MEMCACHED リフレクション攻撃：
DDoS 攻撃は新たな時代へ

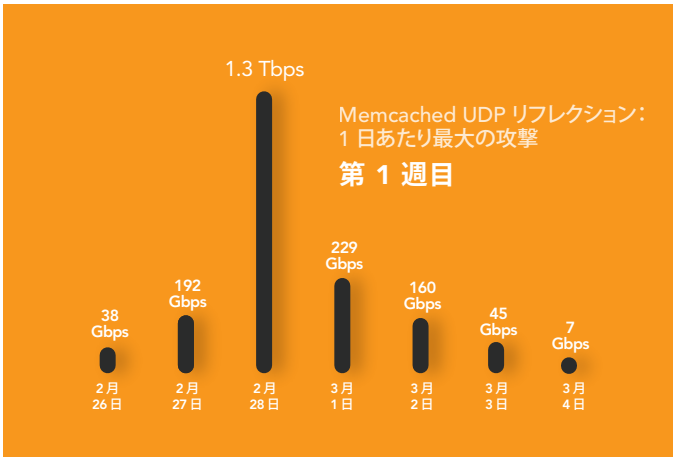
2018 年初頭、攻撃者が新しく大規模な DDoS リフレクションと、攻撃リソースを 50 万倍にする可能性がある増幅方法を発見、採用してから、DDoS 攻撃の規模が 2 倍になりました。この攻撃ベクトルは、Memcached UDP リフレクションと呼ばれ、マルウェアやボットネットを必要とせず、インターネットに公開されているリソースを使用します。

2018 年 2 月 28 日、Akamai のお客様をターゲットにした、1 秒間に 1.3 テラバイト（Tbps）という過去最大規模の DDoS 攻撃が記録されました。この攻撃に使用されていたのは、Memcached リフレクション DDoS トラフィックでした。この攻撃は、それまで最も規模が大きかった、Mirai Internet of Things（IoT）ボットネットを利用した DDoS 攻撃の 2 倍の規模でした。

Akamai の Prolexic DDoS 防御サービスは、お客様のネットワークトラフィックを受信すると即座に、オープンソースのデータ・キャッシュ・ツールである Memcached が使用するデフォルトポートを発信元にしたすべてのトラフィックを除去して、大規模な DDoS 攻撃を緩和しました。お客様のネットワークには、ヨーロッパ、米国、アジアにある Akamai の DDoS スクラビングセンターからクリーンなトラフィックが返され、これ以降、お客様の業務に影響を与えることはありませんでした。

ディスクやデータベースからのクエリに対する応答時間を短縮するために広く使われている Memcached は、攻撃者が DDoS リフレクション技法を使ったために、インターネットの武器に変えられてしまいました。Memcached リフレクションが使用された最初の DDoS 攻撃は、この大規模攻撃のわずか 2 日前に観察されたばかりでした。1.3 Tbps の攻撃が発生したとき、Akamai はすでにお客様をターゲットにした Memcached 攻撃に対する防御策として、自動化された緩和機能を配置済みでした。

この攻撃が始まった最初の 1 週間に、さまざまな業種の Akamai のお客様をターゲットとして 19 箇所で Memcached リフレクション DDoS 攻撃が発生しました。



恐るべき 50 万倍の増幅とパケットレート

Memcached リフレクションの増幅係数は桁外れです。210 バイトのリクエストをトリガーとして、ターゲットに 100 MB の応答を送信できます。Memcached データは、その用途の性質として高速で配信されます。この攻撃が発生している間に Akamai が測定した速度は、127 Mpps（1 億 2,700 万パケット／秒）でした。

保護されていないインターネットサーバー上では、デフォルトで UDP 通信プロトコルが有効になっています。Memcached は、たとえそれがスプーフィング（偽装）された IP アドレスからであっても、相手を制限せずに要求されたデータを配信します。1.3 Tbps の攻撃には、1,000 以上の ASN 上にある何万台ものサーバーが参加し、各サーバーが平均で 1 Gbps 近い攻撃トラフィックを送信していました。研究者は、インターネット上に 9 万台以上の Memcached サーバーが存在し、現在そのうちの 5 万台以上がリフレクターとして悪用される脆弱性があると推測しています。

予想される Memcached DDoS 攻撃と Ransom DDoS 攻撃の増加

セキュリティコミュニティは、現在も他のリフレクション DDoS ベクトルが多く使用されているとしていますが、脆弱性のあるサーバーへのパッチ適用、再構成、排除などをリモートシステムの管理者に求めても、直ちに効果が得られる可能性は低いとしています。今後は、Memcached DDoS 攻撃の発生が予想されます。

Memcached などのリフレクション DDoS 攻撃では、攻撃者がボットネット内のボットを感染させて制御するためのマルウェアを必要としません。攻撃者があまり高度なスキルを持っていなくても、攻撃を開始できます。Akamai は、脆弱性のある Memcached サーバーを特定するためのスキャンが増加していることを確認しています。これまでより多くの攻撃者が、より多くの Memcached サーバーを悪用して、さまざまな規模の DDoS 攻撃を引き起こすでしょう。さらに、Memcached のペイロードは、脅迫メッセージの送信にも使用されています。Akamai は、どのような脅迫に対しても、支払いに応じないことを推奨します。

