Press Release

2022 年 9 月 26 日

Okta Japan 株式会社

報道関係者各位

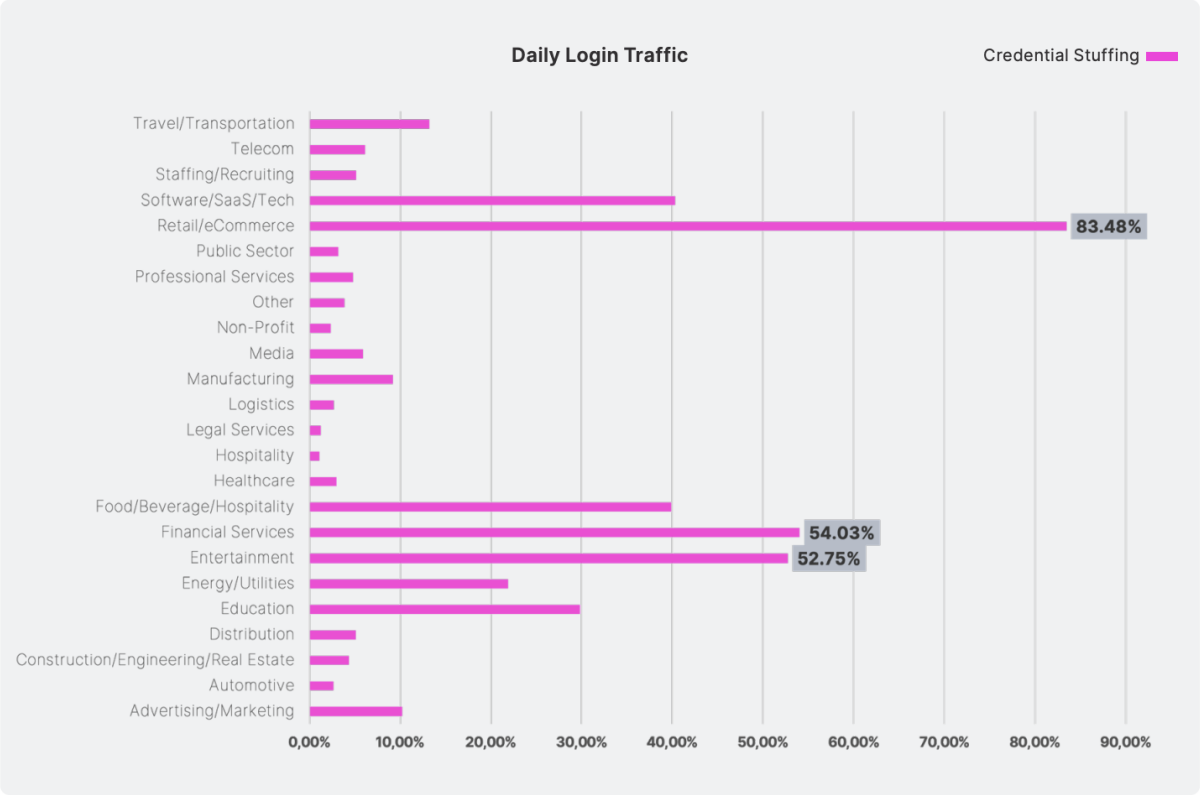
顧客 ID に対する攻撃動向を考察する 2022 年版レポート「2022 State of Secure Identity Report」を公開

Okta Japan 株式会社（本社: 東京都渋谷区、代表取締役社長： 渡邉 崇）は、Okta の顧客 ID 管理プラットフォーム（Auth0）を利用する世界中のお客様のデータに基づいて、顧客 ID に対する攻撃動向を考察する 2022 年版レポート「2022 State of Secure Identity Report」を公開しました。

本レポートでは、2022 年の最初の 90 日間に、Okta の顧客 ID 管理ソリューションのプラットフォーム（Auth0）上で行われた認証を観察して得られた、顧客 ID に対する攻撃の傾向、事例、考察を紹介しています。こうしたインサイトを明らかにすることで、顧客 ID に対する脅威の理解を促進する一助になればと考えています。

