Identificar el origen de una infección interna

Contenido

Introducción

Este documento describe cómo identificar el origen de una infección interna en Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Actividad de botnet de notificación de servidor DNS interno

Si observa una gran cantidad de tráfico inesperado o tráfico identificado por malware/botnet registrado en una de sus redes o sitios en el panel de Umbrella, existe una gran probabilidad de que un host interno esté infectado. Dado que es probable que las solicitudes DNS pasen a través de un servidor DNS interno, la IP de origen de la solicitud se está sustituyendo por la IP del servidor DNS, lo que dificulta el seguimiento en un firewall.

Si este es el caso, no puede hacer nada con el panel de Umbrella para identificar el origen. Todas las solicitudes se pueden registrar con la identidad de la red.

Pasos siguientes

Hay algunas cosas que puede hacer, pero sin ningún otro producto de seguridad que pueda rastrear este comportamiento por usted, el principal es utilizar los registros en el servidor DNS para ver de dónde vienen las solicitudes, y luego destruir el origen.

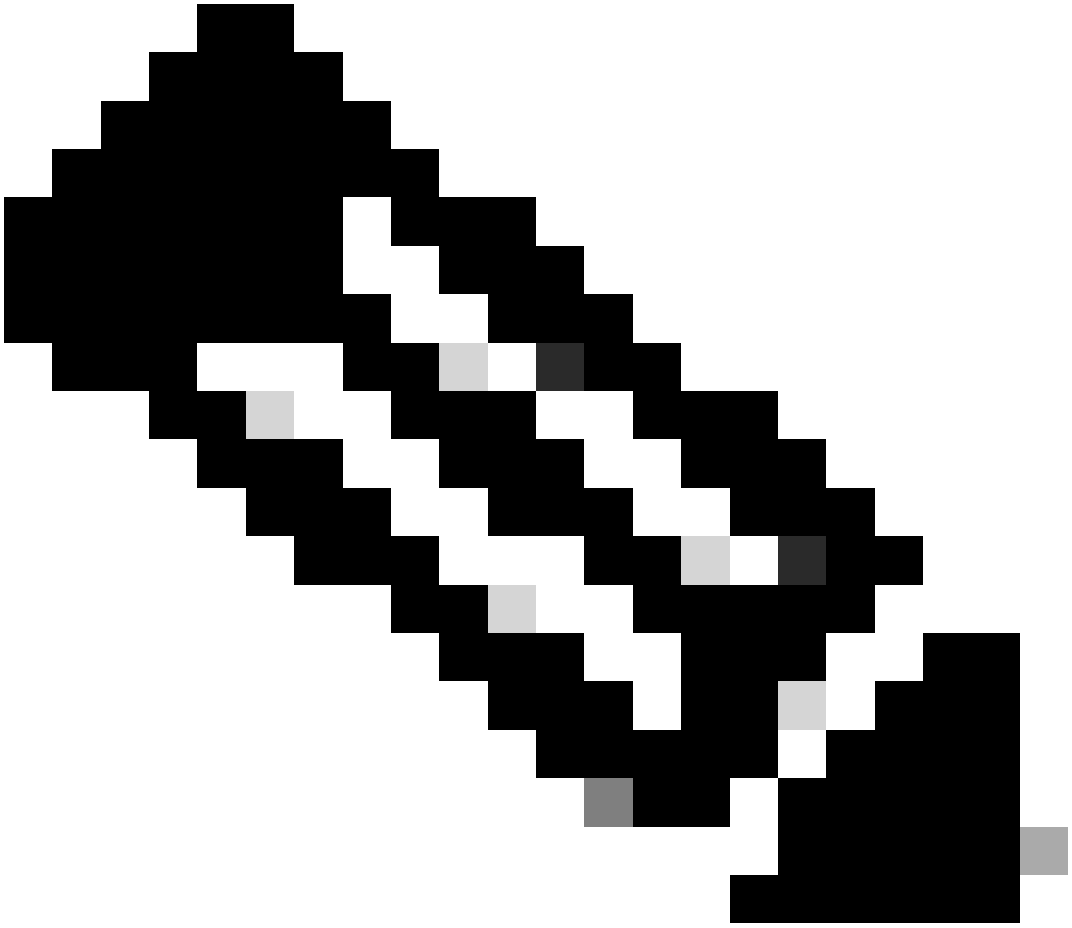
Umbrella normalmente recomienda ejecutar el dispositivo virtual (VA) que, entre otras ventajas, puede proporcionar visibilidad a nivel de host de todo el tráfico DNS en la red interna y detectar rápidamente este tipo de problema.

