2022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

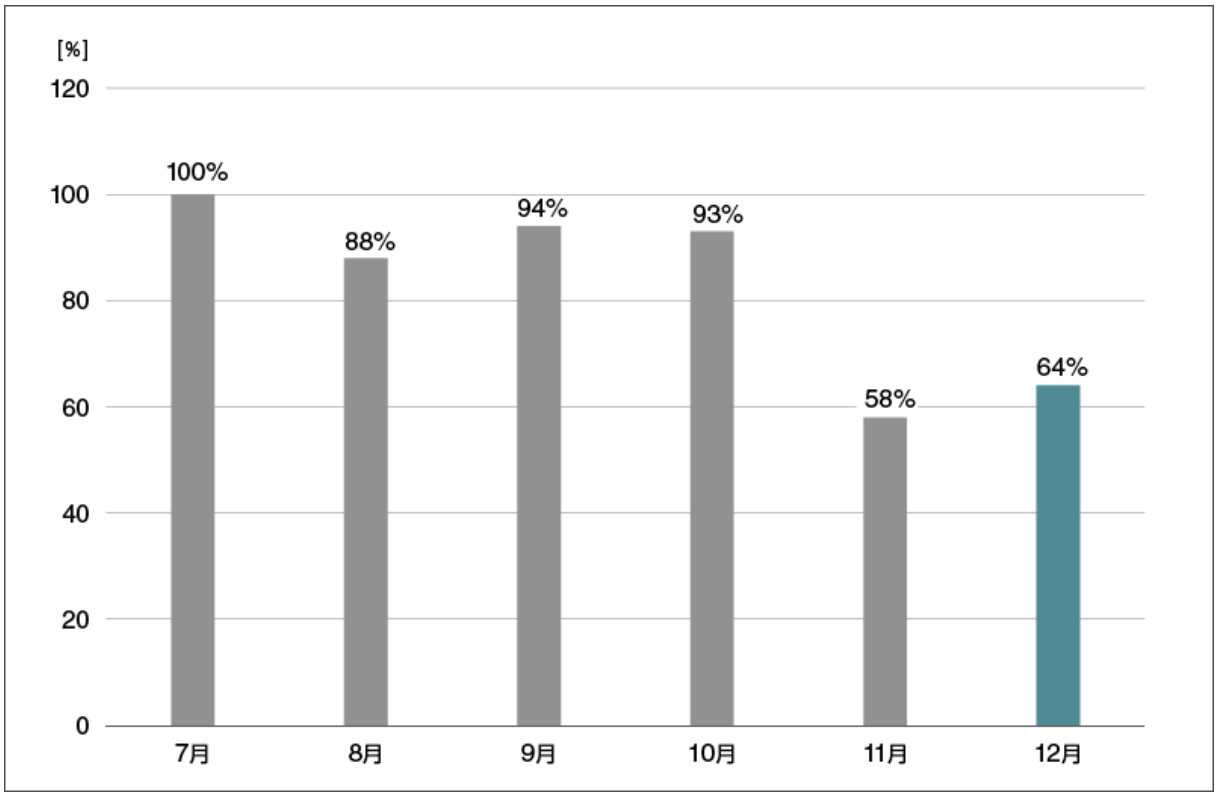
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2022 年 12 月マルウェア検出状況

2022 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
(2022 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。