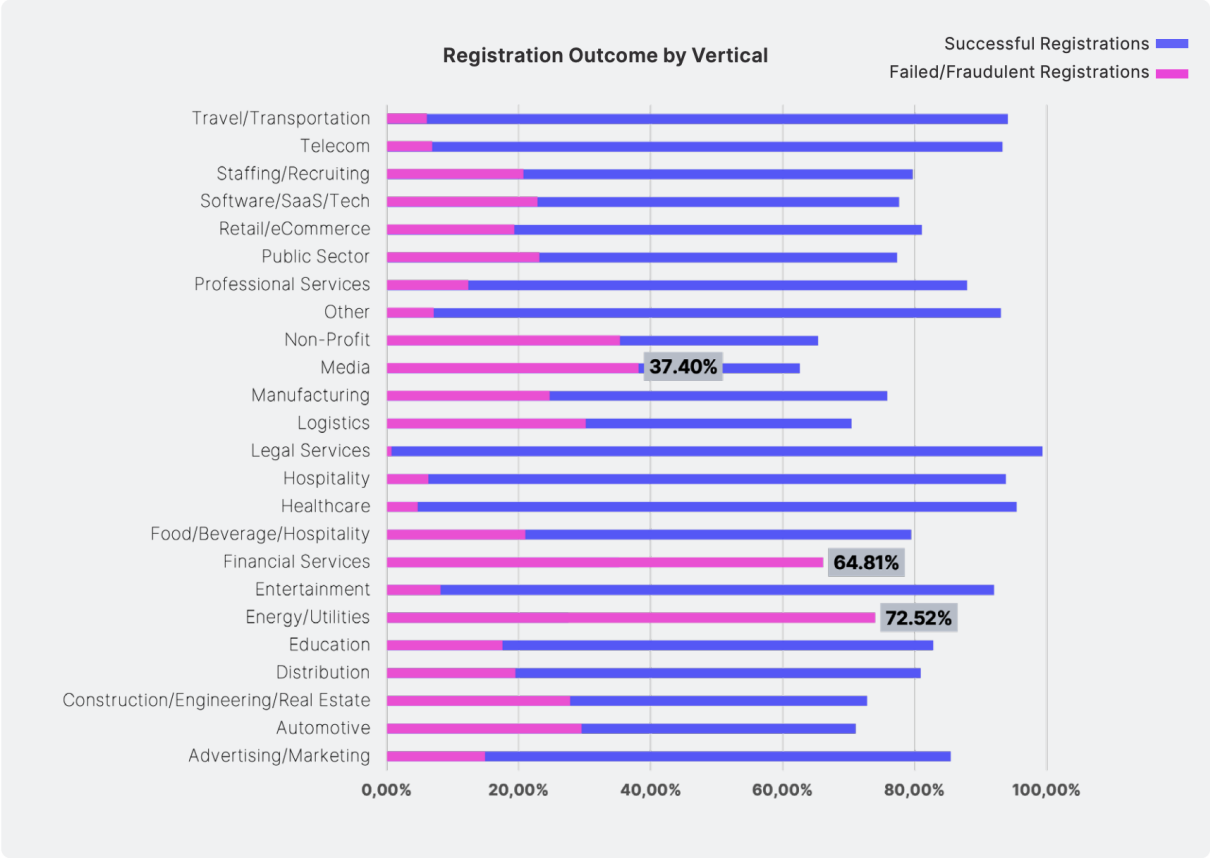
クレデンシャルスタッフィング攻撃が記録的なペースで進行

2022 年の最初の 90 日間で、当社プラットフォーム上で約 100 億件のクレデンシャルスタッフィング攻撃を検出しました。これは全体のトラフィック/ 認証イベントの約 34%に相当します。ほとんどの業種でクレデンシャルスタッフィング攻撃の割合は 10%未満でしたが、「小売/e コマース」では、観測されたログイントラフィックの 80%以上がクレデンシャルスタッフィング攻撃であることが高い信頼度で判定されました。また、「金融サービス」と「エンターテイメント」でも、クレデンシャルスタッフィング攻撃がログイントラフィックの 50%以上を占めることが確認されました。



