2025年
3月
MARCH

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

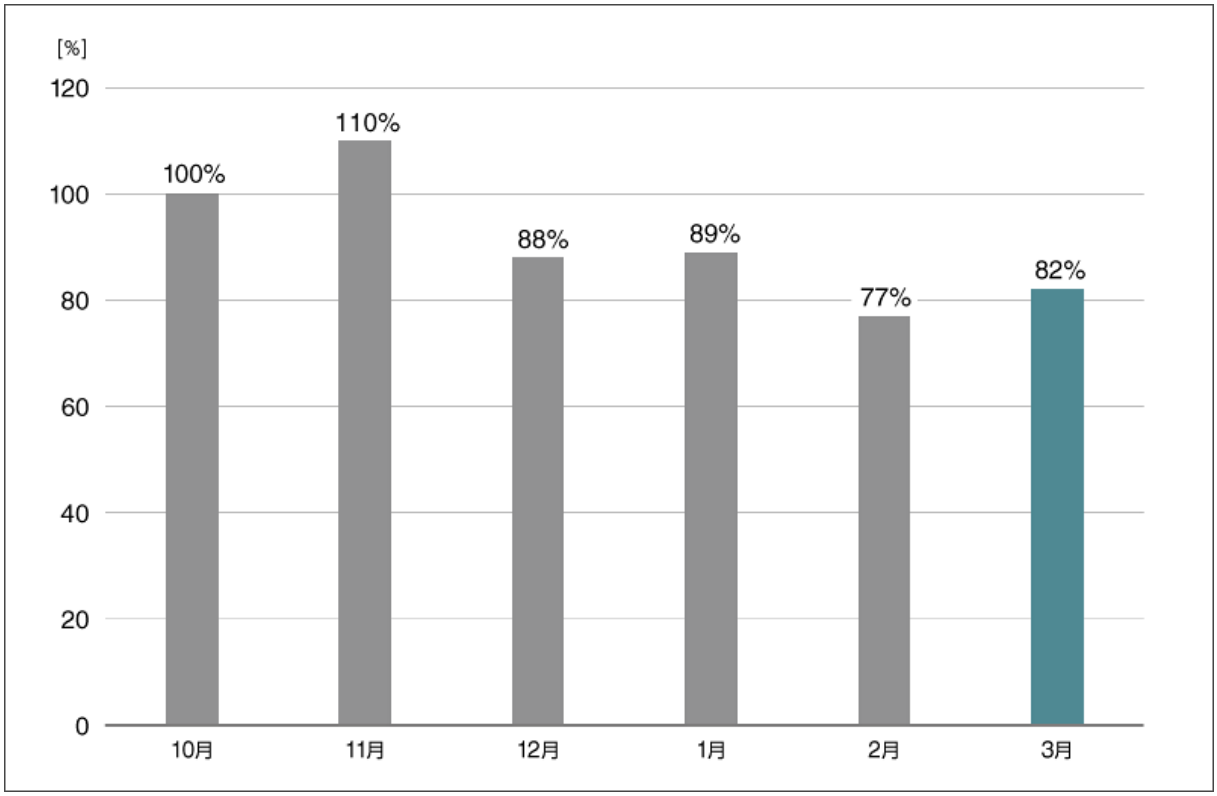
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 3 月マルウェア検出状況

2025 年 3 月（3 月 1 日～3 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 10 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 3 月の国内マルウェア検出数は、2025 年 2 月と比較して増加しました。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 3 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	21.6%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	20.5%	アドウェア
3	HTML/FakeCaptcha	9.6%	偽の CAPTCHA を表示させる HTML ファイル
4	DOC/Fraud	1.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	1.9%	不正な JavaScript の汎用検出名
6	HTML/Fraud	1.7%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	MSIL/Spy.Agent	1.0%	情報窃取を目的としたマルウェアの汎用検出名
8	HTML/Phishing	1.0%	フィッシングを目的とした不正な HTML ファイル
9	HTML/Phishing.WeTransfer	0.8%	特定ブランドを騙ったフィッシングサイトの検出名
10	DOC/TrojanDropper.Agent	0.8%	ドロッパー

