Akamai

ホワイトペーパー

顧客の信頼を脅かす攻撃ベクトル

セキュリティとブランドへの信頼は、かつてないほど密接に関連しています。企業は自社ブランドのプレゼンスを高めるためにアプリケーションと API を活用しています。そして、サイバー攻撃の件数は世界的に急増しています。これを受けて、顧客体験を損なうことなく、デジタルアプリケーションのセキュリティを確保することがセキュリティチームにとっての最優先課題となっています。

優れた顧客体験はブランドへの信頼につながり、ブランドへの信頼は業績に明確な好影響をもたらします。Web サイトのパフォーマンスやデータの保護などのためには、セキュリティソリューションが必要です。しかし、顧客体験に悪影響を及ぼすセキュリティソリューションを選択している企業があまりにも多いのが現状です。企業を保護するために煩雑なセキュリティコントロールを採用していると、それが顧客にとって障壁となり、顧客の信頼を失い、最終的には売上の低下を招くことになります。

セキュリティソリューションの選択は、成長やイノベーションにも影響を与えます。企業がデジタル化を進めて、データやアプリケーションをクラウドに移行すれば、新たな攻撃ベクトルが生まれ、大勢の攻撃者がそこに目を付けることになります。必要なのは、進化し続ける攻撃戦略や巧妙化するマルチベクトル攻撃（異なる種類の攻撃を同時または続けざまに行うこと）の一歩先を行くセキュリティソリューションです。自社のブランドと顧客からの信頼の両方を守ることのできるソリューションです。

最優先で対応すべき攻撃ベクトルとは

最大の標的：API

現在の企業は、ビジネスのあらゆる側面でアプリケーションを活用しています。そのアプリケーション間の通信を可能にするのがアプリケーション・プログラミング・インターフェース（API）です。この API が、攻撃者にとって新たな標的となっています。何故なら、セキュリティチームが API を評価する前に、API を利用するアプリケーションやビジネスプロセスが導入および展開されてしまうことが多く、それが設定ミスや脆弱性につながるためです。攻撃者はこのようなセキュリティ上の欠陥に目を付けて、ビジネスロジックを悪用します。API 攻撃に成功すると、攻撃者は貴社の環境にアクセスして、データを盗み、さらなる攻撃を開始します。標的となるのは、Web アプリケーションファイアウォールで守られていない API だけではありません。WAF によって認証された API であっても、攻撃に対して脆弱な場合があります。現在の攻撃者は、定期的に偵察を行うことで、悪用する API を選別しています。

あらゆる API が標的になり得ることを理解しなければなりません。ヘルスケア業界等では、API を通じて IoT デバイスの相互運用性を確保しています。その API が、個人情報を盗んだり、ランサムウェア攻撃を開始したりするための標的となっています。API を保護するためにはまず、自社と関連のあるすべての API（自社の API 環境）を可視化しなければなりません。

Akamai API Security により、API 環境のインベントリを作成して、すべての API のふるまい履歴を可視化し、API の通常のふるまいと異常なふるまいを把握できます。これにより、脅威を見つけ出して、攻撃者が目的を達成する前に攻撃を迅速に阻止できます。

かつてないほど巧妙化し、容易に展開可能：悪性ボット

ボットは常に貴社の Web サイトにアクセスしています。たとえば、検索エンジン最適化とは、ボット（クローラー）に自社 Web サイトを発見してもらうための取り組みです。しかし、ボットは良性のものばかりではありません。さまざまなサイバー攻撃を行う悪性ボットも存在します。悪性ボットの行為として最も有名なのは、限定商品（スニーカー、コンサートのチケット、ホテルの予約など）の買い占めです。大量のリクエストを送信して企業のネットワークをダウンさせる分散型サービス妨害（DDoS）攻撃も、買い占めと同じような手法を用いています。

あまり知られていないかもしれませんが、今や DDoS は比較的容易かつ低コストで実行できる攻撃となっており、経験の浅い攻撃者が、数十億ドル規模の大企業や重要な公共インフラ（学校、病院、空港、電気・ガス・水道など）をダウンさせるために利用しています。このような攻撃は大規模なサービス中断をもたらし、被害者は分単位で刻々と莫大な収益を失うことになります。従来の攻撃者とは大きく異なり、こうした攻撃のほとんどは、高度なスキルを持つ国家ぐるみの攻撃者、政治的ハクティビスト、プロのサイバー犯罪者がボットネットを活用して実行しています。ボットネットとは、ボットに感染し、ボットによってコントロールされたコネクテッドデバイス（ユーザーのデバイスの場合もあれば、IoT デバイスの場合もあります）の大規模ネットワークです。

