2025年
5月
MAY

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

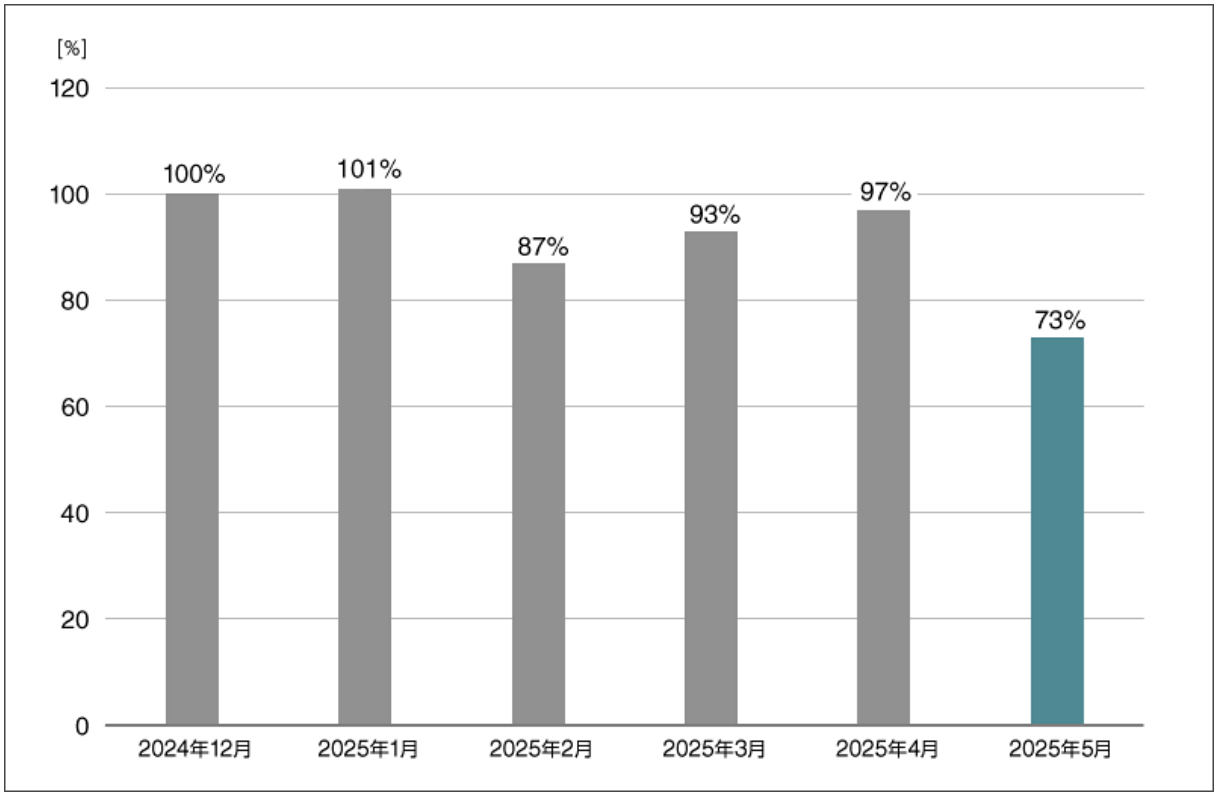
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

# 2025 年 5 月マルウェア検出状況

2025 年 5 月（5 月 1 日～5 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 12 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。

2025 年 12 月の国内マルウェア検出数は、2025 年 4 月と比較してしました。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（2025 年 5 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | DOC/Fraud | 19.5% | 詐欺サイトのリンクが埋め込まれた DOC ファイル |
| 2 | HTML/Phishing.Agent | 18.5% | メールに添付された不正な HTML ファイル |
| 3 | JS/Adware.Agent | 17.8% | アドウェア |
| 4 | HTML/FakeCaptcha | 3.1% | 偽の CAPTCHA を表示させる HTML ファイル |
| 5 | HTML/Phishing.Gen | 2.0% | フィッシングを目的とした不正な HTML ファイル |
| 6 | HTML/Fraud | 1.5% | 詐欺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 | MSIL/TrojanDownloader.Agent | 1.3% | ダウンローダー |
| 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。

5 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルです。主にメールの添付ファイルとして確認されており、不正な金銭の要求や個人情報の詐取といった被害に遭う可能性があります。

