サイバーセキュリティシェフ：

レイヤー 7 DDoS 回復力強化のための究極のレシピ集を作成する

目次

はじめに

今日の分散型サービス妨害（DDoS）攻撃に対して適切な防御を講じることは、熟練のセキュリティ担当者にとっても容易ではありません。これは特に、複雑さが増すレイヤー 7 DDoS 攻撃に言えることです。そのため、さまざまな脅威に対する異なるアプローチの手順説明書、つまり、レイヤー 7 DDoS 防御の「レシピ集」があると便利です。

攻撃者はそれぞれ、異なる方法で DDoS 攻撃を準備します。レイヤー 3 と 4 に対する攻撃は強さが物を言います。ネットワークキャパシティが大きいのはどちらでしょうか？攻撃側か、防御側か？一方、レイヤー 7 攻撃は、ソフトウェアアプリケーションと直接やり取りするオープンシステム相互接続（OSI）モデルのアプリケーションレイヤーを標的にします。キャパシティ、メモリ割り当て、またはシステムのリクエスト処理方法の弱点を悪用して、Web サーバーやデータベース、アプリケーションを過負荷状態にすることが目的です。

したがって、レイヤー 7 DDoS 攻撃の緩和には特定の課題があります。このようなリクエストは正当なトラフィックに見えることが多いため、正当なユーザーに影響を与えることなく悪性のリクエストを除去することが困難になっています。さらに、自動化とクラウドリソースの利用が可能になったことで、攻撃者は、かつてないほど容易に、このような攻撃を迅速かつ大規模に開始することができます。

このホワイトペーパーでは、レイヤー 7 DDoS 攻撃を緩和する際の課題について取り上げるとともに、攻撃者が使用するツールやテクニック、攻撃者に対抗するための検知と緩和の戦術、事後分析と復旧の提案などを説明した詳細なレシピもご紹介します。

Akamai は、コンテンツ配信、サイバーセキュリティをはじめ、世界中に 4,200 か所以上の Point of Presence を擁する分散型クラウドプラットフォームを展開してきた歴史があり、今日の DDoS 攻撃に関して独自の視点を持っています。アプリケーションレイヤーに対する DDoS 攻撃が複雑かつ多面的になり続ける状況においては、独自の視点と徹底した防御戦略を持つことが重要です。本書ではその点を解説していきます。

特定の脅威や脆弱性に関する支援を求めている最前線のセキュリティ担当者、またはセキュリティ体制の改善を求めている CISO などのために、このレシピ集では成功の秘訣をご紹介します。

レイヤー 7 DDoS 攻撃の一般的な標的と攻撃例

レイヤー 7 DDoS 攻撃は、OSI モデルの最上位層であるアプリケーションレイヤーを標的としています。これらの攻撃は、Web アプリケーションがリクエストを処理する方法を悪用して、標的のリソースを過負荷状態に追い込むことを目的としています。以下は、レイヤー 7 DDoS 攻撃の一般的な標的です。

Web サーバー：攻撃者は、Web サーバーを標的にして、正当なユーザーへのコンテンツ配信を妨害します。これにより、Web サイトの読み込みが遅くなったり、完全にアクセスできなくなったりすることがあります。

Web アプリケーション：データベースやバックエンドサービスに依存するアプリケーションは、アプリケーションがクエリーを解析したり、リクエストを処理したり、セッションを管理したりする際の弱点を悪用されるおそれがあり、レイヤー 7 DDoS 攻撃に対して脆弱です。

アプリケーション・プログラミング・インターフェース（API）：API は、最新の Web サービスやモバイルアプリケーションの重要なコンポーネントです。攻撃者は API を標的にして、異なるソフトウェアサービス間のやり取りを妨害し、それらの API を使用するアプリケーションの機能に影響を与えます。

DNS サービス：DNS 攻撃は他のレイヤーでも発生する可能性がありますが、レイヤー 7 に対する攻撃では、DNS サービスに悪性のリクエストを大量に送信することで、ドメイン名の解決を妨害し、広範囲にアクセスの問題を発生させます。HTTP／TLS を介した DNS の採用が増加すると、このような攻撃が増加する可能性があります。

E メールサーバー：E メールサーバーを標的にして通信を妨害し、インバウンドとアウトバウンドの E メールに影響を及ぼします。

支払いゲートウェイと金融サービス：これらは、トランザクションを妨害し、財務業務の混乱を狙っている攻撃者にとって利益の出やすい標的です。

Akamai の「インターネットの現状」（SOTI）に関するレポートとセキュリティに関する知見では、レイヤー 7 DDoS 攻撃の進化を定期的に調査し、攻撃ベクトルの多様性と最もリスクの高い業界を明らかにしています。

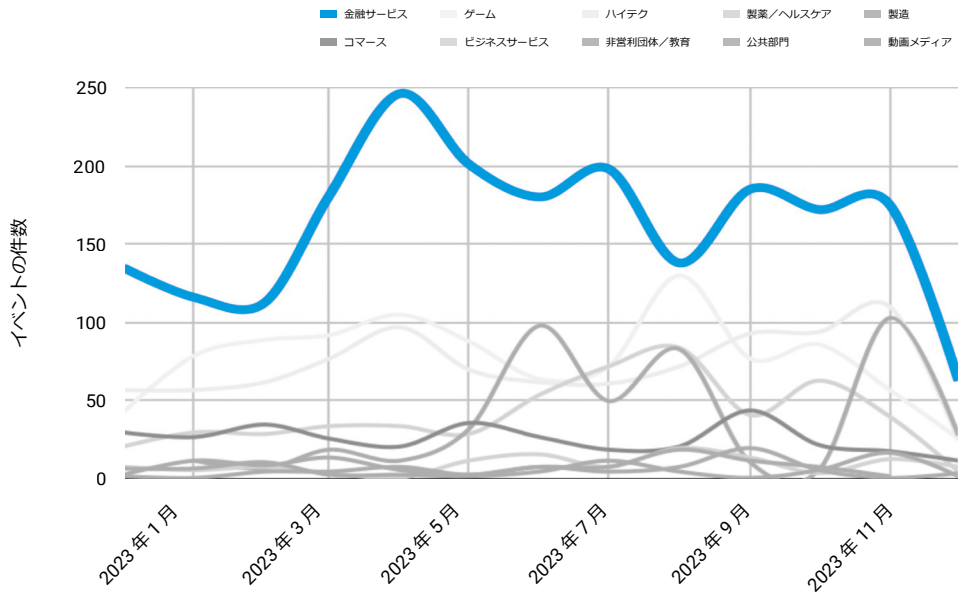
攻撃ベクトル

- Web アプリケーションおよび API 攻撃：攻撃者は通常、Web サイトのエントリーポイントを標的にします。これには、コンテンツや設定によってキャッシュされない API エンドポイントも含まれます。よく標的になるパスには、「/」、「/home」、「/en-us」、「/pricing/」などがあります。
- 次のような攻撃ベクトルがよく見られます。
  - ホームページの HTTP GET/POST フラッド
  - ランダム化されたパスやクエリー文字列の HTTPS GET フラッド
  - Slow Read 攻撃
  - 大容量ファイルのアップロードフラッド

さらに、DDoS 攻撃を受ける企業の数は年々増加していますが、現在、「手法」は変わってきています。まず、攻撃を受ける資産のタイプと量が変わりました。たとえば、同一または類似のエンドポイントに対する 10 件の攻撃ではなく、ネットワーク空間にある異なる IP を狙う 100 件の攻撃が行われる可能性があります。このような攻撃はレイヤー 3 だけでなく、レイヤー 7 も同時に標的にします。

標的となる業界

金融サービス、ギャンブル、製造業界への分散型サービス妨害（DDoS）攻撃イベントの件数は、2023 年、特に EMEA において増加しており、その他すべての地域の件数の合計を上回っています。

