DATA SHEET

LIMELIGHT WEB APPLICATION FIREWALL ADVANCED BOT MANAGER

ボットは検索エンジン用のクローラーやデジタルアシスタントのような自動化されたスクリプトで、インターネットに無くてはならない存在です。しかし一方で悪意を持ったボットも増加しており、インターネット上のボットの半分以上がそうした犯罪的なボットと言われています。これらの悪意を持ったボットは、サイトの脆弱性を探し、脆弱なマシンを侵害してそれをコントロール下に置き、DoS攻撃を引き起こし、データを盗み、詐欺を働きます。インターネットに不可欠なGood Botと悪意を持ったBad Botを見分け、悪意のあるボットからのアクセスを遮断しなければなりません。

Limelight WAF Advanced Bot Managerは、正規のボットトラフィックを通し、悪質なボットトラフィックを排除することによって、ウェブインフラストラクチャのセキュリティを確保し、ビジネスに役立つウェブトラフィックだけを活用し、最大限のサイトの可用性を実現します。

BAD BOTと闘うための課題

悪意を持ったボットは、あらゆる場所に存在しています。現代のハッカーは、ボットを使用して攻撃前のスキャンを行い、スパムコメントを投稿し、脆弱性を狙い、ウェブ上の資産に対するコードインジェクション攻撃やサービス無効化攻撃、パスワード推測攻撃を行います。これらのボットは、クレデンシャル・スタッフィング（パスワードリスト型攻撃）、ECサイトでの購入・キャンセルの繰り返し、注文保留攻撃、サイトスクレイピング、情報の窃取その他の不正な活動や詐欺的な行為を行います。悪意のあるボットはまた、カスタマーエクスペリエンスに影響を持つアプリケーションやAPIの停止を引き起こし、ビジネス上の損失をもたらします。Bad Botによる被害を回避するために、組織は攻撃者や悪意のあるボットに先んじて行動しなければなりません。

しかし、合法的なボットトラフィックはインターネットにとって重要であり、ボットすべてを遮断するわけには行きません。企業はトラフィックの量、時間帯、優先順位をうまく管理してGood Botを有効に利用する必要があります。正規のボットトラフィックを管理しながら悪質なボットトラフィックを排除する能力を持つことは、ウェブサイトを健全な状態に維持するためには不可欠です。

ADVANCED BOT MANAGERが課題を解決

こうした課題への回答が、ライムライトのAdvanced Bot Managerです。Advanced Bot Managerは多機能なクラウドベースのボット管理プラットフォームで、24時間365日サポートのマネージドセキュリティサービスとして提供されます。これまでのボット検知/緩和ソリューションとは異なり、導入が簡単で継続的な管理が可能な、柔軟なプラットフォームを提供します。ボット管理ポリシーを継続的に監視し、常に最適に保つことで、パフォーマンスを犠牲にすること無く、ウェブアプリケーションを守るための最適なセキュリティプロファイルを維持することができます。Advanced Bot Managerはクラウドでホストされているため、新しくハードウェアを用意する必要はありません。
またプラットフォームにはリアルタイムダッシュボードやレポート機能、解析、警告機能が含まれており、すべてのリクエストとAdvanced Bot Managerプロキシによるリクエスト処理について豊富な知見を得ることができます。

ボットの識別

ボットは自動化されたスクリプトのため、ボット防御は接続リクエストが人間から送られたものなのかマシンからなのかを見極めることから始まります。Good BotとBad Botを見分けるためためには、様々な方法があります。

CAPTCHA - Captchaは、写真、文字列、数字などのイメージを表示し、それが何かを理解した上で答えを入力して貰うことで、入力者が人間かどうかを見極めようとするものです。一般的に、スクリプトベースのボットはイメージを読み取って単語や数字に置き換えることができず、人間にはそれが可能です。

Human Interaction Challenge - 正規のユーザー/ビジターのウェブアプリケーション上での行動を解析することで「通常の」使い方のパターンを設定し、それから外れる行動、振る舞い、頻度を識別するためのカスタマイズ可能なセキュリティプロファイルを設定します。

