2024 年 8 月 7 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：アジア太平洋地域における API とアプリケーションに対する Web 攻撃は、昨年 65% 増加

この 6 月だけで世界全体で 260 億件以上の API および Web アプリケーション攻撃を確認

※本リリースは 2024 年 7 月 31 日 (現地時間) シンガポールで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、最新の「インターネットの現状（SOTI）」レポートを公開しました。本レポートでは、API とアプリケーションの需要の増加により、それらが攻撃者にとって利益の出やすい標的へと変化していることが示されています。「包囲されるデジタル要塞：現代アプリケーションアーキテクチャを狙う脅威」で Akamai は、2024 年 6 月だけで API やアプリケーションに対する Web 攻撃を世界全体で 260 億件以上観測したと述べています。アジア太平洋および日本（APJ）地域では過去 1 年間で攻撃が 65% も増加し、特に金融サービスやコマース業界の組織が標的になりました。

このような攻撃の急増は、組織が顧客体験の向上とビジネスの成長を実現するために新たなアプリケーションの展開が急速に進んだ結果とも言えます。こうした展開により、アタックサーフェスが拡大し、Web アプリケーションにおけるコーディングの不備や設計上の欠陥などの脆弱性が露呈することになりました。さらに、API エコノミーの急速な成長は、サイバー犯罪者が脆弱性を悪用し、ビジネスロジックを悪用する機会を増やすことにもつながっています。

APJ における API とアプリケーションのセキュリティ保護：脅威、規制、および新たなトレンドへの対応

2023 年第 1 四半期から 2024 年第 1 四半期にかけて、APJ 地域では API とアプリケーションに対する Web 攻撃が急増し、2024 年 6 月には 48 億件もの攻撃が発生しました。業界別では、この地域の金融サービス業界とコマース業界を標的に、最も多くの Web 攻撃が発生しています。

特に API の悪用は、アプリの機能やサービスへのアクセスを提供する上でのゲートウェイとなる API への依存を強めている企業にとって、ますます大きな懸念となっています。このレポートでは、API 攻撃はデータ漏えい、不正アクセス、分散型サービス妨害（DDoS）といったさまざまな形で発生する可能性があることが示されています。

新たな脅威：レイヤー 7 の DDoS 攻撃と、ソーシャルメディアを介した政治選挙への影響

APJ 地域では、Web サイトとオンラインサービスのアプリケーションレイヤーを標的とするレイヤー 7 DDoS 攻撃が過去 1 年間で 5 倍に増加し、本レポートの観測期間中、合計 5.1 兆件の攻撃が行われました。これらの攻撃は、Web サイトやサービスへ大量のリクエストを送って過剰に負荷をかけることで、速度を低下させたり、アクセス不能にしたりすることを目的としています。

ハクティビストは、この種の攻撃を頻繁に利用して、選挙などの重要な政治イベントを妨害し、ソーシャルメディアを介して有権者の感情を操作します。主要なソーシャル・メディア・プラットフォームに一見正当なものに見える大量の Web リクエストを送信し、これらのサーバーに過負荷をかけるというのが典型的な手口で、候補者情報、有権者登録ポータル、さらには選挙結果の最新情報へのアクセスを妨げています。これは有権者の投票率や選挙プロセスに対する国民の認識に直接的な影響を与えます。

APJ 地域では今年、複数の選挙が実施される予定です。これは、ソーシャル・メディア・プラットフォームや選挙関連の Web サイトを通じて重要な民主的プロセスを混乱させようとするハクティビストにとって、格好の標的となる可能性があります。政府機関や企業は、堅牢な DDoS 緩和テクノロジーの導入、重要インフラの冗長性の確保、潜在的なサイバー脅威に関する一般市民への啓蒙といった予防的な対策を講じて、このような脅威から保護するサイバーセキュリティ対策を強化する必要があります。

