2025年
1·2月
JAN / FEB

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

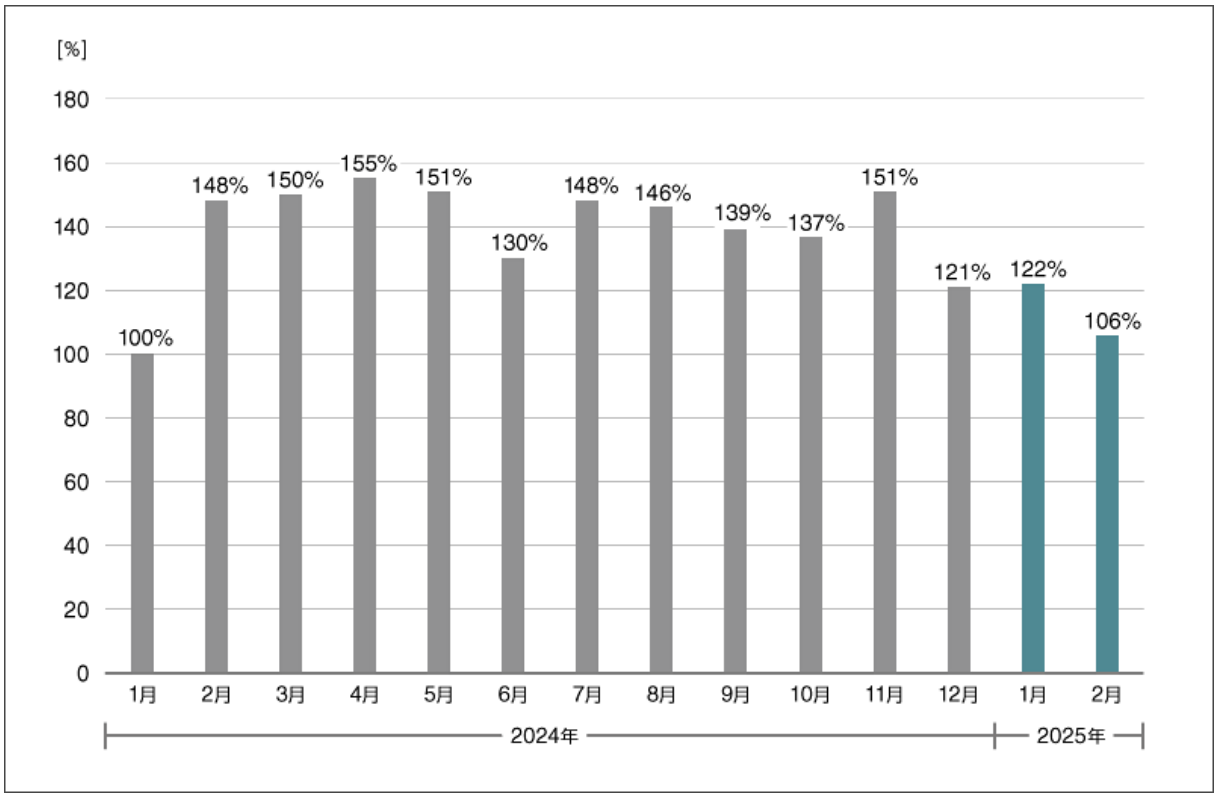
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 1 月･2 月マルウェア検出状況

2025 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 28 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 1 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 1 月の国内マルウェア検出数は、2024 年 12 月と同程度の検出数でした。そして、2025 年 2 月の国内マルウェア検出数は、2025 年 1 月と比較して減少しています。
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 1 月･2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	17.3%	アドウェア
2	HTML/FakeCaptcha	13.1%	偽の CAPTCHA を表示させる HTML ファイル
3	HTML/Phishing.Agent	11.1%	メールに添付された不正な HTML ファイル
4	JS/Adware.Terraclick	10.2%	アドウェア
5	DOC/Fraud	8.5%	詐欺サイトのリンクが埋め込まれた DOC ファイル
6	JS/Agent	5.9%	不正な JavaScript の汎用検出名
7	HTML/Phishing.WeTransfer	3.3%	特定ブランドを騙ったフィッシングサイトの検出名
8	HTML/Phishing	2.3%	フィッシングを目的とした不正な HTML ファイル
9	HTML/Phishing.MetaMask	1.4%	特定ブランドを騙ったフィッシングサイトの検出名
10	HTML/Nomani	0.9%	詐欺を目的とした不正な HTML ファイル

