2024年
12月
DECEMBER

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

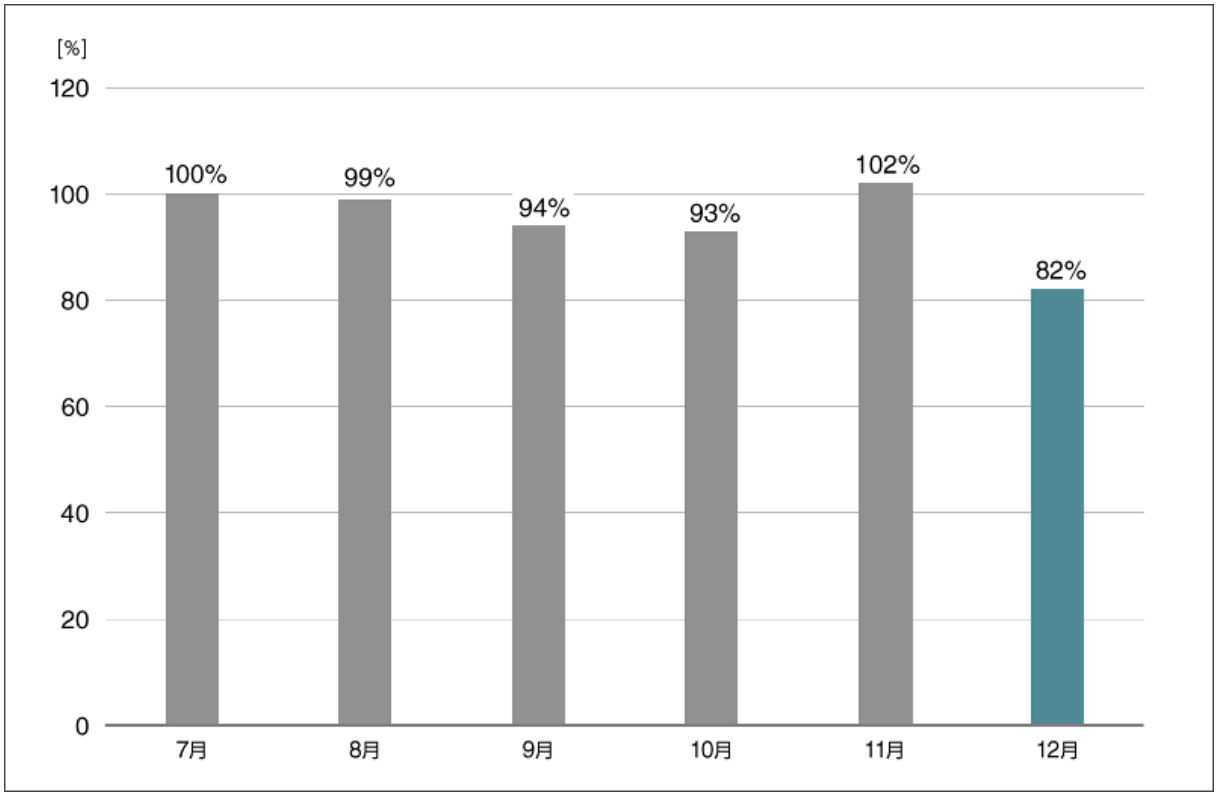
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 12 月マルウェア検出状況

2024 年 12 月（12 月 1 日～12 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 7 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 12 月の国内マルウェア検出数は、2024 年 11 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 12 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	21.9%	アドウェア
2	JS/Adware.Agent	16.4%	アドウェア
3	HTML/Phishing.Agent	14.1%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	6.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	HTML/FakeCaptcha	4.1%	偽の CAPTCHA を表示させる HTML ファイル
6	JS/Agent	2.3%	不正な JavaScript の汎用検出名
7	HTML/Phishing.Gen	2.0%	詐欺を目的とした不正な HTML ファイル
8	HTML/Nomani	1.5%	詐欺を目的とした不正な HTML ファイル
9	HTML/Phishing.Adobe	0.9%	Adobe 社のサービスを騙った不正な HTML ファイル
10	JS/Adware.Sculinst	0.8%	アドウェア

