データシート

ATLAS INTELLGENCE FEED

セキュリティーと脅威の可能性への適切な対応

考えられる全ての視点、エントリーポイント、ベクターからあなたのビジネスにもたらされる脅威の流入を考えれば、攻撃者より一歩先を進んでいる必要が本当にありますか？ コンテキスト（前後関係）は、リスクを把握し、セキュリティ運用チームの時間を優先させ、手元にある次の（多くの）脅威を判断するのに役立ちます。 適切なセキュリティインテリジェンスは、ネットワークベースの攻撃を認識しブロックするためのメカニズムの作成を促進します。 しかし、効果的なセキュリティインテリジェンスは、攻撃を特定するだけでなく、攻撃インフラストラクチャー、方法、およびその他のインジケーターを理解し、カタログ化し、広範でより積極的な対策を確実に実行できるようにします。

高度な脅威への対処

Arbor NetworksのATLAS Intelligence Feed（AIF）は、高度な脅威やDDoS攻撃を構成する各種の攻撃にすばやく対処するためのポリシーと対策を提供しています。 AIFは、ArborのArbor Security Engineering and Response Team（ASERT）による広範囲で深い研究成果を基に顧客へ直接メリットを提供するサービスです。

Arbor Networksは、エンタープライズおよびサービスプロバイダーの両ネットワーク向けに設計された優れた製品ポートフォリオを提供しており、すべての製品ががAIFを利用するメリットを得ています。新たな攻撃情報が見つかると、AIFがアップデートされ、セキュアーなSSL接続を介して最新の脅威情報と共にArbor製品へ更新情報が提供され、現行のDDoS攻撃や高度な脅威を阻止します。組織を保護する最善の方法は、熟練したエキスパートによる広範囲な視野から最新の知見を得ることです。これが、ATLASインテリジェンスフィードです。

効果的な脅威インテリジェンス・フィードのダイナミクス

脅威インテリジェンスを活用するには、3つの要件があります

- 実世界のネットワークトラフィックと脅威データの継続的な取得
- ネットワークトラフィックおよび脅威データを収集および分析するための堅牢なインフラストラクチャー
- 上記のすべてを管理し、「ヒューマンインテリジェンス」の側面を分析に付与する専任のチーム

真に卓越した脅威インテリジェンスは、単に攻撃データを収集し分析するだけではありません。セキュリティー対策プログラムへのシームレスな統合により、既存のスタッフやプロセスを大幅に改善する必要があります。つまり、その情報は実行可能でなければなりません。各脅威からのリスクは明確でなければならず、明白に行動しなければなりません。

Key Features & Benefits

精度の高い防御のための動的な更新
AIF は、最新の脅威情報によって常時更新することによって、Arbor Networks の全製品を 通して検知ポリシーの精度を常に最大限に高めています 。

キャンペーンベースの攻撃特定
マルウェアの特性に焦点をあて、各種の情報源からの攻撃データと組み合わせることよって、 AIF は攻撃ポイントのみならず、キャンペーンの一部として仕掛けられる関連する攻撃を特定します。

攻撃への迅速な対応
AIF ポリシーは、攻撃に関する経緯などのコンテキスト情報を提供することで、的確な情報に基づいた迅速な対応を可能にしています。

脅威検証と優先度付け
脅威データの収集と分析に加えて、ASERTは、脅威の現状および実態にまで踏み込んで脅威の検証と優先度付けを行います。

ARBOR NETWORKS
The Security Division of NETSCOUT

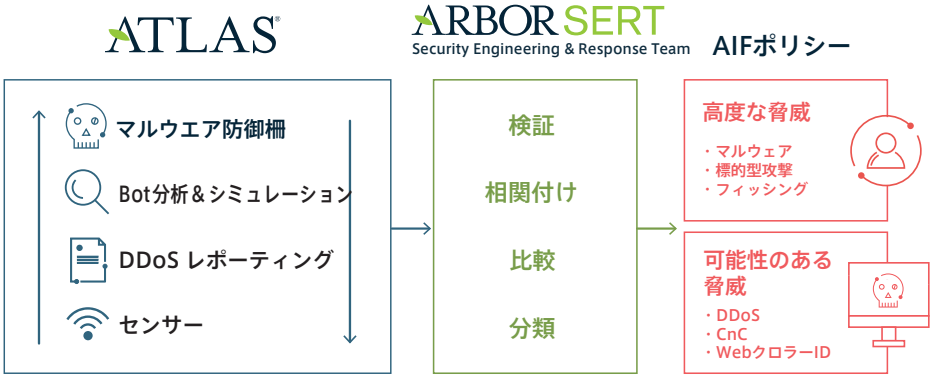

図 ：ATLAS は、さまざまなツールやプロセスを使って、脅威データを収集・解析しています。ASERTは、攻撃の能力および潜在性に焦点を絞り、攻撃キャンペーンの複数の兆候を見つけ出します。これらの兆候のインジケータが、ATLASインテリジェンス・フィードを介してすべてのArbor 製品へ提供されています。