2022 年 12 月の国内マルウェア検出数は、2022 年 11 月と比較して微増しました。検出されたマルウェアの内訳は以下のとおりです。

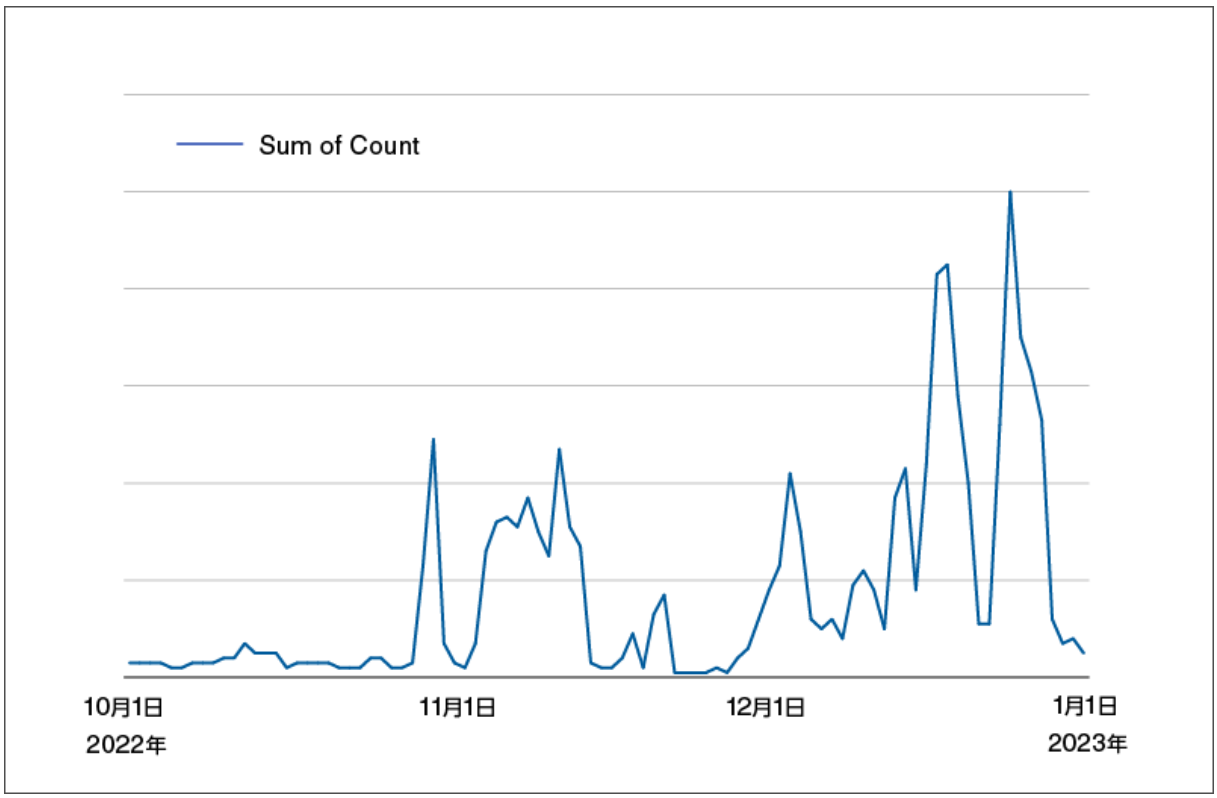
国内マルウェア検出数[*2] 上位（2022 年 12 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	13.4%	アドウェア
2	JS/Packed.Agent	10.5%	パックされた不正な JavaScript の汎用検出名
3	DOC/Fraud	8.2%	詐欺サイトのリンクが埋め込まれた doc ファイル
4	HTML/Pharmacy	7.6%	違法薬品の販売サイトに関連する HTML ファイル
5	JS/Adware.TerraClicks	5.5%	アドウェア
6	JS/Adware.Sculinst	3.0%	アドウェア
7	HTML/Phishing.Agent	2.8%	メールに添付された不正な HTML ファイル
8	HTML/FakeAlert	1.8%	偽の警告文を表示させる HTML ファイル
9	Win32/Kryptik	1.5%	難読化された Win32 形式のファイルの汎用検出名
10	HTML/ScrInject	1.4%	HTML に埋め込まれた不正スクリプト

