确定内部感染源

目录

简介

本文档介绍如何识别Cisco Umbrella中的内部感染源。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

内部DNS服务器报告僵尸网络活动

如果您在Umbrella Dashboard中看到大量意外流量，或针对您的一个网络或站点记录的恶意软件/僵尸网络识别流量，则内部主机很可能会被感染。由于DNS请求可能通过内部DNS服务器，因此请求的源IP将替换为DNS服务器的IP，这样在防火墙上很难进行跟踪。

如果出现这种情况，您就无法使用Umbrella控制面板来识别源。 所有请求都可以根据网络身份进行记录。

后续步骤

您可以执行一些操作，但是如果没有其他任何安全产品可以跟踪此行为，主要操作是使用DNS服务器上的日志来查看请求来自何处，然后销毁源。

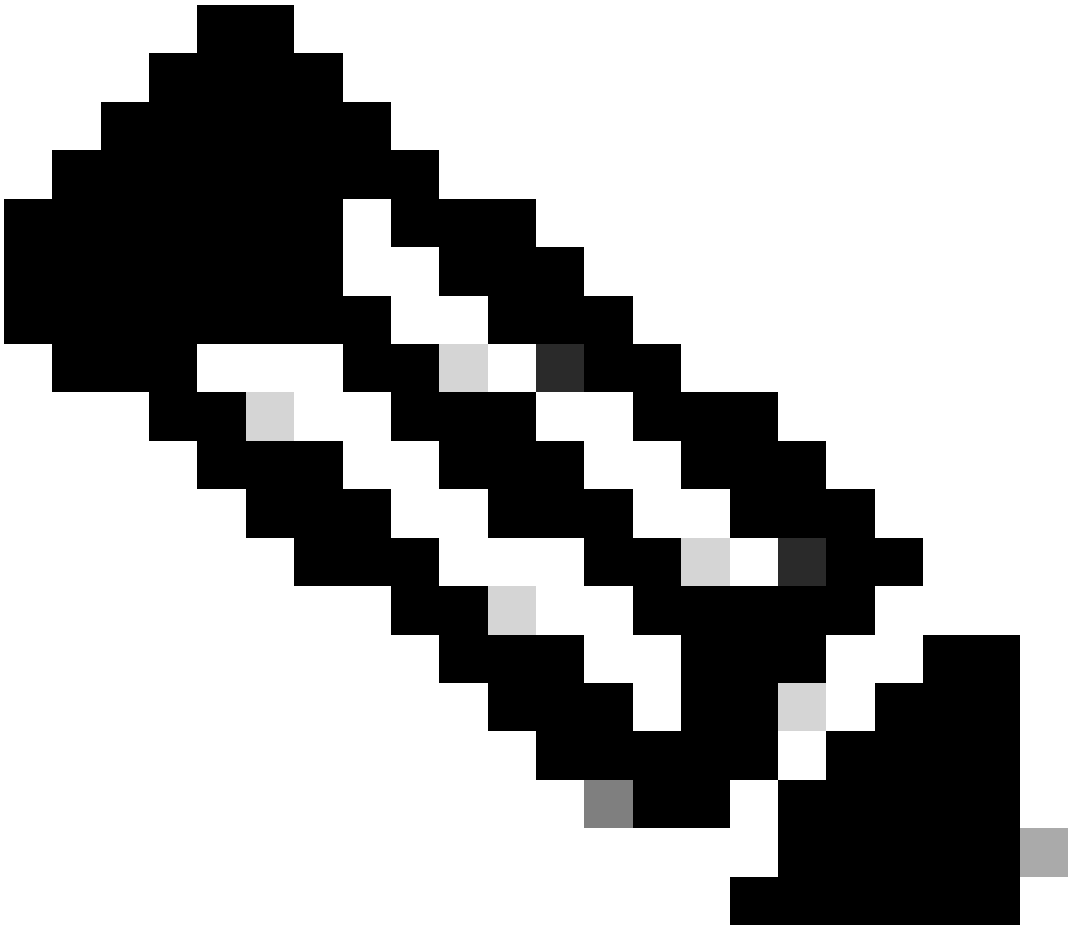
Umbrella通常建议运行虚拟设备(VA)，除了其他优点外，它还可提供内部网络上所有DNS流量的主机级可视性，并快速查明此类问题。

但是，Umbrella支持有时会识别内部主机被感染的问题，该主机不是指向VA的DNS，而是通过Windows DNS服务器发送DNS请求。因为在这种情况下，VA显然无法查看DNS请求（及其源IP地址），所以通过该DNS服务器的所有DNS查询都可以针对网络或站点进行记录。

Pre-Server 2016操作系统的注意事项

但是，在Server 2016之前的操作系统上，默认情况下不记录此信息。您需要手动启用它才能捕获数据。特别要注意的是，对于2012r2，您可以从Microsoft安装修补程序，以获得此级别的日志记录。

对于其他操作系统，以及有关在DNS服务器上设置调试日志记录的详细信息，此Microsoft文章概述了这些选项和用法。



注意：这些选项的配置和使用不属于Umbrella支持的范围。

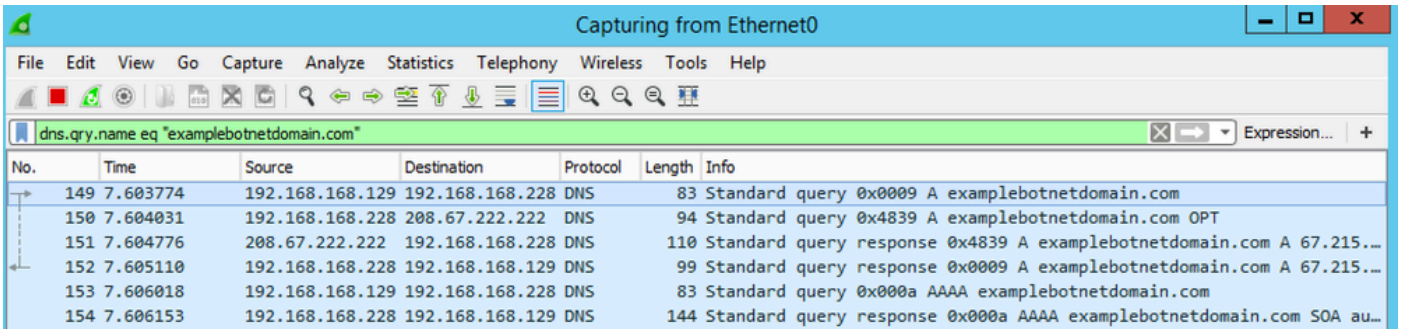
其它选项

您可以运行Wireshark捕获，其中过滤器处于剩余状态，正在查找DNS，而目标Umbrella正在登录控制面板。然后，您可以获得足够的可视性来查找请求的来源。

例如，此捕获在DNS服务器上运行，显示客户端(192.168.168.129)向DNS服务器(192.168.168.228)发出请求，然后DNS服务器向Umbrella任播服务器发出查询(208.67.222.222)，获取响应并将该请求发回客户端。

过滤建议类似于以下内容：

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



examplebotnetdomain.png

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）。