2024年
3月
MARCH

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

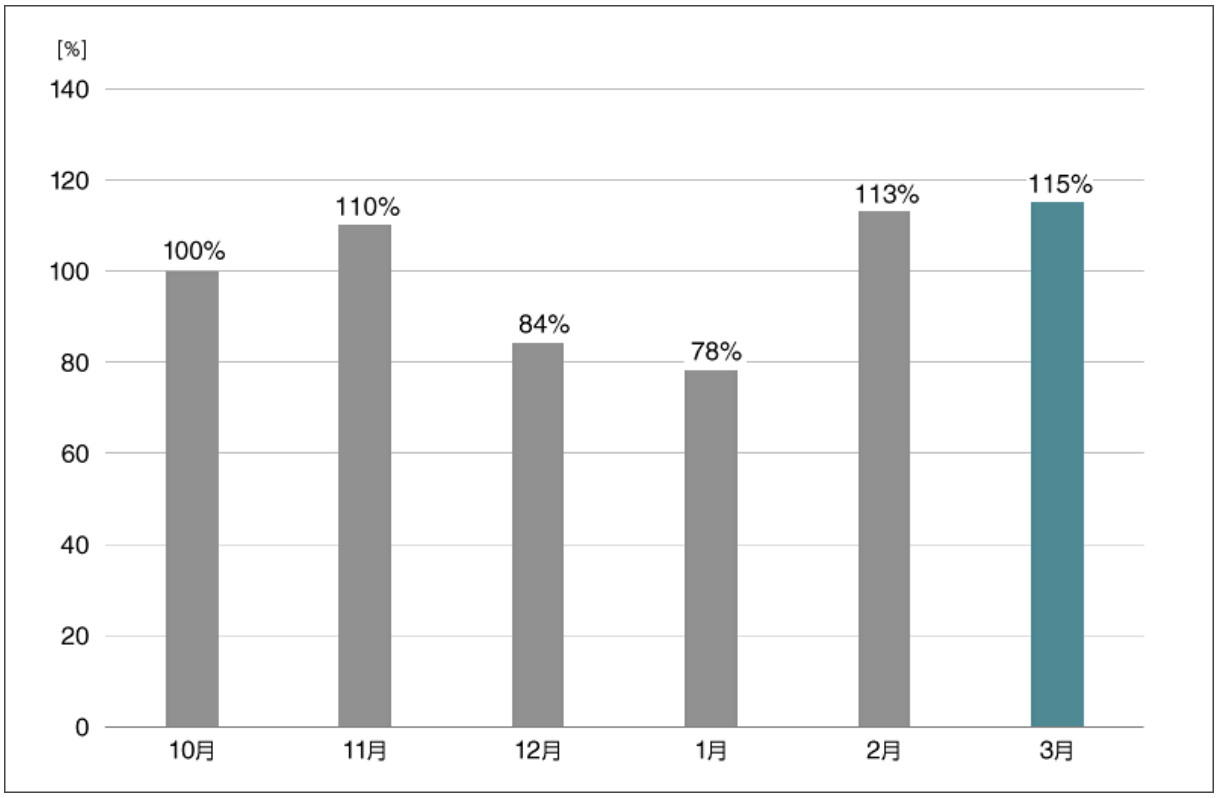
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 3 月マルウェア検出状況

2024 年 3 月（3 月 1 日～3 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 10 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 3 月の国内マルウェア検出数は、2024 年 2 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（2024 年 3 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	16.9%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	15.8%	アドウェア
3	DOC/Fraud	14.8%	詐欺サイトのリンクが埋め込まれた doc ファイル
4	JS/Adware.TerraClicks	12.7%	アドウェア
5	JS/Agent	5.9%	不正な JavaScript の汎用検出名
6	JS/Adware.Sculinst	5.2%	アドウェア
7	MSIL/TrojanDownloader.Agent	1.3%	ダウンローダー
8	HTML/Phishing.Gen	0.9%	フィッシングを目的とした不正な HTML ファイル
9	DOC/TrojanDownloader.Agent	0.7%	ダウンローダー
10	JS/ScrInject	0.7%	不正な JavaScript の汎用検出名

