Próximas mejoras en Umbrella Security: dominios recientemente vistos

Contenido

Introducción

En este documento se describen las próximas mejoras de seguridad de la categoría Dominios recién vistos (NSD) de los servicios Secure Access y Umbrella.

Overview

Nos complace informarle de una importante mejora en la categoría de dominios recién vistos (NSD), un aspecto clave de nuestros servicios de acceso seguro y de protección general, liderados por el equipo de investigación de amenazas de Talos.

¿Qué estamos haciendo?

En nuestros esfuerzos continuos por reforzar su seguridad, estamos implementando un sistema actualizado para NSD, con la transición a la versión 2 (NSDv2). Esta nueva iteración amplía significativamente los datos de origen, ya que ahora incluye el conjunto completo de nuestro DNS pasivo que alimenta nuestro producto Investigate (800B consultas/día), una mejora sobre la metodología de muestreo estadístico de los dominios recién vistos actuales.

Con NSDv2, hemos perfeccionado el conjunto de datos para reflejar con mayor precisión los comentarios y el uso de los clientes, así como el análisis de datos de la incidencia hasta la convicción por parte de nuestro equipo de investigación de amenazas de Talos. El nuevo algoritmo se centra en el descubrimiento de nuevos dominios de nivel registrado y reduce el "ruido" de múltiples subdominios que comparten un padre común.

¿Por qué estamos haciendo esto?

Escuchamos los comentarios de los clientes y analizamos los datos que mostraban cómo NSD podía retrasar la categorización de los dominios de bajo volumen, lo que provocaba resultados inesperados y la interrupción de los dominios si experimentaban un aumento repentino de la popularidad. Además, los cambios en los dominios de gran volumen podrían experimentar

cambios inesperados, por ejemplo, cuando una red de distribución de contenido introdujo cambios en su esquema de nombres.

El equipo de Talos Threat Research ha desarrollado NSDv2 junto con Umbrella para resolver estos problemas, lo que proporciona un sistema más fiable y preciso para identificar los dominios que se acaban de ver.

¿Cómo le beneficia?

La mejora de NSDv2 se ha diseñado teniendo en cuenta su seguridad y eficacia operativa:

- Detección de amenazas mejorada: NSDv2 presume de una mejora mínima del 45% en la tasa de identificación de dominios que posteriormente resultan ser maliciosos.
- Reducción de falsos positivos: Con un sistema de segmentación más preciso, experimentará menos interrupciones de dominios marcados incorrectamente que se utilizan con regularidad.
- Rendimiento optimizado: El conjunto de datos optimizado no solo permite una publicación más rápida, sino que también permite a nuestro equipo de soporte abordar rápidamente cualquier problema, si surge.
- Aplicación de las "mejores prácticas": Esta categoría es más coherente y relevante, y permite una mejor adaptación a las expectativas del sector y de los clientes.
- Datos de informes enriquecidos: La mejora del contexto y la cobertura con NSDv2 enriquece los datos de los informes.
- Predicción mejorada: Esta actualización ayuda al proxy inteligente a determinar los dominios de riesgo que requieren una inspección más profunda.
- No se requiere interacción con el cliente: Se trata de una actualización de nuestros canales para una categorización dinámica y no requiere ningún cambio de migración o política para nuestros clientes. Se trata de una mejora totalmente transparente para los administradores y los usuarios finales.

Los cambios en esta categoría se implementarán el 13 de agosto de 2024. Le agradecemos que siga confiando en nuestros servicios y estamos deseosos de ofrecerle estas importantes mejoras de seguridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).