CLOUDFLARE

ホワイトペーパー

悪意のあるボットのプレイブック：早期警告の兆候と対処法

目次

はじめに

現在、オンライン上のトラフィックの約30%はボットによるものといわれています。そしてその多く（約93%）は、正体が確認されていない、貴社のような企業にダメージを与る可能性の高いボットです。最近では、コンテンツや価格情報のスクレイピング、アカウント乗っ取り、認証情報やクレジットカード情報の総当たり攻撃、在庫の買い占め、さらにはボットネットを使ったDDoS（分散型サービス妨害）攻撃など、悪意のあるボットの活動は年々高度化・巧妙化しています。

さらに、従来のボット対策として用いられるジオブロッキング、IPアドレスブロッキング、従来のCAPTCHAなどでは効果がありません。実際のところ、今では人間よりもボットのほうがCAPTCHAを簡単に突破できるほどです[1]。

そのため、1つの戦略だけで、すべてのボットを抑止したり、従業員やブランドへの悪影響を防止したりすることはできません。唯一効果のあるアプローチは、ボットであることを示すさまざまな兆候に注意を払い、データを収集して、的を絞った措置、パターン検出、予測分析、そのほかの補完的な戦略を講じることでそれぞれのボットに対処することです。

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

ボットの問題を示す兆候

さまざまな潜在指標を追跡することで、深刻なダメージを受ける前に、悪意のあるボットを特定できる確率が高まります。次のような兆候がないか確認しましょう：

業績の向上がないにも関わらずインフラコストが増加している

Webサイトへのすべてのトラフィックに何らかのコストがかかります。そのアクセスが何者から（人間またはボット）のものであっても、ストレージや計算処理にかかる費用負担は必ず発生します。しかし、悪性ボットは、収益をもたらすことなくトラフィックに関連するコストだけを増大させます。良性ボットは、検索エンジンがサイトのコンテンツインデックス作成に使用するため検索順位を上げますが、悪性ボットは帯域幅を過剰に消費して利用料金を増大させます。

需要が高く供給量が少ない商品在庫の異常な購入

在庫の不審なほど大きな割合が一握りの買い手に販売されている場合、ボットによる不正買い占め（インベントリホーディング）である可能性があります。正当な顧客からの購入を阻止するために単に買い物かごを満杯にして放置するだけのボットもあれば、他のサイトで高く転売するために実際に商品を購入するボットもあります。

顧客からのクレームの増加

アカウントロックアウトや不正取引に関連した問い合わせ件数の増加は、ボットを使用したクレデンシャルスタッフィング攻撃の兆候である可能性があります。こうしたボットは、過去の情報漏えいで入手した情報を使用して正当なユーザーのアカウントを乗っ取ります。こうした不正取引は、顧客体験を損なうだけでなく、サーバーを過負荷状態にし、ページ読み込み時間を遅くしたり、場合によってはWebサイトをクラッシュさせたりすることがあります。

失敗したログイン試行回数の増加

どれほど慎重な顧客もパスワードを間違えて入力してしまうことはありますが、失敗したログイン試行回数が急増した場合は、ボットの問題である可能性が非常に高いです。クレデンシャルスタッフィング攻撃を実行するボットは、盗んだ認証情報を用いて正当な顧客のアカウントにアクセスしようとします。これは、ブルートフォース攻撃を仕掛けるためのより簡単で一般的な手口であり、ボットは人気のある数千のユーザー名やパスワードが掲載された辞書を使用してログインを矢継ぎ早に試行します。ボットが特定のアカウントに対するサイトの試行回数の上限を超えると、そのアカウントの正当な所有者は問題が解決するまでロックアウトされてしまいます。これは、ユーザー体験を低下させる大きな要因となります。

広告費に対して売上が低い

デジタル広告は、サイトへのトラフィックを高める効果的なツールですが、悪性ボットにとっては金儲けの武器です。多くのトラフィックボットは人間のユーザーの行動を模倣し、広告を繰り返しクリックしてクリック課金（PPC）の費用をつり上げておいて、結局何も購入せずにサイトを離れます。一部の広告プラットフォームは、クリック詐欺を軽減するために機械学習アルゴリズムを導入していますが、詐欺の多くは検出されていません[2]。
そのため、事前予防的なアプローチで、出した広告のクリックを逐一監視することが重要です。

