顧客事例

グローバルなデーティング プラットフォームが アカウントの乗っ取りを撃退

顧客—50 か国以上に 3,500 万人の会員を擁するグローバルなオンラインデーティング企業。市場のリーダーで、そのモバイルアプリは App Store で人気アプリのトップ 50 に入っています。

課題

平均でクレデンシャルリストの 0.5-2.0% がターゲットサイトにおいて有効

この会社は 2016 年、大規模なクレデンシャルスタッフィング攻撃に直面していました。クレデンシャルスタッフィングは、悪意のある者がサードパーティから盗まれたクレデンシャルを入手し、自動化を通じてターゲットサイトで一斉に試す攻撃です。ユーザが複数のオンラインサービスでパスワードを使い回していることから、クレデンシャルリストの平均で 0.5%-2% はターゲットサイトにおいて有効です。

悪意のある者たちは、Web サイトとモバイルアプリの両方に対して高度なクレデンシャルスタッフィング攻撃を仕掛け、多くのアカウントの乗っ取りにつなげていました。アカウントの乗っ取りに成功すると、攻撃者は、なりすましやスパムメールなどの手法を実行したものです。こうした攻撃はユーザの信頼を低下させるだけでなく、顧客サービスチームに多大なコストを強いることにもなりました。

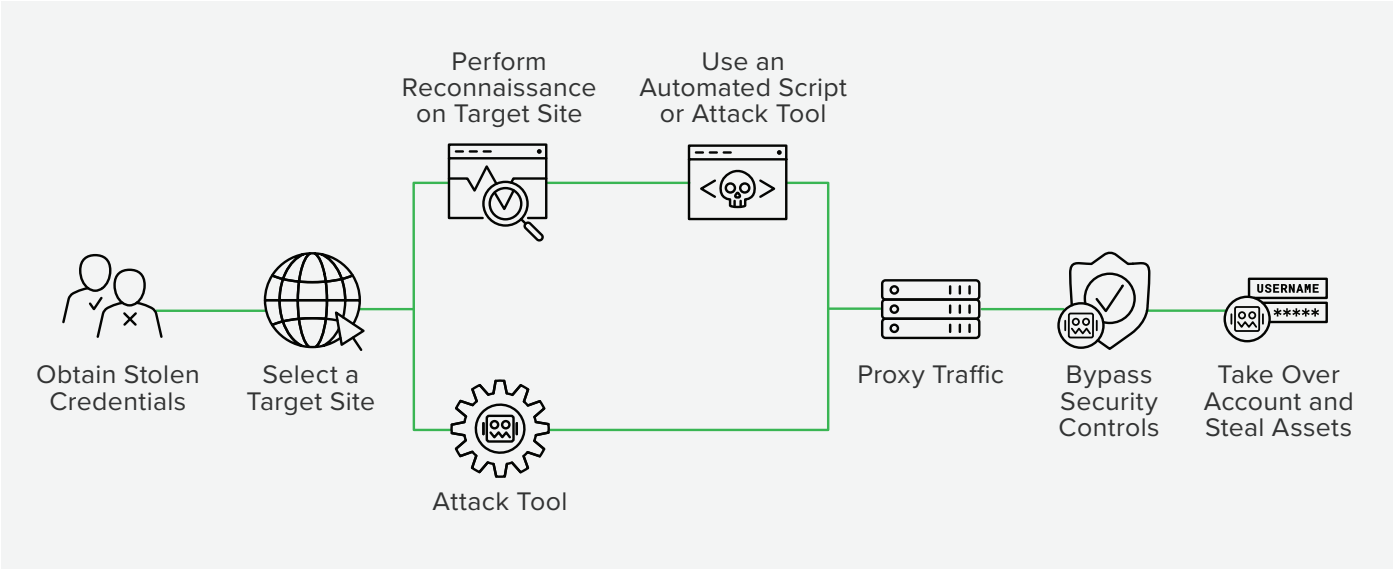

図 1：クレデンシャルスタッフィングのキルチェーン

決断

2016 年、この企業は、Web およびモバイルプラットフォームに対する望ましくない自動化を軽減するために、CDN プロバイダが提供するツールを審査してみました。2 か月間ツールをテストしたところ、セキュリティや不正対策のチームにはフラストレーションが残りました。このツールは、自動化された攻撃のひとつひとつを能動的に処理するために、個々の活動を調査してルールを

記述するなど、内部のリソースが必要でした。ツールの運用に要する時間とリソースの量は持続可能なレベルではなく、費用対効果も劣悪でした。しかも、このツールでは、デーティング Web サイトに対する自動化されたクレデンシャルスタッフィング活動の 20% しか特定できなかったため、不適切と判定されました。

CDN が提供するツールが適切なソリューションでないことが明らかになり、F5 に連絡することにしました。この企業が求めていたのは、特に以下の 4 つの重要な要件を満たすソリューションでした。

図 2：重要なソリューション要件

Company Requirement	F5
Protect Against Credential Stuffing	Recognized as the leader in defending enterprises against credential stuffing attacks.
Web and Mobile API Protection	Provides both a web and mobile solution.
Managed Service	24x7 service acts as an extension of a customer's security team, so customers do not have to dedicate resources to technology management.
Predictable Cost	Service is all inclusive, so sudden increases in attack volume or new system requirements do not incur additional costs for the customer.