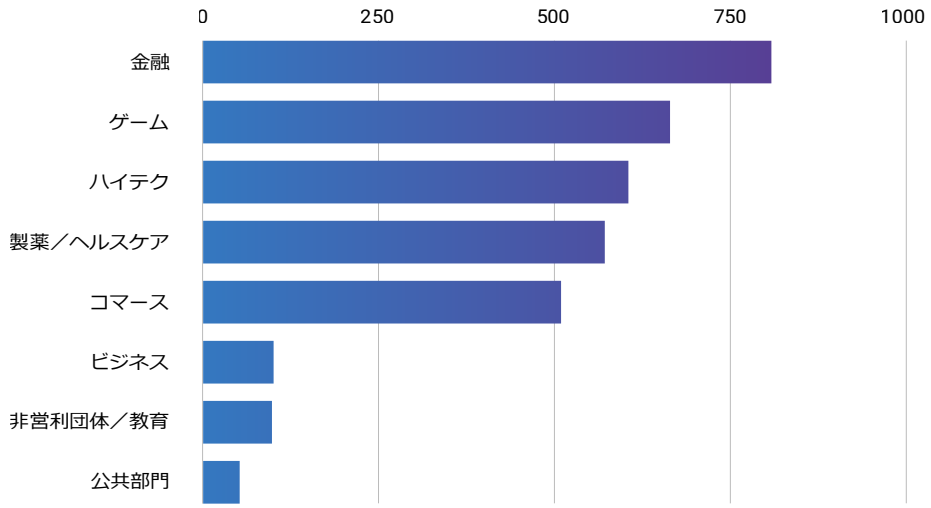


DDoS：Here to Stay、2024 年 3 月

なかでも金融サービスは、レイヤー 7 DDoS 攻撃の標的として狙われることが多くなっています。2021 年以降、Akamai は、金融サービス企業に対する DDoS 攻撃（英語版のみ）の数が顕著に増加していることを観測しています。2023 年には、すべての業界で発生した攻撃の 3 分の 1（35%）が金融サービス機関に対するもので、このセクターはゲーム業界よりも狙われやすくなっています。Akamai の分析によると、世界全体の DDoS 攻撃の 63% が銀行を標的にしていました。EMEA では約 4 分の 3（72%）、APAC では 91% の攻撃が銀行に集中していました。しかし、南北アメリカでは、銀行、保険会社、その他の金融サービス機関に DDoS 攻撃が均等に分散していました。

南北アメリカ：金融サービスは DDoS 攻撃の 28% を占めている

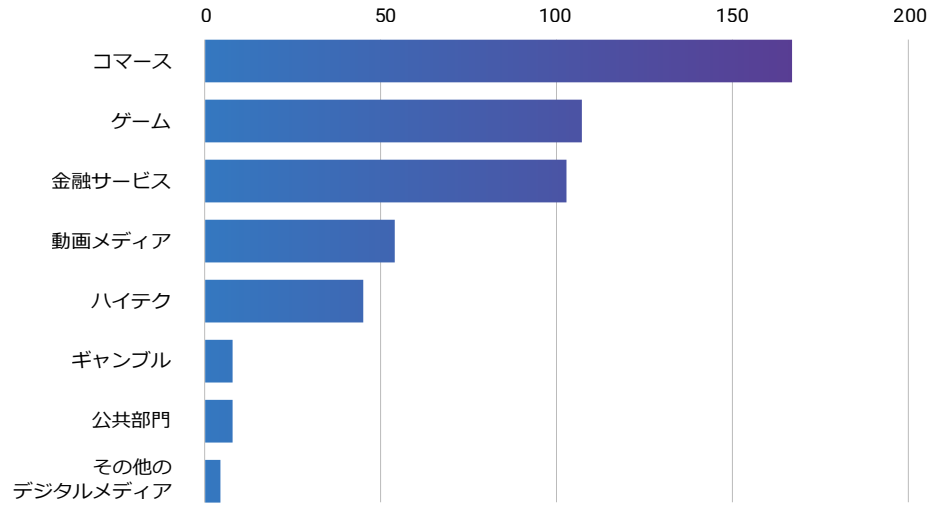
2023 年 6 月～2023 年 12 月



DDoS：Here to Stay、2024 年 3 月

APAC：金融サービスは DDoS 攻撃の 11% を占めている

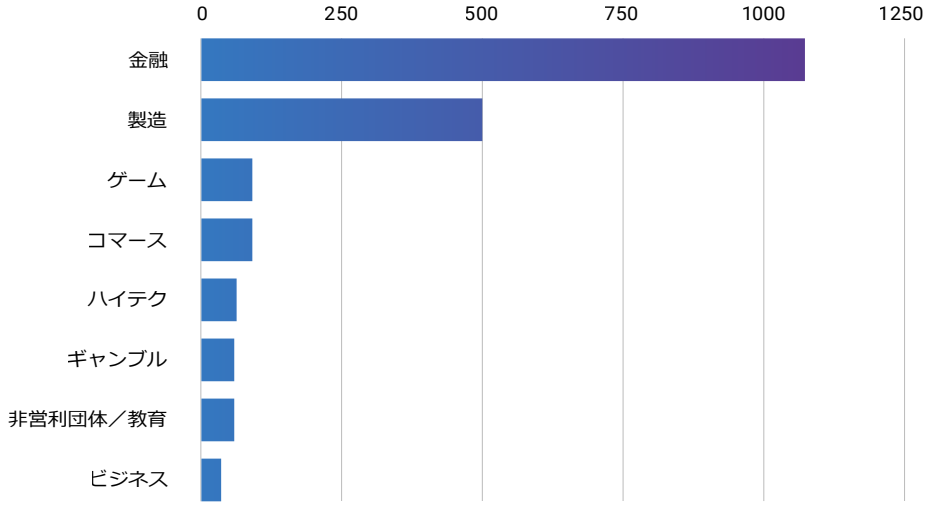
2023 年 6 月～2023 年 12 月



DDoS：Here to Stay、2024 年 3 月

EMEA：金融サービスは DDoS 攻撃の 66% を占めている

2023 年 6 月～2023 年 12 月



DDoS：Here to Stay、2024 年 3 月

Akamai の金融サービス業界の顧客を標的とした最近の高度なレイヤー 7 DDoS 攻撃では、サイバー攻撃者は自動化を利用して高度に分散された攻撃を仕掛けました。この攻撃では、主にキャッシュ不可能な URL（ホームページやログインエンドポイントなど）を狙った HTTP GET フラッドを使用していました。さまざまな事前対応型の制御を導入していたことで、この攻撃は顧客のオリジンに影響を与えることなく、適切に緩和されました。この攻撃ソースのヒートマップは、クラウド・サービス・プロバイダー、Tor 出口ノード、匿名／オープン・プロキシ・ノードの使用が増加していることを明確に示しています。

自律システムによる DDoS 攻撃

2024 年第 1 四半期に 100 か国以上で発生した金融機関に対する
アプリケーションレイヤー攻撃を示した図。いずれも、Akamai が緩和に貢献

DDoS 攻撃者は、世界中のさまざまな国や地域にまたがる大規模ネットワークの動的な IP アドレスを利用して、広範に分散した攻撃インフラを構築して調整する能力を持っています。

最新の DDoS 攻撃レシピの材料

攻撃者が使用するツールとテクニック

残念ながら、DDoS 攻撃者とその手法が停滞することはありません。攻撃者は、攻撃から収益を得る方法を探し続けており、テクニックを適応させ、新しいツールを活用して、今までにない手法を見つけます。この進化を示す要因はいくつもあります。

自動化：攻撃者は、自動化されたスクリプトとボットを使用して正当なユーザーのふるまいを模倣するため、検知が非常に困難になっています。さらに、攻撃者は従来の検知に適応して回避する機械学習アルゴリズムにも目を付けています。

マルチベクトル攻撃：攻撃者は、さまざまな攻撃タイプ（GET や POST フラッドなど）と DNS ターゲット（増幅攻撃やフラグメント攻撃など）を他の要素と組み合わせて、ネットワークリソースとアプリケーションリソースの両方を過負荷状態にするマルチベクトル戦略を採用するようになっています。

API 標的：企業がアプリケーションを強化するために API に依存するようになるにつれ、攻撃者は、DDoS 攻撃において API の脆弱性を悪用し、新たな攻撃機会を生み出しています。これらの攻撃は、数千もの接続を同時に要求することでサーバーリソースを枯渇させること、またはロジックの欠陥を悪用してサービスの中断を引き起こすことを目的としています。

