA を含めていません。

4 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。

今月は、脆弱性を悪用した 2 つの攻撃についてご紹介します。
1 つ目は、QNAP 社製の NAS を狙ったランサムウェア攻撃です。2021 年 4 月 19 日頃から、QNAP 社製の NAS を狙ったランサムウェア攻撃が確認されています。
この攻撃は、QNAP 社製品の脆弱性を突くことで乗っ取った NAS 上で、圧縮・解凍ソフトウェアである 7zip を悪用してファイルの暗号化を行っています。悪用された脆弱性は、CVE-2021-28799「Hybrid Backup Sync 3(HBS 3)における不適切な認証の脆弱性」と CVE-2020-36195「Multimedia Console および Media Streaming Add-on における SQL Injection の脆弱性」が考えられています。また、これらの脆弱性を修正するセキュリティパッチが公開されています。
ESET 製品でも、日本国内において検出名「Win32/Filecoder.Qlocker」が 4 月 22 日頃から検出されています。この攻撃はファイルを暗号化した後、脅迫文が記載された「!!!READ_ME.txt」というファイル名のテキストファイルを残します。ESET 製品は、このテキストファイルを攻撃の痕跡として検出します。



Win32/Filecoder.Qlocker の 4 月の国内における検出状況



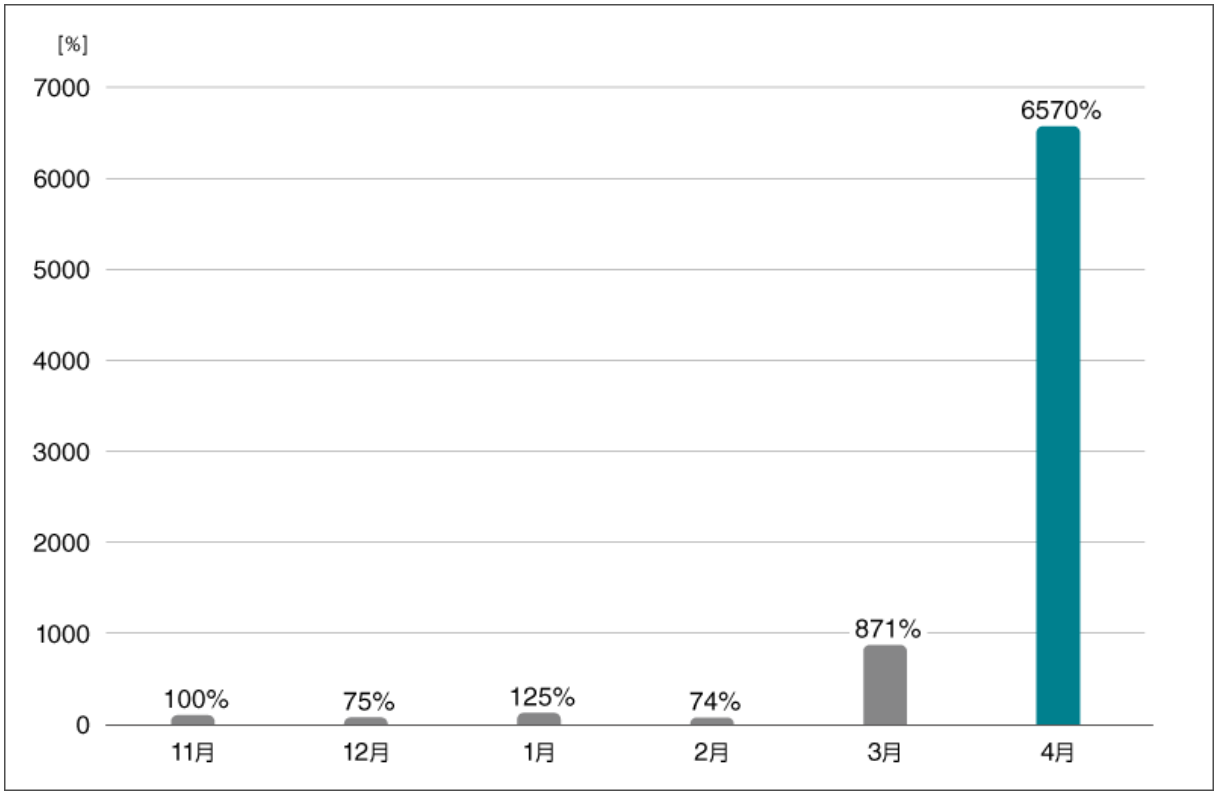
暗号化後に作成される脅迫文のサンプル

脅迫文には、Tor ブラウザをインストールし、攻撃者から指定される Web ページへのアクセスを促されています。アクセス先では、ファイルを復号するための鍵を得るために、約 5 万円から 6 万円相当（感染が始まった 4 月 19 日頃の相場）のビットコインを要求されたという報告もあります。

QNAP 社の HP 上で、今回のランサムウェア攻撃に関する情報が公開されています。感染の予防策や感染後に必要な作業について書かれていますので、製品を利用されている方は確認してください。

2 つ目は、Apache Struts 2 の脆弱性 CVE-2017-5638 を狙った攻撃です。CVE-2017-5638 は、Apache Software Foundation が提供しているソフトウェアフレームワーク Apache Struts 2 の 2017 年に発見された脆弱性です。これは、Jakarta Multipart parser のファイルアップロード処理に起因しています。2017 年に発見された時も、IPA から注意喚起が行われています。この脆弱性を悪用すると、遠隔にいる攻撃者によってサーバー上で任意のコードを実行される恐れがあります。2017 年には、米国の大手消費者信用情報会社においてこの脆弱性の悪用による情報漏えいが生じています。

統計を見ると、2021 年 3 月から 4 月にかけて国内の検出数が増加していることがわかります。CVE-2017-5638.Struts2 が多く検出されている原因の 1 つとして、外部に公開されている Apache Struts 2 を利用した Web サイトやアプリケーションの存在が考えられます。例えば、社内のイントラサイトのように外部に公開していない Web サイトが設定ミスによって外部に公開されているケースなどが想定されます。



CVE-2017-5638 を狙った攻撃の検出状況（国内･2020 年 11 月～2021 年 4 月）
（2020 年 11 月の検出数を 100%として比較）

発見されてから 4 年近く経ちますが、脆弱性は古い･新しいに関係なく利用されます。発見されてから時間が経つと、エクスプロイトキットが開発されることにより簡単に攻撃を行えるようになる恐れもあります。

ご紹介したように、4 月は脆弱性を悪用した攻撃を検出しています。新しく発見される脆弱性による脅威だけでなく、過去に発見された脆弱性も脅威になります。また、脆弱性は組み合わさることで、新たな攻撃につながる可能性もあります。利用している製品や製品に使われている OSS などの脆弱性情報について情報収集を行うことが重要です。定期的に IPA と JPCERT が運営している JVN の HP や製品ベンダーの HP などを確認してください。

■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. 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。

Canon

キヤノンマーケティングジャパン株式会社