即将推出的Umbrella安全增强功能 — 新发现的域

目录

简介

本文档介绍即将推出的安全访问和Umbrella服务的“新发现的域”(NSD)类别的安全增强功能。

概述

我们很高兴地通知您有关新增域(NSD)类别的重要增强功能，这是Talos威胁研究团队牵头的安全访问和Umbrella服务的一个重要方面。

我们在做什么？

在不断努力增强您的安全性的过程中，我们正在实施更新的NSD系统，并过渡到版本2(NSDv2)。这一新的迭代显着扩展了源数据，因为它现在包括我们提供调查产品（800B查询/天）的全套Passive DNS，这比当前新发现的域的统计采样方法有所改进。

使用NSDv2，我们改进了数据集，以便更紧密地反映客户的反馈和使用情况，以及对Talos威胁研究团队所发现事实的数据分析。新算法关注于发现新的注册级别域，并降低了共享共同父级多个子域的“噪声”。

我们为什么要这样做？

我们倾听了客户的反馈，并分析了相关数据，这些数据表明NSD如何延迟低流量域的分类，如果域突然变得普及，将会导致意想不到的结果和对域的中断。此外，对大流量域所做的更改可能会发生意外的变化，例如当内容传送网络对其命名方案进行更改时。

Talos威胁研究团队与Umbrella共同开发了NSDv2以解决这些问题，为识别新发现的域提供了更可靠和更准确的系统。

它如何使您受益？

NSDv2增强功能在设计时充分考虑了安全性和运营效率：

- 改进的威胁检测：NSDv2在识别后来被证明是恶意的域的速率方面至少提高了45%。

- 减少误报：使用更精确的目标系统，您会遇到正常使用的错误标记域造成的中断更少。
- 优化的性能：精简的数据集不仅有助于加快发布速度，还使我们的支持团队能够迅速解决出现的任何问题。
- 实施“最佳实践”：此类别更为一致和相关，可以更好地与行业和客户期望保持一致。
- 丰富的报告数据：NSDv2的改进环境和覆盖范围丰富了报告中的数据。
- 改进的预测：此更新可帮助智能代理确定需要更深入检查的危险域。
- 无需客户交互：这是对我们的管道进行动态分类的更新，不需要对我们的客户进行任何迁移或策略更改。对管理员和最终用户而言，这是完全透明的改进。

对该类别的更改将于2024年8月13日部署。我们感谢您对我们服务的持续信任，并期待为您提供这些重要的安全改进。

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）。