# 内部感染の発生源の特定

## 内容


[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[ボットネットアクティビティを報告する内部DNSサーバ](#)

[次の手順](#)

[Server 2016より前のオペレーティングシステムの考慮事項](#)

[追加オプション](#)


## はじめに

このドキュメントでは、Cisco Umbrellaの内部感染源を特定する方法について説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づいています

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## ボットネットアクティビティを報告する内部DNSサーバ

Umbrellaダッシュボードに大量の予期しないトラフィックが表示される場合、またはマルウェア/ボットネットが特定したトラフィックがネットワークまたはサイトのいずれかに対してログに記録される場合は、内部ホストが感染している可能性が高くなります。DNS要求は内部DNSサーバを経由する可能性が高いため、要求の送信元IPはDNSサーバのIPに置き換えられ、ファイアウォールでの追跡が困難になります。

この場合、Umbrellaダッシュボードを使用してソースを特定することはできません。 すべての要求は、ネットワークIDに対して記録できます。

# 次の手順

実行できる操作はいくつかありますが、この動作を追跡できる他のセキュリティ製品がない場合は、主にDNSサーバのログを使用して要求の送信元を確認し、送信元を破棄します。

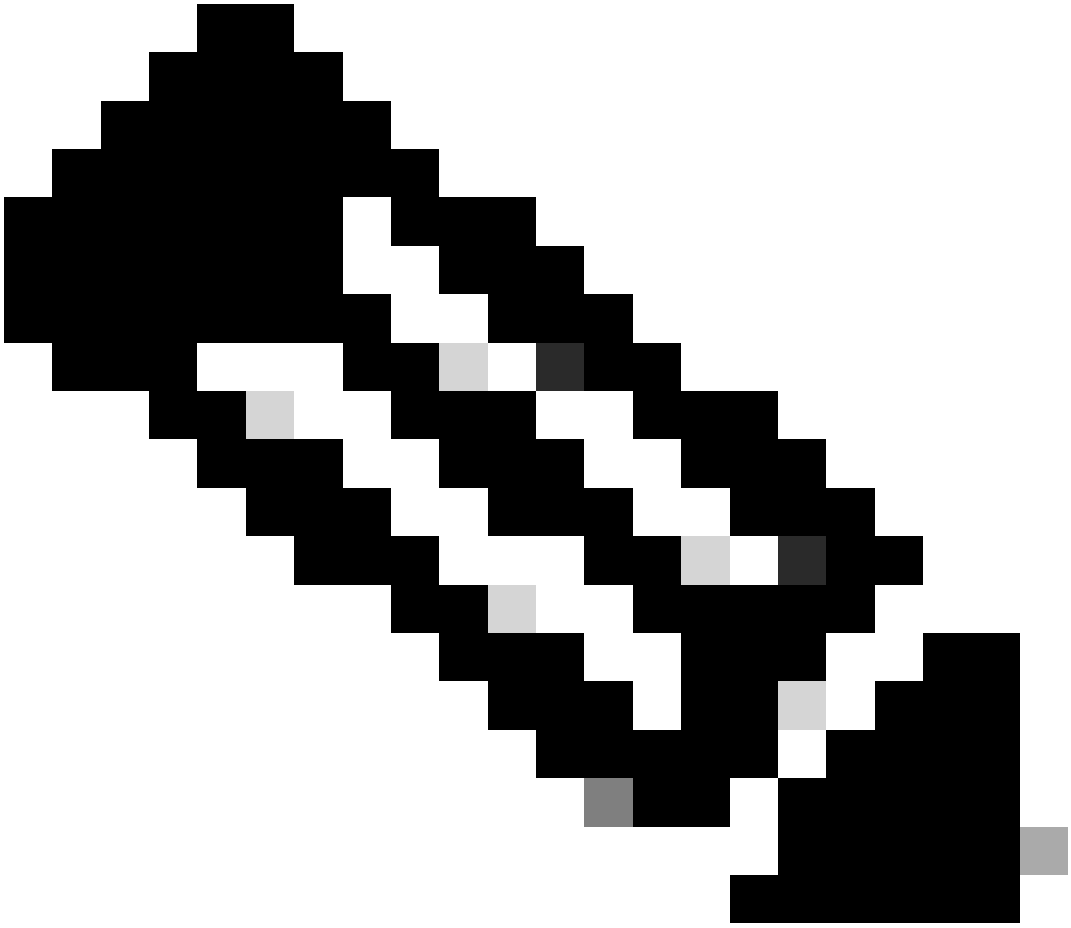
Umbrellaは通常、他の利点の中でも特に、内部ネットワーク上のすべてのDNSトラフィックをホストレベルで可視化し、このタイプの問題を迅速に特定できる仮想アプライアンス(VA)の実行を推奨しています。

