2022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

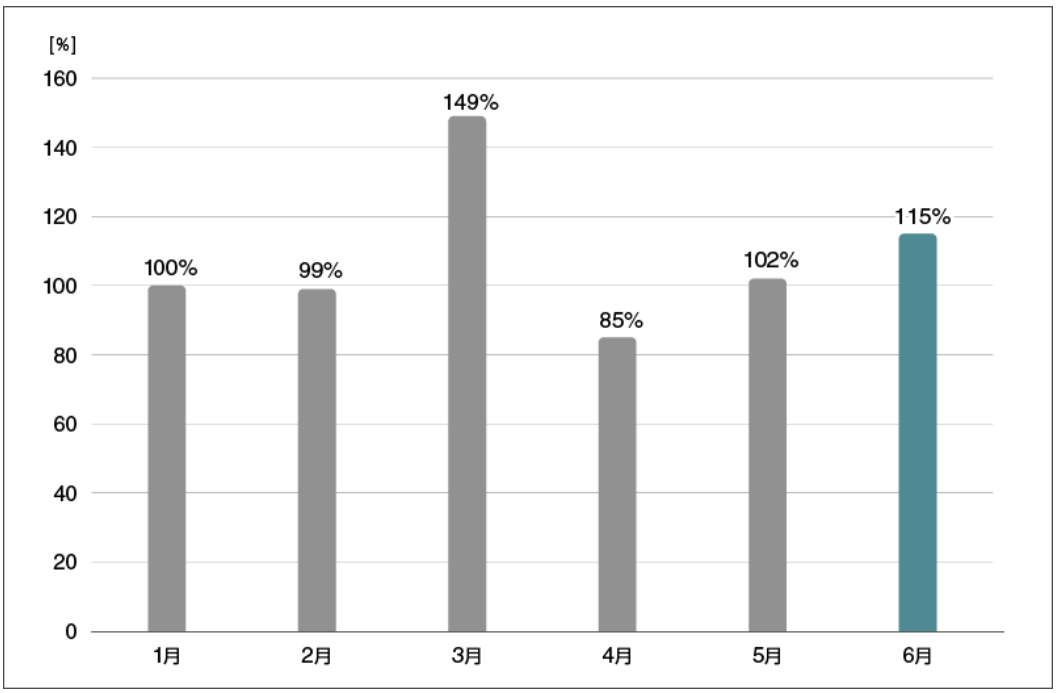
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 6 月マルウェア検出状況

2022 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

(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 6 月の国内マルウェア検出数は、2022 年 5 月と比較して増加しました。検出されたマルウェアの内訳は以下のとおりです。

