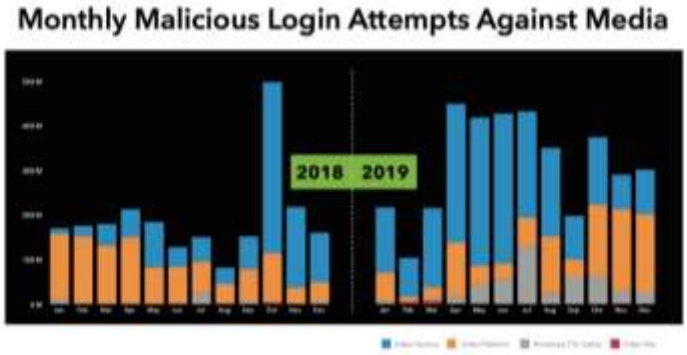
2020 年 8 月 26 日
Press Release
アカマイ・テクノロジーズ合同会社

Akamai、最新の脅威レポートを発表
メディア業界に蔓延するパスワードリスト型攻撃
パスワードリスト型攻撃の 20% がメディア企業を標的としていると判明

Akamai Technologies, Inc. (NASDAQ：AKAM) は、「SOTI インターネットの現状／メディア業界における Credential Stuffing」レポートを発表しました。調査の結果、2018 年 1 月から 2019 年 12 月までの間に、メディア業界に対して約 170 億回の パスワードリスト型 (Credential Stuffing) 攻撃が仕掛けられました。また、調査期間中に観測された全 880 億回の パスワードリスト型攻撃のうち 20% がメディア企業を標的としていたことが明らかになりました。



同レポートによると、メディア企業は攻撃者にとって魅力的な標的であり、動画メディア企業に対する 2019 年の攻撃数は前年比で 63% 増加しました。また、テレビ局と動画サイトに対する 2019 年の攻撃数はそれぞれ前年比 630% と 208% の増加率を示しています。また、動画サービスを標的とした攻撃は 98% 増加し、動画プラットフォームを標的とした攻撃は 5%減少しています。

テレビ局と動画サイトを標的とする攻撃の著しい増加傾向は、2019 年のオンデマンド・メディア・コンテンツの急増と時期的に一致しているようにみえます。さらに昨年、プロモーションキャンペーンが大きな反響を呼んだ、2 つのメジャーな動画サービスが始まりました。これまでの観測から、この種のサイトやサービスも犯罪者の標的範囲に十分入っているものと思われます。

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」レポートの執筆者である Steve Ragan によると、犯罪者にとってのメディア業界アカウントの価値は主に、プレミアコンテンツと個人情報の両方にアクセスできることにあります。Ragan はレポートの中で次のように説明しています。「メディアアカウントの認証情報と地元のレストランから盗んだ特典ポイントへのアクセス権を組み合わせて、『デートナイト』パッケージとして不正なサービスを売り込むというトレンドが見られます。いったん犯罪者が、侵害したアカウントの地理的な場所の情報を手に入れると、これらの情報をうまく組み合わせて、『ディナーと映画』として販売してしまうことができるのです」

さらにメディア業界では、動画サイト以外にもパスワードリスト型攻撃の標的となっているものがあります。レポートによると、公開コンテンツを標的とする攻撃は 7,000% 増加という圧倒的な伸びを見せています。この業種に分類される、新聞、書籍、雑誌はまさにサイバー犯罪の視野に入っており、こうした攻撃にとってはあらゆるメディアが格好の標的であることを示しています。

メディア業界へのパスワードリスト型攻撃発信元のトップは米国です。2019 年の攻撃回数は約 11 億回で、2018 年比 162% となっています。2 位のフランスと 3 位のロシアは米国に大きく引き離されており、攻撃回数はそれぞれ約 3 億 9300 万回と約 2 億 4300 万回でした。

2019 年に最も標的とされた国はインドで、約 24 億回のパスワードリスト型攻撃に見舞われています。次が米国の約 14 億回、続いて英国の約 1 億 2,400 万回です。

「私たちがユーザー名とパスワードを使う限り、それを侵害し、アカウント内の有益な情報を悪用しようとする犯罪者は後を絶ちません。パスワードの共有や使い回しは、パスワードリスト型攻撃を受ける 2 大要因です。これらの攻撃に立ち向かうために、ユーザーには適切な認証情報管理を指導することが重要です。一方、企業には、より強力な認証方法を導入し、テクノロジー、ポリシー、専門知識をうまく組み合わせて、ユーザー体験に悪影響を及ぼすことなくユーザーを保護する責任があります」と Ragan は説明します。

2020 年第 1 四半期更新

Akamai の 2020 年「インターネットの現状／メディア業界における Credential Stuffing」レポートは、COVID-19（新型コロナウイルス）の影響で 4 月から 7 月に発行が延期されました。時間に余裕が生まれたため、当初のレポートに 2020 年第 1 四半期のデータを追加しました。

追加データで最も顕著だったのは、2020 年第 1 四半期に欧州の動画サービスプロバイダーと放送局を対象に発生した急激な不正ログイン試行の増加です。各地で外出自粛や禁止令が出された後の

3 月後半には、1 つのサービスプロバイダーに対して 24 時間で約 3 億 5,000 万回の攻撃が行われました。それとは別に、地元で有名なある放送局は、その四半期の間に、ピーク時で数十億回にわたって集中的に攻撃を受けました。

第 1 四半期で目立ったもう 1 つの傾向は、新聞アカウントへの無料アクセスを共有する犯罪の増加です。これらは、犯罪者自身の売り込みの手段としてよく利用されます。そこで提示するために、有効なユーザー名とパスワードの組み合わせを盗むことを狙い、いまだにパスワードリスト型攻撃キャンペーンが発生しているようです。

また、Akamai の調査では、第 1 四半期の間に盗まれたアカウントの認証情報の価格に下落が見られました。初めは 1 件あたり約 1 ドルから 5 ドル、複数サービスのパッケージの場合は 10 ドルから 45 ドルで取引されていましたが、新しいアカウントとリサイクルされた認証情報のリストが市場に出回るにつれ下落しました。

「SOTI インターネットの現状／メディア業界におけるリスト型攻撃」レポートは、下記よりダウンロードいただけます。
https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-in-the-media-industry-report-2020.pdf

これまで発刊された Akamai「SOTI インターネットの現状／セキュリティ」レポートは、下記よりダウンロードいただけます。
https://www.akamai.com/jp/ja/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.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

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