2020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

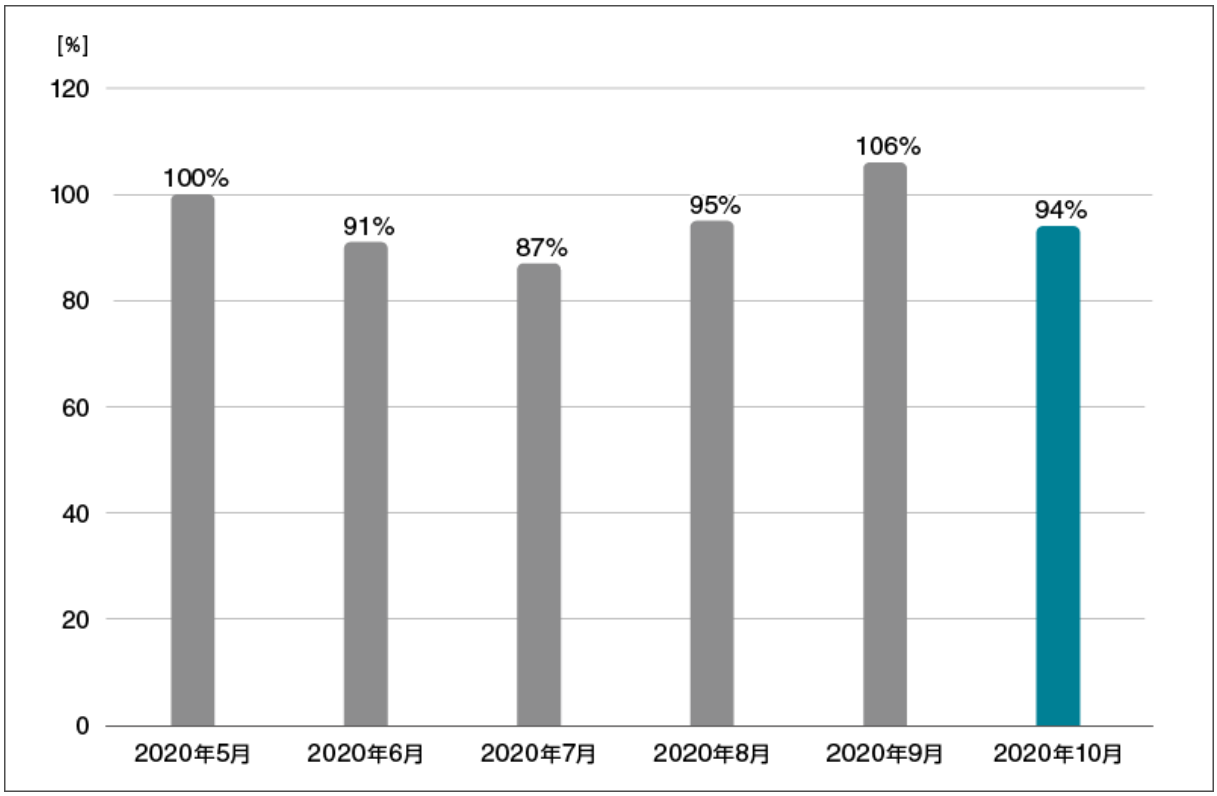
「マルウェアレポート」は、キヤノンマーケティングジャパンが運営する

「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 10 月マルウェア検出状況」

2020 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
(2020 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。

2020 年 10 月の国内マルウェア検出数は、2020 年 8 月と同程度でした。2020 年 5 月の国内検出数を基準とすると、2020 年 7 月に一時的に 10%以上減少していますが、それ以外の月はあまり変動がみられません。10 月に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 10 月）

