AKAMAI 製品概要

Content Protector

巧妙化するスクレイパー攻撃から収益を保護する

コンテンツのスクレイピングによって（攻撃者が）利益を得ることも（お客様が）利益を失うこともあります。コンテンツを公に共有するという戦略的な選択において、消費者のエンゲージメントと有害なスクレイピング行為を区別することは極めて重要です。競合他社や攻撃者がスクレイプされたデータを悪用し、貴社の価格戦略を損ない、貴社のお客様に損害を与える恐れがあるからです。Akamai Content Protector は、スクレイパー攻撃特有のツールや手法に合わせて検知を実行することで、スクレイパーを即座に特定し、阻止します。スピードやパフォーマンスを犠牲にすることなく、ビジネスと収益を保護します。

オンラインビジネスにとって、スクレイピング攻撃は避けられない課題です。開始点と終了点が明確な一般的なサイバー脅威とは異なり、スクレイパーは継続的にサイトにアクセスする可能性があり、その対処を怠ると重大な影響が生じます。影響には次のようなものがあります。

- **Web サイトのパフォーマンスへの影響：**スクレイピング行為が長く続くと、サイトの速度が低下し、ユーザーの不満やコンバージョン率の低下につながります。
- **競争上のデメリット：**競合他社はスクレイピングを使用して、お客様の価格設定を監視し、それを下回る価格を提示してお客様の収益に影響を与える恐れがあります。
- **ブランドの評判へのリスク：**偽造業者がスクレイピングで得たコンテンツを悪用し、ブランド名を騙って偽物を販売することも考えられます。

言うまでもなく、スクレイパーは何年も前から存在していました。ではなぜ、今になって悪化しているのでしょうか？スクレイパー対策への緊急性は、近年になってさらに高まっています。2020 年に発生したコロナのパンデミックとそれに続くサプライチェーンの混乱は、スクレイピングを行う金銭的動機を増大させました。日用品から高級品、旅行サービスまで、需要の高い品目は、巧妙なスクレイピングの格好の標的となっています。

より多くの利益を得られる可能性があるため、ボット運用者はツールの一部（テレメトリーなど）に集中して熱心に技術革新を始め、それらを他のボット運用者が作った部分と連結して、スクレイピング攻撃に特化した高度に専門化したボットを作り出しました。その結果、スクレイパーは危険性を増し、また検知も難しくなりました。さらに、スクレイピングはプラグインのような他の手法でも発生する可能性があるため、スクレイパーを阻止するためには、単なるボット管理だけでは不十分です。

しかし、あらゆるスクレイパーをブロックすればいいというわけではありません。検索ボットは、一般検索に表示させたい新しいコンテンツを探します。また、消費者向けショッピングボットの中には、比較サイトでお客様の製品をクローズアップしてくれるものもあります。パートナーは、最新の製品情報を効率的に収集し、顧客と共有することができます。

ビジネス上のメリット

コンバージョン率の向上
サイトやアプリの速度を低下させるボットを除去し、より多くの顧客をサイトにとどめ、売上を向上させます

コスト削減
ボットトラフィックにコストをかけません

不正流通業者の阻止
スクレイパーが、サイトをチェックして、いつ人気商品の在庫が入手可能になるかを確認する行為を阻止し、ボット運用者が一連の在庫買い占め攻撃の次のステップに進むのを防ぎます

競合他社にフラストレーションを与える
自動スクレイピングを阻止することで、競合他社が価格を引き下げられないようにし、売上低下を防ぎます

偽造の緩和
執拗なスクレイピングを阻止し、偽造業者がお客様のコンテンツを取得してなりすますのを阻止します

マーケティングを強化
サイト分析からボットトラフィックを取り除き、実際のユーザーに向けて最適化できるようにします

Akamai

Akamai Content Protector は、スクレイパーを検知し、阻止するよう独自に設計された検知機能を備えています。Akamai の有するネットワークの可視性、ボット管理における Akamai の世界的な実績、および最先端の検知機能の継続的な開発を活用しながら、この機能を実現しています。脅威の進化に合わせて保護を更新し、脅威インテリジェンスの研究者やデータサイエンティストからの知見を自動的に取り入れることで、Content Protector はスクレイパーの検知において業界をリードし続けています。

スクレイパーを阻止できれば、サイトパフォーマンスやコンバージョン率の向上、競合他社の影響の軽減など、デジタルプレゼンスから最大限の効果を得ることに集中できます。

主な機能

- **検知：**クライアント側とサーバー側で収集されたデータを評価する、ML を利用した一連の検知方法。
  - **プロトコルレベルの評価：**プロトコルフィンガープリントは OSI モデルの異なる層でクライアントがサーバーとの接続を確立する方法を評価します。TCP、TLS、HTTP は、ネゴシエートされたパラメーターが、最も一般的な Web ブラウザーやモバイルアプリケーションで想定されるものと一致していることを確認します。
  - **アプリケーションレベルの評価：**クライアントが JavaScript で記述されたビジネスロジックを実行できるかどうかを評価します。クライアントが JavaScript を実行したときに、Content Protector がデバイスとブラウザーの特性とユーザー設定（フィンガープリント）を収集します。これらのさまざまなデータポイントを比較し、プロトコルレベルのデータとクロスチェックすることで整合性を検証します。
  - **ユーザーとの対話処理：**ふるまい測定では、タッチスクリーン、キーボード、マウスなどの標準的な周辺機器を介した、クライアントと人間との対話処理を評価します。対話処理が欠如していたり、異常な場合、通常、それはボットトラフィックが関係しています。
  - **ユーザーの行動：**Web サイト全体で、ユーザーの行動状況を分析します。ボットネットは通常、特定のコンテンツに狙いを定めるため、正規のトラフィックとは大きく異なるふるまいを示します。
  - **ヘッドレスブラウザーの検知：**クライアント側で実行されるカスタム JavaScript は、ステルスモードで実行されている場合でも、ヘッドレスブラウザーが取り残した指標を探します。
- **リスク分類：**評価中に検出された異常に基づき、トラフィックを低、中、高の各リスクに振り分け、実用的な形に分類します。
- **応答アクション：**単純な監視と拒否アクションを含む一連の応答戦略と、サーバーのハングアップやさまざまなタイプのチャレンジアクションをシミュレートするターピットのような、より高度な応答戦略。クリプトチャレンジは一般的に CAPTCHA チャレンジよりもユーザーがフォールス・ポジティブ（誤検知）の可能性に対処しやすくなっています。

Content Protector の基盤： Akamai のエコシステム

Akamai は、インターネットを高速で確実、かつ安全にします。Akamai の包括的なソリューションは、グローバルに分散された Akamai Connected Cloud 上に構築され、カスタマイズ可能かつ統一された Akamai Control Center を通じて管理されることで、優れた可視性と制御能力を実現します。また、Professional Services のエキスパートは、お客様がソリューションを簡単に導入し利用できるようサポートするとともに、お客様の戦略の進化に伴い、イノベーションに役立つアイデアも提供します。

デモのお申し込みはこちらへ、Akamai 営業チームへのお問い合わせはこちらから、お願いいたします。