IoT デバイスの悪用：安全性の低い IoT デバイスの普及により、膨大な数のボットネットが生まれています。こうしたデバイスは、ネットワーク接続とコンピューティング能力を悪用してハイジャックされ、大規模な DDoS 攻撃を開始するために使用される傾向があります。

進む高度化

このような新しいツールとテクニックにより、DDoS 攻撃の複雑さと頻度が増し、攻撃者は高度な手法を使用して従来の防御策を回避しています。顕著な傾向には次のようなものがあります。

暗号化：HTTPS ベースの DDoS 攻撃への移行が顕著で、緩和はさらに困難になっています。これらの攻撃は暗号化され、正当なトラフィックになりすまします。従来の DDoS 防御ではアプリケーションレイヤーの SSL/TLS トラフィックの復号化に制限があるため、検知と除去がより困難になっています。

ボットネットとプロキシ：DDoS ボットネットの大幅な増加と攻撃者による匿名プロキシの普及により、リクエストは多数の IP アドレスから送信されるようになりました（通常、1 回の攻撃で 10,000 以上の IP）。攻撃者はこの戦略を使用して、単一の IP からのリクエストをカウントする緩和策を回避します。クラウド・ホスティング・プラットフォームの普及とクラウドベースのサービスの導入により、こうした高負荷かつ高度に分散された攻撃を簡単に作成できるようになりました。

自律システムによる DDoS 攻撃

最近のアプリケーションレイヤーへの DDoS 攻撃（650,000 トランザクション／秒（tps）、20 Gbps、合計 90 億件以上のリクエスト）を示した図
（Akamai の金融機関の顧客に対する攻撃）

DDoS 攻撃者は、主にクラウドプロバイダーから、超分散型の攻撃インフラを構築して調整できます。

防御側が採用している最新アプローチの 1 つは、暗号のタイプやその順序など、複数の TLS レイヤー信号で構成される TLS フィンガープリントごとにリクエストを追跡する方法です。この方法はフォールス・ポジティブ（誤検知）が発生しやすいものの、正しく使用すると、攻撃者がさまざまなマシンや IP から操作している場合に、より効果的な緩和が可能になります。これは、侵害されたデバイスに同じソフトウェアがインストールされているためです。これらのデバイスは同様の環境特性を持ち、その 1 つが共有 TLS ライブラリーです。

材料の調達

市場で利用可能なツールは頻繁に変化しています。同時に、攻撃テクニックは進化し、より高度で検知しにくい手法に移行しています。その方法には、次のようなものがあります。

- **侵害された IoT デバイス：**攻撃者は、大規模な DDoS 攻撃を開始する方法としてボットネット内の侵害された IoT デバイスを継続的に使用しており、こうしたデバイスに脆弱性が存在し続けていることを明確に示しています。
- **DDoS 請負サービス：**DDoS 請負サービスが利用できるようになり、攻撃を開始する障壁が低くなったため、幅広い技術知識を持たない人でも大規模な攻撃を実行できるようになりました。

- **回避テクニック：**ランダム化されたヘッダーパラメーターや動的リクエストの引数などの高度な回避技術が、より一般的になっています。これらのテクニックは、悪性トラフィックを正当なリクエストと区別しにくくすることで、従来の検知および緩和アプローチを回避しようとします。

DDoS 攻撃に悪用される一般的な脆弱性

攻撃者がレイヤー 7 DDoS 攻撃で悪用する脆弱性は、多くの場合、Web アプリケーションがユーザー入力を処理し、データを管理する方法に関連しています。これらの脆弱性を緩和するためには、セキュリティ対策を組み合わせて使用することが重要です。

近年、アプリケーションレイヤーに対する DDoS 攻撃で悪用された最も重大な脆弱性の 1 つが、2023 年後半に広く公開された HTTP/2 Rapid Reset の欠陥でした。こうした攻撃では、インターネットとすべての Web サイトの運用の基礎となる HTTP/2 プロトコルの弱点が悪用されました。この脆弱性の悪用により、前四半期と比較して HTTP DDoS 攻撃トラフィックが全体で 65% 増加し、この脆弱性を悪用した攻撃の重大度と影響が明らかになりました。

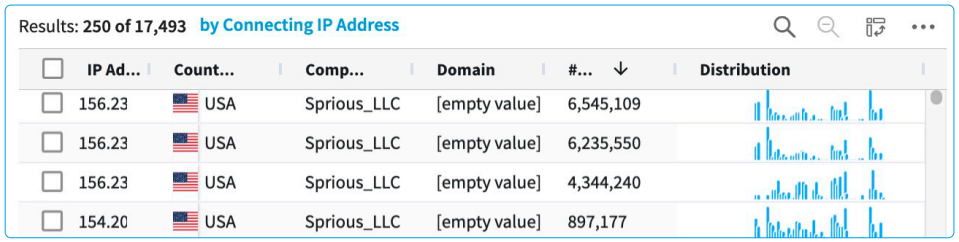
攻撃者はこの脆弱性に目を付け、クラウド・コンピューティング・プラットフォームと HTTP/2 を悪用して、比較的小規模なボットネットによる大量の DDoS 攻撃を可能にすることで、より大きな影響を与えることに成功しました。こうした攻撃の標的となった業界は、ゲーム、IT、暗号資産（仮想通貨）、コンピューターソフトウェア、電気通信であり、最大の攻撃発信元は米国、中国、ブラジル、ドイツ、インドネシアでした。

これを受け、業界全体で連携して HTTP/2 Rapid Reset の脆弱性（CVE-2023-44487）について情報を公開し、この欠陥を悪用した DDoS 攻撃を排除しました。この取り組みでは、クラウドサービスや CDN サービスの主要プロバイダーなど、さまざまなプロバイダーが対象となりました。

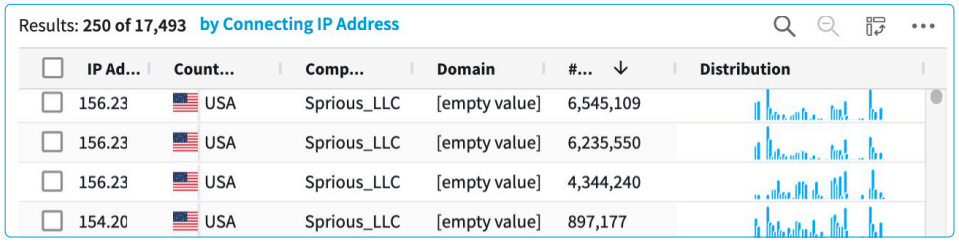
実例：DDoS 攻撃に自動化を使用する

攻撃者は多くの場合、同じ DDoS 攻撃を実行するために複数の DDoS ツールを使用します。それぞれが複数のテクニックを組み合わせて活用し、セキュリティ製品を回避したり、少なくとも効率を低下させたりします。こうした攻撃例を、Akamai Web Security Analytics のデータを使用して以下に示しています。