DDoS やボットネットから企業を防御するAIFの特長

AIFは、Arbor Networksの顧客によってその有効性が実証されています。大規模化・巧妙化する標的型・複合型の高度な脅威を防御しています。

さらに正確に脅威を検出するために、AIFは次のことを可能にします

- 攻撃のボリュームを問わず、ボリュームしきい値に達する前に、脅威を特定
- 信頼性に応じてさまざまなレベルの防御を適用
- 数百万ものマルウェア・サンプルを使って制御下で試された検証に基づいて、攻撃
- インテリジェンスを適用
- ボットネット関連のすべてのマルウェアにほか、特定のマルウェアのリバース・エンジニアリングに対応
- Arborのグローバルなセンサー・ネットワークを活用して、インターネット上の脅威を24時間体制で監視
- 継続的に、ボットネット、そのロケーションおよび攻撃方法を時系列に追跡管理
- ATLASは 、匿名のトラフィック・データをArbor Networksと共有することに同意していただいた 300社を超えるお客様との共同プロジェクトであり、全インターネット・トラフィックの約 3 分の 1 に相当するデータを収集しています。

世界にまたがるArborのセキュリティ調査チームは、新たに発生するインターネット脅威の発見と分析に加え、ターゲットを絞った防衛策の開発に専念しています。 Aroborは、攻撃データ収集、パートナーからの情報、および分析ツールからの情報を高度に組み合わせて、脅威を検出するだけでなく情報に基づいた攻撃緩和策を決定するのに必要なコンテキストなどを組み合わせてAIFポリシーを作成します。

AIFを支える主要技術のひとつにArborのダイナミックなレピュテーション・インテリジェンス（信用度の評価）があります。レピュテーション・インテリジェンスは、AIFポリシーを構成する脅威指標に正当性を与えます。 ASERTはトラフィックと脅威情報を収集するために、特定のマルウェアが脅威となる可能性のある他の種類の脅威を含め、脅威のさまざまな要素を組み合わせることができます。しかし、まだ具体化されていない脅威に対処するのを避けるために、レピュテーションインテリジェンスでは、特定のIP、DNS、またはURLがいつどのくらいの期間、障害が起こったかを明確かつ実証的に証明しています。信頼性スコアリングによって、攻撃の検証が関連するAIFポリシーに追加されます。この種の攻撃の検証は、アーバーの製品に提供される各AIFポリシーに信頼スコアの形で提供されるため、ユーザーは製品によって特定された脅威が重要かつ実在することを確信することができます。

ATLASインテリジェンスの適用

アーバーネットワークスのポートフォリオに含まれる各製品は、AIFを利用するように設計されていますが、フィードのさまざまな部分によって製品内のさまざまな動作を通知します。いくつかの製品はNetFlowを分析し、ネットワークパケットを調べる製品もあります。 AIF内のポリシーには各製品の関連情報が含まれます。

Arobor Networks® APS

APSは、帯域幅のしきい値に基づいて可能性のある脅威をブロックするだけでなく、AIFポリシーを使用して、アプリケーション層を狙った「ローアンドスロー(低帯域幅・低速度)」攻撃を含む複数の種類のDDoS攻撃を識別します。さらに、AIFは、APSがボットネットの特定のカテゴリを検出して停止させ、ネットワークを危険にさらすのを防ぎます。これらの可能性のある攻撃とボットネットの脅威がネットワークに侵入するのを止めることによって、他のセキュリティーデバイスが実行すべき動作を不要にします。

Arobor Networks® Spectrum

SpectrumのATLASセキュリティーインテリジェンスにより、フォレンジック分析のための攻撃イベントを丹念に調査することができます。 AIFで提供される攻撃インジケーターは、攻撃がネットワーク上でどのように発生もしくは発生の可能性があったか、およびその広がりを特定することができます。さらに、この脅威情報を組織内の最も重要な資産との間で送受信されるトラフィックとオーバーレイすることができるため、詳細な調査に向けたイベントのエスカレーションに役立てることができます。

Arobor Networks® SP

AIF からのセキュリティ·インテリジェンスによって、SP の顧客は社内または顧客へのサービスに影響が出る前に大規模 DDoS 攻撃を迅速に検知することが可能になります。

Arobor Networks® TMS

TMS で使用する AIF ポリシーは、DDoS 攻撃をすばやく確実にブロックするための詳細情報を提供します。悪意ある攻撃は多大なコストを伴うダウンタイムを発生させる可能性があり、これをブロックするにはこの正確さが不可欠です。この AIF は、Cisco ASR 9000 vDDoS 防御製品にも同一レベルの防御を提供しています。

ATLAS インテリジェンス・フォード（AIF）の詳細

AIF には 2 つのサブスクリプション（スタンダードとアドバンスド）が用意されています。この 2 つのサブスクリプションによって、自社のニーズに合った攻撃検知/防御レベルを選択することができます。

