macOS에서 Broadcom WSS와 Umbrella DNS 보안 공존 문제

목차

문제

Umbrella 모듈은 Broadcom WSS(Web Security Service)와 공존하는 경우 macOS에서 DNS 트래픽을 인터셉트하지 않습니다. WSS 에이전트가 80 및 443과 같은 특정 웹 포트를 가로채도록 구성된 경우 Umbrella DNS 보안 기능은 모든 DNS 쿼리를 캡처하지 못합니다. 그러나 WSS가 비활성화되면 Umbrella는 예상대로 DNS 트래픽 가로채기를 다시 시작합니다. WSS가 활성화된 경우 가로채는 모든 DNS 트래픽이 아니라 Umbrella에서 특정 DNS 쿼리만 처리됩니다.

환경

- 운영 체제: 맥OS
- Cisco Umbrella DNS Security 모듈
- Broadcom WSS(Web Security Service) 에이전트
- 웹 포트 80 및 443을 가로채도록 구성된 WSS 에이전트

해결

이 문제는 현재 macOS 아키텍처에서 DNS 보안과 WSS를 함께 사용할 수 없는 macOS의 구조적 한계로 분석되었습니다. 이 제한은 Infoblox 및 Cisco Umbrella DNS 보안 솔루션 모두에 적용됩니다.

기술 분석

근본 원인은 macOS DNS 프록시 제한과 관련이 있습니다.

- macOS 제한으로 인해 한 번에 하나의 DNS 프록시만 활성화할 수 있습니다
- DNS 확인자가 utonX 인터페이스 또는 프록시 주입 확인자에 바인딩되어 있는 경우 macOS는 Umbrella가 아닌 터널 내에서 DNS를 확인합니다
- 다른 NEDnsProxyProvider가 macOS의 시스템에서 활성화되어 있으면 Umbrella가 DNS 트래픽을 가로채지 않습니다

진단 명령

macOS에서 어떤 DNS 확인자가 우선 순위를 차지하고 있는지 확인하려면 다음 명령을 사용합니다 .

```
scutil --dns
```

이 명령은 어떤 확인자가 다음과 같이 표시되는지 표시합니다. 범위 지정, 보완 또는 인터페이스: DNS 프록시 충돌을 식별하는 데 도움이 되는 utunX.

해결 방법 옵션

macOS 환경의 경우 WSS는 별도의 DNS 에이전트 없이 DNS를 계속 가로챕니다. DNS 보안 커버리지로 나아가기 위해 한 가지 옵션은 패시브 바이패스 아키텍처를 지원하도록 구현하는 것입니다. 이 접근 방식을 사용할 경우, 제공자는 흐름을 완전히 우회하므로 마치 제공자가 활성 상태가 아닌 것처럼 트래픽을 처리할 수 있습니다.

원인

이 문제는 한 번에 하나의 NEDnsProxyProvider만 시스템에서 활성화할 수 있는 macOS 아키텍처 제한 사항으로 인해 발생합니다. Umbrella DNS Security와 Broadcom WSS가 모두 설치된 경우 DNS 프록시 제어를 위해 경쟁하므로 WSS가 우선순위를 차지하고 Umbrella가 DNS 트래픽을 가로챌 수 없습니다. 이는 macOS 네트워킹 스택의 근본적인 한계이며 Cisco Umbrella뿐만 아니라 모든 DNS 보안 솔루션에 영향을 미칩니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.