2022年
5月
MAY

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

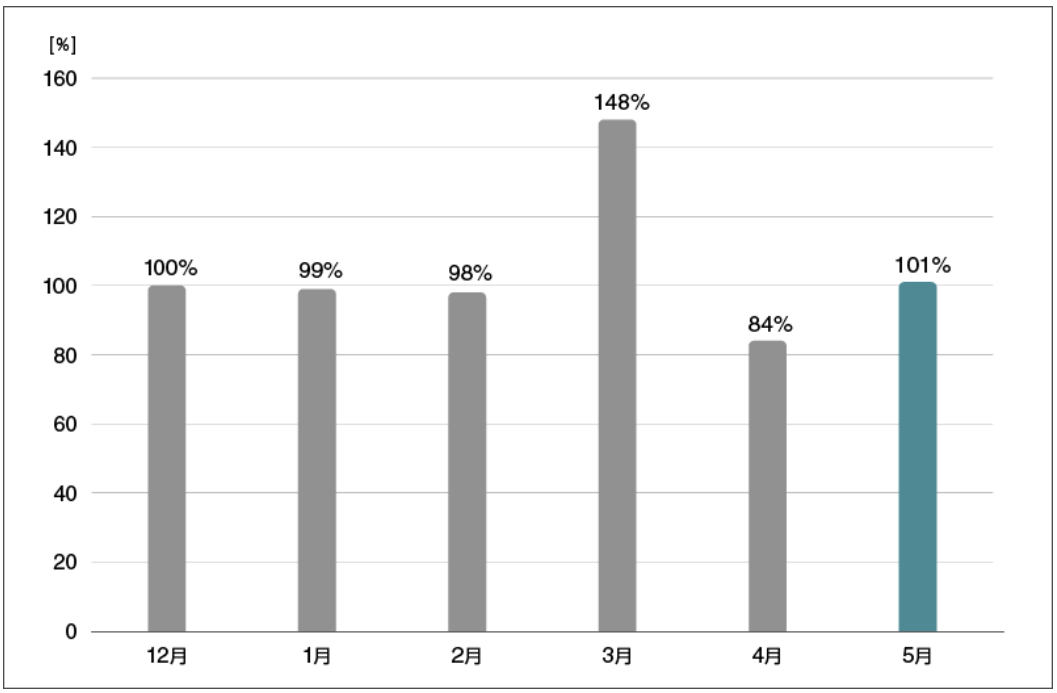
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2022 年 5 月マルウェア検出状況

2022 年 5 月（5 月 1 日～5 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

(2021 年 12 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。

2022 年 5 月の国内マルウェア検出数は、2022 年 4 月と比較して増加しました。
増加要因として、 LNK/TrojanDownloader.Agent の検出数が大きく増加したことが挙げられます。LNK/TrojanDownloader.Agent は、ショートカットファイル形式（LNK 形式）のダウンローダーです。ファイルを開くことによって、スクリプトが実行され、他のマルウェアがダウンロードされます。
2022 年 4 月では、Emotet をダウンロードするものを多数検出していました。詳細については、2022 年 4 月マルウェアレポートでご紹介しています。

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（2022 年 5 月）

順位	マルウェア	割合	種別
1	JS/Adware.TerraClicks	8.3%	アドウェア
2	HTML/Pharmacy	7.6%	薬局を装った詐欺メール
3	JS/Adware.Sculinst	7.4%	アドウェア
4	JS/Adware.Agent	6.4%	アドウェア
5	LNK/TrojanDownloader.Agent	5.0%	ダウンローダー
6	JS/Packed.Agent	4.9%	パックされた不正な JavaScript の汎用検出名
7	HTML/FakeAlert	4.7%	偽の警告文を表示させる HTML ファイル
8	HTML/Phishing.Agent	4.3%	メールに添付された不正な HTML ファイル
9	DOC/TrojanDownloader.Agent	3.3%	ダウンローダー
10	PDF/Phishing	2.6%	フィッシング目的の PDF ファイル

