

2018年第4四半期

DDoS攻撃者の 武器

A10のセキュリティ調査による特別レポート



要旨

DDoS 攻撃の頻度、強度、巧妙さは増大し続けています。しかし、クラッシュを起こすような大規模攻撃を実施するために、ボットネットや脆弱なサーバーを利用するという配信手法は変わっていません。難読化によって攻撃の検知を逃れるような従来のセキュリティ対策とは異なり、広範囲に分散される性質を持つ DDoS 攻撃に対しては、攻撃者の武器がどこであるかに焦点を当てることで未然に被害を防ぐチャンスが生まれます。

反射型アンプ攻撃という武器

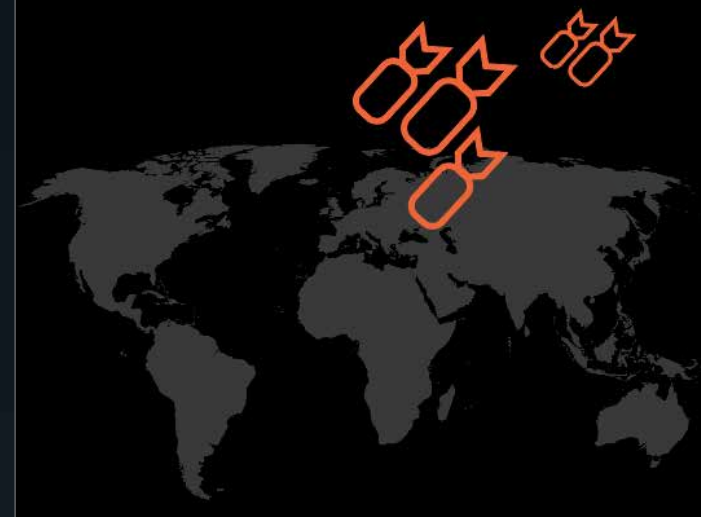
攻撃者は UDP プロトコルの脆弱性を利用して標的の IP アドレスを偽装し、サーバーの脆弱性を悪用して反射的な応答を引き起こします。この方法では、最初のリクエストよりはるかに大きなサーバー応答を生成することで攻撃を増幅します。

DDoS ボットネットという武器

マルウェアに感染したコンピュータ、サーバー、および IoT デバイスが、ボットハーダーに制御されて（通常は DDoS 攻撃請負サービスから）攻撃に利用されていますが、特に IoT デバイスの利用が増えています。これらで形成されるボットネットは、ネットワークレイヤーおよびアプリケーションレイヤーに対するステートフル/ステートレスな攻撃を仕掛けるために使用されます。

A10が追跡したDDoS攻撃用の武器：

22,811,159



DDoS 脅威インテリジェンス

DDoS 攻撃の攻撃元の特定と列挙

脅威の研究者は、DDoS 攻撃請負 (DDoS-for-hire) サービスによって指揮された攻撃エージェントを注意深く監視してハニーポットを仕掛け、見つかった反射ソースのエージェントをスキャンして、DDoS 脅威インテリジェンスを収集します。A10 とパートナーのセキュリティ研究者はこれまでに、DDoS 攻撃で常用されている侵害されたホストの IP アドレスを数百万件収集しています。このデータは、数千万ものエントリを含む大量のフィードを作成するために使用されます。このデータを単なる情報から実用的な情報に変えるために、A10 のソリューションでは数百万のエントリから成るクラスリストに基づいて精度の高いブラックリストとホワイトリストを作成しています。

追跡された DDoS 攻撃の武器 (規模順トップ5)

NTP : 6,658,199



DNS リゾルバ : 5,116,043



SSDP : 3,377,929



CLDAP : 2,953,282



SNMP : 2,408,692



“ DDoS 攻撃の動機やタイミングを完全に理解することは不可能です。しかし、武器や侵害されたネットワークのリストを作ることができます。

A10 Networks の DDoS 脅威インテリジェンスは、防衛側が DDoS 攻撃の状況認識を向上させるのに役立つ重要情報を提供し、攻撃開始前のプロアクティブな自衛を可能にします。”

