WHITE PAPER

APPLICATION AND THREAT INTELLIGENCE RESEARCH CENTER

ラップシート分析システムを備えた最新のセキュリティインテリジェンス

サイバーセキュリティは、現在、世界中の企業における最優先事項の1つです。セキュリティ侵害事件が増え、さまざまな企業が脅威にさらされる中、ネットワーク/セキュリティ管理者は、常に警戒しなければならない状況に置かれています。幸いにもこのリスクに対応するツールは、増え続けており、イクシアのApplication and Threat Intelligence（ATI）リサーチセンターも企業のセキュリティーの改善のために取り組んでいます。

イクシアのATIリサーチセンターは、10年以上前から高度なセキュリティリサーチを行い、世界のあらゆる業界のお客様に最新のインテリジェンスをお届けしています。最新のアプリケーションシグネチャーは、イクシアのBreakingPoint™やPerfectStorm™などの製品をお使いのお客様がディープパケットインスペクション（DPI）ソリューションやアプリケーションサーバーのパフォーマンスを検証する際にご利用いただいています。イクシアのネットワーク可視化製品をご利用の場合は、同じシグネチャーで特定アプリケーションの認識がピンポイントで可能となります。ライブマルウェア、ボットネットパターン、新しい攻撃、不正行為者の位置などの脅威情報は、セキュリティ機器の保護の検証に利用されています。

イクシアのThreatARMOR™もATIリサーチセンターの情報をお客様に提供し、既知の脅威や信頼できない国からの通信を排除することで、セキュリティインフラや運用チームの効率改善をサポートしています。本ホワイトペーパーでは、イクシアがATIリサーチセンターを通じて世界中の脅威に関するリアルタイム情報をどのように収集、検証し、配布しているかをご紹介します。

ラップシートがネットワークリスクを説明

ThreatARMORが既知の不正サイトに出入りするトラフィックをブロックするたびに、そのIPアドレスを不正と判断した理由を記載したラップシートが作成されます。これによりお客様が、自社ネットワークが直面するリスクを詳細に理解でき、誤検出のリスクもなくなります。

ThreatARMORは、そのサイトで悪意ある活動や犯罪行為があることをATIリサーチセンターが100%確信した場合に限り、IPアドレスをブロックします。そしてラップシートにその証拠が残ります。ラップシートにて、各脅威のURL情報、そのマルウェアのバイナリチェックサム、フィッシングページのスクリーンショット、マルウェアのインストーラ、悪意ある活動が最後に確認された日付などの情報を提供します。

