2024年
9月
SEPTEMBER

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

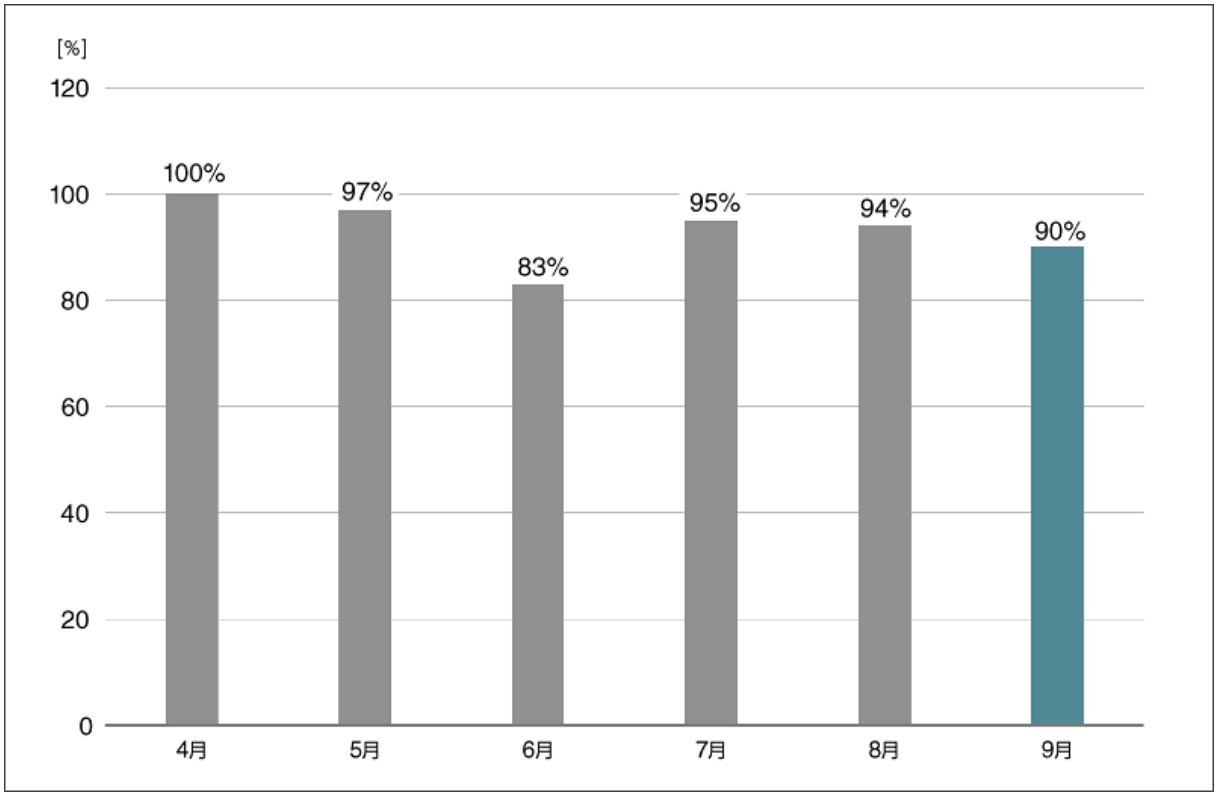
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 9 月マルウェア検出状況

2024 年 9 月（9 月 1 日～9 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

（2024 年 4 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 9 月の国内マルウェア検出数は、2024 年 8 月と比較して減少しました。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 9 月）

