セキュリティリサーチ

DDoS 武器レポート

DDoS 攻撃者の実像：

DDoSの現状を理解する

DDoS攻撃者について知る

攻撃者とはどのような人々でしょうか？このレポートでは、DDoS攻撃の攻撃元、すなわち攻撃者と彼らがDDoS攻撃に使用するボット、アンプリファイア、ボットネットなどの「武器」に焦点を当てています。

このレポートでは、A10セキュリティリサーチチームがインターネットのスキャン、特許を取ったデセプション手法、およびオープンソースインテリジェンスを駆使して収集したデータを使用して、常に変化している世界の「武器」の現状と、DDoS武器の供給源、種類、その他の特性に関する分析結果を提供します。

一般に、分散型サービス拒否（DDoS）攻撃の緩和では、攻撃が検知されてから攻撃の標的が損害の緩和を試みるというリアクティブなアプローチがとられてきました。
このアプローチでは使える時間が限られているため、リスクを正確に評価して効果的な戦略で対応することは困難です。さまざまな理由から、DDoS攻撃に重点を置いた早期セキュリティインテリジェンスシステムが不可欠です。A10は、DDoS武器を継続的に監視して、組織が攻撃を受ける前にDDoS防御を強化するために利用できるリストを作成しています。

主な分析結果

DDoS武器の総数は、
ここ数年**ほぼ一定でしたが**、
このレポートでは前回のレポート
よりやや減少しています。

1700倍

反射型アンプ攻撃では、武器の総数という点ではSSDPが最多である状況が続いていますが、SSDPほど利用数が多くないカテゴリでも、Memcachedのように**武器1つあたりの増幅能力がSSDPの1700倍に達する**ものがあります。

今年、ホストしている潜在的なDDoS武器の数で、**米国が中国をわずかに上回って**トップになりましたが、これはアンプ攻撃の武器数が最大であったためです。

4倍

1人あたりの数で見ると、米国は**中国の4倍の武器**をホストしています。これには、米国のインターネット接続人口が多いことが大きく影響しています。

しかし、ボットの総数では中国がトップとなり、インドが世界第2位のボット供給源となりました。

16%

追跡されているボットは、前回のレポート以来、**世界中で16%増加**しています。悪意のあるボットとボットネットを特定して除去しようとする主要な各国政府や組織の努力にもかかわらず、これほどの増加が生じました。

01. 主な分析結果
02. DDoS攻撃の武器
03. DDoSの攻撃元
04. ボット
05. アンプリファイア
06. 攻撃
07. 防御戦略
08. A10 Defend

2024年に攻撃者が利用できるDDoS武器の数

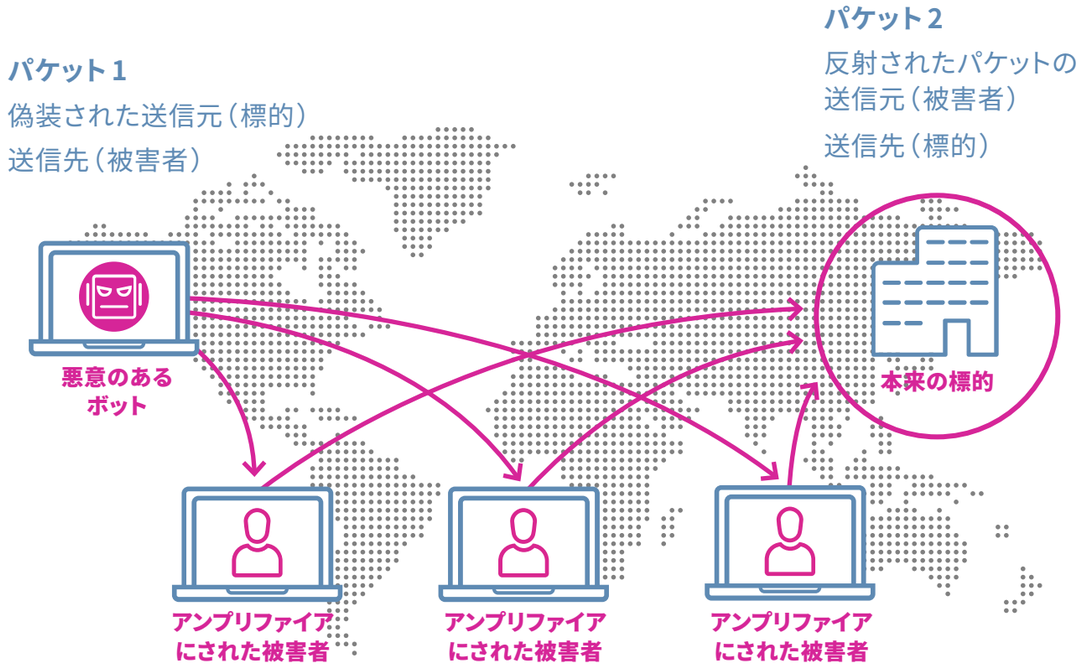
A10が追跡しているDDoS武器は、ボット（ドローンとも呼ばれます）とアンプリファイア（リフレクターとも呼ばれます）で構成されます。これらは、一意のIPアドレスで特定できて標的に対するDDoS攻撃に悪用できる、感染済みまたは脆弱なデバイスです。

