使用Umbrella块页面诊断信息进行故障排除

目录

简介

阻止页面诊断信息

- “块”页面示例

定义

- ACType
- 块类型
- 捆绑包ID
- 域标记
- 主机
- IP Address
- 组织ID
- 源ID
- Prefs
- Query（查询）
- 服务器
- 时间

简介

本文档介绍如何访问和解释块页面诊断信息，以进行配置测试和故障排除。

阻止页面诊断信息

当您进入阻止页面时，可以展开页面底部的诊断信息部分来获得更多详细信息。使用此信息测试您的配置。支持人员可以请求此部分的截图。

“块”页面示例

提供的屏幕截图显示了一个扩展了诊断信息的阻止页面示例：

Cisco Umbrella

This site is blocked due to a phishing threat.

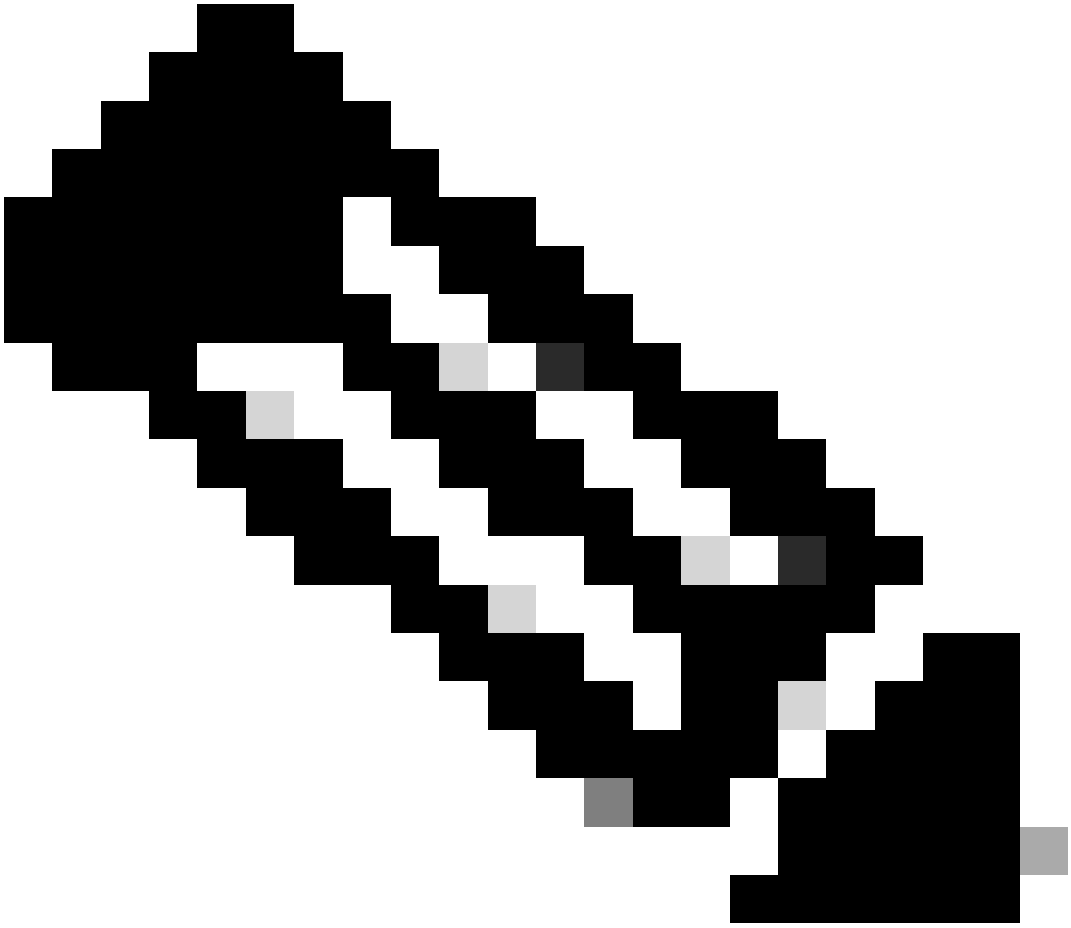
internetbadguys.com

[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-info.png



注意：有关排除策略配置故障的更多详细信息，请参阅如何确定在Umbrella配置中应用了哪个策略。

定义

ACType

- ACType仅对支持有用。

块类型

- Block Type指示块的类别和页面限制的原因。类型包括：
  - aup:内容类别
  - 域列表：目标列表
  - 安全:动态DNS、命令和控制、恶意软件、未经授权的IP隧道访问、新发现的域、可能有

害的、DNS隧道VPN、第三方源（例如，AMP、ThreatGrid）
    - 网络钓鱼：网络钓鱼
    - dlink-phish:通过D-Link高级DNS进行网络钓鱼

捆绑包ID

- 捆绑包ID是应用的策略的标识符。

域标记

- 域标记仅对支持有用。

主机

- 主机是指登录页面。可能的值包括：
    - block.opendns.com:aup、domainlist
    - malware.opendns.com:安全
    - phish.opendns.com:网络钓鱼
    - www1.dlinksearch.com:dlink-phish
    - bpb.opendns.com:阻止页面绕行

IP Address

- IP地址是计算机的公有IP地址。

组织ID

- 组织ID是计算机正在使用的网络的组织ID。

源ID

- 源ID仅对支持有用。

Prefs

- Prefs仅对支持有用。

Query（查询）

- 查询仅对支持有用。

服务器

- 服务器是计算机用于进行查询的资源。有关服务器位置，请参阅相应的资源。

时间

- 时间表示进行查询的时间，采用UTC格式。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。