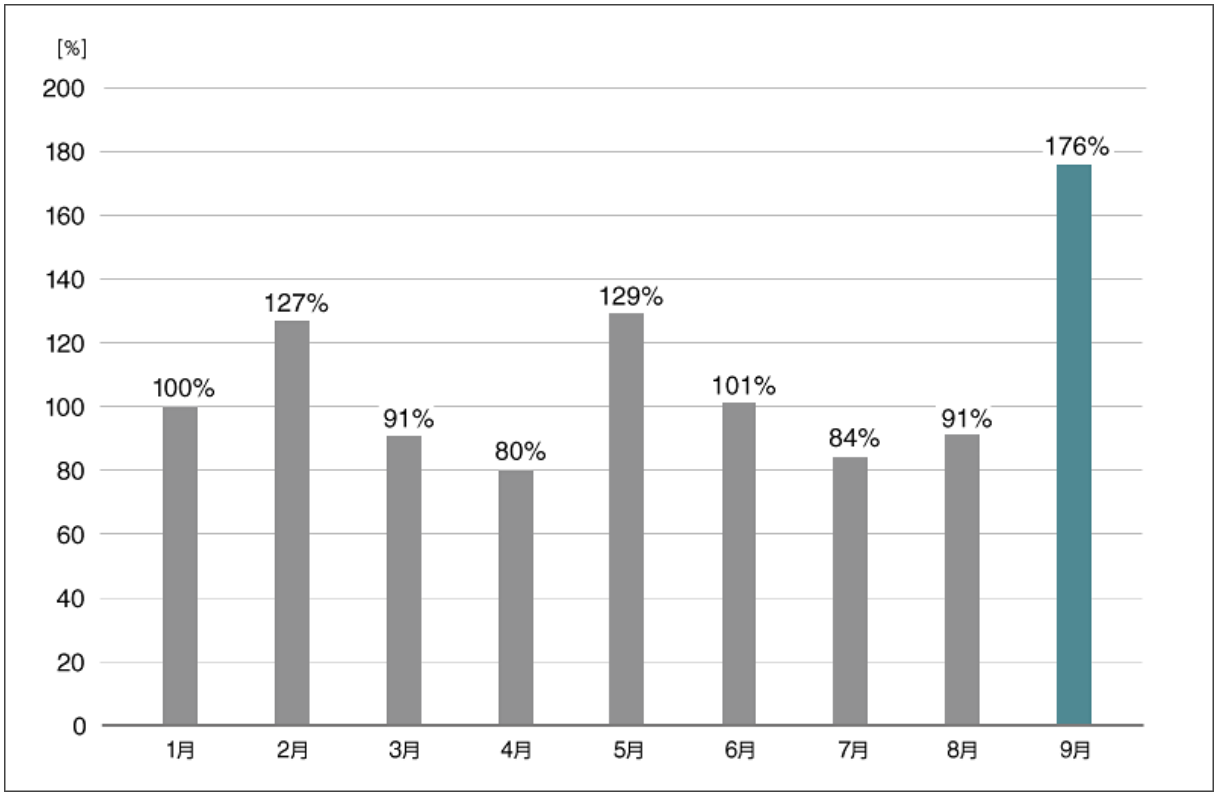
順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	20.9%	アドウェア
2	JS/Adware.Agent	18.7%	アドウェア
3	DOC/Fraud	18.3%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	HTML/Phishing.Agent	9.0%	メールに添付された不正な HTML ファイル
5	JS/Agent	1.4%	不正な JavaScript の汎用検出名
6	Win32/Formbook	1.4%	情報窃取型マルウェア
7	PDF/Fraud	0.9%	詐欺サイトのリンクが埋め込まれた PDF ファイル
8	MSIL/Spy.AgentTesla	0.8%	情報窃取型マルウェア
9	JS/Adware.Sculinst	0.8%	アドウェア
10	HTML/Phishing.WeTransfer	0.8%	WeTransfer を騙ったフィッシング詐欺を目的とした HTML ファイル

*2 本表には PUA を含めていません。

9 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。

情報窃取型マルウェアの増加

前章で紹介したように 9 月の検出数 TOP10 には、Win32/Formbook や MSIL/Spy.AgentTesla といった検出名が入りました。これらは、有名な情報窃取型マルウェアファミリーである Formbook と AgentTesla の検出名です。
2024 年 9 月の情報窃取型マルウェアの検出数は 2024 年 8 月と比較して 2 倍近くに増加しており、2024 年で最も多くなりました。
そこで、今月のレポートでは対策の重要度が増した情報窃取型マルウェアについて紹介します。



情報窃取型マルウェアの検出数月別推移（国内、2024 年）
（2024 年 1 月の検出数を 100%として比較）

情報窃取型マルウェア

- 概要

情報窃取型マルウェアは、感染端末から機密情報をはじめとしたさまざまな情報を窃取することを目的としたマルウェアです。有名な情報窃取型マルウェアとして、Formbook や AgentTesla、RedLine、Stealc が挙げられます。

情報窃取型マルウェアの主な感染経路と感染した場合の想定被害をまとめたものが、表 1 です。

表 1　主に窃取される情報と主な感染経路

主に窃取される情報	OS やハードウェアなどのシステム情報
	ユーザーID やパスワードなどのアカウント情報 例）Web ブラウザーやメールクライアント、FTP クライアントに保存されたアカウント情報
	キーロガー機能による入力情報
	クリップボードに保存された情報
	暗号通貨のウォレット情報
	アプリケーション内データ 例）Steam、Discord
	画面のスクリーンショット
	Web カメラによる録画
主な感染経路	電子メールの添付ファイル 例）Microsoft Office ファイル（Word、OneNote ファイルなど）、ISO ファイル
	悪意のある広告
	正規ソフトウェアの海賊版
	SNS 上に記載された URL

