Akamai

ホワイトペーパー

「パーティーの混乱」を回避するには

適切なアプリケーションレイヤー DDoS 対策プラットフォームの活用を

現在におけるアプリケーションレイヤー DDoS の意味

世界中のセキュリティ専門家が痛感しているとおり、DDoS（分散型サービス妨害）攻撃は、膨大な量の悪性トラフィックを送り込んで運用を停止させることで、Web サイトやネットワークリソースを利用できない状態に追い込む、サイバー攻撃の一種です。DDoS 攻撃は、依然として攻撃者が使用する最も一般的な攻撃手法であり、過去 5 年間で増加傾向にあります。たとえば、1 秒あたりのパケット数（PPS）という観点から見ると、最近発生した大規模な攻撃は約 2 分で最大 809 MPPS に達しました。

攻撃の増加に関するトレンドとして、アプリケーションレイヤー DDoS 攻撃のインスタンスの増加が見られます。レイヤー 7 DDoS 攻撃とも呼ばれるこうした攻撃は、ネットワーク全体ではなく、特定の Web アプリケーションを標的として妨害します。防御側が防御や緩和を行うのは困難である一方で、自動化やクラウドサービスなどのテクノロジーが普及したため、攻撃者はこれらの攻撃を開始するために必要なツールに簡単にアクセスできるようになり、アプリケーションレイヤーを侵害することがかつてないほど簡単になりました。

実際のところ、この種の攻撃で使用されるリクエストは通常のエンドユーザーリクエストのように見えるため、攻撃の巧妙さを測る簡単な方法はありません。標的となるサーバーとネットワークの両方に効率的に影響を与えられるということは、攻撃がより少ない帯域幅でより多くの損害を生み出すことを意味します。要約すると、アプリケーションレイヤー攻撃とは、実装は簡単で、スローダウンや停止させるのは困難であり、標的に特化しているものです。

アプリケーションレイヤーの DDoS 攻撃が自社にどのような独自の影響を与えているかを把握するためには、すべてのカテゴリーの DDoS 攻撃が自社にどのような影響を与えるかを知る必要があります。ここでは、DDoS 攻撃のカテゴリーを、パーティーに潜む危険に例えて考えてみましょう。少数のゲストを自宅に招いて特別な日を祝ったり、週末を楽しんだりする際には、次のようなシナリオに発展してしまう可能性があります。

DDoS 攻撃の種類

シナリオ 1
ボリューム型攻撃

ゲストはあなたのパーティーに招かれたことに大喜びし、（ソーシャルメディアなどで）情報をたくさん共有しました。誰でもパーティーに参加できるという話が独り歩きし、パーティー当日、たくさんの見知らぬ人がやって来ました。あなたが招待していない人によってすべてのリソースが消費されるため、これはボリューム型 DDoS 攻撃に相当します。

シナリオ 2
プロトコル攻撃

あなたが信頼するゲストが危険にさらされています！パーティーに招待されたい（が招待されなかった）人が、ゲストの 1 人を脅して、パーティーの詳細を教えるよう求めました。そのゲストが要求に屈したため、招待されていない大勢の人がパーティーに押しかけられるようになりました。パーティーに関する情報を秘密にしておくべき人が秘密を漏らしたため、これはプロトコル DDoS 攻撃に相当します。

シナリオ 3
アプリケーション攻撃

あなたのパーティーの噂を聞きつけた悪意ある人物が、招待ゲストを装ってあなたの家に侵入し、窃盗や強盗をしようと計画します。この人物は正式なゲストを装っているため、これはアプリケーション DDoS 攻撃に相当します。

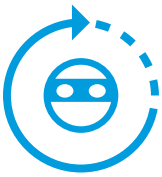
これらのシナリオのすべてには、イベントのために自宅を開放した、という共通の脆弱性が存在します。アプリケーション層は、組織がユーザーとやりとりする層のため、この脆弱性を、アプリケーションレイヤー DDoS 攻撃が利用することは避けられません。また、この層ではユーザーに直接サービスを提供するため、組織がもつ制御がより少ない層となり、アプリケーションレイヤー DDoS 攻撃を緩和するのはますます困難になります。