「世界中の脅威に関するリアルタイム情報」

図1: ラップシート例

ラップシートの情報を収集、分析、検証、配布するため、舞台裏で多くの作業が行われています。生の入力データはさまざまなソースから得られます。

既知の不正サイトに関するデータ

疑わしいサイトに関するデータは、以下のように複数の異なる経路からシステムに入ります。

- ソースフィード
- インターネットスキャン
- ハニーポット
- SPAM
- バイナリ分析
- サンドボックス

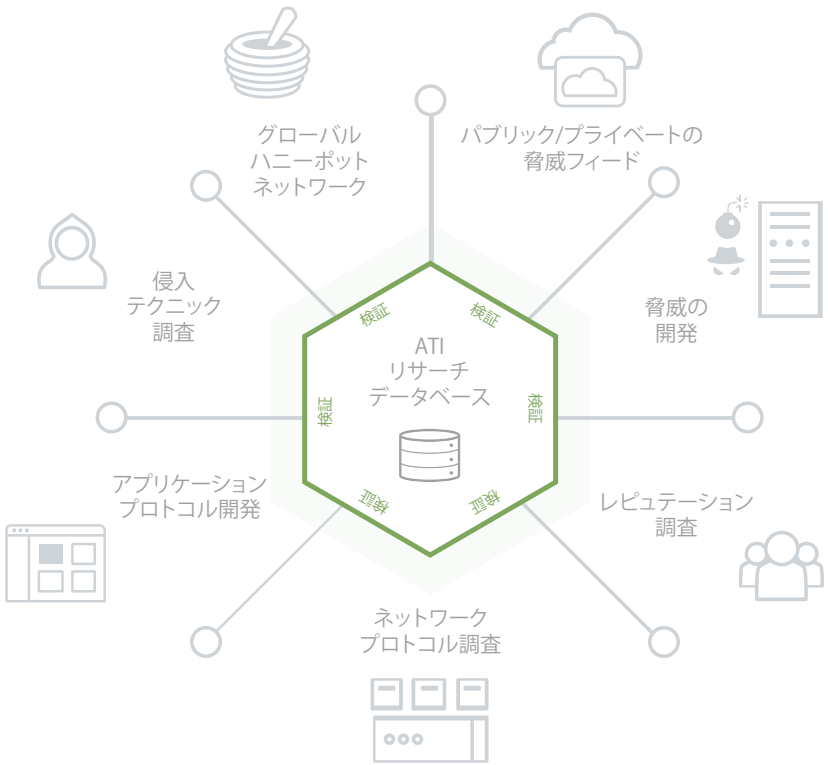

図2: ATI リサーチセンター

ソースフィードは、商用の脅威情報フィードを含め、さまざまなパブリック/プライベートストリームから収集されます。検証を加えずに利用するユーザーやセキュリティベンダーもいます。ATIリサーチセンターもオープンソースコミュニティやさまざまなセキュリティパートナーシップからフィードデータを収集しています。もちろん、これらのフィードからのデータは容疑者と見なされ、ATIリサーチセンターが個別に検証するまで犯罪者とは扱われません。

インターネットスキャンとは、主に注意を引くサイトを探してインターネット上を歩きまわることです。疑わしいサイトを特定するため、24時間年中無休で自動的に行われます。システムが、マルウェアのバイナリなど悪意ある活動の証拠を即座に発見する場合もあります。それらのサイトは自動的にスキャンされ、カタログ化された上で、ラップシートデータベースに追加されます。悪意あるコンテンツはないがパッチを適用していないWebサーバーソフトウェアなど既知の脆弱性を持つサイトが見つかる場合もあります。このような脆弱性を持つサイトはすぐに侵入される可能性が高いため、頻繁な再スキャンの特別キューに組み込まれます。

ハニーポットは、脅威情報収集の定番です。ATIリサーチセンターは、SSH、 FTP、 RDP、VoIP、 HTTP などのサービスを利用できるサイトのグローバルネットワークを持っています。これらのサービスへのアクセスはすべて記録され、ネットワーク内の他のポイントで収集したデータと相互参照されます。これにより、脆弱なサーバーを探すインターネットスキャンサイトが特定されます。それらは頻繁に位置を変える可能性があるため、その活動を検出するには大型でグローバルなネットワークを持つことが重要となります。

SPAMも、ATIリサーチセンターが分析と検証のための入力収集に利用するリソースです。イクシアは、さまざまな商用フィードや内部フィードから収集したSPAM情報を学習エンジンに入力します。SPAMメールの多くはハイパーリンクを組み込み、正当に見せかけた悪意あるWebサイトに無警戒のユーザーを誘導します（「取引パスワードを更新するにはこちらをクリック！」など）。そしてアクセスと同時にマルウェアをユーザーのシステムにプッシュします。イクシアは、このようなリンクをたどり、ユーザーがフィッシングサイトから保護されるよう、悪意あるコンテンツにつながる発見済みのバイナリがないか分析します。フィッシングサイトと確認すると、サイトのスクリーンショットを撮ってラップシートに保存します。フィッシングサイトの調査は、自動化が難しい作業の1つです。このためATIリサーチチームは、手作業でサイトを入念に確認しています。

