Arbor Networks 第 10 版年次ワールドワイド・インフラストラクチャ・セキュリティ・レポート

概要

このレポートには、第 10 版となる Arbor Networks の年次ワールドワイド・インフラストラクチャ・セキュリティ・レポート（WISR）の結果が記載されています。この報告書は、運用に関するセキュリティ・コミュニティの 2014 年における総合的な経験、所見、および懸念事項を文書化することを目的としています。

過去 10 年間にわたり、Arbor Networks は毎年 WISR を作成して、サービス・プロバイダと企業の両面で脅威と懸念事項について詳細な情報を収集するとともに、収集したデータを整理して、すべてのネットワーク事業者が利用できる一般的なリソースとして提供してきました。この年次レポートは、組織が直面する主な脅威と懸念事項、およびそれをミティゲートするための戦略について主な傾向を報告します。

WISR は調査の開始から今日まで、日々の運用上のセキュリティに直接関与している回答者からのアンケート調査によって収集したデータに基づいて作成されてきました。過去 10 年間で WISR の対象範囲は大幅に変化しましたが、中核の目標は、一貫して、運用コミュニティの視点から見たインフラストラクチャ・セキュリティの実態を明らかにすることにあります。

調査結果の概要

1. Arbor Networks がこの調査を続けてきた 10 年間に、DDoS 攻撃の規模が爆発的に増大しました。最大の攻撃規模は、10 年前の 8Gbps から現在では 400Gbps にまで拡大しています。これは 50 倍の拡大であり、年間増加率は複利計算で 54%に上ります。
2. DDoS 攻撃はもはや、単なる迷惑行為ではありません。今日、それはビジネスの継続性と最終利益に対する重大な脅威となっています。DDoS 攻撃によるインターネット帯域幅の枯渇を観測したデータセンター事業者は、全体の 3 分の 1 以上に上り、44%が DDoS 攻撃による収益の損失を報告しています。
3. 回答者の 90%がアプリケーション・レイヤ攻撃を経験しています。また、ファイアーウォールや IPS デバイスなどの既存のインフラストラクチャが、引き続きこれらの攻撃のターゲットとなっており、回答者の 3 分の 1 以上が、DDoS 攻撃によってファイアーウォールや IPS デバイスが機能停止したことを報告しています。
4. DDoS 攻撃と高度な脅威はいずれも、頻度と複雑性が拡大しており、セキュリティ組織の検知およびインシデント対応能力上の課題となっています。
5. 人的要素は、引き続き防御能力を左右する 1 つの要因です。セキュリティ組織に熟練の人材を雇用し、定着させることが困難であると答えた回答者は、前年比 14%増の 59%となりました。

サービス・プロバイダに対する脅威および攻撃

- 顧客に対する DDoS 攻撃は、今回もサービス・プロバイダにとっての運用上の最大の脅威となっていますが、インフラストラクチャに対する攻撃を脅威として挙げる回答者が引き続き急増しています。

- DDoS 攻撃の被害は、エンドユーザー／加入者と E コマースに対するものが最も多く、3 番目が政府機関です。

- 攻撃者は、引き続きリフレクション/増幅の手法を使用して大規模攻撃を仕掛けています。報告された最大の攻撃は 400Gbps で、そのほかの回答者から 300Gbps、200Gbps、170Gbps の攻撃が報告されています。そのほかに 6 人の回答者が 100Gbps のしきい値を超える攻撃を報告しています。

- 3 分の 2 近くの攻撃がボリューム型ですが、ほとんどすべての回答者（90%）がアプリケーション・レイヤ攻撃を報告しており、42%が 1 つの攻撃にアプリケーション型とステートを枯渇させる攻撃の両方を含むマルチベクトル型攻撃を観測しています。

- 今年は、高頻度の攻撃を報告する回答者が増加しました。1 ヵ月に 22 回以上の攻撃を受けた回答者は、昨年度は 4 分の 1 をやや上回る程度でしたが、本年度は 38 パーセントに増加しています。

