顧客事例

自動化されたギフトカード詐欺

小売企業の説明

- **50 億ドルのギフトカードプログラム**
  グローバルな消費者ブランド
- **2,000 万件のアカウント**の大部分はギフトカードとクレジットカードに紐づけられていました
- ギフトカード間で**残高の移動が可能**

不正と課題

- 1 日あたり **1,000 件のアカウント**がクレデンシャルスタッフィング攻撃で乗っ取られました
- **ボットとアカウントチェッカー**は主要な攻撃ツールでした
- 乗っ取られたアカウントの平均残高は **50 ドルで**した

「問題は他の WEB サイトにありました。当社のお客様は、複数のサイトで同じパスワードを再利用しています。詐欺犯罪者は、他のサイトが侵害されることで流出したクレデンシャルを使って、当社のお客様のアカウントを乗っ取ったのです。」
- 同小売企業の CISO

F5 はどのようにしてアカウント乗っ取りを撃退し、数千万ドルを救ったのでしょうか。 Fortune 500 にランクインしているある小売企業は、ストアドバリュー総額が 50 億ドル（1 ドル 110 円換算で 5,500 億円、以下同様）を超えるギフトカードプログラムを管理しています。このプログラムをサイバー犯罪者がターゲットとし、同社とその顧客から数千万ドル（数十億円）を盗んでいました。攻撃者は、別の Web サイトに対する侵害で流出したクレデンシャルを使って顧客のアカウントを乗っ取り、ギフトカードから資金を盗んだのです。不正なログイン試行は 1 日あたり 100 万回を超え、ログイン用 URL に対するトラフィックの 90% 以上を占めました。Web アプリケーションファイアウォール（WAF）、侵入検知防御サービス（IDS/IPS）、不正分析といった従来の防御手段は、このような継続的で自動化された攻撃を防ぐことができませんでした。Fortune 500 のこの小売企業は、F5® Distributed Cloud Bot Defense を導入することで、アカウント乗っ取りを完全に排除しました。

Distributed Cloud Bot Defense

- アカウントの乗っ取りをすべて排除して数千万ドルの被害を防止
- 悪意のあるボットや自動化された攻撃をブロック
- チャージバック手数料とカスタマーサポートに対する問合せ件数を削減

F5 が選ばれる理由

Fortune 500 のこの小売企業は、WAF、IP レピュテーションフィード、レート制限、およびその他の防御策でクレデンシャルスタッフィング攻撃を阻止できなかったため、F5 を採用しました。攻撃者がセキュリティ対策を破るために使っていたのは、ボットネット、自動アカウントチェッカー、Web プロキシでした。ピーク時には小売企業の Web アプリケーションに対する攻撃で 10 万件以上の新規 IP アドレスが関与していましたが、どれも 1 回だけ使われると、再び使われることはありませんでした。攻撃者の中には、ブラウザまたはブラウザエージェントの動作を模倣して、人間の訪問者の挙動をシミュレートする者もいました。

