QNAME 최소화를 통한 Umbrella DNS 이해

목차

소개

이 문서에서는 QNAME을 최소화하는 Cisco Umbrella DNS(Domain Name System)를 사용하는 방법에 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

2019년 6월, Cisco Umbrella는 쿼리 이름 최소화(RFC7816)에 대한 지원을 추가했습니다. QNAME 최소화는 전체 도메인 대상을 루트 네임 서버로 전송하는 것을 제한하는 DNS의 프라이버시 지향 기능입니다. 그 결과 DNS 쿼리 응답을 결정하는 DNS 쿼리 흐름이 수정됩니다.

QNAME 최소화는 전 세계적인 주제입니다. Internet Systems Consortium에는 QNAME Minimization에 대한 소개 기사가 있습니다. Mozilla Firefox는 HTTPS 구현을 통해 DNS에 QNAME 최소화를 사용하려면 리졸버가 필요하며 이 항목에 대한 기사가 있습니다.

쿼리 최소화 이해

쿼리 최소화는 DNS 권한 쿼리에 대한 새로운 데이터 프라이버시 중심 접근 방식입니다. 쿼리 최소화가 무엇인지 알아보려면 현재 DNS 요청이 어떻게 작동하는지 설명하는 것부터 시작하십시오.

인터넷과 인간의 상호작용은 대부분 DNS 쿼리에서 시작되므로, 사용자가 어디로 이동하는지에 대한 빅 데이터는 중요한 정보이며, 이는 개인 데이터로 간주될 수 있습니다.

이 예에서는 umbrella.cisco.com을 방문하려고 합니다. 이 서버가 있는 위치를 확인하려면 DNS 쿼리가 필요합니다. 그러면 Umbrella는 다음 단계를 사용하여 해당 쿼리를 재귀 DNS 서버로 전송하여 해당 기관에서 답을 찾습니다.

1. 재귀 DNS 확인자에 대한 사용자 쿼리: umbrella.cisco.com

2. 재귀 DNS 서버가 루트 네임 서버에서 응답을 쿼리합니다. 여기서 umbrella.cisco.com to root > answer for .com을 찾을 수 있습니다.

3. .com 이름 서버에서 질의합니다. umbrella.cisco.com to .com > cisco.com nameservers의 위치 가져오기

4. cisco.com 이름 서버에 쿼리합니다. umbrella.cisco.com에서 cisco.com으로 > 답변 제공

대부분의 경우 A-record를 찾을 때까지 다른 네임서버에 대해 여러 번 더 반복할 수 있습니다. 단계 1-2에서 Umbrella는 .com 네임 서버의 위치만 적극적으로 찾습니다. 그러나 전체 umbrella.cisco.com 도메인은 루트 및 .com 네임서버로 전송됩니다. 전체 쿼리를 수신하는 cisco.com 네임 서버도 마찬가지입니다.

쿼리 최소화를 사용하면 알고리즘이 업스트림 쿼리에서 필요한 수준의 세부 정보만 묻는 것으로 전환됩니다.

1. 재귀 DNS 확인자에 대한 사용자 쿼리: umbrella.cisco.com

2. 재귀 DNS 서버가 루트 네임서버를 쿼리합니다. 어디에서 .com > .com에 대한 답변을 찾을 수 있습니까?

3. .com 이름 서버에서 질의합니다. cisco.com에서 .com으로 이동 > cisco.com의 위치

4. cisco.com nameservers에서 umbrella.cisco.com > Answer를 쿼리합니다.

이 기능은 대부분의 경우 효과적이며, 루트 또는 TLD 네임 서버에 대해 생성되는 고유한 쿼리를 표시하지 않고 답을 찾을 수 있습니다.

이 개인 정보는 EDNS 클라이언트 서브넷을 사용하는 도메인에서 더욱 중요합니다. 여기서 DNS 인증기관은 쿼리할 때 사용자의 소스 C-Block(/24)에 대해 알림을 받습니다. QNAME을 최소화하지 않으면 루트 및 .com(이 예에서) 네임 서버는 사용자의 일반 위치와 정확히 어디로 가는지 알고 있습니다. QNAME Minimization을 사용하면 루트는 다른 사람이 .com을 찾고 있다는 것만 알고 요청자의 개인 정보를 유지합니다. QMIN 개인 정보 보호 없이는 현재 제공되는 세부 정보 수준이 필요하지 않습니다.

잠재적 부작용

QNAME 최소화는 대부분의 경우 문제 없이 작동합니다. 그러나 직접 질의에 비해 추가 실패 소스가 적용됩니다. 정식 이름 서버에 대한 프로세스의 마지막 단계까지 전체 대상이 드러나지 않으므로, DNS 체인이 끊어지면 도메인 확인이 중단될 수 있습니다. 예를 들어, 여기에 긴 가상의 이름 umbrellas.in.the.rain.umbrella.cisco.com이 있습니다. 이로 인해 다음과 같은 쿼리가 발생할 수 있습니다.

1. 루트 서버에 대한 .com의 네임 서버란 무엇입니까?

2. cisco.com에서 .com 서버로의 네임서버(nameservers)란 무엇입니까?

3. umbrella.cisco.com에서 cisco.com 네임서버로의 네임서버 이름

4. rain.umbrella.cisco.com에서 umbrella.cisco.com으로의 네임 서버란 무엇입니까?

5. the.rain.umbrella.cisco.com에서 rain.umbrella.cisco.com 네임서버로의 네임서버 이름

6. in.the.rain.umbrella.cisco.com에서 rain.umbrella.cisco.com 네임서버로의 네임서버란 무엇입니까? 서브페일

7. rain.umbrella.cisco.com 네임 서버에 대한 umbrellas.in.the.rain.umbrella.cisco.com의 네임 서버란 무엇입니까(이전에 SERVFAIL로 인해 쿼리되지 않음)

8. 이전에 발견된 umbrellas.in.the.rain.umbrella.cisco.com 네임 서버에 대한 umbrellas.in.the.rain.umbrella.cisco.com의 답은 무엇입니까(이전에 SERVFAIL로 인해 쿼리되지 않음)

루트에는 전체 쿼리가 제공되지 않으므로 도메인 레벨 중 하나가 NXDOMAIN, SERVFAIL, RFC-1918 내부 네임서버의 IP 또는 기타 불량 응답을 반환하면 쿼리에서 업스트림 신뢰 응답을 성공적으로 수신하지 못할 수 있습니다. 예를 들어, 이전 여섯 번째 단계(굵게, 밑줄)가 실패하는 경우 umbrellas.in.the.rain.umbrella.cisco.com에 대한 쿼리를 확인하지 못할 수 있습니다. 이러한 문제를 해결하려면 도메인 소유자가 각 수준에 유효한 공용 응답이 있는지 확인해야 합니다.

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.