バイナリ分析は、多くの場合、サイトが悪意ある活動を行っているかどうかを判断する最終的な手段となります。ThreatARMORは、ブロックするサイトを厳しく選択し、悪意ある活動が完全に証明されたサイトのみ接続を禁止します。ATIリサーチセンターは、各ターゲットバイナリについて何十もの静的および動的な（サンドボックスとも呼ばれる）分析を実行します。静的分析では、ファイル自体を分析して既知のマルウェアサンプルのバイナリ内に既知のシグネチャーを探します。サンドボックスでは、実行中のバイナリを調査してバイナリが行うシステム呼び出しやネットワーク呼び出しに特に注意を払います。システムファイルへのアクセスや変更、既知の不正サイトへのネットワーク接続、他のファイルやバイナリのインストールは、悪意ある行動の典型的な兆候です。バイナリがインストーラを起動すると、スクリーンショットがラップシートに保存されます。もちろん、バイナリに悪意があると確認できれば、それが起動するネットワーク接続の調査と記録を行い、それらの接続の行先をすぐに不正サイトの候補リストに追加します。

候補に挙がったIPアドレスは、ソースに関係なく、個別に検証されるまでATIデータベースに追加されません。つまり、ThreatARMORには調整が不要であり、信頼スコアもありません。100%確実でなければブロックされないからです。同じATIフィードはイクシアのPerfect StormおよびBreakingPoint製品にも使用されるため、それらの製品で悪意があるとマークされているIPアドレスは100%確実に悪意があります。

Webサイトの中には、有効なページと悪意のあるページの両方が複数のドメインに分散するものもあります。コンテンツデリバリネットワーク（CDN）やホスティング環境にはよくあります。この場合、ATIリサーチセンターは、サイトをブロックする・しないのどちらがユーザーにとって有害かを判断する必要があります。CDN、Dropbox、Amazon Web Services、Azureなどミッションクリティカルなサイトは、たとえ一部のIPアドレスに悪意ある活動が見られても許可されます。しかし、ThreatARMORはファイアウォールやアンチウイルスシステムの代用としては設計されていません。多くの既知の不正サイトをブロックすることによって防御専用ツールの負担を緩和し、それらが新しい攻撃を見逃す可能性を低減することが、ThreatARMORの目的です。

ATIチームは、ブロックするデータベース内の各IPアドレスを少なくとも1日に1回、あるいはそれ以上の頻度で再調査しています。悪意的な活動がなくなったサイトは、データベースから積極的に削除します。削除の基準はさまざまな要因で調節されますが、標準的には最後の検出から約3日で削除されます。もちろん、マルウェアの配布が観察されたサイトが再度感染することは珍しくありません。このため、ブロックするデータベースから削除した後も頻繁に再感染がないかスキャンします。サイトの中には、ハイジャックされたり、侵入されて悪用されたもの、悪意のある行為者が所有していて特定のマルウェアキャンペーンの終了とともに使用されなくなったものもあります。いずれにしても、ブロックするデータベースを何度も出入りするサイトは珍しくありません。

このような調査の目的は、ネットワークを出入りしようとする悪意ある接続をブロックすることだけではなく、ユーザーのネットワークがどんな脅威に直面しているか、なぜ特定のサイトがブロックされているかについて有用な情報を提示することです。情報はラップシートの形でユーザーに提示され、起動するネットワーク接続を記録すると同時に、接続先は即座に不正サイトの候補リストに追加します。

ブロックするIPアドレスは個別に検証されています。

ラップシートに見られる5つのカテゴリー

ラップシートは以下のカテゴリーに分かれています。:

マルウェア

このカテゴリーには、さまざまな形の悪意あるソフトウェアが含まれます。多くのマルウェアのインスタンスは、シグネチャーベースの検出システムから逃れるため、毎日変形したり、再生成されたりしています。ThreatARMORは、既知の不正サイトからのダウンロードをすべてブロックし、シグネチャーに依存しません。

