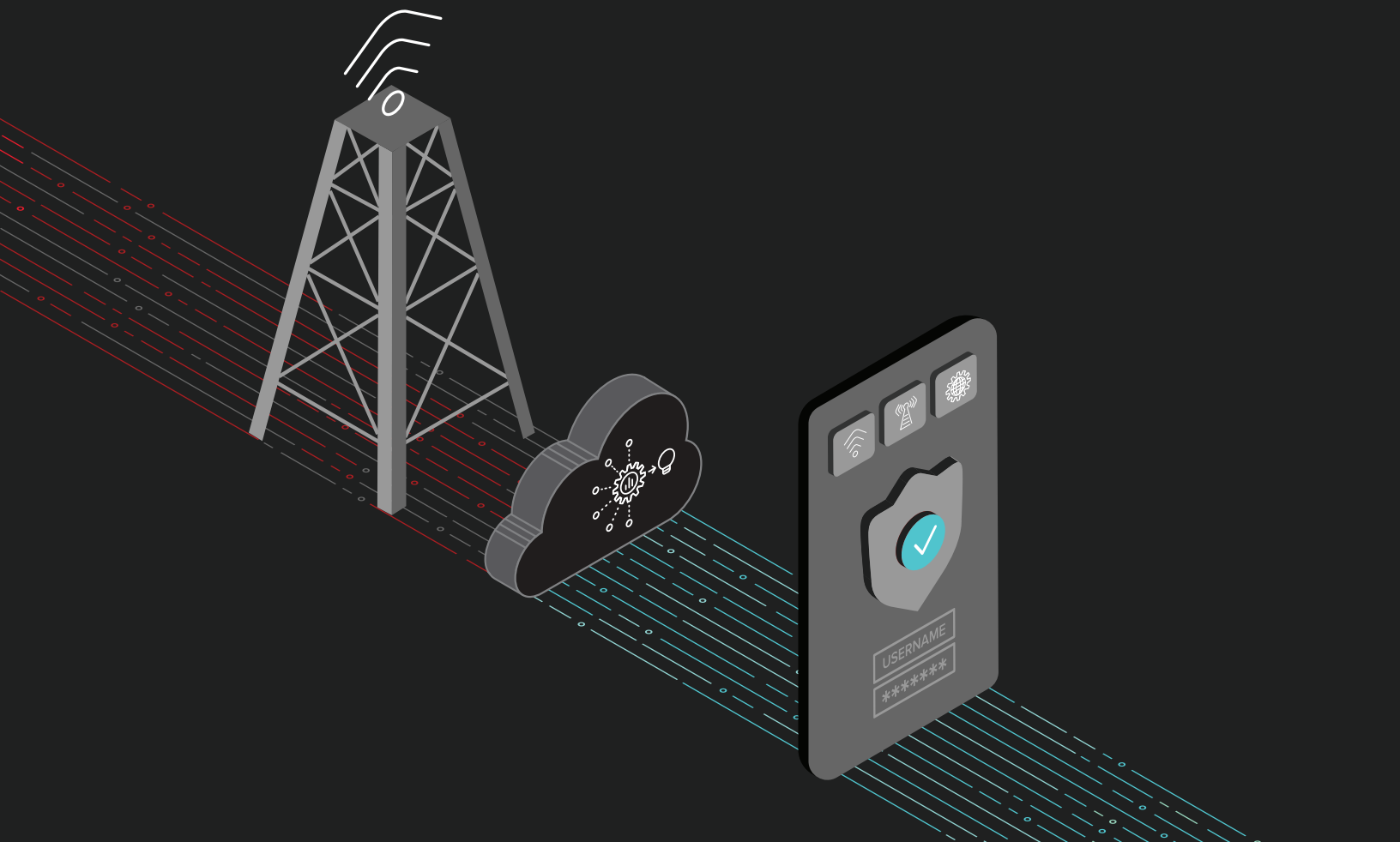
ケーススタディ

トップ3の電気通信プロバイダ、モバイルアカウントのセキュリティを確保



顧客：トップ 3 の電気通信プロバイダ。年間 400 億ドル以上の収益を上げ、約 1 億人の顧客にサービスを提供する米国トップ 3 の電気通信プロバイダ。

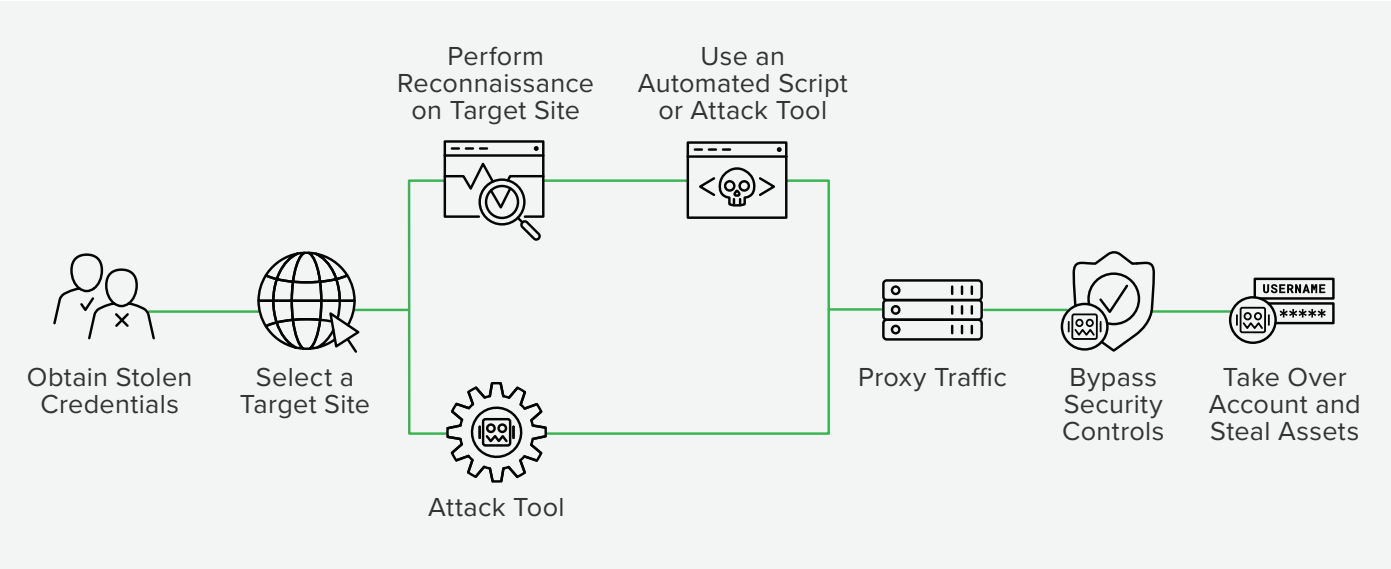


図 1：クレデンシャルスタッフィングのキルチェーン

クレデンシャルスタッフィング攻撃でテストされたすべての認証情報の 0.1% ～ 2%

主な課題：クレデンシャルスタッフィング

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 0.1% ～ 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。

攻撃者は通常、自動化を利用して大規模なクレデンシャルスタッフィングを行います。攻撃者はログインアプリケーション上で認証情報の有効性を確認すると、顧客のアカウントを乗っ取り、不正行為を行います。

2017 年には 20 億件以上の認証情報が流出したことが報告されています。そのため、攻撃者は、常に新鮮な認証情報を電気通信プロバイダで試すことができます。F5 は、顧客データに基づき、米国の電気通信業界は 1 日あたり約 5,000 万件のクレデンシャルスタッフィング攻撃を受けていると推定しています。

クレデンシャルスタッフィング攻撃者は、電気通信プロバイダを標的として、以下のようなさまざまな不正行為を行います。

アップグレードの窃盗

アカウントを乗っ取った後、攻撃者は、被害者に入手権利がある無料または割引のアップグレードを利用します。モバイルデバイスを注文する場合、攻撃者は、自分が管理する配送先住所を