Sin embargo, Umbrella Support a veces identifica problemas en los que un host interno que no señala DNS a los VA está infectado y envía solicitudes DNS a través de un servidor DNS de Windows en su lugar. Debido a que en este escenario obviamente no hay manera de que el VA vea la solicitud DNS (y por lo tanto su dirección IP de origen), todas las consultas DNS que pasan a través de ese servidor DNS se pueden registrar en la red o el sitio.

Consideraciones para los sistemas operativos anteriores a 2016

Sin embargo, en los sistemas operativos anteriores a Server 2016, esta información no se registra de forma predeterminada. Debe activarlo manualmente para poder capturar los datos a continuación. En particular, para 2012r2, puede instalar la revisión de Microsoft para obtener este nivel de registro puesto a su disposición.

Para otros sistemas operativos y para obtener más información sobre la configuración del registro de depuración en el servidor DNS, este artículo de Microsoft ofrece una descripción general de las opciones y el uso.



Nota: La configuración y el uso de estas opciones no entran en el ámbito de Umbrella Support.

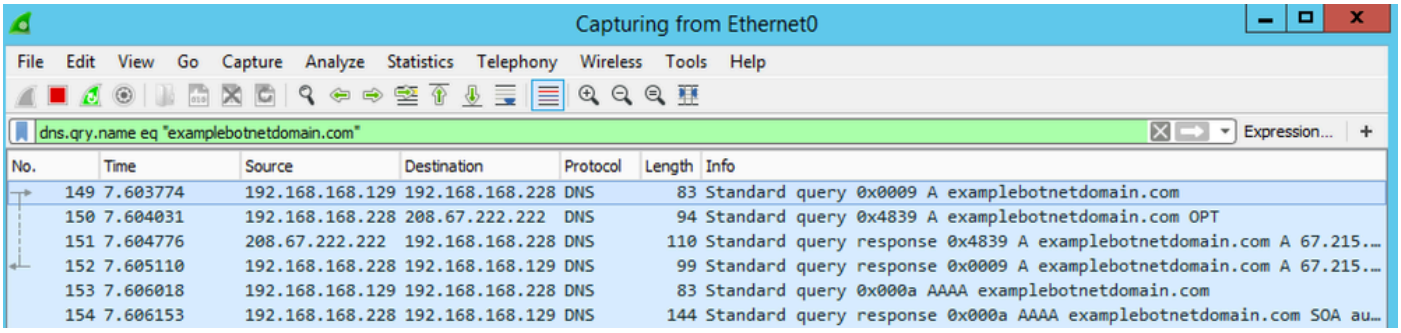
Opciones adicionales

Puede ejecutar una captura de Wireshark con un filtro que se deja en ejecución en busca de DNS y el destino Umbrella está registrando en el panel. A continuación, puede tener suficiente visibilidad para encontrar el origen de la solicitud.

Por ejemplo, esta captura ejecutada en un servidor DNS muestra al cliente (192.168.168.129) realizando la solicitud al servidor DNS (192.168.168.228) y, a continuación, al servidor DNS realizando la consulta a los servidores Umbrella Anycast (208.67.222.222), obteniendo una respuesta y respondiendo al cliente.

Una sugerencia de filtro sería algo como esto:

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



examplebotnetdomain.png

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).