悪質なボット：
詐欺実行の第一歩

ボットは、基礎的なコストと反復するタスクを減らし、ビジネスインテリジェンスと顧客とのエンゲージメントを向上させます。しかし同時に、攻撃者側の攻撃のコストを削減し、規模を拡大させもします。問題となるのは、ボットの目的です。人間の見込み客なのか、SEOの改善を目的とした検索エンジンのボットなのか、それともアカウントの乗っ取り、詐欺による損失、ビジネスの悪化につながりかねない自動化されたクレデンシャルスタッフィング攻撃のボットなのかを見極める必要があります。

安全なボット

検索エンジンボット
インターネットをクロールして、検索エンジンで使用されているデータを収集します。

アグリゲーターボット
サードパーティの情報を収集・伝播します。

商用ボット
マーケティングオーディエンスの最適化のために、ニュース報道や、カスタマーレビュー、広告ネットワークをモニタリングします。

チャットボット
テキストや音声で人間と同じようなサービスを提供し、問い合わせに応えます。

悪質なボット

クレデンシャルスタッフィング
盗み取られたクレデンシャル（認証情報）を利用して、大規模なアカウント乗っ取りを自動で実行します。

偽アカウント
オンラインバンキングからマネーロンダリングを実行し、ポイント/キャッシュバックプログラムを侵害します。

クレジットアプリケーション詐欺
本人になりすまし、につながりかねない不正取引を実行します。

ギフトカードの不正利用
ギフトカードの残高を調べて、盗み出します。

スクレイピング
専有データを収集します。結果として、知的財産の窃盗など、ビジネスにマイナスの影響が生じる可能性があります。

アプリケーションサービス拒否（DoS）攻撃
パフォーマンスを低下させ、ユーザーエクスペリエンスに悪影響を及ぼします。結果として、収益や顧客の喪失につながる可能性があります。

アグリゲーター詐欺
詐欺を働くために、銀行に侵入するバックドアとしてアグリゲーターを利用します。

ボット攻撃の検出

安全なボットはビジネスにメリットをもたらします。いっぽう、悪質なボットはビジネスに打撃を与える可能性があります。すべてのボットをブロックするのは現実的な選択肢ではありません。業務の中断と詐欺の発生につながる前に、既存客と潜在客に対する摩擦を生じさせることなく、悪質なボットを検出し、ブロックするにはどうすればいいのでしょう？

1 トラフィックのレートを制限し、Webサイトでの正規トラフィックの流れを止めることなく、疑わしいトラフィックを調査します。

2 動的に更新されるシグネチャーを利用して、既知のボットを特定します。

3 リバースドメインネームシステム（DNS）ルックアップを利用して、検索エンジンリクエストの正当性を確認します。

4 リクエストが自動化スクリプトからのものでないことを確認します。

5 大量のトラフィックや不規則なトラフィック、および非準拠の検索を利用した機密ファイルや機密データへのアクセスの試みといった、疑わしい動きがないかどうかチェックします。

6 これらの方法を組み合わせて、ポイントを調整することで、セッションにリスクスコアを割り当てます。そのうえで、危険なクライアントに対し、いつどのようなアクションを起こせばいいのかを判断します。

7 デバイス、ネットワーク、環境のシグナルを分析して、ログインの成功率、ユーザー1人あたりのデバイスの数、デバイス1台あたりのユーザーの数、およびIPアドレス、ユーザーエージェント、セッションデータの変動などの異常な動きを見つけます。