指定するか、「店舗での受け取り」オプションを選択します。後者の場合、攻撃者は、運び屋を店舗に行かせてデバイスを受け取らせ、eBay や Craigslist などのサードパーティマーケットプレイスで転売します。

二要素認証の回避

二要素認証を有効にしている消費者のほとんどは、2 つ目の認証手段として携帯電話を使用しています。攻撃者は、顧客の通信アカウントに侵入できた場合、被害者が金融および電子メールアカウントなど他のアカウントで使用している二要素認証を回避できます。

通信アカウントを乗っ取るときに攻撃者は、カスタマサービスに電話をして、被害者になりすまし、その電話番号と新しい SIM カードを結びつけるよう要求します。その後、攻撃者は、二要素認証のために SMS で送信されるコードを傍受できるようになります。

バーチャルコール

消費者が自分の市外局番から発信された電話に出る確率は非常に高いです。アカウントを乗っ取った後、不正行為者は、電気通信プロバイダのバーチャルコール機能を使って、似たような電話番号を持つすべての人に電話をかけ、電話詐欺の成功率を高めます。

問題点

1. クレデンシャルスタッフィングとその結果のアカウント
2. 乗っ取りが企業に与えた多くの悪影響：
    - 加入者の解約
    - 不正行為による損失
    - コールセンターへの過負荷

意思決定

この電気通信プロバイダは、アカウント乗っ取りが頻発したことで、ネガティブな報道を受けるようになり、すぐに解決策を見出す必要があると考えました。F5 がクレデンシャルスタッフィングを包括的に阻止できる唯一のベンダーであったため、それを選択することは明確でした。問題解決が比較的急務であったことから、この電気通信プロバイダは、F5® Distributed Cloud Bot Defense を Web ログインだけでなく、パスワード回復とアカウント作成のアプリケーションにも導入することにしました。[1]

