EG Secure Solutions

News Release

報道関係者各位

2024年10月24日

EGセキュアソリューションズ株式会社

サイバーセキュリティ企業【EGセキュアソリューションズ】
2024年3Qにおける攻撃アクセスの傾向をまとめた
「SiteGuard セキュリティレポート」を発表
～急増するバッファオーバーフローとSQLインジェクション攻撃に警戒！～

イー・ガーディアン株式会社（https://www.e-guardian.co.jp/ 東京都港区 代表取締役社長：高谷 康久　以下、「イー・ガーディアン」）のグループ会社である EG セキュアソリューションズ株式会社（https://www.eg-secure.co.jp/ 東京都港区 代表取締役：高谷 康久　以下、「EG セキュアソリューションズ」）は、当社が開発・提供するクラウド型 WAF「SiteGuard Cloud Edition」で 2024 年第 3 四半期（2024 年 7 月 1 日～9 月 30 日）に検出された攻撃を分析した「SiteGuard セキュリティレポート（2024.3Q）」を発表いたします。

EG Secure Solutions

イー・ガーディアングループは、安心・安全なインターネット環境の実現に向け、ネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供しております。特に EG セキュアソリューションズは、ネットセキュリティにおける課題解決を目的としたサービスを幅広く展開しており、WAF 製品「SiteGuard シリーズ」は、累計導入サイト数・累計導入社数で No.1※を獲得いたしました。

SiteGuard Cloud Edition で観測したサイバー攻撃の検出情報を集約・分析した「SiteGuard セキュリティレポート」、今回は 2024 年第 3 四半期における「攻撃種別」「月別」「接続元（国別）」の 3 つの観点での攻撃傾向および特に注目すべき 2 つの攻撃手法について詳しく解説しています。「バッファオーバーフロー」と「SQL インジェクション」の 2 つの攻撃が全体の 9 割を占めており、両者ともに検出数が急増しました。

さらに、詳細な分析として、バッファオーバーフロー攻撃が過去にないほど増加した理由や、SQL インジェクション攻撃が特定の 59 時間に集中していた経緯についても解説しています。

本レポートの内容

1. 攻撃種別
2. 月別の検出
3. 接続元（国別）の分類
4. 2024 年 3Q の注目トピック：バッファオーバーフロー攻撃が増加
5. 2024 年 3Q の注目トピック：SQL インジェクション攻撃が 59 時間に集中
6. 2024 年 3Q のコメント

本レポートの詳細は、以下よりダウンロードいただけます。

ダウンロード URL：https://siteguard.jp-secure.com/resources/siteguard-security-report-2024-3q

【セキュリティ研究所 所長　直岡克起　コメント】

この 3 ヶ月で一番発生件数が多かったバッファオーバーフロー攻撃ですが、SiteGuard ではパスやパラメータ、ヘッダー等の長さが一定の閾値を超えた場合や、shellcode と呼ばれるバイナリデータの一部を発見した場合に検出されます。今回検出されたものは、ほぼすべて長いパスを検出したものでした。その長いパスは下記のような短いパターンが連続するものです。

▼バッファオーバーフロー攻撃として検出された長いパスの例（/xxx/yyy/は実在するパス）

例 1　/xxx/yyy/20230722/20230722/20230722/20230722/20230722/20230722/20230722/…

例 2　/xxx/yyy/img/img/img/img/img/img/img/img/img/img/img/img/img/img/img/img/…

例 3　/xxx/yyy/files/files/files/files/files/files/files/files/files/files/files/files/files/files/files/files/…

これは攻撃であると明確には言えませんが、通常のアクセスとも言えません。上記のパターンで長さが閾値を超えず、検出されずに Web サイトに到達したリクエストもありますが、特に大きな影響はないと考えられます。これらのリクエストには、User-Agent に「Amazon-bot」や「Baidu-bot」を示す文字列が含まれており、それぞれの IP アドレスを逆引きすると、本物の bot である可能性が高いことがわかります。また、検出されたのが 2 つの Web サイトに限定されていることから、Web サイトの構成や設定によって引き起こされる Web クローラーのバグが原因なのではと推察しています。