その他にも、このレポートでは以下のことが明らかになりました。

- 2023 年第 1 四半期から 2024 年第 1 四半期まで、APJ における Web 攻撃は 65% 増加しており、その後の四半期まで伸びが続いています。APJ では本レポートの観測期間（2023 年 1 月 1 日～2024 年 6 月 30 日）中、オーストラリア（146 億件）、インド（120 億件）、シンガポール（107 億件）が API および Web アプリケーション攻撃を受け、中国（43 億件）、日本（40 億件）、ニュージーランド（21 億件）、韓国（16 億件）、香港特別行政区（15 億件）がこれに続きます。
- 2023 年 4 月から 2024 年 2 月にかけて、ソーシャルメディア業界に対してレイヤー 7 DDoS 攻撃が一貫して増加しました。APJ 地域は、Web アプリケーションに対する攻撃の件数において、北米に次いで 2 位にランクされています。シンガポールが 2.9 兆件と最も攻撃が集中し、次いでインド（9,590 億件）、韓国（5,440 億件）、インドネシア（2,600 億件）、中国（1,880 億件）、日本（830 億件）、オーストラリア（740 億件）、台湾（500 億件）と続きます。
- Akamai によると、ハイテク、商業、ソーシャルメディアがレイヤー 7 DDoS 攻撃の標的になった業界 Top 3 であり、わずか 18 か月の本レポートの観測期間に全世界で 11 兆件を超える攻撃が発生しました。APJ 地域では同じ期間に月毎の攻撃数が約 5 倍に増加し、期間中の合計は 5.1 兆件に達しました。
- DDoS 攻撃は、インフラレイヤーとアプリケーションレイヤーの両方で起き、すべてのポートとプロトコルのトラフィックを試みます。これには、ドメイン・ネーム・システム（DNS）も含まれ、Akamai の調査によると、レイヤ 3,4 DDoS 攻撃イベントのうち約 60% に DNS プロトコルが含まれています。
- コマース業界は API および Web アプリケーションの攻撃の被害を最も多く受けており、他のどのセクターよりも 2 倍以上多い攻撃を受けています（第 2 位はハイテク業界）。APJ 地域では、金融サービス部門とコマース部門の両方が最も多くの Web 攻撃を報告しており、この傾向は以前のレポートと一致しています。

- ローカル・ファイル・インクルージョン（LFI）、クロスサイトスクリプティング（XSS）、SQL インジェクション（SQLi）、コマンドインジェクション（CMDi）、サーバーサイド・リクエスト・フォージェリー（SSRF）といった攻撃は、依然としてビジネスアプリケーションと API を標的とする一般的なベクトルです。

「APJ 地域では、API やアプリケーションを標的とした Web 攻撃が頻繁に発生しており、急速にデジタル化する経済によって、この傾向はさらに悪化しています。企業が市場投入までの時間的なプレッシャーに対応するために業務をオンライン化する速度が増すにつれて、開発リソースとセキュリティリソースはさらに疲弊し、セキュリティプロセスが見落とされることがよくあります。そのため、このような環境でセキュリティと耐障害性を強化するために、堅牢なベストプラクティスを確立することは、特に Web 攻撃が集中して起きていることを考慮すると、非常に重要です」と、Akamai Technologies の APJ 担当 Director of Security Technology & Strategy を務める Reuben Koh は述べています。

Akamai の Application Security 担当 Senior Vice President 兼 General Manager を務める Rupesh Chokshi は次のように述べています。「アプリケーションや API に対する攻撃が成功することは一般的になりつつあり、組織の収益や評判に影響を与える可能性があります。」「『包囲されるデジタル要塞：現代アプリケーションアーキテクチャを狙う脅威』は、攻撃者がアプリケーションや API を標的とする方法と、危険な侵入を防止するための戦略について詳細に分析しています」

「包囲されるデジタル要塞：現代アプリケーションアーキテクチャを狙う脅威」では、セキュリティに関する注目点として、モバイルアプリのユーザー契約に関するアドバイスを取り上げています。また、ヨーロッパ・中東・アフリカ（EMEA）地域と、アジア太平洋および日本（APJ）地域の概要も掲載されており、特にこれらの地域に関するデータと、ランサムウェアを防ぐなどの効果を発揮したマイクロセグメンテーションによるゼロトラスト戦略などのケーススタディを多数取り上げています。

Akamai の「インターネットの現状（SOTI）」レポートは今年で 10 周年を迎えました。SOTI シリーズでは、Akamai Connected Cloud から収集したデータに基づいて、サイバーセキュリティと Web パフォーマンスの状況についての専門家の知見をご紹介します。

９月５日(木)、関連ウェビナーを開催

なお、Akamai では国内のお客様を対象に API セキュリティに関するウェビナーを開催予定です。本ウェビナーでは、WAF で検知できない API 攻撃に特有の仕組みを紐解くとともに、Akamai が観測している攻撃の実態を明らかにします。

詳しくはこちらのページをご覧ください。

Akamai について

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。超分散

型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。