包括グレイリストとグレードメインについて

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

概要

グレードメイン

グレイリスト

はじめに

このドキュメントでは、Cisco Umbrellaのグレイリストとグレードメインについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Umbrellaは、Umbrellaインテリジェントプロキシを使用して、特定の未分類ドメインに関連付けられているURL、潜在的に悪意のあるファイル、およびドメイン名の要求をプロキシする機能を提供します。

グレードメイン

インテリジェントプロキシは、安全で悪意のある事前に特定されたドメインを回避するただし、本質的にリスクを伴う可能性のある特定のドメインがあります。これらのドメインは実際には悪意のあるものではありませんが、悪意のあるサブドメインやドメイン所有者に知られていないコンテンツの作成やホスティングを可能にします。したがって、これらの「灰色の」ドメインは、

安全なサブドメインと悪意のあるサブドメイン/コンテンツの両方をホストする可能性があるため、危険なドメインとしてフラグが付けられます。このような未分類のサイトには、ファイル共有サービスなどの一般的なサイトが含まれます。

グレイリスト

グレイリストは、インテリジェントプロキシが代行受信してプロキシを実行し、実際に悪意があるかどうかを確認する、危険なグレードメインのリストです。セキュリティ調査チームが追跡しているグレードメインの動的なリストです。

たとえば、「examplegrey.com」は、ユーザーが独自のコンテンツをホストできるドメインです。ドメイン自体は安全である可能性がありますが、悪意のあるアクターは「examplegrey.com/malicious」などの悪意のあるコンテンツ/サブドメインをホストする可能性があります。 同時に、他の悪意のないコンテンツを「examplegrey.com/safe」としてホストすることもできます。 したがって、examplegrey.comをグレイリストに残しておくと、安全なコンテンツ(「examplegrey.com/malicious」)を許可しながら、悪意のあるコンテンツ(「examplegrey.com/safe」)をブロックするのに役立ちます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。