偏ったページビュー分析

ページビュー数が特に理由もなく急増した場合も、悪性ボットが原因である可能性があります。新製品やイベントプロモーションを告知した直後ならトラフィックの急増が人間のユーザーによるものである場合もありますが、悪意のあるボットのオペレーターはコンテンツスクレイピングボットをそうしたタイミングに合わせて巧妙にデプロイすることで、コンテンツを盗んで集計分析データに悪影響を及ぼします。

アカウント作成の急激な増加

数百または数千という新規ユーザーアカウントが突如出現した場合、ボットが原因である可能性があります。偽プロフィールを使ってスパムを送りサイトのユーザー評価を下げたり、その他さまざまな形の不正行為を行ったりして、利益やユーザーの定着率だけでなく、ブランドの信頼性をも脅かします。

承認されていないサイトでの重複コンテンツ

お客様のコンテンツを他のサイトが共有することは良い場合もありますが、完全に重複するコンテンツの急増は、ボットによるコンテンツスクレイピング攻撃の特徴です。こうしたボットは、お客様が時間をかけて収集して整理した情報を盗み、悪意のあるサイトオペレーターが所有するドメインでホストできるようにします。その結果、そうしたサイトのアクセス数はぐっと伸びて、お客様のサイトは打撃を受けます。

不審な地理的位置から発生するトラフィック

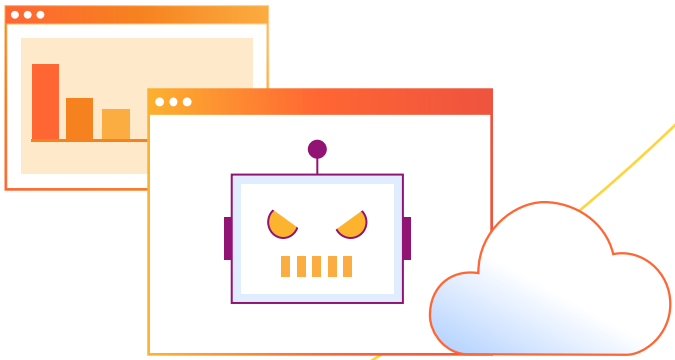
予期しない場所から発生するトラフィックの急増は、悪性ボットの仕業である可能性があります。お客様の顧客が住んでいない地域や、サービスを提供していない地域に集中している場合はなおさらです。通常のユーザーベースと無関係と思われる不審なアクティビティに注意してください。

通常の場所からでも異常な時間帯に発生するトラフィック

予期しない場所からのトラフィック急増が悪意のあるボットの仕業かもしれないように、通常の場所からでも異常な時間帯に発生するトラフィックは、ボットが通常のユーザーになりすまそうとしていることを示唆している場合があります。たとえば、通常の場所であっても真夜中に発生するトラフィックについては、より詳しく調べる必要があります。

カード検証に失敗した件数の増加

悪性ボットの兆候の中で、特に危険なのは、クレジットカード取引の検証に失敗した件数が増加するものです。ボットによるクレジットカードスタッフィングは、盗まれた数千のクレジットカード番号を試して機能するものを見つけようとします。安全性の低いWebサイトで低額の購入取引を実行してから、より規模の大きいサイトでより高額の取引を実行するか、または検証できたカード番号をダークウェブで転売します。こうした攻撃のどの段階においても貴社のサイトは標的になり得ます。検証に失敗した件数があまりに多いと、ペイメントプロバイダーは貴社に罰金を科す場合があります。



2. https://www.entrepreneur.com/article/313943

ボットと戦うための戦術

二つとして同じボット攻撃はないので、すべての攻撃を効果的に阻止するには通常、複数の戦術を組み合わせる必要があります。次のような戦略を検討してみてください：

見つけたらすぐに悪性ボットをブロックする

ボットに対する最も効果が自明な対策は、悪意のあるボットのアクティビティとして特定したすべてのトラフィックを単純にブロックすることです。この戦術だけでも、帯域幅とストレージのコストを大幅に節約できます。顧客の信用とブランドの評判を守ることができることは言うまでもありません。同時に、ボットのオペレーターがその気になれば、戦術を変えて異なる攻撃戦略を再度仕掛けてくる可能性があることを覚えておいてください。

