＊本資料は、2014 年 4 月 2 日に米国で発表されたプレスリリースを翻訳したものです。

報道関係各位

2014 年 4 月 14 日
アーバーネットワークス株式会社

Arbor Networks 独自のグローバルな攻撃インテリジェンスがローカルな保護と統合

Pravail® ソリューションに組み込まれているセキュリティ・リサーチ機能と
新しいインテリジェンス・フィードを発表

米国マサチューセッツ州バーリントン－エンタープライズやサービス・プロバイダのネットワーク向けに分散型サービス拒否（DDoS）攻撃や高度な脅威の対策ソリューションを提供するリーディング・プロバイダ Arbor Networks, Inc.（以下「Arbor Networks」）は、本日、ATLAS®インテリジェンス・フィード（AIF）サービスの一環として新しいレピュテーションベースのスレット・フィードを発表しました。AIF はセキュリティ・ポリシーのリサーチ主導フィードであり、実際の攻撃の活動、レピュテーション、および挙動に基づいた脅威の識別により Arbor Networks の Pravail 製品を素早く正確に更新することを目的としています。

AIF を導入するこの時代、組織は自社ネットワークをターゲットにしたさまざまな脅威に対する対策の不足を感じています。最近公開された、Arbor Networks の依頼により Economist Intelligence Unit が情報セキュリティ最高責任者（CISO）および IT 担当企業幹部に対して実施した世界的な調査によると、インシデントへの対策が万全であると考えている企業は、全体の 17%に過ぎません。『Cyber incident response: Are business leaders ready?（サイバー・インシデントへの対応：ビジネス・リーダーの準備は万全か？）』と題されたレポートでも、ビジネス・リーダーの 41%が、潜在的な脅威に対する理解が深まれば、脅威への対策がより万全に感じられると回答したことが明らかになっています。ATLAS インテリジェンス・フィードは、ビジネス・リーダーが求める視認性と脅威の前後関係に関する、この問題への対処に役立ちます。

動的かつグローバルな攻撃インテリジェンス

Arbor Networks は、ATLAS を中心とする大規模でグローバルなインテリジェンス・ネットワークを作り上げています。ATLAS は 300 社近くのサービス・プロバイダ顧客との比類のない協力関係により実現されたシステムであり、サービス・プロバイダの合意に基づき、Arbor Networks と匿名のトラフィック・データを共有しています。合計 80 Tbps に上るこの大量のトラフィック・データ・セットに加えて、ダーク IP アドレス空間内にセンサーを持つグローバルなハニーポット・ネットワークから収集した情報や、Red Sky Alliance などの戦略的パートナーシップも併用しています。

この豊富なデータ・セットは、Arbor Networks のセキュリティ・エンジニアリングおよびレスポンス・チーム（ASERT）が実施する継続的な調査・分析により、実施可能なインテリジェンスに変換されます。ASERT はセキュリティ業界で最大級の専門リサーチ組織であり、Fortune 25 コンピュータ緊急対応チーム（CERT）、以前の法執行機関、スレット・ミティゲーション・ベンダー、有名なマルウェア研究者など、多様な専門分野を持つ 25 人のセキュリティ・アナリストが所属しています。ASERT がセキュリティの視点から攻撃動向を把握し、マルウェア・インデックス用およびボットネット・シミュレーション用のカスタム・ツールを活用して開発したお客様向け脅威インテリジェンスには、特定の脅威を検知・阻止してセキュリティ対応状況を強化し続けるために必要な、セキュリティの状況が含まれています。

Arbor Networks のセキュリティ・リサーチ・ディレクター（Director of Security Research）であるダン・ホールデンは、「多くのベンダーは、攻撃を特定して、このような攻撃の識別とブロックが可能なシグニチャを作成できますが、これは時代遅れで消極的なアプローチです。ASERT は、攻撃を特定するだけでなく、攻撃のインフラストラクチャや手段を分析してカタログ化し、お客様がより積極的なセキュリティ・ポリシーを導入できるようにしています。重要なのは状況です。単体のボットネットやマルウェアだけを見るのではなく、ボットネットやマルウェア・ファミリー全体のリバース・エンジニアリングを行っています」と語っています。

ASERT は Arbor Networks 製品を更新するだけでなく、このオペレーション・インテリジェンスを世界中の数百もの国際的な CERT や数千もの通信事業者と共有しています。ASERT 独自の知見と分析の例については、チームのブログ（英文）をご覧ください。最近公開された調査では、販売時点管理（POS）マルウェア、NTP 反射/増幅 DDoS 攻撃、Zeus Gameover バンキング・トロイなどについて詳しく取り上げています。

真のレピュテーション分析により強化された ATLAS インテリジェンス・フィード

ASERTは、アドバンスト・パーシステント・スレット、地政学的なキャンペーン、金融詐欺、およびDDoSに焦点を絞って、毎日およそ 100,000 件以上のマルウェアのサンプルを ATLASやその他のソースから収集しています。収集されたマルウェアのサンプルは、自動化された脅威解析システムによって分類され、特異な攻撃は、数百万件に及ぶこのような解析結果のデータベースに保管されます。新たなボットネットやアプリケーション層への攻撃が検知されると、攻撃のポリシーが作成され、ATLASインテリジェンス・フィードを経由してArbor NetworksのPravail製品に配布され、インストールされます。

