2024年
7·8月
JULY/AUGUST

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

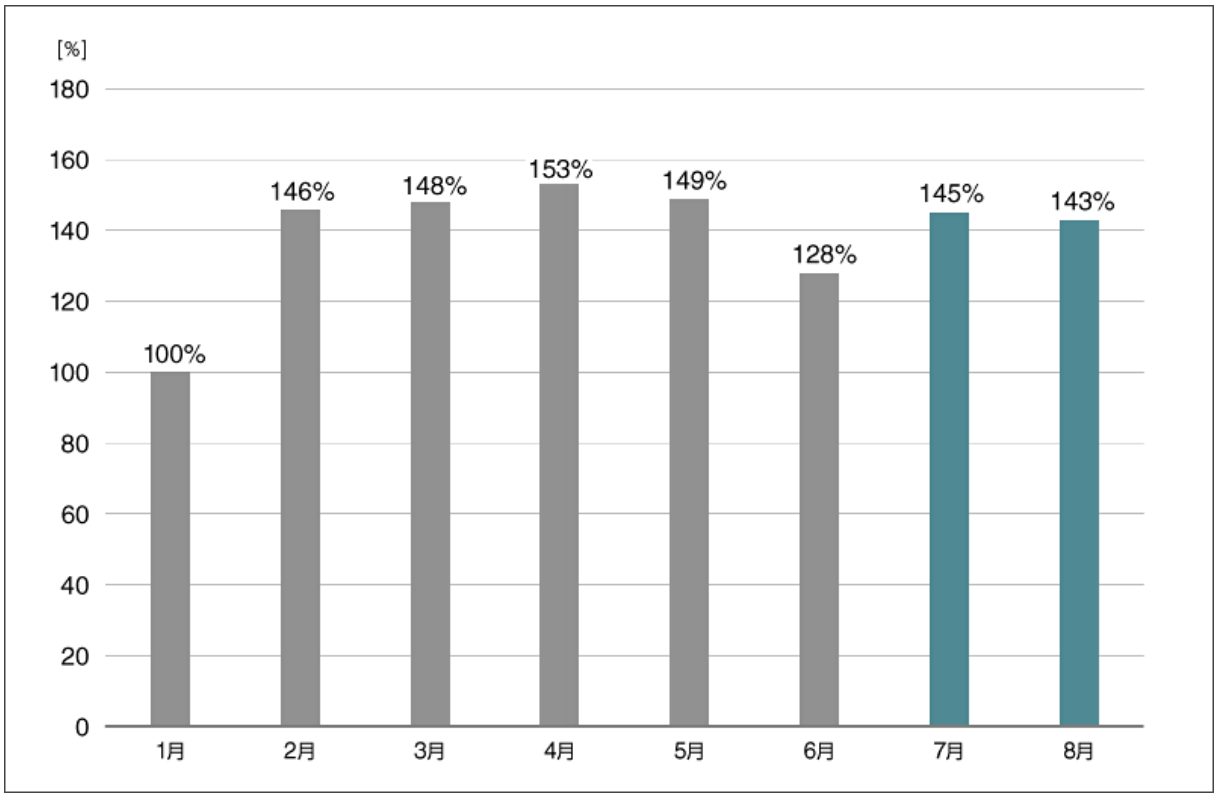
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 7 月･8 月マルウェア検出状況

2024 年 7 月（7 月 1 日～7 月 31 日）と 8 月（8 月 1 日～8 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 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。

2024 年 7 月と 8 月の国内マルウェア検出数は、2024 年 6 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（2024 年 7 月･8 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	19.9%	アドウェア
2	JS/Adware.Agent	18.8%	アドウェア
3	HTML/Phishing.Agent	15.8%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	11.0%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	1.9%	不正な JavaScript の汎用検出名
6	HTML/Fraud	1.4%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	JS/Adware.Sculinst	1.0%	アドウェア
8	HTML/Phishing.Gen	0.8%	フィッシングサイトのリンクが埋め込まれた HTML ファイル
9	JS/Danger.ScriptAttachment	0.7%	メールに添付された不正な JavaScript
10	DOC/TrojanDownloader.Agent	0.7%	ダウンローダー

