2020 年 11 月 06 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発表
狙われるロイヤルティプログラム、アカウントデータはダークウェブ上で売買

過去 2 年間で小売、ホスピタリティ、旅行業界を標的とした、630 億件以上の パスワードリスト型攻撃と 40 億件以上の Web アプリケーション攻撃が明らかに

インテリジェントなエッジプラットフォームにより安全で快適なデジタル体験を提供する Akamai（NASDAQ：AKAM）は、「SOTI インターネットの現状／セキュリティ ｜ リワーズポイント詐欺 – 小売・ホスピタリティ業界における詐欺の実態」を発表しました。本レポートでは、2018 年 7 月から 2020 年 6 月までの 2 年間における、小売、旅行、ホスピタリティの各業界を標的とした攻撃について、その種類や規模とともに詳しく報告しています。また、ダークウェブに掲載された犯罪広告の例を多数取り上げ、攻撃が成功し盗み取ったデータから、犯罪者がどのように利益を得ているのかを解説しています。

「犯罪者はこだわりがなく、利用できるものは何でも利用します」と、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」の著者である Steve Ragan は述べています。「ここ数年パスワードリスト型攻撃（Credential Stuffing）が蔓延しているのはこのためです。近頃、小売や会員向けのロイヤルティプログラムには多岐に渡る個人情報が登録されており、中には所得情報が含まれているものもあります。こうしたデータをすべて収集、販売、取引、蓄積して大規模なプロファイルリストを作成することで、後からアイデンティティ窃盗などの犯罪に利用することができるのです」。

2020 年第 1 四半期の新型コロナウイルス感染症（COVID-19 ）のパンデミックに伴う外出自粛期間中、犯罪者はこの世界的な状況を利用して、ID とパスワードの組み合わせリストを拡散し、このレポートで取り上げた各コマース業界に攻撃を仕掛けています。この時期に、犯罪者は新たに脆弱なアカウントを見つけるために、過去の認証情報リストを再度拡散して、ロイヤルティプログラムに関連する商品と販売に関連した犯罪が大幅に増加しました。

先述の 2 年間に Akamai が観測したパスワードリスト型攻撃は 1,000 億件以上でした。小売、旅行、ホスピタリティの各業界で構成されるコマースカテゴリでは、638 億 2,864 万 2,449 件の攻撃が確認されました。コマースカテゴリの 90% 以上の攻撃は小売業界を標的としていました。

攻撃者が小売、旅行、ホスピタリティの各業界を攻撃する手段として利用するのは、パスワードリスト型攻撃だけではありません。先述の 2 年間で、43 億 7,571 万 1,860 件の小売、旅行、ホスピタリティの各業界に対する Web アプリケーション攻撃が観測されました。これは全業界への攻撃数の 41%を占めています。このコマース業界を狙った Web アプリケーション攻撃のうち 83% が小売業界を標的とするものでした。発信元では SQL インジェクション（SQLi）やローカル・ファイル・インクルージョン（LFI）攻撃も利用しながら、これらの業界の組織を攻撃します。SQLi 攻撃は、小売、旅行、ホスピタリティの各業界に対する全 Web アプリケーション攻撃のうち 79% 弱を占め、攻撃の種類としては突出しています。

世界経済はクリスマスや年末のショッピングシーズンの準備に入っていますが、今年はパンデミック下の劇変した環境の中で行わなければなりません。消費者はかつてのように、流行の品を手に入れようと実店舗の前で行列して待つことはないでしょう。消費者はオンラインで、ポイントの収集や、ロイヤルティプログラムを利用してメンバー限定割引などの特典の入手しようとするでしょう。

犯罪者は、成功を収めているロイヤルティプログラムに侵入するためのあらゆる手段、人々がそれに参加するために提供する必要のある情報などをすべて考慮に入れ、アカウントの乗っ取りから個人情報の窃盗まで、犯罪に関わるさまざまな企てに必要なものすべてを手にします。業者や航空会社、ホテルチェーンに対する個人のロイヤルティやポイントが直接売りに出されていない場合でも、このようなプログラムに関連付けられているアカウントは販売される可能性があります。

Ragan は結論として次のように語っています。「パンデミックであれ、競合他社であれ、行動的でインテリジェントな攻撃者であれ、すべての企業は外で実際に起きている事象に適応する必要があります。標的の上位になっているロイヤルティプログラムには、携帯電話番号と数字のパスワード以外は不要なものもあれば、容易に手に入る情報を認証の手段に利用しているものもあります。アイデンティティの制御と対策を強化し、API とサーバーリソースへの攻撃を回避することは、今喫緊の課題となっています」。

Akamai の 2020 年の「インターネットの現状／セキュリティレポート：小売・ホスピタリティ業界における詐欺の実態」は、こちらからダウンロードできます。

レポートの概要をまとめたエグゼクティブサマリーはこちらをご覧ください。
https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-security-loyalty-for-sale-retail-and-hospitality-fraud-executive-summary-2020.pdf

セキュリティに携わる方々に、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用意しています。
https://www.akamai.com/jp/ja/what-we-do/threat-research.jsp

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。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。

アカマイ・テクノロジーズ合同会社について:

アカマイ・テクノロジーズ合同会社は、1998 年に設立された、アカマイ・テクノロジーズ・インク（本社：米国マサチューセッツ州ケンブリッジ、最高経営責任者：Tom Leighton）が 100%出資する日本法人です。アカマイは、ウェブサイト/モバイルアプリの最適化、快適なユーザー体験、堅牢なセキュリティを実現する各種ソリューションを提供しており、日本国内では約 650 社が当社サービスを利用しています。