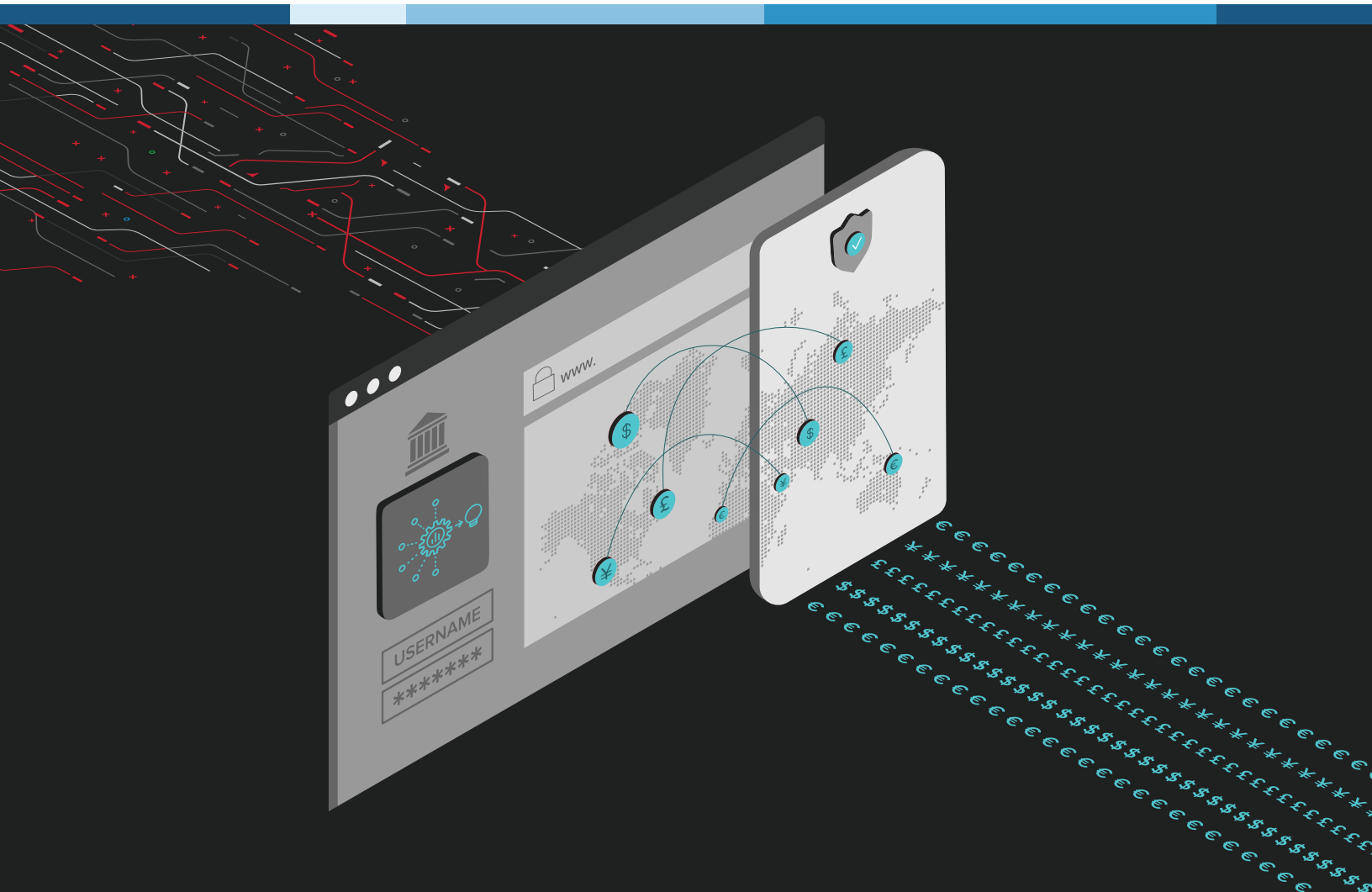
ケーススタディ

Global Money Transfer Service、不正行為者を阻止し、サービス停止を回避



初月で 78 万 6,000 ドルを節約

顧客：Global Money Transfer Service。年間売上 50 億ドル以上のトップ 3 の送金サービスで、100 か国以上の顧客にサービスを提供しています。数十万の代理店、数百万の顧客を持ち、年間 2,000 億ドル以上の元本を計上しています。この企業は最近、自社でも既存のベンダーでも解決できない多くの課題に直面しました。

