Microsoft 365에서 Umbrella Cloud Malware Not Detecting Eicar 테스트 파일 트러블슈팅

목차

소개

이 문서에서는 Microsoft 365에서 Umbrella Cloud Malware가 Eicar 테스트 파일을 탐지하지 못하도록 문제를 해결하는 방법에 대해 설명합니다.

개요

Eicar 테스트 파일 내용은 여러 벤더에 걸쳐 안티바이러스 소프트웨어가 작동하는지 확인하는 데 사용할 수 있는 업계에서 인정하는 텍스트 문자열입니다. 이 파일을 사용하여 Microsoft 365 플랫폼에서 Cisco Umbrella Cloud Malware 기능이 작동하는지 확인하는 경우 Cloud Malware 보고서 또는 Scanned Files 섹션에 Eicar 테스트 파일이 표시되지 않을 수 있습니다.

해결

Cisco는 AMP(Advanced Malware Protection) 테스트 파일을 제공합니다. 이 파일은 클라우드 악성코드 기능에서 탐지되지만 Microsoft 365에 내장된 악성코드 차단에서는 탐지되지 않습니다. 이 파일을 사용하여 Microsoft 플랫폼에서 클라우드 악성코드의 올바른 기능을 확인할 수 있습니다

Cisco Umbrella 설명서에서 AMP 테스트 파일(및 eicar 파일)을 찾을 수 있습니다.

또는 비밀번호로 보호된 파일을 Microsoft에 저장하는 것은 Cloud Malware 보고 내에서 "Suspicious(의심스러움)"로 탐지됩니다. 의심스러운 파일 표시는 클라우드 악성코드 보고의 왼쪽 하단에 있는 "Suspect Files" 옵션을 통해 전환할 수 있습니다.

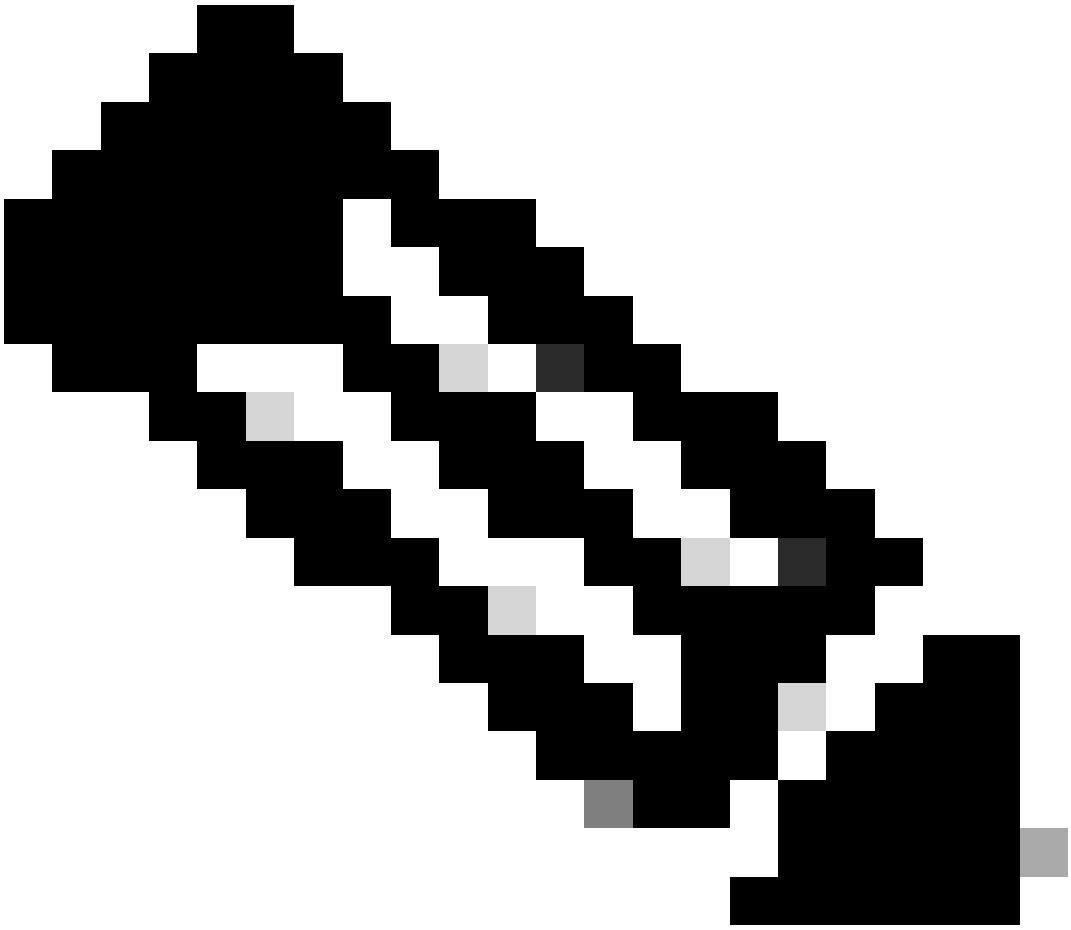
원인

Microsoft는 Microsoft 서브스크립션에 악성코드 차단 레이어를 포함합니다. 이 및 해당 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

- SharePoint Online, OneDrive 및 Microsoft Teams에 내장된 바이러스 방지 기능
- SharePoint, OneDrive 및 Microsoft Teams용 안전한 첨부 파일

Microsoft의 안티멀웨어 레이어는 Eicar를 탐지하므로 파일에 대해 악성코드 플래그를 설정합니다.

이는 무엇보다도 파일이 공유되는 것을 방지하며 Cloud Malware가 Microsoft 365 플랫폼과 통합하는 데 사용하는 API를 통해 파일에 액세스하는 것을 방지합니다.



참고: 기본적으로 Microsoft 365에서 파일에 악성코드로 플래그를 지정하더라도 소유자는 파일을 다운로드할 수 있습니다. 이 다운로드가 Cisco Umbrella SWG(Secure Web Gateway)를 통해 발생하는 경우(HTTPS 검사가 활성화된 경우), 이 다운로드는 전송 중에 차단되며 활동 검색 보고서에 나타납니다.

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.