2024 年 8 月 27 日

【報道関係各位】

本リリースは 2024 年 8 月 14 日に本社 G-Core Labs S.A により発表されたリリースの抄訳です。

Gcore Radar レポート―2024 年上半期で前年同期比 DDoS 攻撃数 46%増

脅威の高まりに伴いピーク時攻撃力の値も更新

ルクセンブルク：2024 年 8 月 14 日 ― AI、クラウド、ネットワーク、セキュリティのグローバルエッジソリューションプロバイダ Gcore は、本日 Gcore Radar レポート 2024 年第 1 四半期・第 2 四半期― DDoS アタックトレンドを発表しました。DDoS 攻撃数は前年同期比 46%増、秒当たりテラビットの攻撃力が観測されました。1 年前に観測された攻撃力の増大がその単位を 2023 年下半期にはギガビットからテラビットに変遷しましたが、この増大傾向は 2024 年上半期においても依然継続しています。

2024 年第 1 四半期・第 2 四半期の動向ハイライト

- 攻撃数：83 万件、2023 年上半期より 46 ポイント増
- ピーク時攻撃力：1.7Tbps、2023 年下半期の 1.6Tbps より上昇
- 攻撃ベクタ：UDP フラッド 61%、TCP フラッド 18%、 SYN フラッド 11%
- 攻撃対象上位 4 業界と分布：ゲーミング 49%、テクノロジ 15%、金融サービス 12%、通信業 10%
- 攻撃対象業界動向の変動：E コマース 7%とメディア＆エンタテインメント 5%、2023 年下半期ではその他カテゴリに計上されていたが、今回の調査で個別計上に。

Gcore Radar は半年毎に刊行されるレポートで、Gcore ネットワーク上の DDoS 攻撃の状況を俯瞰で可視化しています。2024 年第 1 四半期・第 2 四半期の結果では、攻撃数と攻撃力とも増加を示しており、攻撃力については 2023 年下半期より 0.1Tbps の増加にとどまるものの、企業組織にとってはこの増加は大きな脅威です。

攻撃対象業界：テクノロジ業界が標的対象としてクローズアップ

2024 年上半期でも依然最多攻撃対象となったのは、ゲーミング業界で 2023 年下半期から 3 ポイント増でした。調査から浮上したケースとして、ゲーマーやゲームグループが敵対者への優位性を得る目的で DDoS 攻撃が誘発されたというものがありました。一方、前の半年間と比較した場合の最大の変化はテクノロジ業界への攻撃数が増加したことで、比率は 2 倍以上の 15%に上昇しました。クリティカルなインフラストラクチャをホストする企業のビジネスを破壊することを目的としているアクタにとって有益度が高まっているセクタと言えます。

2024 年上半期のネットワークレイヤ攻撃で大きな影響が及ぼされた上位 3 業界の対比分布は、ゲーミング 51%、テクノロジ 34%、通信 15%でした。アプリケーションレイヤ攻撃での上位 3 業界の対比分布は、破壊およびダウンタイムへの寛容度の低さと財政面での見返りが大きいとされる金融サービス 41%、E コマース 28%、メディア＆エンタテインメント 13%でした。

Gcore Head of Security　Andrey Slastenov　コメント

2024 年上半期での攻撃力の上昇が 0.1Tbps にとどまったとは言え、たかだか 300Gps の攻撃であったとしても数秒で未保護状態のサーバをオフラインにしてしまえることを考えると、予断を許さない状況と言えます。テラビット単位の攻撃の威力は計り知れないものです。攻撃力の高まりが小さくとどまったとしても、攻撃からの影響は甚大な結果に帰着しかねません。

攻撃の実行頻度の上昇は懸念材料であり、対象業界はなぜ標的とされるのかを探った上で対策を講じる必要があります。ゲーミング業界では競合間での攻撃が実行されるケースがあります。また一方で、DDoS 攻撃でゲーミングサービスをオフラインにしてしまうことでゲーミング業界のマネタイズ機構に影響を及ぼすよう仕向けているケースもあります。テクノロジ企業がサービス提供において、サーバ、ネットワークやストレージサービスの可用性が妨害を受けるケースがありますが、これも同様にマネタイズ機構への影響を企図した攻撃と言えます。

DDoS 攻撃の発生源・拠点

アプリケーションレイヤでの攻撃発生源の国の特定は攻撃者の IP アドレスを使用します。ネットワークレイヤでの特定には攻撃パケットを受信したデータセンタ拠点を洗い出す手法を採用しています。

2024 年第 1 四半期・第 2 四半期のネットワークレイヤ攻撃の最多発信源は米国、次いでドイツ、オランダ、シンガポールが続く結果になりました。アプリケーションレイヤ攻撃では、オランダ、米国、ブラジル、ポーランドが上位を占めました。これらレイヤ間で共通する発生源が検出されました。

DDoS 攻撃ベクタ

L3～L4 レイヤでの主流は UDP フラッド 61%、TCP 18%と SYN 11%と続き、L7 攻撃での最主流手法は HTTP フラッド 58%でした。

短時間かつ強大攻撃が継続

最長持続時間は 16 時間でしたが、平均的には攻撃時間は短く、ほとんどの攻撃は 10 分間以内でした。短時間攻撃ではあっても、ユーザがサービスからの離脱を余儀なくされる事態を招き、サービスプロバイダのブランド評価に深刻な影響及ぼす強大な攻撃であると言えます。

Gcore Head of Security　Andrey Slastenov　コメント

継続時間他の傾向や動向に見られる変動性は、攻撃者が攻撃効果の最大化を目的に、戦術の洗練を図っていること、手法のカスタマイズを行なっていることを意味しています。攻撃は全く鈍化しておらず、その脅威は進化を止めていないという事実、また、破壊・ダウンタイム・収益損失を回避するためには DDoS 攻撃の検知、緩和、攻撃からの保護が最優先課題とされるべきであるという指針を Gcore Radar レポートで提示しています。

※完全レポートへのアクセスは http://gcore.com/library/wp-security-gcore-radar-q1-2-2024
　または、添付ファイルをダウンロードしてください。

Gcore について ～ Gcore は 2024 年 2 月に 10 周年を迎えました（参考英文記事；Blog, Linkedin Post）。
Gcore はエッジ AI、クラウド、ネットワーク、セキュリティのグローバルソリューションプロバイダです。本社はルクセンブルク、600 超の従業員と世界各地に 10 の営業拠点を擁しています。Gcore の IT インフラストラクチャは自社運用、拠点は 6 大陸にまたがり、グローバル平均レスポンスタイムは 30ms、ヨーロッパ、アフリカ、LATAM における屈指のネットワークパフォーマンスを実現しています。ネットワークは Tier IV と Tier III のデータセンタに配備された世界各地の 180 超の PoP で構成され、200 超 Tbps の帯域を誇ります。
Web サイト
https://gcore.com/
ソーシャルメディア
https://www.linkedin.com/company/g-core/
https://www.youtube.com/@GCoreOfficial
https://www.facebook.com/officialgcore
https://x.com/gcore_official
https://www.instagram.com/gcore.official/

同件に関するお問い合わせ先

Gcore Japan 株式会社

Marketing Manager：白石

tel:03-4567-2817/email: Japan-marketing@gcore.com

共同ピーアール株式会社

担当：栗木、峰松

email: Gcore-pr@kyodo-pr.co.jp