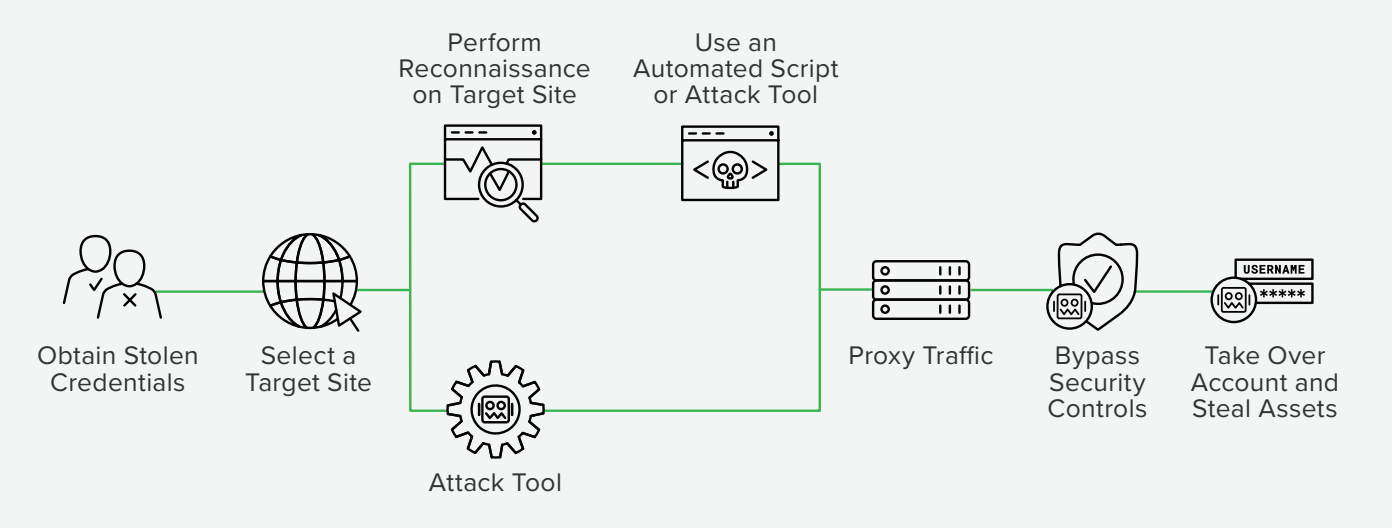


図 1：クレデンシャルスタッフィングのキルチェーン

課題 1：クレデンシャルスタッフィングからアカウント乗っ取り

89% は自動化されたメール検証

この送金サービス企業では、認証情報の流出が公開されるたびに、クレデンシャルスタッフィング攻撃の波を受けていました。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。

攻撃者は、クレデンシャルスタッフィングキャンペーンを利用して、認証情報リストを検証し、金銭を盗み、送金を傍受し、送金サービスのアカウントを乗っ取っていました。

送金アカウント乗っ取りの攻撃者は、関連する銀行口座から自分自身に送金し、転送中の送金を傍受します。

悪意あるアクターは、ログインページ、取引検索、パスワード再設定、メール検証という 4 つの主要なサービスに対して自動化を行っていました。

検証された認証情報のリストは、別の攻撃者に販売され、そこで、頻繁に送金を行うユーザーの関連銀行口座から自分自身に送金することで、それぞれのアカウント乗っ取りを収益化していました。また、攻撃者は、受取人への転送中の送金を検索し、それを傍受していました。

F5 が選ばれる理由

この送金サービス企業は、主に以下のような 3 つの理由から F5 を選択しました。

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：サーバーへの負荷攻撃

送金が盗まれるだけでなく、さらに悪いことに、自動化により起動される取引問い合わせが、検索データベースに影響を与え、タイムアウトやサービス停止を引き起こしていました。この送金サービス企業はグローバルに展開していることから、インターネットが発達した豊かな国から新興国に送金が行われることがよくあります。このような新興国では、Pentium II コンピュータ、IE7、ダイアルアップインターネットを使う街角の「小さな商店」が代理店となることが一般的であるため、データベースがタイムアウトにならなくても送金はすでに不安定であり、そこでサーバー障害が発生すると、適切な支払いが数日遅れることもありました。

課題 3：アカウントのロックアウト

送金サービスのパスワード再設定ページは、自動化に包囲されていて、自動化による再設定により、何千人もの正規の顧客が自分のアカウントにアクセスできない状態に陥っていました。対象ユーザーに対する実際の不正行為が行われていない場合でも、顧客が自分のアカウントへのアクセスを回復（および保護）できるようにするためのコストが発生していました。

決定

この送金サービス企業では、CDN と追加のボット管理機能でこの状況に対処しようとしましたが、効果はありませんでした。適切な防御を講じても、攻撃者は攻撃方法を変え、事態は振り出しに戻るだけでした。さらに、この企業への侵入口は世界中に数百も存在するため、対策は困難でした。そこで、この送金サービス企業は F5 に依頼することにしました。