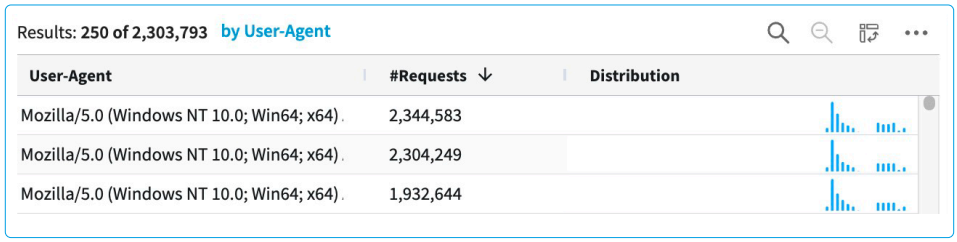
- 17,000 を超える IP アドレスからの攻撃



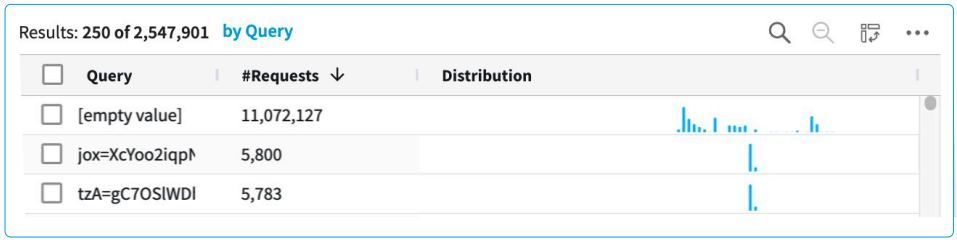
- 400 を超えるネットワークからの攻撃



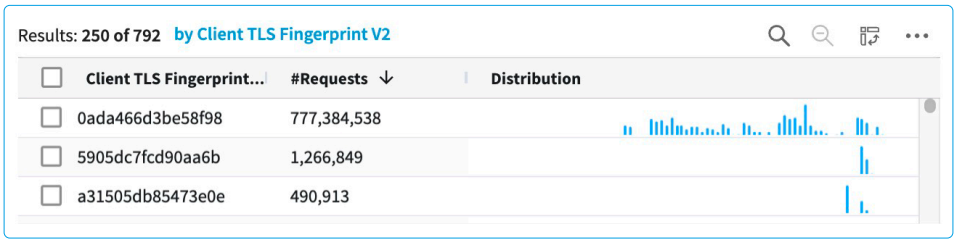
- 2,303,793 の一意のユーザーエージェント



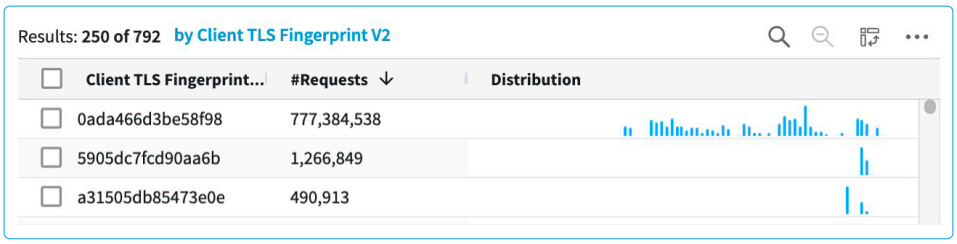
- 2,547,901 の一意およびランダムのクエリー文字列



- HTTP ヘッダーのローテーション（例：Accept-Language、Referer）



- TLS 設定のローテーション



このような高度な攻撃を緩和するためには多層防御戦略が必要です。レート制限におけるリクエストの一致とトラフィック送信元の特性との高度な組み合わせや送信元レピュテーション制御など、事前対応型と事後対応型の制御を併用すると効果的です。

攻撃者はレベルアップする：TLS 信号のなりすまし

最近の観測では、DDoS ツールで TLS 信号を使用する攻撃者が、正当な Chrome ブラウザーからの接続のように見せかけて検知を回避するケースが多発しています。攻撃者は、攻撃の速度を低下させる可能性のあるリソース集約型のヘッドレスバージョンの Chrome を使用せずに、TLS ライブラリーの修正バージョンを使用して、正規ブラウザーの TLS 信号を設定し、なりすましていた可能性があります。TLS フィンガープリントを複製する目的のツールはありますが、DDoS 攻撃ツールでは一般的ではありません。この種の攻撃例からは、攻撃者の技術的能力が高まっており、防御に関する深い知識を得ていることがわかります。そのため、レイヤー 7 DDoS 攻撃の防御戦略には、最新の攻撃傾向に関する定期的な調査結果を反映させる必要があります。これは、TLS スプーフィングを含む DDoS ツールがより一般的になっていることも示唆しているようです。

防御レシピの作成準備

現状の確認：リスク評価と脆弱性の特定

重要な資産を見極め、DDoS 攻撃に対して脆弱な場所を特定することで、レイヤー7 DDoS 緩和戦略を大幅に強化できます。このリスク評価は、重要性と脆弱性に基づいて、保護するリソースの優先順位付けに役立ちます。潜在的な攻撃ベクトルとその影響を理解することで、レート制限、Web アプリケーションファイアウォール、ふるまい分析など特定の対策を実装し、リスクを効率的に緩和できます。さらに、継続的なリスク評価により、新たな脅威や変化するビジネス要件に合わせて防御戦略を進化させることができます。

業界や企業によっては、アプリケーションレイヤーに対する DDoS 攻撃のリスク評価について別のアプローチを取る場合があります。以下に例を示します。

> **E コマース：**大規模な販売イベントの前にリスク評価を行うことにより、支払いプロセスに重大な脆弱性があると特定されるかもしれません。緩和策には、Web Application Firewall（WAF）やレート制限を実装して、サービスを保護する方法などがあります。
>
> **金融サービス：**銀行業務アプリケーションの場合、リスク評価により、ログインページが DDoS 攻撃の主な標的になると判断されることがあります。その場合、銀行は、エンドポイントに合わせたレート制限とふるまい検知を組み合わせて、正当なユーザーと攻撃トラフィックを区別することができます。

脆弱性を具体的に把握することで、的を絞った防御が可能になり、攻撃を受けている間も重要なサービスを強化できます。

「シェフが多すぎる」問題を回避する：役割と責任

明確な役割と責任を決めることは、効果的なレイヤー 7 DDoS 戦略を実現するうえで重要なステップです。これは、攻撃が発生した場合に協調的かつ効率的に対応する機会を最大限に生かすためです。役割を明確にしておかなければ、対応が混乱し、職務が重複したり、防御に隙が生まれたりする可能性があります。責任の定義は、トラフィックの監視や異常の特定から、緩和戦略の実施、関係者とのコミュニケーションまで、各チームメンバーの特定のタスクを決定するうえで役立ちます。こうした調整により、攻撃の影響を最小限に抑え、サービスの可用性を維持しながら、重要な資産を保護することができます。

実際、役割が明確でない意思決定者が数多く存在すると、DDoS 攻撃を受けた時の対応が遅れます。たとえば、ネットワーク運用チームとサイバーセキュリティチームの両方が、調整を行わずに異なる緩和策を独自に決定した場合、不注意で互いの対策を無効化したり、重要な脆弱性を見過ごしたりするおそれがあります。適切な戦略では、インシデント対応リーダーやコミュニケーションコーディネーター、技術対応チームの指名など役割を事前に定義し、攻撃に対して迅速で統一されたアクションを取り、ダウンタイムを最小限に抑え、インシデント後の分析も効率的に実施できるようにします。

自分のキッチンにぴったりのツールを選ぶ

正当なトラフィックと悪性トラフィックを区別することは非常に困難であるため、アプリケーションレイヤーへの攻撃の検知と緩和は容易ではありません。こうした進化し続ける脅威に対応するために、Akamai は次のような多層防御アプローチを推奨しています。

- **オンデマンドではなく Always-on を選択する：**DDoS セキュリティ制御が常にアクティブであることを確認し、新たに出現する脅威に迅速に対処するためにインシデント対応計画を更新します。
- **回復力と信頼性に優れたアーキテクチャを確立する：**攻撃者は、DNS、Web アプリケーション、API、データセンター、ネットワークインフラなど、複数のサービスを標的とする可能性があるため、Single Points of Failure を予測します。レイヤー 7 DDoS 攻撃から防御するためには、適切なアーキテクチャを使用することが重要です。アーキテクチャについては、常時稼働しているエッジまたは CDN ベースの DDoS 防御を選択することを考慮する必要があるかもしれません。信頼性を過大評価しないようにしてください。今日の DDoS 攻撃の規模を考えると、ほとんどのインフラを容易に過負荷状態に追い込むことができます。
- **プロバイダーの SLA を評価し**、戦略に合わせて更新します。
- **プロバイダーの準備状況を確認する：**重要なネットワークコンポーネントのレビューを定期的に実施し、さまざまな DDoS 防御メカニズムを評価して、最新の攻撃手法に対する効果を把握しているプロバイダーを選択します。
- **DDoS 攻撃対応プレイブックを確認する：**IT、運用、セキュリティ、顧客対応の担当者を集めて、攻撃を受けた場合に備えて体制を強化します。
- **緊急の DDoS 防御：**危機発生時に備えて、DDoS 緩和ソリューションプロバイダーをオンボーディングするための計画を作成します。DDoS 防御のベンダーパートナーがいる場合は、DDoS サポートホットラインに連絡してください。

