2023年
10月
OCTOBER

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

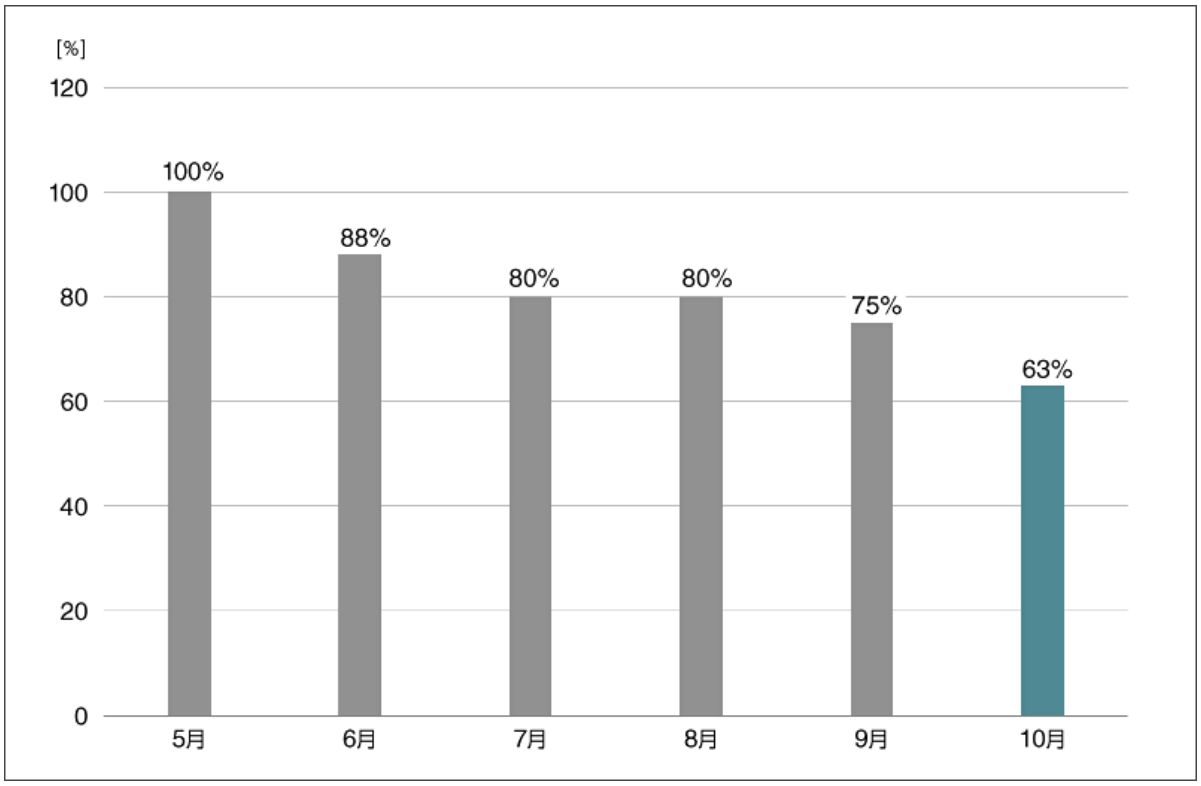
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 10 月マルウェア検出状況

2023 年 10 月（10 月 1 日～10 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 5 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 10 月の国内マルウェア検出数は、2023 年 9 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（2023 年 10 月）

