2019 年 12 月 3 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、
ビジネス化するフィッシングキットの開発・流通の実態が明らかに

サイバー犯罪者が独自のツールやプロセスを開発し、

Microsoft、PayPal、DHL、Dropbox ら世界有数のテクノロジーブランドを悪用

Akamai Technologies（NASDAQ：AKAM）は、最新の「State of the Internet (SOTI) / Security | Phishing : Baiting the Hook （インターネットの現状／セキュリティ | フィッシング：罠を仕掛ける詐欺師たち）」レポートを公開しました。本レポートから、サイバー犯罪者が Phising as a Service (PaaS、サービスとしてのフィッシング）など、企業に見られるような開発と流通の手法を駆使して、世界有数のテクノロジーブランドを悪用しているということが判明しました。観測されたドメインのうちの 42.63% が Microsoft、PayPal、DHL、Dropbox を標的としています。

本レポートでは、フィッシングがもはやメールだけではなく、ソーシャルメディアやモバイルデバイスを悪用し、すべての業界にかかわる脅威を生み出している実態について詳しく説明しています。手法は常に進化していますが、その 1 つがビジネスメール詐欺（Business Email Compromise / BEC）攻撃です。FBI によると、2013 年 10 月から 2018 年 5 月にかけて、世界の BEC 攻撃による損失額は 120 億ドル超 （日本円で約 1 兆 3 千億円に相当）に達しています。

Akamai の「SOTI / セキュリティ」レポートの編集委員を務める Martin McKeay は、「フィッシングは長期に及ぶ問題です。パーソナライズされたセキュリティ教育や多層防御技術によって防がない限り、攻撃者はユーザーと企業に執拗に付きまとうと想定しています。」と述べています。

同レポートは、サイバー犯罪者が高度に組織化された巧妙なフィッシングキットを操って、さまざまな業界の大手グローバルブランドとそのユーザーを標的にしていることを明らかにしています。対象の調査期間中に、フィッシングの標的となった業界のトップはハイテク業界で、6,035 のドメインと 120 種類のフィッシングキットが存在していました。続く金融サービス業界では、3,658 のドメインと 83 種類のキットが存在していました。さらに、E コマース（1,979 ドメイン、19 種類のキット）とメディア（650 ドメイン、19 種類のキット）が上位に入っています。期間中に標的にされたグローバルブランドは、全体で 60 社以上に上ります。

また、フィッシングに関して標的とされた上位のブランドは Microsoft、PayPal、DHL、Dropbox であり、Microsoft は全体のドメインの 21.88% （3,897 ドメイン、62 種類のキット）、PayPal は同

9.37% （14 種類のキット）、DHL は同 8.79%（7 種類のキット）、Dropbox は同 2.59%（11 種類のキット）を占めています。

犯罪者はできるだけ長い間、未検知の状態を維持しようとしますが、フィッシング対策ソリューションにより犯罪者はその手口の変更を余儀なくされています。Akamai の調査によると、観測された 60% のフィッシングキットは、調査期間中に有効だった期間は 20 日以内でした。このように有効期間が短いのは、犯罪者が常にキットを未検知の状態を維持できるように次々と新しい侵入方法を開発しているからだと考えられます。

同レポートでは、フィッシングキット開発者の日常業務を追跡する調査プロジェクトについても論じています。この開発者は、3 種のオプション（高度な侵入技術、デザイン、ジオターゲティング）を持つキットを開発しています。低価格であることやターゲットが一流ブランドであることなど、魅力的な要素をもったこのキットによって、犯罪者はフィッシング市場にたやすく参入できるようになります。

McKeay は次のように締めくくっています。「フィッシングをめぐる状況がさらに進化するにつれ、BEC 攻撃など、より多くの手法が開発され、世界中のさまざまな業界を脅かすことになります。フィッシング攻撃のスタイルはワンパターンではありません。そのため、企業は相当な注意を払って、信頼を悪用しようとするビジネス志向の犯罪者の一歩先を行かなければなりません。」

最新の「SOTI / 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-phishing-baiting-the-hook-report-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。

※その他、記載されている会社名ならびに製品名は、各社の商標または登録商標です