## Lumma Stealer について

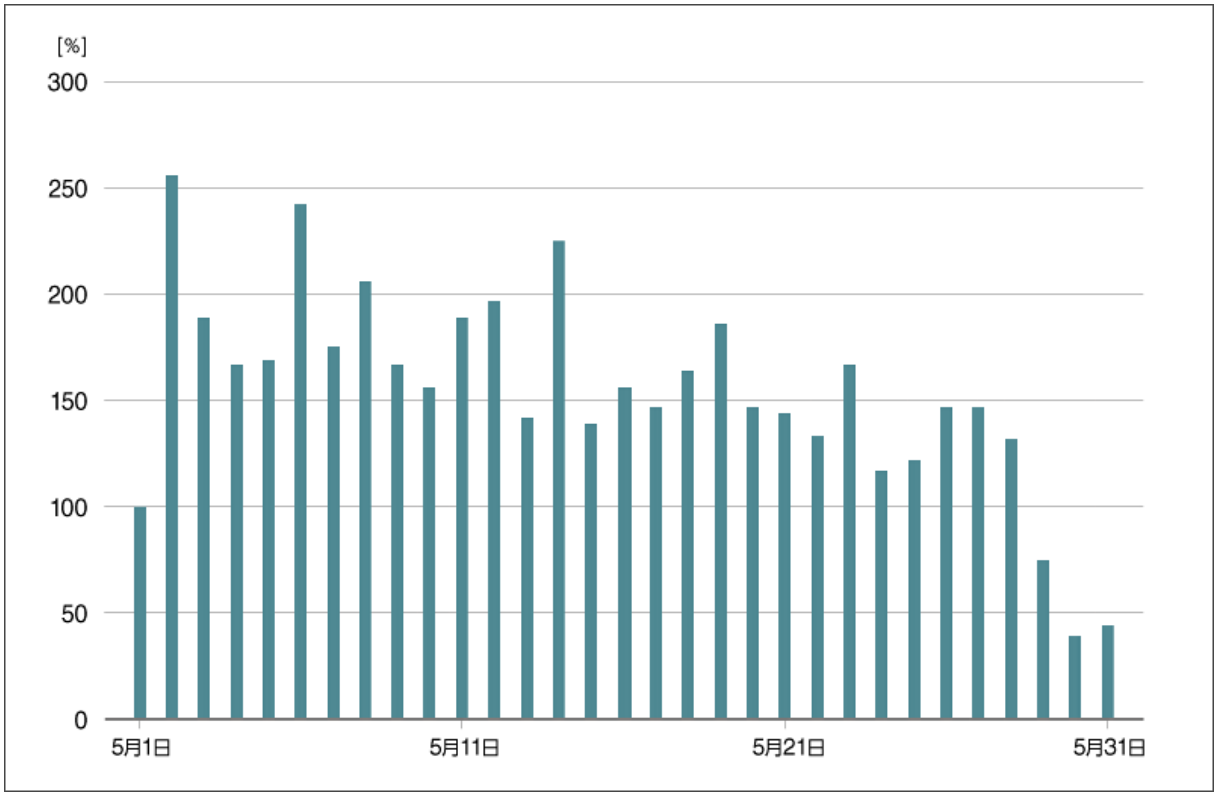
Lumma Stealer は 2022 年頃から活動が確認されている情報窃取型マルウェアであり、ロシア語圏のアンダーグラウンドマーケットで MaaS（Malware as a Service）として販売されています。MaaS は、開発者がマルウェアをサービスとして提供する形態で、専門知識がない人物でもマルウェアを使ったサイバー攻撃が行える仕組みです。主にアンダーグラウンドマーケット上で取引され、サイバー攻撃増加の一端を担っています。
Lumma Stealer は、情報窃取や感染永続化などの機能を有しており、仮想通貨ウォレット、ユーザー認証やブラウザ拡張機能などの重要な秘密情報を標的としています。窃取された情報は、アンダーグラウンドマーケット上で売買されていることも確認されています。
Lumma Stealer の主な感染経路は以下の 3 つです。

① 電子メールの添付ファイルやメール本文に記載された URL からのダウンロード
② ほかのマルウェアによるダウンロードと実行
③ 攻撃者が用意した Web ページからのダウンロード

3 つ目の感染経路では、偽の CAPTCHA 認証を悪用した Web ページが確認されています。偽の CAPTCHA 認証の悪用は ClickFix と呼ばれています。ClickFix による感染プロセスについては、2024 年 12 月マルウェアレポートにて解説しています。
Microsoft 社は、2025 年 3 月 16 日から 2025 年 5 月 16 日の 2 カ月間で、全世界の約 39 万台の Windows 端末に感染していたと報告しています。
このように感染規模が拡大していた Lumma Stealer のインフラを対象としたテイクダウン作戦が実行されました。次節では、このテイクダウン作戦について紹介します。

## Lumma Stealer のテイクダウンについて

2025 年 5 月 21 日、米国司法省が Lumma Stealer のインフラに対するテイクダウン作戦の実施を公表しました。この作戦には、FBI や Microsoft 社デジタル犯罪対策部門（DCU）、ESET 社などの組織が参加しました。また、攻撃者が各地域に設置したインフラに対するテイクダウンを支援するために、Europol や日本サイバー犯罪対策センター（JC3）などの機関も協力しました。この作戦によって、Lumma Stealer が使用していた 2,300 件以上のインターネットドメインや管理用コントロールパネルが押収されています。
今回の措置は Lumma Stealer のインフラに大きなダメージを与えましたが、テイクダウン後も C&C サーバーの活動や窃取した情報の販売が確認されています。




