Upcoming Umbrella Security Enhancements - Newly Seen Domains

Contents

[Introduction](#)

[Overview](#)

[What are we doing?](#)

[Why are we doing this?](#)

[How does it benefit you?](#)

Introduction

This document describes upcoming security enhancements to the Newly Seen Domains (NSD) category of the Secure Access and Umbrella services.

Overview

We are thrilled to inform you about an important enhancement to the Newly Seen Domains (NSD) category, a key aspect of our Secure Access and Umbrella services, spearheaded by the Talos Threat Research team.

What are we doing?

In our ongoing efforts to bolster your security, we are implementing an updated system for NSD, transitioning to version 2 (NSDv2). This new iteration significantly expands the source data, as it now includes the full set of our Passive DNS which powers our Investigate product (800B queries/day), an improvement over the statistical sampling methodology of the current Newly Seen Domains.

With NSDv2, we have refined the dataset to more closely reflect customer feedback and usage, as well as data analysis of the occurrence to conviction by our Talos Threat Research Team. The new algorithm focuses on discovering new registered-level domains, and reduces the “noise” of multiple subdomains sharing a common parent.

Why are we doing this?

We listened to customer feedback and analyzed data showing how NSD could delay the categorization of low-volume domains, causing unexpected results and disruption to domains if they experienced a sudden increase in popularity. Additionally, changes to high-volume domains could see unexpected shifts, for example when a content delivery network introduced changes in their naming scheme.

The Talos Threat Research team has developed NSDv2 in conjunction with Umbrella to resolve these issues, providing a more reliable and accurate system for identifying newly seen domains.

How does it benefit you?

The NSDv2 enhancement is designed with your security and operational efficiency in mind:

- **Improved Threat Detection:** NSDv2 boasts a minimum of 45% improvement in the rate of identifying domains that later turn out to be malicious.
- **Decreased False Positives:** With a more precise targeting system, you experience fewer disruptions from incorrectly flagged domains that are in regular use.
- **Optimized Performance:** The streamlined data set not only allows for faster publishing but also enables our support team to swiftly address any issues, if they arise.
- **Enforcement 'Best practice':** This category is more consistent and relevant and allow better alignment with industry and customer expectations.
- **Enriched reporting data:** The improved context and coverage with NSDv2 enriches the data in reports.
- **Improved prediction:** This update aids the Intelligent Proxy in determining risky domains that warrant deeper inspection.
- **No customer interaction required:** This is an update to our pipelines for a dynamic categorization, and does not require any migration or policy changes for our customers. This is a completely transparent improvement for admins and end-users.

The changes to this category are to be deployed on August 13th, 2024. We are grateful for your continued trust in our services and are eager to provide you with these significant security improvements.