顧客事例

北米トップ10 の銀行がクレデンシャルスタッフィングを排除

クレデンシャルスタッフィング

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、ターゲットとするログインサイトで一斉に試す攻撃。ユーザがパスワードを使い回すことから、盗み出されたクレデンシャルリストの 0.5%-2% は一般に、ターゲットサイトにおいて有効です。

「従業員のあるグループが、現在のベンダーのソリューションを調整するために業務時間の 100% を投入して、攻撃に後れを取るまいと奮闘しています。当行のために攻撃者と闘ってくれる誰かが必要です。」

—サイバーセキュリティ担当ディレクタ

顧客：カナダで 5 指に入る銀行　年間収益が 200 億ドル（1 ドル 110 円換算で 2 兆 2,000 億円）を超え、カナダで「ビッグ 5」[1] に数えられる銀行の 1 つ（以下、「銀行」）は、何か月もの間、Web とモバイルのログインアプリケーションに対する自動化された攻撃に苦しんでいました。

悪意のある者たちは、考えうる全てのチャネルでクレデンシャルスタッフィング攻撃を仕掛けていました。カナダと米国の両方の Web サイト、モバイルアプリ、さらには OFX（Open Financial Exchange）の API エンドポイントもターゲットとなりました。こうした攻撃は、アカウントの乗っ取りという不正がもたらす損失につながるだけでなく、攻撃量が極めて膨大であるために銀行のインフラストラクチャにとって大きな負担ともなっていました。銀行では、カナダと米国の両方の Web サイトでサービス障害が発生し、顧客は自分のアカウントに満足にアクセスできない状態となっていました。こうしたサービス障害は銀行の経営陣にとって受け入れがたいものであったため、セキュリティチームには解決策を見つけることが厳命されました。

課題：CDN 提供のツールでは不十分

自動化された攻撃を軽減するために銀行はまず、CDN が提供するボット緩和ツールをデプロイしました（以下、「ベンダー」）。ベンダーのソリューションは短期的には効果を示しましたが、長期的な防御効果を提供することはできませんでした。ベンダーは攻撃を阻止するためにルールベースのシステムを基盤としていましたが、攻撃者は数時間以内に戦術を変更してルールを回避したため、ツールの手作業による設定を余儀なくされました。

この銀行のインシデントレスポンスチームは、1 日 24 時間、週 7 日体制で攻撃者を監視しながら新しいルールを設定するという、負担のかかる業務に疲れ果てていました。数か月に及ぶ攻撃者とのイタチごっこの末、より洗練されたソリューションを探すことにして、F5 に連絡しました。

[1]「ビッグ 5」はカナダの 5 大銀行を意味し、他の国では一般的な「ビッグ 4」に相当します。

評価：F5 Distributed Cloud Bot Defense とベンダー

この銀行のセキュリティチームは、ベンダーのソリューションを使用したまま、F5® Distributed Cloud Bot Defense を評価し、2 つのソリューションの有効性とサービス品質を比較しました。この評価のために、Distributed Cloud Bot Defense がカナダの Web およびモバイルログインアプリケーションに導入されました。

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、この銀行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 とこの銀行が、銀行の正当なお客様による正規のトラフィックに影響がないと確信した後、F5 は軽減モードを起動します。

観察モード

Distributed Cloud Bot Defense は、観測モードで、ログイン試行の 10 回に 1 回近くが悪意のあるものであることを判別しました。この銀行は、サービスの検知能力と、定期的なブリーフィングでインテリジェンスチームが提供するインサイトのレベルの高さに感銘を受けました。

Distributed Cloud Bot Defense は、悪意のあるログイントラフィックと正規のログイントラフィックを区別できるだけでなく、リクエストを異なる攻撃グループ（「キャンペーン」）にグループ化して分析することもできます。攻撃グループが、ソフトウェアの更新や新しいプロキシの活用などで、攻撃手法を変えて回避しようとしても、このサービスは、他の数百の信号に基づいて攻撃グループを正しく識別できます。

導入後 1 週間で、Distributed Cloud Bot Defense は、4 つのキャンペーンを特定し、それぞれのクレデンシャルスタッフィング活動を追跡しました。

