ホワイトペーパー

攻撃、望ましくない自動化、オンライン不正行為から金融アプリケーションを守る

金融機関向けのボットおよび不正対策ソリューション

攻撃者は、実際の顧客や見込み客を装って、アプリケーションの正面から入り込むだけです。

偽のアプリケーショントラフィックの増加とリスク：世界で最も多く利用されている金融アプリケーションの守護者として、F5 は、金融機関の Web およびモバイルアプリケーションを狙った攻撃がどのように進化しているかを独自の立場から観測しています。

最も被害が大きい攻撃、つまり、最も多額の損害を与え、最も多くの顧客に被害を与え、最も頻繁に発生する攻撃の多くは、斬新で新しい攻撃手法を利用しています。これらの攻撃には、合成 ID と実際の顧客のエミュレーションを組み合わせた、偽のトラフィックが利用されます。攻撃者は、実際の顧客や見込み客を装って、アプリケーションの正面から入り込むだけです。これらの攻撃手法は、アプリケーションのコーディング上の欠陥や脆弱性を必要としないため、主流のセキュリティ制御を回避できます。また、適切にコーディングされ、安全なソフトウェア開発ライフサイクルの一部であるアプリケーションに対しても有効です。その結果、オンライン上で本物と偽物を見分けることは、今日のセキュリティ環境において金融機関が直面する最大の課題の 1 つです。

金融機関アプリケーションへの偽のトラフィックは、さまざまな形態の攻撃、望ましくない自動化、不正行為、悪用を引き起こします。

図 1：偽物のトラフィックとビジネスへのそれぞれの影響

Fake Traffic Threat or Challenge	Business Impact
Credential stuffing	Credential stuffing attacks on web and mobile apps, APIs, and OFX lead to account takeover and new account creation fraud, driving material fraud losses. Large-scale credential stuffing attacks also contribute to site performance issues and can even lead to site outages.
Unmanaged third-party fintech apps	By default, user-enabled, third-party fintech tools log into financial institution apps as if they are actual users. Without proper visibility, management, and controls, these tools can create unnecessary application load and are also being used by cybercriminals as an attack vector to disguise credential stuffing attacks against financial institution apps.
Client-side malware attacks	Man-in-the-browser (MiTB) client-side malware can abuse Zelle and Interac systems to make fraudulent money transfers by hijacking legitimate user browser sessions.
Manual fraud	Fraudsters emulate real users in order to take over accounts or create fake new accounts.

クレデンシャルスタッフィング：金融機関に対するアプリケーションの主要な脅威

金融機関に対するクレデンシャルスタッフィング攻撃は、日常的に起きているとされるデータ侵害によって盗まれた認証情報を利用したサイバー犯罪者が、金融機関のアプリケーションに不正にログインする、または偽の新規アカウントを作成することによって発生します。

F5 Labs が最近発表した調査によると、金融機関はクレデンシャルスタッフィングをアプリケーションの最大の脅威と認識していて、また、トレンドからは、問題が悪化の一途をたどっていることが示されています。
クレデンシャルスタッフィング攻撃は比較的安価で実行できることや、顧客が金融口座の管理に使用するデジタルチャネルが増え続けていることを考えると、当然の結果といえます。

	2016	2017	2018	2019	2020
Number of Spills	52	49	101	77	117
Total Credentials Spilled	3,301,824,415	2,328,576,631	1,978,746,345	2,255,253,881	1,860,648,946
Average Spill Size	63,478,585	47,521,972	19,591,548	29,289,011	16,762,603
Median Spill Size	2,750,000	996,000	411,755	598,683	2,000,000
Maximum Spill Size	1,000,000,000	2,000,000,000	336,000,000	763,117,241	538,000,000
Minimum Spill Size	100	3,120	858	277	2,200

図 2：2016 年から 2020 年までの認証情報流出の概要

多くのアプリケーションにおいて、クレデンシャルスタッフィングやその他の自動化攻撃のトラフィックは、ログイン、新規アカウント作成、パスワード再設定、その他の重要なアプリケーションフローに対するトラフィック全体の 50% 以上を占めているといえます。

