Identificeer de bron van een interne infectie

Inhoud

Inleiding

In dit document wordt beschreven hoe de bron van een interne infectie in Cisco Umbrella kan worden geïdentificeerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Interne DNS-server rapporteert botnetactiviteit

Als u een grote hoeveelheid onverwacht verkeer of geïdentificeerd verkeer van malware / botnet ziet dat is vastgelegd tegen een van uw netwerken of sites in het Umbrella Dashboard, is de kans groot dat een interne host is geïnfecteerd. Omdat de DNS-verzoeken waarschijnlijk via een interne DNS-server gaan, wordt de bron-IP van het verzoek vervangen door het IP van de DNS-server, waardoor het moeilijk is om op een firewall te volgen.

Als dit het geval is, kunt u niets doen met het Umbrella-dashboard om de bron te identificeren. Alle verzoeken kunnen worden geregistreerd tegen de netwerkidentiteit.

Volgende stappen

Er zijn een paar dingen die u kunt doen, maar zonder andere beveiligingsproducten die dit gedrag voor u kunnen volgen, is de belangrijkste om de logs op de DNS-server te gebruiken om te zien waar de verzoeken vandaan komen en vervolgens de bron te vernietigen.

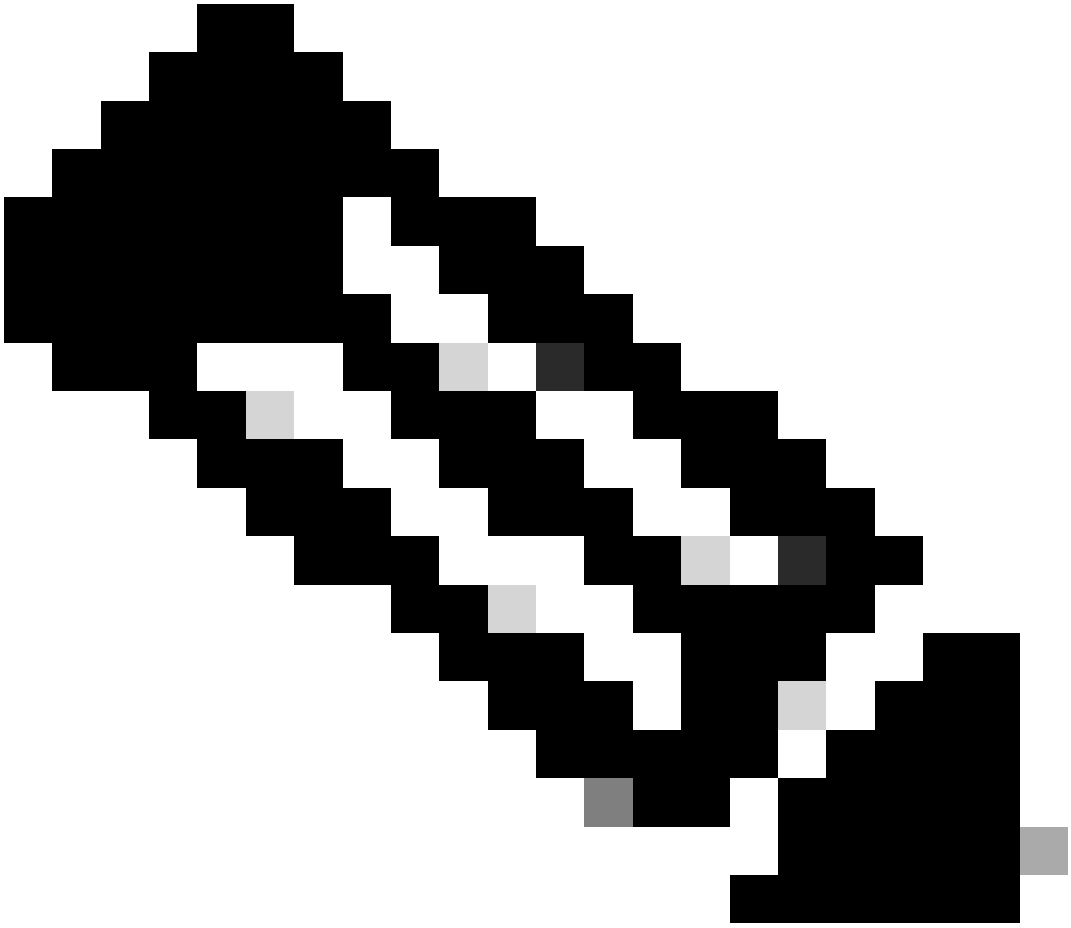
Umbrella raadt normaal gesproken het uitvoeren van de Virtual Appliance (VA), die, naast andere voordelen, kan geven host-level zichtbaarheid van alle DNS-verkeer op het interne netwerk en snel lokaliseren van dit type probleem.

