ホワイトペーパー

DDoS 攻撃の急速な進化と脅威の拡大

攻撃が標的化し、より巧妙になり、頻発する中、すべての企業は常に警戒を怠らずにいる必要があります。

分散型サービス妨害（DDoS）攻撃をかいくぐれる企業はもはやありません。脅迫、ハクティビズム、復讐などを目的としたサイバー犯罪者は、大規模かつ巧妙な攻撃であらゆる組織を簡単に標的にすることができます。このため、デジタル指向のすべての企業で、DDoS 攻撃に対する包括的な防御が必要です。

インターネット初期の攻撃手法の 1 つ

1999 年 7 月 22 日、ミネソタ大学の 1 台のコンピュータが、114 台の感染したコンピュータによって過剰なデータパケットを送られ続け、2 日間にわたり機能を停止しました。

これは、MIT テクノロジーレビューによると、初めて記録された DDoS 攻撃でした。

その後数週間から数か月の間に、CNN や Amazon などの大手企業が被害を受けました。これは、これらの攻撃がいかに簡単に実行できるかをハクティビストや他のサイバー犯罪者が知ったためです。必要なのは数行のコードだけでした。

DDoS は、オンラインビジネスを展開するあらゆる企業にとって脅威となりました。

攻撃の規模と巧妙さが増す

1999 年以来、DDoS 防御は大きく進歩してきました。しかし、犯罪者も同様です。今日の DDoS 攻撃者は、利用できる数十種類の攻撃ベクトルと安価な攻撃ツールキットを持っており、さらにインターネット上の無数の脆弱なデバイスを利用してキャンペーンを拡大しています。2016 年、攻撃者は侵害されたセキュリティカメラ DVR を使用して、インターネットの大部分をダウンさせました。

それ以来、何億台もの無防備な IoT デバイスがオンラインになっています。そして来るべき 5G 革命では、さらに数億台のデバイスが加わることが予想されます。5G の速度、キャパシティ、レイテンシーが飛躍的に向上することで、攻撃の強度と規模が拡大することは想像に難くありません。

また、犯罪者が増幅やリフレクション攻撃のために乗っ取ることができる、インターネット上の無防備で保守されていないサーバーの数も飛躍的に増加しています。これらのサーバーの多くは、犯罪者がその IP を知っているため、なりすまし要求を 50,000 倍以上に増やすことができます。

緊急時には 24 時間 365 日体制で DDoS の緩和と防御に対応いたします

DDoS 攻撃の脅威にさらされている Akamai の既存のお客様は、Akamai Security Operations Command Center（SOCC）にご連絡ください。

Akamai のお客様以外で緊急の防御が必要な場合は、**DDoS ホットラインページ**でフォームを送信するか、**+1-877-425-2624** にお電話ください。すぐにサポートを受けられます。

DDoS 攻撃から逃れられる業界はない

現在、Akamai は毎年数千件の DDoS 攻撃を緩和しています。

一部には、動機が明らかなものもあります。ゲーマーが DDoS 攻撃を利用してネットワーク速度を低下させ、ライバルのプレイヤーに対して優位に立つことがあります。大学生たちが、標的型 DDoS 攻撃を利用して ISP の顧客に不満を与え、ビジネスを競合他社に誘導したこともあります。

しかし、動機がより複雑で分かりにくいものである場合もあります。犯罪者が DDoS 攻撃を利用して、組織の一部でインシデント対応チームの注意をそらす一方で、別の部分に目立たない攻撃を試みることがありました。

