2023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

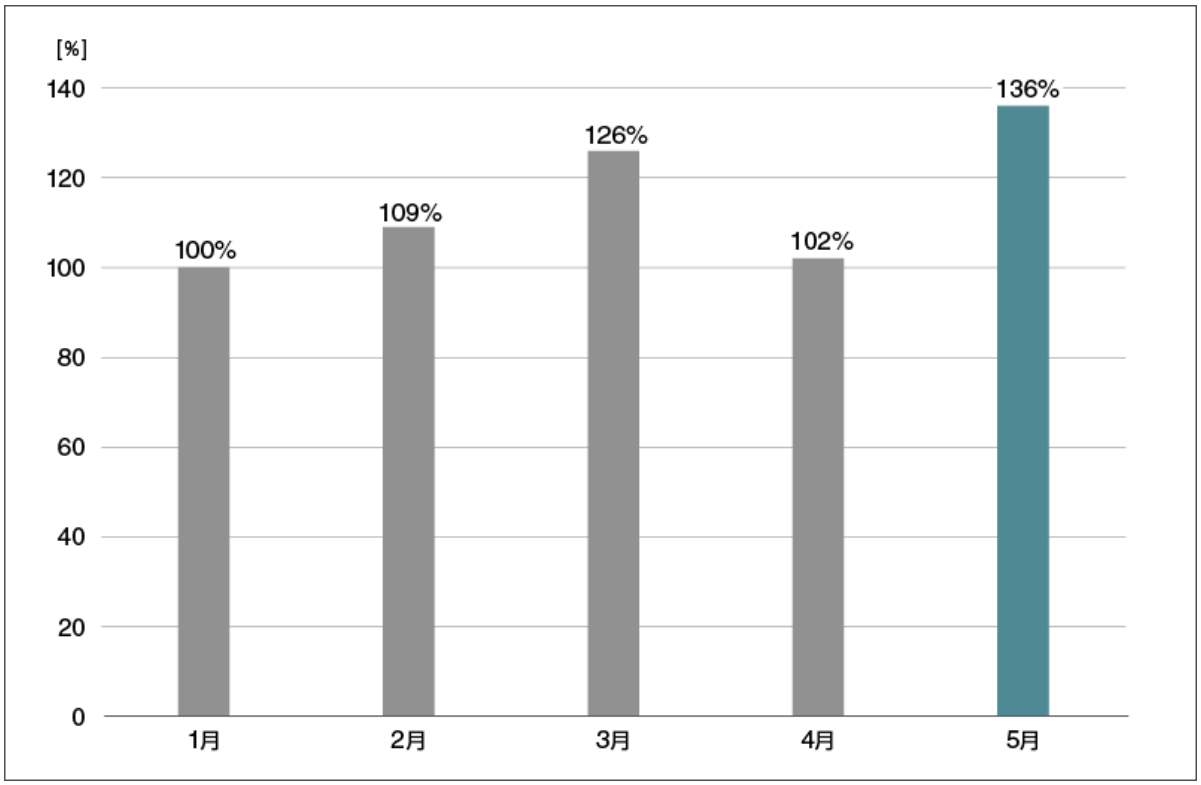
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2023 年 5 月マルウェア検出状況

2023 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
（2023 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。

2023 年 5 月の国内マルウェア検出数は、2023 年 4 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（2023 年 5 月）

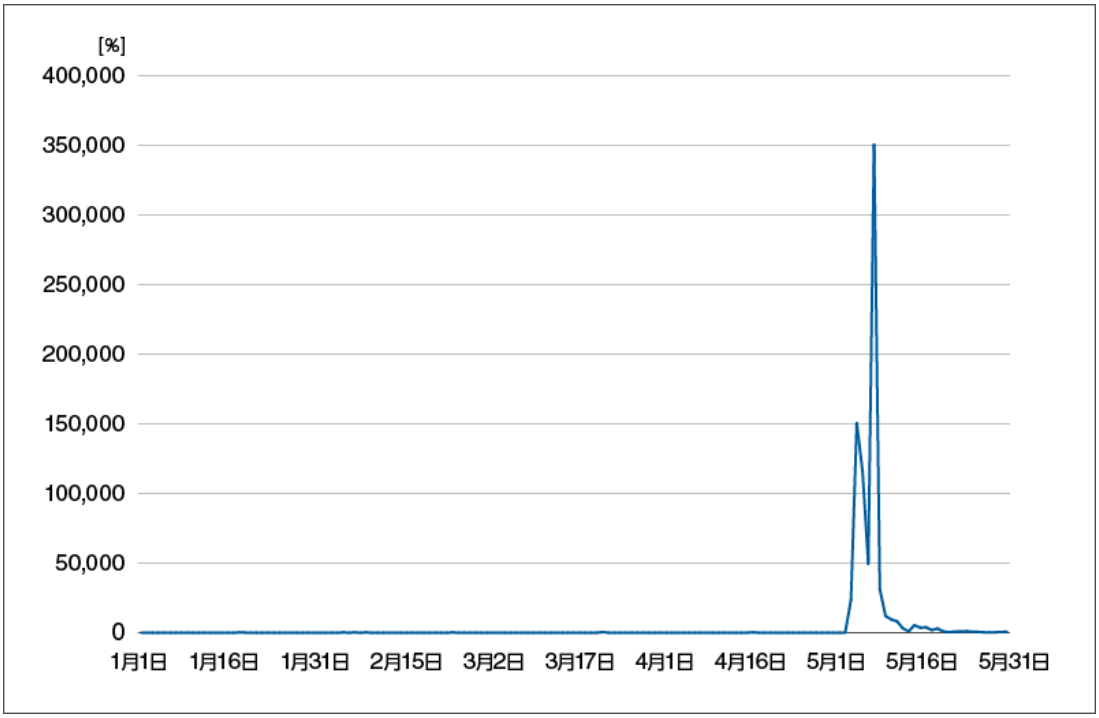
順位	マルウェア	割合	種別
1	JS/Adware.Agent	33.7%	アドウェア
2	DOC/Fraud	14.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
3	HTML/Phishing.Agent	14.7%	メールに添付された不正な HTML ファイル
4	JS/Adware.TerraClicks	6.6%	アドウェア
5	JS/Agent	2.4%	不正な JavaScript の汎用検出名
6	HTML/Phishing	2.0%	悪意のある HTML コードの汎用検出名
7	Win32/Exploit.CVE-2017-11882	1.7%	脆弱性を悪用するマルウェア
8	JS/Adware.Sculinst	1.6%	アドウェア
9	Win64/Riskware.PEMalform	0.7%	ブラウザハイジャッカー
10	MSIL/TrojanDownloader.Agent	0.6%	ダウンローダー

