2020 年 7 月 2 日

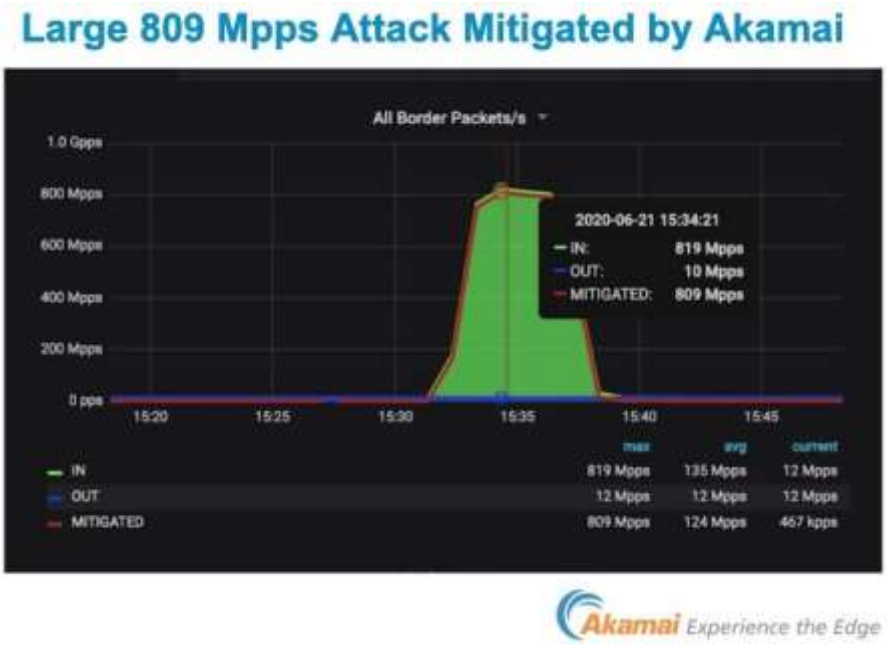
*Press Release*

アカマイ・テクノロジーズ合同会社

# 【セキュリティアラート】
# 大規模で巧妙な DDoS 攻撃の増加傾向に懸念
## アカマイ、短期間で 2 度の大規模 DDoS 攻撃を緩和

※本アラートは 2020 年 6 月 26 日、および 7 月 2 日に公開されたブログをまとめたものです。
6 月 26 日付ブログ: https://blogs.akamai.com/jp/2020/06/akamai-mitigates-sophisticated-144-tbps-and-385-mpps-ddos-attack.html
7 月 2 日付ブログ: https://blogs.akamai.com/jp/2020/07/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html

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 Technologies（以下、「アカマイ」）は、2020 年 6 月に立て続けに 2 度発生した分散型サービス妨害攻撃（DDoS）を緩和したことをお知らせします。特に、6 月 21 日(日)に観測した攻撃は、欧州の大手銀行を標的としたもので Akamai プラットフォームにおいて観測史上最大のパケット／秒（PPS）となる 1 秒あたり 8 億 900 万ものパケット数を記録しました。この攻撃は Akamai の事前対応型緩和制御により完全に緩和されました。



これは、PPS で測った規模としては最高と考えられ、Akamai プラットフォームでこれまで観察された最大記録の 2 倍をゆうに超える規模となりました。また、この攻撃のわずか 1 週間前に Akamai は別の大規模 DDoS 攻撃について発表したばかりでした。
(参考：https://blogs.akamai.com/jp/2020/06/akamai-mitigates-sophisticated-144-tbps-and-385-mpps-ddos-attack.html
『アカマイ 巧妙な 1.44TBPS, 385MPPS の DDOS 攻撃を緩和』Akamai Japan ブログより)
2020 年に入ってからの DDoS 状況を全体的に見ると、大規模で複数の攻撃ベクトルを用いる巧妙な DDoS が今も衰えていないことがわかり、様々な業種の企業にとって非常に懸念される状況です。

**攻撃タイプの違い：BPS と PPS**

DDoS 攻撃は常にボリューム型であることを特徴とし、通常は 1 秒あたりのビット数（bps）で計測されます。このタイプの DDoS 攻撃の目的は、対応できる設計容量を超えるトラフィックを送信することで、標的となるサイトから見てインバウンドのインターネットパイプラインを過負荷状態にすることです。一方で、PPS にフォーカスした攻撃の多くは、標的のデータセンターまたはクラウド環境内にあるネットワーク機器やアプリケーションを過負荷にすることを目的としています。どちらもボリューム型ですが、PPS 攻撃は、回線の容量ではなく、機器のリソースを疲弊させます。

