

WSA Cisco Web聲譽概述

目錄

[簡介](#)

[WBRs概述](#)

[WBRs使用SenderBase](#)

[WBRs粒度](#)

簡介

本檔案概述了思科網路安全裝置(WSA)的思科網路聲譽(WBRs)。

作者：Josh Wolfer和Stephan Fiebrandt，思科TAC工程師。

WBRs概述

WBRs是一種創新方法，可分析Web伺服器的行為和特徵，並在對抗垃圾郵件、病毒、網路釣魚和間諜軟體威脅方面提供最新防禦。

WBRs對龐大、多樣的全域性資料集進行即時分析，以檢測包含某種形式惡意軟體的URL。WBRs是思科安全資料庫的重要部分，可保護客戶免受電子郵件或Web流量的混合威脅。

WBRs使用SenderBase

WBRs利用來自思科通用安全資料庫(SenderBase[®] Network)的資料，該資料庫是全球最大的電子郵件和網路流量監控網路。它會跟蹤50多個不同的引數，這些引數是URL信譽的極佳指標。藉助成熟的安全建模和惡意軟體檢測代理，思科根據這些輸入評估這些URL。

部分引數包括：

- URL分類資料
- 存在可下載代碼
- 存在長期、模糊的終端使用者許可協定(EULA)
- 全域性卷和卷更改
- 網路所有者資訊
- URL歷史記錄
- URL的期限
- 存在病毒/垃圾郵件/間諜軟體/網路釣魚/域名黑名單
- 常用域的URL錯誤

- 域註冊器資訊
- IP地址資訊

WBRs粒度

WBRs不同於傳統的URL黑名單或白名單，因為它分析大量資料並生成高度精細的分數-10到+10，而不是大多數惡意軟體檢測應用程式的二進位制好或壞分類。這種精細評分提高了管理員的靈活性；可以根據不同的WBRs評分範圍實施不同的安全策略。