国内マルウェア検出数*2 上位（2024 年 7 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	20.3%	アドウェア
2	JS/Adware.Agent	19.8%	アドウェア
3	HTML/Phishing.Agent	12.7%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	11.1%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	2.2%	不正な JavaScript の汎用検出名
6	HTML/Fraud	1.3%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	JS/Adware.Sculinst	1.1%	アドウェア
8	JS/Danger	1.1%	メールに添付された不正な JavaScript
9	Win32/Exploit.CVE-2017-11882	1.0%	脆弱性を悪用するマルウェア
10	Win64/Riskware.PEMalform	0.8%	ブラウザハイジャッカー

国内マルウェア検出数*2 上位（2024 年 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	19.4%	アドウェア
2	HTML/Phishing.Agent	18.9%	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	DOC/Fraud	11.0%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	1.6%	アドウェア
6	HTML/Fraud	1.5%	不正な JavaScript の汎用検出名
7	Win32/Formbook	1.0%	ダウンローダー
8	HTML/Phishing.Gen	0.9%	詐欺を目的とした不正な HTML ファイル
9	JS/Adware.Sculinst	0.9%	詐欺サイトのリンクが埋め込まれた HTML ファイル
10	DOC/TrojanDownloader.Agent	0.8%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

7 月と 8 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の検出名です。感染すると、アドウェアが仕組まれた Web 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ブラウザー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。

・無効化された Internet Explorer を悪用する感染の手口

無効化された Internet Explorer を悪用しマルウェアをダウンロードさせる感染の手口が発見されました。この手口を使用するマルウェアとしては、情報窃取型マルウェアである Atlantida Stealer が確認されています。

Internet Explorer は Windows 10 までの Windows OS に標準で搭載されていた Web ブラウザーです。Internet Explorer のサポートは 2022 年 6 月 16 日をもって終了し、現在は Microsoft Edge に置き換えられています。[1)] 互換性の維持のため、現行の Windows 10 や Windows 11 には Internet Explorer が搭載されていますが、デフォルトでは無効化されており使用することはできません。Internet Explorer を起動しようとすると、代わりに Microsoft Edge が立ち上がる仕組みになっています。
Internet Explorer は構造上 Windows OS との結びつきが強かったことやシェアが高かったことから攻撃者に狙われやすいブラウザーでした。開発元である Microsoft も Internet Explorer をデフォルトのブラウザーとして使用することの危険性に言及したことがあります。[2)]
そうした背景を踏まえて、Internet Explorer のサポート終了と Microsoft Edge への置き換えが行われました。

前述のように、通常の手段では Internet Explorer を使用することはできません。しかし、今回紹介する手口では Windows の MSHTML プラットフォームに存在する脆弱性（CVE-2024-38112）を悪用することで、Internet Explorer を起動します。[3)] この脆弱性は 2024 年 7 月の Microsoft セキュリティアップデートによって修正済みです。[4)]

この脆弱性を利用した手口は、以下の 3 点から警戒の必要性が高いものだと考えられます。

- セキュリティアップデートが公開されてから日が浅いこと
- システムを悪用し、ユーザーを誤認させる機能が盛り込まれていること
- 過去にも MSHTML プロトコルハンドラーの類似の脆弱性が悪用されており、今後似た手口が攻撃に用いられる可能性があること

そのため、2024 年 7 月･8 月マルウェアレポートでは、この感染の手口について紹介し、類似の攻撃を受けないためにどのような対策をすべきかについて紹介します。

･Internet Explorer が悪用される流れ

Internet Explorer を悪用する感染の手口について紹介します。

今回紹介する感染の手口では、多くのファイルを経由して被害 PC にマルウェアがダウンロードされます。Atlantida Stealer に感染するまでの流れを以下に示します。

① PDF ファイルに偽装された URL ショートカットファイルを実行する
② URL ショートカットファイルが HTML ファイルにアクセスする
③ HTML ファイルが HTA ファイルにリダイレクトする
④ HTA ファイルが PowerShell スクリプトをダウンロードし実行する
⑤ PowerShell スクリプトが.NET 実行ファイルをダウンロードし実行する
⑥ .NET 実行ファイルが Atlantida Stealer を展開し実行する