*2 本表には PUA を含めていません。

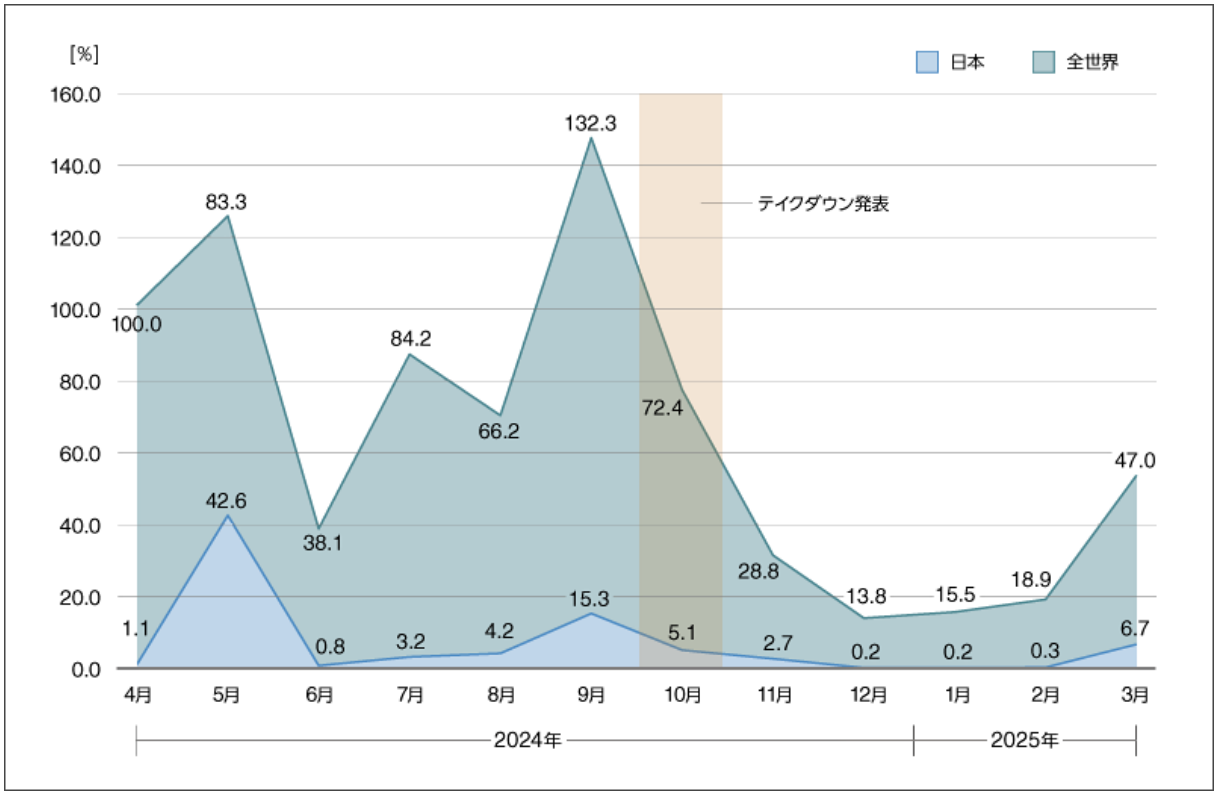
3 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL に接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

RedLine の再燃兆候を観測

2024 年 10 月にテイクダウンが発表されたマルウェア RedLine（RedLine Stealer）について、2025 年 3 月に ESET の検出数が増加したことを確認しました。
RedLine はアンダーグラウンドフォーラムで販売されている情報窃取型のマルウェアで、2020 年 3 月頃から活動が確認されました。このマルウェアに感染すると、ブラウザーに保存されている認証情報やオートコンプリート履歴、感染 PC のハードウェア構成や OS のユーザーアカウント情報、暗号通貨ウォレットに関する情報などが窃取されます。
RedLine の感染被害端末は世界中で数百万台と推定されており、世界的に猛威を奮っていました。そこで世界各国の捜査機関が協力し、「Operation Magnus」と呼ばれるテイクダウン作戦が実行され、RedLine（および META Stealer[*3]）によって使用されていたインフラを押収したことが 2024 年 10 月に発表されました。

*3 コードや操作パネルなど、RedLine と同一の機能が確認されているマルウェアです。

直近の 1 年間における RedLine の ESET 検出傾向を以下に示します。2024 年 9 月に全世界の検出数が最も高い値となっていましたが、その翌月にテイクダウンが発表されて以降、検出数は減少していました。しかし 2025 年 3 月に入ると、国内と全世界のどちらも検出数が大きく増加したことが確認できます。



直近 1 年間における RedLine の検出数推移
（2024 年 4 月の全世界検出数を 100%として比較）

本稿の執筆時点で RedLine が復活した旨の情報は確認できていません。しかしながら、テイクダウンの発表後に活動を再開したマルウェアが過去に存在するため、RedLine についても本格的に復活する可能性は否定できません。ここからは活動再開したマルウェアの事例を 3 つ取り上げ、テイクダウン後も油断せずに警戒することの重要性について説明します。

テイクダウン後に活動再開が確認された事例 1（GameOver Zeus）

GameOver Zeus は 2005 年から活動が確認されたマルウェアです。このマルウェアは、MITM（Man-in-the-Middle）攻撃の手法を用いてオンラインバンキングに関連する個人情報を窃取する機能や、感染した PC 同士でボットネットを形成する機能を有しています。
世界中で 50 万台から 100 万台の PC が感染被害に遭ったと推測されていましたが、米国連邦捜査局（FBI）と欧州刑事警察機構（Europol）が中心となって「Operation Tovar」と呼ばれる作戦が実施さ

れ、テイクダウンしたことが 2014 年 6 月に発表されました。
ところが翌 7 月に、newGOZ と名付けられた GameOver Zeus の亜種が確認されました。この亜種はドメイン生成アルゴリズム（DGA）および Fast Flux 手法という 2 つの技術を新たに取り入れており、通信先の C&C サーバーの特定が困難になるよう改良されていました。