ボットは、アカウントの乗っ取りにつながる Credential Stuffing 攻撃に使用されることもあります。Credential Stuffing とは、攻撃者が大規模なデータ漏えいの際に入手したユーザー名とパスワード（認証情報）のリストを使用して、他の機関への大規模なログイン要求を行うことです。ボットを利用することで、数百万件ものアカウント乗っ取り攻撃を実行できます。多くの人は同じユーザー名とパスワードを使い回しているため、漏えいした認証情報を利用して他の機関にログインできてしまいます。攻撃者がアカウントにアクセスできれば、アカウントの乗っ取り攻撃が成功したことになります。

Credential Stuffing は、正当なアカウントを乗っ取るために攻撃者が用いる数多くの手法の 1 つにすぎません。アカウントの乗っ取りに成功したら、ロイヤルティポイントを奪ったり、デジタル資産を移動したり、ギフトカードの残高を利用したり、保存されたクレジットカード情報を用いて不正に購入したりします。乗っ取ったアカウントを別の攻撃者に売却することさえあります。貴社の顧客がこのような攻撃の被害者となった場合、貴社に対する信頼は取り返しがつかないほど崩壊することになります。Credential Stuffing は、たとえ成功しなくても、発生しただけで貴社のブランドに打撃を与える場合があります。攻撃時に貴社 Web サイトで大量のボットトラフィックが発生することで、リソースの可用性が大幅に低下し、応答時間が遅くなり、顧客やサイト訪問者の体験を低下させて、不満の原因となるためです。

スクレイパーボットには、良性のものと悪性のものがあります。しかし、いずれの場合であっても、スクレイパーボットはサイトのパフォーマンスを低下させて、重要な意思決定のための指標を歪めて、メリットよりもデメリットをもたらす可能性があります。

Akamai では、悪性ボットによる脅威を緩和するためのソリューションを多数ご用意しています。

Akamai App & API Protector（および Malware Protection モジュール）は、データ、個人情報、およびその他のアカウント情報を窃取から保護し、ボットを利用した DDoS 攻撃、ランサムウェア、マルウェアなどをブロックするための基盤となるソリューションです。このソリューションにより、貴社の顧客が貴社の Web 資産に常にアクセスできるだけでなく、攻撃を受けた場合でもサイトのパフォーマンスが低下しません。

Akamai Bot Manager により、ボットトラフィックすべてを検知して、悪性ボットをエッジで緩和できます。このソリューションは、AI モデルを用いてボットのふるまいを分析し、ブラウザーフィンガープリンティングや機械学習（ML）アルゴリズムを利用することで検知の精度を高めて、ユーザーにとってのフリクションを増やすことなく、ユーザーを不正行為から保護します。

Akamai Content Protector により、スクレイパーが貴社の Web コンテンツを盗んで悪用するのを緩和できます。また、サイトのパフォーマンス低下も緩和できます。ML 主導の検知により、悪性ボットスクレイパーがリスク別に分類されるため、その情報に基づいて適切な対応を取ることができます。

貴社の顧客を保護するためには、アカウントへのアクセスを強力に保護することも重要です。Akamai Account Protector により、人間とボットによる不正行為を阻止しながら、正当なユーザーにはフリクションレスかつ安全なアクセスを提供し、サイトの滞在時間やアクセス回数を改善できます。

悪性スクリプトの代償：クライアント側の脅威

ボットと同様、サードパーティスクリプトも多くは良性です。サードパーティスクリプトにより、特定の機能、マーケティングツール、分析などを通じて、全体的なユーザー体験（UX）を強化できます。しかし、このようなスクリプトにより、Web ブラウザーにクライアント側の脅威サーフェスが生じることもあります。

クライアント側の脅威は、貴社の顧客を騙して悪性コンテンツにアクセスさせようとします。このような脅威は、ユーザー（通常は貴社の顧客）が操作するコンピューター（これを「クライアント」と言います）上で実行されているアプリケーションの脆弱性を悪用します。これを防御するのがクライアント側のセキュリティです。クライアント側のセキュリティには、Web ページでの悪性アクティビティから顧客を保護するためのテクノロジーとポリシーが含まれています。