*2 本表には PUA を含めていません。

3 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。

WordPress を狙う攻撃者

WordPress は GNU General Public License (GPL) の下で配布されているオープンソースのコンテンツ管理システム（CMS）です。多種多様なプラグインを使えることや初心者でも扱いやすい GUI を備えていることから、世界各国の個人・企業が WordPress を使用しています。WordPress の発表によると、Web 上の 43%のサイトが WordPress を利用している [1] とされています。

しかし、利用者が多いということは、それだけ攻撃者に狙われやすいということでもあります。
サイバーセキュリティラボでは、WordPress をターゲットとしたマルウェア配布キャンペーンを定期的に確認しています。また、こうした攻撃によって埋め込まれた悪意あるコードが長期にわたり放置されている例もあります。
そのため、WordPress を安全に利用するためには、攻撃を受けることを想定した対策と侵害を受けた際に気付くことができるセキュリティ知識が必要です。

3 月のマルウェアレポートでは、2023 年 12 月に行われた Balada Injector による WordPress を狙ったキャンペーンを例に、WordPress を運用する際に気を配るべき点を紹介したいと思います。

Balada Injector

Balada Injector とは、WordPress をターゲットに不正な JavaScript を埋め込むマルバタイジングキャンペーンの 1 つです。その活動は 2017 年から継続して確認されています。Web サイト向けのサイバーセキュリティ製品を扱う SUCURi が公開した 2022 Website Threat Research Report[2] では、三大マルウェアキャンペーンの 1 つとして紹介されました。

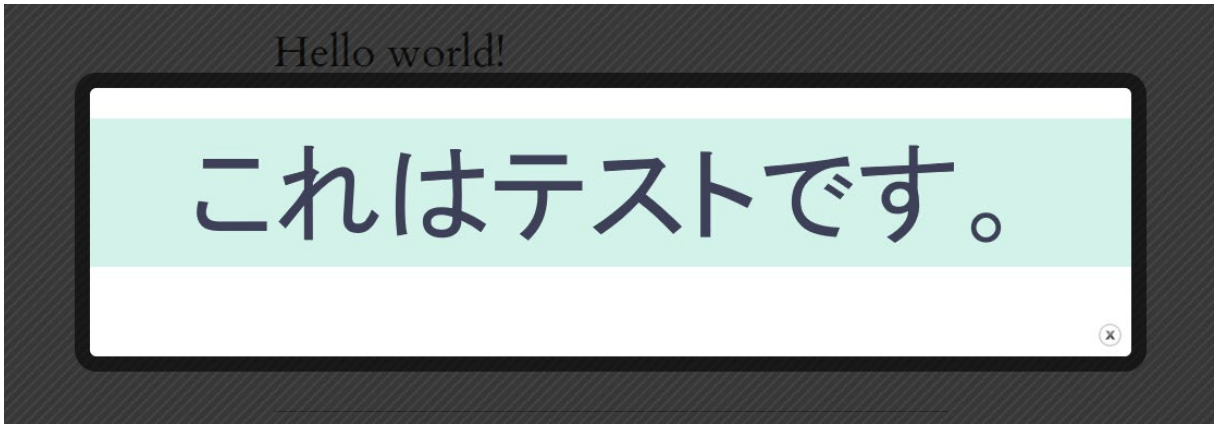
2023 年 12 月のキャンペーンでは、Balada Injector は Popup Builder の脆弱性（CVE-2023-6000）を悪用していました。[3]
Popup Builder は WordPress のプラグインの 1 つで、簡単に Web ページにポップアップを表示できると高評価を得ていたものです。全世界で 20 万回以上このプラグインはインストールされていました。

Popup Builder に存在していた蓄積型クロスサイトスクリプティングの脆弱性が CVE-2023-6000[4] です。この脆弱性を悪用することで、攻撃者は任意のプラグインのインストールや新たな管理者アカウントの作成などを行うことができます。