*2 本表には PUA を含めていません。

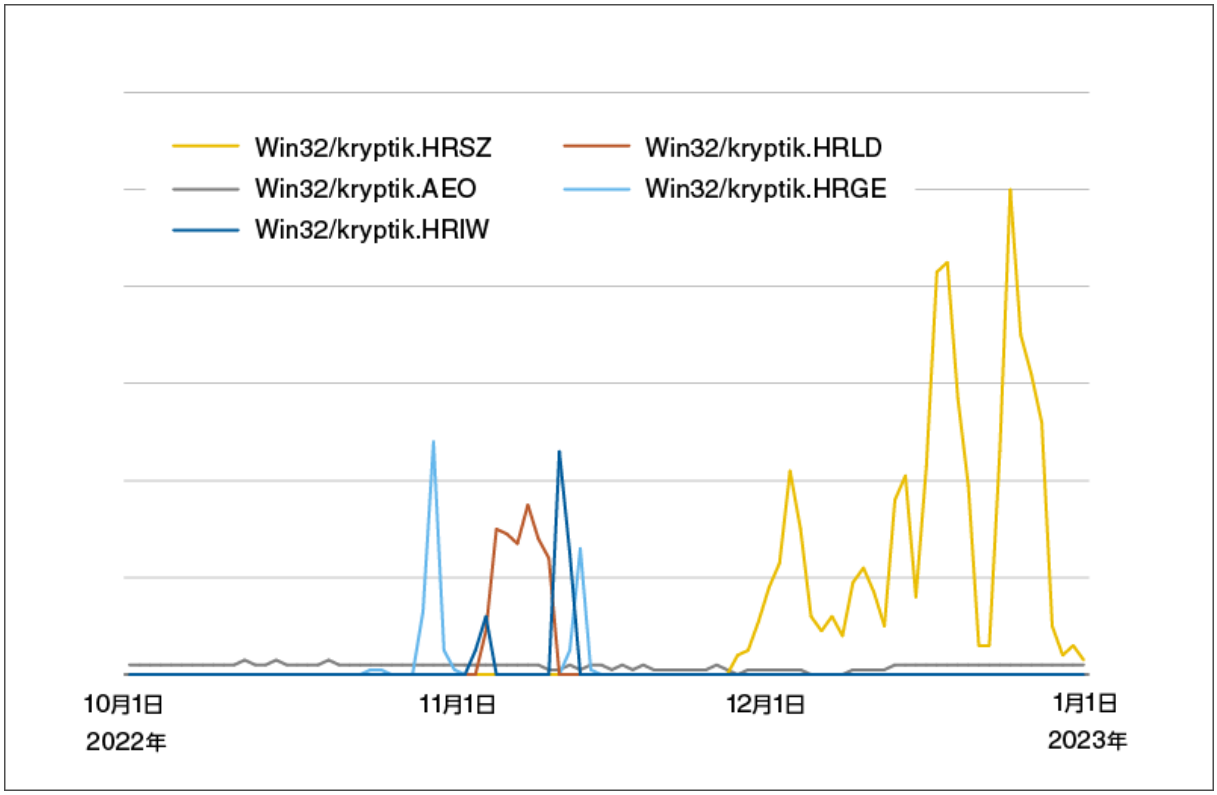
12 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

12 月の国内マルウェア検出数上位の 9 位に Win32/Kryptik がランクインしました。Win32/Kryptik の検出数は 11 月頃から増加傾向にあり、12 月の検出数は先月比で約 2 倍、先々月比では約 5 倍です。この増加率はマルウェア全体で見ても特に目立ったものとなっています。



