Identifizieren der Quelle einer internen Infektion

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Quelle einer internen Infektion in Cisco Umbrella identifizieren.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Interne DNS-Server-Reporting-Botnet-Aktivität

Wenn Sie eine große Menge unerwarteten Datenverkehrs oder von Malware/Botnet identifizierten Datenverkehrs sehen, der in einem Ihrer Netzwerke oder Standorte im Umbrella Dashboard protokolliert wird, besteht eine gute Chance, dass ein interner Host infiziert ist. Da die DNS-Anfragen wahrscheinlich einen internen DNS-Server durchlaufen, wird die Quell-IP der Anfrage durch die IP des DNS-Servers ersetzt, was die Nachverfolgung auf einer Firewall erschwert.

Wenn dies der Fall ist, können Sie die Quelle nicht mit dem Umbrella Dashboard identifizieren. Alle Anfragen können anhand der Netzwerkidentität protokolliert werden.

Nächste Schritte

Es gibt ein paar Dinge, die Sie tun können, aber ohne andere Sicherheitsprodukte, die dieses Verhalten für Sie verfolgen können, ist das wichtigste, die Protokolle auf dem DNS-Server zu verwenden, um zu sehen, woher die Anfragen kommen, und dann zerstören die Quelle.

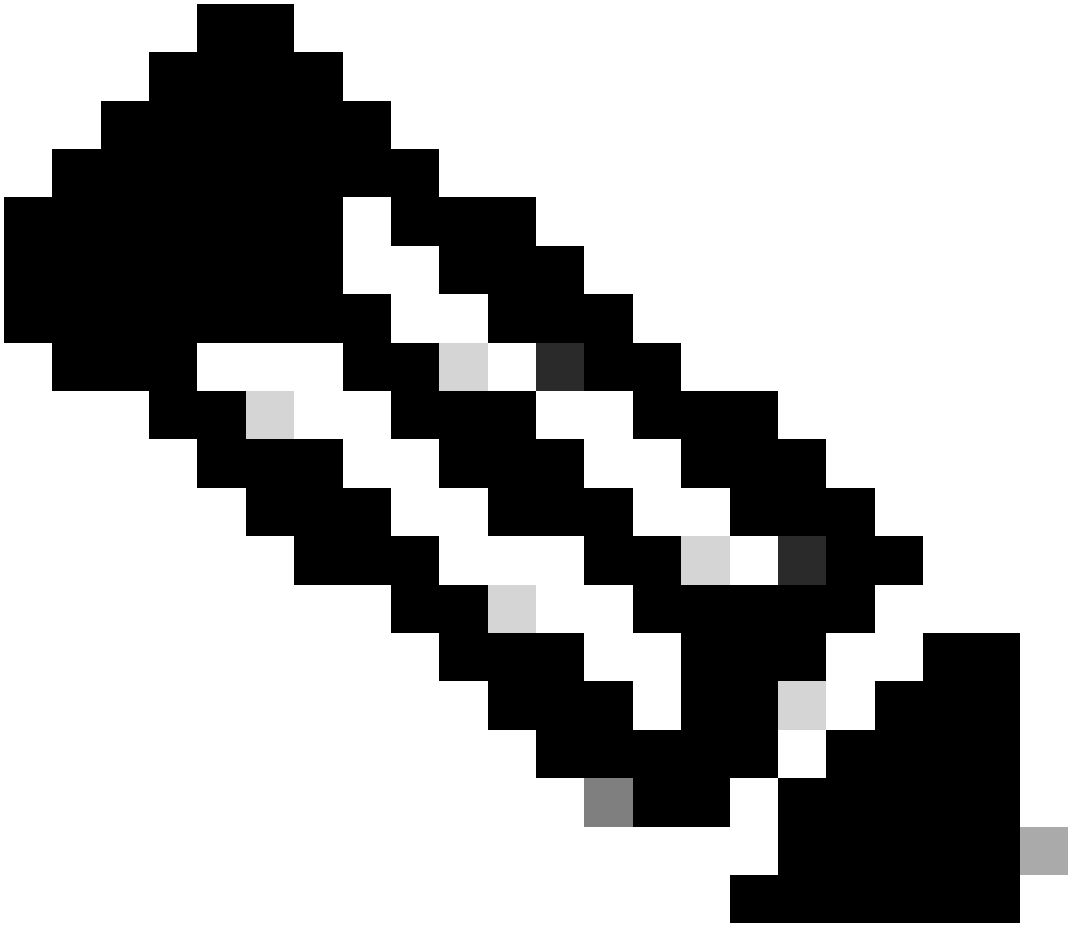
Umbrella empfiehlt normalerweise, die virtuelle Appliance (VA) auszuführen, die neben anderen Vorteilen Transparenz auf Hostebene für den gesamten DNS-Datenverkehr im internen Netzwerk bieten und diese Art von Problem schnell identifizieren kann.