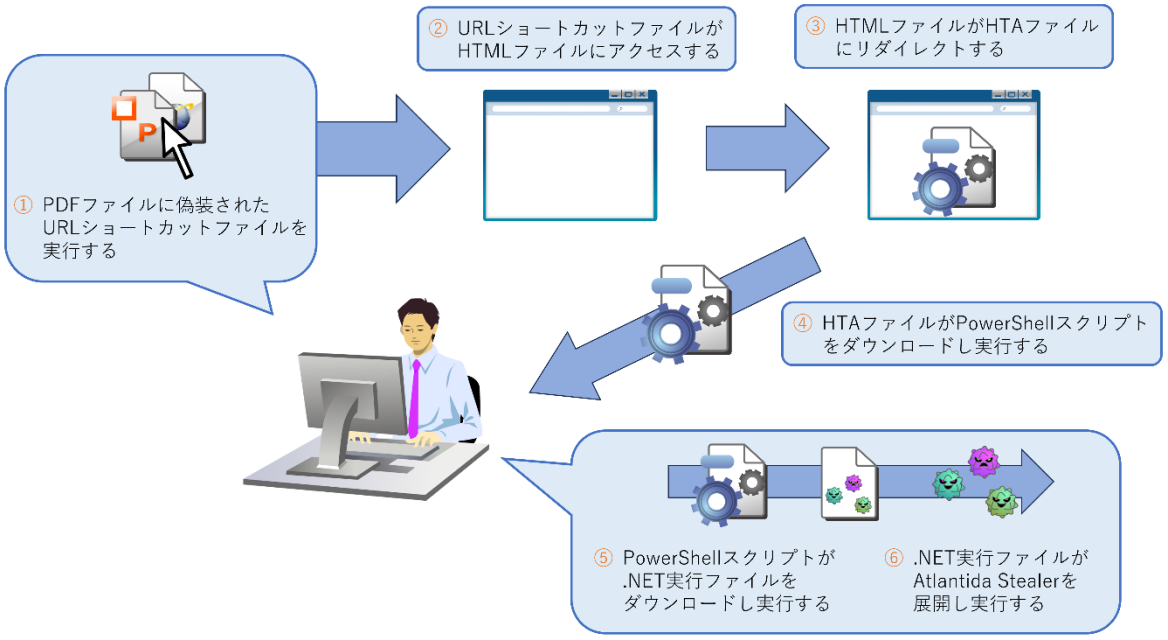


図 1 Atlantida Stealer に感染する流れ

① PDF ファイルに偽装された URL ショートカットファイルを実行する

マルウェアへの感染のきっかけとなるのは、①の URL ショートカットファイルです。

図 2 PDF ファイルに偽装された URL ショートカットファイル

URL ショートカットファイルとは、実行すると既定のブラウザーで指定の Web ページを開くことができるファイルです。上の画像でも拡張子が.url になっていることが確認できます。
この URL ショートカットファイルの特徴的な点として、アイコンが PDF に偽装されていることが挙げられます。拡張子が表示されていない環境でこのファイルを見た場合、ユーザーからは PDF ファイルとの見分けがつきません。なお、.url や.lnk などの拡張子を表示するためにはレジストリの編集が必要です。