さらに、これらの問題のいずれかが生じた場合、追加コストが発生します。消費される食べ物や飲み物が増えた分の費用負担、見知らぬ人があなたの個人情報を手に入れたという状況への対処、そして襲来された自宅の後片付けなどが必要になるため、パーティーは失敗に終わり、代償も多大です。

アプリケーションレイヤー DDoS 攻撃は、現在では頻繁に発生しており、防御が最も困難な攻撃の 1 つです。そのため、多くのセキュリティソリューションが、アプリケーションレイヤー DDoS 攻撃からシステム、リソース、機密情報を保護することをますます約束するようになっています。組織はそれを頼りに、提供する製品やサービスを保護してきました。そのため、結局のところ、DDoS 防御の良し悪しは、保護を委ねるプラットフォーム次第となっています。そこで、最適なアプリケーションレイヤー DDoS 防御プラットフォームを探す際に知っておくべき最新の変化とトレンドを確認しましょう。

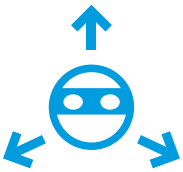
どのようなトレンドと変化があるのか

私たちが特定の攻撃に対するソリューションを作成すると、いつもの通り、ハッカーはそれに対抗して戦略を適応させます。このせめぎあいを観察したところ、次の 4 つのトレンドと変化があることが分かりました。



1. 反復的な短期攻撃に移行

DDoS 攻撃は、期間が短くなっていると同時に、規模や頻度が増加しています。Akamai は、ARM、SYN フラッド、UDP リフレクション（DNS、WS-Discovery など）、HTTP フラッドなどを組み合わせた 9 種類以上の攻撃ベクトルを持つ複雑な攻撃があることを確認しました。



2. マルチベクトル攻撃の使用頻度が増加

攻撃者の 20% 以上がマルチベクトル DDoS 攻撃を使用しており、さまざまな DDoS 攻撃手法を組み合わせた短い攻撃を次々と繰り返しています。Link11 によると、同時に観察されたベクトルの最大数は 18 で、2021 年から 50% 増加しています。

3. 検知とその後の緩和を回避する能力が向上

攻撃トラフィックと通常トラフィックの区別は難しく、アプリケーションレイヤーの場合は特に困難です。たとえば、ボットネットが攻撃対象のサーバーに対し HTTP フラッド攻撃を実行するとします。ボットネット内の各ボットは正当なネットワークリクエストを行っているように見えるため、トラフィックはスプーフィングされず、発信元が「正常」に見える可能性があります。

4. 最初は自動化を利用し、その後戦術を調整

クラウドプラットフォームや IaaS ／ PaaS の普及に伴い、攻撃者は自動化とコンピューティング能力に容易にアクセスできるようになり、攻撃を自動化して迅速かつ大規模に攻撃を開始することが簡単になっています。そのため、これらの攻撃は単にボリュームがあるだけでなく、より分散されており、ランダムで、巧妙に細工されています（リクエストのパラメーターのランダム化など）。

パーティーの例えで説明したように、あなたの家は、リソースの消費、脆弱性のあるゲスト、偽装した攻撃者という 3 つの方法で、危険にさらされる可能性があります。アプリケーションレイヤー攻撃のトレンドと変化に伴って、あなたの家も、気付かれないように画策された混乱状態に陥っているかもしれません。しかも、これら 3 つのカテゴリーにわたり全てが編成され、このステルス性が高められています。つまり、あなたの家にいくつの入口があるかを前もって確認し、事前にパーティーのドレスコードを確認し、偽の SNS プロフィールを作成してあなたのことを把握し、パーティーのゲスト全員を騙して攻撃者があなたの親しい友人だと思わせたりするのです。

アプリケーションレイヤー DDoS 攻撃は複雑化しているため、従来よりも総合的な防御戦略を策定することが有効です。これまでは、社内に構築された WAAP（Web アプリケーションと API の保護）など、どのような WAAP でもニーズを満たすことができました。今では、昨今発生している複雑なアプリケーションレイヤー攻撃に勝る WAAP が必要です。

総合的なアプローチによるアプリケーションレイヤー DDoS 防御

アプリケーションレイヤー DDoS 攻撃の検知が難しい理由は、マルチベクトル攻撃に明らかなパターンがあっても、意欲的な攻撃者は攻撃への対応を監視し、断固とした防御者をかわすように修正するためです。この課題に一貫して正確に対処するためには、検知、緩和、セルフサービスの各機能全体で WAAP を強化する必要があります。