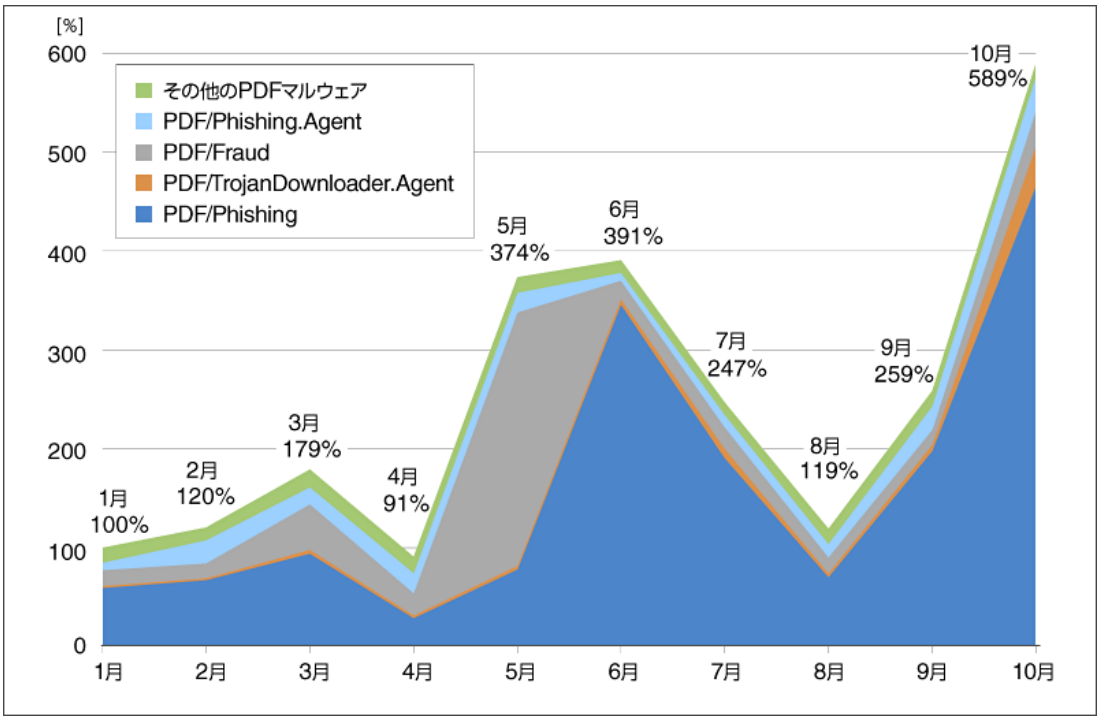
順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	15.6%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	12.2%	アドウェア
3	JS/ScrInject	9.9%	不正な JavaScript の汎用検出名
4	JS/Adware.TerraClicks	8.9%	アドウェア
5	DOC/Fraud	8.4%	詐欺サイトのリンクが埋め込まれた DOC ファイル
6	JS/Adware.Sculinst	5.4%	アドウェア
7	JS/Agent	5.3%	不正な JavaScript の汎用検出名
8	PDF/Phishing	1.8%	詐欺を目的とした不正な PDF ファイル
9	HTML/Fraud	1.6%	詐欺サイトのリンクが埋め込まれた HTML ファイル
10	Win32/Exploit.CVE-2017-11882	1.5%	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。

10 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL に接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

検出数が増加傾向にある PDF 形式のマルウェア

10 月の国内マルウェア検出数上位 10 種を見てみると、先月に引き続いて PDF/Phishing が入っており、このマルウェアの脅威が続いている状況がわかります。この PDF/Phishing は、マルウェアの配布サイトや実在するサービスを模したフィッシングサイトへの URL リンクを含む不正な PDF 形式のマルウェアです。10 月における ESET 検出数を PDF 形式のマルウェアに絞って見てみると、1 位の PDF/Phishing を筆頭に PDF/TrojanDownloader.Agent、PDF/Fraud、PDF/Phishing.Agent の順で上位が続きます。これらの検出数は先月と比較するとすべて増加しており、PDF 形式のマルウェア全体でも 10 月は 2023 年で最も検出数の多い月となりました。



国内 PDF 形式のマルウェア検出数の月別推移
（2023 年 1 月の PDF マルウェアの全検出数を 100%として比較）

PDF 形式のマルウェアの検出数が増加した背景として、攻撃者が新たな攻撃手法を模索していることが推測されます。2023 年上半期サイバーセキュリティレポートでも言及しているように、国内は MS Office 文書のマルウェア（DOC 形式のマルウェア）が多い傾向にあり、これまでに多くのセキュリティ機関が注意喚起を発信してきました。MS Office 文書に対する警戒感が一層高まってきている中で、攻撃者としてはそれに代替する攻撃手法を模索する必要があります。その一環として、PDF 形式ファイルの悪用が増加している可能性があります。
PDF 形式ファイルの悪用自体は以前から存在していますが、今回の脅威拡大を受け、改めて PDF 形式ファイルがどのように悪用されるのかを紹介します。

