2024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

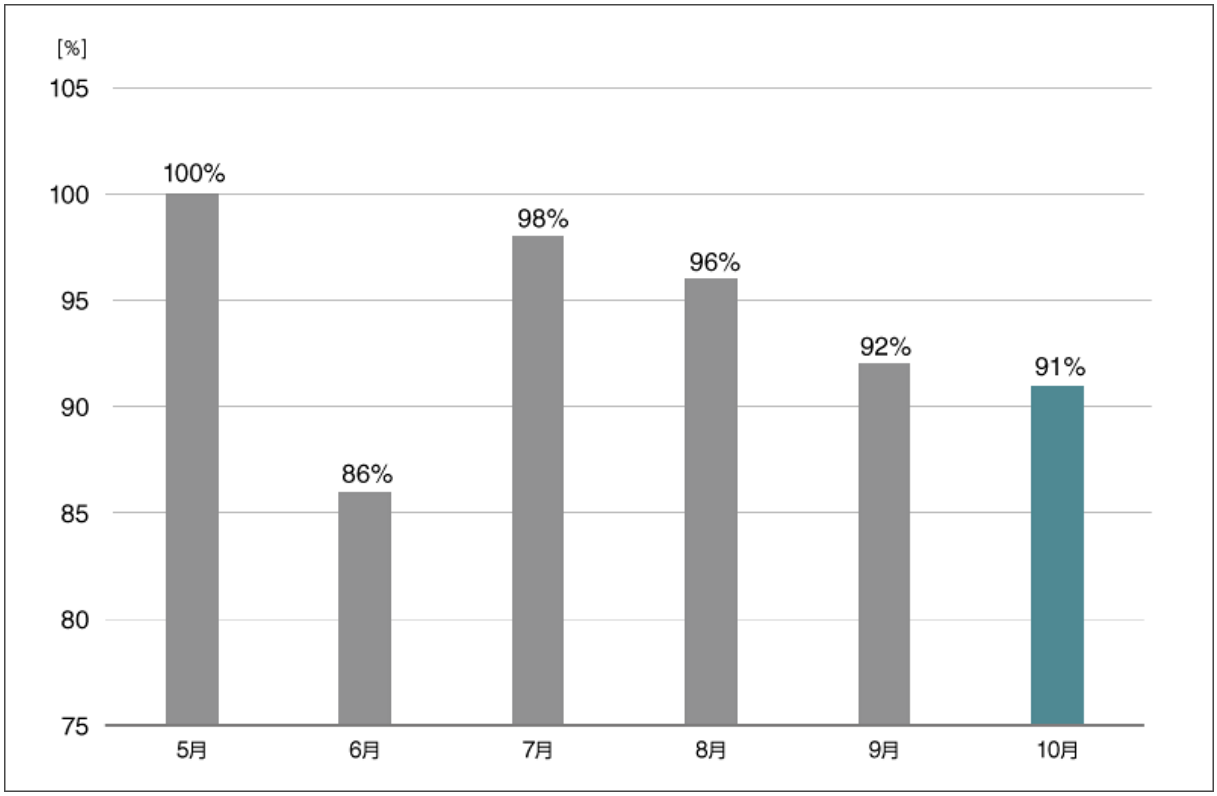
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2024 年 10 月マルウェア検出状況

2024 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

（2024 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。

2024 年 10 月の国内マルウェア検出数は、2024 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（2024 年 10 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	24.3%	アドウェア
2	JS/Adware.Agent	18.2%	アドウェア
3	HTML/Phishing.Agent	11.8%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	5.3%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	WinGo/Spy.Agent	1.5%	情報窃取を目的とした Go 言語 マルウェア
6	HTML/Phishing.Gen	1.4%	フィッシングサイトのリンクが埋め込まれた HTML ファイル
7	JS/Agent	1.3%	不正な JavaScript の汎用検出名
8	DOC/TrojanDownloader.Agent	1.0%	ダウンローダー
9	HTML/FakeCaptcha	0.8%	偽の CAPTCHA を表示させる HTML ファイル
10	MSIL/TrojanDownloader.Agent	0.7%	ダウンローダー