検知と緩和のレシピ

効果的なレイヤー 7 DDoS 防御には、複数の検知と緩和戦略が必要です。手法はいくつかあり、それぞれに強みと重要な考慮事項があります。

ふるまい／異常ベースの検知

強み：このアプローチでは、機械学習と統計分析を使用して通常のトラフィックパターンを把握し、DDoS 攻撃を示す可能性のある逸脱を特定します。これは、以前は見られなかった複雑な攻撃に対して非常に効果的です。

考慮事項：効果的な検知には、「通常」のトラフィックのベースラインを確立する学習期間が必要であり、最長で数週間かかることがあります。この期間中は、効果的な検知が行われない可能性があります。正確にトレーニングされていない場合、モデルは誤検知を返す場合があります。

レートベースおよびスループットベースの検知

強み：この手法は簡単に実装できます。リクエストのレートと量を監視し、トラフィックが事前定義されたしきい値を超えた場合に、アラートまたは緩和プロセスをトリガーします。大量攻撃を迅速に特定する場合に有効です。

考慮事項：プロモーションイベント中などの正当なトラフィックの急増も、DDoS 攻撃と誤検知される可能性があります。レーダーをかいくぐる低容量、低レートの攻撃を検知できないことがあります。

シグネチャーベースの検知

強み：この手法では、既知の攻撃パターンのデータベースとトラフィックを比較することで、認識された脅威を迅速に特定してブロックできます。これは、一般的な攻撃ベクトルや以前に特定された攻撃ベクトルに対して非常に効果的です。

考慮事項：既存のシグネチャーと一致しない新しい攻撃または修正された攻撃は検知できません。有効性を維持するためには、定期的な更新が必要です。

チャレンジレスポンス方式のテスト

強み：このアプローチでは、着信トラフィックが人間やボットによって生成された場合、そのトラフィックにチャレンジを生成します。CAPTCHA または JavaScript の計算により、ボットや自動攻撃ツールを効果的に緩和できます。

考慮事項：チャレンジを積極的に導入すると、ユーザー体験を妨害する可能性があります。より高度なボットはチャレンジレスポンス方式のテストを通過する可能性があるため、チャレンジメカニズムを定期的に更新する必要があります。

ハイブリッドアプローチ

複数の検知と緩和戦略を組み合わせることで、より包括的な保護を提供できます。たとえば、異常ベースの検知を使用して潜在的な攻撃にフラグを付け、より広範なカバレッジを実現するために、レートベースおよびシグネチャーベースの手法で補完することで、より堅牢な防御メカニズムを実現できます。チャレンジレスポンス方式のテストでは、正当なユーザーと高度なボットをさらに区別できます。

従来の手法

IP およびジオフィルタリング：特定の IP／CIDR 範囲や、ビジネスに関係のない地域からのトラフィックをブロックまたは制限すると、これらの地域から発生する攻撃を受ける可能性を減らすことができます。この手法は、ビジネスユーザーのオリジンを把握し、制限をかけている場合に便利ですが、継続的なメンテナンスや承認された送信元リストの更新において問題が生じる場合があります。また、経験豊富なハッカーがプロキシを使用して、ジオブロッキングを回避することもあります。しかし、これは依然としてレイヤー 7 DDoS 攻撃に対する一般的な選択肢であり、初歩的な防御戦略です。

アプリケーションレイヤーのプロトコル分析：この手法では、アプリケーションレイヤープロトコル内のデータを精査して異常や悪性パターンを検知し、事前対応型防御メカニズムを有効にすることで、レイヤー7 DDoS 攻撃を緩和できます。従来のセキュリティ対策を回避する高度な DDoS 攻撃を防止できますが、パケットを詳細に検査する際に多くのリソースを消費し、誤検知のリスクが高まります。その結果、正当なトラフィックを誤ってブロックするおそれがあります。

DDoS 多層防御戦略に適したバランスの取れたレシピを見つける

DDoS 多層防御戦略を策定するためには、組織固有のリスクプロファイルと進化するサイバー脅威に合わせて詳細に調整したアプローチが必要です。この戦略の中核となるのは、重要な資産と攻撃ベクトルの可能性を特定するための最初の評価であり、次に、レート制限やファイアウォールなどの基本的な保護の実装です。高度な手法では、新たな脅威に対する異常ベースの検知、既知の攻撃に対するシグネチャーベースの検知、ボットをフィルタリングするためのチャレンジレスポンスメカニズムを組み合わせて実装する必要があります。

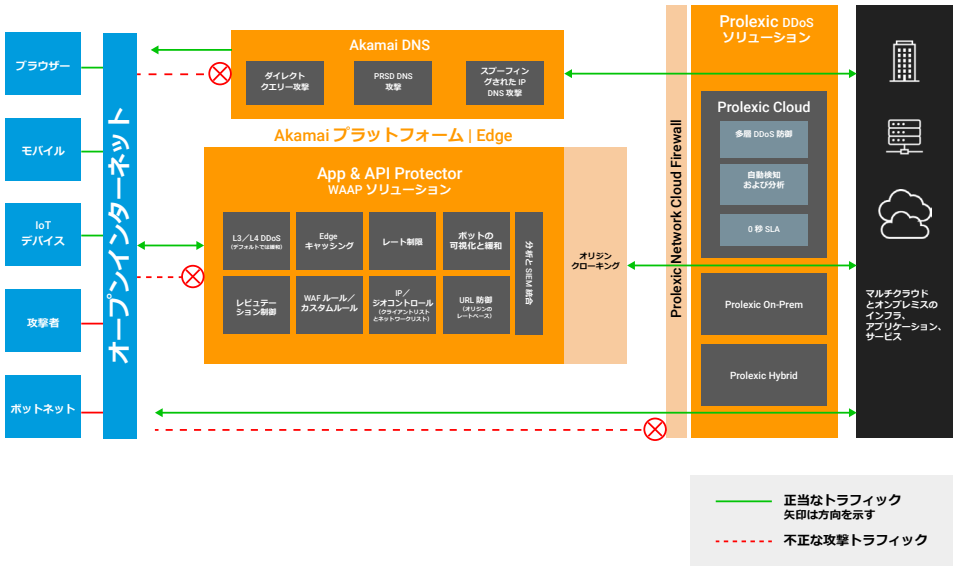
セキュリティシステムは、既知の DDoS 攻撃元と新たに出現した攻撃元の TLS フィンガープリントパターンを決定するアルゴリズムなどの適応型脅威インテリジェンスを組み込むことで、緩和策を自動的に適応させ、そのフィンガープリントを示すトラフィックをブロックしたりチャレンジを送信したりして、攻撃を効果的に緩和することができます。損害を最小限に抑え、攻撃中および攻撃後に信頼を維持するためには、包括的なインシデント対応と復旧計画が不可欠です。過去の攻撃や新たな傾向に基づいた継続的な学習と調整により、防御戦略の有効性と回復力が維持されます。

高度なマルチベクトル DDoS 攻撃に直面している金融機関は、バランスのとれた多層防御戦略を持つことの重要性を示す良い例です。ダウンタイムが業務や顧客の信頼に与える影響を考えると、金融機関は格好の標的です。

レート制限、IP／ジオフィルタリング、IP レピュテーション、リアルタイム脅威インテリジェンスなどの従来の手法を用いながら、トラフィック異常の検知などの検知および緩和の手法を組み合わせ、さらに堅牢なインシデント対応計画を使用することで、金融機関は重要な資産を妨害から保護し、顧客にサービスを提供し続けることができます。この包括的なアプローチは、現代のデジタル環境において多面的な DDoS 攻撃から組織を守る典型的な方法です。

準備：Akamai エッジアーキテクチャによる多層防御戦略

アプリケーションレイヤー DDoS 防御に対する Akamai のアプローチは、包括的で適応型の多層戦略であり、Web サイト、アプリケーション、API を最も高度な攻撃から保護するように設計されています。Akamai の App & API Protector は、Web アプリケーションファイアウォール、ボットの可視性と緩和、API セキュリティ、レイヤー 7 DDoS 防御を 1 つの製品に統合し、包括的な保護を提供する複数の主要機能で幅広く防御します。