テイクダウン後に活動再開が確認された事例 2（Emotet）

Emotet は 2014 年に初めて存在が確認され、国内でもメディアで取り上げられたことをきっかけに存在が広く認知されるようになったマルウェアです。このマルウェアは感染端末からメールのアカウントやデータを窃取し、それらの情報をもとに巧妙なスパムメールを送信して感染を拡大させる特徴があります。
Emotet の世界的な流行を受け、Europol を中心とする欧米の捜査機関が「Operation LadyBird」と呼ばれる作戦を実行し、2021 年 1 月にテイクダウンが発表されました。
しかし同年 11 月には活動再開が確認され、その後ショートカットファイルや Microsoft OneNote 形式のファイルをダウンローダーとして悪用するなど、感染手法を変化させながら再び猛威を奮いました。

テイクダウン後に活動再開が確認された事例 3（Qakbot）

Qakbot は 2008 年から存在が確認されているマルウェアです。当初は銀行に関する個人情報を窃取するバンキングマルウェアとして知られていましたが、徐々に機能を変化させていき、近年ではボットネットを形成してほかのマルウェアを配信する機能が特に脅威となっていました。
2023 年には世界中のおよそ 70 万台の PC が感染していたとされていますが、FBI や各国の捜査機関が中心となり実行した「DuckHunt」と呼ばれる作戦により、2023 年 8 月にテイクダウンしたと発表されました。
しかしながら 2023 年 12 月、悪性の PDF ファイルを介して Qakbot を配信するフィッシングメールについて Microsoft 社が警告し、Qakbot の復活が世間に知れわたりました。その後に確認された Qakbot の亜種には、バイナリに含まれる文字列や C&C 通信の情報を別の手法で難読化する、Adobe のソフトウェアが実行されていることを装うポップアップを出現させるなどの機能変更が報告されています。

また Qakbot のボットネットを使用してランサムウェアを配信していたグループの 1 つである Black Basta は、Qakbot のテイクダウン前まで、被害組織に対する犯行声明を自分たちのブログ上に毎月報告していました。ところがテイクダウン後の 9 月は犯行声明が 1 件も報告されず、10 月半ばに入ってから再び報告されるようになりました。この動きについて、Black Basta がテイクダウンの影響を受けて一時的に活動できなくなったが、Qakbot とは異なるボットネットに乗り換えることで活動を再開した可能性があるとする見解もあります。

過去のマルウェア復活事例を教訓に

今回取り上げたマルウェアの活動再開事例を以下の表にまとめます。特筆すべき点として、どのマルウェアもテイクダウンが発表されてから数カ月後には活動再開していることが挙げられます。したがってマルウェアが復活する可能性を考え、少なくともマルウェアのテイクダウン発表直後にセキュリティ製品の検出ルールから当該マルウェアの情報を削除することは避けるべきです。

マルウェアの活動再開事例のまとめ

マルウェア名	テイクダウン発表の年月	テイクダウンの作戦名	活動再開の年月	活動再開後の動向（※）
GameOver Zeus	2014 年 6 月	Operation Tovar	2014 年 7 月	・機能を追加した亜種の登場
Emotet	2021 年 1 月	Operation LadyBird	2021 年 11 月	・新たな感染手法の利用
Qakbot	2023 年 8 月	DuckHunt	2023 年 12 月	・機能を追加した亜種の登場 ・別のインフラを使用したマルウェアの配布
RedLine	2024 年 10 月	Operation Magnus	–	–

※今回取り上げた内容のみを記載しています。

またテイクダウンした脅威インフラを使用して活動する攻撃グループやマルウェアについて、Qakbot のようにテイクダウンに合わせて一時的に活動が停滞する場合があります。しかしサイバー攻撃の分業化が進んでいる現在では、インフラの乗り換えが容易に実施でき、短期間で活動再開する恐れがあります。よってテイクダウンが発表されても安心せず、常に最新の脅威情報を追いかけて警戒を怠らないようにしてください。

■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

●New Zeus Gameover Employs DGA and Fast Flux Techniques - 脅威データベース | Trend Micro
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/spam/578/new-zeus-gameover-employs-dga-and-fast-flux-techniques

●Qbot malware returns in campaign targeting hospitality industry | Bleeping Computer
https://www.bleepingcomputer.com/news/security/qbot-malware-returns-in-campaign-targeting-hospitality-industry/

●New Qbot malware variant uses fake Adobe installer popup for evasion | Bleeping Computer
https://www.bleepingcomputer.com/news/security/new-qbot-malware-variant-uses-fake-adobe-installer-popup-for-evasion/

●テイクダウンされた QakBot、それでも活動を続けるランサムウェアオペレーション | KELA
https://www.kelacyber.com/ja/blog/surviving-the-qakbot-takedown-black-basta-and-knight-ransomware-operations/

Canon

キヤノンマーケティングジャパン株式会社