ユーザー対応型フィンテックツール：管理の問題とセキュリティリスク

サードパーティのユーザー対応型フィンテックツールは、金融機関にとって多くの課題をもたらすことがあります。これらのツールは、一般的な銀行のアプリケーショントラフィックの最大 20% 以上を占めるとされ、実際のユーザーの 2.5 倍の頻度でログインします。フィンテックツールの可視化と管理制御が不十分なため、アプリと API の最適化およびセキュリティに取り組む金融機関に課題が生じています。

さらに、攻撃者は、金融機関のアプリ自体よりも保護が不十分なフィンテックツールを介して、クレデンシャルスタッフィングやその他の自動化攻撃を仕掛ける新しい創造的な方法を編み出しています。すべてのサードパーティ API へのアクセスをオフにしなければ、フィンテックを介したこれらの攻撃を検出および管理することは特に困難です。

MITB マルウェアは最初から、基本的に ZELLE やその他の金融機関のシステムを攻撃し、何百万ドルもの詐欺被害の原因になっています。

クライアントサイドマルウェア：ログイン後の偽の行動

偽トラフィックのもう 1 つの形態は、クライアントサイドマルウェアによるものです。たとえば、Man-in-the-Browser（MiTB）マルウェアは、ユーザー個人のデバイスのブラウザに感染し、ユーザーが金融機関のアプリケーションにログインするのを待ち伏せます。このマルウェアは、ユーザーが知らないうちにバックグラウンドで、振込先の追加や削除、送金、さらには偽の残高情報の表示など、資金を盗むためのステップを開始します。MiTB マルウェアは最初から、基本的に Zelle やその他の金融機関のシステムを攻撃し、何百万ドルもの詐欺被害の原因になっています。

手動による不正行為：ボットを使わない偽のトラフィック

ボットやその他の不正な自動化されたトラフィックは、当然のことながら、セキュリティ上の多くの注目を集めています。しかし、金融機関のアプリケーションに対して手動で行われる不正行為は、多くの不正対策ツールが導入されているにもかかわらず、依然としてリスクと損失の重大な原因となっています。サイバー犯罪者は、より安価な自動化攻撃で同様の結果を得られない場合、価値の高いターゲットに対して、アカウントの乗っ取りや新規アカウント作成など、このような人力による攻撃を集中して仕掛けます。

金融機関のアプリケーションを偽のトラフィックから守る F5 の防御

F5 のコンバージドプラットフォームは、さまざまな先進技術を活用することで、金融機関の Web およびモバイルのアプリケーションや API を幅広いセキュリティ脅威と不正行為リスクから守ります。

- F5® Distributed Cloud Bot Defense：クレデンシャルスタッフィングや、「OWASP Automated Threats to Web Applications」のその他の脅威を含む自動化攻撃を阻止します。
- F5® Distributed Cloud Account Protection：不正行為を阻止し、オンライン不正行為をリアルタイムで削減する新しい強力なツールを不正対策チームに提供します。
- F5® Distributed Cloud Aggregator Management：フィンテックツールを管理し、これらのツールを介した攻撃から防御するための可視化と制御を提供します。
- F5® Distributed Cloud Client-Side Defense：感染したクライアントブラウザによって引き起こされる、人間によるものではない送金を検知および防止できます。

他のツールにはないセキュリティ効果

F5 は、運用の手間がかからないフルマネージドサービスとして、セキュリティと不正防止の効果を提供します。また、攻撃者は常に進化しているため、F5 のソリューションは、高度な AI および機械学習と、F5 の 24x7 体制の Security Operations Center を活用して、新たな脅威にリアルタイムで対応できるよう備えています。

世界トップクラスの金融機関を守るセキュリティソリューション

米国の消費者向け銀行業界は、クレデンシャルスタッフィングにより、年間最大 17 億ドル損失しています。このようなインシデントが引き起こすコストと評判へのダメージを考慮すると、信頼できるソリューションが必要です。

F5 は、1 日に何十億ものアプリケーション攻撃を検知および防御することに成功しています。F5 が世界有数の金融機関のアプリケーションを守るなかで学んだことはすべて、あらゆる金融機関のアプリケーションを不正行為や悪用から守るために活かされています。

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。