2023 年 12 月 19 日

Press Release

アカマイ・テクノロジーズ合同会社

【メディアアラート】
Akamai、ホリデーシーズンのショッピングサイバー攻撃に注意喚起

オンラインライフの力となり、守るクラウド企業の Akamai Technologies, Inc.（NASDAQ：AKAM）は、ホリデーシーズンのショッピングサイバー攻撃に関して注意喚起するメディアアラートを発表いたしました。

年末年始のホリデーシーズンには大きなセールイベントやデジタルイベントがあり、デジタル領域でも現実世界でも、年間で最も多くのお金が動く時期です。また、それを狙って、セキュリティ上の脅威の発生頻度も高くなる傾向にあります。

「コマース業界における脅威トレンドの分析」レポートによると、世界的に、現在も小売企業はコマース業界の中で最も狙われている業種であり、このセクターへの攻撃の 62% を占めています。アジア太平洋および日本地域（APJ）の小売セクターとホテル・旅行セクターにおける Web 攻撃は主にオーストラリア、中国、インドで発生しており、これは世界第 2 位の多さです。

決済情報や金融情報は、取引を容易にするために、さまざまなプラットフォームや API が頻繁に使用されています。このようにインターネット上やネットワーク上をあちこち移動するデータが突然急増するため、サイバー犯罪者は収益源として非常に上等なターゲットを獲得しやすくなります。

より特別な商品をいち早くオンラインで購入したいと考える消費者はキャンペーンやスペシャルセールなどに誘惑されやすい傾向にあります。本格的な商戦期に入る前に、企業だけでなく個人でも次のような脅威を意識しましょう。

- **Web アプリケーション攻撃と API 攻撃：**E コマースと決済プラットフォームは、特に主要なキャンペーン中に、これらのプラットフォームを強化するソフトウェアの脆弱性を悪用しようとするハッカーによる大きなリスクに直面します。
- **DDoS 攻撃：**顧客が商品を購入するために殺到すると、サービス妨害（DDoS）攻撃のリスクが高まります。DDoS 攻撃によって Web サイトにアクセスできなくなると、売上が最大になるはずのまさにそのタイミングで、収益への直接的な影響が生じます。
- **悪性ボット：**このようなボットは、ショッピングのピーク時期により多くの消費者アカウントを乗っ取るように設計されています。盗まれたアカウントは大規模な攻撃に悪用されます。
- **Web スキミング攻撃：**ホリデーシーズンに Magecart などに代表されるスキミング攻撃が行われることが増えました。このような攻撃は物理的な ATM スキミングと似ていますが、デジタルで実行されます。精巧に作られた偽の決済ページに巧妙に誘導され、気づかぬまに機密性の高いクレジットカード情報や決済情報が盗まれます。取得されたデータは金融詐欺に使用されます。

リスクにさらされているのは小売企業だけではない

オンライン購入とは、ログインして支払いをするだけではありません。E コマースプラットフォームの裏には、さまざまな事業者が関与する複数の異なるプロセスがあります。サイバー犯罪者は最終販売者だけを攻撃する必要はなく、サプライチェーンの脆弱な部分を攻撃する傾向があります。

製品サプライヤー：注文が増えると、サプライヤーはより大きなサプライチェーンの一部となり、脆弱性が生じます。注文送信と決済処理に関わるすべてのプロセスが、サイバー攻撃の標的となり得るポイントです。

金融サービスプロバイダー：FinTech 企業、決済処理業者、e ウォレットプロバイダー、銀行はすべて、取引プロセスに関与しています。ある場所から別の場所へ金融データが転送される場合は必ず、データ漏えいのリスクがあります。

物流業者：物流業者は商品配送に不可欠な顧客データ（氏名、住所、電話番号など）を処理するため、フィッシングなどさらなる攻撃に使うデータを収集しようとするサイバー犯罪者にとって、魅力的なターゲットです。

組織はサイバー犯罪の急増に備える必要がある

組織はホリデーシーズン中に攻撃が急増することを想定しておかなければなりません。こうした脅威に対して適切な防御が行われているかどうかを評価することが重要です。大規模な攻撃を防ぐためにスケーリングできる、適切なツールを備えているでしょうか？前述の 4 つのリスクは、もはやウイルス対策やファイアウォールなどの一般的なセキュリティツールでは防げない攻撃です。

小売企業はセキュリティ体制を継続的に評価する必要があります。また、悪性ボット、Web スキミング攻撃、データスクレイピングから自社と顧客を保護するためにどのような専用ツールを備えているかを確認する必要があります。リスクにさらされている前提で、提供されているサービスの現状を正確に把握することが重要です。守るのは Web サイトだけで大丈夫ですか？アプリや API も使っていませんか？

フィッシング攻撃の高度化に伴い、事業者側も消費者意識向上キャンペーンを強化し、顧客がコミュニケーションと取引の信頼性を検証するためのメカニズムを提供する必要があります。

メールやソーシャルメディアなどで見かける信じられないようなお買い得情報は、多くの場合信じてはならないということを、消費者は理解する必要があります。多くの小売企業がディスカウントを提供し、それよりもさらに多くの小売企業がマーケティングメールや SMS メッセージを送信する年末セールの時期を、攻撃者が利用しているということをお忘れなく。フィッシングやソーシャルエンジニアリングの試みは生成 AI を利用することでより巧妙に本物らしく見えるようになっており、サイバー犯罪者は簡単に魅力的なブランドになりすますことができます。消費者はどのやり取りが正当なものであるかをどのようにして確認すれはよいのでしょうか。

また、消費者に影響を与えてマルウェアのダウンロードや不正な取引を行わせる目的で、ディープフェイク動画が使用されるようになる可能性が高まっています。このような新たな脅威はまだ生まれたばかりですが、それが普及する前に、今すぐ防御策を構築し、認識を高める必要があります。

ホリデーシーズンはお祝いとショッピングの時期であるべきです。しかし、サイバー犯罪がかつてないほど高度化しているため、これまで以上に警戒度を高め、オンラインの安全の確保に優先的に取り組む必要があります。企業と消費者はどちらも事前にリスクを理解し、利益を守るための対策を講じる必要があります。

Akamai Technologies 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。広範に分散した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。