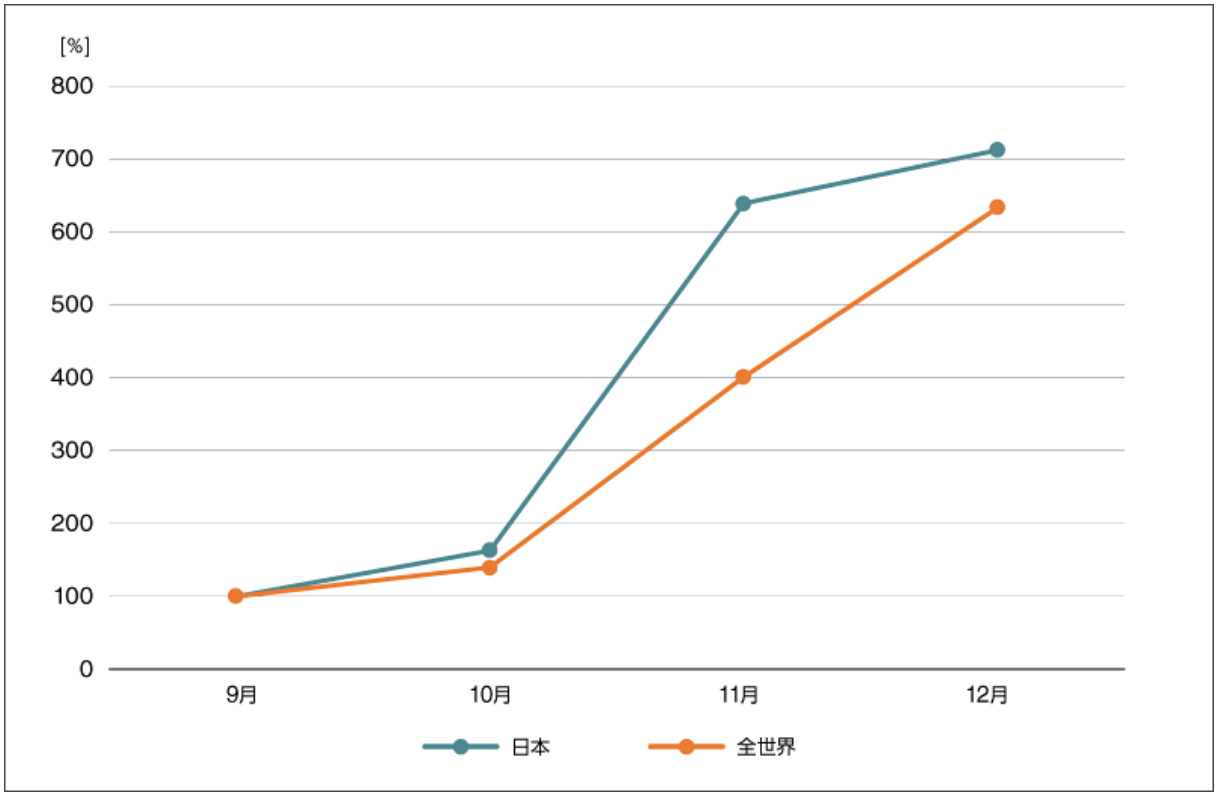
*2 本表には PUA を含めていません。

12 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 Web サイト閲覧時に実行されるアドウェアです。感染すると、アドウェアサイトへのリダイレクト、アドウェアコンテンツの配布や Web ブラウザーの拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。