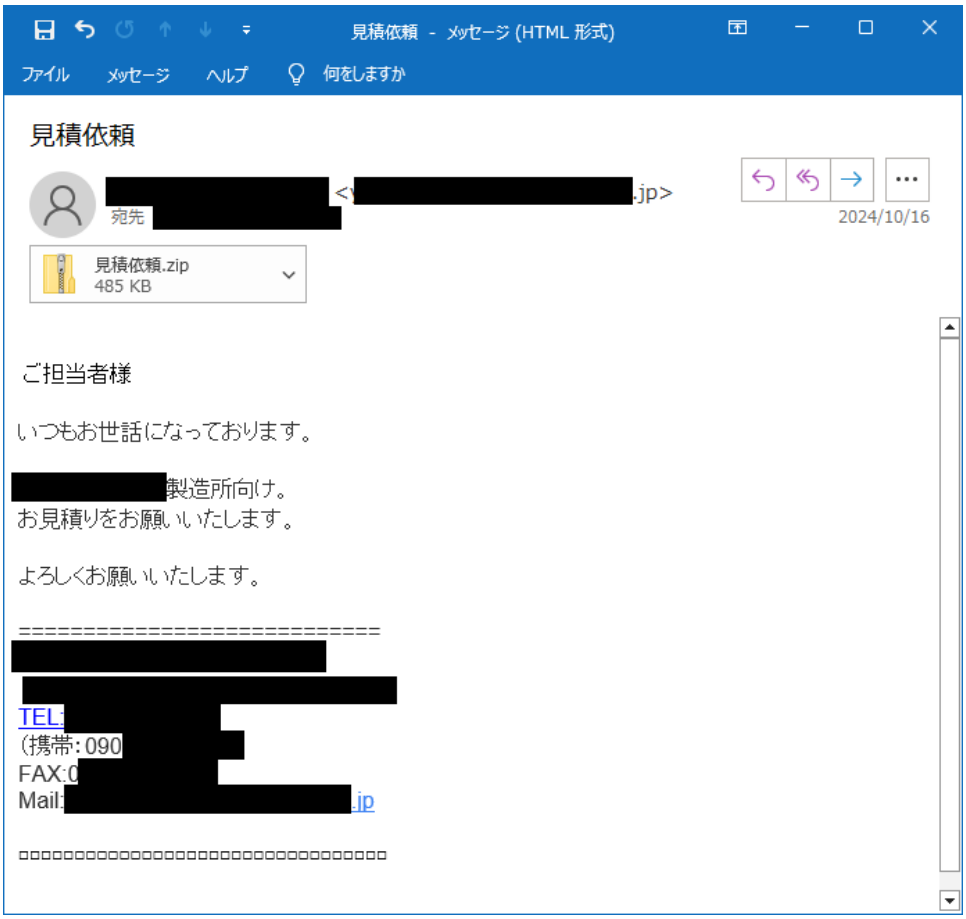
*2 本表には PUA を含めていません。

10 月に国内で最も多く検出されたマルウェアは、JS/Adware.TerraClicks でした。
JS/Adware.TerraClicks は、悪意のある広告を表示させるアドウェアの検出名です。Web サイト閲覧時に実行されます。

Snake Keylogger の感染を狙ったばらまきメール

10 月は、情報窃取マルウェア Snake Keylogger の感染を狙ったマルウェア付きのメールが確認されています。以下では、確認されたメールと Snake Keylogger について紹介します。

今回の攻撃では、「見積依頼」、「見積りのご依頼」などの件名のメールに圧縮ファイルが添付されています。圧縮ファイルは、zip 形式だけでなく rar 形式や 7z 形式などが存在します。