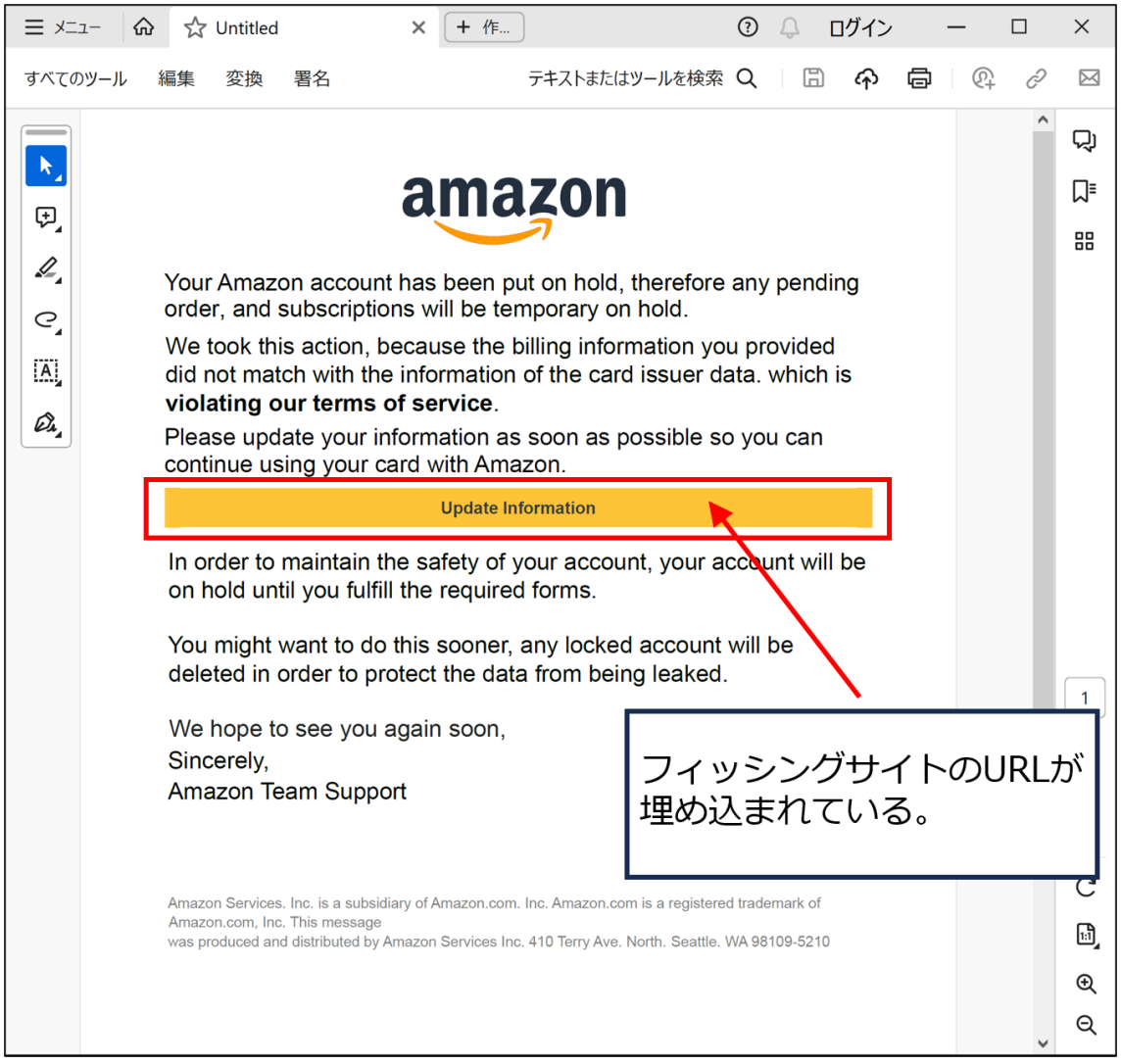
PDF 形式のマルウェアの悪用手法

PDF ファイルの悪用方法はいくつか存在しますが、今回は以下の 3 つについて紹介します。

① 悪意のある URL やコードを埋め込む
② ファイルを開いた際に悪意のある処理を実行させる
③ PDF リーダーの脆弱性を悪用する

① 悪意のある URL やコードを埋め込む

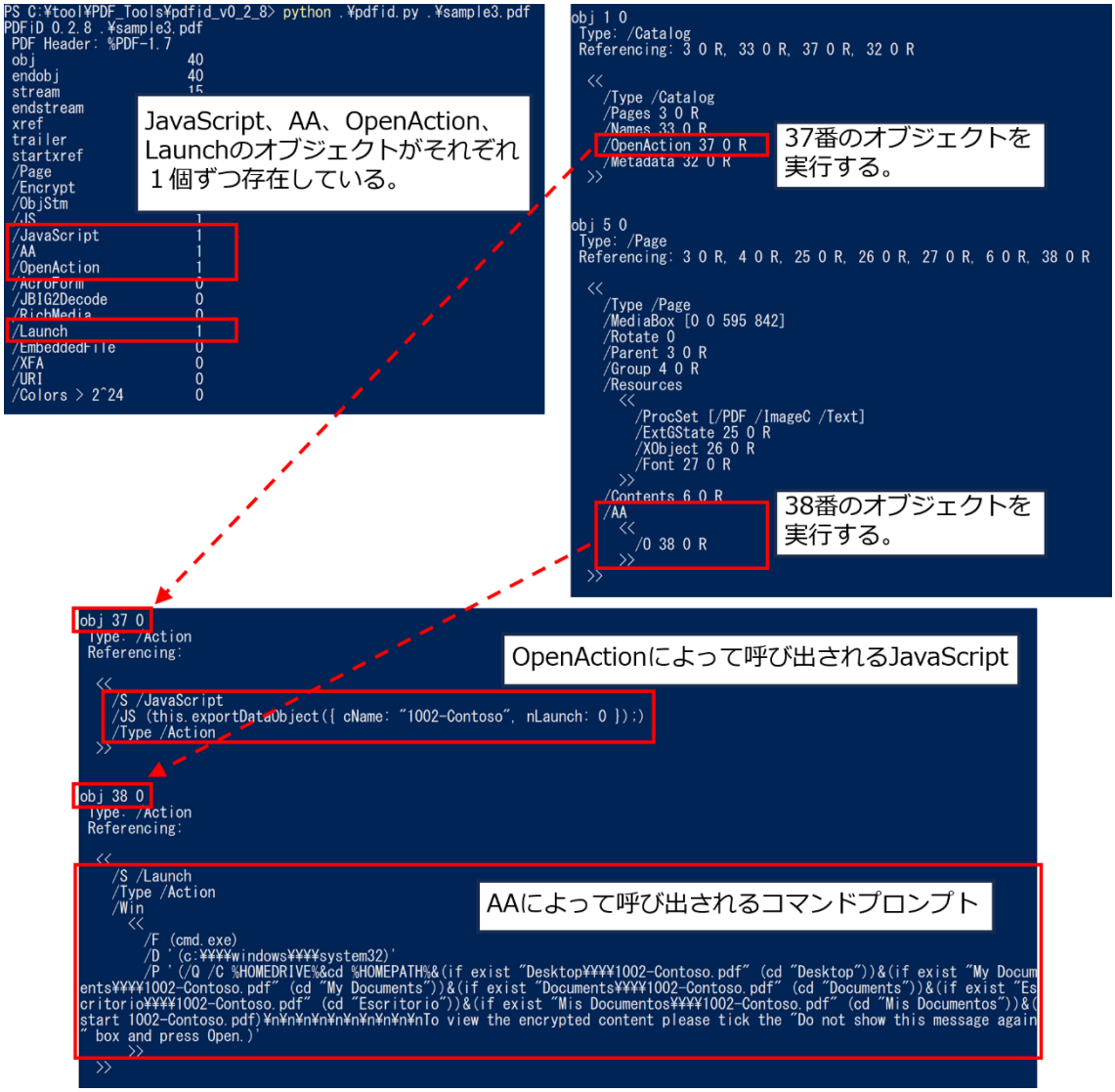
文書中に悪意のある URL やコードを埋め込む方法です。これらの埋め込みリンクやコードは文書中の文字列やオブジェクトに埋め込まれています。標的ユーザーにそれらをクリックさせるため、ファイルのダウンロードを促す文章や緊急性のある文言などで誘導する工夫が見受けられる場合があります。反対にクリックなどのユーザーによる操作を必要とせずコードを実行できる場合、背景と同色、または透過度を 100%に設定したオブジェクトなどに埋め込み、目視では気づかれないような工夫が施される場合もあります。



