2022年
10月
OCTOBER

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

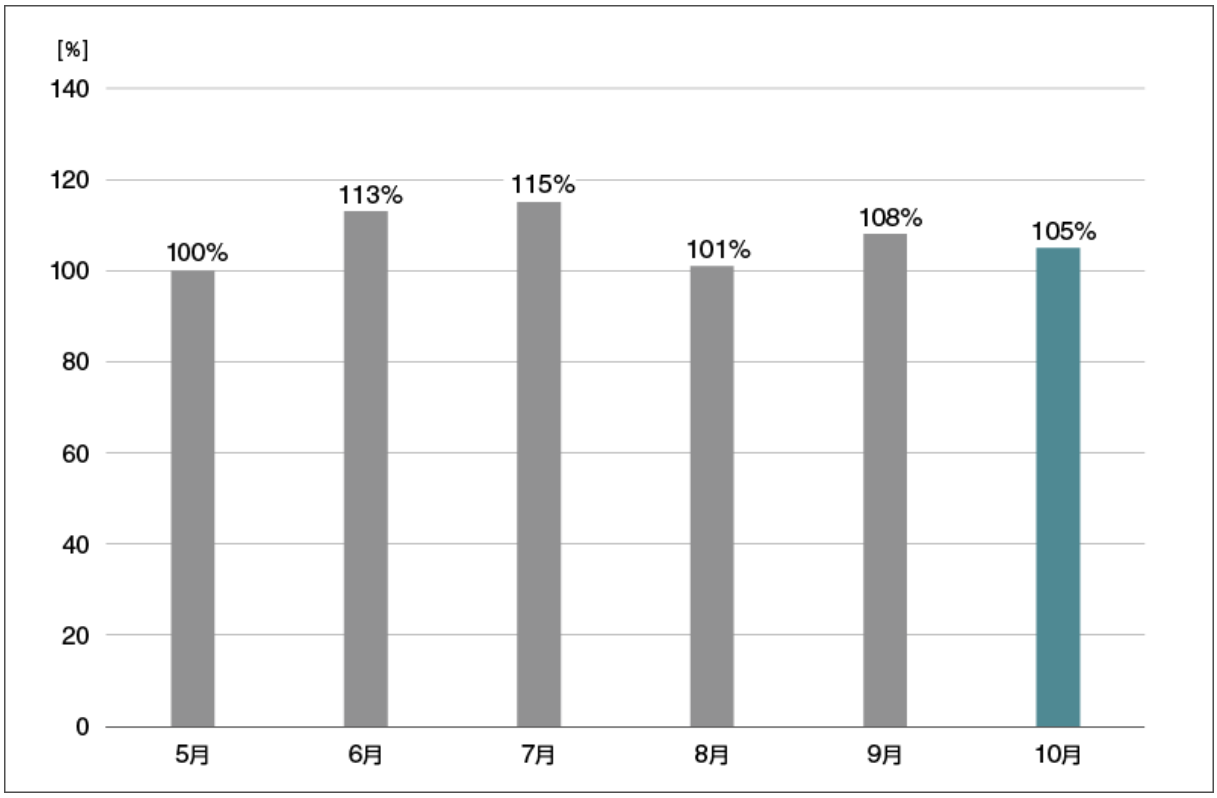
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 10 月マルウェア検出状況

2022 年 10 月（10 月 1 日～10 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 5 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 10 月の国内マルウェア検出数は、2022 年 9 月と比較して微減しました。検出されたマルウェアの内訳は以下のとおりです。

