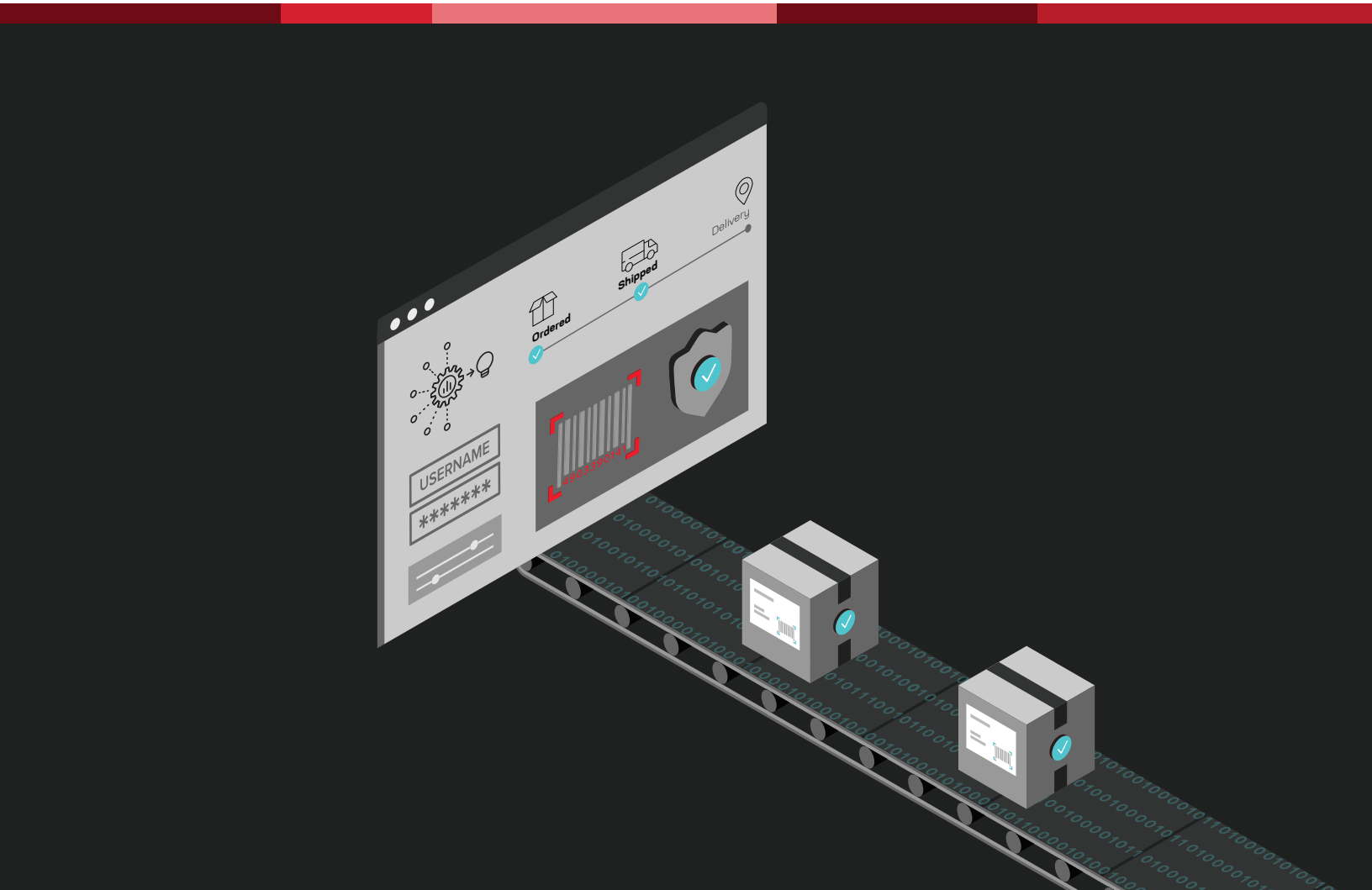
ケーススタディ

宅配業者が不正輸送を防止



攻撃トラフィックは 1 日で 10 万件を超えました

顧客：トップ 5 の宅配業者。年間 500 億ドル以上の売上を誇る世界トップ 5 の宅配業者（以下「プロバイダ」）は、顧客をアカウント乗っ取りから守り、不正アカウント作成を防止したいと考えていました。