— Rich Groves

A10 Networks

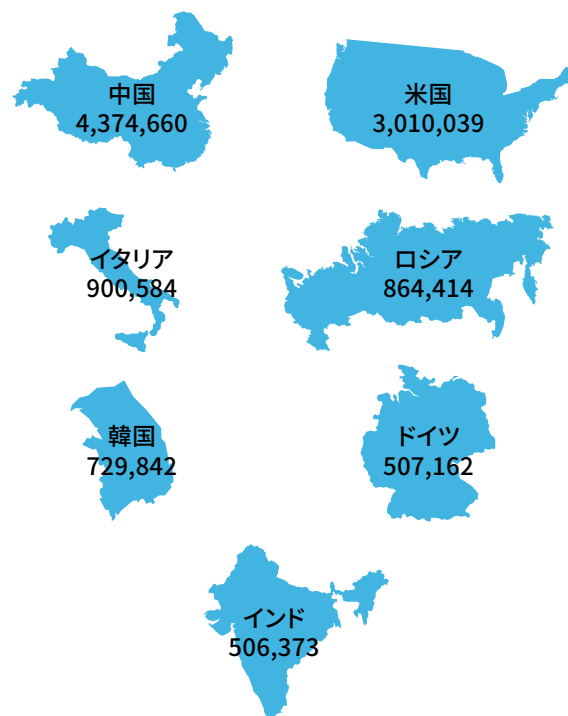
セキュリティリサーチディレクター

DDoS 攻撃用武器の主な供給源

DDoS攻撃は本質的に分散化されていますが、その攻撃元については興味深いデータが見つっています。

DDoS 攻撃用武器が集中している国

DDoS 攻撃用の武器は世界中に分散していますが、インターネット接続人口の密度が高い地域に集中していることがわかっています。



DDoS 攻撃用武器が集中しているASN

ASNは、単一の管理オペレータの制御下にあるIPアドレス範囲の集合です。これらの企業または政府機関のオペレータは、彼らのユーザーに属する多数の武器が自ネットワークに接続したまま他のネットワークやコンピュータを攻撃できるようにします。

 China unicom 中国联通	1,727,301
 ChinaNetCloud 云网科技 CloudNet Technology	1,546,804
 TIM	523,600
 kt	266,413
 OVH.com	250,344
 中華電信 Chungwa Telecom	244,672
 D'LIVE	168,650