ボット、ボットネット、アンプリファイア - DDoS武器の詳しい分析

ボットネット（「ロボットネットワーク」の略語）は、「ボットハーダー」と呼ばれる単一の攻撃者の制御下にある、マルウェアに感染したコンピュータのネットワークです。ボットハーダーに制御されている個々のマシンはボットと呼ばれます。ボットとボットネットは、直接DDoS攻撃を仕掛けるために使用されることもありますが、アンプリファイアを使った反射型アンプDDoS（DrDoS）攻撃に使用される方が一般的です。DrDoS攻撃では、IPアドレスを偽装して標的になりすました攻撃者が、ボットを使ってアンプリファイア（適切に設定されていないDNSサーバーや他のネットワークデバイスなど）にリクエストを送信します。そのリクエストはアンプリファイアで反射されて、レスポンスが標的に送信されます。

図1：

DDoS攻撃者の手法 - アンプリファイアとボット



A10 ネットワークスが追跡した DDoS 武器の総数

攻撃者が利用できる武器が何百万台もあるのです。
ここ数年、A10 の見積りは 1500 万台前後となっています。

図 2：

追跡された DDoS 武器の年間総数

800 社を超えるメーカー（その多くは規制を受けていない）から販売され、世界中で急速に普及している IoT デバイスは、2027 年までに 290 億台を超えると見込まれています。これらのデバイスには、セットトップボックス、モバイルデバイス、スマートテレビ、スマートウォッチ、データ収集端末、プリンター、メディアプレイヤーなどが含まれ、DDoS 攻撃者にとってはつけ込む隙の多い格好の標的になり得ます。この種のデバイスは、ボットとしてもアンプリファイアとしても利用できます。

ボット、ボットネット、リフレクターは、常に変化したり移動したりしています。たとえボットネットやアンプリファイアを見つけて除去し、脆弱性を解消しても、利用可能な武器の総数はほぼ変わりません。武器にできるデバイスの数が増え続けているからです。一例として、アプリケーション層の一意の識別子を追跡しているリサーチチームは、一部のデバイスで毎週 IP 変動を観測しています。この点を示すために、武器をより詳細に SSDP セットまで分類すると、2024 年の武器の総数は前回のレポートよりわずかに減少しただけです。

Microsoft が定義しているように、アンプ攻撃（フラッド攻撃またはボリューム攻撃）では、攻撃者が標的の処理能力を超えたトラフィックの生成に成功し、標的のリソースを浪費させて正規のトラフィックを処理できないようにさせます。攻撃を増幅するためには、リクエストを上回る数のレスポンスを生成する必要があります。攻撃者はこの目標を達成するために、多くのリフレクターを見つけて、最大限の増幅をもたらす巧妙なリクエストを作成します。

図一覧

図	説明	ページ
図 1：	DDoS 攻撃者の手法 - アンプリファイアとボット	4
図 2：	追跡された DDoS 武器の年間総数	5
図 3：	追跡された DDoS 武器の総数（地域別）	6
図 4：	DDoS 武器の上位ホスト国	7
図 5：	接続されたデバイスあたりの DDoS 武器の総数（中国との比較）	7
図 6：	組織別の DDoS 武器の分布	8
図 7：	追跡されたボットの総数	9
図 8：	DDoS ボットの上位ホスト国 / 地域	10
図 9：	DDoS ボットの上位ホスト組織	11
図 10：	アンプリファイアの総数（地域別）	12
図 11：	DDoS アンプ攻撃用武器のトップ 6（プロトコル別）	14
図 12：	各プロトコルの増幅率	15
図 13：	世界中で攻撃の標的になっている国（30 日間のサンプル）	17
図 14：	1 人あたりの DDoS 攻撃件数	17
図 15：	DDoS 攻撃の持続時間	18
図 16：	典型的なクラウドプロバイダーに対する攻撃の多様性と頻度 - 30 日間のサンプル	19
図 17：	A10 Defend Threat Control ポータルのダッシュボード	21

A10 Networks / A10ネットワークス株式会社について

A10 Networksは、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Webサービス事業者まで7000社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。

A10ネットワークスは2004年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

- URL：https://www.a10networks.co.jp/
- X（旧Twitter）：https://twitter.com/a10networksjp
- Facebook：https://www.facebook.com/A10networksjapan

本レポートについて

A10ネットワークスのセキュリティリサーチチームは、DDoS武器に関するインテリジェンスを収集するために、ボットネットのコマンド＆コントロール（C2）の制御下にある攻撃エージェントの厳密な監視や、ハニーポットを使った新しいマルウェアの解明、自己複製するボットネットの通信傍受、インターネットのスキャンによる反射型アンプ攻撃の送信元探索などの活動を行っています。

当社では、インターネットのスキャン、特許を取ったデセプション手法、およびオープンソースインテリジェンスを駆使して、DrDoS攻撃、ボットネットを送信元とする直接攻撃、公開プロキシを経由した攻撃に関するデータを収集しています。このレポートで使用されたデータの90パーセント以上は、A10のソースから直接収集されました。

詳細については、A10Networks.co.jp にアクセスしてください。

Learn More

About A10 Networks

Contact Us

A10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp

Part Number: A10-EB-14115-JA-11 MAY 2024