DDoS 攻撃によって圧迫されるローカル・ネットワーク・パイプ

Akamai のように周到に準備されたクラウドベースの DDoS 緩和策を持ち、コンテンツ・デリバリー・ネットワーク（CDN）を提供するプロバイダーや最大規模の ISP は別として、これまでよりはるかに規模が大きい DDoS 攻撃にさらされても業務を維持できるほどのネットワーク容量を持つ組織は少数です。データセンターやエッジのルーティングデバイスに入るネットワークパイプが最初に圧迫されるため、オンサイトでの DDoS 緩和処理が妨げられます。

DDoS 緩和計画の重要性

この記録的な DDoS 攻撃を受けた Akamai のお客様は、称賛に値するほど準備が整っていたため、Akamai にトラフィックをルーティングして緩和するまでの停止時間は 10 分未満でした。このお客様は、事前に Prolexic DDoS 防御サービスを契約し、DDoS ランブックを作成して実践していたため、担当者は攻撃発生時に何をすればよいか、誰に連絡すればよいかを的確に判断できました。ネットワークトラフィックを監視していた担当者は、異常を特定すると、わずか 5 分以内にすべてのネットワークトラフィックを Akamai にルーティングしたのです。

Akamai を選ぶ理由：DDoS に対する耐障害性を重視した設計

Akamai は、CDN、Prolexic ネットワーク、分散型の Fast DNS インフラストラクチャによってお客様を DDoS 攻撃から保護します。これらのプラットフォームの DDoS 攻撃に対する耐障害性を強化し続けるために、投資を行っています。

最上位レベルでは、容量プランニングモデルにより、検証可能な最大規模の DDoS 攻撃に対応します。また攻撃規模が拡大しても、拡張可能な要素によってトラフィックを増大させて、十分なヘッドルームを確保します。その結果、この攻撃のように最も規模が大きく高度なスキルを用いた DDoS 攻撃の規模が 2 倍になったとしても、適切に緩和できます。

Akamai の Adversarial Resilience（敵対的耐障害性専門）チームは、新たな脅威やインシデントを継続的に評価し、Akamai のシステムが破られる可能性がある箇所を特定し、エンジニアリングチームと協力して自動緩和機能を実装し、あらゆる領域で耐障害性を高めています。

DDoS に対するコンテンツ・デリバリー・ネットワークの耐障害性

注目すべき点は容量だけではありません。Akamai は DDoS 攻撃だけでなく、さまざまな悪条件に備えて可用性と回復力を発揮するように CDN を構築しています。世界全体で

サーバーを 22 万台以上設置している Akamai CDN は、個々のサーバーのステータスを調節し、自動的に停止したサーバーやネットワークの輻輳を回避して、ユーザートラフィックをルーティングします。各サーバーには、レート制御、ブラックリスト、地理的ブロッキングなどを含めた DDoS 防御対策が施されています。

Prolexic ネットワークの DDoS に対する耐障害性

Prolexic ネットワークは、世界で最も強力な DDoS スクラビングサービスの 1 つです。7 か所のグローバル・スクラビング・センターと 3.5 Tbps 以上の容量を擁し、150 人のセキュリティ専門家チームが、毎月数千件以上の DDoS 攻撃からお客様を保護しています。各スクラビングセンターは、複数の事業者用 Tier 1 接続、500 を超えるピアを擁するパブリックピアリング、OSI スタックの複数の層における高性能なトラフィック分析機能とアクティブな緩和機能を備えています。DDoS 防御のキャパシティも継続的に増やしています。

Fast DNS インフラストラクチャの DDoS に対する耐障害性

Akamai は、権威 DNS サービスである Fast DNS を運用することによって、可用性、速度、DDoS に対する耐障害性を確保しています。また、お客様に割り当てるネームサーバーを 20 個以上のセグメントに分割された DNS クラウドに分散することで、Akamai のお客様が攻撃された際に、他に及ぶ影響を最小限に抑えられるようにしました。ネームサーバーのクラスタや、その他の制御機能は、局地的な DDoS 攻撃を最小限に抑えます。

最後に

Akamai は 20 年近くにわたって DDoS 攻撃を防御し、その時点で最大規模の DDoS 攻撃からお客様を守り、インフラストラクチャの可用性を維持してきました。Akamai は、これからも新しい脅威を調査、報告し、常にこれらの悪意に先手を打つために、手順やプラットフォームを強化し続けます。当社は、学んだことを生かしてすべてのお客様を守ることによって、さらに保護を強化します。Akamai は業界で最も堅牢なプラットフォームをお客様に提供することに取り組んでいます。

DDoS 攻撃に対する耐障害性の評価

Akamai による、インフラストラクチャの耐障害性の評価をご希望の場合は、**Professional Services 部門**までお問い合わせください。セキュリティアーキテクトによるコンサルティングをご案内します。

詳細については、**https://www.akamai.com/memcached** をご覧ください。

Akamai