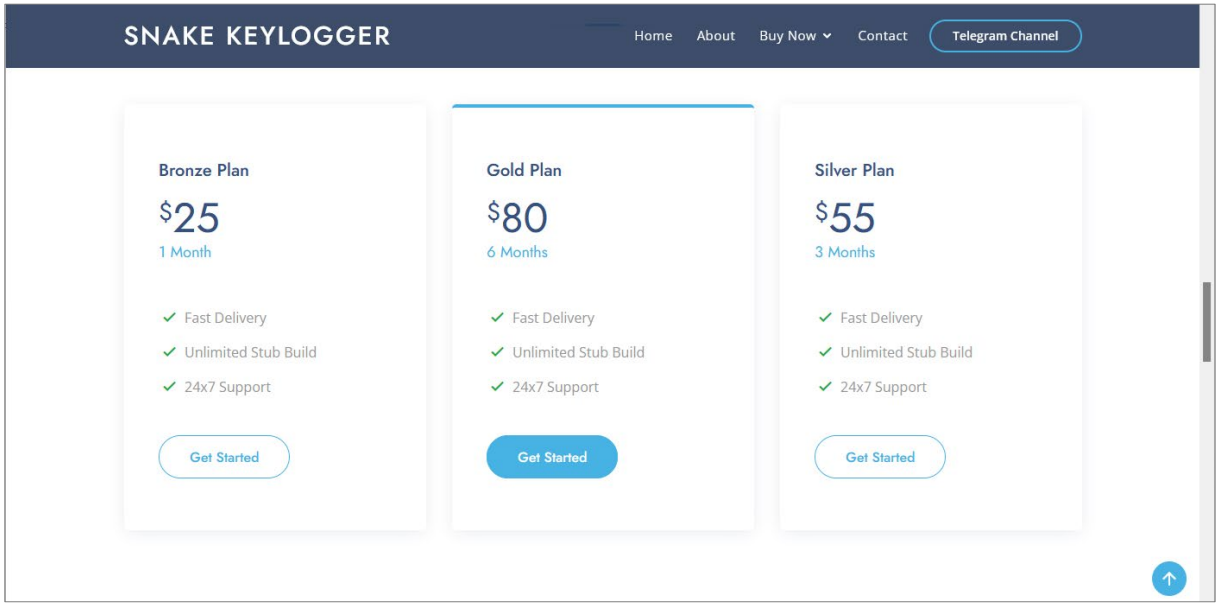
Snake Keylogger の感染を狙ったメール

メールに添付された圧縮ファイルを展開すると、以下のように実行ファイルが確認できます。

添付された圧縮ファイル内の実行ファイル

当該ファイルを実行すると、Snake Keylogger に感染する可能性があります。ESET 製品では、「MSIL/Kryptik」や「MSIL/Cassandra」などの検出名で検出します。

Snake Keylogger（別名: 404 Keylogger）は、.NET で作成された情報窃取マルウェアです。2019 年に登場し、主にメール経由で感染します。Snake Keylogger の販売サイトによると最低 25 ドルで利用が可能になるようです。安価で利用可能であり攻撃者にとっても使い勝手のいいツールであると考えられます。



Snake Keylogger の販売サイト

このマルウェアは、キー入力、スクリーンショット、クリップボードの情報、さまざま様々なアプリの認証情報を窃取します。対象となるアプリは、Firefox などの Gecko ベースのブラウザー、Google Chrome や Microsoft Edge などの Chromium ベースのブラウザー、Thunderbirds などのメールアプリ、Discord などのチャットアプリと多岐にわたります。
これにより窃取された情報は、SMTP、FTP、Telegram などにより攻撃者に送信されます。

今回確認した攻撃には、メール本文に実在する企業の名前が使われているものを確認しています。また、いくつかの企業から今回の攻撃に関するなりすましメールの注意喚起が行われています。
不審なメールを受信した際には、関連する注意喚起が行われていないか検索して確認することも重要です。また、情報窃取には、Telegram が悪用される場合もあるため、業務で Telegram を利用していない場合は、Telegram API へのアクセスをブロックすることで情報流出を防止できる可能性があります。

まとめ

2024 年 10 月マルウェアレポートでは、情報窃取マルウェア Snake Keylogger の感染を狙ったマルウェア付きメールについて紹介しました。
情報窃取マルウェアは、2024 年 9 月のマルウェアレポートでも紹介しており、8 月と比較して 9 月の検出数は倍増しています。近年脅威が増している情報窃取マルウェアについての概要や対策については、9 月のマルウェアレポートも合わせて確認してください。

■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．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

●Snake Keylogger の新しい亜種の詳細分析 | FortiGuard Labs
https://www.fortinet.com/jp/blog/threat-research/deep-analysis-of-snake-keylogger-new-variant

Canon

キヤノンマーケティングジャパン株式会社