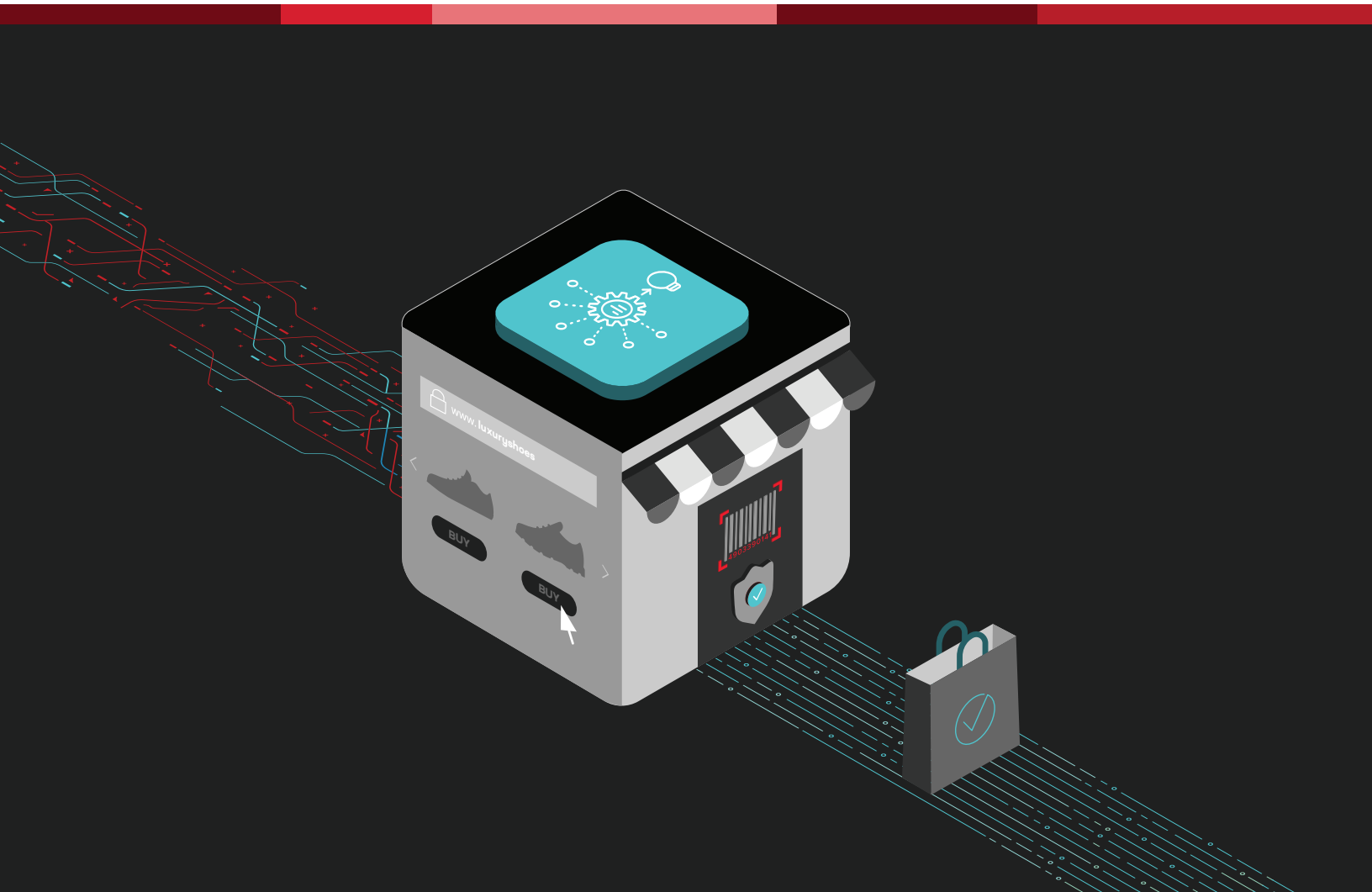
ケーススタディ

小売企業がシューズボットの急増を解決：不正行為、摩擦、偽造を解消



困難な状況：5 つの課題

- 不正行為とチャージバック
- BOPIS を悪用した窃盗
- シューズボットによる買い占め
- サーバーの停止
- ギフトカードのクラッキング

顧客

北米のある百貨店チェーンは、高級感、伝統、顧客満足を象徴する強固なブランドを確立しています。この企業は、北米に店舗を構え、アジア太平洋地域にも多くの店舗を展開しています。