究極的には、WAAP が家の正面玄関だけを守るのではなく、すべての入口を守り、ゲストを装った攻撃者を特定する方法を把握し、同時に複数の攻撃に直面した場合のためにスケーラビリティを確保できることが求められます。幸いなことに、適切なプラットフォームを採用すれば、アプリケーションレイヤー DDoS による混乱を緩和し、通常どおりビジネスを継続することができます。DDoS 緩和戦略は、より総合的で、次のことに重点を置いたものにする必要があります。

プラットフォームのスケーラビリティ

WAAP が日常的にどれほど良好に機能していても、ボリューム型攻撃を吸収できるだけのスケーラビリティがなければ、すぐに破綻します。そのため、WAAP の基盤となるプラットフォームは、WAAP 自体と同じくらい重要です。また、プラットフォームの実行場所も知っておく必要があります。たとえば、Akamai は世界中にエッジロケーションを有しており、多くの場合、攻撃が発生する地域にエッジロケーションがあります。始まった場所で攻撃を緩和できれば、DDoS 攻撃の阻止ははるかに簡単になります。さらに、スケーラビリティがあれば、レート制限やカスタムルールといった最低限の機能を運用しやすくなります。

情報に基づいた保護を行うためのデータリソースとアウトプット

どんな WAAP でもトラフィックを監視し、生成したデータに関するレポートを作成できますが、グローバルな観点からデータを集約できるソリューションを検討することが重要です。ソリューションプロバイダーが何千もの企業のトラフィックを可視化できる場合、生成されたデータは同じ脅威に直面している組織間でコンテキスト化され、ソリューション内の機械学習システムに適切に情報を提供できます。その後、社内チームはこのデータを調達して利用し、それを繰り返しながらソリューションをカスタマイズできます。

ソリューションの可視性と正確性

検知方法にはデフォルトで備わっているものもあります。例えば、ふるまい／異常ベースの検知では、受信クライアントのトラフィックだけでなく、オリジン接続レートやサーバーのパフォーマンスパラメーターにも注目します。しかし、堅牢なデータセットから情報を得るスケーラブルなソリューションを使用すると、WAAP はより的を絞り込んだ、精度が高いものとなります。さらに、トラフィックで何が起こっているのかをより詳細に把握できます。これは、このソリューションが適応性に優れ、攻撃が隠れているかどうか（インターネット上のオープンプロキシの背後に隠れている攻撃など）を把握できるからです。これらすべてが、フォールス・ポジティブ（誤検知）を大幅に減らしながら、適切な担当者に確実に通知するために役立ちます。

つまり、もしあなたが、混乱に陥るリスクのないパーティーを計画したいなら、これらすべての要素を確保するために、招待されていない可能性のある来客にも対応できる十分な大きさの家(スケーラビリティ)を確保する必要があります。パーティーで嫌な体験をしたことのある人（データリソース）に話を聞き、事前に取るべき対策を把握しておく必要があります。招待者リストを事前に共有して、ゲストが家に入る前に全員を出迎え（可視性と正確性)、全員が安全であることを確認する必要があります。

これらの作業のすべてを自分で行いたくなければ、信頼できる協力者を雇い、代行してもらうこともできます。マネージドサービスを利用すれば、通常のゲストと悪性のゲストを区別するために細心の注意を払う必要がある、すべての兆候を監視できます。さらに、一般的になりつつある検知困難なタイプの攻撃を阻止するために、スタッフの時間と専門知識を 24 時間体制で費やさなければならないというストレスもなくなります。

アプリケーションレイヤー DDoS に関する話は、アプリケーションレイヤーの一部として自然に生じる変数や脆弱性に満ちたものです。アプリケーションレイヤー DDoS 攻撃は、組織にとって極めて大きな損害をもたらす可能性があるため、これは重要な話です。しかし、この種の攻撃に対する防御は、複雑で無秩序である必要はありません。必要なのは、戦略的でスケーラブルなデータに基づいたソリューションです。それがあれば、パーティーを楽しむことができるのです。

レイヤー 7 の DDoS 防御に関して Akamai がお客様をどのようにサポートできるかについて、ぜひ詳しくご覧ください。