Comprender las listas grises de paraguas y los dominios grises

Contenido

Introducción

Este documento describe listas grises y dominios grises en Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Umbrella ofrece una función para realizar proxy de solicitudes de URL, archivos potencialmente malintencionados y nombres de dominio asociados con determinados dominios no clasificados mediante Umbrella Intelligent Proxy.

Dominios grises

El proxy inteligente evita cualquier dominio previamente identificado que sea seguro o malintencionado. Sin embargo, hay ciertos dominios que pueden ser de naturaleza riesgosa.

Aunque estos dominios no son realmente malintencionados, pueden permitir la creación o el alojamiento de subdominios malintencionados y contenido desconocido para los propietarios de los dominios. Por lo tanto, estos dominios "grises" se marcan como dominios de riesgo porque pueden alojar subdominios/contenido malintencionado y seguro. Estos sitios no categorizados pueden incluir sitios populares, como servicios para compartir archivos.

Greylist

La lista de rechazo transitorio es una lista de dominios grises de riesgo que el proxy inteligente intercepta y utiliza como proxy para confirmar si es realmente malicioso o no. Se trata de una lista dinámica de dominios grises de los que nuestro equipo de investigación de seguridad realiza un seguimiento.

Por ejemplo: "examplegrey.com" es un dominio que permite a los usuarios alojar su propio contenido. Aunque el propio dominio podría ser seguro, un agente malintencionado puede alojar contenido o subdominio malintencionado como "examplegrey.com/malicious". Al mismo tiempo, también podría tener otro contenido no malintencionado alojado como "examplegrey.com/safe". Por lo tanto, mantener examplegrey.com en la lista de rechazo transitorio ayuda a bloquear el contenido malintencionado ("examplegrey.com/malicious") al tiempo que permite el contenido seguro ("examplegrey.com/safe").

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).