2018 年 11 月 7 日
Press Release
アカマイ・テクノロジーズ合同会社

アカマイ、リスト型攻撃レポートを発表
金融サービス業界が絶え間なく自動アカウント乗っ取りツールの攻撃に
さらされている現状を報告

最新の「インターネットの現状／セキュリティ」レポートで、
不正なログイン試行件数が世界中で増加していることが明らかに。
先の 5 月から 6 月の 2 カ月で 83 億件以上の不正ログイン試行を検出

※本リリースは 2018 年 9 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翻訳版です。

Akamai Technologies, Inc.（NASDAQ：AKAM、以下「アカマイ」）の 2018 年「インターネットの現状／セキュリティ：Credential Stuffing Attacks（リスト型攻撃）」レポートによると、不正ログイン試行は世界中で増加しています。調査結果によると、2018 年 1 月から 4 月までに不正ログインは 1 カ月あたり約 32 億件、2018 年 5 月から 6 月までにボットからの不正ログイン試行は 83 億件以上検出され、月平均 30% の増加となりました。アカマイの研究者の分析によると、2017 年 11 月初めから 2018 年 6 月末までの 8 カ月間で、合計 300 億件以上の不正ログイン試行が発生していることがわかりました。

不正ログイン試行は リスト型攻撃によるものです。ハッカーは組織的にボットネットを使用して、盗んだログイン情報を Web を介して試そうとします。ハッカーは多くの顧客が複数のサービスやアカウントで同じログイン情報を使用しているという前提に立って、銀行や小売店のログインページに攻撃を仕掛けます。Ponemon Institute の「リスト型攻撃がもたらす損失」レポートによると、リスト型攻撃が組織にもたらす損失は年間数百万から数千万ドルに及びえます。

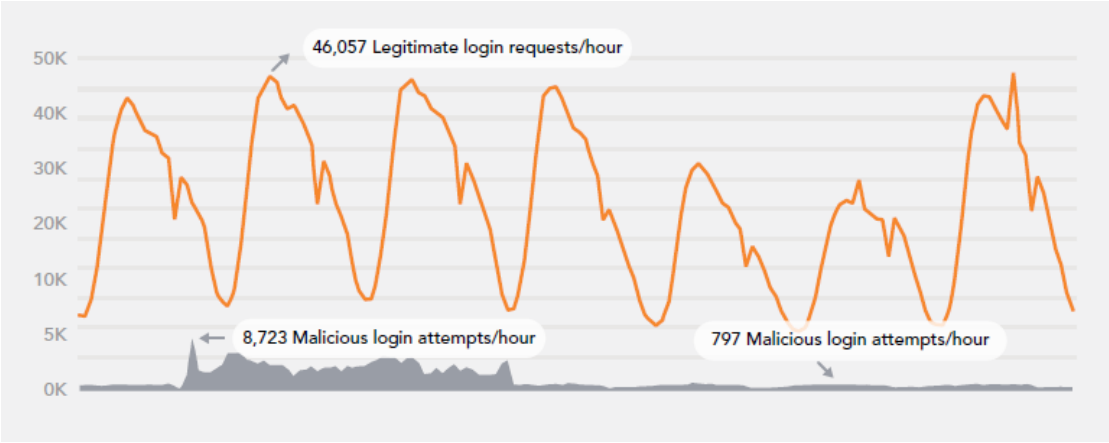
アカマイのセキュリティ／脅威分析にふるまい検出の技術が加わることにより、企業のボット管理テクノロジーは強化されます。アカマイの Web Security 部門 Vice President の Josh Shaul は、お客様をサポートしてリスト型攻撃への対抗措置を講じたときの例を紹介しています。「世界最大の金融サービス企業の 1 社である某社は、月 8,000 件以上のアカウント乗っ取りの被害に遭っており、不正に直接関連する損失は 1 日 10 万ドル以上に達していました。同社は、全利用者のログイン時にふるまい検知によるボット検出を実施するためにアカマイを活用しました。するとすぐに、アカウント乗っ取りの被害が月に 1 ～ 3 件にまで激減し、不正による損失を 1 日 1,000 ～ 2,000 ドルまでに抑えることができました」。

