

Identify the Source of an Internal Infection

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Internal DNS Server Reporting Botnet Activity](#)

[Next Steps](#)

[Considerations for Pre-Server 2016 Operating Systems](#)

[Additional Options](#)

Introduction

This document describes how to identify the source of an internal infection in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Internal DNS Server Reporting Botnet Activity

If you see a large amount of unexpected traffic, or malware/botnet identified traffic logged against one of your networks or sites in the Umbrella Dashboard, there is a good chance that an internal host is infected. Because the DNS requests are likely to be going through an internal DNS server, the source IP of the request is being replaced with the IP of the DNS server which makes it difficult to track on a firewall.

If this is the case, there is nothing you can do with the Umbrella dashboard to identify the source. All requests can be logged against the network identity.

Next Steps

There are a few things you can do, but without any other security products that can track this behavior for you, the main one is to use the logs on the DNS server to see where the requests are coming from, then destroy the source.

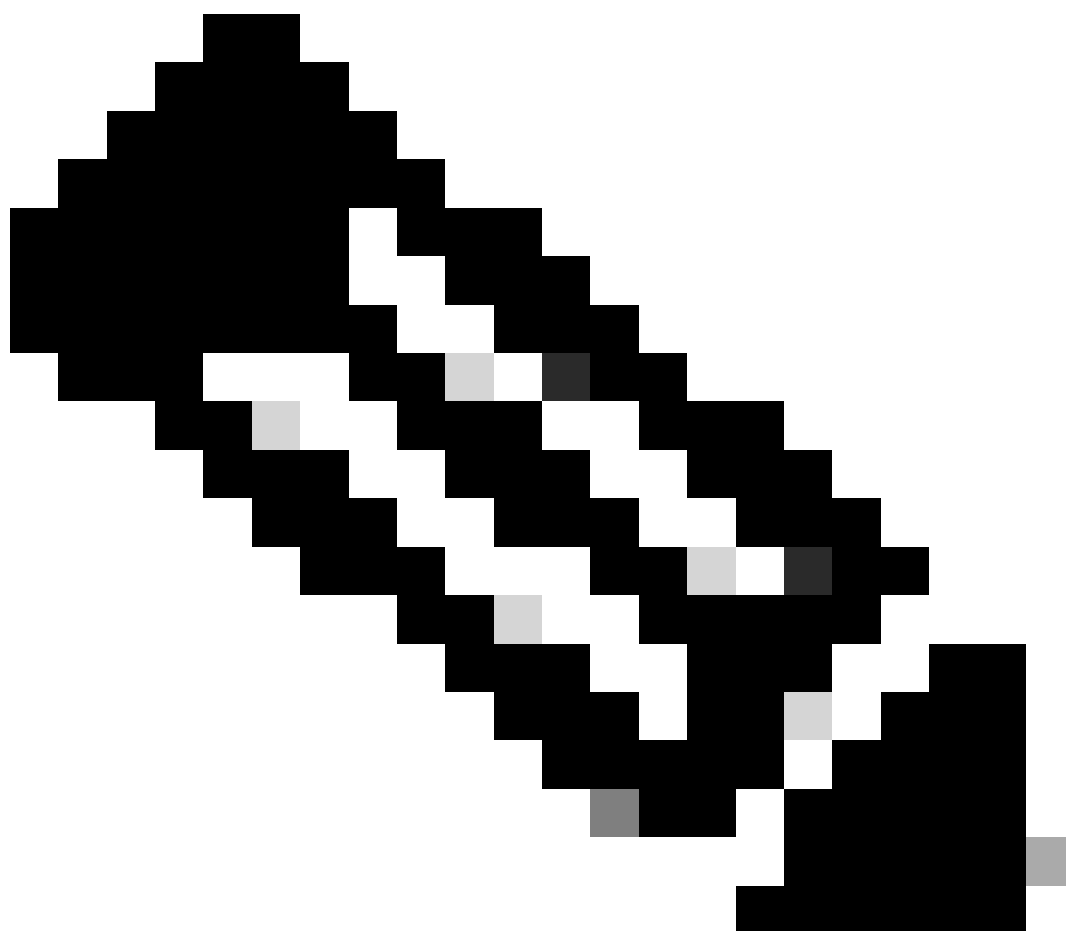
Umbrella normally recommends running the Virtual Appliance (VA) which, among [other benefits](#), can give host-level visibility of all DNS traffic on the internal network and quickly pinpoint this type of issue.