また、この URL ショートカットファイルは、ファイル中の URL の指定方法が一般的な URL ショートカットファイルとは異なっています。

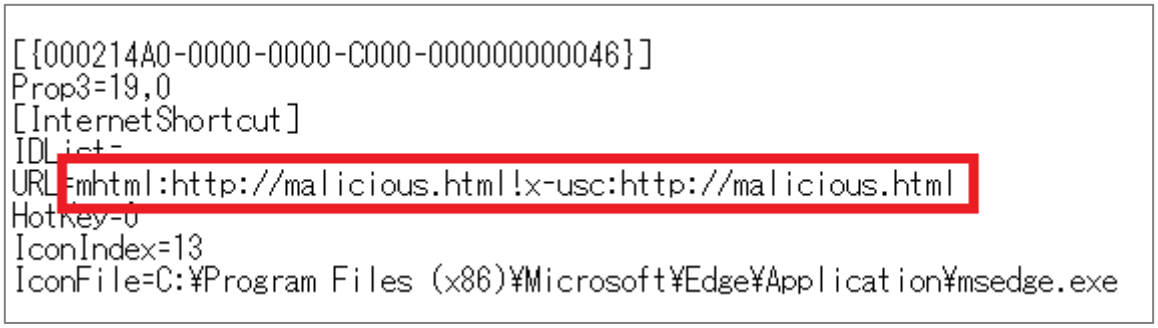


図 3 Internet Explorer を悪用する URL ショートカットファイル

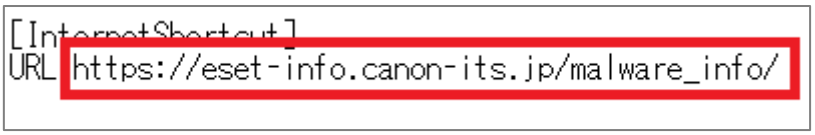


図 4 通常の URL ショートカットファイル

なお、図 3 中の URL は実際の検体の通信先とは異なります。

この URL ショートカットファイルは MSHTML プロトコルハンドラーと x-usc ディレクティブを組み合わせることで、CVE-2024-38112 を悪用しています。
MSHTML は Internet Explorer で動作するレンダリングエンジンです。また、x-usc ディレクティブは URL をエンコードまたは書き換える際に使用されるプレフィックスです。
MSHTML を用いて URL を指定すると Internet Explorer が起動する仕様と x-usc ディレクティブによる URL のデコード、そして CVE-2024-38112 が組み合わさった結果、既定のブラウザーではなく Internet Explorer を用いて指定された Web ページが開かれます。

② URL ショートカットファイルが HTML ファイルにアクセスする

①の URL ショートカットファイルは、攻撃者が用意したサーバー上の HTML ファイルにアクセスします。この HTML ファイルは JS/Redirector.PIY という検出名で検出されるマルウェアであり、別の悪意ある URL にリダイレクトする JavaScript が埋め込まれています。

③ HTML ファイルが HTA ファイルにリダイレクトする

②の HTML ファイルは、同じく攻撃者が用意したサーバー上の HTA ファイルにリダイレクトします。この HTA ファイルは VBS/TrojanDownloader.Agent.AAQA という検出名で検出されるマルウェアです。
HTA とは Html Application の略称であり、Web ブラウザーを利用して Windows アプリケーションを実現するための仕組みです。セキュリティの制約が少なく、ローカルのファイルやレジストリにアクセスすることができます。

この HTA ファイルにアクセスした場合、ユーザーの画面には図 5 が表示されます。

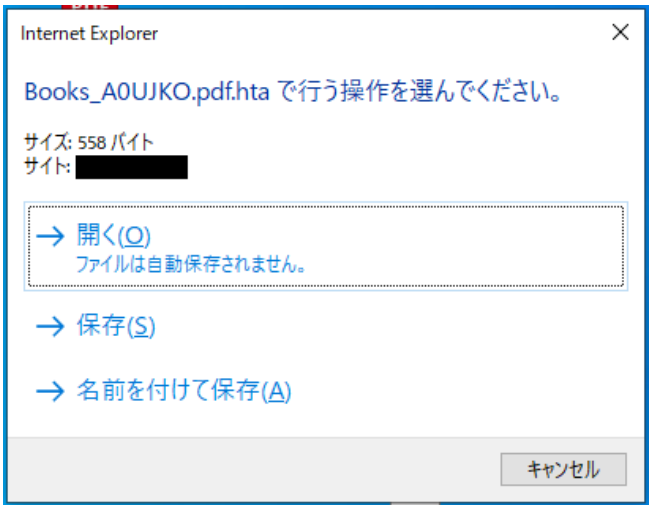


図 5 HTA ファイルの実行許可を求める表示（Internet Explorer）

この画面は一見 PDF を開く許可をユーザーに求めているように見えます。しかし、実際には HTA ファイルの実行許可を求めています。
この HTA ファイルには VBScript が含まれており、実行を許可すると④の PowerShell スクリプトをダウンロードして実行します。

図 5 に示した HTA ファイルの実行許可を求める表示は非常にユーザーに誤解を招きやすいものとなっています。この表示形式は Internet Explorer 特有のものであり、同様の処理を Edge で行おうとした場合は以下の図のように表示されます。

図 6　HTA ファイルの実行許可を求める表示（Edge）

④　HTA ファイルが PowerShell スクリプトをダウンロードし実行する

HTA ファイルは PowerShell スクリプトが書かれたテキストファイルをダウンロードし、その PowerShell スクリプトを実行します。この時、ユーザーに許可が求められることはありません。また、PowerShell スクリプトの実行がユーザーに気付かれないようウィンドウを隠す機能も持っています。