クラウドにホストされたDDoS 攻撃用武器

クラウドの普及とモバイルデバイスの出現により、ネットワークやアプリケーションの配信方法が変化しています。残念ながら、武器も他の業界と一緒に進化しています。

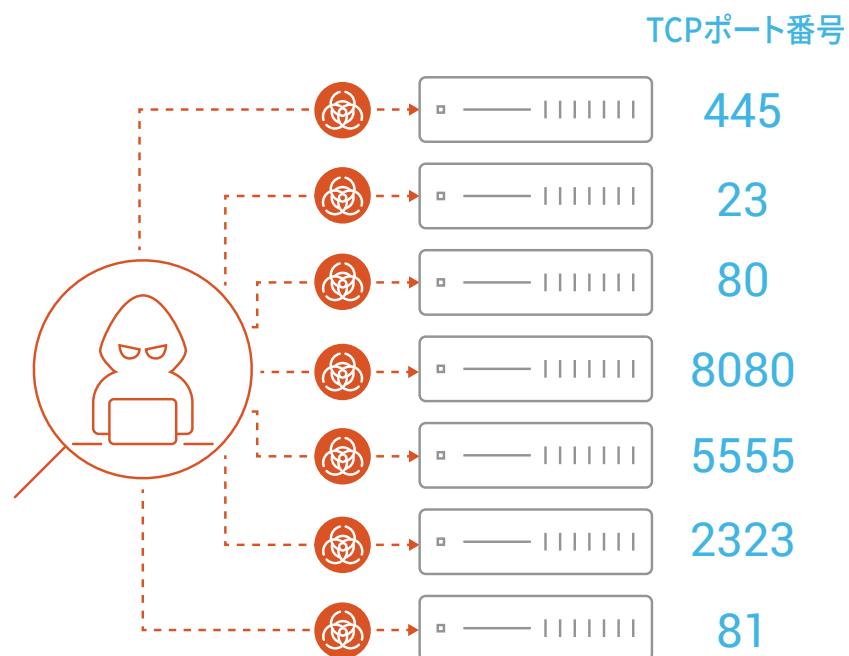
クラウドサービスが
ホストしている
DDoS攻撃用武器の数



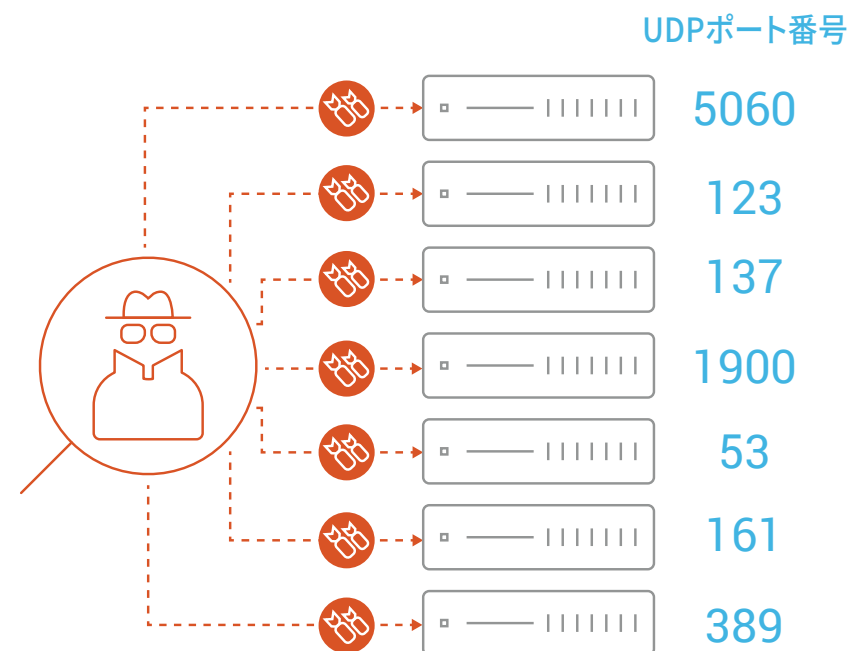
DDoS 攻撃者による偵察

DDoS 攻撃は、動機のある攻撃者、DDoS 攻撃請負サービス、および武器を含む犯罪エコシステムによって行われています。攻撃者は通常、利用可能な DDoS 攻撃用武器のプールを備えたオーケストレーションプラットフォームを持っている DDoS 攻撃請負サービスの力を借ります。DDoS 攻撃請負サービスのボットハーダーは、継続的に武器のストックを補充するために、インターネットをスキャンして、無防備な TCP サービスを通じて脆弱な IoT コンピュータノードを見つけるとともに、アンプ攻撃に利用できる UDP サービスを探っています。

検索件数が多い IoT ポート



検索件数が多いリフレクター



IoTはDDoS ボットネットの温床

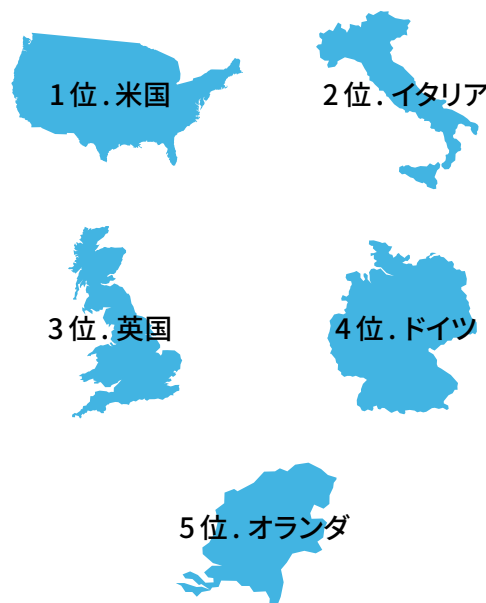
5Gにより攻撃ネットワークが大幅に拡大

インターネットの誕生からたった25年で、全世界人口76億人の55%がネットに接続するようになりました。その人数は、1秒あたり4.6人という増加率で直線的に増えました。1秒あたり127デバイスが新たに接続されているIoTの成長率はこれを上回っており、さらに加速しています。5G（第5世代モバイル通信システム）の出現により、帯域幅速度の大幅な向上、超低遅延、そして地理的なカバー範囲の劇的な拡大がもたらされ、IoTの新たな使用形態の爆発的な増加と、接続されるデバイスの指数関数的増加が予測されます。5Gにより、脅威のすばやい検知と軽減のためには、機械学習とAIを使ったインテリジェントオートメーションが不可欠となります。Linuxで動作するIoTデバイスは、すでに新種のマルウェアの標的になっており、これらのマルウェアは主にDDoS攻撃に使用されています（Eurecom）¹。IoTは、ボットネットにとって完璧なホストです。彼らが残していったマルウェアを見てみましょう。

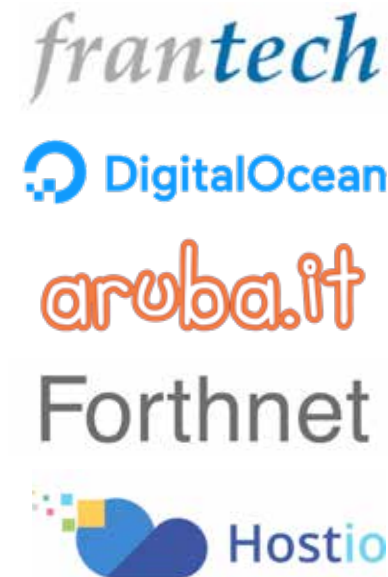
ドロップされた代表的なIoTマルウェア

バイナリ名	ファミリー名
mirai.x86	Mirai.A
sora.x86	Mirai.AT
miori.x86	Mirai.F
hoho.x86	Mirai.D
DEMONS.x86	Gafgyt/Bashlite

