DNS 확인을 CNAME 레코드 도메인 정책 및 보고와 일치

목차

소개

이 문서에서는 DNS 솔루션을 CNAME 레코드 도메인 정책 및 보고와 일치시키는 방법에 대해 설명합니다.

문제

BIND(캐싱이 활성화됨) 또는 Infoblox와 같은 DNS(Domain Name System) 캐싱 서버를 사용하는 동안 DNS 확인이 CNAME 레코드 도메인에 대한 예상 정책 및 보고와 일치하지 않습니다. 허용된 A-record 요청은 차단된 다른 도메인의 다른 A-record에 대한 CNAME 참조로 응답됩니다.

예를 들어 domain.com이 허용되고 blocked.com은 차단되지만 domain.com은 A 레코드가 있는 blocked.com을 가리키는 CNAME 레코드입니다. 이 문제는 대시보드에 이벤트가 기록되지 않은 상태에서 차단된 허용 도메인으로 나타납니다.

솔루션

이 문제를 해결하기 위한 몇 가지 방법이 있습니다.

- Umbrella로 전달된 DNS에 대해 DNS 캐싱을 비활성화합니다. 이렇게 하면 이 문제가 발생하지 않습니다.
- 대상 CNAME이 발생할 때 Umbrella Dashboard(Umbrella 대시보드)에서 이를 허용합니다.
- CNAME 레코드 유형을 캐시하거나 영향을 받는 도메인을 선택적으로 캐시하지 않도록 합니다.

원인

이 문제의 근본 원인은 대상 도메인이 차단된 다른 도메인을 가리키는 CNAME 레코드에 대한 DNS 캐싱입니다. 도메인이 허용되므로 Umbrella 확인자는 전체 쿼리에 허용되는 플래그를 지정하며 CNAME 체인을 적용합니다. 이렇게 하면 쿼리가 허용됩니다.

서로 다른 도메인은 TTL에 따라 다르며 악의적인 카테고리에 대한 Umbrella 블록 레코드의 TTL이

0이므로 캐싱 간섭이 발생합니다.

domain.com이 허용되고 blocked.com이 차단되는 시나리오가 있으며 domain.com은 A 레코드가 있는 blocked.com을 가리키는 CNAME 레코드입니다.

초기 쿼리:

domain.com에 대한 A 레코드: Allow list, CNAME for blocked.com -> CNAME에서 blocked.com에 대한 A-record 쿼리, Umbrella 내부에서 전달된 비트 허용 - blocked.com에 대한 A-record가 반환되었습니다.
분석: Umbrella에 대한 쿼리: domain.com -> blocked.com을 참조하십시오. 결과: 허용됨.
Umbrella는 허용되는 경우 domain.com, 허용되는 경우 blocked.com을 로깅합니다.

후속 쿼리:

domain.com에 대한 A 레코드: CACHED - blocked.com의 CNAME -> blocked.com의 A 레코드 쿼리입니다. CACHED - blocked.com에 대한 A 레코드가 반환되었습니다.
분석: Umbrella에 대한 쿼리: None. 우산 로그가 없습니다.

향후 쿼리(문제 발생):

domain.com에 대한 A 레코드: CACHED - blocked.com의 CNAME -> blocked.com의 A-record 쿼리(독립형 쿼리 - CNAME이 캐시됨) - 차단되었습니다.
분석: Umbrella에 대한 쿼리: blocked.com을 참조하십시오. 결과: 차단됨. Umbrella는 blocked.com을 차단된 것으로 로깅합니다.

추가 정보

- Umbrella 설명서: DNS 확인

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.