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

アカマイ、「インターネットの現状／セキュリティ：ウェブ攻撃」レポートを発表、ボットネットに包囲されるホテルおよび旅行業界の現況が明らかに

ボットによる大量の不正ログイン（Credential Abuse）、新たな手法で ウェブ上のシステムに過剰な負荷を与える DDoS 攻撃が引き続き増加

※本リリースは 6 月 26 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。

アカマイ・テクノロジーズ・インク（NASDAQ：AKAM、以下「アカマイ」）は、「インターネットの現状／セキュリティ：ウェブ攻撃（2018 年/夏）」レポートを発表しました。サービス業界をターゲットとしたボットを利用した不正ログイン（Credential Abuse）の脅威や、高度なサービス妨害攻撃（DDoS）が増えており、サイバーセキュリティ担当者がこれらの脅威に直面している現状が明らかになりました。2017 年 11 月から 2018 年 4 月の最新のサイバー攻撃の傾向分析によると、新たな脅威を緩和するためには、セキュリティチームだけでなく、開発者、ネットワーク事業者、サービスプロバイダーの即時対応力の維持が重要であることが明らかになっています。

ホスピタリティ（ホテル、旅行）業界 vs ボット：不正行為に関する分析

盗んだユーザ認証情報をボットによって悪用する行為が、インターネットビジネスにとって引き続き大きなリスクとなっていますが、本レポートのデータでは、ホテルや旅行などのホスピタリティ業界が他業界に比べ、極めて多くの、不正ログイン（Credential Abuse）を受けていることが明らかになっています。

アカマイの研究者は、特に航空、クルーズ会社、ホテル業など、ホスピタリティ業界のサイトを標的とした、およそ 1,120 億回のボットリクエストと 39 億回の悪意のあるログイン試行を分析しました。ホテルおよび旅行サイトのトラフィックのうちおよそ 40%が、既知の不正ベクトルである「既知のブラウザへの偽装」に分類されるものでした。

攻撃トラフィックの発信元を地理的に分析すると、レポートの対象期間における旅行業界をターゲットとした不正ログイン（Credential Abuse）の主な発信元は、ロシア、中国、インドネシアでした。そして、その約半数はホテル、クルーズ会社、航空会社、旅行会社のサイトに向けられたものでした。ロシアおよび中国を起点とするこれら攻撃トラフィックの数は、両国を合わせると米国を起点とする攻撃量の 3 倍でした。「これらの国々は伝統的にサイバー攻撃における大きな中心的存在でした。重要な攻撃対象としてホスピタリティ業界を選んだのは、ハッカーがボットを利用した不正行為を行ううえで魅力的に映ったからでしょう」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」レポートのシニアエディターでもある Martin McKeay は述べています。

高度な DDoS 攻撃の増加はセキュリティに適応性が必要なことを示している

単純で大規模な DDoS 攻撃は、引き続き全世界で企業や組織の攻撃に使用される最も一般的な方法ですが、その他の手法も継続的に出現しています。アカマイの研究者は今回のレポートにおいて、高度な手法を特定し追跡しました。これらの手法には、セキュリティ対策を打破するために、戦術を途中で変えながら攻撃するインテリジェントで適応力の高い攻撃者の影響が見られます。

レポートで取り上げている攻撃の 1 つは、STEAM および IRC のグループチャットを利用して攻撃を仕掛けたグループからのものでした。こうした攻撃は、ハッカーのコマンドを実行するためにマルウェアに感染したデバイスのボットネットを使用するのではなく、人間のボランティアによって実行されていました。その他の注目すべき攻撃では、ターゲットに直接、持続的に攻撃を行うのではなく、数分間続くバーストによってターゲットの DNS サーバーに過剰な負荷をかけるものがありました。インターネットでは外部のコンピューターが DNS サーバーを見つけられる特性があるため、この攻撃の緩和は難度の高いものとなります。また、このバーストは長期に渡って防御側を疲労させたため、緩和にはさらなる困難が伴いました。

「これらの攻撃タイプは、いずれも攻撃者が悪質な行為を行うために常に新しい防御に適応していることを示しています」と、McKeay は語ります。「これらの攻撃に加えて、今年前半の 1.35 Tbps という記録破りな数字を打ち出した memcached 攻撃もあり、セキュリティコミュニティが現状に甘んじている場合ではないことを示す厳しい警告のようなものとなりました」

数字による分析

「インターネットの現状／セキュリティ：ウェブ攻撃（2018 年夏）」レポートのその他のハイライト：

- 昨年同期比 16%増の DDoS 攻撃数を観測。
- 今年最大の DDoS 攻撃は、memcached リフレクション攻撃を使用したもので、過去最大の 1.35Tbps を記録。
- 研究者は、リフレクションベースの DDoS の数が昨年比で 4%増加していることを特定。
- SQL インジェクションまたはクロスサイトスクリプティングなどのアプリケーションレイヤーの攻撃数が 38%増加。
- 4 月に Dutch National High Tech Crime Unit （オランダのハイテク犯罪を専門とする公的機関）は、13 万 6,000 人ものユーザーを擁する DDoS 請負ウェブサイトを停止。

「インターネットの現状／セキュリティ：ウェブ攻撃（2018 年夏）」レポートは、akamai.com/stateoftheinternet-security から無料でダウンロードできます。アカマイの研究チームによる分析の詳細については、攻撃の注目点をご参照ください。今年前半に発生した memcached 攻撃について詳しく解説しています。アカマイブログでは、グラフなど、レポートのデータを視覚化してご紹介しています。

手法：

アカマイの「インターネットの現状／セキュリティ：ウェブ攻撃（2018 年夏）」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、社内の多様なチームによる調査を行っています。このレポートでは、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他、攻撃傾向の知見について分析しています。「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。

アカマイについて：

世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有するアカマイは、デバイスや場所に関係なく、最高、かつ最もセキュアなデジタル体験をお客様に提供します。アカマイのプラットフォームは 130 カ国に 20 万台以上という比類のないスケールで展開されており、お客様に優れたパフォーマンスとセキュリティを提供しています。ウェブ/モバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、ビデオ・デリバリー・ソリューションによって構成されるアカマイのソリューションは、優れたカスタマーサービスと 365 日/24 時間体制の監視によって支えられています。グローバルトップの金融機関、e コマース事業者、メディア・エンターテインメント企業、政府機関等が、アカマイを信頼する理由について、www.akamai.com/jp/ja/ または blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。