国内マルウェア検出数*2 上位（2025 年 1 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	19.0%	アドウェア
2	JS/Adware.Agent	16.6%	アドウェア
3	HTML/Phishing.Agent	9.6%	メールに添付された不正な HTML ファイル
4	HTML/FakeCaptcha	8.7%	偽の CAPTCHA を表示させる HTML ファイル
5	DOC/Fraud	8.1%	詐欺サイトのリンクが埋め込まれた DOC ファイル
6	JS/Agent	2.9%	不正な JavaScript の汎用検出名
7	HTML/Phishing.MetaMask	2.1%	特定ブランドを騙ったフィッシングサイトの検出名
8	HTML/Phishing.WeTransfer	1.9%	特定ブランドを騙ったフィッシングサイトの検出名
9	HTML/Phishing	1.0%	フィッシングを目的とした不正な HTML ファイル
10	HTML/Nomani	0.9%	詐欺を目的とした不正な HTML ファイル

国内マルウェア検出数*2 上位（2025 年 2 月）

順位	マルウェア	割合	種別
1	HTML/FakeCaptcha	18.1%	偽の CAPTCHA を表示させる HTML ファイル
2	JS/Adware.Agent	18.1%	アドウェア
3	HTML/Phishing.Agent	12.8%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	9.0%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	1.5%	不正な JavaScript の汎用検出名
6	HTML/Phishing	1.4%	フィッシングを目的とした不正な HTML ファイル
7	JS/Adware.Sculinst	0.9%	アドウェア
8	MSIL/Spy.Agent	0.9%	情報窃取型マルウェア
9	HTML/Phishing.WeTransfer	0.9%	特定ブランドを騙ったフィッシングサイトの検出名
10	HTML/Nomani	0.8%	詐欺を目的とした不正な HTML ファイル

*2 本表には PUA を含めていません。

1 月と 2 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent 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。

・検出数上位 10 種にランクインした Web ブラウジング中に遭遇する脅威

2024 年 12 月に引き続き Web ブラウジング中に遭遇する脅威が検出数上位 10 種に多数入っています。2025 年 1 月・2 月の検出数上位 10 種には、HTML/FakeCaptcha や HTML/Phishing.Agent、HTML/Phishing.WeTransfer、HTML/Nomani などの検出名が入っています。これらの検出名は目的が異なるため、検出名と目的を表にまとめました。表は以下のとおりです。

検出数上位 10 種に入っている HTML ファイル

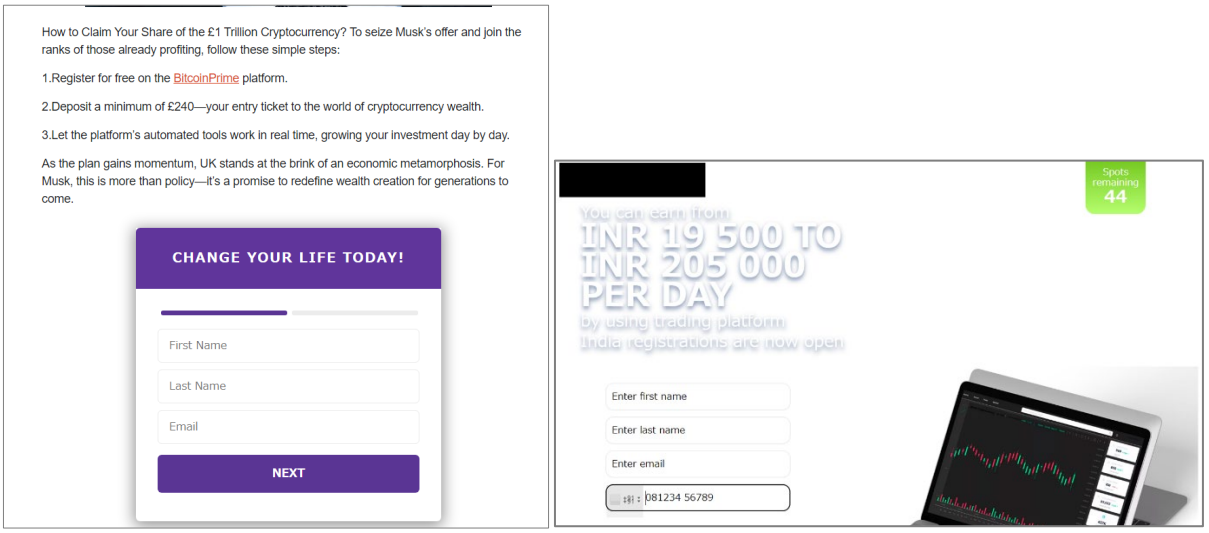
検出名	概要
HTML/FakeCaptcha	ほかのマルウェアのダウンロードを行う HTML ファイル
HTML/Phishing.Agent	フィッシング詐欺を目的とした HTML ファイル
HTML/Phishing.WeTransfer	フィッシング詐欺を目的とした HTML ファイル
HTML/Phishing	フィッシング詐欺を目的とした HTML ファイル
HTML/Phishing.MetaMask	フィッシング詐欺を目的とした HTML ファイル
HTML/Nomani	投資詐欺を目的とした HTML ファイル

