Understand the Potentially Harmful Security Category in Umbrella

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

Details

Introduction

This document describes the Potentially Harmful security category in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

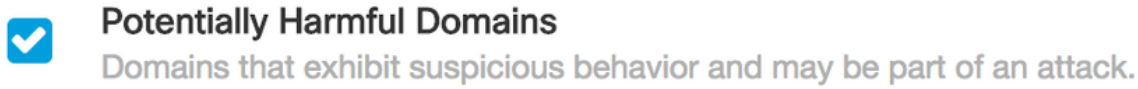
Components Used

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 customers have different levels of risk tolerance when it comes to security. Depending on the industry and type of work you do, it can be beneficial to proactively monitor and block potentially harmful activity. The new "Potentially Harmful" security setting can be found under **Prevent** next to other Security Settings and is set to **Allow** by default:



Details

Potentially Harmful is a security category which contains domains that are likely to be malicious. It is different from Umbrella's "malware" categories because Umbrella ranked them with a lower level of confidence about whether they actually are malicious. Another way of phrasing it is that these domains are considered suspicious according to our research analysts and the algorithms we use to determine overall but not necessarily known to be malicious.

Use of this category depends on your tolerance for risk of blocking potentially good domains. If you have a highly secure environment, this is a good category to block and if your environment is looser, you can simply allow and monitor.

If you are not sure which of these you fall under, you can monitor activity that is confirmed as "Potentially Harmful" in your reports. Having this category available can provide additional granularity in classifying traffic, increasing visibility and delivering greater protection and improving incident response. For instance, if you believe a machine is infected with malware, having a look at the potentially harmful domains that it has been visiting can help you do a better job of assessing the level of compromise.

Umbrella determines what is "Potentially Harmful" by weighing several factors that indicate that although the domain is not clearly malicious, it could pose a threat. For example, there are various types of DNS tunneling services. Some of these services fall into the categories of benign, malicious, and DNS tunneling VPN, but some are more unclear and do not fall into any of these categories. If the use case for the tunneling is unknown and suspicious, the destination can fall into the Potentially Harmful category.

Another example comes from Umbrella's Spike rank model. Umbrella's Spike rank model leverages massive amounts of DNS request data and detects domains that have spikes in their DNS request patterns using sound wave graphing. The traffic that hits high on the Spike rank domain can automatically be classified as malicious, and traffic that is lower on the threshold can fall into the Potentially Harmful category.

To report unwanted detections in either of these categories:

- Please submit all requests for data categorization to Cisco Talos throughTalos Support.
- For general steps on submitting requests to Cisco Talos, please see How To: Submit A Categorization Request.

For the Potentially Harmful category, Umbrella does not re-categorize it as safe without taking assurances that the domain is absolutely legitimate.

Both categories can be filtered against in your reports like any other security category.