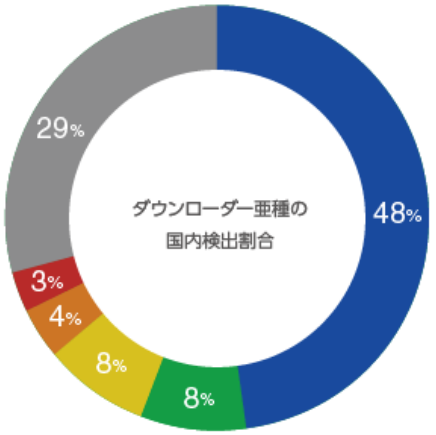
順位	マルウェア	割合	種別
1	JS/Adware.Subprop	15%	アドウェア
2	VBA/TrojanDownloader.Agent	5%	ダウンローダー
3	HTML/ScrInject	5%	HTML に埋め込まれた不正スクリプト
4	JS/Adware.Agent	3%	アドウェア
5	JS/Adware.PopAds	3%	アドウェア
6	HTML/Refresh	1%	別のページに遷移させるスクリプト
7	HTML/Phishing.Agent	1%	別のページに遷移させるスクリプト
8	MSIL/GenKryptik	1%	難読化された MSIL 形式ファイルの汎用名
9	HTML/Fraud	1%	詐欺サイトのリンクが埋め込まれた HTML
10	Win32/TrojanDownloader.Tiny	1%	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.Subprop でした。また、世界全体でも JS/Adware.Subprop が最も多く検出されました。
本マルウェアは、不正な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。2020 年は本マルウェアの検出数が多く、マルウェアレポートでも過去に取り上げています（2020 年 6 月 マルウェアレポート、2020 年上半期 マルウェアレポート）。

10 月に国内で 2 番目に多く検出されたマルウェアは、VBA/TrojanDownloader.Agent でした。本マルウェアは、Office 製品で利用されるプログラミング言語の VBA（Visual Basic for Applications）で作成されたダウンローダーです。メールに添付されている事例が非常に多く見られます。

VBA/TrojanDownloader.Agent には多くの亜種が存在します。下図は、10 月に国内で検出された VBA/TrojanDownloader.Agent 亜種の上位 5 つの割合を示しています。加えて、各々の亜種がダウンロードする主なマルウェアをまとめています。（VBA/TrojanDownloader.Agent がダウンロードするマルウェアは、通信先や環境、時間によって異なる場合があります。）



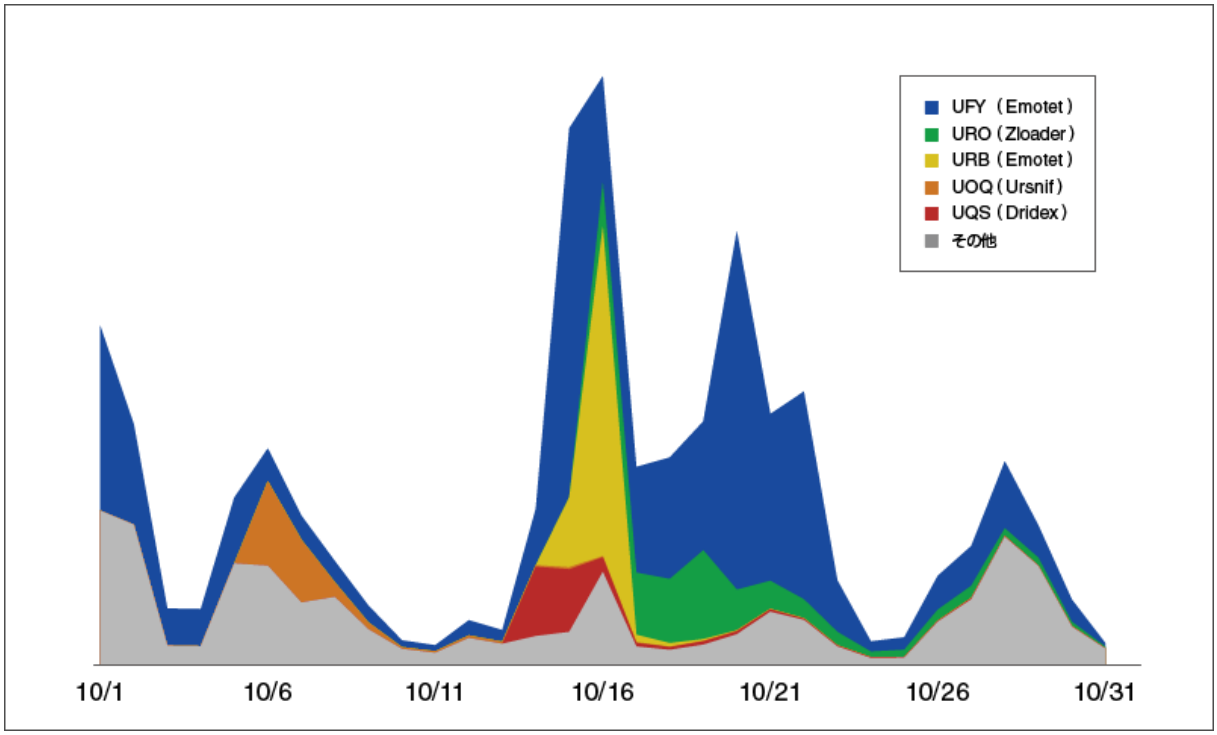
亜種名	ダウンロードする主なマルウェア（ESET検出名）
VBA/TrojanDownloader.Agent.UFY	Emotet（Win32/Emotet）
VBA/TrojanDownloader.Agent.URO	Zloader（Win32/Spy.Zbot）
VBA/TrojanDownloader.Agent.URB	Emotet（Win32/Emotet）
VBA/TrojanDownloader.Agent.UOQ	Ursnif（Win32/Spy.Ursnif）
VBA/TrojanDownloader.Agent.UQS	Dridex（Win32/Dridex）
その他	－