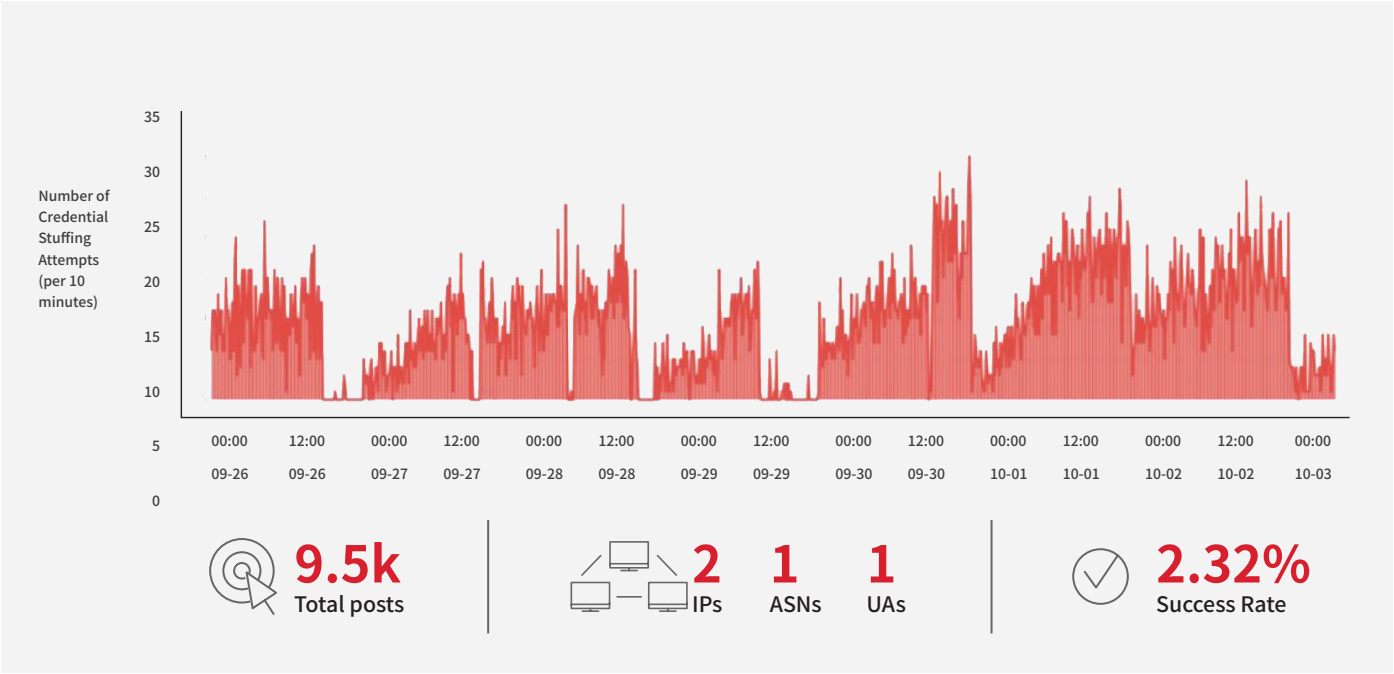

図 1：220 件のログイン成功

これは、Distributed Cloud Bot Defense が、あるクレデンシャルスタッフィングキャンペーンに関してこの銀行に提供したデータの一例です。インサイトには、キャンペーンで使用された IP アドレスと ASN の数、およびログインに成功した認証情報の割合を示すキャンペーンの成功率が含まれます。

緊急事態に伴う緩和モードのアクティブ化

観察モードを開始してから 5 週間後、銀行に突然、かつてないほど強大なクレデンシャルスタッフィングキャンペーンが襲いかかりました。そのトラフィック量は、それまでの他の攻撃の 5 倍に増大していたのです。銀行は大いに憂慮しました。なぜなら、トラフィック量がさらに増大すればインフラストラクチャの処理能力を超え、カナダの Web サイト全体がダウンすることになってしまうからです。

この銀行の CISO は、既存のベンダーから十分な支援を得られなかったため、自ら F5 に連絡し、観測モードから軽減モードへの移行を予定より数週間早め、この深刻な攻撃を阻止してほしいと依頼しました。F5 プロフェッショナルサービスチームは、この依頼に応え、数時間のうちに、この銀行のカナダのサイトに Distributed Cloud Bot Defense を導入、軽減モードを開始しました。

Distributed Cloud Bot Defense が軽減モードになるとすぐに、上の図で、黄色から赤色のトラフィックに変化しているように、攻撃は緩和しました。このサービスにより、この銀行のオリジンサーバーに押し寄せていた自動化されたトラフィックは完全に排除され、インシデントレスポンスチームはトラフィックを安定化させ、顧客へのサービスの可用性を確保できました。