この小売企業は、革新により店舗とオンラインの両方で顧客体験を向上させることを確固たる信念としていて、簡単なログイン、使いやすいギフトカード、支払い情報の保存など、摩擦のないショッピング体験を提供することに努めています。また、Buy Online Pick-up In Store（BOPIS）（オンラインで購入し店舗で受け取り）のパイオニアでもあります。

この小売企業は、その主力プロモーションの一環として、著名人お墨付きの有名ブランドの限定スニーカーを大々的に宣伝しています。

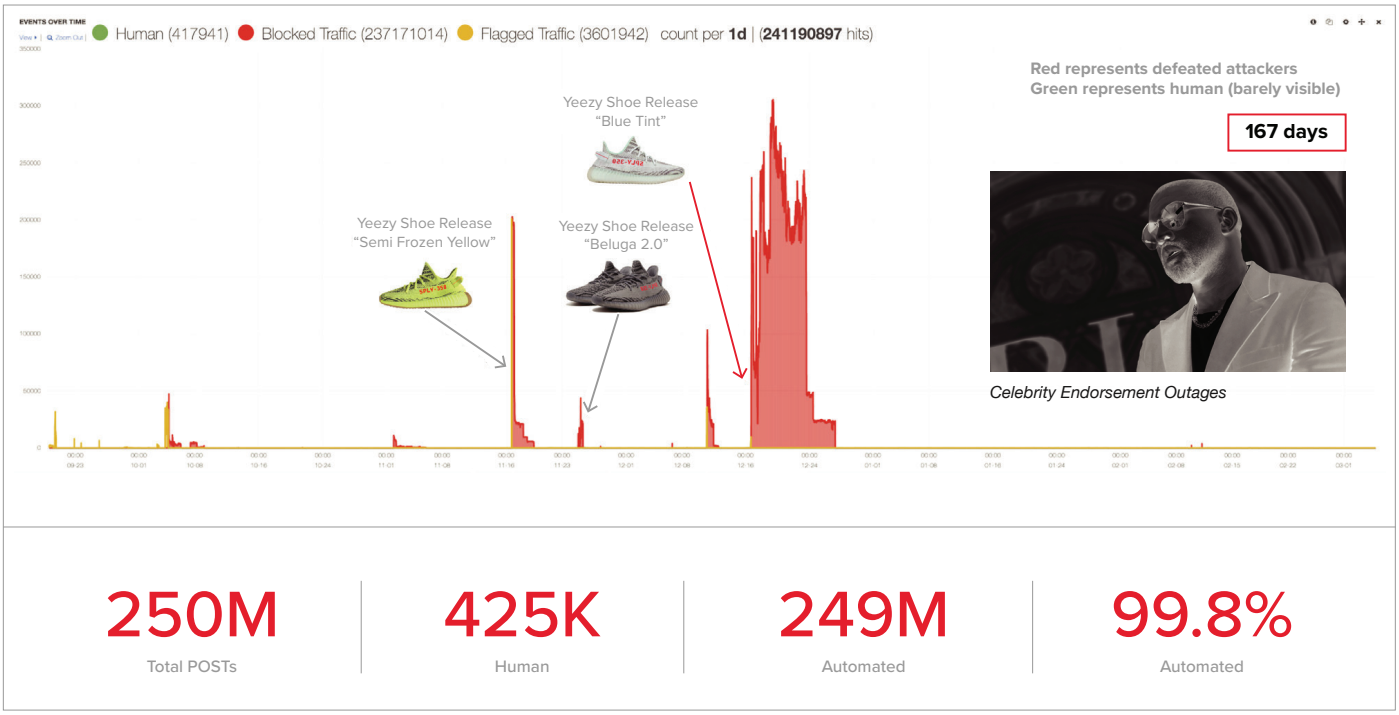


図 1：攻撃トラフィック

最初の 30 日間で 50 万ドルを節約

課題：不正行為と摩擦

この小売業者は、摩擦のないショッピング体験を提供することに努めていましたが、これが、自動化を利用する強欲な攻撃者に扉を開くことになり、同社の IT 部門と損失対策部門は 5 つの課題に直面することになりました。