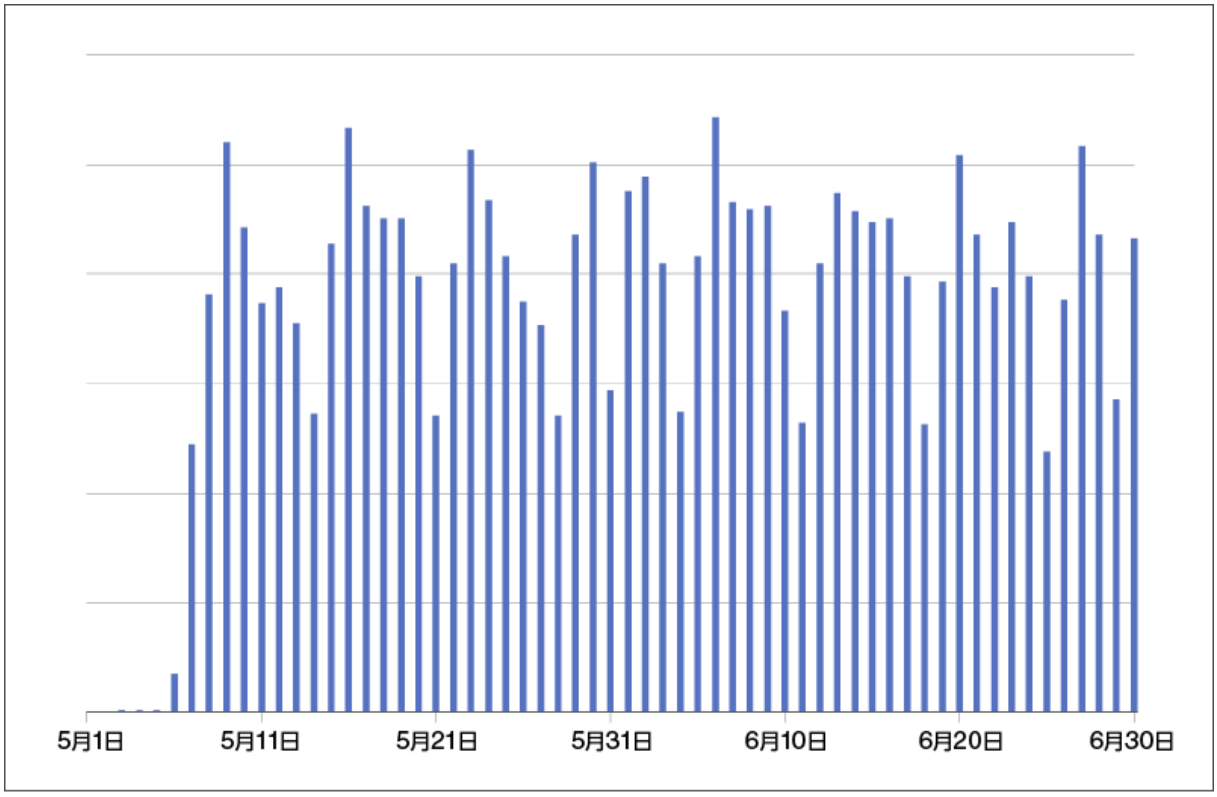
国内マルウェア検出数*2 上位（2022 年 6 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	17.4%	アドウェア
2	DOC/TrojanDownloader.Agent	12.7%	ダウンローダー
3	HTML/Pharmacy	8.3%	違法薬品の販売サイトに関連する HTML ファイル
4	JS/Adware.Agent	8.0%	アドウェア
5	JS/Packed.Agent	4.0%	パックされた不正な JavaScript の汎用検出名
6	HTML/FakeAlert	3.0%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.Sculinst	2.6%	アドウェア
8	LNK/TrojanDownloader.Agent	2.5%	ダウンローダー
9	HTML/Phishing.Agent	2.3%	メールに添付された不正な HTML ファイル
10	HTML/ScrInject	2.3%	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。

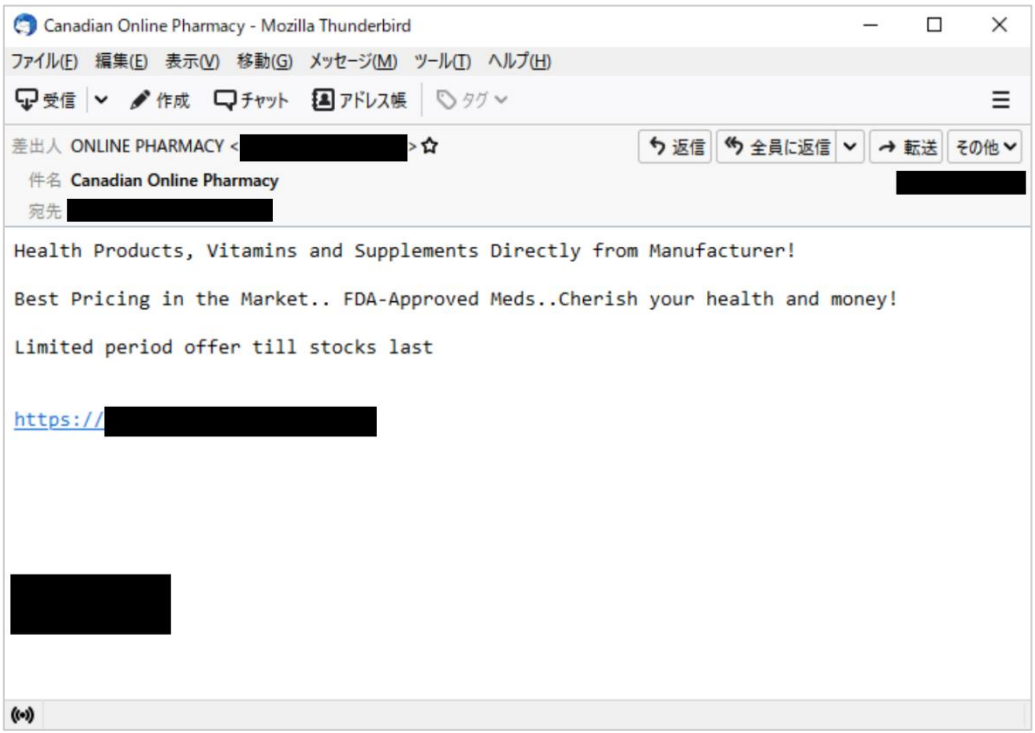
6 月に国内で最も多く検出されたマルウェアは、JS/Adware.TerraClicks でした。
JS/Adware.TerraClicks は、Web サイト閲覧時に実行されるアドウェアです。感染すると、アドウェアサイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。

