2019 年 8 月 15 日
Press Release
アカマイ・テクノロジーズ合同会社

Akamai が脅威レポートを発表、金融サービス業界を標的とした不正ログイン試行が 35 億件に

フィッシング、不正ログイン攻撃が金融サービス業界と顧客を標的にした脅威のトップであることが明らかに - 脅威に対する Akamai 独自の可視性を示す

※本リリースは 2019 年 7 月 31 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」)が、2019 年「インターネットの現状 State of the Internet (SOTI)／セキュリティ | 金融サービスへの攻撃エコノミー」レポートで新たに発表したデータでは、検出されたフィッシングサイトの被害を受けた組織の 50% は金融サービス部門であることが明らかになりました。調査データでは、このような特徴的なフィッシング攻撃に加え、18 ヵ月間で確認された 35 億回の攻撃試行が行われた不正ログイン (Credential Stuffing) 攻撃もレポートで取り上げており、金融サービスの顧客の個人データや銀行口座情報がリスクにさらされていることが見て取れます。

同レポートによると、2018 年 12 月 2 日から 2019 年 5 月 4 日までの間に 200,000 件近く（正確には 197,524 件）のフィッシングサイトを検出し、その 66% がユーザーを直接標的としたものでした。ユーザーを標的としたフィッシングサイトのみに注目すると、その 50% が金融サービス業界の企業を標的としていました。

Akamai の 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 は次のように述べています。「この 1 年間で不正ログイン攻撃は着実に増加しています。その一因が、ユーザーを標的としたフィッシング攻撃の増加です。犯罪者は、盗んだ認証情報データをフィッシングによって補完し、アカウントの乗っ取りや、作成したリストの転売などで利益を得ているのです。Akamai は、攻撃エコノミー全体が、金融サービス組織とその顧客を標的にするべく発展していると見ています」。

犯罪者は計画が成功すると、次に不正に得たデータや金銭を処理する必要があります。Akamai のレポートでも注目していますが、これに使われる手段の一つが「バンクドロップ」を中心としたものです。バンクドロップとは、特定の金融機関に不正に口座を開設するために使用するデータのパッケージです。通常、不正取得した個人情報が含まれます。オンラインの犯罪者には「fullz」とも呼ばれ、氏名、住所、

生年月日、社会保障情報、自動車免許情報、信用スコアなどが含まれています。不正アカウントへのアクセスを確実に行うため、銀行と「fullz」の地理的位置と一致するリモート・デスクトップ・サーバーが用いられます。

金融機関は、犯罪者によるこのようなドロップ口座の開設方法を継続的に探り、先手を打てるよう懸命に取り組んでいます。しかし、犯罪者が古い攻撃手法を再利用しているという点にほとんどの企業は気づいていません。

Akamai のリサーチ結果から、金融サービス部門を標的とした攻撃として検出されたもののうち 94%が、SQL インジェクション（SQLi）、ローカル・ファイル・インクルージョン（LFI）、クロスサイトスクリプティング（XSS）、OGNL Java インジェクション（調査期間中に発生した攻撃試行のうち 800 万件以上を占める）のいずれかの手法を利用していることが明らかになりました。Apache Struts2 の脆弱性によって有名になった OGNL Java インジェクションは、パッチが発行されてから数年たった現在でも攻撃者たちによって使われています。

金融サービス業界では、犯罪者は不正ログイン攻撃を仕掛けるため、あるいはウェブベースの脆弱性を悪用するための目くらましとしても、DDoS 攻撃を利用し始めています。実際に調査期間の 18 ヵ月間で、金融サービス業界に対して 800 回を超える DDoS 攻撃が確認されました。

McKeay は次のように語ります。「攻撃者は、金融サービス機関の弱点であるユーザーやウェブアプリケーション、可用性を狙ってきます。そうすれば成功すると考えているのです。金融機関側のこのような攻撃に対する検知方法や防御方法も向上してはいますが、ポイント防御では失敗するでしょう。サービスの顧客を守るには、多種多様なツールを駆使するインテリジェントな犯罪者を検知して分析し、防御できるようになる必要があるのです。Akamai は 20 年以上に渡り、このような進化し続ける悪質な活動からお客様を保護するために、様々な攻撃に対する独自の可視性を活用しています」。

犯罪エコノミーは、金融サービス業界を標的としているため、ある意味「繁栄」しています。たとえば、犯罪者は銀行を標的にして機微な情報を盗もうとし、入手すると、そのデータを使って不正口座を開設し、融資枠を得ます。これが継続的な犯罪のサイクルです。犯罪者が生き続けるために必要な業界そのものを標的にしているというのは、皮肉なことといえます。そして金融機関の攻撃検知力がますます向上している一方で、攻撃者は古い仕掛けで成功し続けているということが問題です。

Akamai の 2019 年「インターネットの現状／セキュリティ」レポート（英文）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-financial-services-attack-economy-report-2019.pdf

本レポートのエグゼクティブサマリー（日本語）は、こちらからダウンロードできます。

https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-executive-summary-2019.pdf

また、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する Akamai Intelligent Edge Platform からの知見をまとめた Akamai の脅威リサーチの特設ページはこちらをご覧ください。
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。