課題 1：不正行為とチャージバック

攻撃者は、この小売企業に対してクレデンシャルスタッフィングキャンペーンを仕掛け、流出した認証情報によるログインを利用してアカウント乗っ取り（ATO）を行い、保存されている支払い情報を悪用して高価な高級品を購入していました。これにより、この小売企業は、攻撃者に 1 回、顧客へのチャージバックでもう 1 回と 2 回支払う羽目になっていました。さらに悪いことに、顧客の信頼を失っていました。

課題 2：BOPIS FRAUD

攻撃者は、この小売企業の BOPIS システムにも攻撃を仕掛け、侵害されたアカウントから保存されている支払いデータを使用してオンラインで商品を購入した後、被害者を受けた顧客が不正請求に気付く前に、運び屋を店舗に向かわせ商品を回収していました。

課題 3：シューズボットによる買い占め

この小売企業は、限定スポーツシューズの特別プロモーションを定期的に行っていました。商品提供は数百足程度でした。消費者はこれらの商品を「ドロップデー」に買おうと楽しみにしていたのですが、自動化されたシューズボットが発売後数秒以内ですべての在庫を買い占めてしまうため、直帰率が上がり、実際の人間のユーザーにストレスを与えました。

課題 4：限定シューズに起因するサーバーの停止

キャンペーン期間中、シューズボットは、この小売企業のオンラインストアに容赦なく攻撃を仕掛けました。この小売企業は、靴の販売に関連するトラフィックのほとんどが自動化されていることを知っていましたが、人間とボットの区別はできていませんでした。自動化された大量のクエリが洪水のように押し寄せ、内部サーバーエラーが多発する深刻な混乱を引き起こしました。これは、靴だけでなく、他のすべての商品のコンバージョンに影響を与えました。

課題 5：ギフトカードのクラッキング

不正行為者は、16 桁のギフトカード番号の組み合わせを何百万通りも試し、購入済みの未使用カードを探しました。攻撃者はカードをクラックすると、残高を合わせる、または商品を買うなどして、価値を奪いました。

「CAPTCHA は、まったく効果がなく、直帰率やカート放棄率を上昇させるだけです。」
- 同小売企業 CIO

決定

この小売企業は、まず従来の対策で攻撃者に対抗しようとしました。チェックアウトプロセスに CAPTCHA を追加しましたが、結果は求めていたものとは逆になり、不正行為を大幅に減らすどころか、ユーザー体験の摩擦が増え、実際の人間のユーザーのショッピングカート放棄率が上がってしまいました。

また、IP アドレスによるブロックも試みましたが、攻撃者はすぐにこれに適応してプロキシを使ってブロックを回避してしまい（この目的でのプロキシのコストは 1,000 IP あたりわずか 2 ドル）、一方で IT スタッフメンバーは、ブラックリストの管理に手一杯になり他の仕事の時間がなくなってしまいました。さらに、地域別のブロックを試みましたが、偽陽性率があまりにも高く、これも不正行為の大幅な減少には至りませんでした。

最終的に、顧客体験ジャーニーに摩擦を加えることなく不正行為を未然に防ぐことができる F5® Distributed Cloud Bot Defense を採用することにしました。

この小売企業は以下のような特徴を持つソリューションを必要としていました。

- 利便性を維持する（支払い情報の保存）
- 摩擦がないユーザー体験
- 偽陽性率が低い

成果

「F5 がブロックモードに移行した初日から、自動化による不正行為は、100%近く減少しました。」
- 同小売企業 CIO

Distributed Cloud Bot Defense の導入には、観測と軽減の 2 つの段階があります。観測モードでは、F5 は、受信リクエストを分析し、この小売企業のトラフィックプロファイルを学習して、カスタマイズされた防御策を作成します。F5 とクライアントは、Distributed Cloud Bot Defense を軽減モードに移行する前に、偽陽性率が低い最適な防御策を協力して検討します。