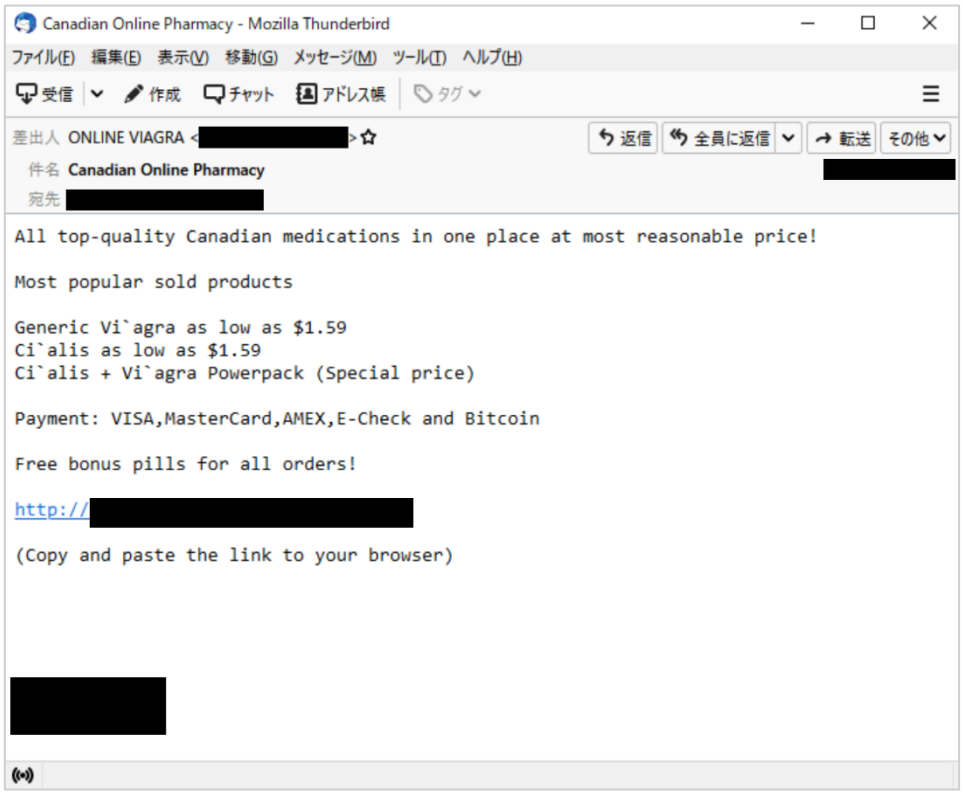
6 月の国内マルウェア検出数の 3 位は HTML/Pharmacy ですが、これは 5 月の国内マルウェア検出数でも 2 位となっており、高い検出数を維持しています。HTML/Pharmacy は違法な医薬品（表示成分が含まれていない医薬品、表示にない成分が含まれている医薬品、未承認の医薬品などが該当）を販売する詐欺サイトであり、スパムメールの URL リンクにアクセスした場合や Web サイト閲覧時に表示される広告経由でアクセスした場合に検出する可能性があります。