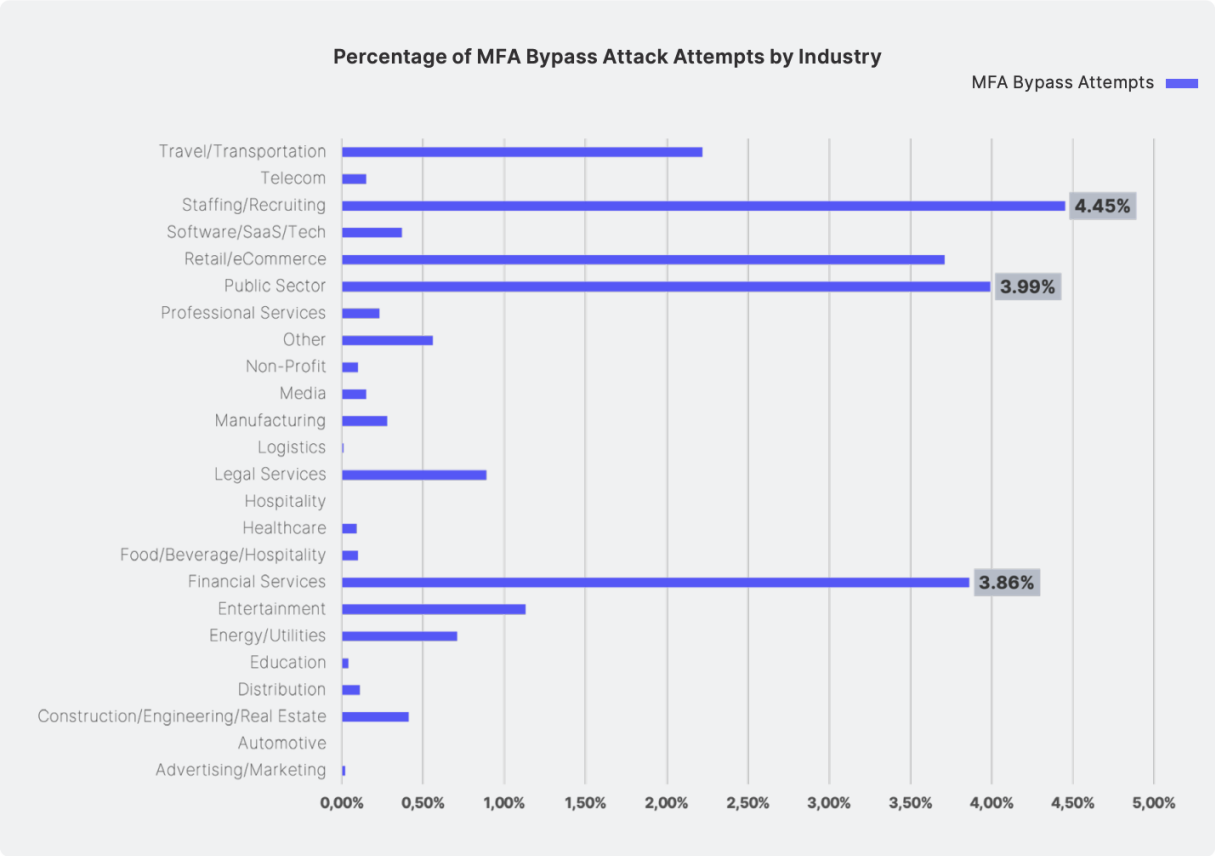
不正なアカウント登録による脅威の拡大

2022 年の最初の 90 日間で、当社プラットフォーム上で約 3 億件の不正なアカウント作成の試みを観測しました。その試みはサインアップ試行の約 23%（昨年同期の 15%からアップ）を占めます。特に、サインアップ攻撃の割合が最も高い業種は、「エネルギー/公益事業」（72.52%）と「金融サービス」（64.81%）でした。



脅威者は価値の高いターゲットの MFA を集中的に攻撃

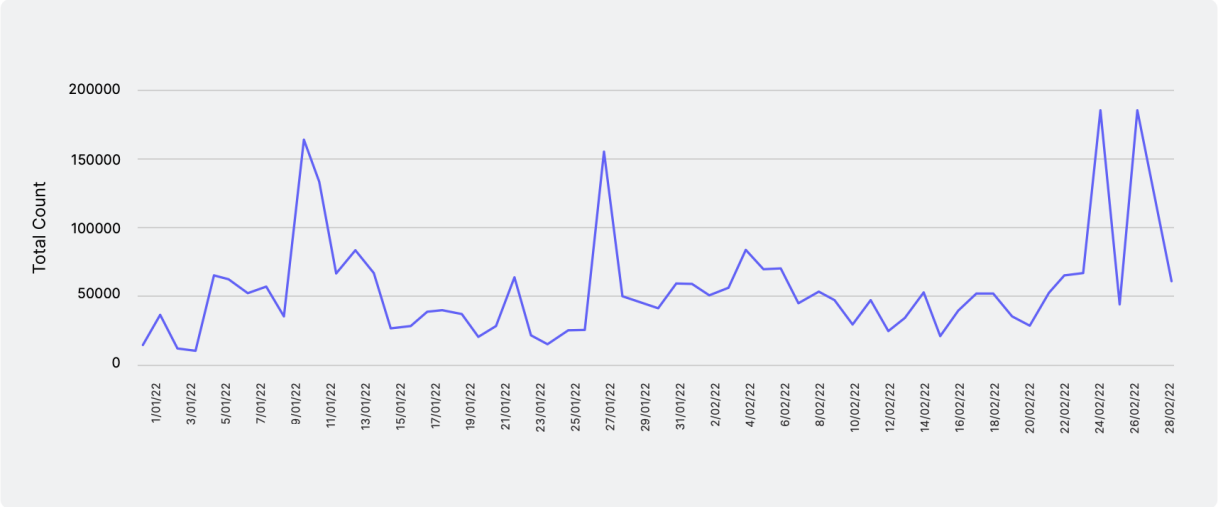
2022 年の最初の 90 日間で、当社プラットフォーム上で MFA に対する約 1 億 1,300 万件の攻撃を観測しました。MFA をうまく回避するためには労力が必要なため、このような MFA バイパス攻撃は価値の高いターゲットに集中する傾向があります。実際、業種別の攻撃率を調べると、脅威者は「人材派遣/人材紹介」、「公共部門」、「小売/e コマース」、「金融サービス」に攻撃を集中していることがわかります。



