2019年第1四半期

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。

このレポートの主な見解

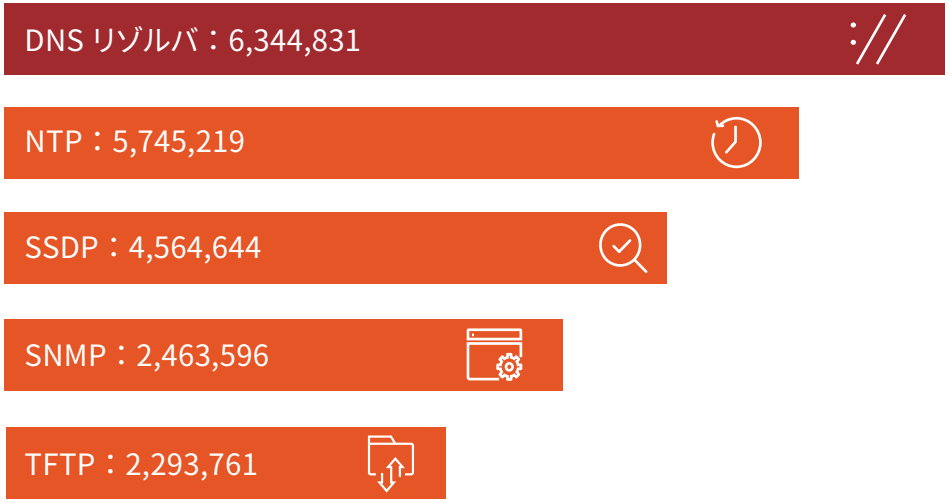
- TFTP による反射型アンプ攻撃が DDoS 攻撃に使用される武器トップ 5 に入る
- CoAP による反射型アンプ攻撃の武器にされた IoT デバイス 414,130 台を特定
- DDoS 攻撃の武器が急増しているスペインが世界第 3 位のホスト国へ
- UDP ポート 1434 を介した SQL 反射型攻撃のためのスキャン活動が増加