結果：94% の自動化を検出

導入して 1 週間、Distributed Cloud Bot Defense は、ログインアプリケーションのすべてのトラフィックの 94%、つまり約 6,500 万件の POST が自動化されていることを検出しました。そのうち、5,000 万件以上のリクエストは、クレデンシャルスタッフィング攻撃でした。このサービスは、そのすべてについてオリジンサーバーへの到達を阻止できました。

Distributed Cloud Bot Defense は、この電気通信プロバイダが受信していた他の種類の自動化されたトラフィックも解明できました。たとえば、このサービスは、電気通信プロバイダが受信していた 100,000 を超える POST が、金融アグリゲータの Mint から発信されていることを特定しました。

Mint のような金融アグリゲータは、Web スクレイパーとして動作し、顧客の金融アカウントの実際の認証情報を求め、顧客に代わって継続的にログインし、金融データをスクレイピングして、そのデータを独自のアプリで表示します。特に、Mint は、電気通信プロバイダの顧客の一部が利用する請求書の自動支払い機能を提供しており、そのため安定した POST が発生します。電気通信プロバイダは、Distributed Cloud Bot Defense を導入したことで、これまで知られていなかったこのトラフィック源を特定し、アグリゲータのトラフィックを観察および管理できるようになったことに満足しています。

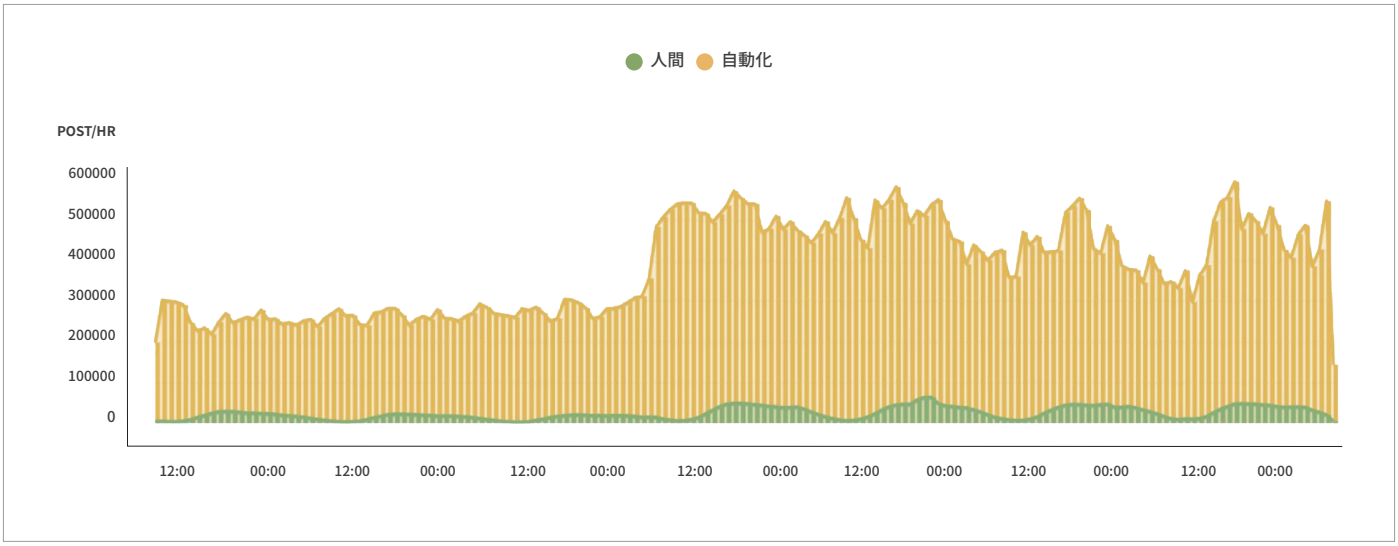


図 2：導入後 1 週間のログイントラフィック

次のステップ：モバイル保護

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。F5 の顧客の多くは、Distributed Cloud Bot Defense 導入後の最初の数週間または数か月間で、このサービスにより、Web アプリケーションへの攻撃が積極的に軽減され、攻撃者がモバイルアプリに標的を変えていることを観察しています。

電気通信プロバイダは、クレデンシャルスタッフィングの大量のトラフィックが示すように、攻撃者にとって極めて魅力的な標的です。これらの攻撃者の一部が、標的をモバイルアプリに変えることは確実です（完全に他社に移動するだけではありません）。そのため、この電気通信プロバイダは間もなくモバイルアプリにも保護を拡大する予定です。

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。

[1] これら 2 つのアプリケーションは、攻撃者がクレデンシャルスタッフィングやアカウント乗っ取りの成功率を上げるためによく利用されます。