コンテンツ向け Cisco AMP（高度なマルウェア防御）

Cisco の高度なマルウェア防御（AMP）は、攻撃の一連のサイクル（攻撃前、攻撃中、攻撃後）をカバーする、唯一の高度マルウェア防御システムです。これは、Cisco E メール セキュリティ アプライアンスおよび Cisco Web セキュリティ アプライアンス上でシスコのレトロスペクティブ セキュリティ機能をサポートする、継続的かつ高度な分析を提供します。セキュリティ マネージャは、レトロスペクティブ セキュリティを使用して、過去の時点にさかのぼってシステム内の脅威を調査できます。高度な分析と集約されたインテリジェンスによって、クリーンなファイルなのか、それとも悪意のあるファイルなのかが判断されます。詳細な分析の後にファイルの要素が変更されると、アラートがトリガーされます。また、ファイル サンドボックスを使用して、非常にセキュアな環境でマルウェアを実行して分析し、その動作をテストできます。これらのレトロスペクティブ セキュリティ ツールを使用すれば、侵害が発生したときに、その範囲を特定して可視化し、制御することができます。セキュリティ チームはこれらを活用して、手遅れになる前に、迅速かつ効果的にすべての脅威に対処して修復できるようになります。

ポイントインタイム検出単独の場合の欠点

ポイントインタイム検出単独では、100 % の効果は望めません。検出を回避して環境を危険にさらすには、たった 1 つの脅威で十分です。巧妙な攻撃者は、標的型でコンテキスト認識型のマルウェアを使用します。また、ポイントインタイム防御を出し抜いて任意の組織を危険にさらすためのリソース、技能、そして粘り強さを持っています。さらに、ポイントインタイム検出は、脅威が発生した後では、どこまで侵害されているのか認識できません。

コンテンツ向け AMP の機能

コンテンツ向け Cisco AMP は、次の 3 つの重要な機能をベースにしています。

- ファイル レピュテーション：AMP は、各ファイルがゲートウェイを通過するときに、そのフィンガープリントを採取します。これらのフィンガープリントは、AMP のクラウド ベースのインテリジェンス ネットワークに送信され、ゼロデイ エクスプロイトに対するレピュテーションが判定されます。
- ファイル サンドボックス：AMP は、マルウェアが検出されたときに、ファイルの動作を細部にわたって収集します。次に、収集したデータをまとめて、人間および機械で詳細に分析し、サンドボックス内でファイルの脅威レベルを判断します。
- 継続的な分析：コンテンツ向け AMP は、クラウド ベースのビッグデータ分析を使用し、長期間かけて収集された新旧のデータを絶えず再評価して、ステルス攻撃を検出します。これは、ポイントインタイム検出にはない機能です。

これらは、次に示すような各種機能をサポートします。

高度な脅威に対抗するレトロスペクティブ セキュリティ：高度な脅威および標的型攻撃を効果的に防ぐには、新しいマルウェアが見つかってから数週間、ときには数ヵ月後にリリースされるマルウェア シグネチャでは間に合いません。AMP は、これらのシグネチャに依存していません。代わりに、ファイル レピュテーションおよびファイル サンドボックスを使用し、シグネチャが存在しない場合でも、疑わしいファイルを識別してブロックします。レトロスペクティブ ファイル分析には、アウトブレイクが発生した特定の時点にさかのぼって攻撃の範囲を可視化するという、独特な機能が備わっています。

攻撃の一連のサイクルからの保護：攻撃の一連のサイクル（攻撃前、攻撃中、攻撃後）にわたって保護できます。Cisco Security Intelligence Operations（SIO）からのスパム フィルタおよびゼロデイ脅威インテリジェンスは、脅威がネットワークに侵入する前に阻止し、ファイル レピュテーションおよびファイル サンドボックスは、攻撃を行っている脅威を識別します。そして、高度なマルウェアが他の防御層をすり抜けた場合には、レトロスペクティブ分析が攻撃後の保護を担います。

可視性と制御：豊富なデータを含む扱いやすいレポートを使用して、ネットワークへの侵入を試みたファイルのレピュテーションと動作を把握できます。ネットワーク上の誰がいつ感染したかをはじめとして、要素のすべての変化がアラートとしてレポートされます。ファイル レピュテーション、ファイル動作、などのデータに基づいて、セキュリティ ゲートウェイの動作（許可、ブロック、または検疫）を定義するポリシーを設定できます。

柔軟性と選択肢：シスコの既存のセキュリティ ゲートウェイと AMP を統合すると、環境に最も適した方法で AMP を導入するためのオプションが増えるので、柔軟性が高くなり選択肢が増えます。シスコの Web セキュリティおよび E メール セキュリティの追加ライセンス機能として AMP をアクティブ化すれば、高度マルウェア防御を最も簡単かつコスト効率の高い形で導入できます。

レトロスペクティブ セキュリティ：レトロスペクティブ セキュリティとは、過去にさかのぼって、プロセス、ファイル アクティビティ、および通信をトレースする機能です。これにより、感染の全体像を把握して根本原因を明らかにし、修復を実行できるようになります。イベント トリガー、ファイル要素の変更、IoC トリガーなど、侵害の痕跡が見られたときに、レトロスペクティブ セキュリティの必要性が生じます。

利点

- ファイル内のマルウェアの正確な検出
- 未知のゼロデイ脅威の発見
- 最初の防御を突破したマルウェアの検出と無効化

集約されたセキュリティ インテリジェンス

Cisco SIO の集約されたセキュリティ インテリジェンス、および Sourcefire の脆弱性調査チーム（VRT）は、リアルタイムの脅威インテリジェンスの膨大なコレクションとなっています（Sourcefire は現在シスコの一部です）。このコレクションには、世界中に分散された 160 万のセンサーが含まれています。シスコは、1 日あたり 100 TB のデータおよび 180,000 のファイルを受信しています。また、世界中の E メール トラフィックの 35 % を監視する能力があります。600 名を超えるエンジニア、技術者、および研究者が、40 を超える言語で 365 日 24 時間体制で活動しています。これらのスタッフは、情報を分析することに加えて、公開および非公開で脅威に関するフィードを提供しています。また、Sourcefire Awareness, Education, Guidance, and Intelligence Sharing（AEGIS）プログラムへの参加に加え、FireAMP™、Snort、および ClamAV コミュニティとの継続的な交流も、脅威インテリジェンスおよび修復のベスト プラクティスの共有に役立っています。シスコには、将来の攻撃に対する防御体制が整っています。

シスコが選ばれる理由

シスコには、統合された高度マルウェア防御ソリューションの幅広いポートフォリオがあります。継続的な可視性と制御をお客様に提供し、攻撃の一連のサイクル（攻撃前、攻撃中、攻撃後）を通じ、ネットワーク全体でマルウェアを無効化します。AMP は、Cisco E メール セキュリティおよび Cisco Web セキュリティ、FirePOWER® ネットワーク セキュリティ アプライアンス、モバイル システムおよび仮想システム、PC のエンドポイント保護を包括する統合機能として使用できます。また、柔軟な導入オプションを備え、広い範囲をカバーして、攻撃の侵入経路を閉ざします。

次のステップ

詳細については、Cisco AMP のホームページを参照してください。また、シスコの販売担当者、チャネル パートナー、システム エンジニアが、お客様の環境でシスコ製品からどのようなメリットを得られるかを評価するお手伝いをいたします。

C45-731873-00　05/14