漏洩した認証情報による攻撃

漏洩した認証情報を利用したアカウント乗っ取り攻撃は、最も一般的でコストのかかるサイバー脅威の１つです。第三者による不正アクセスで流出した認証情報のリストを販売するマーケットプレイスも存在します。実際、当社のプラットフォームを利用する全顧客のアプリケーションの 58%は、漏洩した認証情報を利用した攻撃を少なくとも１回は経験しています。さらに、漏洩したパスワードの保護をうたうサービスのほとんどは、ウェブスキャナーやスクレイパーを使用しており、漏洩したデータが公開されることを前提にしているため、最初の漏洩から数ヶ月、あるいは数年経っている可能性があります。

下記の図は、当社のプラットフォームで観測された１日あたりの使い回しされた認証情報の量を示しています。１日あたり約 50,000 件の基底レベルは、主にユーザー側でのパスワード使い回しに起因し、クレデンシャルスタッフィング攻撃は少量となっていますが、図中の急増している部分は、漏洩した認証情報を使用した大規模な攻撃の発生を示しています。



顧客 ID を狙った攻撃を阻止するための基本的な推奨事項

今日の高度な顧客 ID を狙ったクレデンシャルスタッフィング攻撃、サインアップ攻撃、MFA バイパス攻撃を阻止するには、自社でアイデンティティスタックを構築するよりも、顧客 ID 管理ソリューションを導入することがはるかに効果的なアプローチです。

アプリケーション構築者の課題は、ユーザーエクスペリエンスを尊重しながら、攻撃者の摩擦を高めるという適切なバランスを保つセキュリティ対策を開発し、実装することです。

社内で独自のソリューションを開発する場合でも、アイデンティティ管理サービスを利用する場合でも、顧客 ID を狙った攻撃を阻止するには、次のような基本的な推奨事項があります。

MFA の導入と奨励：MFA は攻撃を阻止する最も効果的な方法の 1 つです。強力なセカンダリ要素を持つ複数の方法を導入し、ユーザーでの採用を奨励しましょう。WebAuthn を採用し、サポートされているデバイスで有効化してください。

ログインの試行回数を制限する：ブルートフォース攻撃、クレデンシャルスタッフィング攻撃、パスワードスプレイング攻撃は、ログインの成功にともなって多くのログイン失敗も発生しがちです。この挙動を利用して、攻撃を検知し、対策を講じてください。

漏洩したパスワード使用の監視：多くのユーザーが複数のサイトで同じまたは類似のパスワードを再利用しているため、1つのサービスでの侵害が他の多くのサービスに脅威を与える可能性があります。漏洩した認証情報をユーザーに変更させてください。

本レポートの完全版（英語）は以下よりダウンロードしてください。
https://auth0.com/resources/whitepapers/2022-state-of-secure-identity-report

調査方法

本レポートは、Okta の顧客 ID 管理プラットフォーム（Auth0）を利用する世界中のお客様のデータに基づいており、顧客 ID 攻撃に関する現実的な観察結果を表しています。データは、当社のセキュリティ研究者が、運用遠隔測定データベースに対して匿名性の高いクエリを実行することにより取得したものです。業種区分は、各顧客が自己申告した区分に基づいています。特に断りのない限り、2022 年の最初の 90 日間を対象としています。

Okta について

Okta は、すべての人のアイデンティティとアクセスを安全に管理するベンダーニュートラルなサービスプロバイダーです。Okta が提供するプラットフォーム「Okta Identity Cloud」により、クラウド、オンプレミスを問わず、適切な人に適切なテクノロジーを適切なタイミングで安全に利用できるようにします。7,300 以上のアプリケーションとの事前連携が完了している「Okta Integration Network」を活用して、あらゆる人や組織にシンプルかつ安全なアクセスを提供し、お客様の潜在能力を最大限発揮できるように支援します。JetBlue、Nordstrom、Siemens、Slack、武田薬品、Teach for America を含む 16,400 以上のお客様が Okta を活用して、職場や顧客のアイデンティティを保護しています。
https://www.okta.com/jp/

【本件に関するお問い合わせ先】
■ Okta Japan 株式会社
広報担当：中田清光
Email: kiyomitsu.nakata@okta.com
■Okta PR 事務局（株式会社プラップジャパン内） 担当：山本 •中根 •冨安 •藤沢
TEL: 080-9821-6995（山本携帯）、080-6859-3639（中根携帯）
Email: okta@prap.co.jp