Identifier la source d'une infection interne

Table des matières

Introduction

Ce document décrit comment identifier la source d'une infection interne dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Activité de botnet de signalement de serveur DNS interne

Si vous voyez un trafic inattendu important, ou si le trafic identifié par un programme malveillant ou un botnet est consigné sur l'un de vos réseaux ou sites dans le tableau de bord Umbrella, il y a de fortes chances qu'un hôte interne soit infecté. Étant donné que les requêtes DNS sont susceptibles d’être acheminées via un serveur DNS interne, l’adresse IP source de la requête est remplacée par l’adresse IP du serveur DNS, ce qui rend difficile le suivi sur un pare-feu.

Si c'est le cas, il n'y a rien que vous puissiez faire avec le tableau de bord Umbrella pour identifier la source. Toutes les requêtes peuvent être consignées par rapport à l'identité réseau.

Étapes suivantes

Il y a quelques choses que vous pouvez faire, mais sans aucun autre produit de sécurité qui peut suivre ce comportement pour vous, le principal est d'utiliser les journaux sur le serveur DNS pour voir d'où viennent les requêtes, puis détruire la source.

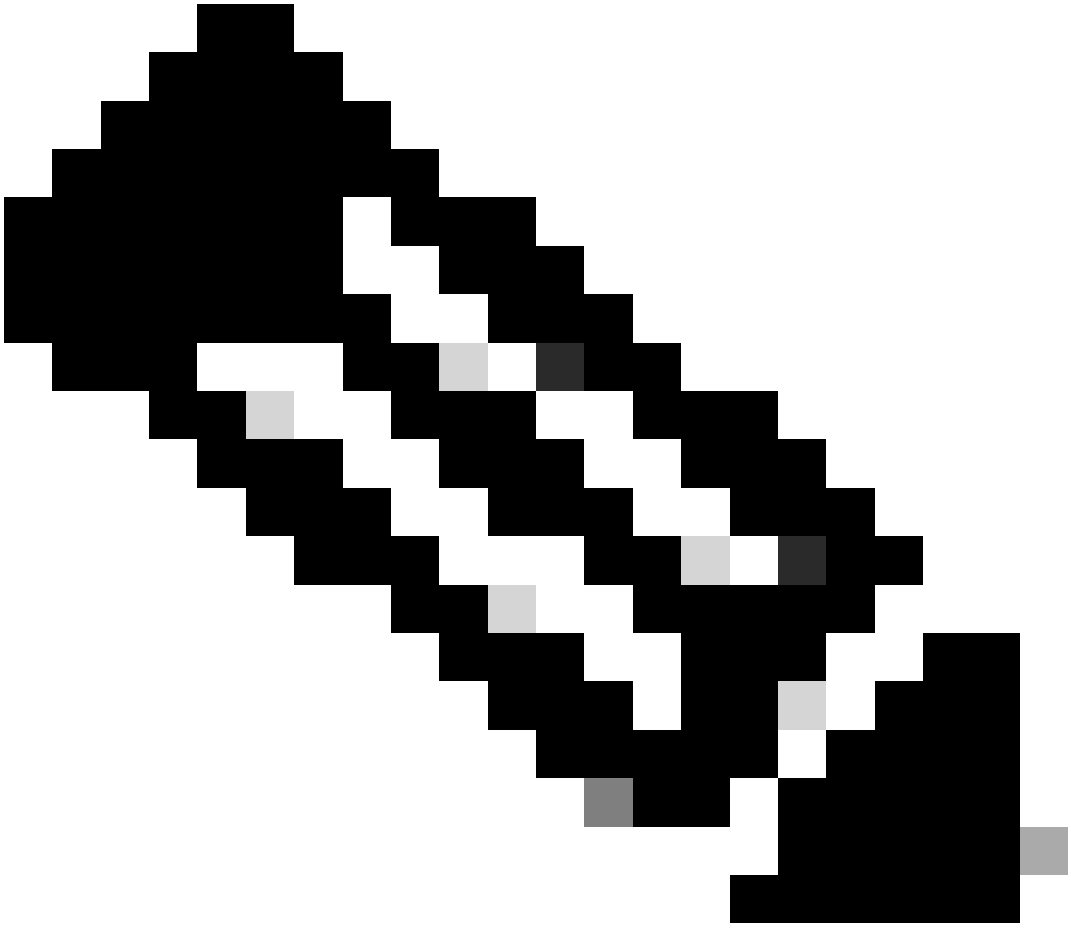
Umbrella recommande normalement d'exécuter l'appliance virtuelle (VA) qui, entre autres avantages, peut fournir une visibilité au niveau de l'hôte de tout le trafic DNS sur le réseau interne et identifier rapidement ce type de problème.