*2 本表には PUA を含めていません。

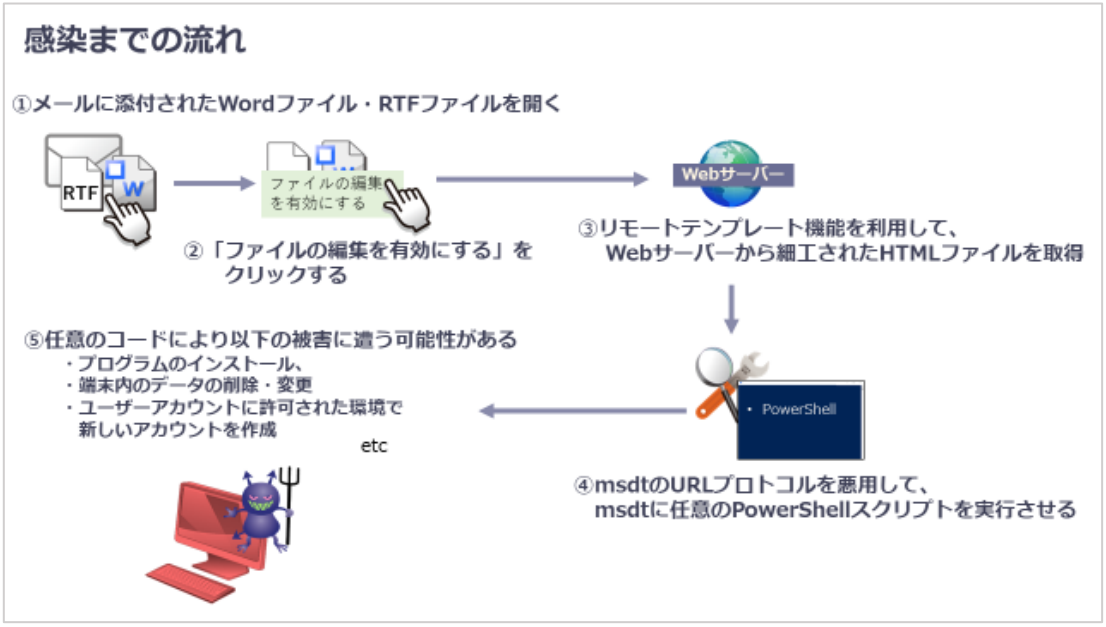
5 月に国内で最も多く検出されたマルウェアは、JS/Adware.TerraClicks でした。
JS/Adware.TerraClicks は、Web サイト閲覧時に実行されるアドウェアです。感染すると、アドウェアサイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。

5 月 30 日に Windows サポート診断ツール（Microsoft Support Diagnostic Tool：MSDT）に関する脆弱性 CVE-2022-30190 が公開されました。
この脆弱性は「Follina」と呼ばれており、Word などの呼び出しアプリケーションから MSDT URL プロトコルを使用して MSDT が呼び出されると、リモートでコードが実行されるという脆弱性です。本脆弱性は、以下の OS とバージョンが対象となります。詳細な情報については、Microsoft のセキュリティアップデートガイドに掲載されています。

