2021 年 7 月 2 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：
金融機関を狙う相次ぐ パスワードリスト型攻撃、
Web アプリケーション攻撃とその背景の考察
Akamai と WMC Global が複数のフィッシングキットを共同調査
「Kr3pto」は英国の大手銀行 11 社の顧客を標的としていたことが判明

※本リリースは 2021 年 5 月 19 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抄訳版です。

世界で最も信頼されているソリューションで安全なデジタル体験の提供を実現する Akamai Technologies, Inc.（NASDAQ: AKAM）は、最新のレポート「SOTI インターネットの現状／セキュリティ：金融業界に対するフィッシング攻撃」の日本語版レポートを発表しました。本レポートでは、Web アプリケーション攻撃と Credential Stuffing 攻撃 (パスワードリスト型攻撃) について、世界全体のトラフィックと金融サービス固有のトラフィックの両方を分析しています。その結果、2020 年には、前年の 2019 年と比較してアタックサーフェスが大幅に増大したことが明らかとなりました。

本レポートではさらに、Akamai と、脅威インテリジェンス企業である WMC Global との連携により、2 つのフィッシングキット「Kr3pto」と「Ex-Robotos」を検証しています。Kr3pto は英国の大手銀行 11 社の顧客を標的とし、Ex-Robotos は企業の従業員への詐欺を目的としていました。

数字による分析

2020 年に Akamai は世界全体で 1,930 億件の Credential Stuffing 攻撃を確認しました。そのうち 34 億件は明確に金融サービス組織を狙ったものであり、金融業界への不正ログイン試行数の増加率は、前年比で 45%を超えています。

一方、2020 年に Akamai が観測した Web アプリケーション攻撃は約 63 億件でしたが、そのうち、金融サービス業界を標的としたものは 7 億 3,600 万件を超え、2019 年と比べて 62%の増加となっています。

Web アプリケーション攻撃のなかでは、2020 年も全業種で SQL インジェクション（SQLi）攻撃が首位の座を維持し、全体の 68%を占めています。2 位はローカル・ファイル・インクルージョン（LFI）攻撃で、全体の 22%でした。ただし、金融サービス業界だけを見ると、2020 年の Web アプリケーション攻撃タイ

プで最も多かったのは LFI 攻撃で、全体の 52%を占めています。次いで SQLi が 33%、クロス・サイト・スクリプティングは 9%でした。
過去 3 年間（2018～2020 年）の Akamai 観測データによると、金融サービス業界への DDoS 攻撃はこの期間中に 93%増加しています。犯罪者は今もシステムの破壊を目的とし、日常業務に必要なサービスやアプリケーションを標的としていると考えられます。

脅威インテリジェンスでの連携
今回 Akamai は、脅威インテリジェンス企業の WMC Global と連携してレポートに取り組みました。WMC Global は、SMS フィッシング（スミッシング）や、これらの攻撃を可能にするために犯罪者が利用するツールキットについて専門的な知識を有しています。二社の協業によって 2 つのフィッシングキット「Kr3pto」と「Ex-Robotos」の検証が行われました。

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」の著者も務める Steve Ragan は次のように述べています。「パスワードリスト型攻撃の継続的かつ大幅な増大は、金融サービス業界におけるフィッシングの状況と直接的に関係しています。犯罪者はさまざまな方法でサービス利用者の認証情報のコレクションを増やしていますが、フィッシングはその主要な手段の 1 つです。銀行の顧客やこの業界の従業員を標的とすることで、犯罪者は潜在的な犠牲者を指数関数的に拡大しています。」

Kr3pto フィッシングキットは、SMS を通じて金融機関とその顧客を標的としていますが、2020 年 5 月以降、英国の大手銀行 11 社になりすまし、そのドメイン数は 8,000 を超えています。WMC Global は、2021 年第 1 四半期の 31 日間に SMS メッセージングの利用者を標的とする Kr3pto に関連した 4,000 以上のキャンペーンを追跡しました。

Ex-Robotos は、企業の認証情報のフィッシングにおける基本的なフィッシングキットといえます。Akamai Intelligent Edge Platform のデータによると、43 日間に Ex-Robotos が使用した API IP アドレスへのヒット数は 22 万を超えていました。実際、そのアドレスへのトラフィックは、2021 年 1 月 31 日から 2 月 5 日までの期間に、平均して 1 日あたり数万のヒット数に達していました。

WMC Global で Senior Threat Hunter を務める Jake Sloane 氏は次のように述べています。「Kr3pto や Ex-Robotos のようなキットは、企業とその顧客を標的とする多数のキットの一部にすぎません。重要なのは従業員は消費者でもあるという点です。企業環境では在宅勤務やモバイルデバイスの利用が拡大していますが、犯罪者は標的がどこにいても攻撃を控えることはありません。これは最近 SMS ベースのフィッシング攻撃が拡大している状況とも符合します。」

最後に、Steve Ragan は次のように付け加えています。「今回のレポートでは、WMC Global と連携することで、金融業界に関するこれまでの調査範囲を拡大し、金融組織が日常的に直面している攻撃についてより広範に詳細情報を提供できました。」

Akamai の最新レポート「SOTI インターネットの現状／セキュリティ：金融業界に対するフィッシング攻撃」は、Akamai のインターネットの現状ページからご覧いただけます。
全文レポート https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf
エグゼクティブサマリー https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-phishing-for-finance-executive-summary.pdf

また、Akamai の脅威リサーチハブでは、セキュリティに携わる方々にご利用いただけるよう、Akamai 脅威リサーチャーの見解や、変化する脅威状況に関して Akamai Intelligent Edge Platform から得た知見などをご紹介しています。

アカマイ 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。