**Lumma Stealer 検出数日別推移（2025 年 5 月･国内）**
**※2025 年 5 月 1 日の検出数を 100%として比較**

ESET 製品による検出統計では、テイクダウン後も一定数の検出が継続していますが、5 月末に検出数の顕著な減少が見られます。

活動継続の兆候や統計情報から考えると、Lumma Stealer を用いた攻撃が再び活発化する可能性に注意が必要です。

## 今後考えられる Lumma Stealer 利用者の動向について

前述したとおり、Lumma Stealer には活動継続の兆候が確認されています。一方、Lumma Stealer 利用者の今後の動きとして、Lumma Stealer から別の情報窃取型マルウェアサービスへ移行する可能性が考えられます。Lumma Stealer は MaaS として提供されており、利用者にとって Lumma Stealer は、数ある選択肢の 1 つに過ぎません。テイクダウンによる機能低下や、法執行機関による追加措置を考慮すると、Lumma Stealer が MaaS 利用者の選択肢から外れる可能性もあります。
実際に Check Point 社の調査によれば、アンダーグラウンドマーケット上では Lumma Stealer のサービス継続を危惧する意見も交わされているようです。
また、過去の事例として、REvil ランサムウェアのテイクダウン後に、利用者が LockBit ランサムウェアへ移行したことも示唆されています。
これらの状況を踏まえれば、Lumma Stealer 利用者が今後 Lumma Stealer 以外の情報窃取型マルウェアサービスに移行し、活動を活発化させたとしても不思議ではなく、警戒を怠ってはいけません。以降は情報窃取型マルウェア全般の対策について紹介します。

## 情報窃取型マルウェアの対策について

今回は、「感染経路段階で脅威を防ぐ対策」と「万が一感染した場合に被害を軽減する対策」の 2 つの観点から情報窃取型マルウェアの対策を紹介します。

■感染経路段階で脅威を防ぐ対策
① 感染経路を検査・遮断するためのセキュリティ製品の導入・運用
② 情報収集と情報共有

① 感染経路を検査・遮断するためのセキュリティ製品の導入・運用
前述した感染経路である「メールの添付ファイル」「メール本文内の URL リンク」と「偽の CAPTCHA 認証を悪用した Web ページ」を対象にセキュリティ製品による検査を実施し、初期段階での侵入を防ぐ体制を整えてください。具体的な検査として、サンドボックス機能による添付ファイルの検査やネットワーク保護機能による通信先の検査が挙げられます。

② 情報収集と情報共有

情報窃取型マルウェアの中には、感染時にユーザーの操作が必要なケースがあります。知らない脅威には対応が難しいものですが、知識があれば備えることは可能です。組織内のメンバーが適切に脅威に対応できるよう、情報窃取型マルウェアの動向や感染手法について継続的に情報を収集し、組織内で共有してください。

■万が一感染した場合に被害を軽減する対策

① 端末／ネットワーク内の脅威を監視・検知するためのセキュリティ製品の導入・運用

② インシデント対応手順の策定と運用

① 端末／ネットワーク内の脅威を監視・検知するためのセキュリティ製品の導入・運用

情報窃取型マルウェアは多くの情報を窃取するために、感染の痕跡を隠して動作します。端末／ネットワーク内の異常な挙動を監視する EDR などのセキュリティ製品を導入・運用することで、情報窃取型マルウェアを早期検知する体制を整えてください。

② インシデント対応手順の策定と運用

万が一感染した場合に被害を軽減するためには、迅速な報告と対応が欠かせません。感染時の報告先や報告手順を明文化し、組織内に周知してください。最大限効果を発揮するためにも、定期的な手順の見直しと訓練の実施を推奨します。

## まとめ

今月は Lumma Stealer のテイクダウン後の動向から情報窃取型マルウェアの対策を紹介しました。今後、別の情報窃取型マルウェアサービスが Lumma Stealer になり替わる可能性も考えられます。本レポートで紹介した対策を元に、組織内の備えを見直してください。

■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

●Lumma Stealer | MITRE ATT&CK
https://attack.mitre.org/software/S1213/
●Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations | CISA
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b
●ESET takes part in global operation to disrupt Lumma Stealer | WeliveSecurity
https://www.welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-lumma-stealer/
●Europol and Microsoft disrupt world’s largest infostealer Lumma | Europol
https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
●Lumma Infostealer – Down but Not Out? | CHECKPOINT
https://blog.checkpoint.com/security/lumma-infostealer-down-but-not-out/

Canon

キヤノンマーケティングジャパン株式会社