ケーススタディ

国際航空会社、運賃スクレイパーと戦う

概要

スクレイパーによるデータ盗難：ある大手国際航空会社は、フライト情報の提供やフリークエントフライヤーのアカウントへのサービスのために、11 か国語で 30 のウェブサイトを運営しています。サイバー犯罪者や運賃アグリゲータは、自動化された攻撃により、顧客のアカウントを侵害し、航空会社の情報を不正に入手しています。

2014 年、サイバー犯罪者が自動化されたクレデンシャルスタッフィング攻撃により多数のフリークエントフライヤーのアカウントを侵害する事件が発生しました。その後フリークエントフライヤーのマイレージが盗まれ、これが国際的に報道され、ソーシャルメディアに否定的なコメントが寄せられ、顧客の不満が生まれました。

アグリゲータは、スクレイピングボットを使用して、非準拠のチケットオプションを発見し、公開していました。これらの不正な予約は、この航空会社の収益管理能力を妨げ、運用の柔軟性を低下させました。

これらの攻撃は経済的な動機から行われました。旅行アグリゲータは、手数料を請求または広告を販売することで、航空会社の情報を収益化していて、サイバー犯罪者は、盗んだ特典チケットやフリークエントフライヤーのマイレージをダークネットマーケットで転売していました。

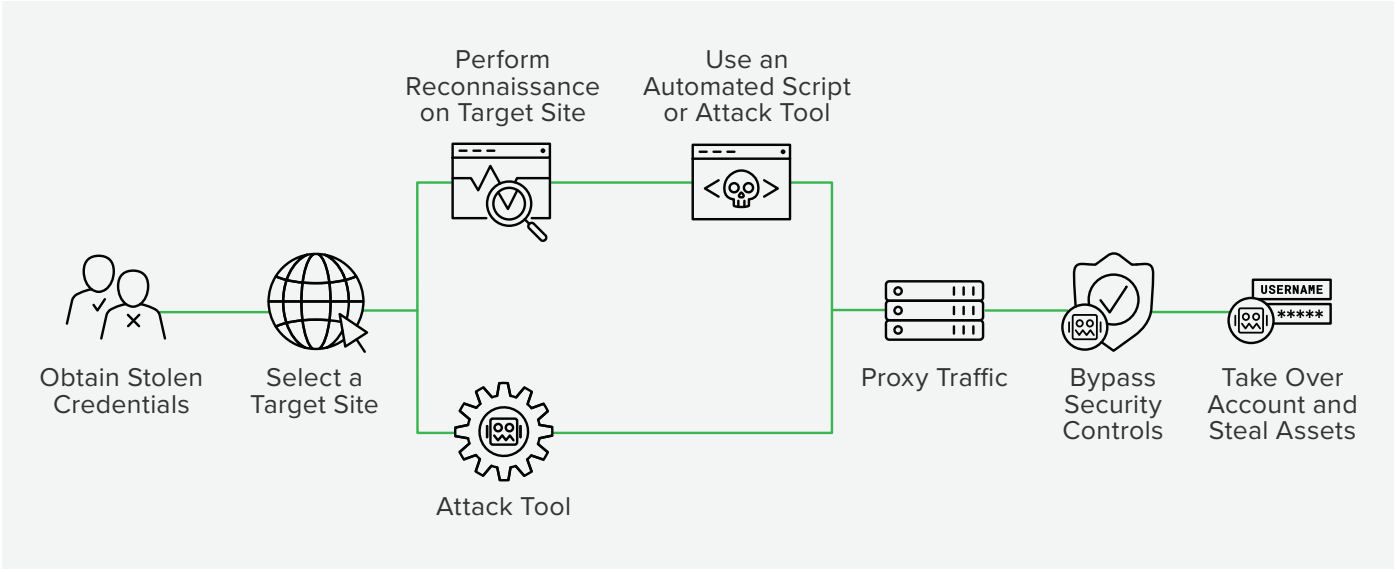


図 1：クレデンシャルスタッフィングのキルチェーン

攻撃対象

スクレイピングボットは、この航空会社の検索機能に攻撃を仕掛け、経路情報を抽出し、それを再パッケージ化してアグリゲータの顧客に提供していました。この航空会社のメインの検索 URL における検索トラフィックの約 4 分の 1 は、自動化が占めていました。スクレイパーはごく短い期間で 85 万件以上の自動検索を実行していました。

