

目次

[概要](#)

[WBRs 外観](#)

[SenderBase の WBRs 使用](#)

[WBRs 細かさ](#)

概要

この資料は Cisco Web セキュリティ アプライアンス (WSA) に Cisco Web 評判 (WBRs) の外観を提供したものです。

Josh Wolfer およびスティーブン Fiebrandt によって貢献される、Cisco TAC エンジニア。

WBRs 外観

Webサーバの動作および特性を分析し、スパムに対する戦いの最新の防御を、ウイルス提供する WBRs は革新的な方式、phishing、およびスパイウェア脅威で。

WBRs は malware の形式が含まれている URL を検出するために広大で、ダイバースで、グローバルなデータセットのリアルタイム分析を使用します。WBRs は電子メールまたは Webトラフィックからの混ぜられた脅威から顧客を保護する Cisco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 は世界で最も大きい電子メールおよび Webトラフィック モニタリング ネットワークである Cisco の共通の安全保障 データベース (SenderBase[®] ネットワーク) からのデータを活用します。それは URL の評判の優秀なインジケータである 50 の個別のパラメータにトラッキングします。高度なセキュリティ 模倣および malware 検出 エージェントによって、Cisco はこれらの入力に基づいてこれらの URL を評価します。

いくつかのパラメータは下記のものを含んでいます:

- URL 分類データ
- ダウンロード可能コードの存在
- 長くの存在、混乱させたエンドユーザー 使用 許諾 契約 (EULAs)
- 音量のグローバルな 音量および変更
- ネットワーク 所有者 の 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/phishing/pharming ブラックリストの存在

- 普及したドメインの URL タイプエラー
- ドメイン レジストラ 情報
- IP アドレス 情報

WBRs 細かさ

WBRs は従来の URL ブラックリストか whitelist と広いデータセットを分析し、ほとんどの malware 検出アプリケーションのバイナリよくか悪い分類の代りに -10 から +10 の非常に細かいスコアを生成するので、異なります。この粒状スコアは管理者に高められた柔軟性を提供します ; 異なるセキュリティポリシーは異なる WBRs 記録範囲に基づいて設定されます。