国内における Win32/Kryptik 検出数の推移

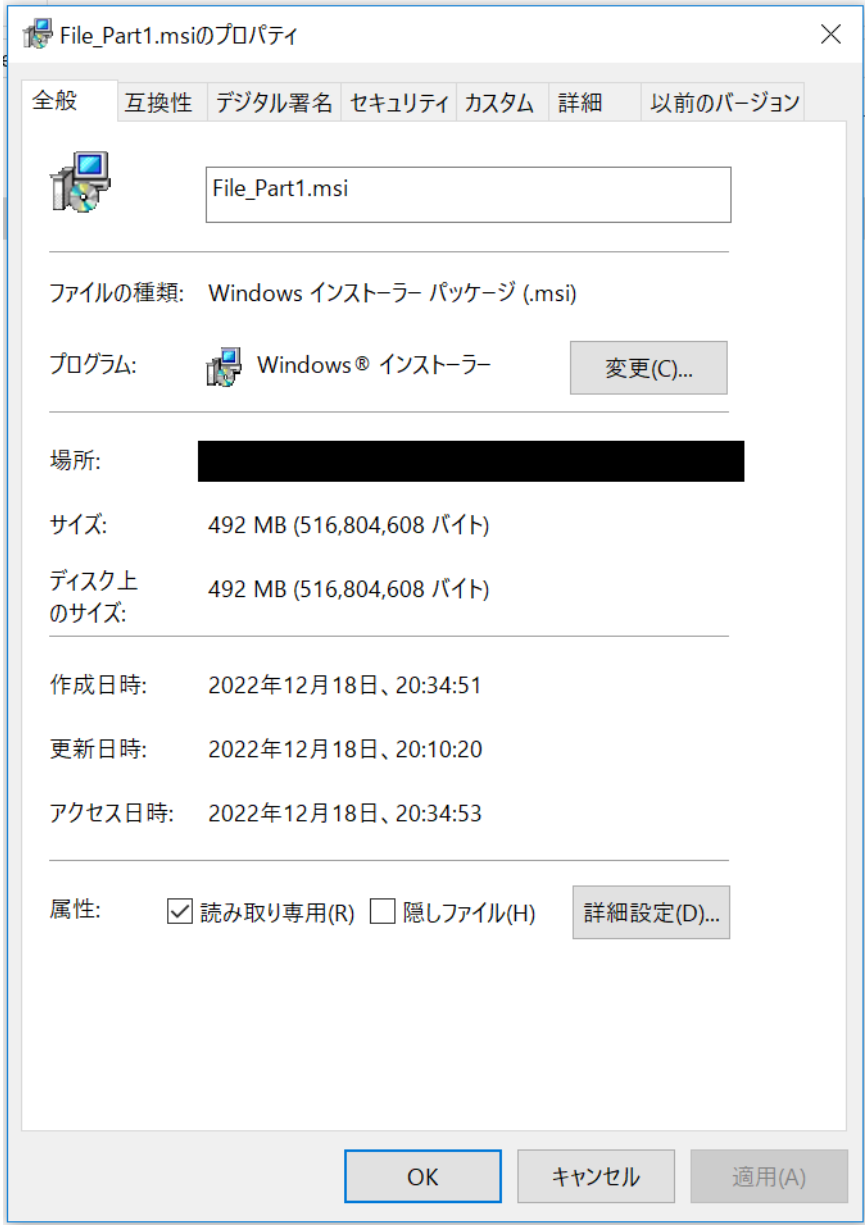
Win32/Kryptik は難読化が施されたファイルの汎用検出名であり、その検出数は多くの亜種の合算です。どの亜種の検出数が増加しているのかを確認するために、亜種ごとの検出数の変化をグラフに示しました。これら 5 種類の亜種は、2022 年 7 月からの半年間の検出数上位 5 種です。



国内における Win32/Kryptik 亜種別検出数の推移

検出数上位 5 種の推移データから、12 月の Win32/Kryptik の検出数急増は Win32/Kryptik.HRSZ が原因だと考えられます。

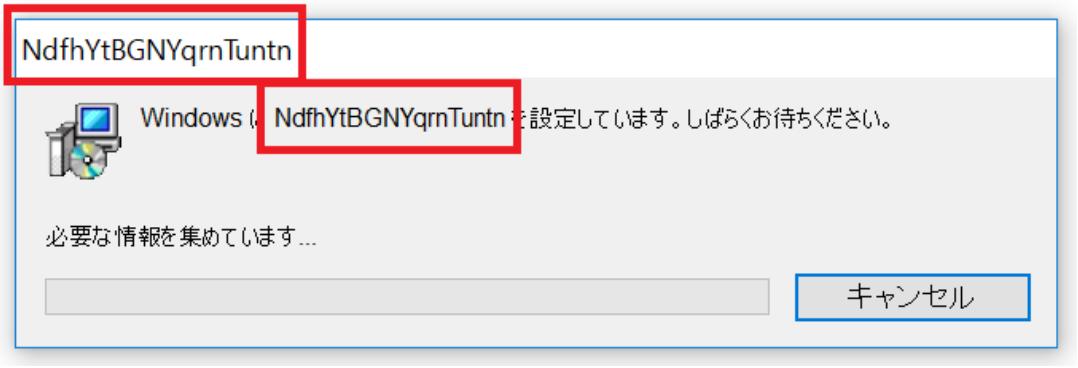
Win32/Kryptik.HRSZ は、主に MSI ファイル（Windows Installer）やそれを ZIP 形式に圧縮した形でインターネット上に出回っています。ZIP 形式の場合は、中に MSI ファイルの実行を促すテキストファイルが含まれているものも確認しました。Win32/Kryptik.HRSZ のファイル名は Windows OS のアップデートファイルを装ったものになっており、誤って実行してしまうとパソコンにマルウェアがインストールされます。