課題 1：アカウント乗っ取り

このプロバイダは、クレデンシャルスタッフィング攻撃から Web およびモバイルアプリケーションの顧客ログインを保護したいと考えていました。クレデンシャルスタッフィングとは、犯罪者が第三者から盗んだ認証情報をログインアプリケーション上で一斉にテストし、アカウント乗っ取りを行う攻撃です。攻撃者は、盗まれた認証情報の膨大なリストを入手します。そして、ユーザーがパスワードを使い回すため、このリストの約 0.1% ～ 2% がターゲットサイトで有効であることを一般的に知っています。

このプロバイダでは、8 か月の間で、持続的な自動化トラフィックに加え、大量の自動化スパイクの波が 3 回発生しました。攻撃トラフィックは 1 日で 10 万 POST を超えることもあり、これは正規のトラフィックを 50% 上回るスパイクでした。
2017 年秋にネイティブモバイル API の大規模なアップグレードをリリースしましたが、これも頻繁に攻撃されました。

攻撃を受けたプロバイダは、顧客から盗まれた資金だけでなく、アカウントにリンクされたクレジットカードを使用した不正取引によるチャージバック料金も返金しなければなりませんでした。クレデンシャルスタッフィング攻撃自体でも、このプロバイダの損失となり、顧客がヘルプデスクに押し寄せ、荷物が届かない、またはアカウントがロックされた（攻撃者からの過剰なログイン試行失敗が原因）などの苦情が殺到しました。

課題 2：不正アカウント作成

このプロバイダは、不正アカウント作成に基づく 2 つの異なる手口の攻撃にも悩まされていました。1 つめの手口は、富裕層の郵便番号の住所を使い、公開されている利用可能な個人情報を使ってナレッジベース認証の質問に正しく回答することで、プログラムにより偽アカウントを作成するものでした。その後、攻撃者は、このプロバイダが提供する荷物の追跡と発送通知の無料サービスを利用して、荷物を盗み、それらの多くを転売していました。

2 つめの手口は、偽アカウントを作成し、盗んだクレジットカードをそのアカウントに紐づけるというものでした。攻撃者は、偽のアカウントを使って配送ラベルを購入し、送料の割引や荷物の転送などのサービスを違法なマーケットプレイスで宣伝していました。クレジットカードを盗まれた被害者がこの不正行為に気づいた場合、宅配業者は送料を返金しなければならず、場合によってはクレジットカード発行会社にチャージバック料金を支払わなければなりません。

F5 が選ばれる理由

F5 Distributed Cloud Bot Defense が採用された主な 3 つの理由：

1. 巧妙な攻撃者を長期的にブロックでき、不正行為につながる悪意ある行為を特定可能
2. Web、モバイル、API エンドポイントを含むオムニチャネルの保護
3. プロバイダのセキュリティチームの拡張部となり、望ましくない自動化をすべて停止させるという、望ましい成果を実現することに特化したフルマネージドサービス

解決策

このプロバイダはまず、これらの課題を解決するために独自のソリューションを構築しようとしました。Web アプリケーションファイアウォール、ロードバランサ、分析ツールを組み合わせて使用し、ヘルプデスクのチケットと顧客の苦情を関連付け、パスワード再設定を強制的に行うことで問題を解決しようとしました。この DIY のアプローチは、自動化された攻撃を軽減する効果はなく、不正行為はなくなりませんでした。

自力で問題を解決できなかったため、F5® Distributed Cloud Bot Defense を採用して、Web とモバイルの両方のログインとアカウント作成アプリケーションに導入することにしました。

成果

一般的な Distributed Cloud Bot Defense の導入には、観測モードと軽減モードの 2 つの段階があります。観測モードでは、F5 はアプリケーションに送られるすべてのリクエストを分析して、防御をカスタマイズし、自動化されたトラフィックにフラグを付けます。軽減モードでは、自動化の性質とプロバイダのニーズに基づいて、F5 がプログラムによるアクションを実行します。