However, Umbrella Support sometimes identifies issues where an internal host which is not pointing DNS to the VAs is infected and sending DNS requests through a Windows DNS server instead. Because in this scenario there is obviously no way for the VA to see the DNS request (and therefore its source IP address), all DNS queries that go through that DNS server can be logged against the Network or site.

Considerations for Pre-Server 2016 Operating Systems

However, on pre-Server 2016 operating systems, this information is not logged by default. You need to enable it manually to then be able to capture the data. Notably, for 2012r2, you can install the [hotfix from Microsoft](#) to get this level of logging made available to you.

For other OS's, and for further information on setting up debug logging on the DNS server, this [Microsoft article](#) gives an overview of the options and usage.



Note: The configuration and use of these options do not fall within the scope for Umbrella Support.

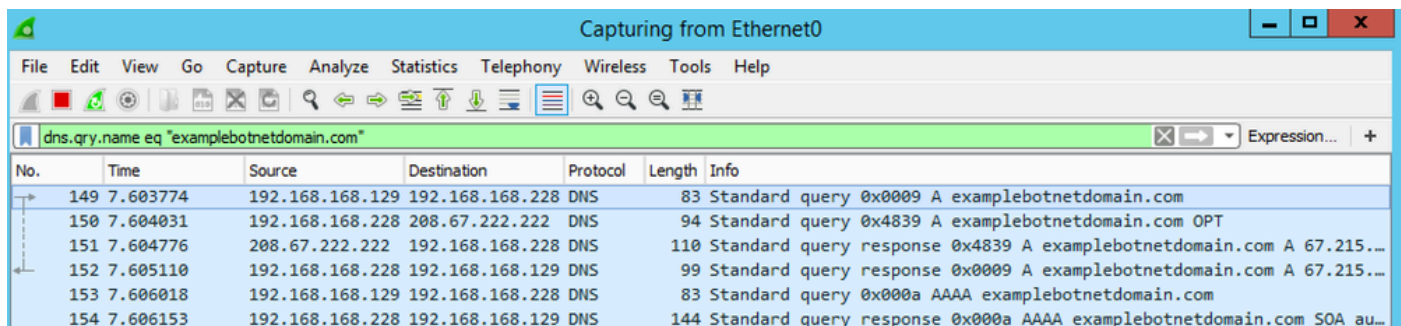
Additional Options

You can run a Wireshark capture with a filter left running looking for DNS and the destination Umbrella is logging in the dashboard. Then you can have enough visibility to find the source of the request.

For example, this capture run on a DNS server shows the client (192.168.168.129) making the request to the DNS server (192.168.168.228), then the DNS server making the query to the Umbrella Anycast servers (208.67.222.222), getting a response and serving this back to the client.

A filter suggestion would be something like these:

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



The screenshot shows a Wireshark capture window titled "Capturing from Ethernet0". The filter bar contains the expression "dns.qry.name eq \"examplebotnetdomain.com\"". The packet list shows six packets:

No.	Time	Source	Destination	Protocol	Length	Info
149	7.603774	192.168.168.129	192.168.168.228	DNS	83	Standard query 0x0009 A examplebotnetdomain.com
150	7.604031	192.168.168.228	208.67.222.222	DNS	94	Standard query 0x4839 A examplebotnetdomain.com OPT
151	7.604776	208.67.222.222	192.168.168.228	DNS	110	Standard query response 0x4839 A examplebotnetdomain.com A 67.215...
152	7.605110	192.168.168.228	192.168.168.129	DNS	99	Standard query response 0x0009 A examplebotnetdomain.com A 67.215...
153	7.606018	192.168.168.129	192.168.168.228	DNS	83	Standard query 0x000a AAAA examplebotnetdomain.com
154	7.606153	192.168.168.228	192.168.168.129	DNS	144	Standard query response 0x000a AAAA examplebotnetdomain.com SOA au...

examplebotnetdomain.png