ケーススタディ

航空会社がWebおよびモバイルへの自動攻撃を阻止

顧客：年間売上高 150 億ドル以上、ロイヤリティプログラム会員数 2,000 万人の世界**トップ 10 航空会社**

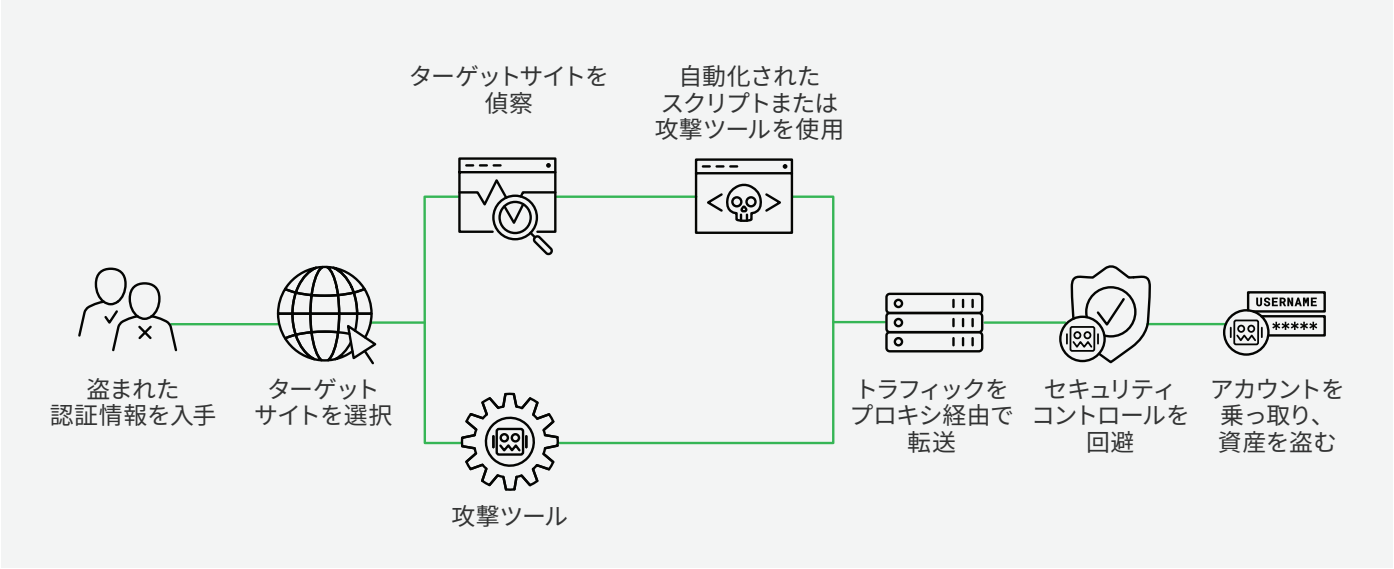

図 1：クレデンシャルスタッフィングのキルチェーン

課題 1：クレデンシャルスタッフィング

この航空会社は、Web およびモバイルアプリケーションに対し、主に 2 種類の攻撃を受けていました。1 つは、クレデンシャルスタッフィング攻撃で、1 日で 1,000 件近くの顧客アカウントが侵害されることもありました。

クレデンシャルスタッフィングとは、盗まれた第三者の認証情報を別のログインアプリケーションで一括してテストする攻撃です。ユーザーはオンラインサービス間でパスワードを使い回すため、通常、盗まれた認証情報リストの 0.5% ～ 2% が標的サイトでも有効であり、攻撃者はユーザーのアカウントを乗っ取ることができます。

攻撃者がクレデンシャルスタッフィングによって顧客のフリークエントフライヤーのアカウントの乗っ取りに成功した場合、この航空会社には、盗まれたマイレージポイントの返金や、アカウントにリンクされたクレジットカードを使った不正取引へのチャージバック料金のコストがかかります。

