2023 年 1 月 12 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：金融サービス業界の Web アプリケーションおよび API に対するサイバー攻撃の調査結果を発表

APJ 地域でのサイバー攻撃は前年比 449%増加、約 14 億件の攻撃
特に日本・インド・オーストラリアが最も多く攻撃を受けていることが判明

※本リリースは 2022 年 11 月 28 日 (現地時間) マサチューセッツ州ケンブリッジで発表されたプレスリリースをベースに、APJ 地域での傾向を取り上げた編集版です。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、最新の調査レポート「SOTI インターネットの現状／セキュリティ：差し迫る敵」を発表しました。このレポートでは、攻撃の活発化と攻撃手法の巧妙化により、アジア太平洋・日本（APJ）地域の金融サービス業界が深刻なリスクに直面していることを指摘しています。特に、Web アプリケーション攻撃と API への攻撃が警戒すべき速さで増加しており、その複雑さも増しています。さらに、本レポートによると、サイバー攻撃者の約 80% は、最も抵抗の少ない方法を通じて金銭的利益を得るために、金融機関ではなく、金融サービスの顧客を標的としています。例えばアカウント乗っ取り攻撃やフィッシングはここで指摘されている顧客を直接狙う攻撃です。

APJ の金融サービス機関は、複数の重要分野（Web アプリ攻撃と API 攻撃、DDoS、フィッシング、ゼロデイ・エクスプロイト、ボットネット活動）において、最も多くの攻撃を受けている業界の 1 つです。最も懸念されるのは、Web アプリケーション攻撃と API への攻撃の急増です。APJ の金融サービス業界に対する攻撃は前年比で 449% 増加しています。Akamai は今年初め、ランサムウェア集団が脆弱性を悪用して侵入する際によく使用する Web アプリケーションおよび API への攻撃ベクトルを発見しました。Web アプリケーション攻撃と API への攻撃が APJ で急増している背景には、同地域に高 GDP 国が含まれることが関係していると考えられます。その反面で、サイバーセキュリティに関するスキルや人材が不足していることも要因となっている可能性もあります。攻撃者の標的を把握することで、APJ の組織やセキュリティ担当者はリスクを正確に理解し、潜在的な弱点を優先的に保護できます。

その他にも、このレポートでは以下のことが明らかになりました。

- 攻撃の増加と巧妙化により、APJ での Web アプリケーションおよび API への攻撃が増加しているが、この地域でランサムウェアに起因するサイバー攻撃が増加していることと一致している。最近発表した Akamai ランサムウェア脅威レポート「APJ Deep Dive 2022 年上半期」では、Web アプリケーション攻撃と API への攻撃およびランサムウェアの関係について指摘している。

- APJ で Web アプリ攻撃と API 攻撃を最も多く受けているのは、オーストラリア、日本、インドである。

- 新たに発見されたゼロデイ脆弱性が金融サービス業に対して悪用されると、24 時間以内に 1 時間あたりの攻撃が数千回となり、急速にピークに達する可能性がある。そのためパッチの適用や対応にかける時間はほとんどない。

- ローカル・ファイル・インクルージョン（LFI）攻撃とクロス・サイト・スクリプティング（XSS）攻撃の大幅な増加は、攻撃者が、社内ネットワークのセキュリティに多大な負担をもたらすリモートコード実行に移行していることを示している。

- 金融サービス業界の顧客を標的とするフィッシングキャンペーンでは、金融機関が用意した二要素認証ソリューションを突破する攻撃手法が用いられている。

- 顧客アカウントの乗っ取りが攻撃タイプの 40% 以上を占めている。さらに、より巧妙なフィッシング詐欺に利用するための Web スクレイピングも 40% を占めている。

「金融サービス業界は、新たな脆弱性が発見された際に最も多くの攻撃を受ける業界の 1 つです。金融サービス機関の顧客は常に DDoS 攻撃やフィッシングキャンペーンの標的となっており、これらの攻撃の被害を受けています」と、Akamai の Advisory CISO の Steve Winterfeld は述べています。「攻撃者は、ネットワークに侵入したり、顧客に被害をもたらしたりする方法を常に模索しています。アタックサーフェスを理解することで重大なリスクに関する知見を得て、セキュリティ制御や緩和計画を策定し、顧客の保護を強化できます」。

詳細な情報については、新しい Akamai セキュリティハブにアクセスするとともに、Twitter で @Akamai_Research をフォローしてください。Akamai の脅威リサーチャーと交流し、貴重な知見を得ることができます。

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。クラウドからエッジまで、世界で最も分散されたコンピューティングプラットフォームにより、Akamai は、アプリケーションの開発や実行を容易にし、同時に、体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。