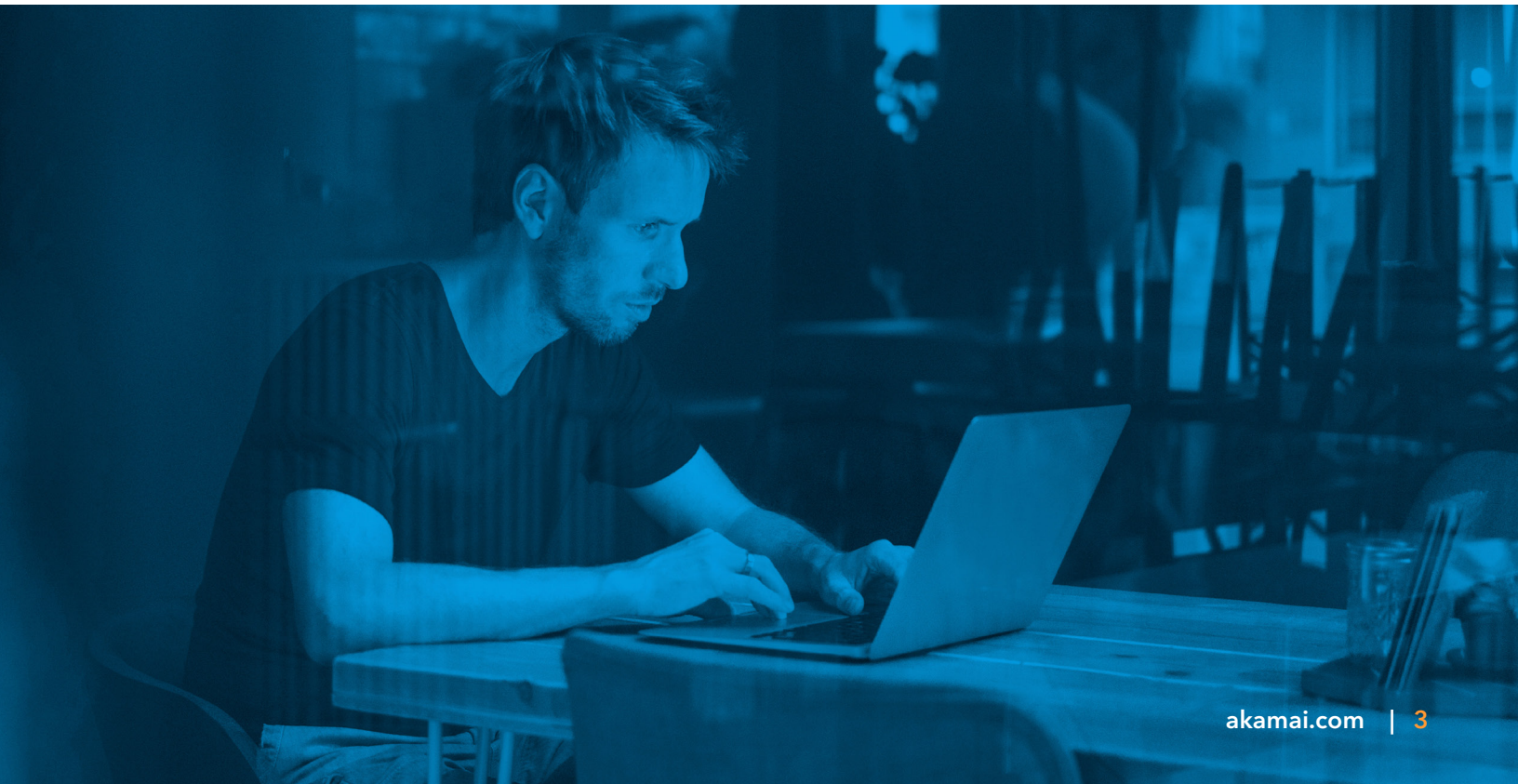
スキルを持たない攻撃者の場合、ダークウェブ上には「DDoS 請負」ビジネスが存在します。料金は 5 分間の攻撃で 5 ドルから始まり、24 時間では 400 ドルまで上昇します。不満を持つ誰かが、200 ドルや 300 ドルを支払い、企業に何百万もの損害を与えることができるのです。

2020 年はより大規模で高度な攻撃が登場

2020 年上半期に、Akamai は毎秒 1.44 テラビット（Tbps）および毎秒 8 億 900 万パケット（Mpps）の大規模な攻撃を阻止しました。これは、観測史上最大の Mpps 攻撃でした。

これらの攻撃は 1 秒未満で緩和されましたが、100 Gbps 以上の攻撃は増える傾向にあります。多くの攻撃は、複数のベクトルの独自かつ複雑な組み合わせを使用します。これらの攻撃は、防御を過負荷にしたり回避したりして、インシデント対応リソースを消費することを目的としています。

また、自動化された対応だけでなく、少なくとも一部人間による緩和を必要とする攻撃も増加しています。



史上最大規模の DDoS 脅迫キャンペーンに突入

2020 年 8 月、Akamai の Security Intelligence Research Team は、さまざまな業界の企業が DDoS 脅迫のメールを受け取っているという警告を発しました。攻撃者は業務を停止させると脅し、ビットコインで身代金を支払わなければ、企業は大規模なダウンタイムと多額の金銭的損失を被ることになるとほのめかしました。

そのわずか数週間後、FBI は世界中の数千もの組織が同様の脅迫メールを受け取っていると報告しています。攻撃者は群を成してある業界の企業を脅迫した後、別の業界に軸足を移し、さらに別の業界へと脅迫を続けます。高度に組織化された攻撃者は、戻ってきて以前のターゲットを脅迫することがよくあります。