クレデンシャルスタッフィング攻撃自体でもこの航空会社に損失を与えていました。攻撃者が顧客のアカウントへのログインに何度も失敗すると、正規の顧客は、誤って自分のアカウントからロックアウトされ、カスタマサービスに連絡しなければならなくなり、これがカスタマサービスへの負担となりました。それだけでなく、顧客の不満が高まり、航空会社にとって容認できないものとなりました。

F5 が選ばれる理由

この航空会社は、主に以下の 3 つの理由から F5 Distributed Cloud Bot Defense を選びました。

1. Web、モバイル、API ソリューションを含むオムニチャネル保護
2. 高度な攻撃者に対する長期的な有効性
3. 不正対策およびセキュリティチームがデータを共有できる総合的なプラットフォーム

課題 2：運賃スクレイピング

この航空会社は、スクレイピングという課題にも直面していました。オンライン旅行代理店（OTA）や競合他社を含む第三者がスクリプトを実行し、「フライト検索」や「今すぐ予約」などのアプリケーションからリアルタイムの運賃データを収集していました。これらの継続的なリクエストは、インフラストラクチャチームの顧客対応能力を超えて行われ、正規の顧客が利用するサイトの速度を低下させ、ユーザーの摩擦を引き起こしていました。

この航空会社は一部の OTA とパートナーシップを結んでいましたが、その OTA の一部が不誠実に行動し、データ契約条件に違反していました。しかし、この航空会社は、正規のユーザーと不要な第三者を区別できなかったため、問題を軽減できませんでした。

導入

2017 年 6 月にアカウントのロックアウトがピークに達したとき、この航空会社はクレデンシャルスタッフィング攻撃の解決策をすぐに見つける必要があるとわかりました。F5 はクレデンシャルスタッフィングと運賃スクレイピング攻撃を包括的に阻止すると同時に、セキュリティおよび不正対策チームが ROI を証明できる唯一のベンダーであったため、それを選択することは明確でした。クレデンシャルスタッフィングが緊急の課題であったため、この航空会社は F5® Distributed Cloud Bot Defense をまず Web ログインアプリケーションに導入することにしました。

初期の成果：49 日で投資回収

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着信するすべてのリクエストを分析し、顧客にとって最善な結果となるように防御をカスタマイズします。F5 と顧客が、人間による正規のトラフィックに影響がないと確信したら、F5 は軽減モードを起動します。

観測モードでは、下の図で黄色のトラフィックが示すように、クレデンシャルスタッフィング攻撃が、この航空会社のすべてのログイントラフィックの 90% 以上を占めていました。4 週間の観測期間を過ぎた頃、F5 は、この航空会社からの依頼により、軽減モードを起動しました。その後すぐに、攻撃者からの POST は、オリジンサーバーに到達する前に阻止され、攻撃者はログインを成功できなくなりました。

攻撃者は、ROI を最適化するために、常に最も簡単な方法を選びます。そのため、クレデンシャルスタッフィングを行う攻撃者の大半は、突破できないほど難しい防御に遭遇すると、より簡単な標的に移ります。以下の赤いトラフィックの減少が示すように、Distributed Cloud Bot Defense がアクティブな軽減モードになってからわずか 1 週間で、膨大な量の試行回数は 5 分の 1 に減少しました。