ただし、Umbrellaサポートは、DNSをVAにポイントしていない内部ホストが感染し、代わりにWindows DNSサーバを介してDNS要求を送信する問題を特定することがあります。このシナリオでは、VAがDNS要求（およびその送信元IPアドレス）を参照する方法が明らかに存在しないため、そのDNSサーバを通過するすべてのDNSクエリはネットワークまたはサイトに対してログに記録されます。

# Server 2016より前のオペレーティングシステムの考慮事項

ただし、Server 2016より前のオペレーティングシステムでは、この情報はデフォルトではログに記録されません。データをキャプチャできるようにするには、手動で有効にする必要があります。特に、2012r2の場合、Microsoftからのホットフィックスをインストールすることで、このレベルのロギングを利用できます。

その他のOSの場合、およびDNSサーバでのデバッグロギングの設定の詳細については、このMicrosoftの記事でオプションと使用方法の概要を説明しています。



注：これらのオプションの設定と使用は、Umbrellaサポートの範囲に含まれません。

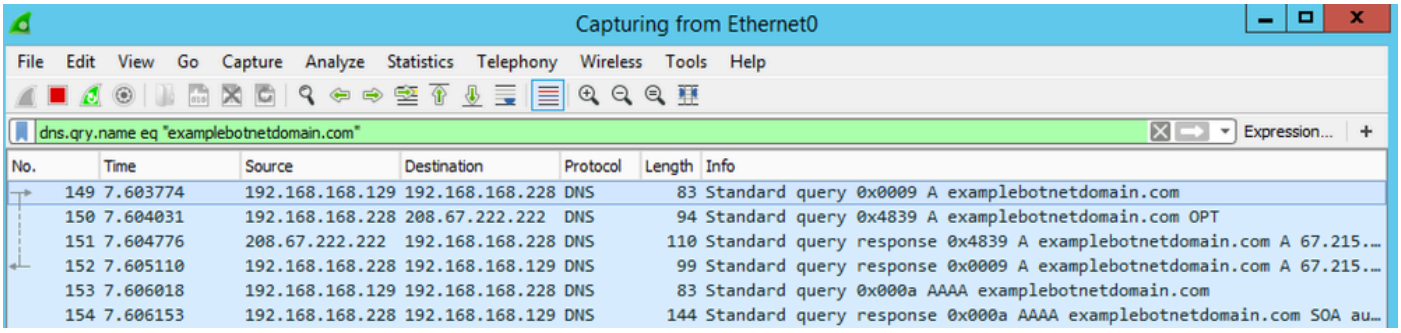
## 追加オプション

DNSを検索するためにフィルタを実行したままWiresharkキャプチャを実行すると、宛先Umbrellaがダッシュボードに記録されます。その後、要求の送信元を見つけるために十分な可視性を得ることができます。

たとえば、DNSサーバで実行されるこのキャプチャは、クライアント(192.168.168.129)がDNSサーバ(192.168.168.228)に要求を行い、次にDNSサーバがUmbrella工ニーキャストサーバ(208.67.222.222)にクエリを行い、応答を取得してクライアントに戻戻示します。

フィルタの提案は次のようになります。

```
dns.qry.name contains examplebotnetdomain
dns.qry.name eq "examplebotnetdomain.com"
```




examplebotnetdomain.pngファイル

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。