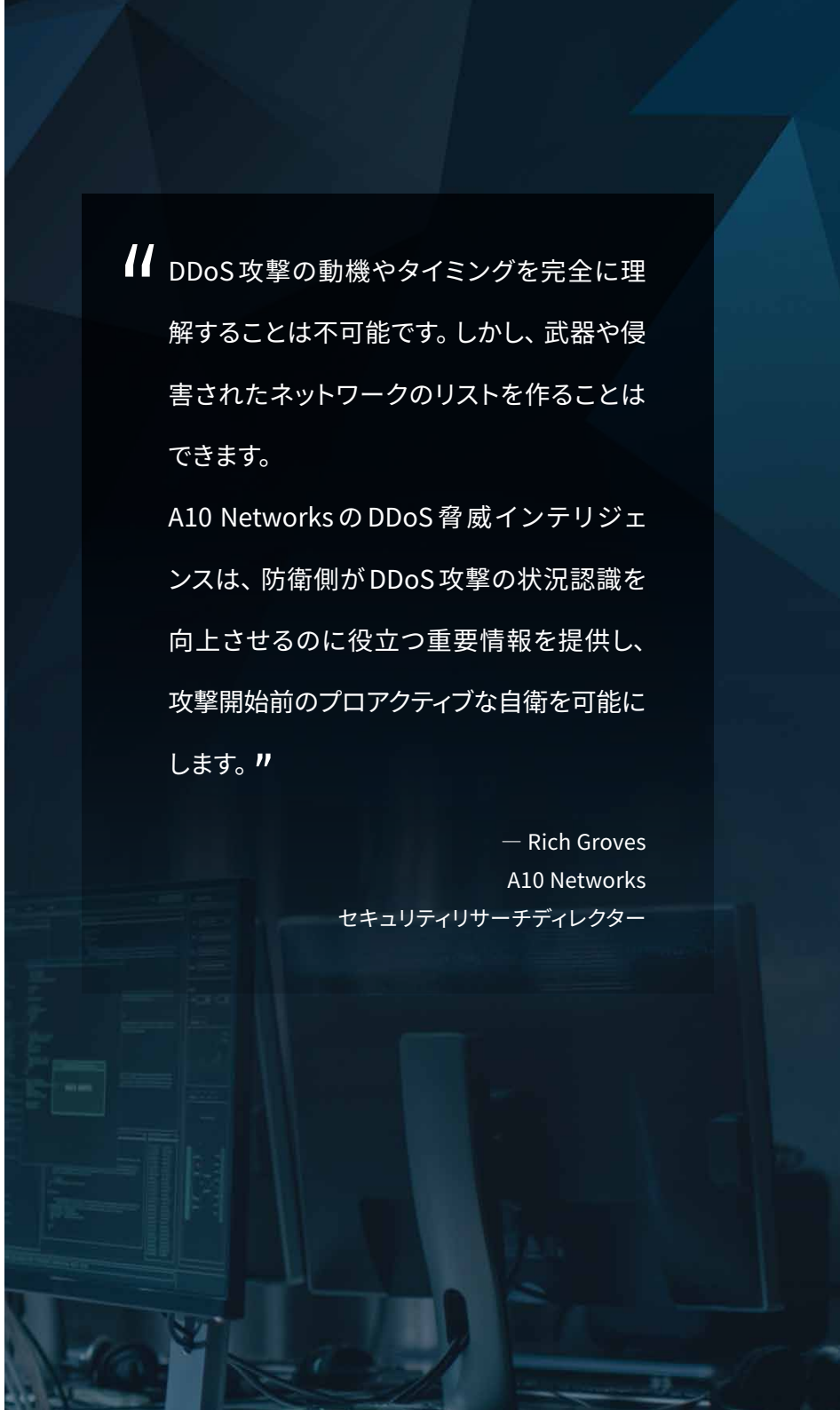
DDoS 脅威インテリジェンス

DDoS 攻撃の攻撃元の特定と列挙

脅威の研究者は、ボットネットコマンドアンドコントロール（C2）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）





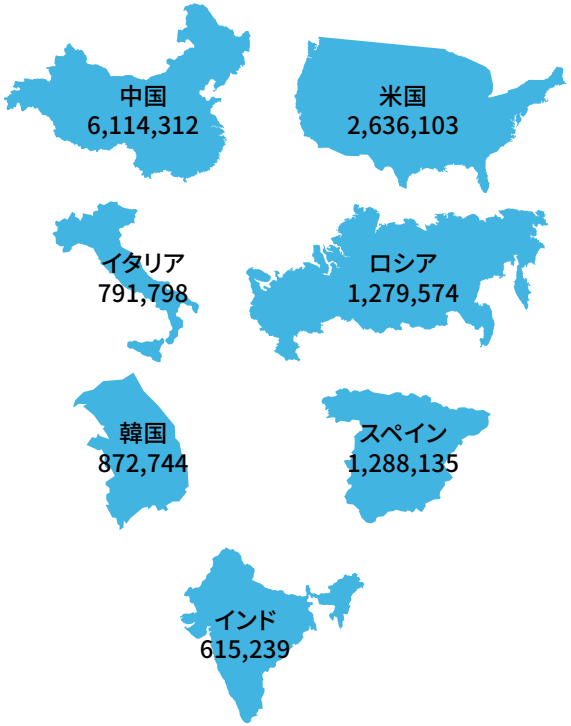
> “DDoS 攻撃の動機やタイミングを完全に理解することは不可能です。しかし、武器や侵害されたネットワークのリストを作ることはできます。
>
> A10 Networks の DDoS 脅威インテリジェンスは、防衛側が DDoS 攻撃の状況認識を向上させるのに役立つ重要情報を提供し、攻撃開始前のプロアクティブな自衛を可能にします。”
>
> — Rich Groves
> A10 Networks
> セキュリティリサーチディレクター

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かっています。

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	2,626,265
中国电信 CHINA TELECOM	2,154,504
vodafone	1,075,512
中華電信 Chunghwa Telecom	397,227
TIM	387,771
Rostelecom	372,422
kt	371,305

