了解Umbrella中的潜在有害安全类别

目录

简介

本文档介绍Cisco Umbrella中的潜在有害安全类别。

先决条件

要求

本文档没有任何特定的要求。

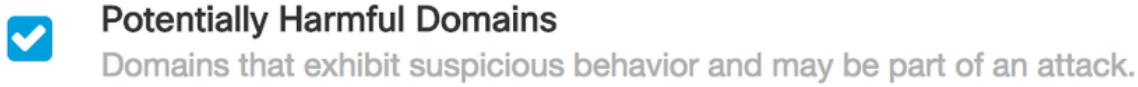
使用的组件

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

在安全性方面，Umbrella客户具有不同的风险承受级别。根据您从事的工作的行业和类型，主动监控和阻止潜在有害活动可能会非常有益。新的“潜在有害”安全设置可以在Prevent下找到，位于Other Security Settings旁，默认设置为Allow:



115011476788

详细信息

“潜在危害”是一个安全类别，其中包含可能为恶意的域。它不同于Umbrella的“恶意软件”类别，因为Umbrella对这些恶意软件进行了较低程度的自信。另一种说法是，根据我们的研究分析人员和我们用来确定总体信息的算法，这些域被视为可疑域，但不一定被认为是恶意域。

此类别的使用取决于您对阻止潜在良好域风险的容忍度。如果您有一个高度安全的环境，这是一个要阻止的良好类别；如果您的环境更松散，您只需允许和监控即可。

如果您不确定您属于哪个类别，可以监控报告中被确认为“潜在危害”的活动。提供此类别可以在流量分类方面提供更高的精细度，提高可视性，提供更强大的保护，并改善事件响应。 例如，如果您认为某台计算机感染了恶意软件，查看其访问的潜在有害域可以帮助您更好地评估危害级别。

Umbrella通过权衡几个因素，确定什么是“潜在有害”，这些因素表明该域虽然不是明显的恶意域，但可能构成威胁。例如，有各种类型的DNS隧道服务。其中有些服务属于良性、恶意和DNS隧道VPN类别，但有些服务则不太清楚，不属于这些类别中的任何一个。如果隧道使用案例未知且可疑，则目标可能属于“潜在危害”类别。

另一个例子来自Umbrella的Spike等级模型。Umbrella的Spike排名模型利用大量DNS请求数据，并使用声波绘图检测其DNS请求模式中存在尖峰的域。在Spike等级域中达到高位的流量可自动归类为恶意流量，阈值较低的流量可归入潜在有害类别。

要报告以下任一类别中的不需要的检测，请执行以下操作：

- 请通过Talos支持将所有数据分类请求提交给思科Talos。
- 有关向Cisco Talos提交请求的一般步骤，请参阅如何：提交分类请求。

对于潜在有害类别，Umbrella不会将其重新分类为安全类别，除非保证该域绝对合法。

与任何其他安全类别一样，这两种类别都可以在报告中进行过滤。

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）。