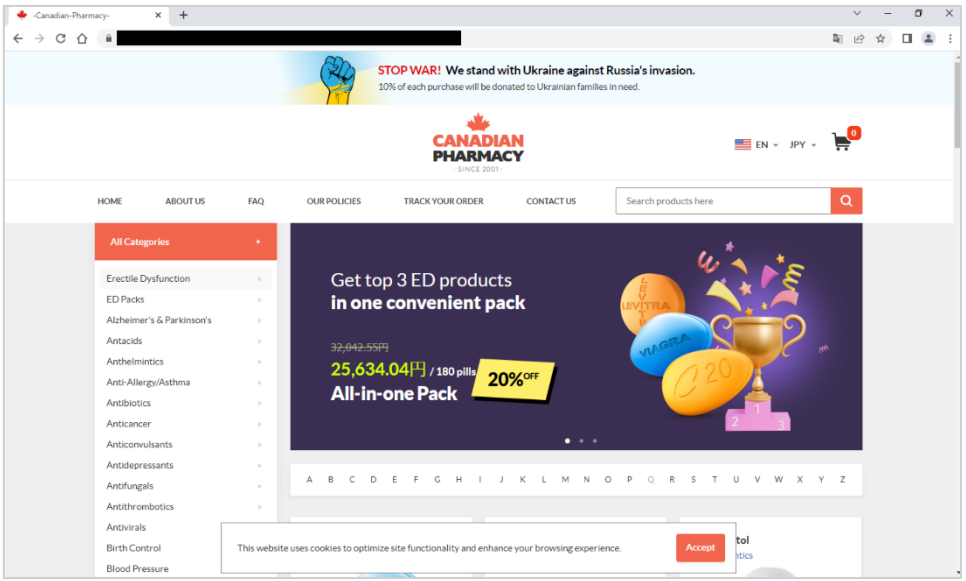
5 月および 6 月の国内における HTML/Pharmacy 検出数の推移

スパムメールを例にすると、ビタミン剤や治療薬といったユーザーが興味を引く医薬品についての内容がメール本文に記載されています。また、期間限定の案内または割引価格である旨が記載されている場合もあり、ヘルスケアに興味のあるユーザーに対して URL リンクをクリックさせようと誘導している意図が推測されます。
メール本文中の URL リンクにアクセスすると、オンラインの医薬品販売サイトと思われる Web ページが表示されます。