モバイルキャリアがDDoS攻撃の武器をホスト

DDoS攻撃の武器をホストするモバイルキャリアがレポート期間中に急増しています。

Vodafone Spain（ボーダフォンスペイン）

DNSリゾルバ攻撃のホスト第1位

Guangdong Mobile（広東モバイル）

CoAP（UDP）反射型攻撃のホスト第1位

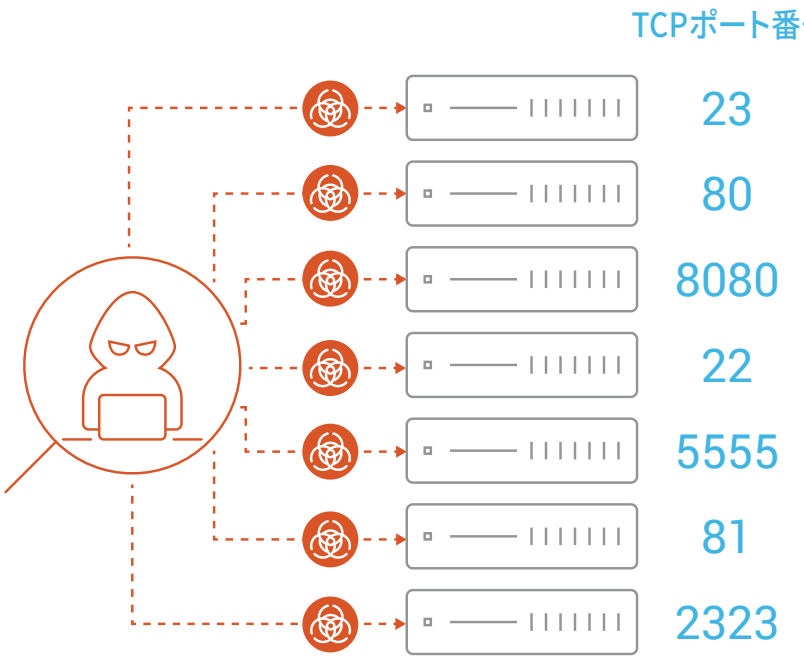
Shandong Mobile（山東省モバイル）

50万以上のSSDPアンプ攻撃に利用できるシステム

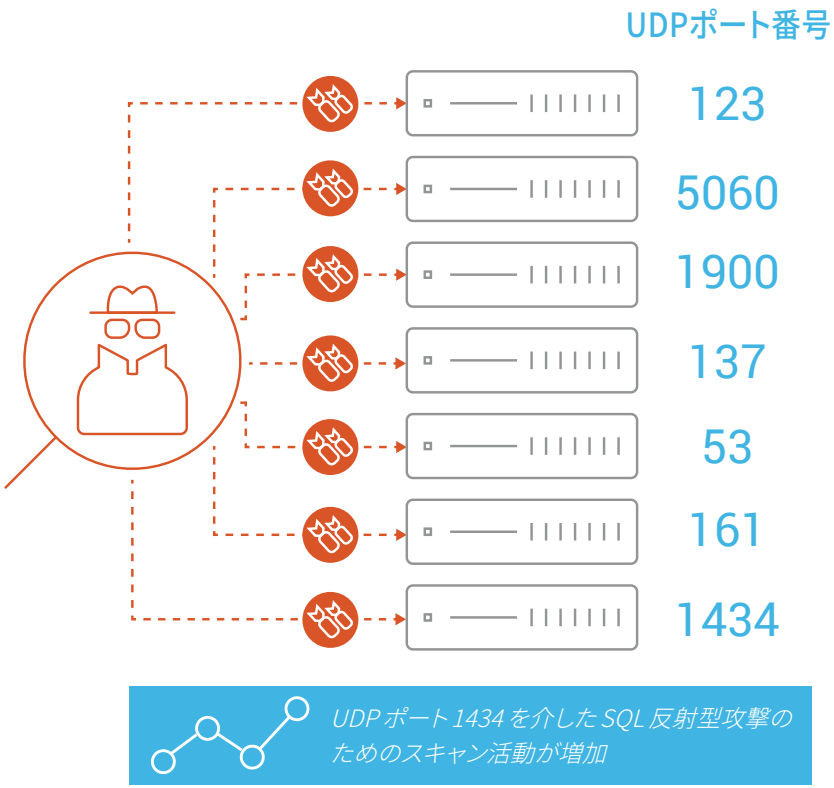
DDoS攻撃者による偵察

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

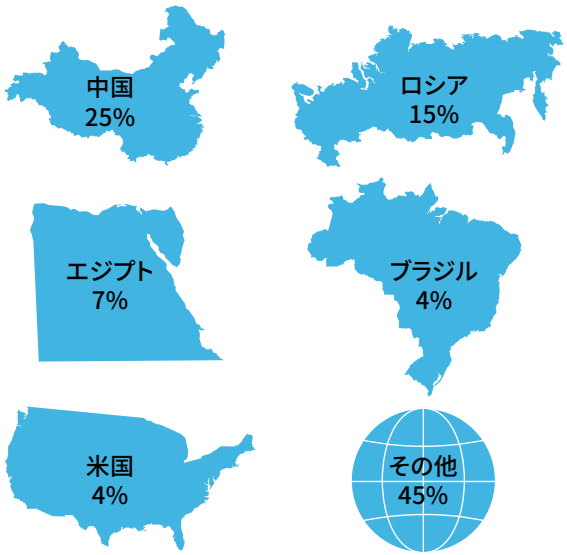


DDoS ボットネットエージェント

マルウェアに感染して攻撃者の制御下にあるコンピュータ、サーバー、ルーター、カメラおよびその他の IoT デバイスなどのノードは DDoS 攻撃の重要な武器になります。これらは一般的にボットまたはボットネットと呼ばれ、DDoS 攻撃を柔軟に仕掛けることができます。