AIF スタンダード

スタンダード·フィードによって、マルウェアやボットネット、サービス拒否（DoS）など、企業を標的とする今日の最も一般的な攻撃を検知し、これに対処できます。ポリシーと防御策は常時アップデートされ、新しい攻撃の情報を入手できるため、広範囲の正確な検知が可能になります。このフィードに含まれるポリシーおよび防御策の例は以下のとおりです。

	脅威ポリシーのタイプ		APS	Spectrum	SP	TMS+
コマンド&コントロール	·ピアツーピア ·HTTP ·IRC		✓	✓	✓	
DDoSレピュテーション脅威	·攻撃者 ·標的		✓	✓	✓	
マルウェア	• Webshell • ランサムウェア • RAT • 偽装アンチウイルス • バンキング • 仮想通貨 • スパイウェア • ドライブ·バイ • ソーシャルネットワーク	• DDoS ボット • ドロッパ • 詐欺広告 • ワーム • 認証情報窃盗 • バックドア • エクスプロイトキット • POS • その他	✓	✓	✓	
IP地理ロケーション	• インバウンドのソースに対して国別にケーションを特定 • アウトバウンドトラフィックのデスティネーションに対して国別にロケーションを特定		✓	✓	✓*	✓*
DDoS RegEx	• ATLASから入手したIPアドレスに基づいてDDoS 攻撃者を特定 • ATLAS HTTP Flooderから入手した兆候に基づいてDDoS 攻撃者を特定		✓			✓
Webクローラーの特定	既知の検索エンジンからの Webサービスへのインバウンド接続を特定		✓			
ETPro(SA導入時の基準)	IDSシグニチャー			✓		

図 ：AIF スタンダード · フィードを使って特定された脅威の例すべての防御策およびポリシーは常時アップデートされるため、上記のリストは随時変更されます。

高度な脅威への取り組みにおけるArbor独自のポジショニング

Arbor は、長年にわたり、ボットネットに関する調査研究やDDoSミティゲーションに取り組んできました

DDoSは日々進化しています。サイバー犯罪や APT 攻撃に用いられるマルウェアやボットネットのいわば分派から主力の攻撃となっています。この中、ArborはASERTチームとそのリサーチ力を拡張し、新たに生まれる脅威を特定し、分析してきました。ASERTの脅威インテリジェンスへのアプローチには、脅威の特定を支援するだけではなく、その蔓延度や重大度を確認するなどの、次のような各種の要素が含まれています。

- Red Sky Allianceなどの有用なパートナーシップ。これを通じて、2,300 万台以上のPCにアクセスし、その徹底解析よって集積された脅威インテリジェンスを活用
- Red Sky Allianceから入手した実環境でのインジケータに基づいて攻撃キャンペーンを追跡するとともにレピュテーション監視を実施
- 外部パートナーのテクノロジーと自社構築のる分析/プロセスの両方から構成される高度なマルウェア分析バックエンド・システムを活用

これらの脅威データと分析を活用して、ASERTがAIFを作成します。Arborのお客様はこれを使用して、自社のネットワークやその周辺で発生するイベントを検知することがかのうです。ネットワークに関するミクロな視点と、ATLASポータルを介して提供されるグローバルなインターネット・トラフィックに関するマクロな視点を組み合わせ活用することにより、高度な脅威への対処における優位性を手にすることができます。

* 製品パッチを介してSP、TMSおよびCisco ASR 9000 DDoS防御製品にアップデートされるIP地理ロケーション

** TMS内で使用されるAIFポリシーは、Cisco ASR 9000 DDoS防御のためのものと同一です

AIF アドバンスト

アドバンストAIFは、検知が困難なステルス型の攻撃が懸念される場合に最適です。このフィードのサブスクリプションを利用すれば、スタンダード·フィードに含まれるすべての防御策およびポリシーのほか、キャンペーン型の持続的な攻撃などの攻撃パターン（特定の企業を標的とし、高度にカスタマイズされている上に、正規のアクセスに見えるために検知が困難）を発見するための追加ポリシーをご活用いただけます。このサブスクリプションに含まれる防御策とポリシーの例は以下のとおりです。

	脅威ポリシーのタイプ	APS	Spectrum	SP	TMS+
ロケーションに基づく脅威	• トラフィック匿名化サービス • TOR • プロキシー • シンクホール • スキャナー • その他	✓	✓		
メール脅威	• スパム • フィッシング	✓	✓		
標的型攻撃	• APT • ハクティビズム • RAT • ウォータリング·ホール • ルートキット	✓	✓		
モバイル	• モバイル C&C • スパイウェア • 悪意あるアプリ	✓	✓		

図 ：AIF アドバンスド・フィードを使って特定された脅威の例すべての防御策およびポリシーは常時アップデートされるため、上記のリストは随時変更されます。アドバンスド・サブスクリプション内のポリシーは、現在、SP、TMSまたはCisco ASR 9000 DDoS 防御では利用することができません。

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

DS/AIF/JA/1117-A4

米国本社
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

アーバーネットワークス株式会社
〒101-0063
東京都千代田区神田淡路町2-105
ワテラスアネックス13階
TEL: 03 3525 8040
EMAIL: japan@arbor.net
WEB: jp.arbornetworks.com