Amazon 社を騙り悪意のある URL を埋め込んだ PDF ファイルの例

② ファイルを開いた際に悪意のある処理を実行させる

PDF ファイルのフォーマットには OpenAction、AA(AutoAction)、Launch といった機能が定義されています。OpenAction は PDF ファイルを開いた時に何らかの処理を実行する機能、AA は指定の操作をトリガーに何らかの処理を実行する機能、Launch はアプリケーションの起動やファイルの印刷などを実行する機能です。これらの機能を悪用することで、PDF ファイルを開くと同時にファイル内のコードを実行してマルウェアをダウンロードさせるといったことが可能です。



ファイルを開いた際に悪意のある挙動を示す検体の解析

③　PDF リーダーの脆弱性を悪用する

PDF ファイルを開く場合、基本的には Adobe Acrobat Reader や Web ブラウザーなどの PDF リーダーを使用します。これらの PDF リーダーには脆弱性が発見されることがあり、マルウェアはその脆弱性を悪用する場合があります。

例えば最近の例として、2023 年 9 月に Adobe Acrobat および Reader の脆弱性（CVE-2023-26369[*3]）が公表されました。この脆弱性が悪用されると、任意のコードが実行される恐れがあります。悪用が比較的容易であることや悪用された場合の影響が大きいことなどから、深刻な脆弱性としてセキュリティ機関から注意喚起が発信[*4]されています。

