Eicar로 파일 검사 테스트

목차

소개

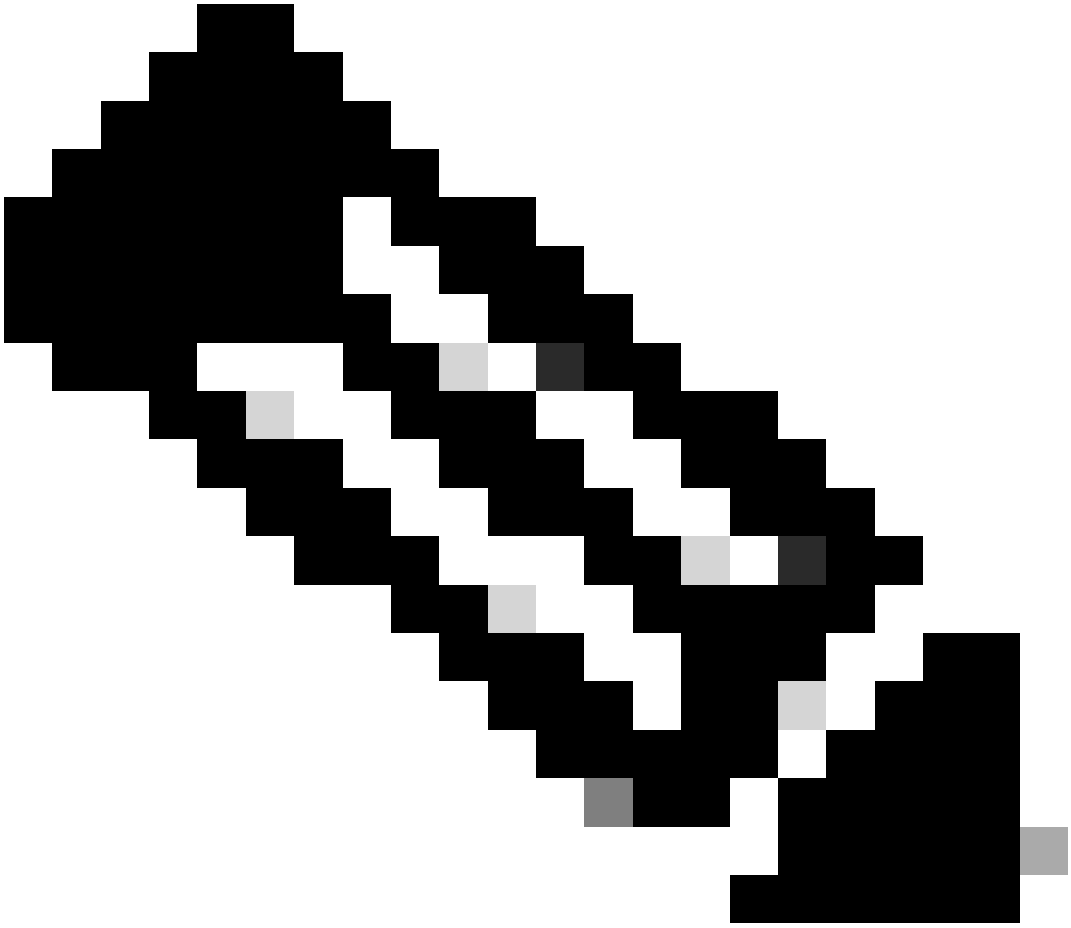
이 문서에서는 Eicar를 사용하여 파일 검사를 테스트하는 방법에 대해 설명합니다.

개요

현재 eicar.org 테스트 다운로드 파일을 사용하여 파일 검사 기능이 활성화되었는지 여부를 테스트할 때 "SSL 암호 해독"이 활성화되었거나 비활성화되었을 때 다른 동작이 나타납니다. SSL 암호 해독이 활성화된 경우 eicar.org에서 Umbrella File Inspection(Umbrella 파일 검사)에서만 AV 검사 다운로드가 수행됩니다.

Eicar에 대한 탐지 프로세스 이해

eicar.org의 차단을 활성화하려면 SSL 암호 해독을 활성화하십시오.



참고: HTTP를 통해 사이트를 방문하는 경우에도 SSL 암호 해독이 필요합니다. SSL 암호 해독이 활성화되지 않은 경우 프록시는 HTTPS를 통해 트래픽을 제공하는 도메인을 우회합니다.

- Umbrella Intelligent Proxy는 DNS 레이어의 프록시에 도메인을 보낼지 여부를 결정합니다.
- DNS 요청은 HTTP/HTTPS 연결 전에 발생합니다. 즉, 도메인이 프록시의 대상이 되는 경우 HTTP 및 HTTPS 트래픽 모두 항상 프록시됩니다.
- HTTP/HTTPS 트래픽이 인텔리전트 프록시에 도달하면 사용자를 식별하기 위해 리디렉션을 수행하는 것이 첫 번째 단계입니다.

이 리디렉션은 SSL 암호 해독 없이 가능하지 않습니다. 즉, 일부 시나리오에서 사용자(예: 로밍 사용자)를 올바르게 식별하지 못할 수 있습니다.

이러한 사용자의 HTTPS 요청 중단을 방지하기 위해 Umbrella는 SSL 암호 해독이 활성화되어 있지 않으면 HTTP/HTTPS 트래픽을 모두 처리하는 프록시 도메인(예: eicar.org)을 사용하지 않습니다.

요약...

이 기능을 통해 최상의 보안 및 효율성을 얻으려면 Cisco Root CA를 설치하고 SSL 암호 해독을 활성화하는 것이 좋습니다. 이렇게 하면 eicar.org 테스트 파일을 차단할 수 있으며 인텔리전트 프록시를 통해 파일 검사가 적용되는 도메인의 수가 늘어납니다.

다음은 예상되는 동작의 요약입니다.

- SSL 암호 해독 해제
  - Eicar.org 사이트는 https://www.eicar.org/download/eicar.com에서 차단되지 않습니다. SSL 암호 해독이 비활성화되어 있기 때문에 도메인이 전혀 프록시되지 않습니다.
  - Cisco의 자체 테스트 사이트 호스팅 EICAR가 차단되었습니다. http://proxy.opendnstest.com/download/eicar.com
- SSL 암호 해독 설정
  - http://www.eicar.org/download/eicar.com 및 https://www.eicar.org/download/eicar.com에서 AV 스캔에 의해 Eicar가 차단됨

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.