防御力を高めれば、攻撃される可能性は低くなる

サイバー犯罪者は他の犯罪者と同じです。彼らは弱点を探すために「下見」を行います。DDoS の場合、標的となる被害者の DNS、Web アプリケーション、インターネットに面したデータセンター資産を調べます。

この偵察行為で脆弱なリソース、サイト、またはサービスが発見された場合、サイバー犯罪者が侵入する可能性があります。一方、防御が強固であることが判明した場合、多くが次に移ります。

実際、Prolexic プラットフォームへのルーティングを導入する前に攻撃を受け、Prolexic に緊急対応を求めた新規顧客の大半は、Prolexic の防御が導入された後、再び攻撃を受けることはありませんでした。サイバー犯罪者にとって、特に他のたやすい標的が存在する場合、Prolexic で防御された標的に時間をかける価値はないでしょう。

全体的な DDoS 防御の仕組み

Akamai は、175 Tbps を超える総ネットワークキャパシティを持ち、透明の網目のような専用エッジ、分散型 DNS、クラウドスクラビング緩和ソリューションを通じて多層型の DDoS 防御を提供します。これらの専用クラウドは、DDoS セキュリティの態勢を強化すると同時に、アタックサーフェスを縮小するように設計されています。このエンドツーエンドの DDoS 防御は、緩和の品質を向上させ、フォールス・ポジティブ（誤検知）を減らしながら、最も複雑な最大規模の攻撃への耐障害性を高めるように設計されています。

さらに、それらのソリューションは、Web アプリケーションやインターネットベースサービスの特定の要件に合わせてきめ細かく調整できます。

エッジ防御

Akamai は、グローバルに分散されたインテリジェント Edge プラットフォームをリバースプロキシとして設計し、ポート 80 および 443 上のトラフィックだけを受け付けるようにしています。ネットワークレイヤーへの DDoS 攻撃はすべて、エッジで即座に阻止されます（0 秒 SLA）。

API 経由で実行される攻撃などアプリケーションレイヤーでのイベントは、Kona Site Defender が攻撃を阻止しながら、正規ユーザーにアクセス権を付与します。

DNS 防御

Akamai の権威 DNS サービスである Edge DNS も、トラフィックをエッジでフィルタリングします。Akamai Edge DNS は、他の DNS ソリューションとは異なり、DDoS 攻撃に対抗する可用性と耐障害性を重視した設計となっています。Edge DNS は、ネームサーバー、Point of Presence、ネットワーク、およびセグメント化された IP Anycast クラウドなど、アーキテクチャの冗長性も多層的に備え、優れたパフォーマンスを実現します。

クラウドスクラビング防御

Prolexic は、全世界 20 か所のスクラビングセンターと 8.2 Tbps の専用 DDoS 防御により、すべてのポートとプロトコルにわたり、データセンターとハイブリッドインフラ全体を DDoS 攻撃から保護します。このキャパシティは、あらゆる情報セキュリティプログラムの土台となるインターネットに面したアセットの可用性を維持するように設計されています。

完全なマネージドサービスである Prolexic は、ポジティブとネガティブの両方のセキュリティモデルを構築できます。このサービスは、自動防御機能と Akamai のグローバルな SOCC ネットワークによるエキスパート対応を組み合わせたものです。さらに、Prolexic は事前対応型防御による**業界トップクラスの** 0 秒緩和 SLA を提供します。

Prolexic が記録的な攻撃を阻止した方法

2020 年 6 月の 809 Mpps 攻撃は、インターネットで観測史上最大のパケット／秒（PPS）攻撃でした。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しようとする一般的なビット／秒攻撃とは異なり、PPS 攻撃はデータセンターやクラウドのネットワーク機器を疲弊させることを目的としています。

この手強い攻撃には、膨大な数のソース IP アドレスが関係していました。そのうち 96% 以上は、これまでの攻撃で観測されたことのないものでした。またこの攻撃は、わずか 2 分で 418 Gbps から 809 Mpps まで増大しました。

幸いにも、標的となった組織は Prolexic のお客様であり、0 秒 SLA のサポート対象となっていました。Akamai SOCC は、このお客様と協力して平時のトラフィック・ベースライン・プロファイルを把握し、DDoS 攻撃を即座に阻止するための制御とセキュリティポリシーを導入しました。

カスタム脅威ブリーフィングに今すぐお申し込みください

お申し込みはこちら：**akamai.com/ddos-briefing**