Comprendre les listes grises et les domaines gris des parapluies

Table des matières

Introduction

Ce document décrit les listes grises et les domaines gris dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Umbrella offre une fonctionnalité de proxy pour les requêtes d'URL, les fichiers potentiellement malveillants et les noms de domaine associés à certains domaines non classés via Umbrella Intelligent Proxy.

Domaines gris

Le proxy intelligent évite tout domaine préidentifié qui est sûr et/ou malveillant. Cependant, certains domaines peuvent présenter des risques dans la nature. Bien que ces domaines ne soient pas réellement malveillants, ils peuvent permettre la création et/ou l'hébergement de sous-

domaines et de contenus malveillants inconnus des propriétaires de domaines. Par conséquent, ces domaines « gris » sont marqués comme des domaines à risque car ils peuvent héberger à la fois des sous-domaines/contenus sûrs et malveillants. Ces sites non classés peuvent inclure des sites populaires, tels que des services de partage de fichiers.

Greylist

La liste grise est une liste de domaines gris risqués que le proxy intelligent intercepte et proxie pour confirmer s'il est effectivement malveillant ou non. Il s'agit d'une liste dynamique de domaines gris que notre équipe de recherche en sécurité suit de près.

Exemple : "examplegrey.com" est un domaine qui permet aux utilisateurs d'héberger leur propre contenu. Bien que le domaine lui-même puisse être sûr, un acteur malveillant peut héberger du contenu/sous-domaine malveillant tel que « examplegrey.com/malicious ». En même temps, il pourrait également avoir d'autres contenus non malveillants hébergés comme "examplegrey.com/safe." Par conséquent, garder examplegrey.com dans la liste grise aide à bloquer le contenu malveillant ("examplegrey.com/malicious") tout en permettant le sûr ("examplegrey.com/safe").

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.