【「SiteGuard セキュリティレポート」とは】

EG セキュアソリューションズが開発・提供するクラウド型 WAF「SiteGuard Cloud Edition」で検出された攻撃を分析し、サイバー攻撃の傾向や動向、新たな脅威への対応などを四半期ごとにまとめたレポートです。昨今サイバーセキュリティ上の脅威が増大している現状を受け、幅広い役割や年齢層の方々へセキュリティに関する情報をお届けし、セキュリティに関する知見を高め備えてほしいという思いから公開することとなりました。ぜひ皆様のセキュリティ意識の向上・セキュリティ対策の参考としてお役立ていただければ幸いです。

＜集計条件＞

・SiteGuard Cloud Edition の検出情報をもとに集計しています。
・検出名や分類は、SiteGuard Cloud Edition による検出情報をもとにした表記になっています。
・対象サービスの利用者によるセキュリティ診断等のアクセスが集計対象に含まれている場合があります。
・不正ログインの試行（ログインの失敗）のほか、ウェブ以外の不正アクセス（スパムメールやマルウェア等）の情報は含まれていません。

【累計導入サイト数・累計導入社数 No.1※「SiteGuard シリーズ」概要】

SITEGUARD

ウェブサイトの脆弱性を悪用した攻撃を防御するソリューションとして、官公庁や金融機関をはじめとした大企業から個人向けホスティングサービスまで、幅広い導入実績をもつ国内トップシェアクラスの純国産 WAF（Web Application Firewall）製品です。かんたん導入・運用お任せのクラウド型「SiteGuard Cloud Edition」、インストールタイプでカスタマイズ性に優れたソフトウェア型（ホスト型 WAF「SiteGuard Server Edition」、ゲートウェイ型「SiteGuard Proxy Edition」）の 3 製品をご用意しております。
製品詳細 URL：https://siteguard.jp-secure.com/

EG Secure Solutions

News Release

※ 2023 年 12 月期_指定領域における市場調査
調査機関：日本マーケティングリサーチ機構（https://jmro.co.jp/）

【イー・ガーディアングループ 概要】

1998 年設立。2016 年に東証一部上場。2022 年に東証プライム市場へ移行。イー・ガーディアンはネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供する総合ネットセキュリティ企業です。センターは、提携先を含めてグループで国内 8 都市海外 3 都市 19 拠点の業界最大級の体制を誇ります。昨今は Fintech・IoT 業界への参入や RPA 開発による働き方改革への寄与など、時代を捉えるサービス開発に従事し、インターネットの安心・安全を守っております。

■EG セキュアソリューションズ 会社概要

代表者　：代表取締役　高谷 康久
所在地　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　：2008 年 4 月
資本金　：1,000 万円（2024 年 9 月末日現在）
業務内容　：1. 情報セキュリティ、情報システムに関する監査、コンサルティング
2. 情報セキュリティに関する調査、研究、執筆
3. 情報セキュリティ関連の教育及びコンテンツ制作
4. セキュリティ製品の開発、販売、サポート
URL　：https://www.eg-secure.co.jp/

■イー・ガーディアン株式会社 会社概要

代表者　：代表取締役社長　高谷 康久
所在地　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　：1998 年 5 月
資本金　：1,967 百万円（2024 年 9 月末日現在）
業務内容　：ブログ・SNS・掲示板企画コンサルティング/リアルタイム投稿監視業務/ユーザーサポート業務/
オンラインゲームカスタマーサポート業務/コンプライアンス対策・風評・トレンド調査業務/
コミュニティサイト企画・サイト運営代行業務・広告審査代行サービス業務/人材派遣業務
URL　：https://www.e-guardian.co.jp/

【本件に関するお問い合わせ先】
イー・ガーディアン株式会社　担当　：小野
TEL：03-6205-8857　FAX：03-6205-8858　E-mail：info@e-guardian.co.jp