VBA/TrojanDownloader.Agent 亜種の国内検出割合とダウンロードするマルウェア（10 月）

上図から、10 月の国内において VBA/TrojanDownloader.Agent を使用するサイバー攻撃の大半が Emotet の感染を目的とするものであったことがわかります。

バンキングマルウェアの Zloader、Ursnif、Dridex は、Emotet が二次的にダウンロードする代表的なマルウェアとしても知られています。これらのマルウェアが Emotet を介さずに VBA/TrojanDownloader.Agent から直接ダウンロードされる事例も、これまでと同様に確認されていました。

下図は、10 月の国内における VBA/TrojanDownloader.Agent 亜種の検出数推移を示しています。下図凡例の表記は、“VBA/TrojanDownloader.Agent 亜種名の末尾 3 文字（主にダウンロードするマルウェア）”としています。



VBA/TrojanDownloader.Agent 亜種の国内検出数推移（10 月）

上図より、10 月は Emotet を主にダウンロードする亜種の検出数が、数回急増していることがわかります。また Emotet 以外にも、Ursnif、Dridex、Zloader の順番で、VBA/TrojanDownloader.Agent を使用したサイバー攻撃があったことがわかります。
上図の 10/28 は、その他（灰色）の割合が比較的高いです。その構成を調査した結果、Dridex（Win32/Dridex）と情報窃取などを行う IcedID（Win32/Spy.IcedId）を最終的にダウンロードする複数の亜種が多くを占めていました。

以上より、10 月の国内において VBA/TrojanDownloader.Agent を使用し、Emotet をはじめとする様々なマルウェアの感染を目的とするサイバー攻撃があったことがわかりました。不審なメールに添付されている Office 製品を実行する際は、注意が必要です。

今回ご紹介したように、10 月は国内で JS/Adware.Subprop と VBA/TrojanDownloader.Agent が多く検出されました。JS/Adware.Subprop は、2020 年を通して世界全体で検出数が多いため、今後も警戒が必要です。
10 月に国内で検出された VBA/TrojanDownloader.Agent の亜種を解析した結果、本ダウンローダーを利用し、Emotet をはじめとする様々なマルウェアの感染を目的とする攻撃があったことがわかりました。
対策として、セキュリティ製品を適切に利用すること、不審なメールの添付ファイルを安易に開かないこと、マクロを安易に有効化しないことなどの対策が重要です。加えて、様々なマルウェアの脅威動向に関する情報を収集し、組織内で共有することも有効です。

■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

■2020 年 6 月 マルウェアレポート｜マルウェア情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2006.html

■2020 年 上半期マルウェアレポート｜マルウェア情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/200917.html

■フィッシングメールによって拡散された Dridex ダウンローダーの解析レポート
https://eset-info.canon-its.jp/files/user/malware_info/images/threat/201120/Malware_Report_Dridex_202011.pdf

Canon

キヤノンマーケティングジャパン株式会社