中でも HTML/Nomani は 12 月から継続して上位 10 種に入っている検出名であり、国内においても大きな脅威の 1 つとなっています。
そこで今回は、近年被害報告が多く、被害規模も大きい投資詐欺につながる詐欺サイトを検出した HTML/Nomani を取り上げます。

・HTML/Nomani について

HTML/Nomani は、個人情報を収集する詐欺サイトである HTML ファイルの検出名です。HTML/Nomani は、投資詐欺の前段階の情報収集として機能しています。有名企業ブランドや有名人を騙った広告に加えて、偽のニュースサイトや偽の暗号資産について掲載した Web サイトである HTML/Nomani が現在確認されています。詐欺サイトにアクセスしたユーザーに名前や電話番号、メールアドレスといった個人情報を入力させることが目的となっています。

実際に HTML/Nomani として検出された Web サイト例がこちらです。

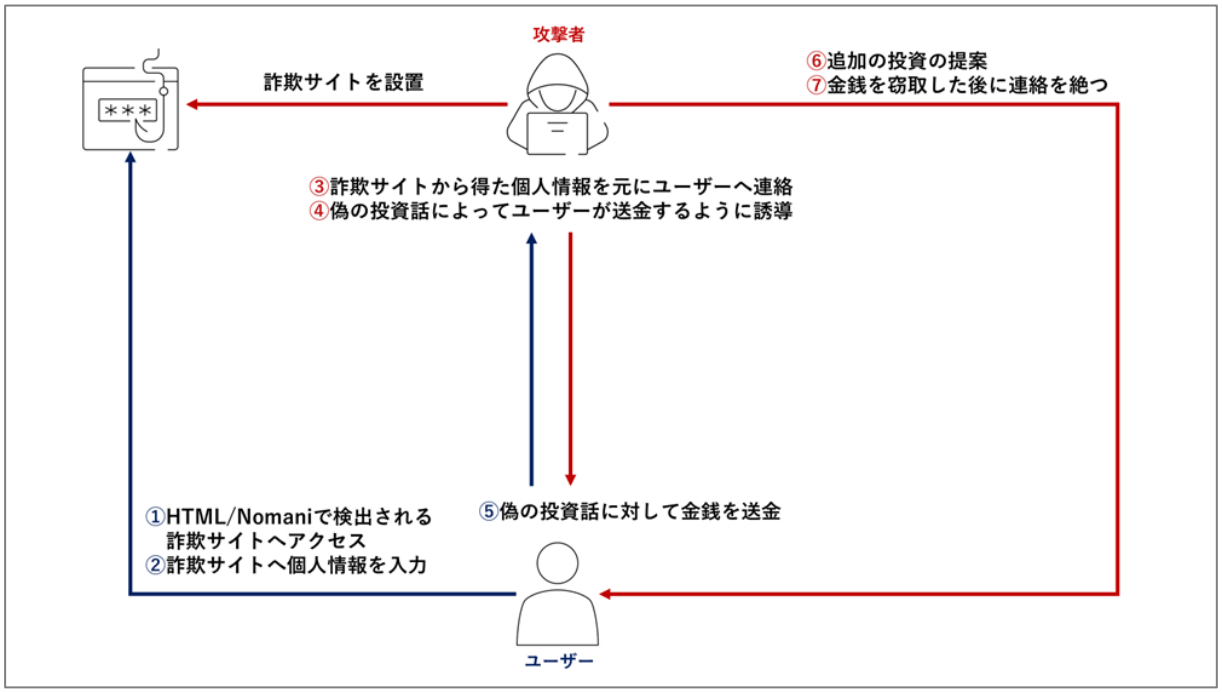


HTML/Nomani として検出された HTML ファイルを開いた様子

ユーザーに投資を持ち掛ける文章が記載されており、氏名・メールアドレス・電話番号などの個人情報の入力を促します。それ以外に HTML/Nomani として検出される Web サイトの中には、ユーザーに投資参加費用を求めるものもありました。
攻撃者は、この方法で収集した個人情報を利用して、投資詐欺を行います。

