DDoS 防御を発展させた新プラットフォーム：

包括的なDDoS 防御：可視性、保護、レポート/アドバイス

包括的かつプロアクティブなアプローチで DDoS 防御を強化

DDoS は最大の脅威インシデントであり、特殊な防御が必要です。ハードウェアアプライアンスまたはクラウドスクラビングのみに依存する既存の DDoS 保護では、基本的な DDoS 攻撃を阻止するだけで十分とは言えません。今日の DDoS 攻撃は複雑で大規模なため、より精密かつプロアクティブに既存の DDoS 防御を補完することが必要です。複雑化したインフラを守るには、その補完的な DDoS 防御は、容易に既存への統合・導入が可能であることが重要です。包括的な DDoS 防御プラットフォームである **A10 Defend Threat Control は、DDoS 攻撃の可視性を強化し、DDoS 保護を提供し、プロアクティブな DDoS 脅威調査が可能です。**

ユースケース 1:

A10 独自の AI で強化されたデータ収集および検証方法により、Defend Threat Control は非常に精密な予防的知見と防御的知見の両方を提供可能です。Threat Control を導入している組織は、ネットワークに対する敵対的な視点を得ることができ、世界中の外部脅威に関する詳細な調査を実施することができます。DDoS 攻撃は様々な方法で実行され、最近の HTTP2 高速リセットの脆弱性で示されているように、あまり知られていなかった攻撃手法が使用されることもあります。このような知見は、組織インフラを改善するための推奨事項を提供し、より多くの潜在的な DDoS 攻撃を確実に可視化します。

ユースケース2：

A10 Defend Threat Control の実用的なブロックリストは、A10 独自の検出・検証により作成されます。リストの精度が高く、実用的で、既存のセキュリティデバイスで簡単に利用できます。それは、現在 DDoS 対策が不十分な組織にとって、最初の防御層となります。組織に既存の DDoS 防御機能がある場合、Threat Control のブロックリストを追加して、より包括的に DDoS 攻撃を調査し防御することができ、既存の防御機能の有効性を高めることができます。これらのブロックリストは、組織固有のカスタマイズと ISP ガイドラインに準拠しています。さらに、これらのリストを組織が利用している ISP に提供でき、DDoS 攻撃を受けている際の追加の防御層としても機能します。

A10 Defend Threat Control の利点

- 既存の DDoS 防御を補完
  DDoS 対策専用ハードウェアを必要とせずに精密な最初の防御層を確立
- 有益な知見を提供
  プロアクティブな DDoS 防御を導入
- 潜在的な脅威を監視・調査
  ネットワークに対する敵対的な視点を得る

> *DoS 攻撃は依然として蔓延しており、ここ数年はインシデントのトップです。*
>
> – Verizon 2023 Data Breach Investigations Report

ソース: verizon.com/business/resources/Tbc9/reports/2023-data-breach-investigations-report-dbir.pdf

お問い合わせ

https://info.a10networks.com/JP-WebContactUs.html

 | A10-GR-70361-JA-02 FEB 2024

A10 Defend Threat Control

自社の環境に合わせたプロアクティブなIPインテリジェンスで完璧なDDoS対策を実現

A10 Defend Threat Controlは、攻撃前の活動やデータを積極的に活用して、発見しにくい攻撃者や複雑化するDDoS攻撃にユーザがいち早く対処できるようにします。A10のセキュリティリサーチチームは、脅威のパターンやシグナルを常に分析・収集し、世界中の1,500万以上のDDoS武器（DDoS攻撃ツール化したデバイス）を追跡しています。これにより、独自の、実用的でカスタマイズ可能な脅威インサイトを提供します。