Cependant, Umbrella Support identifie parfois des problèmes où un hôte interne qui ne pointe pas DNS vers les VA est infecté et envoie des requêtes DNS via un serveur DNS Windows à la place. Comme dans ce scénario, il n'y a évidemment aucun moyen pour l'AV de voir la requête DNS (et donc son adresse IP source), toutes les requêtes DNS qui passent par ce serveur DNS peuvent être enregistrées sur le réseau ou le site.

Considérations relatives aux systèmes d'exploitation antérieurs à Server 2016

Toutefois, sur les systèmes d'exploitation antérieurs à Server 2016, ces informations ne sont pas consignées par défaut. Vous devez l'activer manuellement pour pouvoir ensuite capturer les données. Notamment, pour 2012r2, vous pouvez installer le correctif logiciel de Microsoft pour obtenir ce niveau de journalisation mis à votre disposition.

Pour les autres systèmes d'exploitation et pour plus d'informations sur la configuration de la journalisation de débogage sur le serveur DNS, cet article Microsoft donne une vue d'ensemble des options et de l'utilisation.



Remarque : La configuration et l'utilisation de ces options ne font pas partie du champ d'application d'Umbrella Support.

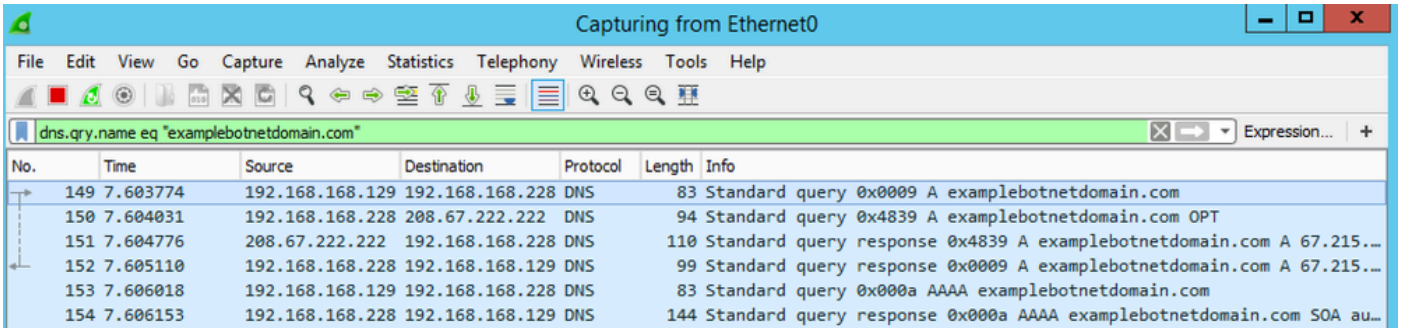
Options supplémentaires

Vous pouvez exécuter une capture Wireshark avec un filtre à gauche en cours d'exécution à la recherche de DNS et la destination Umbrella se connecte dans le tableau de bord. Vous disposez alors d'une visibilité suffisante pour trouver la source de la demande.

Par exemple, cette capture exécutée sur un serveur DNS montre le client (192.168.168.129) qui effectue la requête au serveur DNS (192.168.168.228), puis le serveur DNS qui effectue la requête aux serveurs Umbrella Anycast (208.67.222.222), obtient une réponse et la renvoie au client.

Une suggestion de filtre pourrait ressembler à ceci :

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



exemple botnetdomain.png

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.