結果

以下のトラフィックチャートが示すように、攻撃者の挙動は典型的なものでした。
この企業が F5® Distributed Cloud Bot Defense を選択すると、F5 は数週間で導入を開始しました。Distributed Cloud Bot Defense は、監視モードで、平均して全 Web トラフィックの 80% が自動化されていることを確認しました。F5 が軽減モードを開始するとすぐに、攻撃はブロックされ、オリジンサーバーへの到達を阻止できました。

- 加速（第 0 ～ 2 日）：最初にブロックされると、攻撃者は攻撃量を増やし、物量作戦で新たな防御を突破しようと試みます。
- 手法変更（第 3 ～ 7 日）：失敗の期間を経て、攻撃者は攻撃の手法を変更するために、いったん活動を停止します。
- 再来襲（第 8 日）：攻撃者は変化させた攻撃手法を伴って再来襲し、総力を挙げてデプロイします。
- 断念（第 9 ～ 10 日）：攻撃者は防御を突破できないことをすぐに認識し、より攻略しやすいターゲットへ移っていきます。

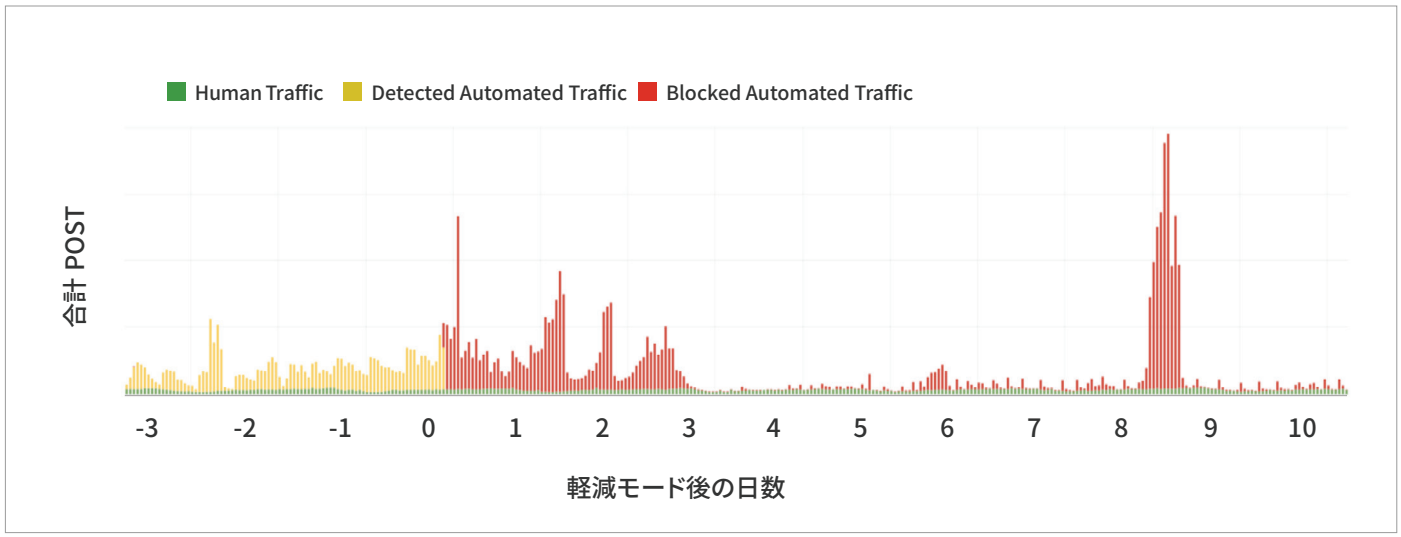

図 3：トラフィックチャート

注意：この期間にはトラフィックの最大 95% が自動化されていたため、人間によるトラフィック（緑で示す部分）は表示が見えづらくなっています。

自動化された攻撃の軽減に成功したことで、Distributed Cloud Bot Defense は、企業全体に以下のような価値をもたらしました。

1. **セキュリティ：** F5 のマネージドサービスにより、セキュリティチームは他のセキュリティ優先事項に集中できるようになりました。
2. **不正：** Distributed Cloud Bot Defense が、アカウント乗っ取り（ATO）の大半の発生を防いでいることから、不正対策チームは、高度な不正行為の検知と防止にリソースを使うことができるようになりました。
3. **カスタマーサービス：** アカウントの乗っ取りが減ったことで、カスタマーサービスに対する要求も動揺するユーザも減少する結果となっています。
4. **IT:** 自動化されたトラフィックがオリジンサーバーに到達しなくなったため、IT チームの処理が必要なトラフィックは以前の 20% だけとなり、インフラストラクチャコストを削減できました。 さらに、サイトの遅延が 250ms から 100ms に低下しており、サイトのパフォーマンスが改善しています。

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。