Web ブラウジング中に遭遇する脅威の急増

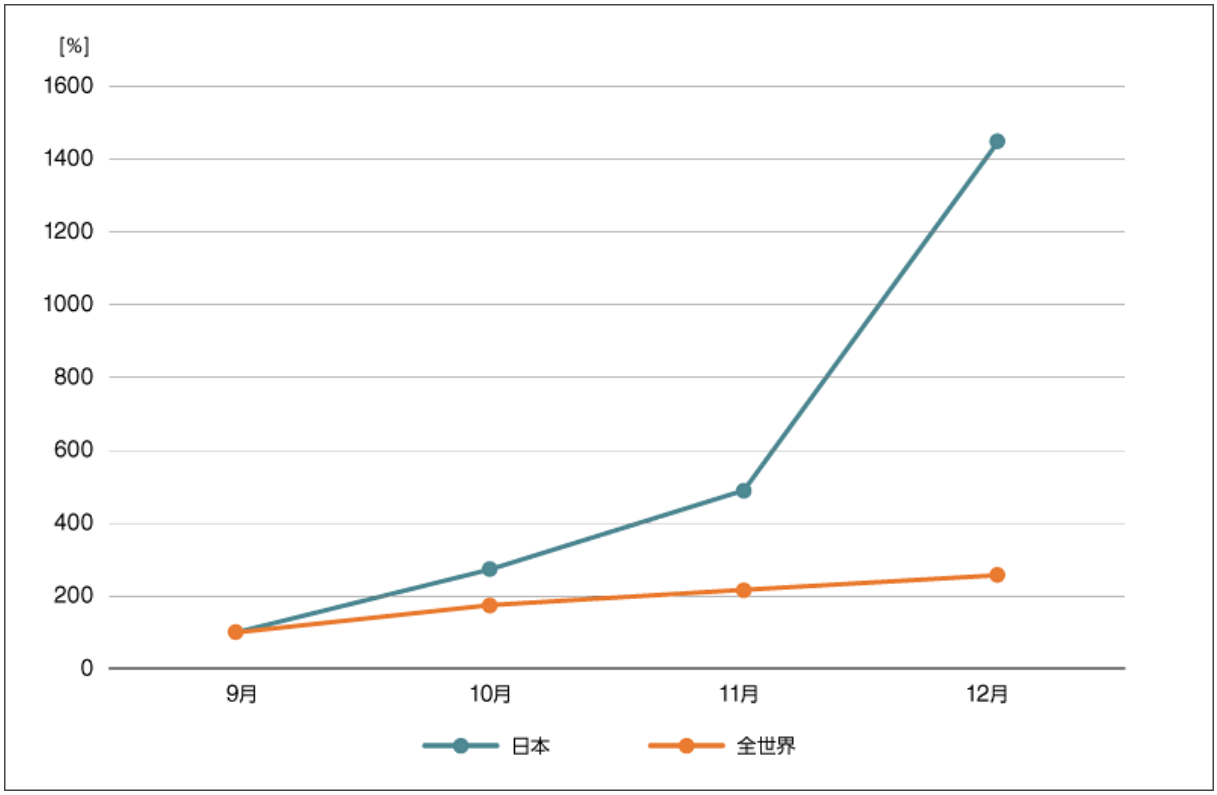
2024 年 12 月の国内マルウェア検出数では、HTML/FakeCaptcha や HTML/Nomani といった Web ブラウジング中に遭遇する脅威が上位にランクインしました。
HTML/FakeCaptcha は偽の CAPTCHA（画像を用いた認証）を表示し、利用者にクリックや情報入力などを促す不正な HTML ファイルを検出した際に表示される検出名です。
また、HTML/Nomani は生成 AI を用いたディープフェイクビデオや企業ブランドの投稿を使用した詐欺を含む悪意ある HTML ファイルを検出した際に使用される検出名です。
これらの脅威は 2024 年上半期の TOP10 には一度も入ったことがないため、2024 年下半期から現れた比較的新しい脅威と捉えることができます。