セキュリティ研究者は、DDoS 攻撃で繰り返し使用されるホストの情報を蓄積し、マルウェア感染の特徴を示したホストを調査します。DDoS 攻撃が発生したら、その IP アドレスをさらに精査して慎重に対処します。

DDoS ボットネットエージェントが集中している国



DDoS ボットネットエージェントが集中している ASN

China unicom 中国联通

Rostelecom

中国电信 CHINA TELECOM

TE Data

中華電信 Chunghwa Telecom

IoT は DDoS ボットネットの温床

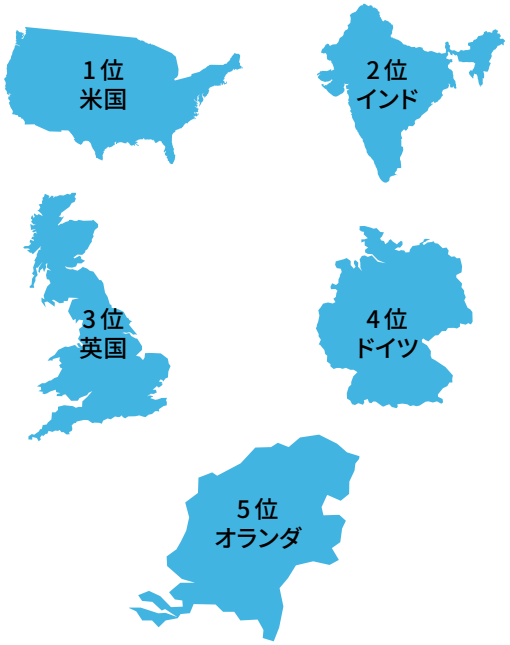
5G により攻撃ネットワークが大幅に拡大

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

ファミリー名	バイナリ名
Mirai	sora.x86
Gafgyt	Mx86
Hajime	storm.x86

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

DigitalOcean
aruba.it
Hostwinds
DSLEXTREME
3winfra

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

最新のIoT脅威：COAP

IoTを悪用した新しいDDoS攻撃では、Miraiやマルウェアは使用されません。IoTデバイスのテクノロジはセキュリティが脆弱なため、何百万ものデバイスを武器に反射型アンプ攻撃を実行できます。新しい攻撃戦略では、UDPで実装されたCoAP（Constrained Application Protocol）がベースになります。このM2M（マシンツーマシン）の管理プロトコルは、スマートエネルギーやビルオートメーションなどのアプリケーションをサポートするIoTデバイスに導入されています。

DDoS攻撃者にとってCoAPは、TCPとUDPの両方で実装され、小さな要求に対して大きな応答を返すのに認証を必要としないプロトコルです。

40万以上の脆弱な
IoTデバイスを特定
（特定した台数：414,130台）

96%

の応答が350バイト以上

応答の62パーセントが
1KB以上

749バイト

応答の平均サイズ

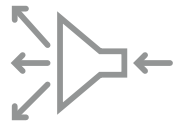
98%

が中国に存在している

UDPポート5683から
任意の宛先ポートへの攻撃

4Kバイト

応答の最大サイズ



平均増幅率：35倍

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

中国	1,495,968
スペイン	1,177,411
米国	769,138
ロシア	281,765
台湾	264,611

NTP

米国	1,306,043
中国	1,082,210
イタリア	492,617
ロシア	393,771
ドイツ	273,534

SSDP

中国	2,669,332
ロシア	323,592
台湾	125,253
米国	115,090
イタリア	98,463

SNMP

韓国	263,820
米国	259,959
インド	143,398
中国	126,336
イタリア	116,188

TFTP

中国	305,971
米国	292,882
ロシア	272,917
韓国	240,397
カナダ	102,033

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。

> "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

DDoS 脅威インテリジェンス

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。

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

Part Number: A10-EB-14115-JA-03　MAR 2019