Understand Umbrella Greylists and Grey Domains

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

Grey Domains

Greylist

Introduction

This document describes greylists and grey domains in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Overview

Umbrella offers a feature to proxy requests for URLs, potentially malicious files, and domain names associated with certain uncategorized domains through Umbrella Intelligent Proxy.

Grey Domains

The intelligent proxy avoids any pre-identified domains which are safe and/or malicious. However, there are certain domains that can be risky in nature. While these domains are not actually malicious, they can allow the creation and/or hosting of malicious subdomains and content unknown to the domain owners. Hence, these "grey" domains are flagged as risky domains because they can host both safe and malicious subdomains/content. These uncategorized sites can include popular sites, such as file-sharing services.

Greylist

The greylist is a list of risky grey domains that the Intelligent Proxy intercepts and proxies to confirm if it

indeed is malicious or not. It is a dynamic list of grey domains our security research team keeps track of.

For example: "examplegrey.com" is a domain which allows users to host their own content. While the domain itself could be safe, a malicious actor can host malicious content/subdomain such as "examplegrey.com/malicious". At the same time it could also have other non-malicious content hosted as "examplegrey.com/safe." Hence, keeping examplegrey.com in the greylist helps block the malicious content ("examplegrey.com/malicious") while allowing the safe one ("examplegrey.com/safe").