⑤　PowerShell スクリプトが.NET 実行ファイルをダウンロードし実行する

PowerShell スクリプトによって、.NET 実行ファイルのダウンロードと実行が行われます。

⑥　.NET 実行ファイルが Atlantida Stealer を展開し実行する

.NET 実行ファイルは RegAsm.exe プロセスを介して Atlantida Stealer を展開して実行します。
Atlantida Stealer は被害 PC 内のシステム情報や機密情報を収集すると、攻撃者のサーバーに送信してしまいます。

･対策

今回紹介した感染の手口に対する対策を紹介します。

- **ファイルの拡張子を表示し、実行前に確認する**

今回紹介した検体は、URL ショートカットファイルを PDF ファイルに偽装していました。ファイルのアイコンは偽装が

容易であり、多くのマルウェアが PDF など無害に見えるファイルに偽装されています。ファイルの拡張子を表示しない設定になっている環境では、注意深くプロパティなどを確認しないとファイル形式を見抜くことが困難です。拡張子を表示できる設定にして、普段から実行するファイルの拡張子に意識を向ける習慣をつけるようにしてください。
文字の流れを右から左の向きに書き換える制御記号 Right-to-Left Override を用いた拡張子の偽装など、拡張子を確認しているだけでは騙されてしまうファイル形式偽装の手法も存在します。あくまでもこれらは判断基準の 1 つとして、実行前に「本当にこのファイルを実行する必要があるのか」を考えるようにしてください。

- **2024 年 7 月のセキュリティアップデートを適用する**

今回紹介した手法は脆弱性（CVE-2024-38112）を悪用しています。この脆弱性は 2024 年 7 月の Microsft セキュリティアップデートで修正されました。セキュリティアップデートを適用することで URL ショートカットファイルから Internet Explorer が実行されることはなくなるため、今回紹介した手法でのマルウェアへの感染を防ぐことができます。
関連して、Windows 10 のサポート終了が約 1 年後の 2025 年 10 月 14 日に迫ってきています。サポートの終了後はこうしたセキュリティアップデートが行われなくなります。また、サポート終了後の脆弱な Windows 10 を使用し続けるユーザーを狙った攻撃キャンペーンが行われる可能性もあります。そのため、計画的に Windows 11 への切り替えを行うことを推奨します。

・まとめ

本レポートでは、無効化された Internet Explorer を悪用する感染の手口について紹介しました。また、こうした手口によるマルウェア感染を防ぐために、注意すべき点や対策についても紹介しました。
Internet Explorer に限らず、サポートが終了したソフトウェアにはリスクがあります。自分が利用している環境を把握し、以下の 3 点に気を配るようにしてください。

- サポートが終了しているソフトウェアが端末内にインストールされていないか
- 不要なソフトウェアが端末内にインストールされていないか
- サポートが行われているソフトウェアであっても、 OS やソフトウェアを最新の状態に更新しているか

こうした日々の精査で、マルウェア感染の可能性を大きく引き下げることができます。
また、本レポートでは、マルウェアがユーザーを騙す手口についてもいくつか紹介しています。こうした偽装が施されたマルウェアを見抜くのは非常に困難です。セキュリティソフトの導入などの事前の対策で、マルウェアを可能な限り駆除する体制を整えてください。その上で、信頼のおけない出所のファイルについては、実行の可否を慎重に判断する必要があります。

■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

1）Internet Explorer のダウンロード | Microsoft
https://support.microsoft.com/ja-jp/windows/internet-explorer-%E3%81%AE%E3%83%80%E3%82%A6%E3%83%B3%E3%83%AD%E3%83%BC%E3%83%89-d49e1f0d-571c-9a7b-d97e-be248806ca70

2）The perils of using Internet Explorer as your default browser | Microsoft
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-perils-of-using-internet-explorer-as-your-default-browser/ba-p/331732

3）攻撃グループ Void Banshee、ゾンビ化した Internet Explorer の脆弱性「CVE-2024-38112」を悪用して Windows ユーザにゼロデイ攻撃を仕掛ける | Trend Micro
https://www.trendmicro.com/ja_jp/research/24/g/CVE-2024-38112-void-banshee.html

4）Windows MSHTML Platform Spoofing Vulnerability | Microsoft
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

5）Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起 | JPCERT/CC
https://www.jpcert.or.jp/at/2021/at210038.html

Canon

キヤノンマーケティングジャパン株式会社