Umbrella 그레이리스트 및 그레이 도메인 이해

목차

소개

이 문서에서는 Cisco Umbrella의 그레이리스트 및 회색 도메인에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella는 Umbrella Intelligent Proxy를 통해 URL, 악의적인 파일, 분류되지 않은 특정 도메인과 연결된 도메인 이름에 대한 프록시 요청을 처리할 수 있는 기능을 제공합니다.

회색 도메인

지능형 프록시는 안전한 도메인 및/또는 악의적인 도메인의 사전 식별을 방지합니다. 그러나, 본질적으로 위험할 수 있는 특정 영역이 있다. 이러한 도메인은 실제로 악의적이지 않지만, 도메인 소유자에게 알려지지 않은 악성 하위 도메인 및 콘텐츠의 생성 및/또는 호스팅을 허용할 수 있습니다. 따라서 이러한 "회색" 도메인은 안전한 하위 도메인과 악의적인 하위 도메인/콘텐츠를 모두 호스팅할 수 있으므로 위험한 도메인으로 플래그가 지정됩니다. 이러한 분류되지 않은 사이트에는 파일 공유 서비스와 같은 인기 사이트가 포함될 수 있습니다.

그레이리스트

greylist는 Intelligent Proxy가 가로채기 및 프록시를 통해 악성 여부를 확인하는 위험한 회색 도메인 목록입니다. Cisco 보안 연구 팀이 추적하는 회색 도메인의 동적 목록입니다.

예를 들면 다음과 같습니다. "exampgrey.com"은 사용자가 자신의 콘텐츠를 호스팅할 수 있도록 허용하는 도메인입니다. 도메인 자체는 안전할 수 있지만 악의적인 행위자는 "examplegrey.com/malicious"과 같은 악의적인 콘텐츠/하위 도메인을 호스팅할 수 있습니다. 동시에 "examplegrey.com/safe"으로 호스팅되는 다른 비악성 콘텐츠도 포함할 수 있습니다. 따라서 그레이리스트에 examplegrey.com을 유지하면 안전한 콘텐츠("examplegrey.com/safe")를 허용하는 동시에 악성 콘텐츠("examplegrey.com/malicious")를 차단할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.