Umbrella Support identifiziert jedoch manchmal Probleme, bei denen ein interner Host, der nicht auf die VAs verweist, infiziert ist, und sendet stattdessen DNS-Anfragen über einen Windows DNS-Server. Da die VA in diesem Szenario die DNS-Anforderung (und damit die Quell-IP-Adresse) offensichtlich nicht sehen kann, können alle DNS-Abfragen, die diesen DNS-Server durchlaufen, im Netzwerk oder am Standort protokolliert werden.

Überlegungen zu Betriebssystemen vor Server 2016

Unter Betriebssystemen vor Server 2016 werden diese Informationen jedoch nicht standardmäßig protokolliert. Sie müssen diese Option manuell aktivieren, um die Daten dann erfassen zu können. Beachten Sie, für 2012r2, können Sie den Hotfix von Microsoft installieren, um diese Ebene der Protokollierung zur Verfügung zu stellen.

Für andere Betriebssysteme und für weitere Informationen zum Einrichten der Debug-Protokollierung auf dem DNS-Server gibt dieser Microsoft-Artikel einen Überblick über die Optionen und die Verwendung.



Anmerkung: Die Konfiguration und Verwendung dieser Optionen fällt nicht in den Anwendungsbereich von Umbrella Support.

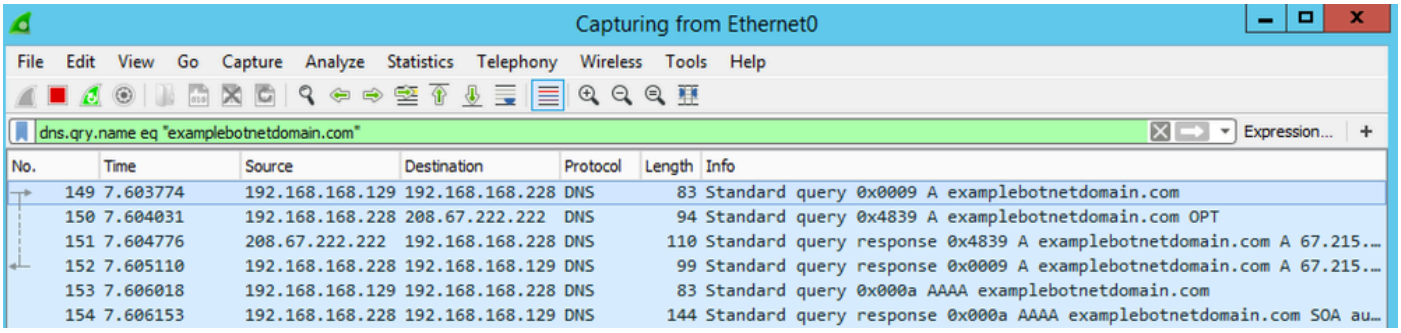
Zusätzliche Optionen

Sie können eine Wireshark-Erfassung mit einem Filter ausführen, der links auf der Suche nach DNS ausgeführt wird, und das Ziel, das Umbrella im Dashboard anmeldet. So haben Sie genügend Transparenz, um die Quelle der Anfrage zu finden.

Bei dieser Erfassung auf einem DNS-Server wird beispielsweise der Client (192.168.168.129) angezeigt, der die Anforderung an den DNS-Server (192.168.168.228) sendet, während der DNS-Server die Abfrage an die Umbrella Anycast Server sendet. (208.67.222.222), eine Antwort erhält und diese an den Client zurücksendet.

Ein Filtervorschlag sieht in etwa wie folgt aus:

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



BeispielBotnetdomain.png

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.