*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.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。

5 月に増加した Win64/TrojanDownloader.Agent.ACN について

Win64/TrojanDownloader.Agent は、Win64 形式のダウンローダーの検出名です。
5 月に検出数が急増しており、検出数第 12 位に入っています。



Win64/TrojanDownloader.Agent の日別検出数の推移（2023 年･国内）
2023 年 1 月 1 日の検出数を 100%として比較

5 月に検出された Win64/TrojanDownloader.Agent のうち、亜種の 1 つである Win64/TrojanDownloader.Agent.ACN が最も多く検出されています。亜種別の割合を見ると、約 99%を Win64/TrojanDownloader.Agent.ACN が占めています。

Win64/TrojanDownloader.Agent の亜種別内訳（2023 年 5 月・国内）

亜種名	検出内訳(%)
Win64/TrojanDownloader.Agent.ACN	99.923
Win64/TrojanDownloader.Agent.KE	0.064
Win64/TrojanDownloader.Agent.ADP	0.013

以下では、Win64/TrojanDownloader.Agent.ACN の概要や動作について紹介します。

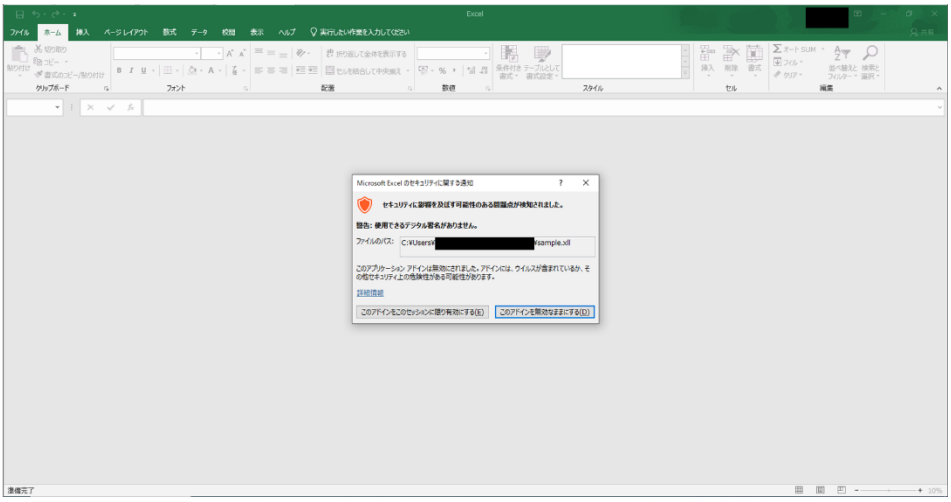
概要

Win64/TrojanDownloader.Agent.ACN は、Excel XLL アドインファイル形式[*3] のダウンローダーです。検出される XLL アドインファイルは、Office 製品が 64bit 版の場合のみ動作します。
また、今回調査した Win64/TrojanDownloader.Agent.ACN の検体では、Office 製品のバージョンが古いと動作しないことを確認しています。Office 2016 では動作せず、Office 2019 では動作していました。

*3 XLL アドインファイルは、Excel のアドインファイルです。Excel でのみ開くことができる DLL ファイルの一種で、C または C++言語で記述されています。カスタム関数やその他の機能といった Excel の機能拡張に利用されています。