対象となる Windows OS バージョン

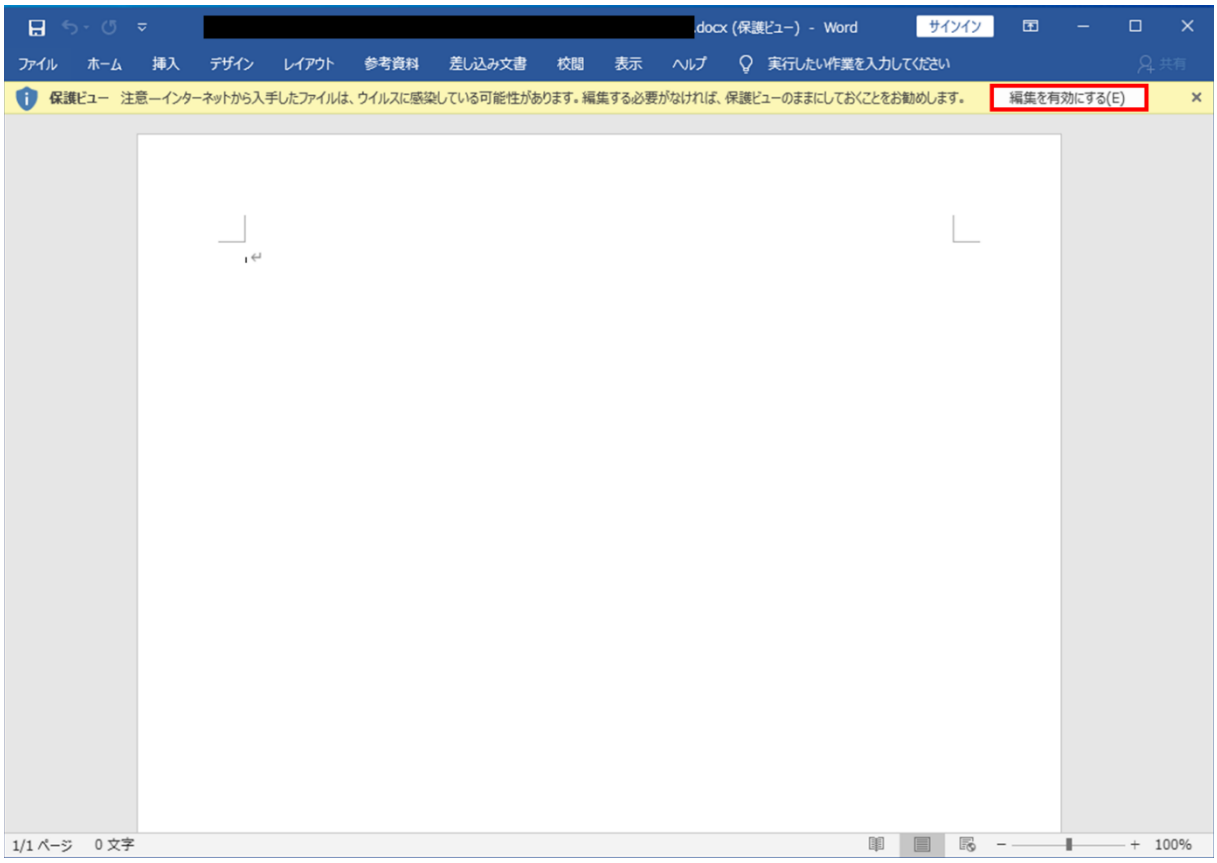
Windows	Windows server
Windows 11	Windows Server version 20H2(Server Core Installation)
Windows 10	Windows Server 2022
Windows 8.1/RT8.1	Windows Server 2019
Windows 7	Windows Server 2016
	Windows Server 2012/2012 R2
	Windows Server 2008/2008 R2

本脆弱性を悪用するマルウェアによって、任意のコードが実行されるまでの流れは以下の通りです。



感染までの流れ

本脆弱性を悪用した Word ファイルを開いた場合でも、保護ビューが機能していると任意のコードの実行はありません。ユーザーが「ファイルの編集を有効にする」をクリックし保護ビューを解除することで、任意のコードを実行される恐れがあります。