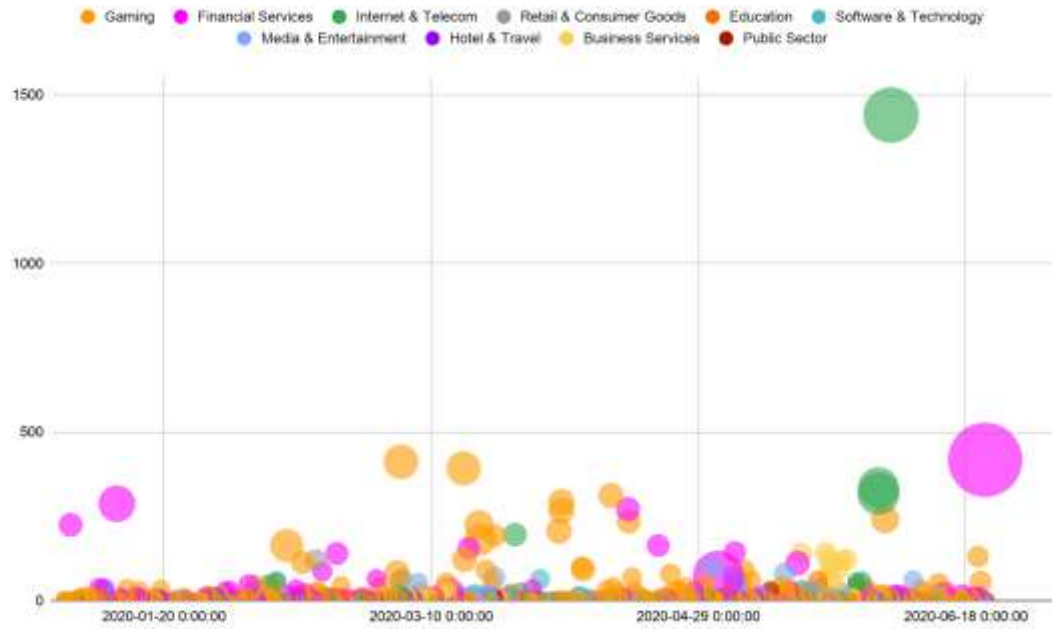
DDoS 攻撃のタイプをわかりやすく比較するため、食料品店のレジに例えてみます。bps で計測され、大きな帯域幅を消費する攻撃は、1,000 人の買い物客がそれぞれカートをいっぱいにしてレジに並ぶようなものです。一方、PPS ベースの攻撃は 100 万人の客がそれぞれガムを 1 個買うといったものです。どちらのケースも、最終的にはサービスまたはネットワークがトラフィックに対応できなくなります。
今回の攻撃は明らかに PPS の負荷を高めて DDoS 緩和システムを疲弊させるという目的で最適化されていました。

**その他の特徴**

- **ソース IP 数の増加**
  今回送信されたパケットはソース IP アドレスの数が短時間で大幅に増加したという点も特徴の 1 つでした。標的となったお客様を宛先とするトラフィックのソース IP 数は今回の攻撃中に大幅に増加しました。これは非常に分散度が高いことを示しています。このお客様を宛先とするトラフィックに利用された 1 分あたりのソース IP 数は通常の 600 倍以上でした。
- **ソース IP の 96.2%が未知**
  この攻撃ではほとんどのトラフィックが 2020 年になるまで攻撃で記録されたことのない未知の IP から送信されています。初めて観察された（少なくとも最近の攻撃に関連して追跡されていない）ソース IP が 96.2%も占めているのは、非常に稀なケースです。
- **ピークまでの速度**
  6 月 21 日の攻撃は、サイズだけでなく、ピークに到達する速度の面も特徴的でした。数秒間で通常のトラフィックレベルから 418Gbps に拡大し、約 2 分でピークサイズである 809Mpps に到達しました。攻撃全体の継続時間は 10 分弱です。

**大規模 DDoS 攻撃の標的となっている業界**

今回の攻撃は欧州の大手銀行を標的としていましたが、下のグラフのピンク色の円で示されている通り、金融サービスは標的として狙われやすい業種といえます。このグラフは経過時間（X 軸）における Gbps（Y 軸）と Mpps（円の大きさ Z）を業界別に表したものです。2020 年に発生した記録的な PPS 攻撃は両方とも金融企業に対するものでしたが、グラフの右上の緑色の円が示すように 1 週間前に起きた過去最高を記録した Mbps 攻撃は大手のインターネット&電気通信企業（この攻撃ではホスティングプロバイダー）を標的としていました。




**Akamai の対応**

こうした大規模な攻撃を有効に緩和するためには、計画と専門的なリソースが必要です。最初に顧客のトラフィックの内容を深く把握し、通常の、つまりベースラインとなるトラフィックパターンとボリュームを特定して、事前対応型の緩和制御を設定します。目的は、正当なトラフィックに影響を及ぼすことなく、悪性のトラフィックを検知し、緩和を成功させることです。事前対応型の緩和制御は、様々な攻撃に対する緩和効果を高めるために極めて効果的な方法であることが実証されています。ただし、事前対応型の緩和は Akamai の SOCC チームが採用している多数のツールや機能の一例にすぎません。Akamai の SOCC は、DDoS 検知時間と緩和効果を継続的に改善しています。

Akamai は常に業界をリードする SLA (Service Level Agreement) に基づいた、DDoS 攻撃の検知と緩和を成功させています。テクノロジーと人とプロセスを組み合わせた Akamai 独自の手法により、これまでも最大規模の攻撃を緩和してきました。Akamai、特に当社の SOCC チームにとって大規模な DDoS 攻撃は日常茶飯事です。自動緩和と人間による緩和を組み合わせることで、インターネットをより安全な場所にすることが可能になります。

最先端の Akamai DDoS 緩和プラットフォームと SOCC の詳細については、こちらをご覧ください。
https://www.akamai.com/jp/ja/products/security/prolexic-solutions.jsp

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