さらに、この「インターネットの現状」レポートでは、2 件のケースを取り上げて詳しく報告しています。これらのケースでは、アカマイが顧客のために取り組んだリスト型攻撃との闘いの詳細が記載されており、その手法が重要な意味を持つことを示しています。

1 件目のケースでは、Fortune 500 企業の某金融サービス機関が直面した問題を取り上げています。このケースでは、平時は 1 週間で 700 万回ほどのログインアクセスのあるサイトで、攻撃者はボットネットを使用して 48 時間足らずの間に 850 万回の不正ログイン試行を行いました。このボットネットには 20,000 台以上のデバイスが関与しており、1 分間に数百回のリクエストを送信することができました。アカマイの調査では、この特定の攻撃で発生したトラフィックの約 3 分の 1 がベトナムと米国からのものであることを突き止めました。

2 件目のケースでは、今年はじめに某信用組合（クレジット・ユニオン）で確認された low & slow（ローアンドスロー）タイプの攻撃を取り上げています。この信用組合に対しても不正ログイン試行が急増しましたが、このケースでは最終的に 3 つのボットネットがサイトに攻撃を仕掛けていたことが判明しました。特に目立つボットネットは検知されやすいものですが、極めてゆっくりと巧みに侵入しようとしていたボットネットが検出されたことで、より深刻さが増しました。

「当社の調査によると、リスト型攻撃の実行犯は常に攻撃手法を進化させています。大量の目立つ攻撃から、検知されにくい「low & slow（ローアンドスロー）」の攻撃まで多様化しています」と、アカマイの Senior Security Advocate であり、「インターネットの現状／セキュリティ」レポートの筆頭執筆者である Martin McKeay は述べています。さらに「特に警戒すべきなのは、1 つのターゲットに対して同時に複数の攻撃が仕掛けられている場合です。こうした多数混合型の攻撃の防御に必要な専門知識やツールを持たない組織は、最も危険なリスト型攻撃をたやすく見過ごしてしまう可能性があります」と続けています。



危険なステルス型のローアンドスロー攻撃

2018 年「インターネットの現状／セキュリティ：Credential Stuffing Attacks（リスト型攻撃）」レポート全文は、こちらからダウンロードいただけます。

https://content.akamai.com/PG11573-soti-credential-stuffing-attacks-report.html?lang=jp-ja

リスト型攻撃から組織を保護するための課題と方法の詳細については、こちらをご覧ください。
https://www.akamai.com/jp/ja/campaign/credential-stuffing-is-on-the-rise.jsp

手法

アカマイの 2018 年「インターネットの現状／セキュリティ：Credential Stuffing Attacks（リスト型攻撃）」レポートでは、アカマイのグローバルインフラストラクチャから収集された攻撃データをもとに、社内の複数のチームが調査を行っています。本レポートでは、Akamai Intelligent Platform から収集したデータを使用して、現在のクラウドセキュリティと脅威の状況の分析のほか、攻撃傾向に対する知見を提供しています。「インターネットの現状／セキュリティ」レポートには、Security Intelligence Response Team（SIRT）、Threat Research Unit、Information Security、Custom Analytics グループなど、アカマイのさまざまな部署のセキュリティ専門家が携わっています。

Akamai 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/jp/ja/、blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。

アカマイ・テクノロジーズ合同会社について:

アカマイ・テクノロジーズ合同会社は、1998 年に設立された、アカマイ・テクノロジーズ・インク（本社：米国マサチューセッツ州ケンブリッジ、最高経営責任者：Tom Leighton）が 100%出資する日本法人です。アカマイは、静的なコンテンツ配信だけでなく各種コンサート・スポーツ試合等の国内限定ストリーミング配信や Web アプリケーションなどの動的配信を多数実現し、日本国内では 350 社以上が当社サービスを利用しています。

アカマイ・テクノロジーズ合同会社は、2018 年をもって設立 15 周年を迎え、それを記念しブランディングムービーを公開しました。是非ご覧ください。
https://youtu.be/GfrXsG1AUns

※アカマイとアカマイ・ロゴは、アカマイ・テクノロジーズ・インクの商標または登録商標です
※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
※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動しうるものです