● 情報窃取型マルウェアの特徴

ここでは、情報窃取型マルウェアの主な特徴を 3 つ紹介します。

・特徴①：感染に気付きにくい

情報窃取型マルウェアは、長期的に多くの情報を収集できるようにセキュリティ製品による検知を回避する機能が実装されています。具体的には、ProcessHollowing と呼ばれる手法を用いる AgentTesla が挙げられます。この手法は、正規プロセスに悪意のある動作を実行させることで、セキュリティ製品からの検知を回避しようとする狙いがあります。そのため、一度感染すると感染に気付かず、長期的に情報窃取被害に遭う恐れがあります。

・特徴②：窃取された情報による二次被害

情報窃取型マルウェアによって窃取された情報が、攻撃の実行犯以外の攻撃者にも広がる可能性があります。具体的には、RedLine などの情報窃取型マルウェアによって窃取された情報がダークウェブ上の専用フォーラムや Telegram チャンネルで販売されていることが挙げられます。こういったプラットフォームで販売された情報には、FTP クライアントや VPN などの認証情報が含まれていたことが確認されています。窃取された認証情報を購入した攻撃者が、組織内ネットワークに対して不正アクセスやランサムウェア感染といった二次被害に繋がる攻撃を実施する恐れがあります。

・特徴③：MaaS（Malware as a Service）形式での販売

情報窃取型マルウェアの中には、MaaS 形式でダークウェブ上のフォーラムを介して販売されているものがあります。有名なファミリーとして概要で紹介した 4 つのファミリーもダークウェブ上で購入可能です。これは、マルウェア開発などの特別な技術を持っていない攻撃者にも情報窃取型マルウェアによる攻撃を試せるようにしています。さまざまな攻撃者が参入可能なため、ユーザーが被害に遭遇する機会が多くなると考えられます。

情報窃取型マルウェアへの対策

情報窃取型マルウェアへの感染を未然に防ぐ対策と感染による被害を軽減する対策を紹介します。

・対策①：情報窃取型マルウェアの感染経路への対策

主な感染経路である電子メールの添付ファイルに対しては、添付ファイルを不用意に開かないことが重要です。また、Web サイトへアクセスする時には、セキュリティ製品のセキュアブラウザー機能を利用してください。ほかにも、ハッシュ値が公開されているソフトウェアのインストーラーをダウンロードする場合、ダウンロードしたファイルのハッシュ値と突き合わせて、ファイルが改ざんされていないかを確認してください。

・対策②：万が一情報窃取型マルウェアに感染した場合に備える対策
感染端末内の情報窃取型マルウェアの不審な挙動の早期発見には、EDR といった端末を監視できるツールが効果的です。EDR は端末内から収集した情報を常時監視し、情報の窃取やファイルの暗号化といった不審な挙動や端末内の異常を検知します。EDR は脅威を事前に防ぐことよりも、感染後の被害を最小限に抑えることに重きを置いたツールです。未然に防ぐための対策と合わせることで、より大きな効果を得られます。

まとめ

2024 年 9 月マルウェアレポートでは、情報窃取型マルウェアについて紹介しました。
情報窃取型マルウェアの 2024 年 9 月の検出数は、先月と比較して 2 倍近くに増加していました。情報窃取型マルウェアによる被害に遭わない／被害を最小限に抑えるためにも、今回紹介した対策の実施や組織内への情報共有を行ってください。併せて、IPA・JPCERT/CC といった機関やセキュリティベンダーから公表される注意喚起を収集してください。

■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

1) Trojan-as-a-service: From Formbook to XLoader | Acronis
https://www.acronis.com/en-sg/cyber-protection-center/posts/trojan-as-a-service-from-formbook-to-xloader/
2) ESET 脅威レポート 2023 年上半期版（2022 年 12 月～2023 年 5 月）を公開 ～変幻自在に姿を変え攻撃を仕掛けるサイバー犯罪者を確認～ | ESET Japan
https://www.eset.com/fileadmin/ESET/JP/Blog/threat-report/H1-2023_Threat-Report_JP_FINAL.pdf
3) Youtube を通じて拡散している情報窃取型マルウェア | ASEC
https://asec.ahnlab.com/jp/32488/
4) Process Injection: Process Hollowing | Mitre ATT&CK
https://attack.mitre.org/techniques/T1055/012/
5) 攻撃者によって窃取されたデータのアンダーグラウンドマーケットでの行き着く先 | TREND MICRO
https://www.trendmicro.com/ja_jp/research/24/g/your-stolen-data-for-sale.html

Canon

キヤノンマーケティングジャパン株式会社