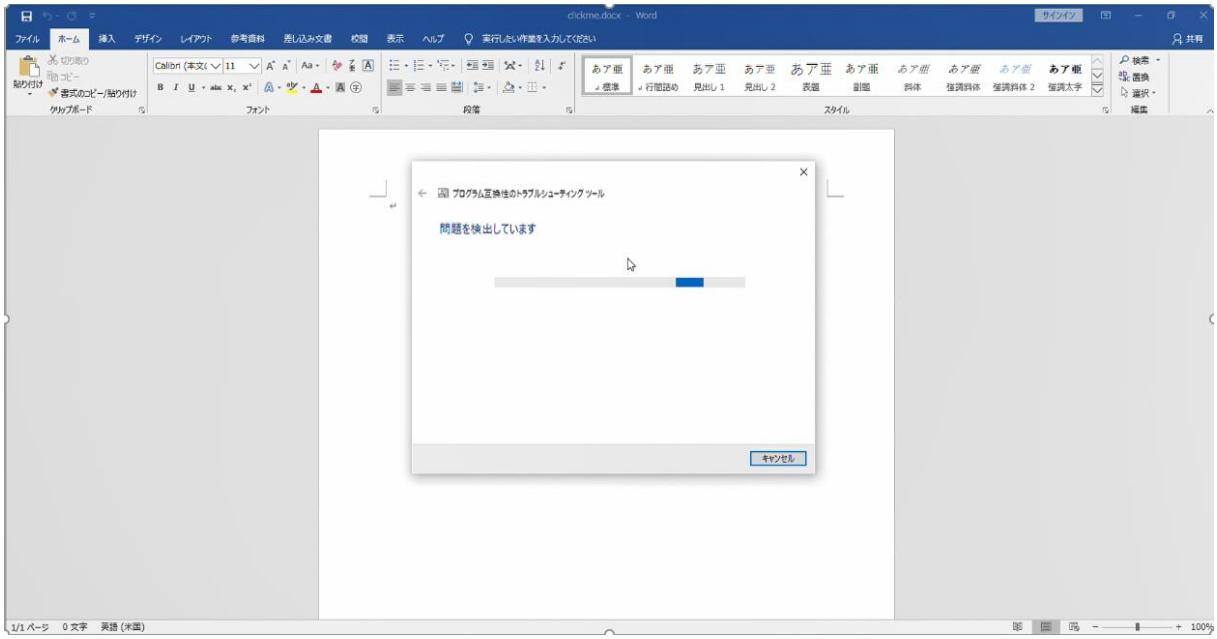


本脆弱性を悪用するファイルを開いた際の表示画面の例

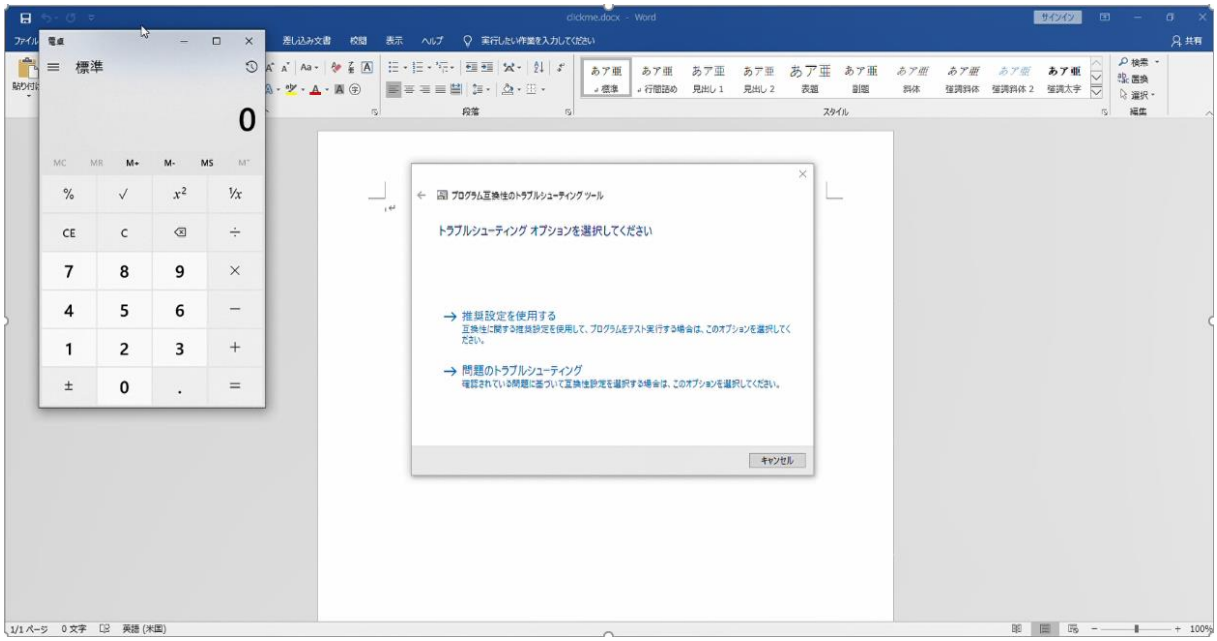
また、この手法ではマクロを有効化する必要がないため、Word 形式だけでなくリッチテキストファイル形式（RTF 形式）としても悪用されています。RTF 形式だと、保護ビューで開けないため、ファイルを開くだけで任意のコードが実行される恐れがあります。