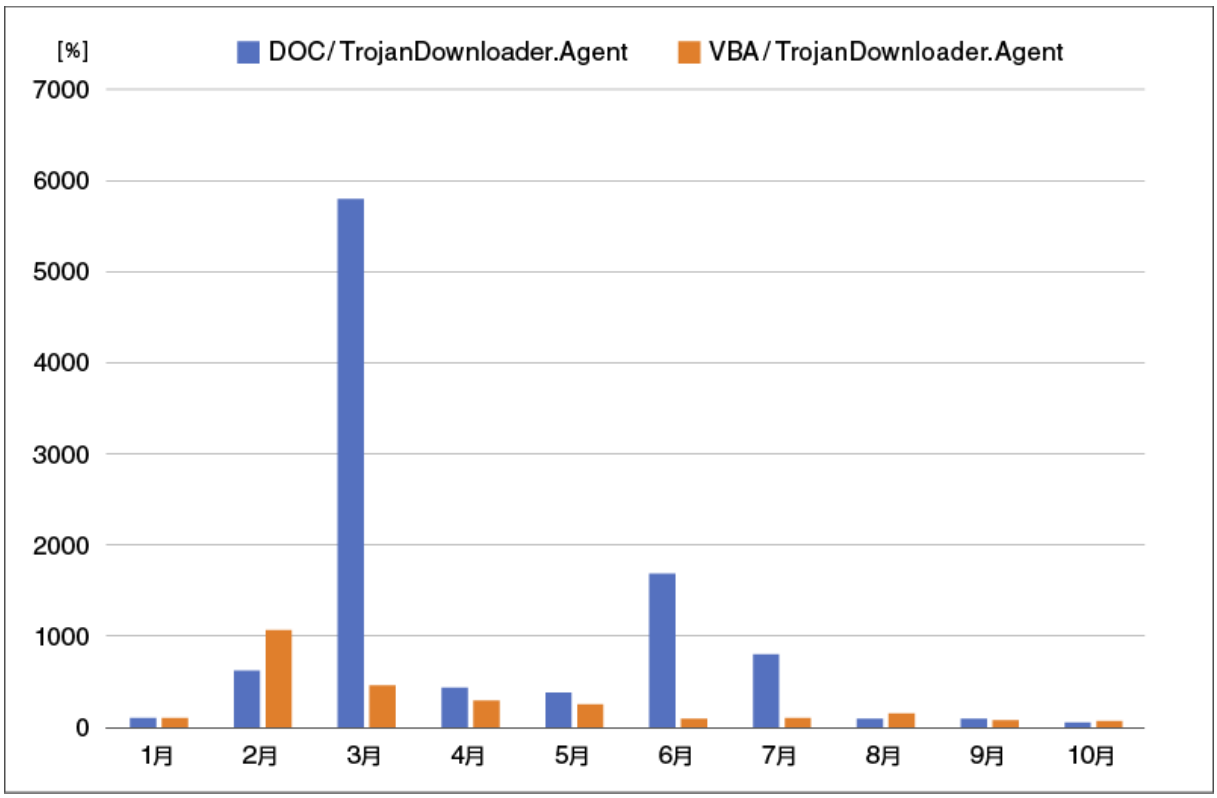
国内マルウェア検出数[*2] 上位（2022 年 10 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	12.6%	アドウェア
2	JS/Packed.Agent	11.8%	パックされた不正な JavaScript の汎用検出名
3	JS/Adware.TerraClicks	11.8%	アドウェア
4	HTML/Pharmacy	8.1%	違法薬品の販売サイトに関連する HTML ファイル
5	HTML/Phishing.Agent	4.5%	メールに添付された不正な HTML ファイル
6	HTML/FakeAlert	3.7%	偽の警告文を表示させる HTML ファイル
7	JS/Adware.Sculinst	3.3%	アドウェア
8	DOC/Fraud	2.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
9	HTML/ScrInject	2.4%	HTML に埋め込まれた不正スクリプト
10	MSIL/TrojanDownloader.Agent	2.0%	ダウンローダー