Win32/Kryptik.HRSZ と検出される MSI ファイル

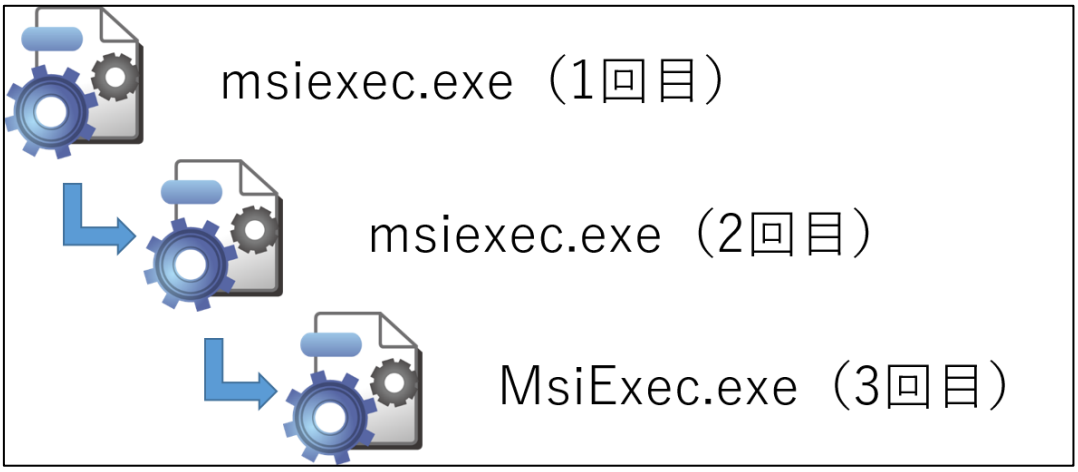
また、Win32/Kryptik.HRSZ の特徴的なダウンロード元として「cdn[.]discordapp[.]com」から始まる URL を確認しています。この URL は、オンラインチャットアプリの「Discord」でファイル共有した際に作成される URL です。Discord を通じたファイル共有はセキュリティ製品によるアクセスのブロックをすり抜けるために、多くの攻撃者に悪用されています。

この MSI ファイルを実行すると、以下のようなポップアップウィンドウが表示され、マルウェアのダウンロードが行われます。一見すると普通の Windows Installer のようですが、表示されるプログラム名が自動生成された文字列になっています。



Win32/Kryptik.HRSZ 実行時のポップアップウィンドウ

Win32/Kryptik.HRSZ 実行時のプロセスツリーは以下のようになっています。連鎖的に 3 回実行される msiexec というプロセスが、Windows Installer を実行するプログラムです。



Win32/Kryptik.HRSZ 実行時のプロセスツリー

それぞれのプロセスは以下のような処理を行っています。

1 回目　C ドライブ直下に MSI ファイルの複製を作成
2 回目　C:¥Windows¥Installer フォルダーに MSI ファイルの複製と MSI****.tmp（DLL）を作成
3 回目　MsiExec.exe のカスタムアクションで DLL である MSI****.tmp を呼び出し

こうした MSI ファイルを利用したマルウェアのインストール手法は、過去に LokiBot*3 や Magniber*4 の配布でも確認されており、検出を困難にする目的で攻撃者に悪用されているものと思われます。

*3 Windows Installer “msiexec.exe” を利用して「LokiBot」感染に誘導 | Trend Micro
*4 正常な Windows インストーラー(MSI)に偽装した Magniber の配布が再開 (2/22) | ASEC

Win32/kryptik.HRSZ に関連した記事を、1 月 2 日にイスラエルのセキュリティ企業が公開しました。*5 この記事によれば、Win32/Kryptik.HRSZ は Raspberry Robin と呼ばれるマルウェアの新型であり、感染すると C2 サーバーから更なる悪意あるソフトウェアがインストールされる可能性があるとされています。

*5 Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe | Security Joes

今回のレポートでは、12 月に検出数が急増した Win32/Kryptik の亜種を紹介しました。
このマルウェアは、Windows Installer を悪用し、非常に気づきにくい形でパソコン内部に侵入します。このようなマルウェアへの感染を防止するためには、平時からセキュリティソフトを最新にアップデートし、信頼できないサイトからはファイルをダウンロードしないことが大切です。

■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

■ Windows Installer “msiexec.exe” を利用して「LokiBot」感染に誘導｜Trend Micro
https://www.trendmicro.com/ja_jp/research/18/b/victims-are-led-to-lokibot-indections-using-the-windows-installer-msiexec-exe.html

- 正常な Windows インストーラー(MSI)に偽装した Magniber の配布が再開 (2/22)｜ASEC
  https://asec.ahnlab.com/jp/32161/
- Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe
  ｜Security Joes
  https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe

Canon

キヤノンマーケティングジャパン株式会社