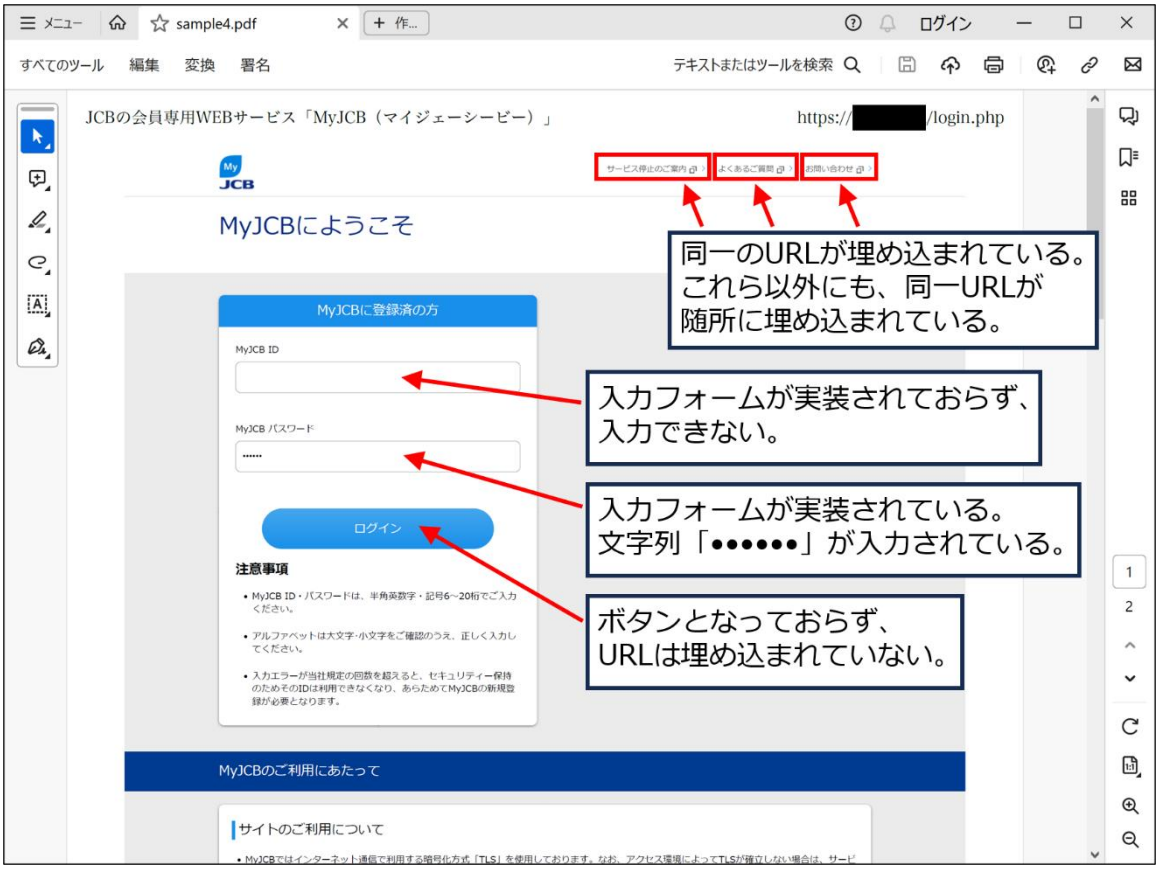
*3 CVE Record | The MITRE Corporation

*4 Adobe Acrobat および Reader の脆弱性対策について(APSB23-34)(CVE-2023-26369) | IPA 独立行政法人 情報処理推進機構

PDF 形式のマルウェアのばらまき準備を観測

サイバーセキュリティラボが実施している調査の中で、不審なファイルや URL を検査する Web サービスとして知られる VirusTotal[*5]に興味深い PDF 形式のマルウェアを発見しました。発見した検体はクレジットカード会社のログインフォームを模した PDF ファイルであり、フォームに入力した個人情報の窃取を目的とした検体であると思われます。悪性と思われる URL が随所に埋め込まれていましたが、「ログイン」ボタンに URL が埋め込まれていなかったり、ID 情報の入力欄が機能していなかったりと、実装に不備がある状態に見受けられました。

*5 VirusTotal - Home



VirusTotal にアップロードされていた JCB 社を騙る検体

この検体の情報を詳しく見てみると、検体の VirusTotal アップロード日時が「2023/11/7 10:33:44（日本時間）」、検体の作成日時が「2023/11/7 10:30:47（日本時間）」となっており、検体が作成されてからわずか 3 分後に VirusTotal へアップロードされていることがわかります。また VirusTotal にログインしていないユーザー（匿名ユーザー）が Web のフォームから検体をアップロードしたこともわかります。検体の状態が不完全だったことも考慮すると、今後のフィッシングキャンペーンに使用する予定のテスト検体がセキュリティ製品に検知されるか否かについて、攻撃者が確認を行っていたことが可能性の 1 つとして考えられます。

アップロードされていた検体の詳細情報

攻撃者による活動の痕跡と断定はできませんが、仮に攻撃者が確認のためにアップロードした検体である場合、今後この検体の完成版が国内でばらまかれる可能性があるため注意が必要です。

まとめ

ESET 製品による日本国内での PDF 形式のマルウェアの検出数が増加傾向にあります。加えて、攻撃者によるマルウェア配布に向けた準備と思われる痕跡を確認しました。よって今後も PDF 形式のマルウェアの脅威が続く可能性があります。

PDF 形式のマルウェアの対策として、まずは組織で利用している PDF リーダーを最新のバージョンにアップデートしてください。PDF リーダーに関するセキュリティ情報は各製品ベンダーの Web サイトに掲載される場合があるため、定期的に確認することを推奨します。

また PDF リーダーの設定を見直すことも有効です。例えば Adobe Acrobat Reader であれば、アプリケーショ

ンの設定から JavaScript の実行ポリシーを変更することが可能[*6] です。組織の業務体系を考慮して、PDF における JavaScript を無効化することも検討してみてください。
その他、組織で導入しているセキュリティ製品の定義ファイルを最新バージョンに保つことや、EDR 製品を導入して万が一の被害を最小限に留めることなど、PDF に限定しない包括的な対策も実施してください。

*6 セキュリティリスクとしての PDF の JavaScript | Adobe

■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

■CVE Record | The MITRE Corporation
https://www.cve.org/CVERecord?id=CVE-2023-26369
■Adobe Acrobat および Reader の脆弱性対策について(APSB23-34)(CVE-2023-26369) | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/security-alert/2023/0913-adobereader.html
■VirusTotal - Home
https://www.virustotal.com/gui/home/upload
■セキュリティリスクとしての PDF の JavaScript | Adobe
https://helpx.adobe.com/jp/acrobat/using/javascripts-pdfs-security-risk.html

Canon

キヤノンマーケティングジャパン株式会社