セキュアなWebアプライアンスマルウェアおよびスパイウェア対策について

内容

はじめに

このドキュメントでは、Cisco Secure Web Appliance(SWA)の包括的なマルウェアおよびスパイウェア防御機能について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWA管理。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Cisco SWAは、さまざまなスパイウェアやWebベースのマルウェアに対して、堅牢で包括的なゲートウェイ防御メカニズムを提供するように設計されています。ネットワークリソースの枯渇やサポートの問題を引き起こすことで悪名高いアドウェアから、トロイの木馬、ブラウザハイジャック、ブラウザヘルパーオブジェクト、フィッシング、ファーミング、システムモニタ、キーロガー、ワームなど、さらに厳しい脅威に至るまで、さまざまな脅威に効率的に対処します。

SWAの主な差別化要因

統合レイヤ4トラフィックモニタ(L4TM)

L4トラフィックモニタは、すべてのネットワークポート（合計65,535）をワイヤスピードでスキャンし、マルウェアや不正な通信の試みを包括的に検出してブロックします。この機能は、ポート80や443などの一般的なポートをバイパスしようとするマルウェアを効果的に阻止し、不正なピアツーピア(P2P)およびインターネットリレーチャット(IRC)アクティビティも抑制します。

プロキシレイヤ処理

SWAには、キャッシュ機能とコンテンツアクセラレーション機能が統合された高性能なWebプロキシが組み込まれています。Cisco独自のAsyncOSを搭載したこのWebプロキシは、従来のUNIXベースのプロキシサーバの最大10倍の接続を管理できます。Webプロキシとして、アプリケーションレイヤでの包括的なコンテンツインスペクションを促進します。これは、Webベースのマルウェアに対する正確な防御に不可欠です。

Webレピュテーションフィルタ

業界のパイオニアであるWebレピュテーションフィルタとして、これらのフィルタは防御の追加レイヤを提供します。SenderBase®を使用して、50以上のWebトラフィックとネットワーク関連のパラメータを評価し、URLの信頼性を判断します。高度なセキュリティモデリング技術を使用して各パラメータに個別の重みを割り当て、最終的に–10 ~ +10のレピュテーションスコアを導き出します。管理者が設定したポリシーは、これらのスコアに基づいて動的に適用されます。

Dynamic Vectoring and Streaming(DVS)エンジン

DVSエンジンは、マルウェアスキャンのためにInternet Content Adaptation Protocol(ICAP)やマルチボックス展開に依存するレガシーアーキテクチャとは別に、SWA内で高速シグニチャスキャンを導入します。この最先端のプラットフォームは、高度なオブジェクト解析、ベクトル化技術、ストリームスキャン、判定キャッシングを利用し、第1世代のICAPベースのソリューションと比較して最大10倍のスキャンスループットの向上を実現します。

Ciscoアンチマルウェアシステム

このシステムは、Webrootから送信された複数のシグニチャタイプとともにDVSエンジンを活用し、多様なWebベースの脅威に対して優れた保護を提供します。脅威のスペクトルには、アドウェア、ブラウザハイジャック、フィッシング、ファーミング攻撃、およびトロイの木馬、システムモニタ、キーロガーなどの悪意のあるエンティティが含まれます。SWAは、ゲートウェイで業界最大のマルウェアシグニチャデータベースを誇り、包括的な保護を実現します。

そのため、Cisco Webセキュリティアプライアンスは、広範なWebベースの脅威からネットワークゲートウェイを保護し、堅牢な保護と高パフォーマンスのネットワークスループットを実現するリーダーとして位置付けられています。

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。