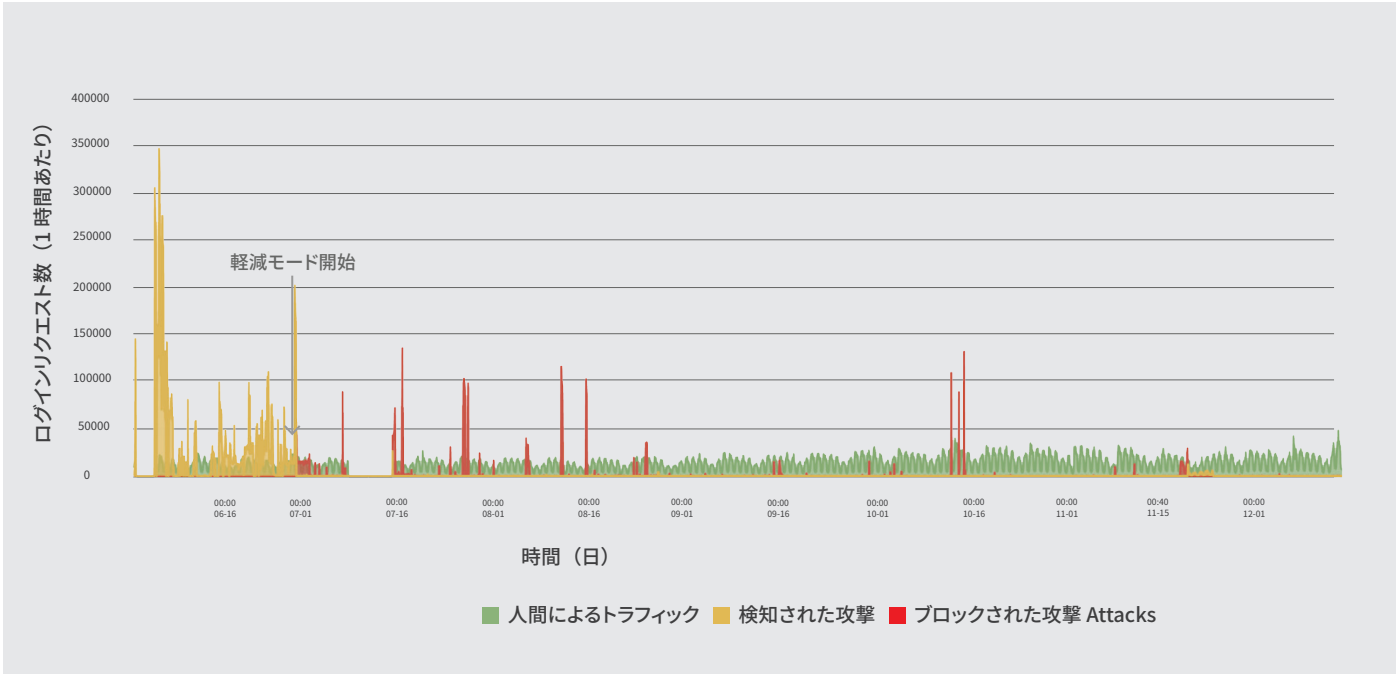

図 2：F5 Distributed Cloud Bot Defense 導入後 6 か月間のログインリクエスト数

長期的な成果：モバイルへの拡大

残念ながら、「より簡単な標的」とは、必ずしも無関係な標的を意味するわけではありません。多くの攻撃者は、Web サイトがオープンドアではなくなったことを認識するようになり、この航空会社のモバイルアプリに注目するようになりました。

この航空会社は、モバイルアプリケーションでは F5 による保護やトラフィックの可視化を利用していなかったため、攻撃の正確な分布を把握できていませんでしたが、攻撃者がモバイルに移行していることを示す有力なデータは他にありました。

クレデンシャルスタッフィングの強力な指標は、存在しないユーザー名がログインアプリケーションで試行される割合です。以下の図に示すように、存在しないユーザー名の試行は、Web 上では 6 月の導入後着実に減少しましたが、モバイル上では急速に増加しました。

そのため、この航空会社は、F5 に保護をネイティブモバイルアプリに拡大するよう依頼し、SDK ソリューションは 1 か月で完全導入されました。

また、上の図に示すように、ここでも、攻撃者の大半は、防御が強すぎるとわかるとすぐに、より簡単な標的に移動しています。つまり、モバイル導入後、Web もモバイルも侵入可能な攻撃対象ではないことが明らかになり、ほとんどの攻撃者は 12 月には姿を消し、まったく別の標的に移っていきました。