Edge DNS、App & API Protector、Prolexic ソリューションを使用した総合的な DDoS 防御のリファレンスアーキテクチャ

Akamai の DDoS 防御戦略は、Akamai の超分散型のプラットフォームを介してトラフィックをルーティングするエッジ防御アーキテクチャを基に構築されており、すべてのリクエストがリアルタイムで検査されます。この設定により、DDoS 攻撃、Web アプリケーションおよび API 攻撃、悪性ボットをエッジで防御し、アプリケーションやインフラに到達できないようにします。その結果、攻撃に合わせてスケーリングする高速で安全性が高く、常時利用可能なアーキテクチャが維持され、事業継続性が向上します。

Akamai の堅牢なツールスイートは、事前対応型と事後対応型の制御を提供し、それぞれが総合的な防御戦略において明確な役割を果たします。

事前対応型の制御

事前対応型の制御は、脆弱性を最小限に抑えるセキュリティ体制の強化に重点を置いており、攻撃を未然に防ぐのに役立ちます。次の内容が含まれています。

- **IP コントロール（ブロック IP、CIDR 範囲、ASN）：**基本的な防御レイヤーであるこれらの制御は、既知の悪性 IP アドレスや脅威インテリジェンスによって特定された範囲をブロックします。
- **ジオコントロール（特定の地域をブロック）：**特定の地域からのトラフィックを許可または制限することで、リスクの高い地域から送信される攻撃を事前に制限できます。
- **Web Application Firewall（WAF）ルール：**FiberFox のような DDoS ツールなど、既知の脆弱性や攻撃ベクトルに対するルールを実装することで、強力な防御の最前線を実現できます。
- **IP レピュテーション制御：**DDoS、Web スクレイピング、その他の悪性アクティビティの既知のリソースに関するヒューリスティックに基づいてインテリジェンスを活用することで、疑わしいトラフィックを予防的にブロックしたり精査したりできます。
- **プラットフォーム DDoS インテリジェンス：**グローバルに分散した Akamai Edge プラットフォームから得た DDoS 攻撃の知見は、アプリケーションレイヤーへの DDoS 攻撃に対抗する事前対応型の緩和戦略の作成に役立ちます。
- **キャッシング：**コンテンツキャッシングを最適化することで、オリジンサーバーの負荷を大幅に軽減し、エッジキャッシュからのリクエストを処理することで DDoS の影響を間接的に緩和できます。
- **Site Shield：**Akamai エッジネットワークを経由したオリジンへのリクエストのみを許可するオリジンクローキングにより、サーバーの負荷をさらに軽減することができます。

事後対応型の制御

事後対応型の制御は、検知された攻撃に対応して、その影響を緩和し、サービスの可用性を維持することを目的としています。

- **レート制限（レートポリシー）：**これらは、DDoS 攻撃を示唆するトラフィックの急増を緩和するために不可欠です。設定は、顧客固有のトラフィックプロファイルに合わせて設定およびカスタマイズできます。多くの場合、レート制限は、大量の DDoS 攻撃や分散型の DDoS 攻撃から顧客のオリジンを保護する防御の最前線として役立ちます。
- **Slow POST Protection：**この制御は、特に低速な HTTP POST 攻撃に的を絞り、サーバーリソースの消費を目的とした異常なトラフィックパターンに対応します。

- **WAF のカスタムルール：**新たな脅威に対応してルールを迅速に調整し、柔軟で動的な防御メカニズムを提供できるようになります。
- **ボットの可視化と緩和：**ブラウザーの偽装を検知する機械学習により、自動化を利用した高度な DDoS 攻撃を特定してブロックできます。
- **インテリジェントな負荷制限による URL 保護：**オリジンへの過剰なリクエストを制限し、悪性のトラフィックよりも正当なユーザーを優先する制御により、DDoS 攻撃を受けている間、サービスのアップタイムを維持することができます。
- **プラットフォーム DDoS インテリジェンス：**負荷制限は URL 保護のカテゴリです。グローバルに分散した Akamai プラットフォームから得た DDoS 攻撃の知見を利用し、アプリケーションレイヤーへの DDoS 攻撃に対抗する事前対応型の緩和戦略を作成できるようにします。

材料を混ぜ合わせて、レシピどおりにバランスを調整する

- **例：**大規模な金融サービス組織は、Akamai WAAP ソリューションを使用して詳細な防御戦略を構築しています。

組織によっては、DDoS 攻撃の標的として狙われやすい場合があります。たとえば、Akamai の調査によると、2023 年には DDoS 攻撃の 3 分の 1 以上が金融サービス機関を標的としていました。大手金融サービス企業である Akamai のお客様は、ログインページを標的にした攻撃を受けましたが、実績のある防御のレシピに従って対応することができました。他の組織も同じことができます。

攻撃者のプロファイル：ハクティビスト

対象：ログインエンドポイント

方法：HTTP POST フラッド

攻撃の発生元：約 66,000 の IP アドレス、約 140 か国

レシピ
HTTP POST フラッド攻撃の緩和

材料：

事前対応型の制御：

- **IP コントロール**：脅威インテリジェンスを使用して、既知の悪性エンティティに関連付けられた IP アドレスまたは CIDR 範囲をブロックします。
- **ジオコントロール**：「Anonymous Sudan」に関係している地域など、ハクティビストグループをかくまうことで知られている国や地域からのトラフィックをブロックリストに追加します。
- **Web Application Firewall（WAF）ルール**：HTTP GET フラッドの典型的なパターンなど、既知の DDoS ツールや戦術に対抗するために特別に設計されたルールを実装します。
- **IP レピュテーション制御**：レピュテーションスコアが低い送信元からのトラフィックを注意深く監視したり、（リアルタイムで）アクティブにブロックしたりします。
- **プラットフォーム DDoS インテリジェンス**：Akamai のグローバル DDoS 攻撃データから得た知見を生かして、新たな脅威ベクトルを予測し、対抗します。
- **Site Shield**：ファイアウォールのアクセス制御リスト（ACL）を有効にして、Akamai エッジネットワークからのトラフィックのみを許可し、残りをブロックします。

事後対応型の制御：

- **レート制限**：トラフィックの急増を緩和するレートポリシーを確立し、ホームページに対する 1 秒あたりのリクエストに適切なしきい値を設定します。レート制限を最適化するためには、（1）リクエスト速度を測定する時間を 1 秒あたり 1 リクエストに縮小し、（2）接続元の IP ソースの地理的位置とレピュテーションスコアに基づいてレート制限を適用し、その一方で、金融機関の企業 IP アドレスやパートナーなどの送信元を許可リストに登録します。
- **WAF のカスタムルール**：攻撃が検知されると、攻撃の特定の特性に応じてカスタマイズされたルールを作成します。カスタムルールでトラフィック・サンプリング・コントロールを使用すると、トラフィック分析が容易になり、上位の攻撃元をより効率的に確認できます。一方、カスタムルールで IP／ジオコントロールを使用すると、迅速な緩和が可能になります。
- **ボットの可視化と緩和**：ブラウザー偽装検知を使用して、正当なユーザーのふるまいを模倣し、フラッドの一部になっているリクエストを識別してブロックします。
- **URL 防御**：正当なユーザーの帯域幅を維持しながら、ログイン URL に限定してリクエストレートを制限する制御を適用します。プロキシ、Tor 出口ノード、基本ボット、低レピュテーション IP などのカテゴリを使用したインテリジェントな負荷制限の設定により、悪性の可能性が高い送信元よりも実際のユーザートラフィックを優先させることができます。

準備方法：

レビューのフェーズ：

- **設定を確認する**：現在のセキュリティ体制を徹底的に確認します。発見した内容に基づいて事前対応型の制御を設定し、関連するすべてのジオ／IP コントロールが適切に管理されるようにします。
- **設定を最適化する**：HTTP POST フラッド攻撃の特性など、異常なトラフィックパターンを認識して緩和するように設定を調整します。

