2024 年 9 月 25 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：アジア太平洋地域では金融機関が DDoS とフィッシング攻撃の最大の標的となっていることが明らかに

API の導入が増加したことにより、アジア太平洋・日本（APJ）地域の金融サービス業界がサイバー攻撃に対して脆弱に

※本リリースは 2024 年 9 月 18 日 (現地時間) シンガポールで発表されたプレスリリースの抄訳版です。

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、最新のインターネットの現状（SOTI）レポート「高まる波を乗りこなす：金融サービス業界の攻撃トレンド」において、金融サービス業界は 2 年連続で世界で最も頻繁にレイヤー 3 および 4 の DDoS 攻撃の標的となっている業界であることを明らかにしました。DDoS 攻撃の標的となった業界のうち 34%が金融サービスで、次いでゲームが 18%、ハイテクが 15%となっています。

金融機関は膨大な量の機微な情報と高価値のトランザクションを管理しており、攻撃が成功すれば大きなリターンに繋がるため、DDoS 攻撃者にとって魅力的なターゲットとなっています。レイヤー 3 およびレイヤー 4 の DDoS 攻撃は、ネットワークレイヤーとトランスポートレイヤーを標的とし、ネットワークインフラを過負荷状態にして、サーバーリソースと帯域幅を枯渇させます。金融機関に対する DDoS 攻撃が成功すると、顧客の信頼への影響、ダウンタイムの発生、規制上の罰則など、深刻な問題につながる可能性があります。そのため、攻撃者は多くの場合、金融機関を標的にすることで潜在的な実益を最大限に高めようとします。

「高まる波を乗りこなす：金融サービス業界の攻撃トレンド」では、DDoS イベントの増加は、今なお続く地政学的緊張によりハクティビスト活動の増加が加速したことに端を発することが明らかになりました。同レポートでは、REvil、BlackCat（ALPHV）、Anonymous Sudan、KillNet、NoName057 などの攻撃者の関与について詳しく説明しています。これらはすべて、ロシア・ウクライナ紛争に関連する活動で注目を浴びています。さらに、イスラエル・ハマス紛争をきっかけに、世界の金融機関に対する大規模なサイバー攻撃がどのように開始されたかについても説明しています。

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。

- 金融サービスはブランドのなりすましと悪用の影響を最も受けている業界である（36%）これは、Akamai が監視している不審なサイトの総数に基づいています。標的とされることが 2 番目に多い業界はコマースであり（26%）、1 位と大きな差があります。

- フィッシングは金融サービスを標的とする偽ドメインの中で最多であり、記録されたすべてのインスタンスの 68% を占めている第 2 位はブランドなりすましで、記録されたすべてのドメインの 24% を占めています。

- 特に API を介してアプリケーションを標的とするレイヤー7DDoS 攻撃の数が急増している重大な懸念としては、ドキュメント化されていないシャドウ API です。シャドウ API は情報セキュリティチームに存在を認識されていないため、保護されていないことがよくあります。攻撃者はこのような API を悪用して、データを窃取したり、認証制御を回避したり、破壊的な行為を実行したりする可能性があります。

- DDoS イベントの頻度と攻撃の強度が必ずしも相関するとは限らない攻撃がほとんど見られなかった期間が数か月ありましたが、逆にその期間のデータはトラフィックの急増を示しています。これは、DDoS 攻撃を評価する際には攻撃の頻度と量の両方を考慮する必要があることを表しています。

Akamai の Advisory CISO である Steve Winterfeld は「サイバー犯罪は、広範囲にわたる破壊と深刻な経済的損害をもたらすため、金融サービス業界にとって大きな脅威となっています。『高まる波を乗りこなす：金融サービス業界の攻撃トレンド』は、世界中の金融サービス専門家がますます複雑化する脅威の状況に対応するための支援をすることを目的として、特別に作成されています」と述べています。

デジタル化の進展に伴い、APJ の金融業界はサイバー攻撃に対してより脆弱に

APJ 地域では、国内総生産（GDP）の高い先進国と発展途上国が攻撃の主要なターゲットになっています。このような分断された状況が原因で、同地域は固有のサイバーセキュリティ問題に直面しています。このレポートでは、特に疑わしいドメインとリクエストの数に関して、APJ が全地域で最もフィッシングの脅威スコアの中央値が高いことが明らかになりました。この地域ではフィッシングやブランドなりすましのドメインが世界の他の地域に比べて少ないにもかかわらず、銀行の急速なデジタル化と、フィッシングの危険性に対する意識の低さが相まって、消費者は高い攻撃リスクにさらされています。これは、この地域の消費者が、Web サイトを訪問する際に銀行情報などの機微な情報を盗まれるリスクが高いことを示しています。

APJ の金融サービス業界は、デジタルテクノロジーや新興テクノロジーを急速に導入していますが、サイバーセキュリティ対策は欧州と米国に後れを取っています。この地域の金融サービスは、高水準のデジタル化とソーシャルメディアの積極的な利用という 2 つの重要な要因により、ブランド悪用のリスクの増大に直面しています。APJ はインターネットの利活用が浸透しており、ほぼすべてのサービスがオンラインで利用できるからこそ、サイバー犯罪者の主要なターゲットとなっています。さらに、世界でも最も活発な市場の一部において金融機関によるソーシャルメディアでのエンゲージメントが拡大していることが、フィッシングやなりすまし攻撃によってそのようなプラットフォームに対するユーザーの信頼が悪用されることにつながっています。

Akamai Technologies で APJ の Director of Security Technology & Strategy を務める Reuben Koh は、「APJ の金融機関は、今日の情勢における三大課題に直面しています。それは、資産とデータの保護、コンプライアンスの確保、イノベーションの最前線を行き、最新のフィッシングや詐欺の戦術について顧客に情報を提供することです。従来のセキュリティメカニズムは、ランサムウェアや API の悪用などの高度な脅威を検知するためには不十分である場合が多く、最新の AI 搭載セキュリティテクノロジーによって組織をより適切に保護し、新しい規制基準を満たし、顧客の信頼を守る必要があることは明らかです。金融サービスは、APJ において最も Web アプリケーションおよび API 攻撃の標的とされ続けている業界です。そのため、最高情報セキュリティ責任者などのテクノロジーに関する意思決定者は、どこを自動化、委任、アウトソーシングするかを慎重に決定し、デ

ジタル化が進む世界で資産を守ることができるだけでなく顧客ロイヤルティを維持できる、スケーラブルなセキュリティソリューションを確保する必要があります」と、述べています。

「高まる波を乗りこなす：金融サービス業界の攻撃トレンド」には、FS-ISAC のゲストコラム、Credential Stuffing 攻撃に関するケーススタディ、DDoS 攻撃の強度に関する注目すべきセキュリティ情報、地域データ、ゼロトラストとマイクロセグメンテーションに関するセクション、DDoS 攻撃を防ぐための緩和戦略も含まれています。

Akamai の「インターネットの現状（SOTI）」レポートは今年で 10 周年を迎えました。SOTI シリーズでは、Akamai Connected Cloud から収集したデータに基づいて、サイバーセキュリティと Web パフォーマンスの状況についての専門家の知見をご紹介します。

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。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツ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、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。