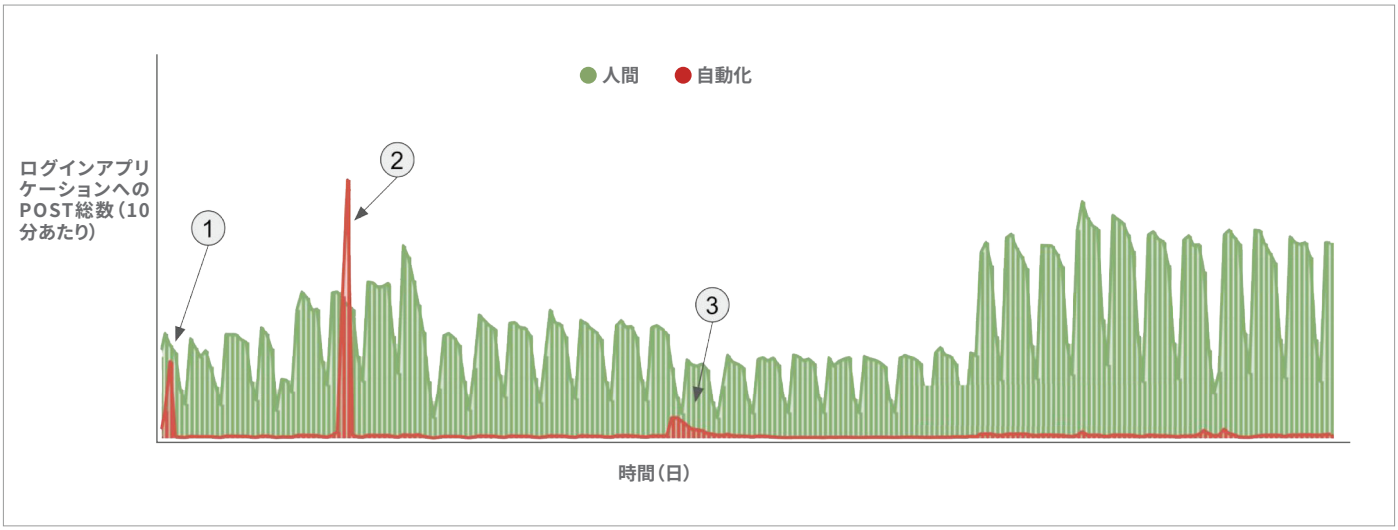


図 1：観測モード時のログイントラフィック

観測モード

Distributed Cloud Bot Defense が観測モードに入るとすぐに、ログイントラフィックの本質をすべて確認し理解できました。図 1 に示すように、このサービスにより、観測モード中のログインアプリケーションにおける、人間による正規のトラフィック（緑）と望ましくない自動化（赤）が区別されました。

また、Distributed Cloud Bot Defense により、自動化されたトラフィックのソースに関するインサイトを含む、高度な脅威インテリジェンスレポートがこのプロバイダに提供されました。これにより、たとえば、これまではわからなかった、自動化された行動の半分が無害であることが確認されました。

さらに、観測モード中、Distributed Cloud Bot Defense は、図のラベル 1、2、3 で示された 3 つの独立した自動キャンペーン [1] を特定しました。これらのグループは、全観測期間中の自動化されたトランザクションのほぼ半分を占めていました。攻撃グループが、たとえば、トラフィックをルーティングする新しいプロキシを利用する、あるいは異なるタイプのブラウザを模倣することで、Distributed Cloud Bot Defense を回避しようとしても、他の信号に基づいて攻撃グループを特定できます。

このプロバイダの推定では、F5 が消費者ログインとアカウント作成アプリケーションを保護することで、不正行為による損失を少なくとも年間 350 万ドル削減できました。