HTML/FakeCaptcha の 2024 年 9 月から 12 月にかけての検出数の推移を以下に示します。



HTML/FakeCaptcha 検出数の推移（国内･全世界）
（2024 年 9 月の日本、全世界での検出数を 100%として比較）

同様に、HTML/Nomani の 2024 年 9 月から 12 月にかけての検出数の推移を以下に示します。



HTML/Nomani 検出数の推移（国内･全世界）
（2024 年 9 月の日本、全世界での検出数を 100%として比較）

これらのグラフから、HTML/FakeCaptcha と HTML/Nomani は以下のような共通点を持つことが確認できます。

- 12 月の検出数が国内、全世界ともに 9 月の検出数の 2 倍以上になっている
- 全世界の伸び幅と比較して、国内の伸び幅の方がより大きい

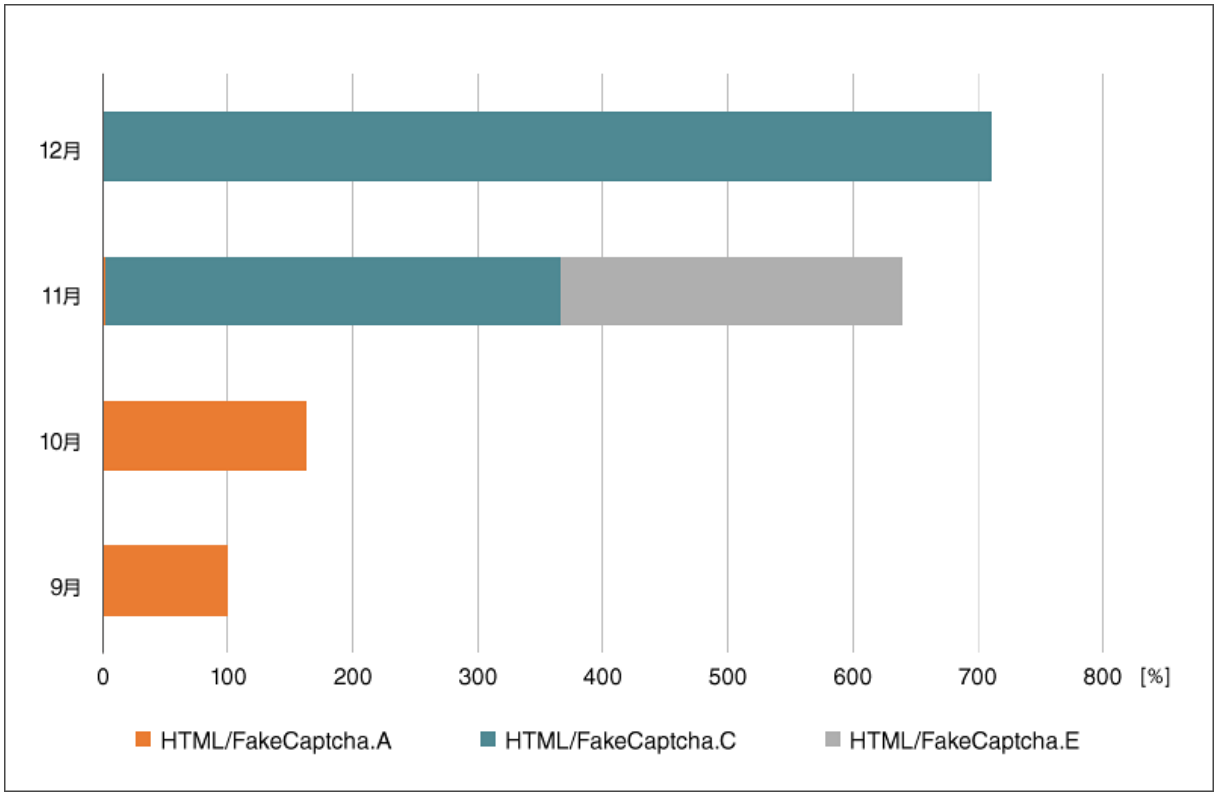
つまり、全世界的に Web ブラウジング中に遭遇する脅威は増加しており、特に日本国内をターゲットとしたものが著しく増加していると読み取ることができます。