シグニチャを使用してポリシーを作成する他の多くのソリューションとは異なり、ASERT は実際のマルウェアのリバース・エンジニアリングとボットネット分析に基づいてレピュテーション・ポリシーを割り当てます。ASERT はシグニチャや一般的に使用されている業界リストだけに頼るのではなく、全面的に依拠できる非常に信頼性が高い脅威識別技術を構築しました。ASERT は、数十万件に上るマルウェアのサンプルやその他の脅威インテリジェンスからセキュリティ・データを収集しています。データと兆候の分析には、外部パートナーの技術と社内構築による分析・プロセスの両方からなる、特許申請中の高度なマルウェア分析バックエンド・システムを使用します。この分析から、IP アドレス、ポート、ドメイン名、URL、正規表現など、攻撃の主な兆候を抽出します。最も包括的な分析を行うために、ASERT は特定した攻撃の兆候を他の業界レポートや Red Sky Alliance のデータと比較します。その後、これらの兆候をポリシー別に分類・カテゴリ化します。ポリシーは、ATLAS インテリジェンス・フィードを経由して数日間隔で Pravail アプライアンスにアップロードされます。AIF は Pravail 用セキュリティ・データのバックボーンを提供しており、優先順位付けや対策の実施に役立つ貴重な詳細情報を含め、攻撃活動を迅速に検出できます。

Arbor Networks の Pravail 製品ファミリー

IDC のセキュリティ製品担当リサーチ・マネージャであるジョン・グレイディ氏は、「各組織は自社ネットワーク内に潜む高度な脅威の問題への対処に役立つソリューションを求めています。Arbor Networks は、NetFlow、パケット・キャプチャ、および ATLAS インフラストラクチャによるグローバルな脅威インテリジェンスをユニークに組み合わせたソリューションを提供しており、シグニチャベースのソリューションをくぐり抜ける昨今のダイナミックな脅威に対処しています」と語っています。

ATLAS と ASERT の知識と専門技術に裏付けられた Arbor Networks の Pravail 製品は、高度な脅威や DDoS 攻撃から企業を保護するように設計されています。

- Pravail® ネットワーク・セキュリティ・インテリジェンス（Pravail NSI）は、セキュリティ展開の中枢として機能します。Pravail NSI はネットワーク内に実装され、ネットワーク全体におけるネットワーク・トラフィックのパターンやセキュリティ・イベントに関する情報を収集し、攻撃や違反が行われていることを示すイベントについてセキュリティ・チームにアラートを送信します。Pravail ネットワーク・セキュリティ・インテリジェンスは、高度なマルウェア脅威や、内部からのネットワークの不正使用や悪用による、またはネットワークに接続し感染しているモバイル・デバイスを経由した盗難や損失から、お客様が知的財産およびデータを防御できるようにします。

- Pravail Security Analytics は、大量のデータに意味のある前後関係を与えることで、セキュリティ・チームがごく一部の重要なデータに的を絞ってより素早く対応し、自社ネットワーク環境内に潜んでいる脅威が業務に影響を与える前に、その脅威を特定できるようになります。Pravail Security Analytics は、リアルタイムな攻撃への対応決定に利用できるほか、データを将来の確認のため保存することで、最新の脅威インテリジェンスを使用して以前は検出されなかった攻撃を特定できるようにします。また、Pravail Security Analytics を利用するお客様は、フォレンジック分析を行うことで、コントロールの効果の特定、セキュリティの強化、さまざまな法令遵守の要件への対応が可能になります。

- 既存のデータセットを活用した Pravail Security Analytics クラウド・ソリューションの無料デモンストレーションが用意されています。ユーザーはこれを利用してソリューションを試用し、その強力な機能を実際に体感してみることができます。クラウド・ソリューションの無料トライアルも用意されているため、自社のネットワーク・パケット・キャプチャを脅威、異常、誤用などについて素早く分析できます。無料トライアルでは、30 日間で最大 1GB のデータをアップロードできます。

- Pravail 可用性防御システムは、アプリケーションやサービスの可用性への脅威から企業の境界領域を安全に守ることを支援します。特に、Pravail 可用性防御システムはアプリケーション層 DDoS 攻撃からの企業の防御に役立ち、事前設定やユーザーの操作なしでただちに攻撃を阻止するよう設計されています。この製品は、DDoS 攻撃認識機能とミティゲーション機能を利用でき、攻撃を受けている最中でさえ速やかに導入できます。

Arbor Networks について

Arbor Networks は DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービス・プロバイダのネットワークを安全に守ることを支援しています。Arbor Networks は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューションプロバイダです（Infonetics Research 社調べ）。高度化する脅威に対する Arbor Networks のソリューションは、パケットキャプチャと NetFlow 技術を組み合わせることで、ネットワーク全体を可視性し、マルウェアや悪意のあるインサイダーの脅威を迅速に検出し、削除することを可能にします。Arbor Networks はまた、動的なインシデント対応、履歴分析、視認性、フォレンジクスについても市場をリードする分析機能を提供しています。Arbor Networks は、企業のネットワークやセキュリティの担当者がセキュリティのエキスパートになり、企業のセキュリティ強化を実現することを目指しています。Arbor Networks の目標は、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるよう、ネットワーク上の脅威の視認性とセキュリティ・インテリジェンスの提供を可能することです。

Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイト www.arbornetworks.com/jp/ を参照してください。また、業界唯一の革新的なインターネット監視システ

ム ATLAS®のデータに基づく調査、分析および知見については、ATLAS セキュリティポータル（英文）をご覧ください。