2019 年 6 月 14 日
Press Release
アカマイ・テクノロジーズ合同会社

Akamai が脅威リサーチレポートを発表、
ゲーム業界に対する 120 億件の攻撃を記録、脅威の高まりを指摘

ゲーム業界に対するデータ侵害やパスワードリスト型攻撃が、
最も活発で急発展している地下経済を生み出していることが明らかに

※本リリースは 2019 年 6 月 12 日 (現地時間) に米国マサチューセッツ州で発表されたプレスリリースの翻訳版です。

安全なデジタル体験を実現するインテリジェント・エッジ・プラットフォームを提供する Akamai (NASDAQ：AKAM、以下「アカマイ」)は、ゲームウェブサイトを標的としたボットによる不正ログイン (Credential Stuffing) 攻撃に関する詳細な調査結果を公表しました。「インターネットの現状 (State Of The Internet, SOTI)/セキュリティ|Web 攻撃とゲーム業界への攻撃」レポートによると、ゲーム業界はハッカーの標的となっていましたが、調査対象となった 17 ヵ月間(2017 年 11 月～2019 年 3 月)で、ゲームウェブサイトを標的としたボットによる不正ログイン (Credential Stuffing) 攻撃が 120 億件も発生していたことが明らかになりました。このことから、同レポートはゲーム関連業界において、不正ログイン攻撃の脅威が急激に高まっており、手っ取り早く利益を狙う犯罪者に格好の標的となっていると指摘しています。なお、同時期に、全業種に対しては、合計 550 億件の不正ログイン攻撃が確認されています。

レポートでは、現在、SQL インジェクション(SQLi)攻撃が全ウェブアプリケーション攻撃の 3 分の 2 近く(65.1%)を占め、ローカル・ファイル・インクルージョン(LFI)攻撃も 24.7%に達していることも明らかにしています。データによると、この SQLi 攻撃は 2018 年の年末商戦期間中に急増し、その後も増加傾向にあることから、攻撃ベクトルとして警戒すべきレベルの成長を続けています。2017 年四半期の SQLi 攻撃の割合は、アプリケーションレイヤーへの攻撃全体の 44%でした。

SQLi 攻撃と不正ログイン攻撃には直接的なつながりがあります。闇サイトなどで出回っている不正ログイン用のリストの大半は、世界最大規模のデータ漏えいの数々から得られたデータが悪用されており、漏えいの根本原因は多くの場合 SQLi 攻撃です。年初に Akamai のリサーチチームは、脆弱なウェブサイトに対して SQLi 攻撃を仕掛ける方法や、取得した認証情報からリストを生成する方法を解説した動画を見つけました。このような方法で不正に入手されたリストが人気オンラインゲームに対する不正ログイン攻撃に利用されていると考えられます。

セキュリティ調査担当であり、「SOTI /セキュリティ」レポートの解説者でもある Martin McKeay は次のように語ります。「ゲーム業界がハッカーにとって魅力的なターゲットである理由の 1 つに、ゲーム内アイテムを犯罪者が簡単に換金できる点があります。さらに、ゲーマーはお金を使うことが知られている特殊な消費者層なので、経済的にも魅力的なターゲットなのです。」

攻撃の一例を見ると、犯罪者は人気ゲームの有効なアカウントと個性的なスキンを標的としています。スキンとは、ビデオゲーム内のアイテムやアバターの外観を変えるもので、プレーヤーのアカウントのハッキングに成功すると、それらの取引や売却ができてしまいます。

ハッカーにとってさらに価値が高いと見られるのが、有効なクレジットカードなどの金銭取引情報が紐付けられているアカウントです。そのようなアカウントを取得すると、ゲーム内で使う通貨などの追加アイテムを購入してから、さらにそのアカウントを高値で取引または売却できます。

「ゲーム会社は継続的に防御策を新たに導入したり、強化していますが、同時にユーザーにも自身で身を守る方法を伝え続ける必要があります。多くのゲーマーは若者です。アカウント保護のベストプラクティスを教えることができれば、今後それを実践するようになるでしょう」と McKeay は語ります。

その他、本レポートでは下記の地理的な特徴について取り上げています：

- アプリケーションレイヤー攻撃の 67%近くが米国の組織を標的としている。
- ロシアはアプリケーション攻撃の発信元国として第 2 位である一方で、標的としては上位 10 ヵ国に入っていない。同様に、中国も発信元国としては第 4 位だが、標的としては上位 10 ヵ国に入っていない。
- 英国は標的国として第 2 位である一方、発信元国としては順位が低く第 10 位。オーストラリア、イタリアも標的国の上位だが、発信元となると上位 10 ヵ国に入っていない。
- 全業種では米国が不正ログイン攻撃の発信元国として群を抜いてトップだが、ゲーム業界を標的とした攻撃に限定すると、ロシアとカナダが 1 位と 2 位を独占している。
- カナダは、アプリケーションレイヤー攻撃の発信元国として上位 10 位に入っていないが、不正ログイン攻撃の発信元国では第 4 位。
- ベトナムは、不正ログイン攻撃の発信元国では第 9 位だが、ゲーム業界を標的とした攻撃では第 4 位。
- 日本は、不正ログイン攻撃の発信元国としては 16 位となっている。

Akamai の 2019 年「SOTI/セキュリティ|Web 攻撃とゲーム業界への攻撃」レポートはこちらからダウンロードできます。
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf

不正ログイン、特に リスト型攻撃の詳細およびこのタイプの攻撃に直面している組織へのアドバイスについては、こちらをご覧ください。
https://www.akamai.com/us/en/campaign/credential-stuffing-is-on-the-rise.jsp

アカマイ について：

アカマイ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。アカマイ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アカマイを利用しています。アカマイは、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アカマイ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アカマイを信頼する理由について、<www.akamai.com/jp/ja/>、<blogs.akamai.com/jp/>および Twitter の@Akamai_jp でご紹介しています。

本プレスリリースに関するお問い合わせ先 ----------

◆ アカマイ・テクノロジーズ合同会社
マーケティング本部 広報担当：森(Mail: info_akamai@akamai.com)