スクリプト攻撃により、多額の経済的損失を被り、顧客、パートナー、決済業者からの信頼を失うおそれがあります。クライアント側のセキュリティは、Payment Card Industry Data Security Standard（PCI DSS v4.0）の新しい要件でも重点分野となっています。この要件に準拠するためには、オンライン上でクレジットカードを処理するすべての組織が、自社サイトでどのようなスクリプトが実行され、そのスクリプトにいつ変更が加えられ、そのスクリプトがいつ停止したのかを把握できなければなりません。

このような攻撃を阻止するのは簡単ではありません。サードパーティスクリプトは数多く存在し、常に変化しているため、監視するのが非常に困難です。また、スクリプト攻撃には、Web スキミングやフォームジャッキングなど、さまざまな種類があります。スクリプト攻撃を用いてクレジットカード情報や個人情報を盗むことに特化した犯罪組織も存在します（最も悪名高いのが Magecart です）。

デジタル決済、オンラインショッピング、オンラインリサーチが広く普及した現在、クライアント側のセキュリティはかつてないほど重要になっています。個人情報や財務データを収集する会計／決済ページの場合は特にそうです。自社サイトで実行されるスクリプトすべてを可視化して、疑わしいふるまいを検知し、緩和策を導入することで、攻撃を阻止する必要があります。Akamai では、このような脅威に対応するためのソリューションをご用意しています。

Client-Side Protection & Compliance により、すべてのユーザーをクライアント側の攻撃（Web スキミング、フォームジャッキング、Magecart など）から保護することで、顧客のプライバシーを守り、信頼を維持できます。

インフラを保護して、顧客体験を守る

顧客体験の決め手となるのは、貴社のブランドを展開するための基盤のデジタルインフラです。必要なときに貴社の顧客が貴社のサービスにアクセスできるかどうかは、DNS のセキュリティ、信頼性、性能によって決まります。つまり、DNS システムが貴社のオンラインプレゼンスを左右することになるのです。DNS システムがダウンすれば、貴社のデジタルプレゼンスも消滅してしまいます。だからこそ、攻撃者は絶え間なく DNS システムに DDoS 攻撃を仕掛けるのです。あらゆる業界の組織が熾烈な競争に直面しています。顧客や見込み客に最高の体験を提供するためには、DNS の可用性とアップタイムを 100% の状態に維持することが不可欠です。

Akamai では、さまざまな DDoS 攻撃からデジタルインフラを保護するための代表的なソリューションポートフォリオをご用意しています。

最も強力な DDoS 防御を実現するのが、Akamai Prolexic です。このソリューションは複数の保護オプション（世界各地に 32 か所以上あるスクラビングセンター、20 Tbps の専用防御機能など）を備えています。

Akamai Edge DNS は、専用設計された総合的な権威 DNS ソリューションです。Akamai Connected Cloud のスケール、セキュリティ、キャパシティを活用して、DNS ゾーンを管理できます。

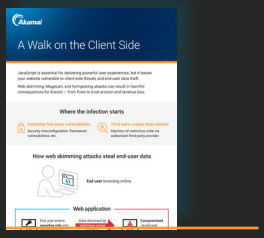
Akamai Shield NS53 は、セキュリティポリシーを動的に適用できる、双方向 DNS プロキシソリューションです。このソリューションにより、オリジン DNS インフラ（オンプレミス、クラウド、ハイブリッド）の主要コンポーネントをリソース枯渇攻撃から保護できます。

Akamai ソリューションで顧客の信頼を維持

Akamai は 25 年以上にわたって、ブランドのオンラインプレゼンスに注力してきました。コンテンツ・デリバリー・ネットワークのパイオニアとして、デジタル店舗が直面する速度の問題を黎明期から解決してきました。過去 10 年間にわたり、当社の世界最大級のコンテンツ・デリバリー・ネットワークを通じてトラフィックを可視化して、脅威を日々監視および分析し、組織的に調査することで、攻撃ベクトルの拡大や変化に合わせて当社のセキュリティソリューションを進化させてきました。Akamai は、重要なセキュリティパートナーとして、お客様のビジネスを中断させることなく、顧客体験を保護し、新しいデジタル体験を安心して導入できるよう取り組んでいます。

次のステップ

貴社のブランドを保護するための最適なステップについて検討する際には、以下の参考資料をご利用ください。



クライアント側の保護で Web ページの整合性を強化する

Web サイト、アプリケーション、API の強力なセキュリティをワンストップで提供する

ボット管理戦略の主な考慮事項を学ぶ

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。