THREATARMORは、シグネチャーに依存しません。

フィッシング

フィッシングとは、無警戒のユーザーに正当を装ったメールを送り、メールに組み込まれているリンクをクリックさせる攻撃です。フィッシングメールは通常、ユーザーの雇用主や銀行など正当な送信者から送られているように見えます。受信者がリンクをクリックすると、個人情報の入力を求めたり（「社会保障番号を入力して、銀行手数料の返金を申請してください」など）、システムにマルウェアをプッシュしたりします。データベース内のフィッシングサイトをブロックすることにより、ThreatARMORはユーザーをフィッシング攻撃から保護します。

ボットネット

ボットネットとは、感染した多数のホストによる組織的な攻撃です。各ホストは悪意のあるキャンペーンに参加していることを知らず、ボットネットの「ハーダー」または「コントローラー」に操られています。ボットネットコントローラーは、「Command and Control（C2）」接続で感染ホストと通信します。この接続はIRC、HTTP、DNSなど多くの一般的なプロトコルで送信され、たいていは検出されないよう暗号化されています。ボットネットコントローラーは感染ホストにコマンドを送信し、機密データをリークさせたり、他のマルウェアをダウンロードさせたり、DDoS攻撃で他の標的を攻撃させたりします。ThreatARMORは、ATIデータベースにあるすべてのボットネットコントローラーとの接続をブロックすることにより、C2接続を阻止し、感染ホストによるコマンドの受信や個人/企業データのリークを防止します。また、社内のどのホストがボットネットコントローラーと通信していてクリーンアップが必要かを特定します。

エクスプロイト

ハッカーは、脆弱性のあるホストを見つけるため、頻繁に大規模な偵察を行います。HTTP/HTTPS、SSH、VoIP、RDP、VPNなど、多くのサービスはビジネスのためにインターネットで公開する必要があります。これらのサービスを宣伝するソフトウェアパッケージには脆弱性が発見されており、ハッカーは常に脆弱性のあるサービスを実行するサイトを探しています。ATIリサーチセンターは、一般的なサービスを宣伝するハニーポットのグローバルネットワークを利用し、接続を監視しています。これらのサービスに接続しようとしたサイトはカタログ化し、分析によって組織的なスキャンを実行していることがわかれば、ブロックするデータベースに追加します。

ハイジャック

IP範囲がハイジャックされるとは、通常、インターネットのバックボーンルーターにあるルーティングテーブルの破壊によって、特定の範囲のIPが正当な所有者から盗まれることです。ハイジャックされたIPは、フィッシングやマルウェア配布などの悪い目的に利用されます。このテクニックはIPレピュテーションやURLフィルタリングに依存したセキュリティソリューションをすり抜けることが珍しくありません。ハイジャックされるまで、長年、正当に使用されてきたドメインやIPアドレスだからです。ATIリサーチセンターは、ハイジャックされた何百万ものIPアドレスをインターネット上で継続的に追跡します。それらのアドレスが関与する接続は、当然ながら正当なネットワーク所有者のものではないため、ThreatARMORがすべてブロックします。

インターネット上では何百万ものIPがハイジャックされています。

まとめ

ATIリサーチセンターは、検出機能と分析機能を常に進化させるとともに、インターネット上で悪意あるホストを検出するセンサーネットワークを拡大しています。ATIのデータベースは、新しい脅威が検出されるとリアルタイムで更新され、クリーンアップ済みのサイトは削除されます。ThreatARMORデバイスも5分ごとにATIクラウド経由で更新されます。ATIリサーチセンターの検出、収集、分析機能は、ThreatARMOR、BreakingPoint、ATIプロセッサなど多くのイクシア製品を強化しています。それらの機能はThreatARMORを通じてユーザーをさまざまな攻撃から守り、ファイアウォール、SIEM、IPS/IDSシステムやそれを運用するチームの貴重なリソースを節約することにより、ネットワークのセキュリティを高め、運用チームを効率化しています。

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805

WWW.IXIACOM.COM

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44 1628 408750
(FAX) +44 1628 639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127