LummaStealer への感染を狙う HTML/FakeCaptcha

HTML/FakeCaptcha として検出される HTML ファイルは、いくつかの亜種に分類することができます。2024 年 9 月から 2024 年 12 月の期間で検出された亜種は、以下の 3 種類でした。

- HTML/FakeCaptcha.A
- HTML/FakeCaptcha.C
- HTML/FakeCaptcha.E

以下のグラフに日本国内での HTML/FakeCaptcha の亜種ごとの検出数推移を示します。2024 年 11 月は HTML/FakeCaptcha 全体の約半数で留まっていた HTML/FakeCaptcha.C の検出数が、2024 年 12 月には 2 倍程度に増加し HTML/FakeCaptcha のほぼ全体を占めるようになっています。



HTML/FakeCaptcha 検出数の推移と亜種ごとの内訳（国内）
（2024 年 9 月の総検出数を 100%として比較）

HTML/FakeCaptcha.C は、LummaStealer の感染を狙うキャンペーンに悪用されていたことが報告されています。

LummaStealer は 2022 年に発見された比較的新しい情報窃取型マルウェアです。MaaS としてさまざまな攻撃者に悪用されているため、定期的に被害報告が上がっています。LummaStealer に感染した場合、仮想通貨ウォレットや Web ブラウザーに保存した各種認証情報の窃取などさまざまな被害に遭う可能性があります。LummaStealer が検出された際に表示される検出名である Win32/Spy.LummaStealer は、2024 年 11 月の国内マルウェア検出数で第 6 位に入りました。

Web ブラウジング中に遭遇する脅威といえば、フィッシングなど利用者の不注意を利用してさまざまな情報を不正に収集するものが代表的です。「ただブラウジングしているだけでは、マルウェアに感染することはない」と考えている方も多いと思われます。
HTML/FakeCaptcha.C はそうした意識の隙を狙い、LummaStealer という情報窃取型マルウェアへの感染を試みます。このようなマルウェアの感染手法は、仕組みを理解することで警戒・対策が容易になります。
ここでは Web ブラウジング中に遭遇する脅威の一例として、HTML/FakeCaptcha.C がどのように LummaStealer への感染を行っているかを解説し、遭遇時の対処方法をまとめます。

HTML/FakeCaptcha.C の動作

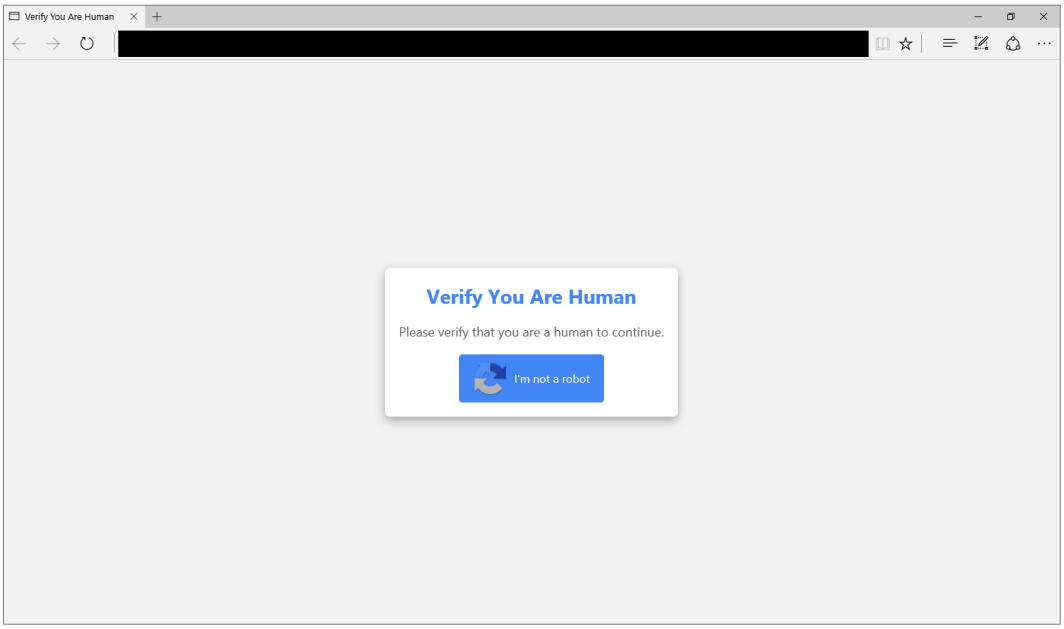
HTML/FakeCaptcha.C の感染動作は次の 2 段階に大きく分けることができます。