検知および緩和のフェーズ：

- **監視とアラート**：Akamai のエッジ防御アーキテクチャは、受信トラフィックを監視し、DDoS 攻撃を示す可能性のあるパターンを探します。異常なトラフィックスパイクや、HTTP POST フラッドなどの既知の DDoS 手法に一致するパターンに対してアラートを設定できます。
- **検知と緩和**：IP レピュテーション、キャッシング、IP／ジオコントロールなどのさまざまな事前対応型の制御は、正しく設定されていれば、自動的に検知機能と緩和機能を提供します。攻撃が検知されると、レート制限、URL 保護、ブラウザー偽装検知などの制御がユーザーの介入なしに自動的に開始されます。
- **分析と適応**：攻撃パターンを継続的に分析し、防御策をリアルタイムで適応させ、進化する戦術に対抗します。たとえば、最近の攻撃トラフィック分析に基づいて、独自のカスタムルールやレート制限ポリシーを作成します。

復旧と攻撃後の分析：

- **ログ分析**：攻撃後、詳細なトラフィックログ分析を実行して、攻撃ベクトルおよび展開されている制御の有効性を特定します。
- **調整**：攻撃分析から得た知見に基づいて、事前対応型および事後対応型の制御を必要に応じて調整します。

提案：

- 進化する DDoS 戦術に適応するために、防御戦略を定期的に見直し、更新してください。レビューは、特定のニーズ、脅威に対する露出度、業界のベストプラクティスに影響され、組織によって大きく異なる場合があります。金融サービス企業は、四半期ごとにこのようなレビューが必要になる場合がありますが、E コマースプラットフォームでは、半年ごとのレビューを目標にしてショッピングシーズンのピークに備えることができます。
- 新しい DDoS 攻撃ベクトルを認識して対応するために、セキュリティチームの継続的なトレーニングに参加します。
- 攻撃のシミュレーションを実施して、展開された対策の有効性をテストし、実際のインシデントに対するチームの準備体制を整えます。

復旧と攻撃後の分析

アプリケーションレイヤー（レイヤー7）に対する DDoS 攻撃の防御では、攻撃後のフェーズが将来の防御を強化し、攻撃者を把握するうえで極めて重要です。これには、攻撃パターンを分析し、分析に基づいて防御を強化するという 2 つの重要なステップが含まれます。これらのステップは、回復力に優れた防御戦略を作成し、オンラインサービスの継続性と完全性を確保するうえで重要な役割を果たします。

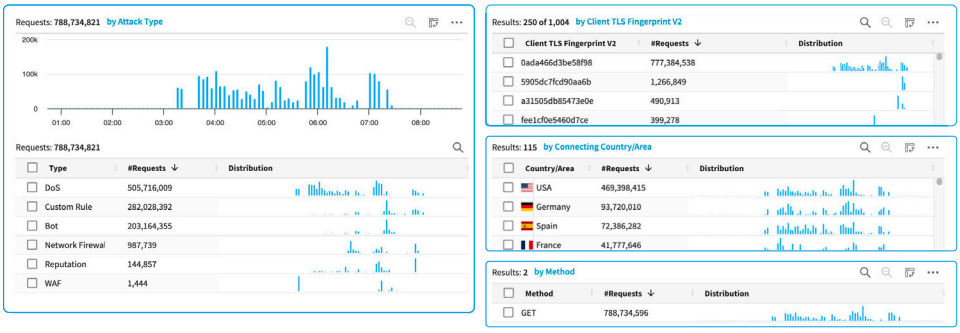
トラフィックと攻撃パターンの分析

攻撃に対処した後の次のステップは、インシデントを分析して、どの戦略が適切に機能し、どの戦略が想定どおりに機能しなかったかを理解することです。この評価では、顧客の信頼、データの完全性、潜在的な財務的損失への影響など、長期的な要因も分析します。攻撃トラフィックとその影響を理解するために、このフェーズでは、Akamai Web Security Analytics などの包括的なセキュリティ分析システムが不可欠なツールです。

この分析では、攻撃者が使用する戦術、テクニック、手順（TTP）を明らかにします。使用する主な質問は次のとおりです。

- トラフィックスパイクはどのような性質だったか？
- 特定のアプリケーション機能が標的にされたか？
- 攻撃は既知の脆弱性を悪用したか？

Akamai Web Security Analytics では、トラフィックパターンの異常を特定し、攻撃の地理的オリジンを突き止め、観察されたふるまいに基づいて攻撃タイプを分類できます。次の例は、DDoS 攻撃を調査するために適用できるトラフィックの特性またはディメンションの一部を示しています。



Web Security Analytics からの画像。セキュリティイベントについてこれまでにない可視性と事前対応型の分析を提供する

攻撃分析に基づいて防御戦略を見直し、更新する

攻撃分析に基づいて防御戦略を見直し、更新することは、組織のサイバーセキュリティ対策を強化するための重要な要素です。過去の攻撃について詳細を調べることで、現在の防御の脆弱性を特定し、情報に基づいて調整を行うことができます。ここでは、Akamai Web Security Analytics を使用してこのプロセスを適用する方法をいくつか紹介します。

例 1：攻撃パターンに基づいて WAF ルールを更新する

シナリオ：ある組織は、Web アプリケーションを標的としたレイヤー7 DDoS 攻撃を受け、大量の悪性リクエストがアプリケーションのホームページに送信されました。

レビュー：攻撃分析の結果、既存の Web Application Firewall（WAF）ルールが攻撃トラフィックの 90% 以上を適切に検知してブロックしていましたが、残りの 10% 近くが漏れていたことが判明しました。これは、地域の明示的な許可リストがあり、その地域の攻撃送信元がこのリストを使ってアプリケーションを過負荷状態にしていたためです。

更新：分析結果に基づいて、WAF 設定を更新し、この地域からの攻撃トラフィックに見られる特定の特性に合ったカスタム WAF ルールを使用するようにしました。オーバーライドでは、この地域を許可したまま、攻撃トラフィックの特定の属性をブロックできます。さらに、この地域のレート制限設定をより厳密なものにしました。

例 2：オリジン保護を強化する

シナリオ：小売業向け Web サイトのログインプロセスが、自動ボットを利用した分散型の高度なレイヤー 7 DDoS 攻撃を受けました。

レビュー：攻撃後の分析では、攻撃トラフィックが 150 を超える国から高度に分散され、正当なブラウザーのように見える数百の TLS フィンガープリントがあったことがわかりました。クラウドプロバイダーから発信された相当量のトラフィックのうち、一部は信頼できるパートナーソースとして許可されていました。攻撃は効果的に緩和されましたが、分析により、追加の防御策が必要であることが明らかになりました。

更新：この組織は、支払いプロセスのような高コンピューティング URL を保護するために、URL 保護を実装しました。これは、高度に分散されたアプリケーションレイヤー DDoS 攻撃から計算負荷の高い URL と API エンドポイントを保護するために特別に設計された機能です。セキュリティアーキテクトは、ボット、プロキシ、IP レピュテーションなどのインテリジェントな負荷制限も実装しました。URL 保護のこのサブ機能は、悪性の可能性が高い送信元からのリクエストを最初に拒否することで、実際のユーザートラフィックの優先順位付けを支援します。

また、高速攻撃中にスケーリングできなかったオンプレミス・ボット・ソリューションが存在するため、以前は適切に考慮されていなかった WAF のボット保護機能を組み込むことも決定しました。

例 3：API エンドポイントのレート制限を実装する

シナリオ：金融サービスアプリケーションの API エンドポイントが大量の不正なトランザクションリクエストによって過負荷状態に追い込まれ、サーバーリソースの枯渇を狙ったレイヤー 7 DDoS 攻撃を受けたことが判明しました。

レビュー：攻撃パターン分析により、攻撃者は、大量のリクエストを処理できない比較的手薄な API エンドポイントを標的にしたことがわかりました。

更新：これに対応して、すべての API エンドポイント、特に脆弱であると特定された API エンドポイントに厳密なレート制限を実装しました。また、API ロジックの悪用、シャドウ API の脅威、API 脆弱性の監視など、API セキュリティの高度なレイヤーを提供する専用 API セキュリティアドオンも採用しました。