Umbrella Support identificeert echter soms problemen waarbij een interne host die niet naar DNS wijst naar de VA's, is geïnfecteerd en in plaats daarvan DNS-verzoeken verzendt via een Windows DNS-server. Omdat in dit scenario is er duidelijk geen manier voor de VA om de DNS-verzoek (en dus de bron IP-adres) te zien, kunnen alle DNS query's die gaan door die DNS-server worden aangemeld tegen het netwerk of de site.

Overwegingen voor Pre-Server 2016-besturingssystemen

Op pre-Server 2016-besturingssystemen wordt deze informatie echter niet standaard vastgelegd. U moet het handmatig inschakelen om vervolgens de gegevens te kunnen vastleggen. Met name voor 2012r2 kunt u de hotfix van Microsoft installeren om dit logniveau beschikbaar te maken.

Voor andere besturingssystemen en voor meer informatie over het instellen van debug-logging op de DNS-server, geeft dit Microsoft-artikel een overzicht van de opties en het gebruik.



Opmerking: de configuratie en het gebruik van deze opties vallen niet binnen het bereik van Umbrella Support.

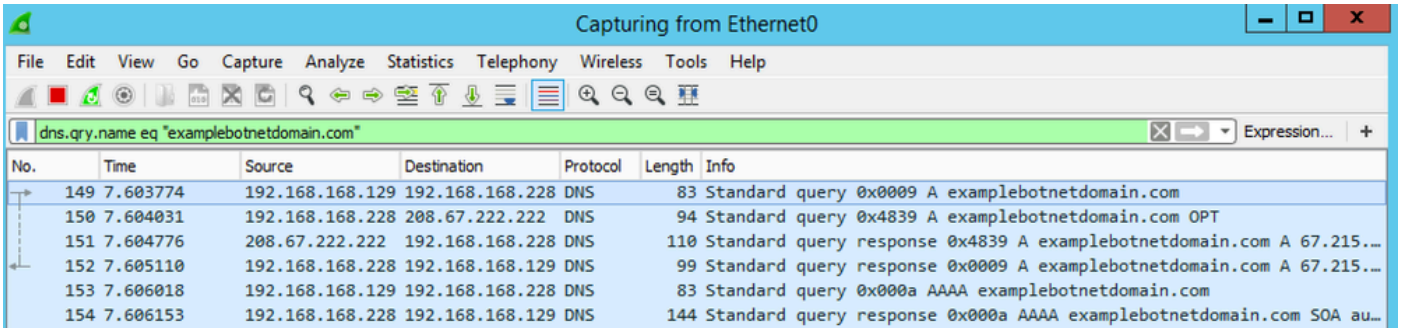
Extra opties

U kunt een Wireshark-opname uitvoeren met een filter dat is uitgevoerd op zoek naar DNS en de bestemmingsparambrella logt in op het dashboard. Dan kunt u voldoende zichtbaarheid hebben om de bron van het verzoek te vinden.

Bijvoorbeeld, deze capture run op een DNS-server toont de client (192.168.168.129) het maken van het verzoek aan de DNS-server (192.168.168.228), vervolgens de DNS-server het maken van de query naar de Umbrella Anycast servers (208.67.222.222), het krijgen van een antwoord en het dienen van deze terug naar de client.

Een filtersuggestie zou zoiets zijn als deze:

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



voorbeeld botnetdomain.png

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.