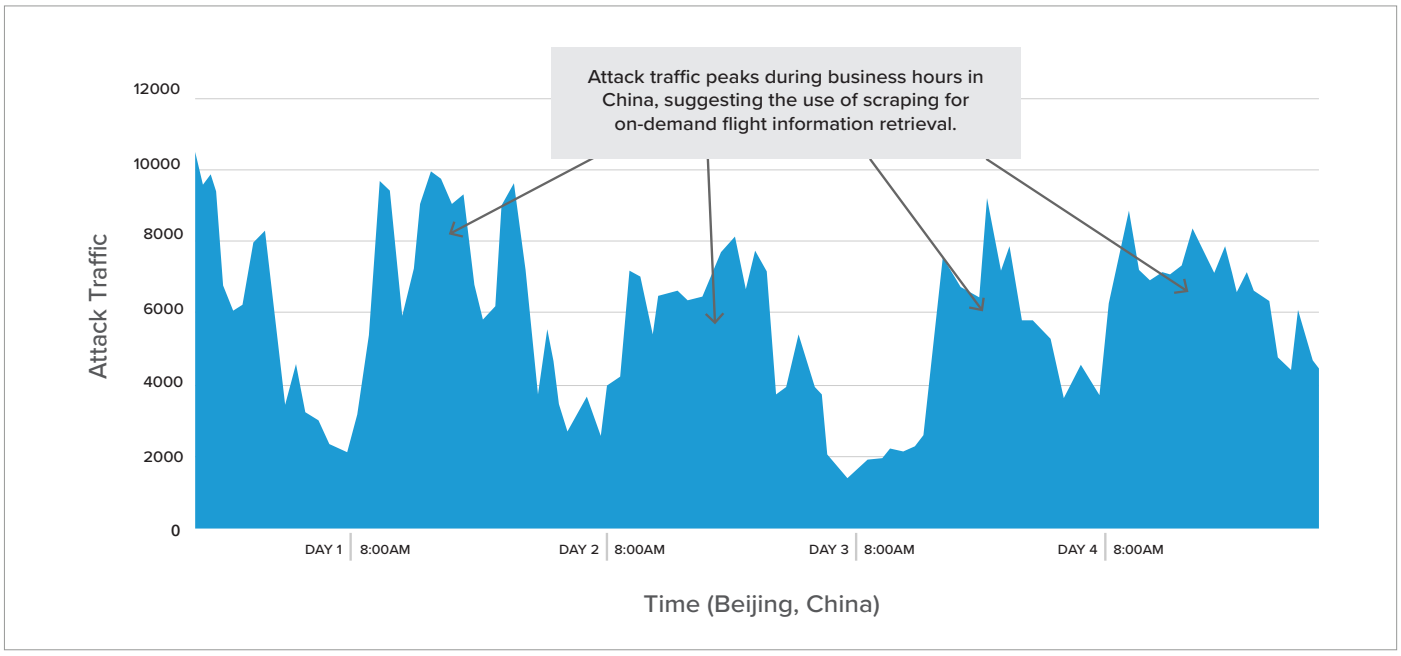
攻撃方法

この航空会社に仕掛けられたスクレイピング攻撃には、多数の異なる IP アドレスを使用する異常に大規模なボットネットが関与していました。望ましくないトラフィックの約 85% の発信源は中国でした。これらのスクレイパーの大半は、単純な HTTP のみのツールを使用していました。また、F5 は、クレデンシャルスタッフィングスクリプトが使用されていることも確認しました。このスクリプトと同様の他のツールは、自動化を使用して、他のサイトから盗んだユーザー名とパスワードをテストします。

攻撃の影響

複数のボットグループが確認され、最もトランザクション量の多いグループのトラフィックレートは、中国の営業時間中にピークに達していました。これは、このグループが中国市場向けにオンデマンドのフライト情報を提供していたことを意味します。

以下のグラフ（F5® Distributed Cloud Protection Manager のダッシュボードから取得したデータに基づく）は、攻撃の盛衰を示しています。このグラフにあるすべてのトラフィックは、攻撃によるものであることに注意してください。正規のトラフィックは含まれていません。



既存のセキュリティソリューションの失敗

この航空会社は、Web アプリケーションファイアウォール、IP レピュテーションチェッカー、レートリミッター、その他のセキュリティソリューションなど、多層的な防御で Web サイトを保護しています。各要素が意図したとおりに機能したにもかかわらず、これらの攻撃は、正規の検索やログインの試行を忠実に模倣することで、既存の防御を回避していました。

さらに、これらの活動をカモフラージュするために、プロキシや大規模なボットネットを活用して、検索やログインがそれぞれ別の訪問者から行われているように装っていました。従来のセキュリティソリューションは、既知の攻撃の防止、IP アドレスのブラックリスト化、または単一ホストからの過剰なトラフィックのブロックを目的としていたため、これらの高度な回避手法によって簡単に回避されてしまいました。

攻撃の軽減

この航空会社の Web プラットフォームは、AJAX ページを使用して、応答性と可用性の高い訪問者体験を提供しています。

F5® Distributed Cloud Bot Defense は、すべての自動化されたトラフィックをかわし、この航空会社の Web サイトに到達しないようにしました。クレデンシャルスタッフィング攻撃は完全に軽減されました。自動化された運賃スクレイピングは、調査のために引き続き許可されていますが、いつでもブロックできます。

まとめ

ボットや回避手法を利用して、独自のフライト情報の窃取と顧客アカウントの乗っ取りが行われていました。既存のウェブサイト防御は、人間の訪問者を装った自動化された攻撃者に対しては効果がありませんでした。Distributed Cloud Bot Defense は、最も洗練されたボットでもかわすことができ、これらの Web サイト攻撃を確実に阻止できました。

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。