また、F5 は、各キャンペーンを詳しく調べました。図 2 は、このプロバイダに仕掛けられたキャンペーン #2 に焦点を当てた図です。このキャンペーンは、25,000 以上の IP アドレスから仕掛けられた、高度に分散されたクレデンシャルスタッフィング攻撃でした。この攻撃は、3 日間にわたるキャンペーン期間中、全トラフィックの 50% 以上を占めていました。このキャンペーンは、攻撃者がログインフローを超えてワークフローをナビゲートしようとした点でも注目されます。

軽減モード

約 6 か月の観測期間を経て、このプロバイダは Distributed Cloud Bot Defense を軽減モードに移行しました。このサービスは、クレデンシャルスタッフィング攻撃を即座にブロックし、何千ものアカウント乗っ取りを防止できました。このプロバイダの推定では、F5 が消費者ログインとアカウント作成アプリケーションを保護することで、不正行為による損失を少なくとも年間 350 万ドル削減できました。

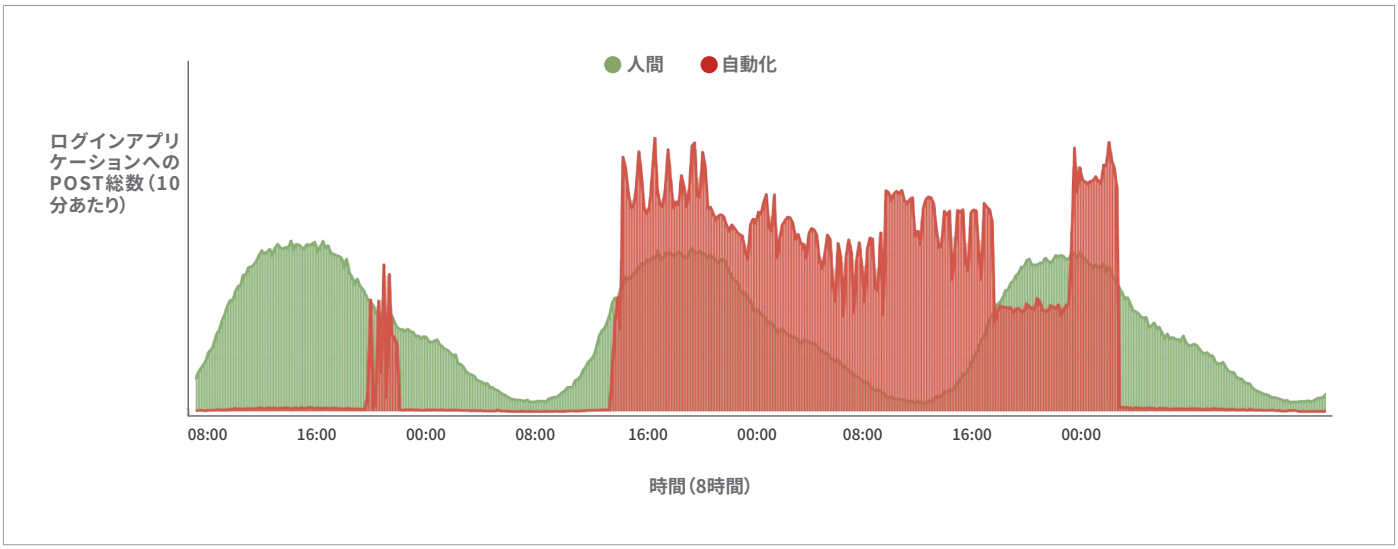


図 2：キャンペーン #2 期間中のログイントラフィック

今後の計画

Distributed Cloud Bot Defense により Web およびモバイルアプリの消費者ログインの保護に成功したことで、このプロバイダは、企業顧客の新規アカウント登録や、ビジネスログイン、配送、支払い、追跡サービスなどの他のビジネスアプリケーションの保護に導入を拡大する予定です。

また、F5 と協力して、消費者ログインアプリケーションで自動化を使用している企業顧客からの正規の（安全な）自動化を効率的に許可して、製品出荷を効率化しています。

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。

[1] F5 では、数百の独自の信号によって識別される、同じ発信元から発信される自動化されたリクエストのグループをキャンペーンと定義しています。