2020 年 10 月 13 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
ゲーム企業およびプレイヤーを標的とする
広範かつ執拗なサイバー攻撃の存在が明らかに

ゲーム業界では 3 年間で約 100 億件のパスワードリスト型攻撃と
約 1 億 5,200 万件の Web アプリケーション攻撃が発生
COVID-19 に伴うロックダウン期間中に攻撃が急増

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、以下「Akamai」）は、「SOTI インターネットの現状／セキュリティ」レポート、「ゲーム業界―セキュリティも一人ではプレイできません」を発表しました。本レポートでは、2018～2020 年の間に、ビデオゲーム企業およびプレイヤーを標的に大量のサイバー攻撃が発生していた事実を明らかにしています。また、COVID-19（新型コロナウイルス感染症）に伴うロックダウンの期間中に、攻撃トラフィックが上昇していると指摘しています。加えて、攻撃の動機について、ゲームプレイヤーが自身の個人情報、アカウント、ゲーム内アセットを守るために実施すべき対策について検証しています。さらに、世界最大級のゲーミング・ライフスタイル・フェスティバルを開催する DreamHack と共同で実施したセキュリティに対するゲームプレイヤーの意識調査（近日中に発表予定）のポイントを紹介しています。

「ビデオゲーム企業およびプレイヤーは、格闘ゲームさながらの攻撃を現実世界でも受けています」と、Akamai の Security Researcher であり「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。「犯罪者は、アカウントを乗っ取り、個人情報やゲーム内アセットを盗んで儲けを得るとともに、競争優位性を獲得することを目的として、ゲームやプレイヤーを標的に苛烈な攻撃を仕掛けています。プレイヤー、ゲームパブリッシャー、ゲームサービスが協力して、警戒を怠ることなく、テクノロジーと優れたセキュリティ対策を組み合わせて、これらの攻撃に対抗することが重要です」。

最新のレポートでは、ゲームプレイヤーが常に大量の攻撃（主にパスワードリスト型（Credential Stuffing）攻撃、およびフィッシング攻撃）に晒されていると指摘しています。Akamai が 2018 年 7 月～2020 年 6 月の間に観測したパスワードリスト型攻撃の数は 1,000 億件を超えています。そのうち、100 億件近くがゲーム業界を標的とするものでした。この種の攻撃を行うために、犯罪者はユーザー名とパスワードの組み合わせのリストを用いてゲームやゲームサービスにアクセスします。このリストの多く

は、不正な Web サイトやサービスを通じて購入されたものです。このログインに成功すると、プレイヤーのアカウントが侵害されたことになります。

ゲームプレイヤーを標的とするもう 1 つの主な攻撃手法がフィッシングです。この攻撃は、ゲームまたはゲーミングプラットフォーム関連の、一見正規のサイトに見える Web サイトを作成し、そのサイトにログイン認証情報を入力させる手法です。

また、Akamai が同時期に観測した Web アプリケーション攻撃は 106 億件に上りました。そのうち、1 億 5,200 万件以上がゲーム業界を標的とするものでした。攻撃の圧倒的多数は SQL インジェクション（SQLi）攻撃でした。攻撃の目的は、ユーザーのログイン認証情報、個人情報、および標的となるサーバーのデータベースに保存されたその他の情報を悪用することです。この他に目立った攻撃ベクトルとして、ローカル・ファイル・インクルージョン（LFI）があります。これは、プレイヤーやゲームに関する詳細情報を盗み出して、チートと呼ばれる不正行為に利用する攻撃です。犯罪者は、SQLi 攻撃や LFI 攻撃の標的として、モバイルゲームおよび Web ベースのゲームを選択しています。ユーザー名、パスワード、アカウント情報にアクセスするだけで悪用できるためです。

2019 年 7 月～2020 年 6 月の間に Akamai が観測した 5,600 件（重複排除）の DDoS 攻撃のうち、3,000 件以上がゲーム業界を標的とするものでした。これは、すべての業界の中でも突出して多い件数です。Minecraft のサーバーを停止させることを目的に複数の大学生が作成した Mirai ボットネットは、その後、最大級の DDoS 攻撃にも利用されました。レポートでは、ゲーム関連の DDoS 攻撃がクリスマスシーズンや学校の休み期間中に急増していると指摘しています。これは、学生が休み期間中に自宅から攻撃している可能性が高いことを意味しています。

今年前半は、COVID-19 によるロックダウンに際して、エンターテインメントやソーシャルコミュニケーションの主な手段としてビデオゲームが大きな役割を果たしました。一方、犯罪者もこのパンデミックを攻撃の機会として利用しました。世界中で自宅待機措置が実施されるなか、パスワードリスト型攻撃が明確に急増しました。攻撃トラフィックの多くは、攻撃者が過去に盗み出した認証情報を使用して、既存のユーザー名とパスワードで作成された新規アカウントに侵入できるかどうかを試したものです。

多くのゲームプレイヤーが被害に遭ったものの、そのほとんどは気にも留めませんでした。Akamai と DreamHack が共同で実施した、セキュリティに対するゲームプレイヤーの意識調査（近日中に発表予定）によると、自らを「ゲームのヘビーユーザー」と称する調査回答者の 55%が、アカウント侵害の被害に遭ったことがあると回答しています。そのうち、その被害について「心配している」または「非常に心配している」と回答した人はわずか 20%にとどまりました。

このレポートでは、ゲームプレイヤーは自身のアカウントに関連するデータの価値を認識していない可能性があるが、犯罪者は間違いなくその価値を認識していると指摘しています。

ゲームプレイヤーは犯罪者が求めているいくつかの条件と一致するため攻撃の主要な標的となっています。ゲームプレイヤーはソーシャルコミュニティへの関心が高く、積極的に参加しています。自由に使える収入のある人が多く、それをゲームアカウントやゲーム体験に使う傾向があります。これらの要素は犯罪者の目から見ると、ゲーム業界は絶好の標的となります。

「SOTI State of the Internet／Security: Gaming — You Can't Solo Security」は、こちらからダウンロードいただけます。なお、日本語版「SOTI／セキュリティ：ゲーム業界ーセキュリティも一人ではプレイできません」は近日中に公開予定です。
https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

さらに、10 月 28 日（水）に開催されるウェビナー「Gaming Leadership Summit」では、Akamai のセキュリティエキスパートが、本レポートの調査結果を引用しながら、ゲーム業界におけるボットによる不正攻撃の現状と対策を解説したり、ニューノーマルに向けたゲーム企業の働き方をテーマに、最新動向をご紹介いたします。本ウェビナーへのお申し込みはこちらのページをご覧ください。
https://www.akamai.com/jp/ja/campaign/gaming-leadership-virtual-summit.jsp

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。