・HTML/Nomani による投資詐欺

HTML/Nomani による投資詐欺は、大きな利益を得られるという偽の投資にユーザーを誘導することでユーザーから多額の金銭を窃取する詐欺です。ユーザーを騙すために攻撃者は密に連絡を取ってユーザーとの関係を構築します。ESET の脅威レポート内では、投資による金銭窃取が一度ではない事例が報告されています。利益の支払いを求めたユーザーに対して、追加料金の支払いやクレジットカード情報といったさらなる情報の提供を求めるケースがありました。
ESET の脅威レポート内で紹介されている投資詐欺の概要を元に作成した詐欺の流れを以下に示します。



HTML/Nomani による投資詐欺の流れ

HTML/Nomani による投資詐欺を時系列に並べたものは、以下のとおりです。

① 【ユーザー】HTML/Nomani で検出される詐欺サイトへアクセス
② 【ユーザー】詐欺サイトへ個人情報（氏名、メールアドレス、電話番号など）を入力
③ 【攻撃者】詐欺サイトから得た個人情報を元にユーザーへ連絡
④ 【攻撃者】偽の投資話によってユーザーに送金するように誘導
⑤ 【ユーザー】偽の投資話に対して金銭を送金
⑥ 【攻撃者】追加の投資の提案（ユーザーからの問い合わせへの対応も実施）
⑦ 【攻撃者】金銭を窃取した後に連絡を絶つ

フィッシング詐欺による不正送金の場合、窃取した情報を利用するため、攻撃者が金融機関などの認証を突破する必要があります。しかし、このケースの場合、ユーザー自身が攻撃者へ送金するため、攻撃者がわざわざ金融機関の認証をすり抜ける必要はありません。

・HTML/Nomani による投資詐欺への対策

今回紹介した HTML/Nomani による投資詐欺への対策を紹介します。

■推奨する対策

対策①：普段からアクセスする Web サイトはブックマークからアクセスする

対策②：セキュリティ製品のセキュアブラウザ機能を使って Web ブラウジングする

対策③：投資や金銭の授受について記載に疑問を抱く Web サイトや持ち掛けられた投資話を以下の注意すべきポイントと照らし合わせる

【対策③の注意すべきポイント】

警察庁が公開している特殊詐欺対策ページを元に注意すべきポイントを紹介します。

- 投資先が実在しているか
- 金融商品取引業や暗号資産交換業の登録を行っている業者かどうか
- 「必ずもうかる」「あなただけ」という文言に注意
- 投資を勧めている「著名人」がなりすましされていないか
- 相手が勧める「暗号資産」「投資アプリ」などの商品が実在するか
- 振込先の口座に不審な点がないか

※金融商品取引業や暗号資産交換業の登録を行っている業者については、以下の金融庁 Web サイトを確認してください。

https://www.fsa.go.jp/ordinary/chuui/highrisk.html

・まとめ

2024 年 1 月･2 月では、投資詐欺の前段階として個人情報を収集する Web サイトである HTML/Nomani を紹介しました。ネットで知り合った人から投資を勧められた場合、その投資対象に不審な点がないかどうかや登録されている業者かどうかを確認してください。また、警察庁や金融庁といった機関から公開されている注意喚起を収集し、組織内で共有を行ってください。

■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) ESET 脅威レポート 2024 年下半期 | ESET
https://www.eset.com/fileadmin/ESET/JP/Blog/threat-report/H2-2024_Threat-Report_J_FINAL.pdf
2) 詐欺的な投資勧誘等にご注意ください！ | 金融庁
https://www.fsa.go.jp/ordinary/chuui/attention.html
3) SNS 型投資･ロマンス詐欺 | 警察庁･SOS47 特殊詐欺対策ページ
https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/sns-romance/
4) 無登録業者との取引は要注意！！ ～無登録業者との取引は高リスク～ | 金融庁
https://www.fsa.go.jp/ordinary/chuui/highrisk.html

Canon

キヤノンマーケティングジャパン株式会社