イノベーションに潜む高いリスク

金融サービス業界の攻撃トレンド

前例のないデジタルトランスフォーメーションを特徴とする今の時代において、金融サービス業界はイノベーションとリスクの岐路に立たされています。テクノロジーは、金融取引の状況を刷新すると同時に、経済の安定の中心を狙う新たな脅威の時代も招いています。

金融サービスとその顧客に対する攻撃

90 億
金融サービスに対する Web アプリケーション攻撃と API 攻撃の数

第 1 位
金融サービスは、最も多くの DDoS 攻撃を受けた業界であり、その数はゲーム業界を上回っています

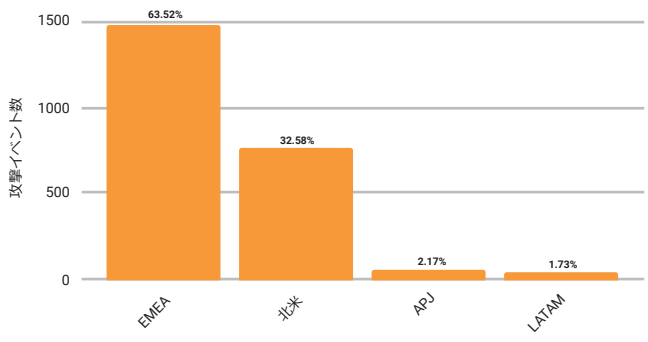
50.6%
金融サービスは、2023 年第 2 四半期のフィッシング攻撃の被害者数が最多となっています

1 兆以上
悪性ボットリクエストの数

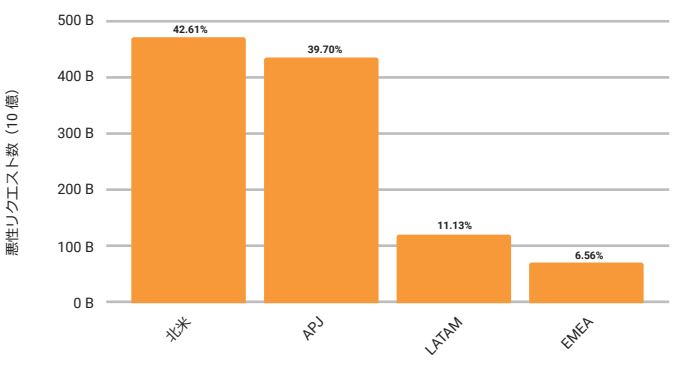
地域別のスナップショット

ヨーロッパ、中東、アフリカ（EMEA）地域におけるレイヤー 3 とレイヤー 4 の DDoS 攻撃の数は、北米の約 2 倍に達しています

地域別の DDoS 攻撃イベント数：金融サービス
2022 年 1 月 1 日～2023 年 6 月 30 日



地域別の悪性ボットリクエスト数：金融サービス
2022 年 1 月 1 日～2023 年 6 月 30 日



アジア太平洋・日本（APJ）地域は、2 番目に多く悪性ボットリクエストの標的となっている地域です

警戒するべき潜在的なセキュリティリスク

シャドウ API
ドキュメント化されていない API や追跡されていない API は、誰がどのような方法でこれらの API を使用しているのかを認識していない企業にとって、監視上の問題となる可能性があります。

サードパーティーのスクリプト
攻撃者は、クライアントサイドの脆弱性を悪用したり、Web サイトの一部として読み込まれるサードパーティーのスクリプトに悪性コードを挿入する可能性があります。これによって金融サービス企業は Web スキミングのリスクに晒され、顧客のデータが盗まれたり、不正なトランザクションに使用されたりする恐れがあります。

金融アグリゲーター
金融アグリゲーター間のセキュリティギャップやデータの収集方法を利用して攻撃者は新たな悪用手段を生み出し、アイデンティティ窃取につながる可能性があります。

セキュリティ上の推奨事項とベストプラクティス

- アタックサーフェスを理解して、緩和戦略を策定し、セキュリティ制御を確立する
- 不正な API を検知・監視するための API セキュリティツールを導入する
- OWASP API Security Top 10 および MITRE ATT&CK フレームワークを活用して、レッドチーム／侵入テストグループのトレーニングおよびテスト計画を作成する
- 定期的なセキュリティ監査を実施し、高度な検知と緩和を実装するなど、多層的な防御戦略を採用する
- クライアントサイドの攻撃によるリスクを緩和できる、Client-Side Protection & Compliance（旧 Page Integrity Manager）などのソリューションを導入する
- エッジベースのガバナンスモデルを構築して、ボット／API トラフィックを可視化する
- 過去 3 四半期に DDoS 攻撃を受けていない場合は、ライブ演習を実施する。プレイブックを検証し、攻撃規模と速度の両方の傾向を追跡して、現在の能力に基づいてリスクを評価する

金融サービス業界における攻撃の傾向に関する詳細と知見については、レポートの全文をお読みください。

レポートをダウンロード

 | サポート | 公開日：2023 年 10 月