활동 보고서에서 비정상적인 DNS 쿼리 식별 및 이해

목차

소개

이 문서에서는 활동 보고서에 나타날 수 있는 무작위 DNS 요청의 특성과 원인, 그리고 그 출처를 확인하는 방법에 대해 설명합니다.

랜덤 DNS 요청의 예

이러한 요청의 예를 찾을 수 있으며, 이러한 요청은 종종 비정상적이거나 무작위로 보이는 문자열로 나타납니다.

```
iafkbge
nwvkqqojgx
uefakmvidzao
claeedov
cjkcmrh
cjemikolwaczyb
ccshpypwvddmro
cdsvmfjgvfcnbob
cegzaukxjexfrk
ceqmhxowbcys
cewigwgvfd
cexggxhwgt
```

임의 DNS 요청 설명

모든 인터넷 서비스 공급자가 DNS 응답에 대해 RFC 규칙을 준수하는 것은 아닙니다. 활동 검색 보고서에 표시되는 이러한 모호한 DNS 요청은 Google Chrome이 최종 사용자를 보호하기 위해 고유한 요청을 보내는 방법에서 비롯됩니다.

이러한 요청이 발생하는 이유

- 일부 인터넷 서비스 공급자는 공급자 소유 주소를 가리키는 A 레코드가 있는 존재하지 않는 도메인에 대한 DNS 쿼리에 응답합니다. 결과 랜딩 페이지에는 일반적으로 "무엇을 의미했습니까..."와 같은 광고와 메시지가 표시됩니다. 이러한 유형의 조작 및 관련 결과에 대한 개요는 DNS 하이재킹에 대한 위키피디아 기사에서 설명합니다.

- RFC 표준에 따르면 존재하지 않는 도메인에 대한 DNS 요청에 대한 올바른 응답은 NXDOMAIN입니다. 광고는 일반적으로 원치 않기 때문에, Google은 이러한 행동을 테스트하기 위한 방법을 개발했습니다. 시작할 때 Chrome은 3개의 요청을 전송하고 응답이 무엇인지 확인합니다. 테스트 도메인이 NXDOMAIN으로 확인되지 않고 동일한 A 레코드로 확인되는 경우 Chrome은 이 동작을 감지하고 최종 사용자의 광고를 숨깁니다.

- 이 기술은 무작위로 보이는 DNS 요청의 유일한 원인은 아니지만 가장 일반적인 시나리오 중 하나를 나타냅니다.

Chrome을 원인으로 식별하는 방법

- 동일한 내부 호스트에서 전송된 세 개의 특이한 DNS 쿼리 그룹을 찾습니다. 이 패턴은 Chrome에서 테스트 쿼리를 생성하고 있음을 나타냅니다.

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.