Akamai

ホワイトペーパー

高度な攻撃からビジネスを守る

IT 環境の複雑さが増すにつれて、サイバー攻撃は進化し、新たな障害点を利用するようになっています。アプリケーション、API、マイクロサービス、コンポーネントにより、オンラインでのビジネスの方法が常に拡大し、変化しています。残念ながら、それらによって攻撃者が悪用する新たな脆弱性や脅威も発生しています。サイバーセキュリティソリューションは、内部の脅威への対処（自社データのセキュリティ確保）と外部の脅威への対処（ランサムウェア、DDoS、リソース枯渇などの攻撃の阻止）の両方を行わなければなりません。

Akamai の研究者は毎日平均 788 TB のデータを分析しているため、Akamai はそのことを身をもって理解しており、その知識を生かして製品を継続的に革新し、攻撃が進化しても極めて危険な攻撃者や高度なキャンペーンからお客様とユーザーを保護しています。

貴社が直面する可能性のある最も危険な攻撃は何でしょうか。その攻撃に備えるためにはどうすればよいのでしょうか。

ランサムウェアの増加

自社のデータとお客様のデータへのアクセスが失われることは、企業にとって最大の脅威の 1 つです。Akamai の「猛威を振るうランサムウェア」レポートによると、2022 年第 1 四半期から 2023 年第 1 四半期の間にランサムウェア攻撃の数が全世界で 143% 増加しており、攻撃者はゼロデイ脆弱性やワンデイ脆弱性を悪用しています。高度な攻撃が発生する可能性とその影響は、セグメンテーションによって低減することができます。

セグメンテーションとは、パフォーマンスとセキュリティを強化するためにネットワークを小さいセグメントに分割するアーキテクチャ手法です。それに対し、マイクロセグメンテーションとは、個々のワークロードのレベルまで、ネットワークを細かいセキュリティセグメントに論理的に分割するセキュリティ手法です。これにより、分割したセグメントごとにセキュリティ制御やサービスデリバリーを定義できます。

Akamai Guardicore Segmentation は、ゼロトラストを実現するための Akamai Guardicore Platform の一部であり、すべての重要なシステムに対する攻撃を封じ込めて、資産全体への拡散（水平方向の移動）を防止し、応答と復旧を支援します。その結果、侵害が成功することによって生じる評判の失墜、データの損失、収益の損失を防ぐことができます。

Akamai Guardicore Platform はエージェントレスのマイクロセグメンテーションソリューションであるため、ネットワークに物理的な変更を加えたり、サーバーやデバイスの場所を気にしたりすることなく、迅速かつ簡単に展開できます。ネットワーク内のすべての接続をインタラクティブな形式で視覚化することで、展開を妨げる障害の 1 つである、可視性の欠如を克服できます。さらに、Akamai はパフォーマンスの潜在的なボトルネックやコンプライアンス要件に能動的に対処する方法を考案し、さらにはさまざまな種類のインフラに対応できるポリシー適用を可能にしました。つまり、環境全体での広範な可視性ときめ細かい制御が単一のプラットフォームで実現されます。

Akamai は超分散型グローバルネットワーク全体のオンライントラフィックを比類ないレベルで可視化することができます。Akamai Guardicore Platform はその能力を活用して、お客様の環境、資産、アクセス、ネットワークフローを詳細に可視化します。このリアルタイムの情報により、ビジネスの中断を確実に防ぐことができます。

攻撃を受けるアプリと API

貴社はいくつのアプリケーションをお使いですか？きっと自覚している以上の数を使用しているはずです。平均的な企業では 1,000 以上のアプリケーションが使用されています。ほぼすべてのオンライン取引が API に強く依存しており、マイクロサービスベースのアーキテクチャの採用も増加しているため、アプリケーションは複雑化しています。残念ながら、イノベーションを起こして急成長しなければならないというプレッシャーにより、企業は厳格なテストによって潜在的なセキュリティ問題を把握する前にアプリケーションをリリースし、アプリケーションエコシステム全体のリスクを高めてしまうことがよくあります。

Akamai の最新の「インターネットの現状」レポートによると、アプリケーション・プログラミング・インターフェース（API）はほとんどのデジタルトランスフォーメーションの核となっており、全世界の攻撃の 29% は API を標的にしています。欧州・中東・アフリカ地域では、この割合は 47% 強でした。API は、従来の手法と API に特化した手法の両方を使用するサイバー犯罪者がよく利用する攻撃ベクトルです。ボット、分散型サービス妨害（DDoS）攻撃、マルチベクトル攻撃はすべて阻止しなければなりません。

Akamai App & API Protector を使用して Web アプリケーションを保護することで、ワークフロー、ユーザー、ビジネスを悪性の活動や不正行為から保護できます。このソリューションは、設定可能なファイアウォール保護機能により、API　を介して実行される攻撃など、アプリケーションレイヤーを標的とした攻撃を吸収できます。ボットトラフィックをリアルタイムで可視化することで、歪曲された Web 分析を調査し、オリジンの過負荷を防止し、アクセス許可をカスタマイズしてサードパーティやパートナーのボットが滞りなくアクセスできるようにすることができます。

ここで元の質問に戻りましょう。すべてのアプリと API を把握していない場合、どうすればよいのでしょうか。重要なのはやはり可視性です。Akamai API Security はすべての API　を特定し、そのリスクレベルを評価し、攻撃に対応します。これにより、攻撃者がデータにアクセスしたり、悪性ファイルをサーバーにロードしたり、トラフィックの急増によってサーバーを過負荷状態にすることを防止できます。