感染までの流れ

今回確認した感染までの流れは以下のとおりです。
１． XLL アドインファイルを開く
検体の XLL アドインファイルを開くと、Excel が起動しアドインを読み込みます。読み込み時に表示されるポップアップが下図です。



XLL アドインファイルを開いた際に表示されるポップアップ画面

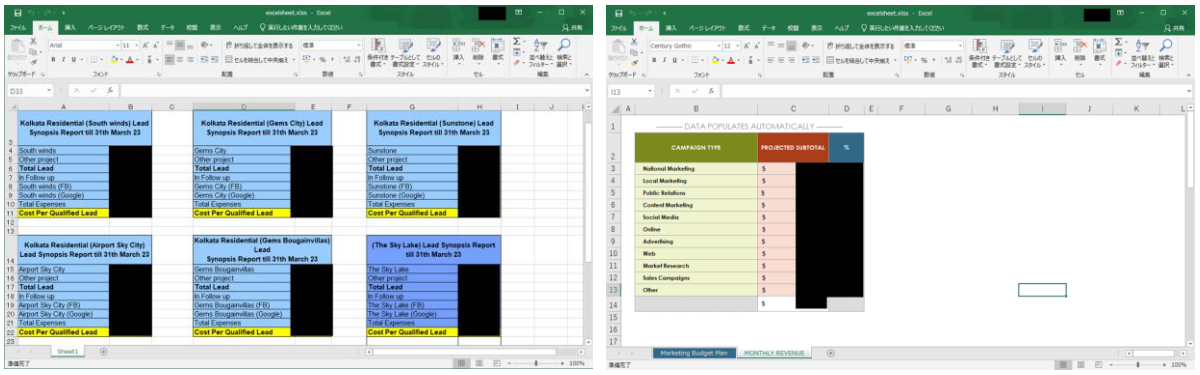
ポップアップは、アドイン実行に関する警告です。「このアドインをこのセッションに限り有効にする」をクリックすると、XLL アドインファイルが読み込まれ、悪意のあるコードが実行されます。

２．アドイン実行時に通信先からダウンロードした Excel ファイルを開く

XLL アドインファイルは、バックグラウンドで実行されます。

アドイン実行時に通信先から Excel ファイルをダウンロードし、「excelsheet.xlsx」として開きます。今回確認したファイルは、広告に関する Excel ファイルでした。

悪意のある動作をユーザーに気づかせないために、ダミーファイルを表示している可能性があります。



今回確認したアドイン実行時にダウンロードされる Excel ファイル

過去の事例でも、新型コロナウイルス感染者数が書かれた Excel ファイルがダミーで表示されていたことが確認されています。

３．攻撃者が用意した通信先から実行ファイルをダウンロードする

今回、通信先のドメインとして、Discord のファイル共有機能を悪用した「cdn[.]discordapp[.]com」や、公開されている IPFS[*4] ゲートウェイである「ipfs[.]io」を悪用した URL を確認しました。

*4 IPFS（InterPlanetary File System）は、P2P ネットワークを用いた分散型のファイルストレージプロトコルです。

今回調査した検体がアクセスした通信先

プロトコル	ドメイン	設置されていた実行ファイル名の ESET 検出名
HTTPS	cdn[.]discordapp[.]com	MSIL/Spy.Kiangthi.A
HTTPS	ipfs[.]io	MSIL/GenKryptik.GJMH

通信先には実行ファイルが設置されていました。設置されていた実行ファイルは、情報窃取型マルウェアでした。

対策

Microsoft 社は、2023 年 3 月 28 日にインターネットからダウンロードした XLL アドインファイルをブロックするように、Excel の既定の設定を変更しています。
Excel をバージョン 2303（ビルド 16227.20212）以降にバージョンアップすることをおすすめします。
アップデートの対象となる Excel 製品は以下のとおりです。

- Microsoft 365 Apps
- Excel 2021/2019/2016

今回紹介した Win64/TrojanDownloader.Agent.ACN は、Excel XLL アドインファイルを悪用したダウンローダーです。端末環境によっては動作しない可能性もありますが、事前の対策が重要です。セキュリティ製品を正しく導入・運用し、OS やソフトウェアは最新の状態に保ってください。また、不用意に添付ファイルを開かないことや紹介した個別の対策の検討を行ってください。

■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

■Office アドイン「XLL ユーザー定義関数を使用してカスタム関数を拡張する」| Microsoft
https://learn.microsoft.com/ja-jp/office/dev/add-ins/excel/make-custom-functions-compatible-with-xll-udf
■サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2021 年 7 月～9 月]《付録》～Excel-DNA を悪用した Excel アドインファイルのウイルス～ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000094144.pdf
■Discord を利用していなくても感染するマルウェアとは | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/230627.html
■Cloudflare Docs「Interplanetary File System (IPFS)」| Cloudflare
https://developers.cloudflare.com/web3/ipfs-gateway/concepts/ipfs/
■Microsoft 365「現在のチャネルのリリースノート」| Microsoft
https://learn.microsoft.com/ja-jp/officeupdates/current-channel#version-2303-march-28

Canon

キヤノンマーケティングジャパン株式会社