了解Umbrella灰名单和灰色域

目录

简介

本文档介绍Cisco Umbrella中的灰名单和灰色域。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Umbrella通过Umbrella Intelligent Proxy为与某些未分类域关联的URL、潜在恶意文件和域名的代理请求提供了功能。

灰色域

智能代理可避免任何预先确定的安全和/或恶意域。但是，有些领域在本质上可能具有风险。虽然这些域实际上不是恶意的，但它们允许创建和/或托管域所有者未知的恶意子域和内容。因此，这些“灰色”域会标记为有风险的域，因为它们可以托管安全子域和恶意子域/内容。这些未分类的站点可能包括常用站点，例如文件共享服务。

灰名单

灰名单是风险灰色域的列表，智能代理会拦截并代理以确认其是否确实是恶意的。它是我们的安全研究团队所跟踪的灰色域的动态列表。

例如：“examplegrey.com”是一个允许用户托管其自己内容的域。虽然域本身可能很安全，但恶意攻击者可以托管恶意内容/子域，例如“examplegrey.com/malicious”。 同时，它还可以将其他非恶意内容托管为“examplegrey.com/safe”。因此，将examplegrey.com保留在灰名单中有助于阻止恶意内容(“examplegrey.com/malicious”)，同时允许安全内容(“examplegrey.com/safe”)。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。