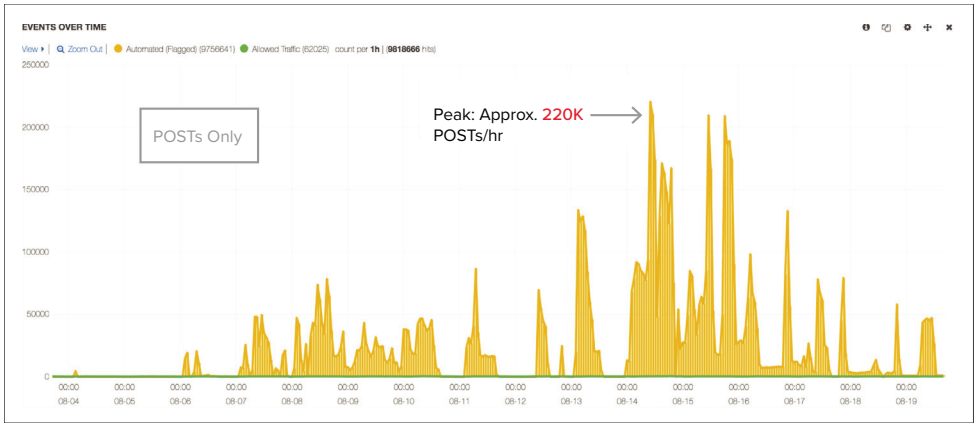
この小売企業は、Web トラフィックの大部分が自動化ではないかという疑念を抱いていました。限定シューズのプロモーション期間中、ページリクエストの 99.8% は自動化でした。また、この小売企業のギフトカード残高ページへの訪問者の 98.5% はボットでした。全体として、この Web プロパティのページリクエストの自動化は 97% でした。

「F5 のおかげで初めて、偽の顧客、つまり偽の人間であることがわかりました。100 回中 99 回、ギフトカードの残高を確認しようとする行為は攻撃者によるものでした。」
- 同小売企業 CIO

観測モードでは、Distributed Cloud Bot Defense は、何千ものアカウント乗っ取り（ATO）の成功を記録しました。ここから、年間にして 5 万件以上の ATO が発生すると予測されました。攻撃者のクレデンシャルスタッフィングキャンペーンは、1 時間あたり 25 万件以上のリクエストでピークに達していました。

3 週間の観測期間を経て、F5 と小売企業は軽減モードに移行しました。結果はすぐに現れました。その後 30 日間で、この小売企業は、アカウント乗っ取りやギフトカードのクラッキングによって失われていたはずだった 50 万ドル以上の不正行為を回避できました。

攻撃者は、F5 の防御を 2 度回避しようと試みました。しかし、Distributed Cloud Bot Defense は、数百のクライアント信号を使用して攻撃者を追跡するため、攻撃者は自動的に発見され、再びブロックされました。この小売企業は「顧客は忠実ですが、不正行為者はそうではなく、一度阻止したら、去っていきました。」と語っていました。



F5 によって自動化攻撃者が撃退され、オリジンサーバーには人間の訪問者だけがアクセスするようになりました。負荷は以前のわずか 1% になりました。トラフィックの 99% を削減することで、Distributed Cloud Bot Defense は、「インフラストラクチャから大きな負担を取り除き、収益に直接好影響を与えました」。

内部サーバーエラーがなくなり、実際の顧客は再び限定スポーツシューズを購入できるようになりました。この小売企業は、サイトのあらゆる部分から CAPTCHA を取り除き、ユーザーの摩擦をなくし、スムーズな顧客体験ジャーニーを取り戻したことに満足していました。

革新の自由

最後に、おそらく最も重要なことですが、「アカウント乗っ取りからギフトカードのクラッキングまで、あらゆる種類の不正行為が F5 により効果的に阻止された」後、この小売企業は、スタッフの労力を顧客に向けて解放し、インタラクティブな体験やプロモーションを提供して、革新という確固たる信念に戻ることができました。

詳しくは、F5 の担当者にお問い合わせいただくか、f5.com をご覧ください。