戦略上の重要ポイント

- **継続的な監視とロギング：**堅牢な監視およびロギングシステムを確立して、異常を迅速に検知し、攻撃中および攻撃後に損害を正確に評価します。
- **脆弱性管理：**既知の脆弱性を緩和するためにシステムを定期的に更新してパッチを適用することで、悪用のリスクを軽減します。
- **攻撃パターンの分析：**攻撃パターンを詳細に分析するための適切な可視化ツールを使用して、攻撃者の手法と意図を理解します。

攻撃後の分析

攻撃による損害を評価し、攻撃パターンを分析することは、堅牢なレイヤー 7 DDoS 防御戦略の重要な要素です。これらの手順を踏むことで、攻撃の即時の影響を理解して緩和するだけでなく、防御メカニズムの継続的改善の方向性を決めることができ、将来の脅威に向けてしっかり準備することができます。

レシピのメンテナンスと更新

強力なレイヤー 7 DDoS 防御を維持するためには、最新の傾向とテクニックを常に監視する必要があります。

攻撃者は常に、新しいツールと脆弱性を利用して攻撃パターンを組み合わせて仕掛けてきます。こうした脅威にプロアクティブに対処するためには、防御策の調査、監視、評価、保護の自動化、脅威インテリジェンスコミュニティとの連携に時間と労力を費やす必要があります。

まずは、主要なサイバーセキュリティフォーラムをモニタリングすることから始めるとよいでしょう。Akamai では、より規範的なアプローチを推奨しています。

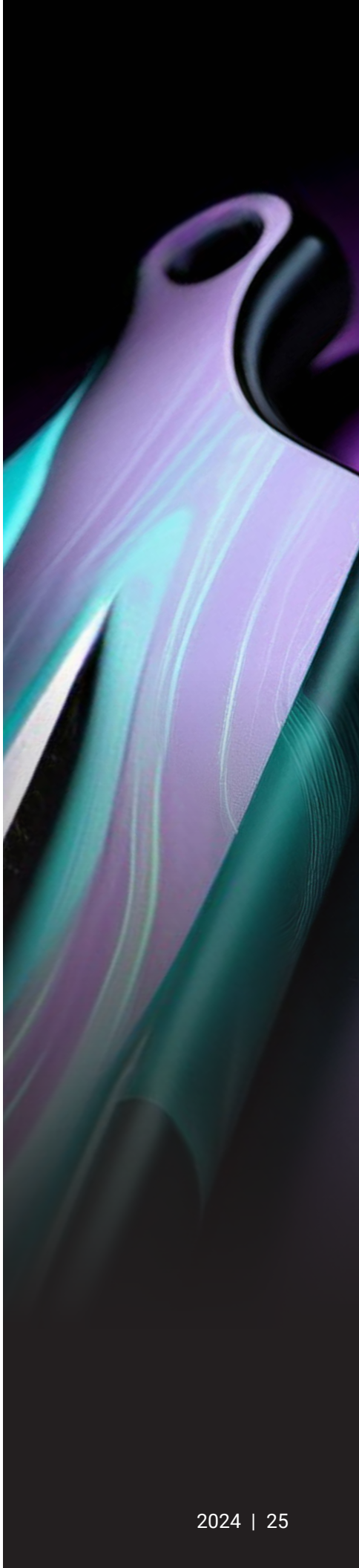
継続的に監視と評価を行う — ネットワークとアプリケーションのパフォーマンスを定期的に監視して、新たな脅威を示す新しいパターンや異常を検知します。このデータを使用して、既存の防御メカニズムの有効性を評価し、改善または調整の領域を特定します。

DDoS 対策チームを設立する — 組織内の担当者または担当チームを決め、その担当者が DDoS 攻撃の状況を調査、監視し、少なくとも四半期ごとに重要な調査結果と推奨事項を報告します。

脅威インテリジェンスコミュニティに参加する — 攻撃者は、最新かつ最も効果的な手法について攻撃者同士で情報を共有しています。防御する側も他の企業や業界の人と最善の防御策について情報を交換してしかるべきです。脅威インテリジェンスについて常に最新の情報を入手するようにしてください。セキュリティフィードの購読、サイバーセキュリティフォーラムへの参加、業界の担当者との連携を検討します。こうした情報は、新しい攻撃ベクトルを予測し、それに応じて防御を調整するのに役立ちます。

サイバーセキュリティベンダーを頼る — テクノロジーベンダーは、専用の脅威調査グループを持っていることが多く、コンテンツ・デリバリー・ネットワークを持つ企業は他では得られない知見を提供できます。いつでも、どこでも、こうした学習機会を活用してください。また、セキュリティコンサルティングの専門家を定期的に迎えることも賢明な対策です。

自社の防御策をテストする — 準備を怠ることは失敗するための準備をするようなものです。「練習を重ねることで完璧に」という決まり文句も同じことを意味しています。定期的なテストや演習を実施することで成果が得られます。



定期的にレビューと攻撃シナリオのシミュレーション（レッドチーム演習）を実施して、防御戦略の回復力をテストしてください。これらの演習では、現在の体制の弱点が明らかになり、攻撃者がシステムを悪用する方法について情報を得ることができます。

ネットワークのテストは、少なくとも年に 1 回実施してください。最近の攻撃プロファイル、特に同じ業界の企業で発生したものは、テストケースの良い材料になります。

教訓をコミュニティと共有する — 繰り返し伝えることが大切です。攻撃者がツールや戦術を共有するのと同様に、組織は効果的な防御戦略について積極的に知識を共有する必要があります。

成功と失敗の両方を文書化することで、サイバーセキュリティ担当者は、実例に基づく知見を提供し、ナレッジベース全体を充実させることができます。業界フォーラムに参加し、新しい担当者に助言を与え、共同プロジェクトに参加することは、堅牢な防御エコシステムの形成に不可欠です。このような取り組みは、より効果的な戦略やツールの開発に貢献するだけでなく、さまざまな経験や知見を集め、攻撃者の変化する戦術に適応していくのに役立ちます。こうした連携の精神は、サイバーセキュリティの世界で一歩先を行くために不可欠であり、それぞれの貢献がより強力で回復力に優れたデジタル世界の構築には重要です。

重要ポイント

DDoS の脅威の状況は変化しており、攻撃者は常に防御を回避する新たな方法を模索しています。レイヤー 7 DDoS 防御戦略の維持と更新は、警戒と適応、そして事前対応型のアプローチを必要とする継続的なプロセスです。常に最新情報を入手し、定期的なテストとレビューを行い、継続的な改善の文化を促進することで、現在および将来の脅威に対する強固な防御策を維持できます。

結論

レイヤー 7 DDoS 攻撃は高度化が進んでおり、自動化の発展と攻撃者同士の連携もあり、これまで以上に容易に仕掛けることができます。一方、組織は、失敗コストが増加しても、より大規模で複雑な環境を防御する必要があります。

確かに、防御のレシピを作るのは簡単な作業ではありません。レイヤー 7 DDoS 攻撃に対する万能の防御策というものはありません。ここまで説明したように、複数の検知戦略と緩和戦略を組み合わせた多面的なアプローチが最も堅牢な防御策です。

さらに、保護対象のアプリケーションやサービスの特定のニーズ、トラフィックパターン、リスクプロファイルに応じて手法を選択する必要があります。ビジネス、トラフィック、脆弱性を理解せずに防御を構築することはできません。これらの戦略を定期的に更新し調整することは、進化する DDoS 脅威に適応するために不可欠です。

最後に、攻撃が終了してもあなたの仕事は終わっていません。攻撃後の分析と調整は、継続的な成功に必須であり、知識の共有とキャリアの開発にも大きく貢献します。

幸い、Akamai にはあらゆる段階で支援を提供できる体制が整っています。多くの企業が、アプリケーションと API の保護から、グローバルトラフィックに関する他社にはない知見、攻撃後の専門的な分析まで、レイヤー 7 DDoS 防御に必要なすべての要素を 1 社のプロバイダーから調達しています。

Akamai のレイヤー 7 DDoS 防御について詳細をご確認ください。
App & API Protector の無料トライアルをぜひお試しください。

クレジット

共同執筆者

Aseem Ahmed
Barney Beal

校閲およびテーマ別寄稿者

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

マーケティング・出版

Georgina Morales Hampe
Shivangi Sahu

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 10 月。