HTML/Pharmacy に関連するスパムメールの例



スパムメール内の URL リンク接続先の例

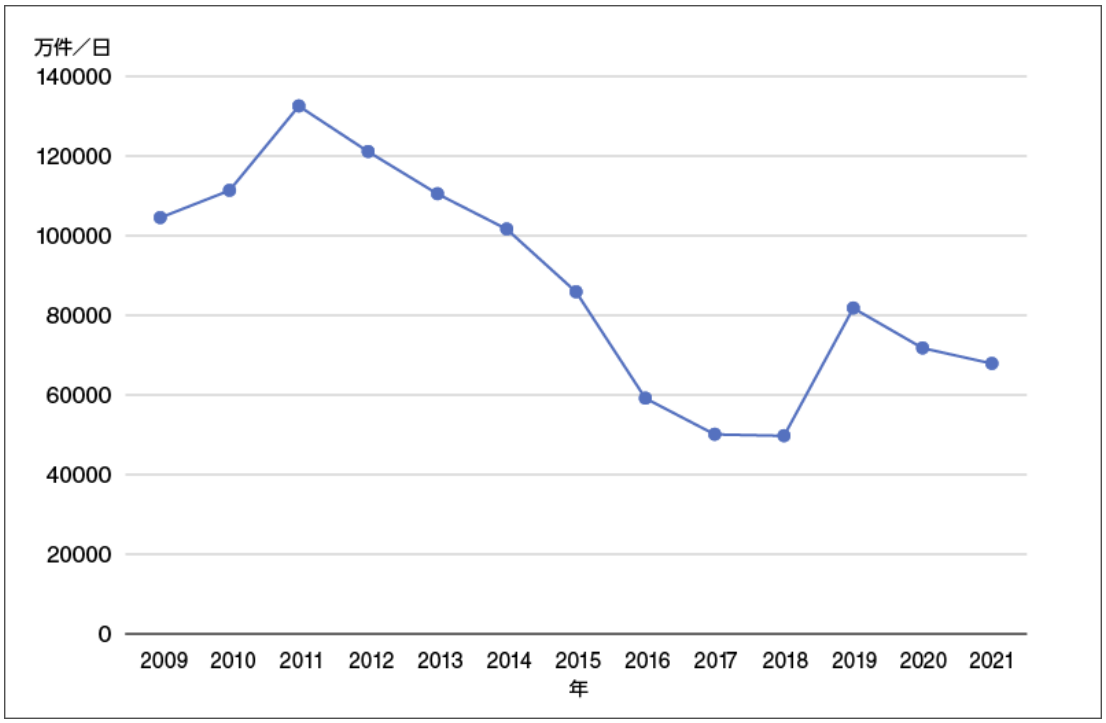
スパムメールや URL リンクの接続先ページに「Canadian Pharmacy」あるいは「Canadian Online Pharmacy」というキーワードが見受けられます。この「Canadian Pharmacy」は、2010 年 10 月まで活動していた「Spamit」と呼ばれる組織がスパムメール配信者にアフィリエイトプログラムとして提供していたコンテンツの 1 つとして知られています*3,4。スパムメールが送信される方法の 1 つとして、マルウェアに感染した端末によって形成される Botnet から送信される方法が挙げられますが、中でも「Rustock」と呼ばれた Botnet は、「Spamit」が提供していた医薬品関連のコンテンツを多く送信していました。Rustock Botnet は 2011 年にテイクダウンされており*5、この他にも多くの Botnet が今日までにテイクダウンされてきました。この結果、スパムメール配信量は 2011 年をピークに減少傾向にあります*6。しかし依然としてスパムメールは観測され続けているため注意が必要です。

*3 世界のスパム流通量が突然激減、その理由は？ | ITmedia エンタープライズ

*4 Spam Affiliate Program Spamit.com to Close | Krebs on Security

*5 Download Rustock の脅威との闘い from Official Microsoft Download Center | Microsoft

*6 電気通信事業者 10 社の全受信メール数と迷惑メール数の割合 | 総務省



2009 年から 2021 年の国内における 1 日当たりのスパムメール受信件数
（総務省の統計から作成）

前述のとおり、2022 年 6 月は違法な医薬品を販売する Web サイトの検出数が多く観測されました。このような Web サイトで医薬品を購入すると、予期せぬ健康被害を受けたり、金銭詐欺にあったりする可能性があります。また、何らかのマルウェアに感染して組織の端末が Botnet に組み込まれると、スパムメールを送信する加害者となってしまう恐れもあります。よって不審なメールの URL リンクや添付ファイルを安易にクリックしない、EDR 製品を導入してマルウェア感染にいち早く気づく仕組みを作るなど、個人および組織レベルで対策を講じることが重要です。

■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．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

- 世界のスパム流通量が突然激減、その理由は？ | ITmedia エンタープライズ
  https://www.itmedia.co.jp/enterprise/articles/1010/07/news017.html
- Spam Affiliate Program Spamit.com to Close | Krebs on Security
  https://krebsonsecurity.com/2010/09/spam-affialite-program-spamit-com-to-close/
- Download Rustock の脅威との闘い from Official Microsoft Download Center | Microsoft
  https://www.microsoft.com/ja-jp/download/details.aspx?id=26673
- 電気通信事業者 10 社の全受信メール数と迷惑メール数の割合 | 総務省
  https://www.soumu.go.jp/main_content/000693529.pdf

Canon

キヤノンマーケティングジャパン株式会社