Arbor Networks 第 11 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

本文書は Arbor Networks の第 11 回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）の調査結果の概要を提示するものです。WISR は、運用に関するセキュリティ・コミュニティの 2015 年における集合的な経験、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 11 年間で WISR の対象範囲と規模は大幅に変化しましたが、中心的な目標は、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. インシデント対応時間の短縮に向けた取り組みが、企業、政府機関、教育機関、サービスプロバイダ、通信事情者からの大きな注目を集めています。プロセスをスピードアップさせる技術への投資が増えているため、対応時間は改善に向かっています。
2. 高度な攻撃は企業にとって最大の懸念事項の 1 つです。個人情報の流出や業務プロセスの中断は、高度な脅威がもたらす最大の業務リスクと見なされています。
3. Arbor Networks が本調査を開始してからの 11 年間に、DDoS 攻撃の最大規模は劇的に拡大し、報告された最大の攻撃は 11 年前に報告された 8 Gbps から、2015 年には 500 Gbps に増加しました。これは 60 倍の規模に相当し、前年比ベースで攻撃の規模が増加している傾向を示しています。
4. 攻撃の複雑性が引き続き増大しています。アプリケーション・レイヤ攻撃はほぼすべて（93%）のサービスプロバイダで観測されました。さらに、56%はマルチベクトル攻撃を体験しています（2014 年は 42%）。
5. ファイアウォールや IPS デバイスなどの既存インフラストラクチャが引き続き DDoS 攻撃の対象となり、企業の半数以上が DDoS 攻撃の結果、こうしたデバイスが機能停止したと報告しています。この割合は 2014 年の 3 分の 1 から大幅に増加しています。
6. データセンター事業者はボリューム型攻撃の増加に引き続き苦慮しており、半数以上のデータセンター事業者がインターネット帯域幅を枯渇させる DDoS 攻撃を体験しました。この割合は 2014 年の 33%から増加しています。

DDoS 攻撃に関する主要な調査結果

- 今回は初めて、最も一般的に認められる DDoS 攻撃の動機として「犯罪者の能力誇示」と「犯罪者の恐喝行為」が加わりました。これらは例年の調査に見られた「ニヒリズム／バンダリズム（オンラインにおける破壊攻撃）」と「ハクティビズム（政治などの思想的な理由による攻撃）」に代わるものです。
- マルウェアの侵入またはデータ漏洩のいずれかを遂行するために DDoS 攻撃が注意を逸らす手段として使われた回答者の割合が増えています。2015 年には、回答者の 26%がこれを DDoS 攻撃に共通する、または極めて一般的な動機と考えています（2014 年は 19%）。
- リフレクション／増幅の使用による攻撃は規模の拡大が続き、500 Gbps、450 Gbps、425 Gbps、337 Gbps の規模の攻撃が回答者から報告されています。

- クラウドベースのサービスは大きな標的となっています。2015 年にはサービスプロバイダの 33%がクラウドサービスを標的とした攻撃を体験しました（2014 年は 29%、2013 年は 19%）。
- リフレクション／増幅を利用したボリューム型攻撃が大型化する傾向に注目が集まる一方で、アプリケーション・レイヤ攻撃は続いています。アプリケーション・レイヤ攻撃を体験したサービスプロバイダの割合は、引き続き増加しています。2015 年には 93%に達しました（2014 年は 90%、2013 年は 86%）。
- 企業回答者の 4 分の 1 以上が 1 か月当たり 10 件以上の攻撃を受け、半数は攻撃の規模が自社の合計インターネット容量を上回ったと報告しています。
- サービスプロバイダの 9%が IPv6 DDoS 攻撃を観測したと報告しています。これは前回調査時の 2%から大幅に増加しています。
- 企業の 56%において、DDoS 攻撃の際にファイアウォールや 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（2014 年は 34%）。これは、サービスが十分に保護されていると知った攻撃者によるインフラストラクチャを標的とした攻撃の頻度が増大しているという事実を裏付けています。
- データセンター事業者の 9%が、1 か月当たり 50 件以上の攻撃を体験していると報告しています。2014 年にこれほど高い活動レベルを報告した回答者はいませんでした。
- ネットワーク内のサーバーに向けたアウトバウンド攻撃を体験したデータセンター事業者は、2014 年の 24%から 34%に急増しています。

高度な脅威に関する主要な調査結果

- 2015 年には、正規のインシデント対応計画を策定し、少なくとも一部のリソースをインシデントの対応に専念させた企業回答者の割合が、2014 年の約 3 分の 2 から 75%へと増加しました。
- 一方で、インシデントへの即応態勢を改善するために内部リソースを増やす予定であると述べた回答者の割合は、46%から 38%に微減しています。
- 即応態勢の改善が重要－企業の 57%は、インシデント対応プロセスを迅速化するソリューションを展開したいと考えています。
- 悪意ある内部関係者を観測した企業の割合は 2015 年に 17%に増加し（2014 年は 12%）、APT を体験した企業の割合は前年比で 18%から 23%に増加しました。
- 高度な攻撃は企業組織にとって最大の懸念事項の 1 つです。個人情報の流出や業務プロセスの中断は、高度な脅威がもたらす最大の業務リスクと見なされています。

DNS オペレータ

- 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は、2014 年の 17%から 2015 年には 30%へと大幅に増加し、2013 年のレベルに戻りました。この数字は、サービスプロバイダに限定すると半数近くにまで増加しています。
- DNS セキュリティ担当者を置く企業が増えています。しかし、サービスプロバイダの 17%と企業の 26%はリソースを割り当てていません。これは、DNS インフラストラクチャを標的とする攻撃が増えていることを考えると憂慮される状況です。

モバイルネットワークオペレータ

- 回答者の 38%が、パケットコアに関するセキュリティ・インシデントによって顧客が影響を受けたことがあると報告しています。
- 回答者の 68%が、モバイルユーザーまたはモバイルインフラストラクチャを標的とする DDoS 攻撃を観測したと報告しています。この数字は、2014 年はわずか 36%でした。興味深いことに、回答者の約 3 分の 1 が、1 か月当たり 20 件以上の攻撃を報告し、毎月 500 件を超える攻撃を報告する回答者は数人でした。
- モバイルネットワークオペレータの 15%は自社ネットワーク上のモバイルユーザーが開始した DDoS 攻撃を特定していますが、59%はこの脅威を特定するために必要な視認性を欠いています。
- 注意すべきことに、モバイルネットワークオペレータの 43%はパケットコアの視認性がゼロであると報告しています（2014 年は 30%、2013 年は 20%）。この視認性の欠如は、モバイル IP インフラストラクチャをセキュリティの脅威から守るうえで引き続き課題の 1 つになっています。
- モバイルネットワーク内での IPv6 の採用率は 2015 年に大幅に上昇しました。回答者の約 3 分の 1 が IPv6 を採用したと報告し、そのうち 13%は加入者のデバイスとモバイルインフラストラクチャの両方に IPv6 を採用しました

調査の範囲とデモグラフィックス

- WISR の調査データは、354 人（昨年度は 287 人）の回答者から得られたものです。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、エンタープライズとその他の種類の通信事業者で構成されています。
- 例年と同様に、回答者の過半数（52%）がサービスプロバイダ組織です。
- 企業組織は全回答者数の 38%を占めています。残りのサービスプロバイダ以外の回答者は、政府機関（6%）と教育機関（4%）です。
- 本調査は、2014 年 11 月から 2015 年 11 月までのデータを対象としています。