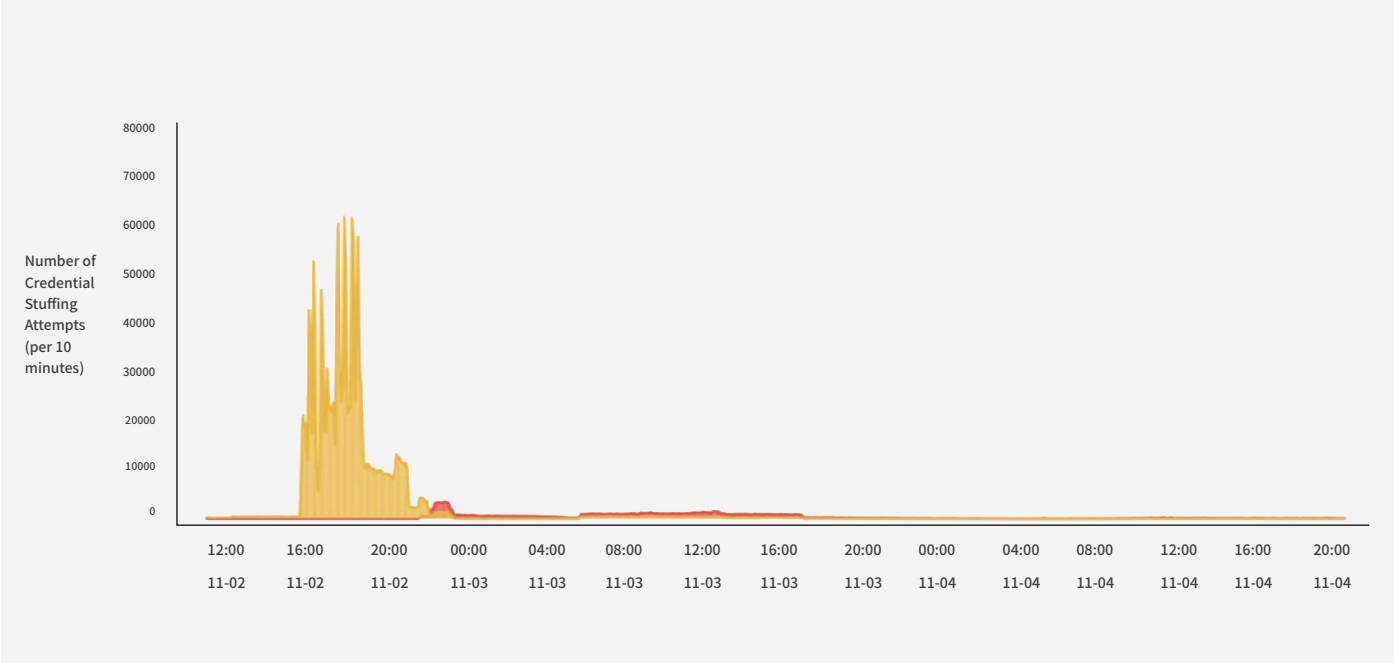

図 2：Distributed Cloud Bot Defense は、前例のない攻撃を即座に撃退

銀行が DISTRIBUTED CLOUD BOT DEFENSE から得ているメリット

1. 悪意のあるログイントラフィックを排除して、サイトの可用性を保証
2. 金融情報アグリゲーション事業者（Plaid、Mint、Yodlee など）に対するきめ細かな管理を実現
3. 顧客のアカウントを不正から保護

今後の計画：ベンダーのソリューションの完全なリプレース

F5 は、Distributed Cloud Bot Defense サービスと脅威インテリジェンスチームを通じ、ベンダーよりも優れていることを証明、困難な状況で代役を務めることに成功しました。この銀行は、Distributed Cloud Bot Defense の有効性だけでなく、F5 のチームが、大規模な攻撃中でも導入に協力して、実現できたことを高く評価しています。

Distributed Cloud Bot Defense がカナダのログインアプリケーションの防御に成功したことを受け、この銀行は、以下のことを含め、このソリューションの利用を拡大する予定です。

- すべての Web プロパティからオリジナルのボット軽減ベンダーを削除する
- Distributed Cloud Bot Defense の適用範囲を全地域の Web およびモバイルプロパティの 100% まで拡大する
- サービスのダッシュボードで利用可能なデータを活用し、不正行為の分析能力を強化する

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- 823941821