2020 年 3 月 26 日
Press Release
アカマイ・テクノロジーズ合同会社

Akamai、最新の脅威レポートを発表
金融サービス機関を狙ったサイバー犯罪で API が標的に
不正ログイン全体の 75% が API を標的としていたことが判明

Akamai Technologies, Inc. (NASDAQ：AKAM) は、「SOTI インターネットの現状／セキュリティ: 金融サービス– 敵対的アカウント乗っ取り攻撃」レポートを発表しました。調査の結果、2019 年 5 月から 2019 年末までの期間に、攻撃の傾向が大きく変化したことがわかりました。攻撃者は API を標的として狙い始め、セキュリティ制御を回避しようとしています。Akamai のデータによると、金融サービス業界に対する不正ログイン（Credential Abuse）全体の 75% が直接 API を標的としていました。

本レポートの調査結果によると、2017 年 12 月から 2019 年 11 月までに、Akamai は 854 億 2,207 万 9,109 回の 不正ログインの試行を観測しました。その 20% 近く（165 億 5,787 万 5,875 回）は、明確に API エンドポイントであると特定できるホスト名に対する攻撃でした。さらに、これらのうち、金融サービス業界の組織に対する攻撃は、4 億 7,351 万 8,955 件でした。

しかし、すべての攻撃が API だけを標的にしていたというわけではありません。2019 年 8 月 7 日には、ある金融サービス企業に対してリスト型攻撃 (Credential Stuffing) が行われ、5,514 万 1,782 回もの不正なログイン試行が観測されました。これは、1 回の攻撃として Akamai 観測史上最大の規模です。この攻撃では、API 標的攻撃と他の攻撃手法が併用されていました。また、8 月 25 日に発生した別の攻撃は、直接 API を標的としたものでしたが、1,900 万回を超える 不正ログイン試行が確認されました。

Akamai のセキュリティリサーチャーであり、「SOTI インターネットの現状／セキュリティ」レポートの主著者ある Steve Ragan は、「犯罪者は、目的とする犯罪の達成に必要なものへのアクセス権を得るため、新たな方法を生み出すことに注力しています。金融サービス業界を狙う犯罪者は、金融サービス機関が使用している防御策に細心の注意を払い、攻撃パターンを適宜、調整します」と述べています。

攻撃は流動的で変化しやすく、犯罪者は引き続きさまざまな手法でデータの侵害を図っていることがわかります。サーバー上に強力な足場を築き、最終的な犯罪目的を達成するためです。

このレポートの対象となっている 24 カ月の期間について、全業界のデータを見たところ、SQL インジェクション（SQLi）が攻撃全体の 72% 以上を占めていました。一方で金融サービスに対する攻撃だけを見てみると、その割合は半分の 36% にとどまっています。金融サービスセクターに対する攻撃タイプとして最も多かったのはローカル・ファイル・インクルージョン（LFI）であり、観測されたトラフィックの 47% でした。

LFI 攻撃はサーバーで稼働するさまざまなスクリプトを標的とするため、このタイプの攻撃には、機微な情報を強制的に開示する手法が利用される可能性があります。また、LFI 攻撃は、クライアント側で悪意のあるコマンド（脆弱な JavaScript ファイルなど）を実行することにも利用されます。これは、クロスサイトスクリプティング（XSS）攻撃やサービス妨害（DoS）攻撃につながる可能性があります。XSS は金融サービスに対する攻撃のなかで 3 番目に多い攻撃タイプです。攻撃数は 5,070 万件で、観測された攻撃トラフィックの 7.7% に該当します。

このレポートの調査では、犯罪者が手持ちの攻撃手法として引き続き、 DDoS (分散型サービス妨害) 攻撃を活用していることもわかりました。特に金融サービス業界の組織を標的とする攻撃でこの傾向が顕著です。2017 年 11 月から 2019 年 10 月までの期間における Akamai の観測では、金融サービス業界は攻撃ボリュームで第 3 位となっています。最も標的となりやすい業界はゲームとハイテクでした。一方、重複を除いた DDoS 標的数については、総数の 40 %以上が金融サービス業界であり、犠牲となった組織の数（重複を除いた数）では金融サービス業界がトップとなっています。

「攻撃者は十分に組織化され、資金も豊富である場合が多く、セキュリティチームがこうした攻撃者を撃退するためには、常にポリシー、手順、ワークフロー、ビジネスニーズの検討を続ける必要があります。Akamai のデータをみる限り、金融サービス業界の組織は、変化に対応できるセキュリティ対策を採用することで、絶えず手法を改善していますが、それに応じて犯罪者の方も手法を変化させています。」

Akamai 2020 年「SOTI インターネットの現状／セキュリティ」レポートは、こちらからダウンロードいただけます。

セキュリティに携わる方々に参考になるような、Akamai の脅威リサーチャーの見解や、変化する脅威の状況に関して Akamai Intelligent Edge Platform から得られる知見をご紹介する Akamai の脅威リサーチハブもご参照ください。

Akamai について

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザー

の最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日/24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai でご紹介しています。