JavaScript Challenge - すべてのクライアント、攻撃者および実ユーザーへ向けてJavaScriptによるチャレンジ（問い合わせ）を送ります。正規のブラウザーであれば、ユーザーが何もしなくともこのチャレンジを通過ことができますが、ボットの多くはJavaScriptをサポートしていないため、通過することができません。

Device Finger Printing Challenge - ウェブサイトにリクエストを送ってきたデバイスについて、50以上の属性をベースにしてシグネチャを生成します。ボットは特定の環境をコピーして使うことが多いため、同じシグネチャを持つデバイスが大量にアクセスしてくる場合、そのトラフィックはボットによるものと考えられます。

インタラクションによる識別やマシンベースのチャレンジなど、様々なボット検出メカニズムを搭載することは、Good BotとBad Botを見分けるために最適な方法です。

防御機能

IPレート制限 - これは、疑わしいボットが創り出したトラフィックを検知してその優先度を落とし、正規のトラフィックに帯域を割り当てるためのトラフィック制御メカニズムです。正規のトラフィックをホワイトリストで検知して、優先的に帯域を確保します。

Good Botのホワイトリスティング - ホワイトリストを作成し、WAFを使って既知のGood Botを識別することで、チャレンジすることなくボットトラフィックを許可します。

BOT MANAGERの導入

ボットトラフィックの管理に加え、Limelight WAF Advanced Bot Managerは導入も運用も簡単に行うことができる機能を備えています。この柔軟なソリューションはクラウドでホストされているため、ハードウェアやソフトウェアを導入・管理するためにIT部門に頼る必要はありません。ボット管理ポリシーを継続的に監視して最適化する機能により、パフォーマンスに影響を与えること無く、ウェブアプリケーションを安全に守るための最適なセキュリティプロファイルを維持することが可能です。リアルタイムのダッシュボードや解析・レポート機能、セキュリティ担当者への通知機能により、ボットによる攻撃に迅速に対応できます。

導入のメリット

- **ブランド価値を保護** - セキュリティ侵害はブランド価値に長期的な悪影響を与えます。コンシューマの40%以上が、侵害を受けたウェブサイトではオンライントランザクションを行わないと言っています。Bad Botを検知して排除し、顧客データを守るためにウェブアプリケーションセキュリティを強化することで、ブランドへの信頼を維持しなければなりません。
- **お客様との関係を維持** - コンシューマは、高速なウェブサイトを好む傾向があります。リソースを食い潰すボットを排除し、高速なオンラインエクスペリエンスを提供することで、ユーザーエクスペリエンスを向上させることができます。
- **進化するセキュリティ上の脅威に対抗** - ボット管理ポリシーを継続的に監視して最適化する機能により、パフォーマンスに影響を与えること無く、ウェブアプリケーションを安全に守るための最適なセキュリティプロファイルを維持することが可能です。

ORCHESTRATE PLATFORMについて

Limelight Orchestrate Platformは、現代の視聴者が望むエクスペリエンスを提供するための速度、機能、安定性を併せ持った世界規模のプライベートネットワーク上に構築されています。この業界をリードするプラットフォームには、コンテンツ配信、ウェブ高速化、オリジンストレージ、ビデオ管理、クラウドセキュリティ、そしてサポートサービスが含まれています。世界規模のプライベートネットワークと先進的ソフトウェア、そしてエキスパートサービスというユニークな組み合わせは他のCDNを凌駕し、ワークフローを改善してエンドユーザーのエクスペリエンスを第一に考える「Experience First」を実現します。

LIMELIGHT NETWORKSについて

Limelight Networks (NASDAQ: LLNW) は、デジタルコンテンツ配信のグローバルリーダーです。デジタルコンテンツを安全に管理し、世界中の多種多様なデバイスに送り届けることで、お客様がオンラインの視聴者とよりよい関係を築くためのお手伝いをします。詳しくは jp.limelight.com をご覧下さい。

info-jp@llnw.com | jp.limelight.com | EXPERIENCE FIRST

ライムライト・ネットワークス・ジャパン株式会社
〒107-0061 東京都港区北青山2-7-28 NAビルディング2F
TEL: 03-5771-4230