本脆弱性を悪用して任意のコードが実行される様子が以下の通りです。今回は PoC を用いて、計算機アプリを起動させています。

Word を起動時にリモートテンプレート機能によってサーバーへアクセスしている様子



Windows サポート診断ツールが起動し、任意のコードが実行されている様子



任意のコードが実行された結果、計算機アプリが起動している様子

Word ファイルを起動し、リモートテンプレート機能を利用して、HTML ファイルを取得しています。次に、取得した HTML ファイルから Windows サポート診断ツールを起動しています。そして、任意のコードを Windows サポート診断ツール経由で実行させています。

本脆弱性に対する正式なパッチが、6 月の月例セキュリティ更新プログラムで公開されました。早急にセキュリティパッチの適用をご検討ください。
Microsoft 社は、一時的な回避策として MSDT URL プロトコルの停止を挙げています。
この回避策を実行すると、OS 全体を通してリンクからの Windows サポート診断ツールの起動が阻止されてしまいます。その一方で、Get Help アプリケーションやシステム設定、追加のトラブルシューティングから手動で実行することは可能です。

・回避策（MSDT URL プロトコルを無効化）

1. 管理者としてコマンドプロンプトを起動
2. 「reg export HKEY_CLASSES_ROOT¥ms-msdt 任意のファイル名」を実行して、レジストリキーのバックアップをとる
3. 「reg delete HKEY_CLASSES_ROOT¥ms-msdt/f」を実行する

・回避策を元に戻す方法

1. 管理者としてコマンドプロンプトを起動
2. 「reg import 上記指定したファイル名」を実行する

2022 年 5 月には、脆弱性 CVE-2022-30190 を悪用して任意のコードを実行させる Word ファイルが確認されています。実際に Qbot マルウェアを配布する手段として利用された事例も報告されています。6 月の月例セキュリティ更新プログラムにてセキュリティパッチが公開されていますので、早急にセキュリティパッチの適用をご検討ください。また、セキュリティパッチをすぐに適用できない環境では、Microsoft 社の推奨する一時的な回避策の実施が推奨されます。

■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

- マイクロソフト セキュリティ レスポンス センター | 「Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability」
  https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

- Microsoft Security Response Center | 「CVE-2022-30190 マイクロソフト サポート診断ツールの脆弱性に関するガイダンス」
  https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability-jp/

- WeliveSecurity | 「Vulnerabilidade critica “Follina” e explorada atraves de documentos do Office」
  https://www.welivesecurity.com/br/2022/06/08/vulnerabilidade-critica-follina-e-explorada-atraves-de-documentos-do-office/

- BleepingComputer | 「Qbot malware now uses Windows MSDT zero-day in phishing attacks」
  https://www.bleepingcomputer.com/news/security/qbot-malware-now-uses-windows-msdt-zero-day-in-phishing-attacks/

- Microsoft Security Response Center |「2022 年 6 月のセキュリティ更新プログラム（月例）」
  https://msrc-blog.microsoft.com/2022/06/14/202206-security-updates/

Canon

キヤノンマーケティングジャパン株式会社