1. Web ブラウザー上に偽の CAPTCHA が表示される
2. 利用者が指示に従い、表示されたコマンドを入力する

それぞれの段階について具体的な動作を紹介します。

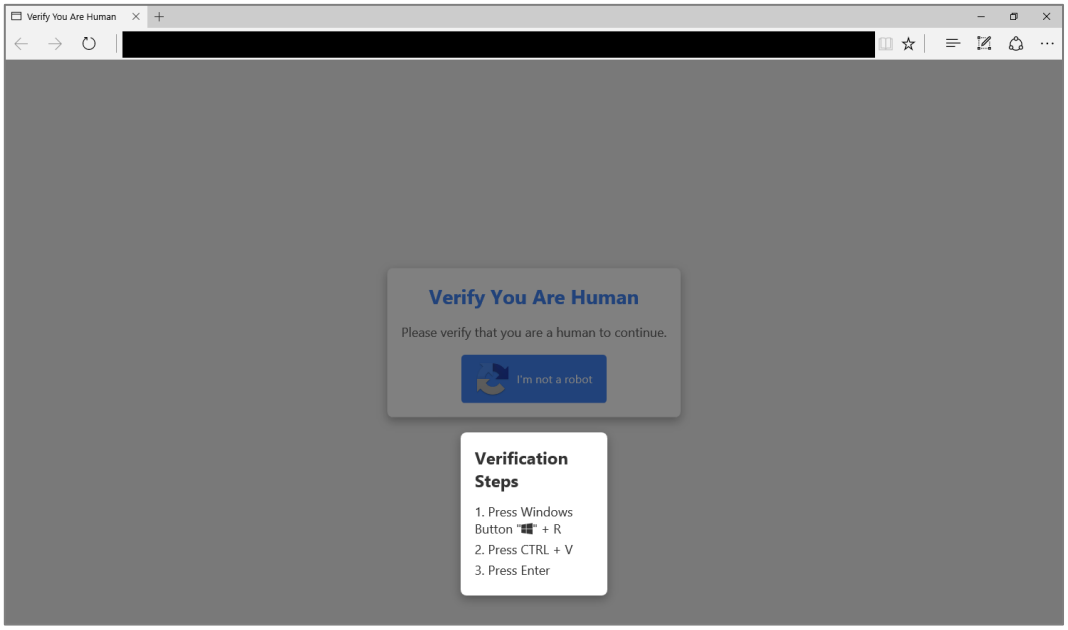
1. Web ブラウザー上に偽の CAPTCHA が表示される

前述のように、HTML/FakeCaptcha は偽の CAPTCHA を表示し、利用者にクリックや情報入力などを促す不正な HTML ファイルです。HTML/FakeCaptcha.C の場合は、次のような画像が Web ブラウザー上に表示されます。



Web ブラウザー上に表示される偽の CAPTCHA①

中央にある「I'm not a robot」ボタンを押すと、次のように検証のための指示が表示されます。



Web ブラウザー上に表示される偽の CAPTCHA②

この CAPTCHA 画像は、主に次のような Web サイトを開いた際に表示されます。

- 正規の Web サイトの閲覧時に表示される広告から誘導される Web サイト
- 非公式なソフトウェアのダウンロードリンクから誘導される Web サイト

どちらも利用者が本来求めている情報にたどり着く前のワンクッションとしてこの CAPTCHA 画像が表示されるため、CAPTCHA の指示に従うことで求めている情報が得られると錯覚してしまう構造になっています。