攻撃手法

どのような流れで CVE-2023-6000 が悪用されるのかを解説します。

攻撃のターゲットとなるのは、脆弱性に対応していない古いバージョンの Popup Builder がインストールされた WordPress です。
Popup Builder で作成したポップアップを適用した Web ページには、以下の画像のようにポップアップが表示されます。今回は「これはテストです。」という文字列を含む画像をポップアップとして表示しています。HTML コードで表示内容を指定することもできます。



ポップアップ画像が表示されている様子

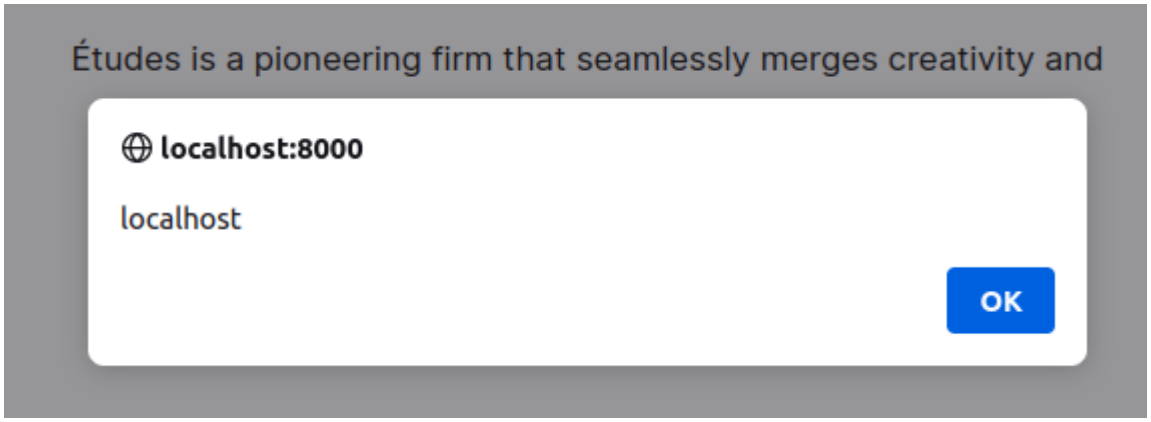
上記の設定が施されている Web ページに対して、curl コマンドを用いて通信を行います。以下の画像に curl コマンドの data オプションに含まれているコードの一部を示しました。画像内のコードには、可読性のためにデコードや整形を行っています。

```
sgpb-copy-to-clipboard-message=Copied to Clipboard!
sgpb-open-animation-effect=No effect
sgpb-close-animation-effect=No effect
sgpb-enable-content-scrolling=on
sgpb-popup-order=0
sgpb-popup-delay=0
sgpb-ShouldOpen=alert(document.domain);
sgpb-WillOpen=
sgpb-DidOpen=
```

curl コマンド data オプションの一部

curl コマンドの data オプションには、Popup Builder の設定情報が入力されています。特に sgpb-ShouldOpen=alert(document.domain);と設定されている点が重要であり、ポップアップが開かれた際の動作が指定されています。今回はシンプルなアラートを表示する JavaScript のコードを用いて、動作確認を行います。

curl コマンド実行後にポップアップが表示される Web ページにアクセスすると、本来表示されるはずの設定したポップアップ画像ではなく JavaScript のアラートが表示されます。

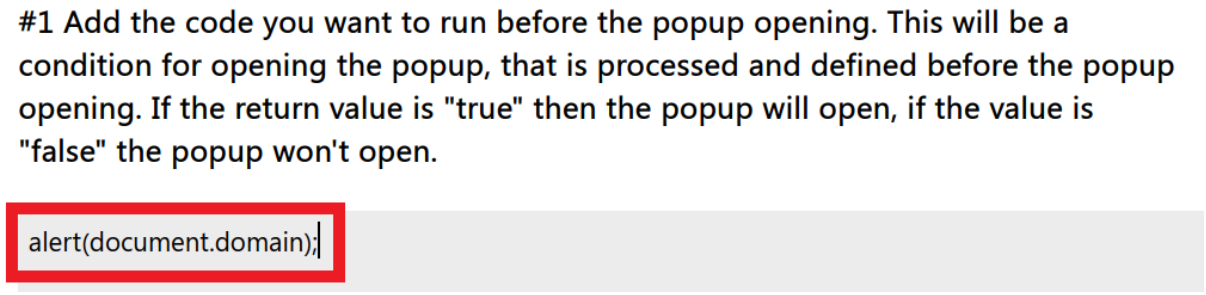


ポップアップ画像ではなくアラートが表示されている様子

WordPress の管理者画面からポップアップ一覧を確認すると、プラグインのタイプが画像から HTML に変更されていることがわかります。これは、先ほど実行した curl コマンドによって、ポップアップの内容が書き換えられた結果です。