ご存じでしたか？

DDoS 攻撃は 2021 年から 2023 年の間に 50% 増加しました

2023 年の全 DDoS 攻撃の 60% 以上に DNS コンポーネントがありました

DDoS やリソース枯渇を阻止

分散型サービス妨害（DDoS）攻撃は、最も有名で巨大なオンライン脅威の 1 つです。インターネットが生まれたときから DDoS 攻撃は存在しており、その影響力はオンライン上にあるその他すべてのものとともに拡大してきました。近年、DDoS 攻撃は大規模化、長期化、高度化しており、さまざまな攻撃ベクトルや標的で使用されています。極めて大規模な DDoS 攻撃の件数は 2021 年から 2023 年の間に 50% 増加しました。また、2023 年の全 DDoS 攻撃の 60% 以上に DNS コンポーネントがありました。

このような悪性のボットネットによって最大規模の企業でさえダウンする可能性があり、そうなると数百万人の顧客へのサービスが停止し、ビジネスが中断してしまいます。資金豊富なサイバー犯罪者、国家主導の攻撃者、地政学的な動機のあるハクティビストは、大規模な分散型ボットネットを利用して、大企業だけでなく重要な公共機関（学校、病院、空港、公共事業者など）もダウンさせようとしています。破壊的な DDoS 攻撃やリソース枯渇攻撃は、すべてのレイヤー、ポート、プロトコル、さらには企業や機関の DNS を狙います。

DDoS 攻撃からインフラを保護するためには、リアルタイムの脅威インテリジェンスが必要です。Akamai が収集したデータは、Akamai の DDoS 防御および緩和ソリューションである Prolexic に供給されます。このソリューションは企業のデジタルアプリケーションと体験を支える基本的なデジタルインフラを保護することができ、ビジネスに影響が生じる前にクラウド、オンプレミス、またはその両方のすべてのポートとプロトコルで攻撃を阻止します。

近年、企業の DNS インフラを標的としたリソース枯渇攻撃が再び大幅に増加しています。DNS は企業のオンラインプレゼンスの基本要素です。DNS システムがダウンすると、組織のオンラインプレゼンスは消滅します。Akamai Edge DNS と Shield NS53 は DNS リソース枯渇トラフィックをエッジでドロップし、正当な DNS クエリーのみがお客様のオリジンに到達できるようにします。

攻撃の規模が 2 年ごとに倍増し、それと同時に複雑さも増大するなか、DDoS 防御は長い間、企業にとって最低限必要なものとされてきました。収益とお客様の信頼を失わないためには、すべての潜在的な障害点のセキュリティを確保する必要があります。

攻撃にどのように対処するか

デジタルプレゼンスを持つ組織はいつか攻撃の標的になると考えて、まず間違いありません。セキュリティ戦略の目的の 1 つは、攻撃が発生する前に組織を保護することです。つまり、重要な資産を保護し、ネットワーク全体を可視化して何が起こっているかを把握できるようにし、攻撃が開始されたらそれを検知することで、標的にされにくくします。

しかし、ゼロデイ攻撃のような事態が発生した場合はどのように対処すればよいのでしょうか。そのようなときこそ、Akamai App & API Protector などのソリューションの要である、ふるまい分析の出番です。

Akamai は高度に自動化されたソリューションとマシンインテリジェンスを、Akamai の世界中の Security Operations Command Center（SOCC）の最前線で活動する 225 名を超えるスタッフによるヒューマンインテリジェンスと組み合わせて、お客様のデータ、インフラ、エンドユーザーのデジタル体験を保護しています。

Akamai は毎日 13 兆件以上のドメイン・ネーム・システム（DNS）クエリーを確認し、1 四半期あたり 120 億件以上の Web アプリケーションファイアウォール（WAF）攻撃を防いでいます。すべてを確認し、お客様を通じて経験を蓄積して、攻撃に関する分析を強みに変えます。その脅威インテリジェンスを活用し、ソリューションの応答性と有効性を高めているのです。

攻撃を受けた場合は、ぜひ　Akamai　のサイバー脅威ホットラインへお問い合わせください。Akamai のセキュリティソリューションをまだご利用でなくても大丈夫です。セキュリティの専門家が、現在発生している攻撃を緩和するための次のステップを電話でお知らせします。

ビジネスと世界がつながるあらゆる場所をセキュアに

死を迎えたり税を徴収されたりするように、サイバー攻撃もこの世界で確実に起こることの 1 つです。しかし、最新の脅威インテリジェンスを活用し、アプリケーションやネットワークを高度に可視化し、脅威の状況に合わせて進化するセキュリティソリューションを利用することで、自社と顧客を守ることができます。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、システム、データを守ります。Akamai の広範なソリューションポートフォリオは、グローバルプラットフォームによる脅威の可視性を活用し、業界をリードする信頼性を提供します。お客様は、脅威に先んじて、変化するセキュリティ環境に迅速に適応することができます。

その他のリソース

ランサムウェアのキルチェーンを断ち切るために必要な 5 つのステップを知る

DDoS 攻撃を防ぎながらハイブリッドクラウド戦略を支援する

強力な API セキュリティでビジネスの構成要素を防御する

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。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。公開日：2024 年 6 月。