WSA思科Web声誉概述

目录

简介

本文档概述了思科网络安全设备(WSA)的思科网络信誉(WBRS)。

作者：Josh Wolfer和Stephan Fiebrandt，Cisco TAC工程师。

WBRS概述

WBRS是一种创新方法，可分析Web服务器的行为和特征，并提供抵御垃圾邮件、病毒、网络钓鱼和间谍软件威胁的最新防御。

WBRS对大量、多样化的全局数据集进行实时分析，以检测包含某种形式恶意软件的URL。WBRS是思科安全数据库的关键部分，可保护客户免受来自电子邮件或Web流量的混合威胁。

WBRS使用SenderBase

WBRS利用思科通用安全数据库(SenderBase®网络)中的数据，该数据库是全球最大的电子邮件和网络流量监控网络。它跟踪50多个不同参数，这些参数是URL信誉的良好指标。思科利用先进的安全建模和恶意软件检测代理，根据这些输入来评估这些URL。

一些参数包括：

- URL分类数据
- 存在可下载代码
- 存在冗长且模糊的最终用户许可协议(EULA)
- 全局卷和卷变化
- 网络所有者信息
- URL的历史记录
- URL的使用期限
- 存在病毒/垃圾邮件/间谍软件/网络钓鱼/域欺骗黑名单
- 常用域的URL拼写

- 域注册器信息
- IP地址信息

WBRS粒度

WBRS不同于传统的URL黑名单或白名单，因为它会分析大量数据并产生–10到+10的高度精细的分数，而不是大多数恶意软件检测应用的二进制**好**或**坏**分类。这种精细的分数为管理员提供了更高的灵活性；可以根据不同的WBRS评分范围实施不同的安全策略。