既知の良性ボットをすべて許可リストに追加する

悪性ボットを検出してブロックする場合でも、検索エンジンやパートナーからの良性ボットが貴社のサイトを引き続きスクレイピングできるようにすることが重要です。そうすることで、SEO順位を維持するだけでなく、貴社にトラフィックを差し向けるサードパーティサービスからの正当な顧客のトラフィックがスムーズに流れるようにすることができます。許可に追加することで、人間の訪問者のアクセスに悪影響を及ぼさないボットブロックルールをより簡単に設定できるようになります。

検出した不審なボットの身元を確認する

ログインのパターンが不審である、ページのクリック深度が低い、クレジットカードの検証に失敗した、というような典型的なボットの動作に気付いたら、すぐにセキュリティテストを実装することが重要です。以前は、そのような状況下ではCAPTCHAチャレンジが最善策と見なされていました。しかし現在では、高度なボットの多くが、このような認証テストを人間よりも速く、しかも正確に解くことができるようになっています。

現在の最も効果的な方法は、「CAPTCHAを使わない認証方式」を採用することです。この方式では、ネットワーク情報、デバイス、JavaScriptのフィンガープリントなど、さまざまな要素を分析し、アクセスしているのが本当に人間なのか、それともボットなのかを自動的に判定します。
このような「CAPTCHAを使わない認証」は、最大限の精度を得るために、完全なボット管理ソリューションと組み合わせて運用することが理想的です（詳細については結論を参照）。

ユーザーが情報を求めるリクエストの数を制限する

レート制限は、あまり高度でないボットを寄せ付けないようにするのに効果的な手法である場合があります。IPアドレスが貴社のサイトに送信できる要求の回数を制限することで、数千の辞書の単語や一般的なパスワードを使用してサインインしようとする、多くの単純なボットによるブルートフォース攻撃を防止することができます。しかし、今日のより高度なボットは、要求の数がレート制限をわずかに下回るようにして、検出されずにダメージを与え続けることができます。

すべてのサイトトラフィックの詳細なログを残す

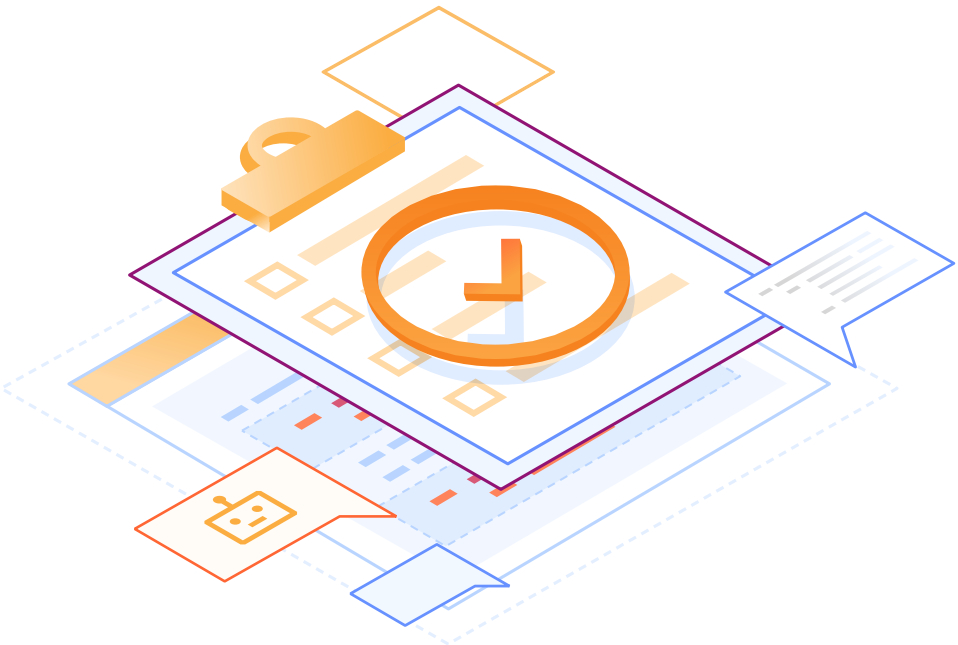
ページビューやアカウントログインの日次ログはすでに維持管理していると思いますが、IPアドレス、ブラウザー、デバイス、OS、位置情報、参照元、ネットワーク、ページビューといったユーザー情報のより詳細なログは、より巧妙なアクティビティパターンを検知するのに欠かせない情報となります。ログは、貴社のサイトにおいてボットがどのように動作する傾向があるかを把握するために必要な道具であり、より効果的なセキュリティポリシーを設定できるようになります。また、多くの場合、実際にデータ漏えいが発生した場合、ログはレポーティングやコンプライアンスにとって極めて重要なものになります。