*2 本表には PUA を含めていません。

10 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。

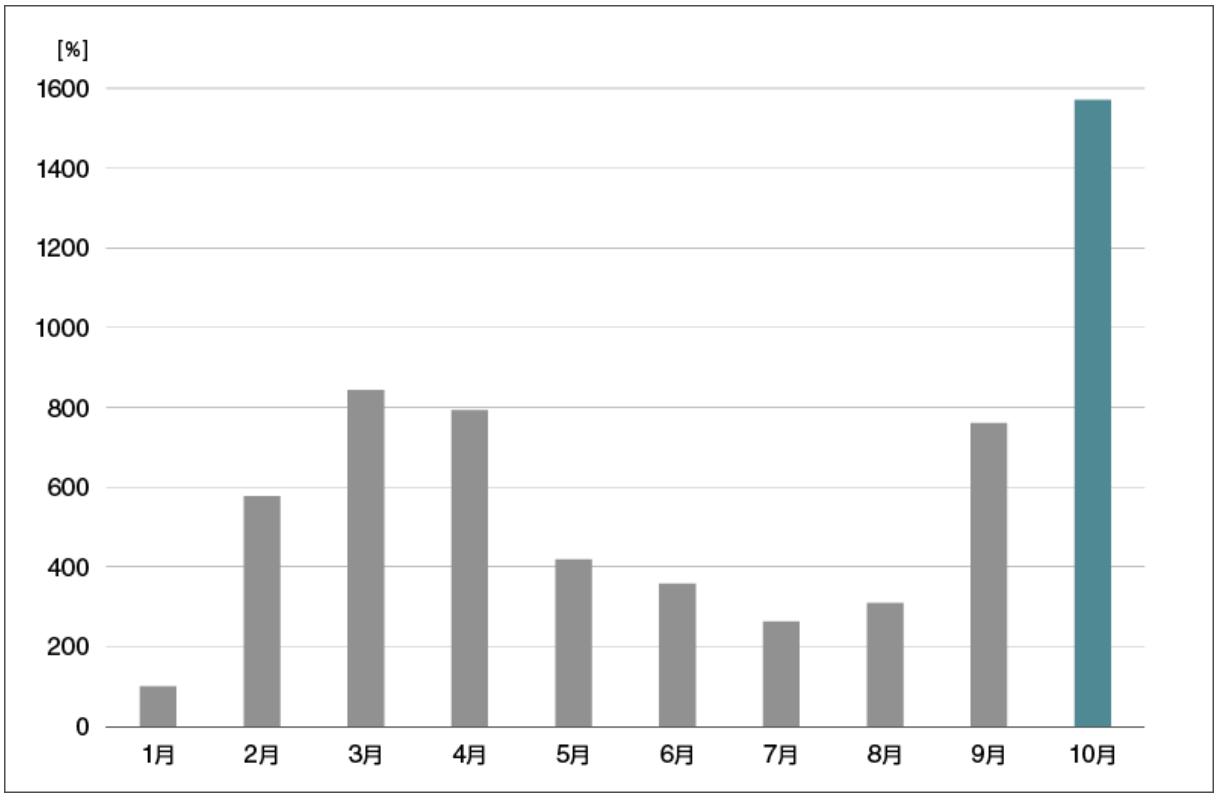
Emotet に感染させるためのばらまきメールの活動が、2022 年 7 月上旬に停止しています。それに伴い、それらの添付ファイルとして主に利用されていた DOC/TrojanDownloader.Agent や VBA/TrojanDownloader.Agent の検出数は、7 月以降減少しています。



DOC/TrojanDownloader.Agent と VBA/TrojanDownloader.Agent の検出数月別推移
（2022 年･国内）
※2022 年 1 月の検出数を 100%として比較