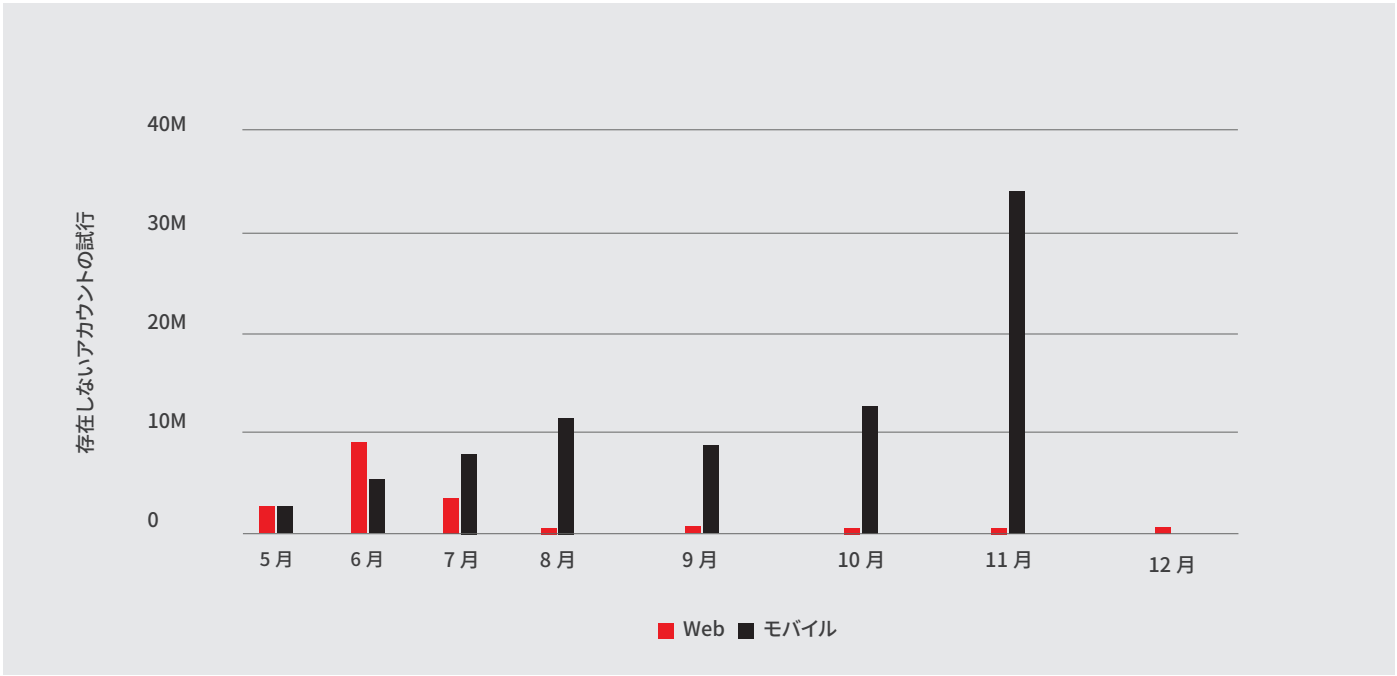

図 3：学習 Web が守られた後、攻撃者は着実にモバイルに移行

クレデンシャルスタッフィング攻撃が止まると、それに対応する不正行為も止まりました。

まとめ：全体的かつオムニチャネルの防御

この航空会社にとって最も重要なことは、クレデンシャルスタッフィング攻撃が止まると、それに対応する不正行為も止まったということです。セキュリティチームは、アカウントを侵害した攻撃者が不正行為を行っていることを直感的にわかっていましたが、クレデンシャルスタッフィング攻撃とアカウント乗っ取りの不正行為を関連付けることはできていませんでした。この航空会社は、F5 のデータダッシュボードを介してトラフィックを完全に可視化して、初めて、悪意のあるログイン試行の減少と、アカウント乗っ取りや不正行為による損失の減少を直接関連付けることができました。

この航空会社は、F5 によるログインアプリケーション保護の有効性が実証されるとすぐに、Distributed Cloud Bot Defense をスクレイパーに攻撃されている Web およびモバイルアプリケーションに拡大しました。自動化された攻撃を完全に解決したこの航空会社のセキュリティチームでは、フルタイムの従業員が、ビジネスにおける他の戦略的に上位の優先事項に集中できるようになりました。

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。