確定內部感染源

目錄

簡介

本檔案介紹如何在Cisco Umbrella中識別內部感染來源。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科資安防護傘

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

內部DNS伺服器報告殭屍網路活動

如果您在Umbrella Dashboard中看到大量意外流量，或針對您的一個網路或站點記錄的惡意軟體/殭屍網路識別流量，則內部主機很可能會受到感染。由於DNS請求可能通過內部DNS伺服器，因此該請求的源IP將替換為DNS伺服器的IP，這使得在防火牆上難以跟蹤。

如果是這種情況，則無法使用Umbrella控制面板來識別源。 可以根據網路標識記錄所有請求。

後續步驟

您可以執行一些操作，但是如果沒有其他任何可以跟蹤此行為的安全產品，主要的方法是使用DNS伺服器上的日誌來檢視請求來自何處，然後銷毀源。

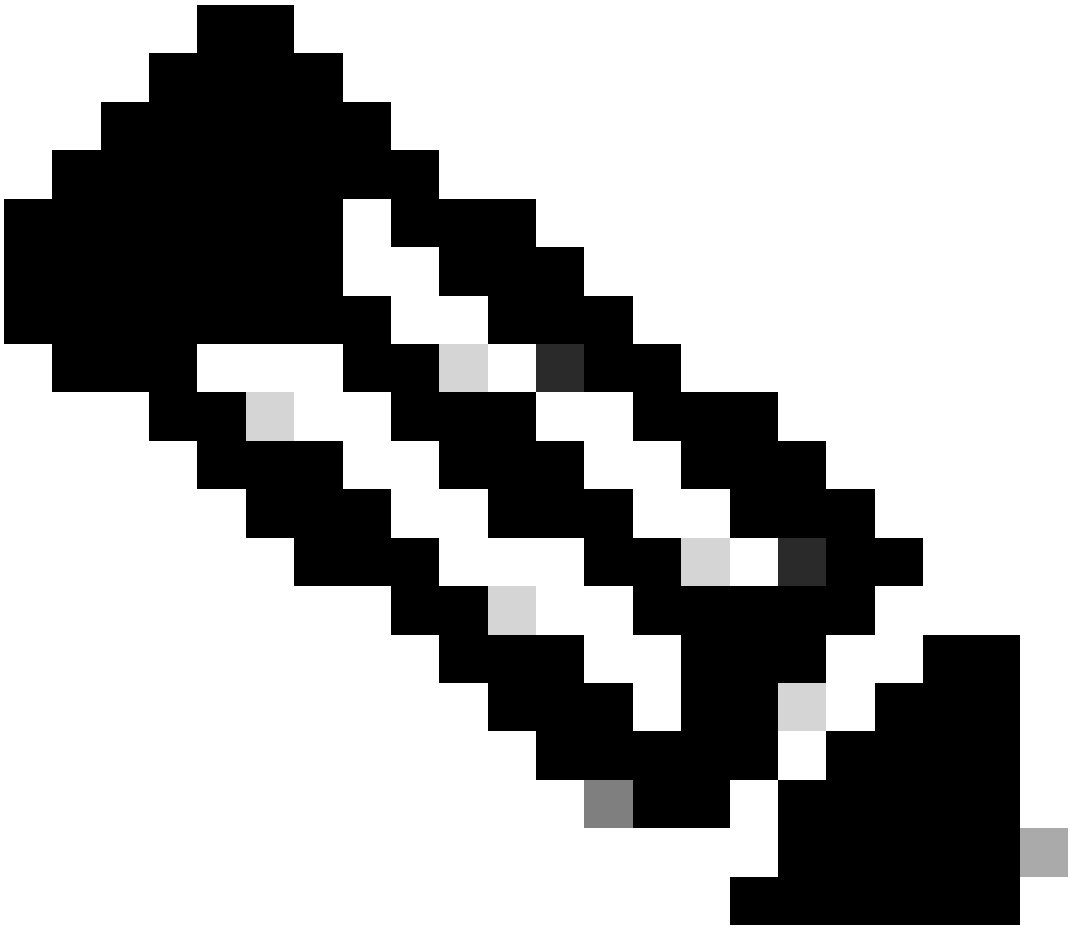
Umbrella通常建議運行虛擬設備(VA)，除了其他優點外，它還可提供內部網路上所有DNS流量的主機級可見性，並快速查明此類問題。

但是，Umbrella支援有時會發現內部主機沒有指向VA的DNS被感染的問題，而是通過Windows DNS伺服器傳送DNS請求。由於在此案例中，VA顯然無法檢視DNS請求（因此也無法檢視其源IP地址），因此通過該DNS伺服器的所有DNS查詢都可以針對網路或站點進行記錄。

Pre-Server 2016作業系統的注意事項

但是，在Server 2016之前的作業系統上，預設情況下不記錄此資訊。您需要手動啟用它才能捕獲資料。特別要注意的是，對於2012r2，您可以從Microsoft安裝修補程式，以獲得此級別的日誌記錄。

有關其他作業系統以及在DNS伺服器上設定調試日誌記錄的詳細資訊，此Microsoft文章概述了這些選項和使用情況。



附註：這些選項的配置和使用不在Umbrella支援的範圍內。

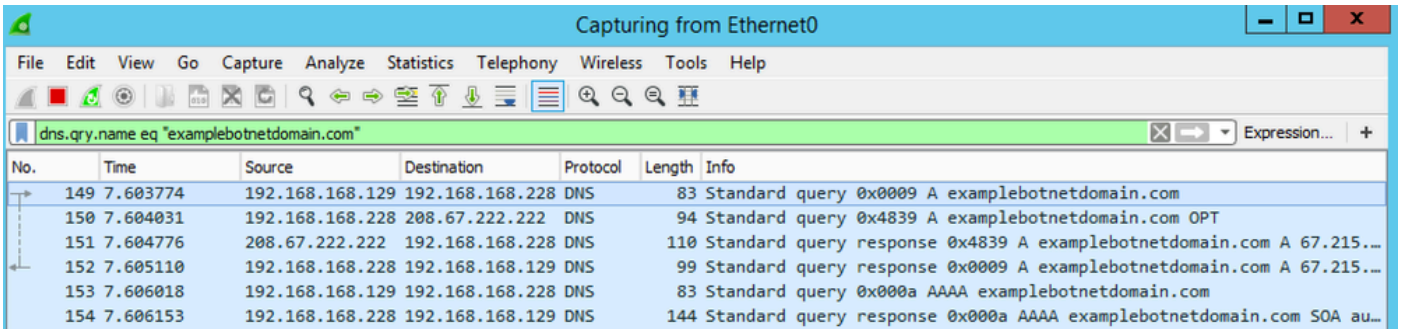
其他選項

您可以運行Wireshark捕獲，並且篩選器保持運行狀態以查詢DNS，並且目標Umbrella正在儀表板中記錄。然後，您就可以有足夠的能見度來查詢請求的來源。

例如，此捕獲在DNS伺服器上運行顯示客戶端(192.168.168.129)向DNS伺服器(192.168.168.228)發出請求，然後DNS伺服器向Umbrella任播伺服器(208.67.222.222)發出查詢，獲取響應並將該響應發回客戶端。

過濾建議大致如下：

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



示例botnetdomain.png

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。