- 暗号化された Web サービス（HTTPS）をターゲットとするアプリケーション・レイヤ攻撃を受けた回答者の割合は、（意外なことに）昨年度の 54%から 42%に減少しました（それでも 2012 年の 37%を上回っています）。

- 攻撃の動機の上位 3 つは、ニヒリズム／破壊行為、オンラインゲーム、イデオロギー的ハクティビズムであり、これらはすべて過去数年間、上位 3 位までを占めてきた動機です。今回、ゲームを動機とする攻撃の割合が増加しましたが、本年度、注目を集めたゲーム・サイトに対する攻撃キャンペーンの数を考えれば不思議ではありません。

- 半数以上の回答者が、自身の企業ネットワークでセキュリティ・インシデントが増加したと答えています。しかしながら、回答者の半数が、セキュリティ・インシデントに対して「何らかの」対策を講じているが改善が必要だと答えており、さらに 8%がまったく準備されていないとしています。

企業、政府機関、教育機関に対する脅威および攻撃

- エンタープライズ・ネットワークで最も多くみられる脅威は、DDoS 攻撃、偶発的なデータ損失、およびボットや他の手段によるホストの侵害で、これら 3 つで全回答者の 3 分の 1 を占めます。

- 回答者の 50%近くが調査期間中に DDoS 攻撃を観測し、そのうちの 40%近くでインターネット接続が飽和状態になりました。

- 3 分の 1 以上の組織で、DDoS 攻撃の間にファイアーウォールや IPS デバイスが機能停止したか、機能停止の一因となりました。

- DDoS 攻撃のビジネスへの影響として、運用コスト、評判に対する損害、および顧客の減少が上位 3 つを占めています。

- 感染／データ漏洩の隠蔽工作が、攻撃の動機の第 3 位でした。

- 3 分の 2 がクラウド・サービスへの攻撃を観測しており、サービス・プロバイダによる観測の割合を上回っています。

- 3 分の 1 強が、本年度はセキュリティ・インシデントが増加したと答え、約半数が昨年度と同様のレベルだと回答しています。セキュリティ・インシデントへの対策がかなりまたは十分整っていると感じている回答者は全体の半数弱であり、対策を全く行っていないという回答が 10%見られました。

データセンター

- 3 分の 1 以上のデータセンター事業者が、DDoS 攻撃によるインターネット帯域幅の枯渇を観測しています。

- データセンター事業者にとっての DDoS 攻撃のコストとして、運用コストが群を抜いて第 1 位にランクされています。DDoS 攻撃による収益の損失も大幅に増加しています（データセンター事業者の 44%が、DDoS 攻撃による収益の損失を経験しています）。

- 半数弱の回答者が、DDoS によってファイアーウォールがダウンしたか、ファイアーウォールダウンの一因となったと答えており、その割合は昨年度の 42%から増加しています。ロード・バランサーでも問題が観測されており、昨年度、回答者の 3 分の 1 以上で DDoS 攻撃によるロード・バランサーの機能停止が観測されています。

DNS

- DNS を担当する専任のセキュリティ・グループは、昨年度に比べて減少しています。

- DNS による再帰的問い合わせを制限するというベスト・プラクティスを実施している回答者の割合には、ほとんど変化がありません。

- DNS インフラストラクチャへの DDoS 攻撃により顧客に影響が生じた事案の報告件数は、前年度よりも減少しています。

調査の範囲とデモグラフィックス

- 回答者数は 287 人（昨年度は 220 人）。回答者は、世界の Tier 1 ならびに Tier 2／3 サービス・プロバイダ、ホスティング、モバイル、エンタープライズ、およびその他の種類の通信事業者で構成されています。

- 10 年前の WISR の回答者数は 36 人でした。現在の WISR のデータは、地理的にもネットワーク事業者の種類においてもより広い範囲からまとめられています。

- 本年度の回答者の 60 パーセント以上がサービス・プロバイダ、約 18%が企業組織です。トラフィックに加え、ネットワーク、サービス、顧客をターゲットとする脅威について、世界的な状況の把握が可能です。

- 調査対象期間は 2013 年 11 月から 2014 年 10 月まで。