ボットを代替コンテンツにリダイレクトする

特定の発信元からのトラフィックがボットである可能性がかなり高い場合、代替えコンテンツをボットに与え、そこで計算リソースを消費します。間違った価格情報といった偽のデータをコンテンツスクレイピングボットに提供して、データがオペレーターにとって無益なものになるようにすることができます。こうした手法をとることは、各ボットの動作を観察する、アクティビティのパターンを把握する、ボットを撲滅するための戦略を準備する、といったことを行うための時間稼ぎになります。

すべてのユーザーに追加の認証を要求する

ボット攻撃が顕在化するにつれて、正当な人間のログインであっても、より多くのサイトがセキュリティ対策を強化するようになっています。たとえば、二要素認証（2FA）では、複数のデバイスまたはアカウントでユーザーの本人認証を行います。一方、ワンタイムパスワード（OTP）は、アカウントにアクセスしにくくすることで、ボットによるクレデンシャルスタッフィング攻撃を阻止します。ただし、こうした手法は、ログインプロセスを煩わしいものにするので、ユーザー体験に悪影響を及ぼす可能性があることを覚えておいてください。

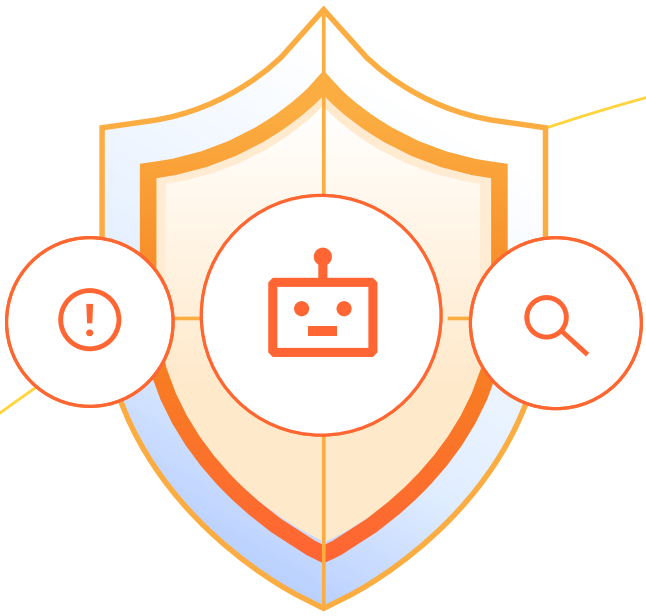


結論

こうした戦術を検討するときは、どの戦術も単独ではすべてのボットを阻止できないという点を忘れてはなりません。お客様が自社のビジネスを保護するためには、複数の戦術を組み合わせて、高度な多変量パターン解析を加える必要があります。Cloudflareボット管理は、多岐にわたる業界の企業がこうした多面的な対策を採用するのに役立ちます。全世界の330以上の都市に展開し、数百万のインターネットプロパティをサポートする広範なCloudflareネットワークに組み込まれています。

Cloudflareボット管理は、そのネットワーク全体から継続的に得られる脅威インテリジェントを利用することにより、挙動分析、機械学習、クライアント側のフィンガープリンティングを提供し、悪性ボットとの戦いの大方を肩代わりします。さらに、Cloudflareは、「Turnstile」という、わずか数行のコードで、あらゆるWebアプリケーションに統合できる、ユーザーにほとんど負担を感じさせないCAPTCHA不要のボットチャレンジを提供しています。

Cloudflare Bot Managementの詳細をご確認ください。



enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

REV:BDES-6333.2024SEPT03