コマンド実行前後の Popup builder のポップアップ

また、ポップアップの詳細から、表示される際にどのようなコードが実行される設定になっているかを確認できます。元々は空欄でしたが、alert(document.domain);と変更されており、curl コマンドで指示した関数が実行される設定になっていることがわかります。



ポップアップの詳細画面

この例では、デバッグのために用いられる無害なコードを使用しましたが、実際には悪意あるコードを送信することで、攻撃者の思い通りの操作を実行させることができてしまいます。具体的には、WordPress の管理者によるアクセスをトリガーとして、バックドアとして機能する悪意あるプラグインをインストールさせます。

対策

WordPress を安全に使用するために、次のような対策を行うことが大切です。

- WAF（Web Application Firewall）を導入する
- WordPress やプラグインのバージョン管理を適切に行う
- 関連するゼロデイ攻撃の情報を収集する
- 不審なユーザーやリソースが作成されていないか定期的に確認する
- 不審な通信が行われていないか定期的にチェックする

2024 年に入ってから JVN[5] に追加された WordPress に関連する脆弱性は 200 件を超えます。また、2023 年 12 月の Balada Injector の攻撃は、対応するアップデートが公開された直後に、アップデートに未対応な環境を狙って行われました。こういった攻撃に対応するために、バージョン管理を適切に行うと同時に、攻撃者が狙う脆弱性に関する情報を収集する必要があります。
ゼロデイ攻撃であっても、攻撃の特徴を把握し、関連するプラグインの使用を一時中断する、特徴に合致する通信を遮断するといった方法で被害を軽減できます。
Nuclei[6] や WPScan のようなペネトレーションツールを用いて、利用している環境に既存の脆弱性が含まれていないかをチェックすることも有効です。管理者と相談した上で、これらのツールを利用することも検討してみてください。
また、さまざまな対策をすり抜けて WordPress が侵害されてしまうケースに備え、定期的に改ざんが行われていないか確認することも重要です。各種ファイルのバックアップを作成し、不審な変更が行われていないか差分を調べてください。暗号化した JavaScript をポストしていたり、リソースの ID を取得する通信を行っていたりと、攻撃を目的とした通信にはそれぞれ固有の特徴が現れます。

まとめ

3 月のマルウェアレポートでは、WordPress を狙った攻撃の一例と必要な対策を紹介しました。
利用者が多く、セキュリティ面が脆弱なことがある WordPress は、攻撃者の格好のターゲットとなります。定期的に WordPress を狙ったマルウェア配布キャンペーンが行われており、2023 年の年末にも大規模な攻撃が行われました。今後もこうした活動は続くものと思われます。
上記の対策を参考に、今一度 WordPress を運用している環境を見直してみてください。

■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

1）ブログから大規模サイトまで作れる CMS | WordPress
https://ja.wordpress.org/
2）2022 Website Threat Research Report | SUCURi
https://sucuri.net/reports/2022-hacked-website-report/
3）Thousands of Sites with Popup Builder Compromised by Balada Injector | SUCURi BLOG
https://blog.sucuri.net/2024/01/thousands-of-sites-with-popup-builder-compromised-by-balada-injector.html
4）Popup Builder < 4.2.3 - Unauthenticated Stored XSS | WPScan
https://wpscan.com/vulnerability/cdb3a8bd-4ee0-4ce0-9029-0490273bcfc8/
5）JVN iPedia にようこそ | JVN iPedia 脆弱性対策情報データベース
https://jvndb.jvn.jp/
6）ProjectDiscovery - Nuclei | ProjectDiscovery
https://projectdiscovery.io/nuclei

Canon

キヤノンマーケティングジャパン株式会社