WSA Cisco Web Reputation について

内容

概要

このドキュメントでは、Cisco Web セキュリティ アプライアンス（WSA）の Cisco Web Reputation（WBRS）に関する概要について説明します。

著者：Cisco TACエンジニア、Josh WolferおよびStephan Fiebrandt

WBRSの概要

WBRSは、Webサーバの動作と特性を分析し、スパム、ウイルス、フィッシング、およびスパイウェアの脅威に対する最新の防御を提供する革新的な方法です。

WBRSは、さまざまなグローバルデータセットに関するリアルタイム分析を使用して、何らかの形式のマルウェアを含むURLを検出します。WBRSは、EメールやWebトラフィックから顧客を保護するシスコのセキュリティデータベースの重要な部分です。

SenderBaseのWBRS使用

WBRSは、世界最大の電子メールおよびWebトラフィック監視ネットワークであるシスコのCommon Security Database(SenderBase® Network)のデータを活用します。URLのレピュテーションを示す優れたインジケータである50以上の個別のパラメータを追跡します。高度なセキュリティモデリングおよびマルウェア検出エージェントを使用して、シスコはこれらの入力に基づいてこれらのURLを評価します。

パラメータには次のものがあります。

- URL分類データ
- ダウンロード可能なコードの存在
- 長い難読化されたエンドユーザライセンス契約(EULA)の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク所有者情報
- URLの履歴

- URLの経過時間
- ウイルス/スパム/スパイウェア/フィッシング/ファーミングブラックリストの存在
- 一般的なドメインのURLタイプ
- ドメインレジストラ情報
- IPアドレス情報

WBRS精度

WBRSは従来のURLブラックリストやホワイトリストとは異なり、ほとんどのマルウェア検出アプリケーションのバイナリ**good**または**bad**カテゴリの代わりに、広範なデータセットを分析して–10 ~ +10の非常にきめ細かなスコアを生成します。この詳細なスコアにより、管理者の柔軟性が向上します。異なるセキュリティポリシーは、異なるWBRSスコア範囲に基づいて実装できます。