8 類似した攻撃プロファイルとリスク領域を持つ組織を基準に、人工知能（AI）と機械学習（ML）を利用して、人間の行動を検出します。

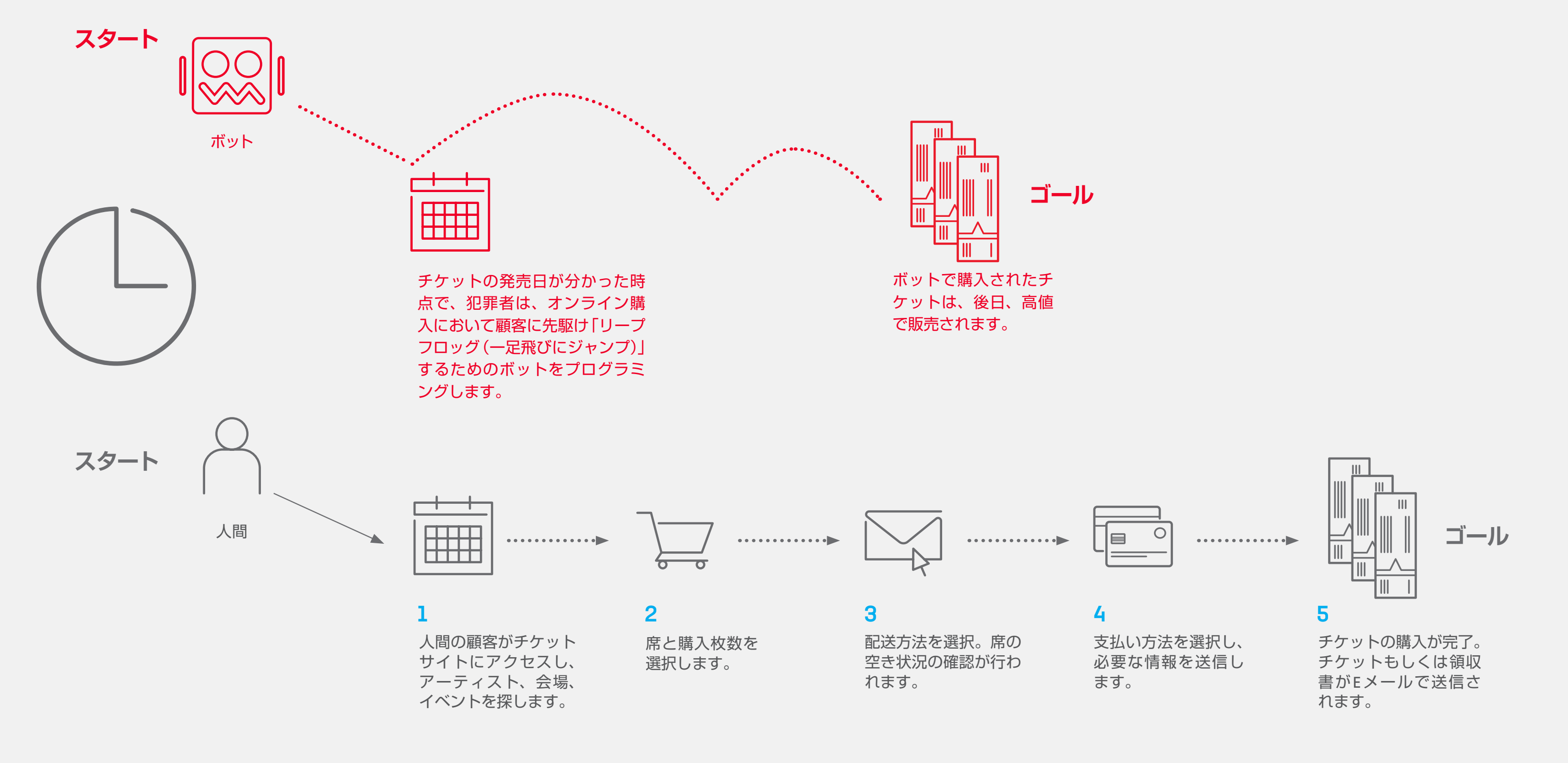
9 完全な有効性を確保しつつ、対策を迂回しようとする攻撃者に対応します。

10 ボットを利用した自動化攻撃の標的となることが増えているAPIとモバイルアプリにまで、防御の範囲を拡大します。

人間および安全なボットを受け入れ、悪質なボットを除外する

こちらのシナリオは、オンラインでチケットを購入するというものです。ボットがチケットを手に入れる前に、人間がチケットを購入することができません。チケットが完売した場合、後日、詐欺師はより高額でチケットを販売できます。

オンラインチケット争奪戦



チケットの発売日が分かった時点で、犯罪者は、オンライン購入において顧客に先駆け「リープフロッグ（一足飛びにジャンプ）」するためのボットをプログラミングします。

ボットで購入されたチケットは、後日、高値で販売されます。

1 人間の顧客がチケットサイトにアクセスし、アーティスト、会場、イベントを探します。

2 席と購入枚数を選択します。

3 配送方法を選択。席の空き状況の確認が行われます。

4 支払い方法を選択し、必要な情報を送信します。

5 チケットの購入が完了。チケットもしくは領収書がEメールで送信されます。

ボットの時代を勝ち抜くためには

悪質なボットトラフィックをブロックすることで、カスタマーエクスペリエンスを最大限高めつつ、優れたビジネスインテリジェンスを獲得し、詐欺を防止することができます。

ビジネスにフォーカス

1. ボットトラフィックによって生じる法外なクラウドの課金とセキュリティチームの混乱を防止。
2. データの漏洩やアカウントの乗っ取りにつながる可能性のあるクレデンシャルスタッフィング攻撃を阻止。
3. ボットと自動化を利用して人間の行動を模倣する巧妙な詐欺を抑制。

ボットに打ち勝つことで…

人間行動のロジックを理解：
類似の攻撃プロファイルとリスク領域を持つ組織を基準に、人工知能と機械学習を利用して、ヒューマントラフィックとノンヒューマントラフィックを検出し、意図を見極めます。

侵害被害の一番乗りを避け、市場への一番乗りを目指す：
ボットや自動化攻撃の標的となることが増えているモバイルアプリケーションとAPIを保護します。

既存客と潜在客の両方を保護：
ユーザーのブラウザーやモバイルデバイスから機密情報を直接盗み出す攻撃を防止します。

ユーザーエクスペリエンスの保護：
顧客に満足してもらいつつ、正確なアナリティクスを実行するために、顧客に摩擦を生じさせることなく、悪質なボットを検出・ブロックします。

プロアクティブで多層的なボット対策は、組織のアプリケーションセキュリティの最適化にどう役立つのでしょう。https://www.f5.com/ja_jp/solutions/application-security/bot-management で詳細な情報をご覧いただけます。