多くのマルウェアドロッパーがホストされている国



多くのマルウェアドロッパーがホストされているASN



¹ http://www.s3.eurecom.fr/docs/oakland18_cozzi.pdf (フランスに本拠を置く EURECOM)

最大規模の DDoS 攻撃の共通点 - アンプ(増幅)攻撃

反射型アンプ攻撃は、規模について言えば最大クラスに入ります。反射型アンプ攻撃とは、誤って構成されているインターネット上の無防備なサーバーに対して偽装したリクエストを送りつける、UDP プロトコルのコネクションレスな性質を悪用した DDoS 攻撃の一種です。

この攻撃戦略では、偽装した被害者の IP アドレスを使用して、大量の小さなリクエストが無防備なサーバーに送信されます。リクエストを受信した各サーバーは、増幅された大量の応答を何も知らない被害者に返します。これらのサーバーが標的となる理由は、攻撃を増幅できるサービスを使用できる構成になっていることにあります。

この種の最も一般的な攻撃では、無防備な DNS、NTP、SSDP、SNMP、CLDAP の UDP ベースのサービスを何百万回も利用できます。このような攻撃は、1.3 Tbps の Memcached ベースの GitHub 攻撃など、記録的な巨大な量の攻撃となり、DDoS 攻撃の大部分を占めています。

反射型アンプ攻撃の武器の主要な地理的分布

DNS リゾルバ

米国	1,401,407
中国	885,625
ロシア	233,535
ドイツ	207,390
フランス	177,629

NTP

米国	1,302,440
中国	1,202,017
イタリア	630,826
ロシア	403,180
ドイツ	283,821

CLDAP

米国	1,233,398
中国	265,816
日本	159,868
ドイツ	97,503

SNMP

韓国	293,702
米国	283,264
インド	277,696
中国	182,414
イタリア	138,710

SSDP

中国	2,167,058
ロシア	194,892
台湾	115,913
米国	97,363
韓国	92,531

5G でさらに大規模化する DDoS 攻撃

DDoS 攻撃の規模と巧妙さの進化は加速し続けています。新たな 5G ネットワークが稼働し始めるにつれて、攻撃の規模がこれまでの記録をはるかに超えて大きくなっていくと推測されます。5G によって、新たなスマートワールドの多種多様な IoT アプリケーションと使用形態が利用できるようになりますが、それに伴って攻撃者が利用できる DDoS 攻撃用武器も増えていきます。エリクソン社は最近、携帯接続される IoT デバイスの数が 2024 年までに 41 億を超えるという予測を発表しました。これらのデバイスは、数が増えるだけでなくその通信速度も増大します。この急速な拡大の背後にある主な推進要因は、データ通信をはるかに高速化して遅延を大幅に減少させる 5G です。サービスプロバイダーは、これらの増大する脅威に備えて急速に進化して、セキュリティの異常を瞬時に検知して軽減できるようにインテリジェントオートメーションを導入する必要があるでしょう。

高度な DDoS 脅威インテリジェンスと、リアルタイムの脅威検知、攻撃に対抗するシグネチャの自動生成を組み合わせることで、攻撃の発生元がどこであるかにかかわらず、最も大規模なマルチベクトル型 DDoS 攻撃に対しても防御を固めることができます。実用的な DDoS 脅威インテリジェンスは、DDoS ボットネットと DDoS 攻撃に利用されやすい脆弱なサーバーの IP アドレスの最新かつ正確なフィードに基づいてブラックリストを作成することで、プロアクティブな DDoS 防衛アプローチを可能にします。A10 Networks とパートナーのセキュリティ研究者が、この DDoS 脅威インテリジェンスの最前線に立っています。A10 は、サービスプロバイダーが全範囲における DDoS 攻撃対策を実現できる包括的で集約されたシステムを提供しています。

A10 Networks の DDoS 脅威インテリジェンスの詳細については、
弊社の DDoS 脅威マップ <https://threats.a10networks.com> をご覧ください。

“ プロアクティブなインテリジェンスの
収集と適用には、攻撃者が使用する
インフラストラクチャを攻撃者と同時
に特定できるユニークな能力があり
ます。”

— John Bambenek 氏
ThreatSTOP 社セキュリティリサーチ
およびインテリジェンス担当 VP



A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE: ATEN) はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networks 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拠地を置き、世界各国の拠点からお客様をサポートしています。

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 : <http://www.a10networks.co.jp/>

Facebook : <http://www.facebook.com/A10networksjapan>

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

©2019 A10 Networks, Inc. All rights reserved. A10 Networks、A10 Networks ロゴ、ACOS、A10 Harmony は米国およびその他の各国における A10 Networks, Inc. の商標または登録商標です。その他の商標はそれぞれの所有者の資産です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。www.a10networks.com/a10-trademarks