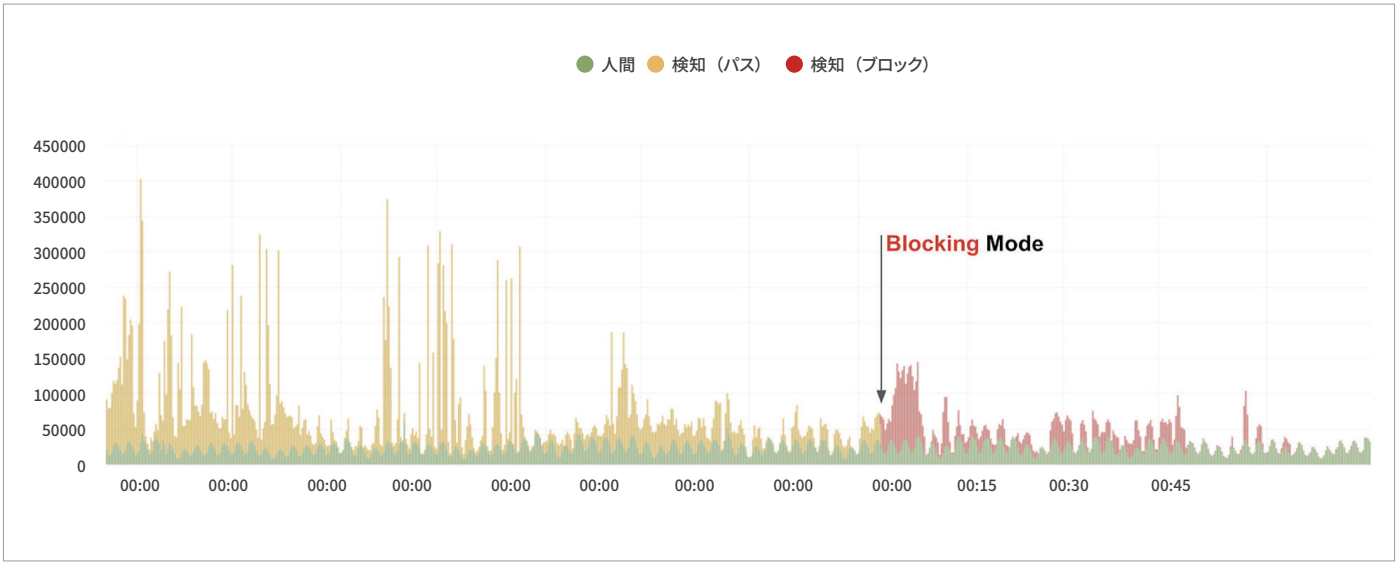


図 2：攻撃トラフィック

初期の成果：初月に 78 万 6,000 ドルを節約

F5® 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。

この送金サービス企業での観測モードにおいて、Distributed Cloud Bot Defense は、4,500 万件の POST トランザクションを観測し、上の図の黄色のトラフィックで示されるように、クレデンシャルスタッフィング攻撃が全トラフィックの 61% 以上を占めていることを発見しました。観測期間の 4 分の 1 を過ぎた頃、F5 は、この企業から軽減モードを起動するよう依頼されました。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、攻撃者は認証情報のテストや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。Distributed Cloud Bot Defense がアクティブな軽減モードを起動してから最初の 2 週間、攻撃者は、上の図の赤いトラフィックで示すように、攻撃方法を変え 3 種類の攻撃キャンペーンを試みましたが、諦めて、より簡単な標的に移っていきました。

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、サービスのモバイルアプリに注目するようになりました。

この送金サービス企業は、買収によって積極的に成長し、数百か国で事業を展開していたため、モバイルアプリケーションの数は 50 以上と、驚くべき数になっていました。F5 は、自動化された Web トラフィックがブロックされた攻撃者は、モバイルクライアントのなりすましに移行するとこの企業に警告しました。

50 のモバイルアプリが保護されました。

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。存在しないユーザー名の試行は、Web 上では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。

F5 はこの企業と協力し、F5® Distributed Cloud Defense Mobile SDK の保護をその 50 のモバイルアプリケーションすべてに統合し、そこでも攻撃者のブロックに成功しました。しかし、それで終わりではありませんでした。

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。

F5 は、この送金サービス企業の Web およびモバイルサイトを保護し、不正行為、サーバー攻撃、メール検証キャンペーンを阻止しました。ここでこの企業を驚かせたことは、メール検証キャンペーンが、この送金サービス企業のサードパーティパートナに対して行われたことでした。正規の顧客がこの企業にログインするときに、これらの信頼できるパートナを経由していることから、攻撃者は、この信頼できるパートナを含めたメール検証キャンペーンのテストを開始しました。

この送金サービス企業は、パートナに F5 Distributed Cloud のセキュリティソリューションを採用するよう促しました。現在、F5 サービスはそのすべてのパートナにも展開され、そこで攻撃者は諦めました。

まとめ：全体的かつオムニチャネルの防御

この送金サービス企業にとって最も重要だったことは、クレデンシャルスタッフィング攻撃が止まったときに、それに対応する不正行為とサーバー攻撃も止まったことでした。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。この企業は、Distributed Cloud Bot Defense 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サーバー攻撃の減少を直接関連付けることができました。

T 現在、F5 は、この企業の数百のエントリーポイント、数十のモバイルアプリケーション、そしてそのパートナも保護しています。この企業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。

DC0122 | FUJ-CORP-828934945