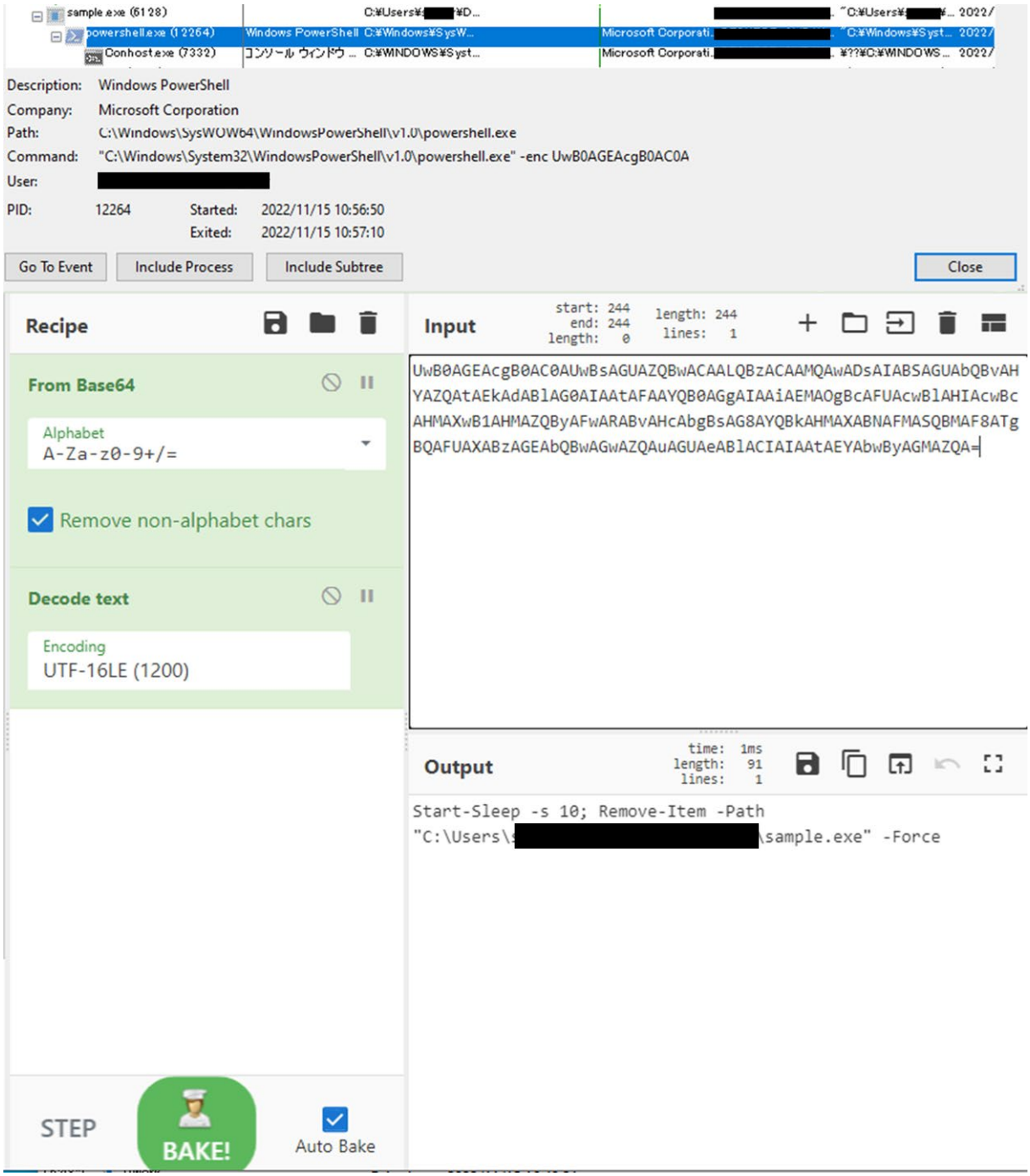
しかし、ダウンローダーによる脅威は、依然として検出しています。

今回は、検出数が増加した MSIL/TrojanDownloader.Agent を紹介します。
MSIL/TrojanDownloader.Agent は、.NET プラットフォームにおける実行ファイル形式のダウンローダーです。機能を複数に分けてダウンロードするマルウェアなどにおいて利用されていることがあります。実際にダウンロードされるマルウェアも多岐にわたり、「AgentTesla」「Smoke Loader」といった情報窃取型マルウェアのダウンロードを確認しています。
2022 年における MSIL/TrojanDownloader.Agent の国内での検出状況は、以下のとおりです。



MSIL/TrojanDownloader.Agent の検出数月別推移（2022 年・国内）
※2022 年 1 月の検出数を 100%として比較

2022 年の ESET 社の第 1 三半期脅威レポートでは、世界全体での検出数増加がトピックとして取り上げられており、日本においても 3 月に検出数が増加しています。今月は、増加した 3 月の検出数を上回る結果となっています。AgentTesla、FormBook や Smoke Loader といったマルウェアをダウンロードする MSIL/TrojanDownloader.Agent の亜種の多数検出が、10 月における検出数増加の要因として考えられます。
今回確認した亜種の中には、実行時に PowerShell が起動し、自身を削除するコマンドを実行するものがありました。コマンドは、Base64 でエンコードされていました。



起動した PowerShell と文字列を Base64 でデコードした結果

※Base64 デコードに加えて、UTF-16 のデコードを行っています

また、MSIL/TrojanDownloader.Agent がアクセスする特徴的な通信先として「cdn[.]discordapp[.]com」から始まる URL を確認しています。この URL は、オンラインチャットアプリの「Discord」でファイル共有した際に作成される URL です。Discord のファイル共有機能を利用すると、ファイル共有用の URL を知っていれば、アカウントを持っていなくてもファイルを受け取ることが可能です。この機能を悪用し、攻撃者が用意した URL にアクセスさせることで、マルウェアや追加のモジュールをダウンロードします。また、ファイル共有で生成される URL は、Discord の正規ドメインということもあり、セキュリティ製品によるアクセスのブロックをすり抜ける恐れがあります。このような Discord を用いたマルウェアの配布は、以前から確認されており、最近ではコロンビアにおける njRAT マルウェアの配布で利用されていたことが ESET 社から報告されています。

今回ご紹介したように、Emotet への感染を狙ったダウンローダー以外にもさまざまなダウンローダーが検出されています。不審な実行ファイルを実行しないことはもちろんのこと、公式ホームページや公式アプリストアからアプリケーションをダウンロードすることを心掛けてください。また、よく利用する Web サイトの場合は、ブックマークに登録することも重要です。

■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

■ ESET｜ESET Threat Report T1 2022
https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

- ESET | WeliveSecurity「Discord: una plataforma atractiva para cibercriminales utilizada más allá de la comunidad gamer」
  https://www.welivesecurity.com/la-es/2021/08/19/discord-plataforma-atractiva-cibercriminales-utilizada-comunidad-gamer/
- ESET | WeliveSecurity「Campaña de espionaje distribuyó el malware njRAT en organizaciones de Colombia」
  https://www.welivesecurity.com/la-es/2022/05/20/campana-espionaje-malware-njrat-organizaciones-colombia/

Canon

キヤノンマーケティングジャパン株式会社