문제 해결을 위해 Umbrella Block Page 진단 정보 사용

목차

소개

이 문서에서는 구성 테스트 및 문제 해결을 위해 블록 페이지 진단 정보에 액세스하고 이를 해석하는 방법에 대해 설명합니다.

차단 페이지 진단 정보

차단 페이지에 도달하면 페이지 하단의 진단 정보 섹션을 확장하여 추가 세부 정보를 볼 수 있습니다. 이 정보를 사용하여 컨피그레이션을 테스트합니다. 지원 팀에서 이 섹션의 스크린샷을 요청할 수 있습니다.

차단 페이지 예

제공된 스크린샷은 진단 정보가 확장된 차단 페이지의 예를 보여줍니다.

Cisco Umbrella

This site is blocked due to a phishing threat.

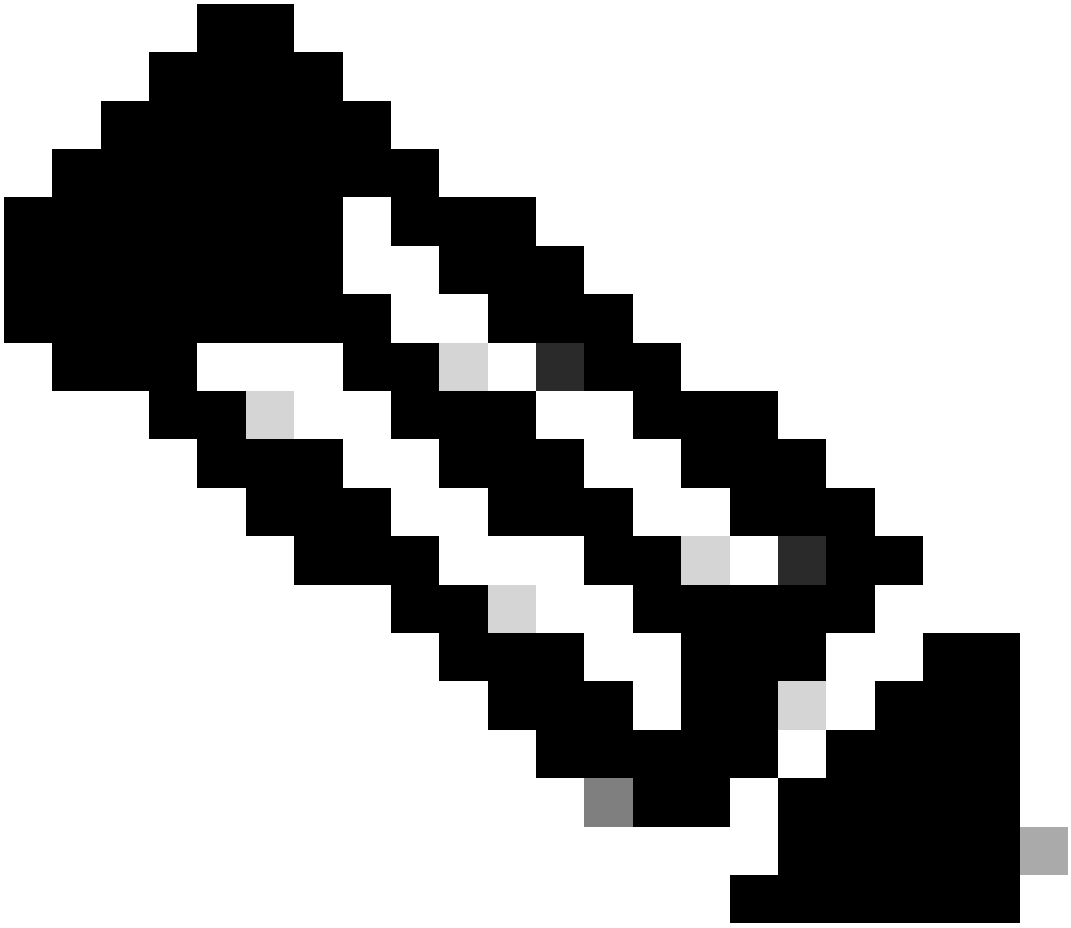
internetbadguys.com

[redacted]

Diagnostic Info

ACType: 0
Block Type: phish
Bundle ID: 1
Domain Tagging: -
Host: phish.opendns.com
IP Address: [redacted]
Org ID: [redacted]
Origin ID: [redacted]
Prefs: -
Query: url=internetbadguys.com&server=ash24&prefs=&tagging=&nr
Server: ash24
Time: 2018-07-12 01:12:29.180338193 +0000 UTC
m=+3221152.293186035

diagnostic.png



참고: 정책 컨피그레이션 트러블슈팅에 대한 자세한 내용은 How To Determine Which Policy Is Being Applied In My Umbrella Configuration(내 Umbrella 컨피그레이션에서 어떤 정책이 적용되는지 확인하는 방법) 문서를 참조하십시오.

정의

ACType

- ACType은 지원에만 유용합니다.

블록 유형

- Block Type(블록 유형)은 블록의 범주 및 페이지 제한 사유를 나타냅니다. 유형은 다음과 같습니다.
  - aup: 콘텐츠 범주

    - 도메인 목록: 대상 목록
    - security: 동적 DNS, C&C(Command and Control), 악성코드, 무단 IP 터널 액세스, 새로 확인된 도메인, 잠재적으로 유해할 수 있는 DNS 터널링 VPN, 서드파티 피드(예: AMP, ThreatGrid)
    - 피싱: 피싱
    - dlink-phish: D-Link 고급 DNS를 통한 피싱

번들 ID

- 번들 ID는 적용된 정책의 식별자입니다.

도메인 태깅

- 도메인 태깅은 지원에만 유용합니다.

호스트

- 호스트는 랜딩 페이지를 가리킵니다. 가능한 값은 다음과 같습니다.
    - block.opendns.com: aup, 도메인 목록
    - malware.opendns.com: 보안
    - phish.opendns.com: 피싱
    - www1.dlinksearch.com: dlink-phish
    - bpb.opendns.com: 차단 페이지 우회

IP 주소

- IP 주소는 시스템의 공용 IP 주소입니다.

조직 ID

- 조직 ID는 시스템이 사용 중인 네트워크의 조직 ID입니다.

원본 ID

- 원본 ID는 지원에만 유용합니다.

기본 설정

- 기본 설정은 지원에만 유용합니다.

Query

- 쿼리는 지원에만 유용합니다.

서버

- 서버는 시스템이 쿼리를 만드는 데 사용한 리소스입니다. 서버 위치는 해당 리소스를 참조하

십시오.

Time

- Time은 쿼리가 작성된 시간을 UTC로 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.