Threat Controlを使用することで、DDoS武器に対する防御が容易になるため、攻撃が発生した際、組織はより迅速な対応が可能になり、ユーザーの組織内で武器化されてしまったインフラも特定できるようになります。Threat Controlは、攻撃の傾向を視覚化し、発生中の攻撃や過去の攻撃を調査し定期的に更新・カスタマイズされたIPブロックリストを提供します。ユーザーはそのIPブロックリストを自身のインフラの防御に活用できます。これは、組織が持っている既存のDDoS対策を補完し、強化します。

ボットネットの検出

世界中に分散配置した脅威偵察用デバイスのネットワークが、さまざまなポートでインターネットのトラフィックを監視し、悪意のあるトラフィックを特定します。これらのデバイスは、複数のネットワーク層で動作し、様々なボットネットとその拡散活動を検出します。この豊富なデータと、詳細なペイロード分析により、A10は既知の脆弱性やゼロデイ攻撃を見つけることができます。現在追跡されているボットネットの例は以下のとおりです。

- Miraiとその亜種
- Mozi
- Hajime
- Bashlite
- Omni

Threat Controlは、ボットネットのIPアドレスの正確なリストをユーザーに提供し、これらを防御システムで使用することで、悪意のあるトラフィックをブロックし、自組織のインフラストラクチャを監視することができます。

コマンド&コントロールの検出

コマンド&コントロール（以下、C2）サーバーは、サイバー犯罪者が侵害したデバイスやネットワークを管理・制御するために使用されます。これらは、しばしばDDoSボットネットやマルウェアの一部として機能します。A10のセキュリティリサーチチームは、調査用に独自に設計・準備したシステムに、ボットや悪意ある攻撃者をあえて感染させることで、リクエストやアップロードされたサンプルを分析し、C2システムとの通信を観察することを可能にしています。

Threat Controlは、C2のIPアドレスの正確なリストを提供します。そのリストを用いてユーザーは、自組織のネットワーク内のC2通信の特定や、DDoSボットネットに参加するなど侵害されたマシンの識別が可能となります。

リフレクターの検出

リフレクション攻撃は、正規のマシンを悪用して被害者のIPアドレスに応答を送るという点で、ボットネットとは異なります。これらの攻撃は、小さなリクエストで大量のレスポンスを生成するため強大な増幅効果を伴うことが多くなります。

A10はインターネット上のリフレクターを常時監視し、自動化されたツールで応答をキャプチャーして分析しています。レスポンスのペイロードを分析することで、独自に設計されたシステムが様々なタイプのリフレクターを確実に識別します。リフレクターの攻撃カテゴリーは、DNS、TFTP、Mitel、SSDP、Chargen、CoAP、CLDAP、Plexmedia、Ubiquity、Dahua-UDP、SNMP、SLP、NTP、WSDiscovery、VSE、Jenkins、Memcached、OpenVPN、MSSQL、NATPMP、DTLS、RDPなど、よく知られたものと、あまり知られていないものに分類されます。

Threat Controlは、ユーザーにリフレクターの正確なIPリストを提供し、リフレクション攻撃の予測と自組織のインフラ内に潜在するリフレクターの特定を支援します。

オープンソースインテリジェンス

Threat Controlは、Torの出口ノードやIPv4のBogonなどの情報を含む、定期的に更新されるオープンソースのフィードを提供しています。ユーザは、これを単一の信頼できる提供元（A10）からのネットワークリストとして利用することができ、デバイスを簡単に設定することができます。

なぜA10 Defend Threat Controlなのか

DDoS攻撃者の高度化に対抗するために、多層防御戦略や実用的なインサイト、特定の脅威シナリオに合わせた最新のIPインテリジェンスの使用を含む、「プロアクティブな対策」をA10は推奨しています。

A10 Defend Threat Controlは、ユーザーに、幅広い種類のDDoS攻撃に対応したネットワークとインフラの防御を強化するためのプロアクティブなツールを提供します。これにより、ダウンタイムを回避し、収益の減少やブランドの損傷を軽減することができます。

 | A10-GR-70361-JA-02 FEB 2024