2. 利用者が指示に従い、表示されたコマンドを入力する

偽の CAPTCHA 画像は、利用者にキーボードで以下の入力を行うよう求めています。

A) 「Windows」キー ＋「R」キー
B) 「Ctrl」キー ＋「V」キー
C) 「Enter」キー

偽の CAPTCHA 画像の指示に従い A から C の入力が順番に行われた場合、攻撃者の用意した任意のコマンドが利用者の PC で実行されます。
具体的には、それぞれの入力で次のような処理が行われます。

A) 「Windows」キー ＋「R」キー
→「ファイル名を指定して実行」のウィンドウを呼び出す
B) 「Ctrl」キー ＋「V」キー
→「ファイル名を指定して実行」のウィンドウに攻撃者が用意した文字列をペーストする
C) 「Enter」キー
→ ペーストされた文字列で指定されたプログラムを実行する

攻撃者が用意した文字列として、外部 URL からプログラムをダウンロードして実行する PowerShell スクリプトや更なる HTML アプリケーションへリダイレクトする mshta コマンドなど複数のパターンを確認しています。これらの文字列は利用者が「I'm not a robot」ボタンをクリックしたタイミングで、端末のクリップボードへ自動的にコピーされます。

A から C の入力を利用者に自発的に行わせることにより、上に挙げた PowerShell スクリプトやコマンドが実行され、最終的に外部のサーバーから LummaStealer などのマルウェアがダウンロードされます。

偽の CAPTCHA に遭遇した際に取るべき対処

HTML/FakeCaptcha.C が通信を行う URL には、2024 年 12 月現在でもアクセス可能なものが含まれていることを確認しています。この節では、こうした不審な CAPTCHA に遭遇した際にどう対処すべきかをまとめます。

第一に、信頼がおけないサイトの指示には従わないようにしてください。また、信頼がおけるサイトであっても、精巧に似せて作られたフィッシングサイトである可能性があります。Web ブラウザーのブックマーク経由でアクセスするなど、偽サイトに誘導されない工夫をすることで安全性が高まります。
HTML/FakeCaptcha.C であるか否かは、「I'm not a robot」ボタンを押した後にメモ帳などにペーストを行うことで判断が可能です。身に覚えのない文字列が貼り付けられた際は、HTML/FakeCaptcha.C である可能性が極めて高いです。

第二に、指示に従ってしまった場合の対処について紹介します。
この場合は、マルウェアが PC 内に潜伏している可能性が高いです。ネットワークから切り離した上で、セキュリティソフトによるフルスキャンを実施してください。その後は、必要な情報を控えた上で PC を初期化する、専門家に相談するといった対応を取ることを推奨します。
また、クレジットカード情報や ID、パスワードなどの認証情報が PC 内に保存されていた場合は、それぞれ停止・変更の対応を行ってください。

まとめ

HTML/FakeCaptcha や HTML/Nomani といった Web ブラウジング中に遭遇する脅威について 2024 年下半期の検出状況を紹介し、一例として HTML/FakeCaptcha.C の仕組みを取り上げました。いくつかのデータにも表れているように、Web ブラウジング中にこうした脅威に遭遇する可能性は高いです。どういった脅威が存在しているかを把握し、仕組みを知ることで、脅威がもたらす危険を適切に回避できるよう準備しておく必要があります。
HTML/FakeCaptcha.C のような脅威に遭遇した場合にどうするのか、指示に従ってしまった場合にどうするのか、対処法について一度シミュレーションしてみてください。

■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

●ESET Threat Report H2 2024 | welivesecurity
https://www.welivesecurity.com/en/eset-research/eset-threat-report-h2-2024/
●Behind the CAPTCHA: A Clever Gateway of Malware | McAfee
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/
●2024 年 11 月 マルウェアレポート | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2411.html

Canon

キヤノンマーケティングジャパン株式会社