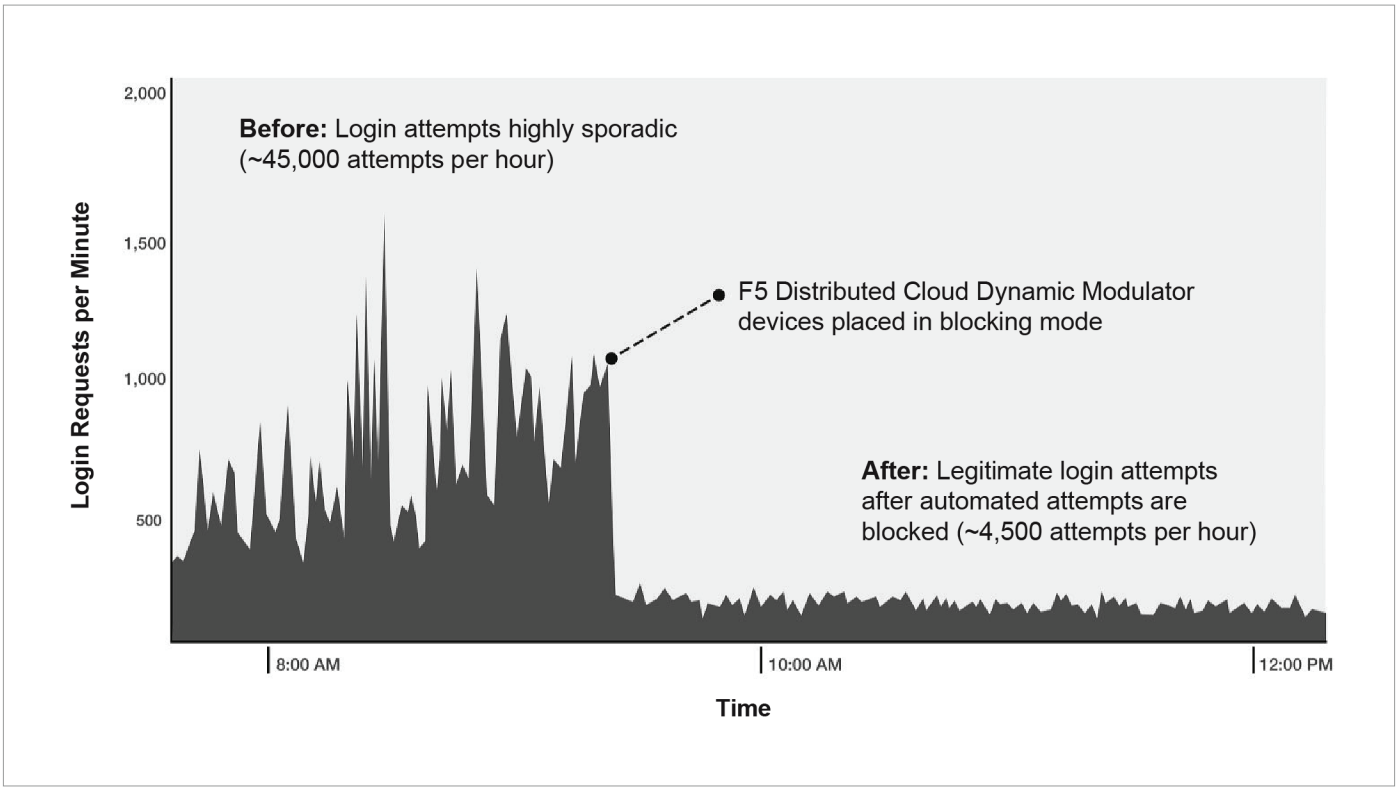


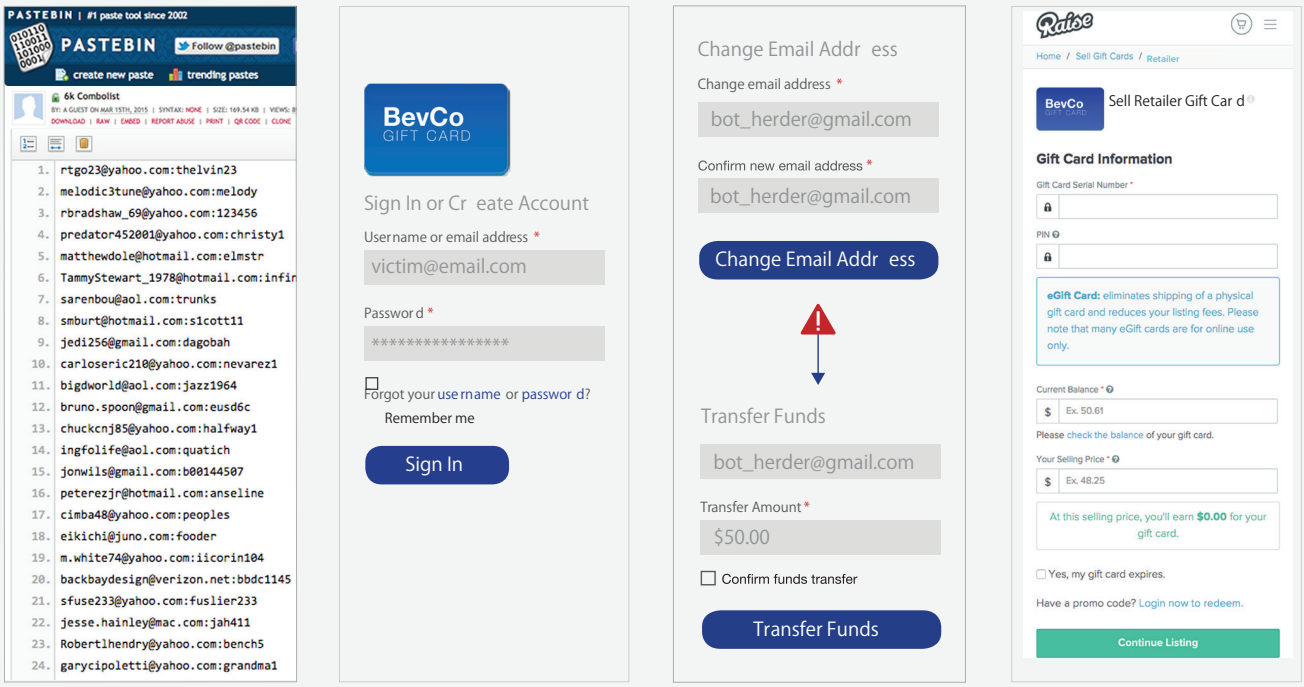
図 1：ログインリクエスト

「F5 は、私のチームと協力して、2 週間で本稼働させることができました。従来のセキュリティソリューションと異なり、SHAPE のソリューションから価値を引き出すために追加のトレーニングや要員は必要ありません。ユーザが不便な思いをしたり、当社のチームに大きな負担がかかったりすることなく、攻撃を完全にブロックしています。」

- 同小売企業の CISO

F5 Distributed Cloud Bot Defense の利点

- Fortune 500 小売企業の Web サイトをリアルタイムで防御し、自動化された攻撃をそらすことに成功
- 攻撃者が異なるアプローチを取ってきたときには新しい対策をデプロイ
- 同小売企業の Web インフラストラクチャに、２週間で導入、および統合されました。



ステージ 1

流出したクレデンシャルを攻撃者がオープン Web（犯罪市場およびパスワード捨て場となるサイト）から入手

ステージ 2

防御を回避するために、攻撃者が分散ボット、Web プロキシ、その他の戦術を用いてクレデンシャルをテスト

ステージ 3

クレデンシャルが有効な場合には攻撃者がアカウントを乗っ取り

ステージ 4

攻撃者が eBay や Raise.com などの流通市場を通じて、ギフトカードを額面の 85 ～ 90% で売却

図 2：攻撃の構造

まとめ

Fortune 500 のこの小売企業は、F5 Distributed Cloud Bot Defense を大規模に展開し、初期導入の成功に続き、他の Web アプリケーション、およびモバイルアプリケーションで使用される API サービスを保護しました。これにより、不正取引とチャージバック料金を数千万ドル削減できました。また、F5 の自動化攻撃対策の専門家が提供する脅威インテリジェンス（F5 の導入環境全体で収集および関連付けされる）とコンサルティングによる恩恵を継続的に受けることで、サイバー犯罪者の一歩先を進むことができます。

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。