Identifique a origem de uma infecção interna

Contents

Introdução

Este documento descreve como identificar a origem de uma infecção interna no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Servidor DNS Interno Relatando Atividade de Botnet

Se você vir uma grande quantidade de tráfego inesperado ou tráfego identificado por malware/botnet registrado em uma de suas redes ou sites no Umbrella Dashboard, há uma boa chance de que um host interno esteja infectado. Como as solicitações DNS provavelmente passarão por um servidor DNS interno, o IP de origem da solicitação está sendo substituído pelo IP do servidor DNS, o que dificulta o rastreamento em um firewall.

Se esse for o caso, não há nada que você possa fazer com o painel do Umbrella para identificar a origem. Todas as solicitações podem ser registradas na identidade da rede.

Próximas etapas

Há algumas coisas que você pode fazer, mas sem nenhum outro produto de segurança que possa rastrear esse comportamento para você, o principal é usar os logs no servidor DNS para ver de onde vêm as solicitações e, em seguida, destruir a origem.

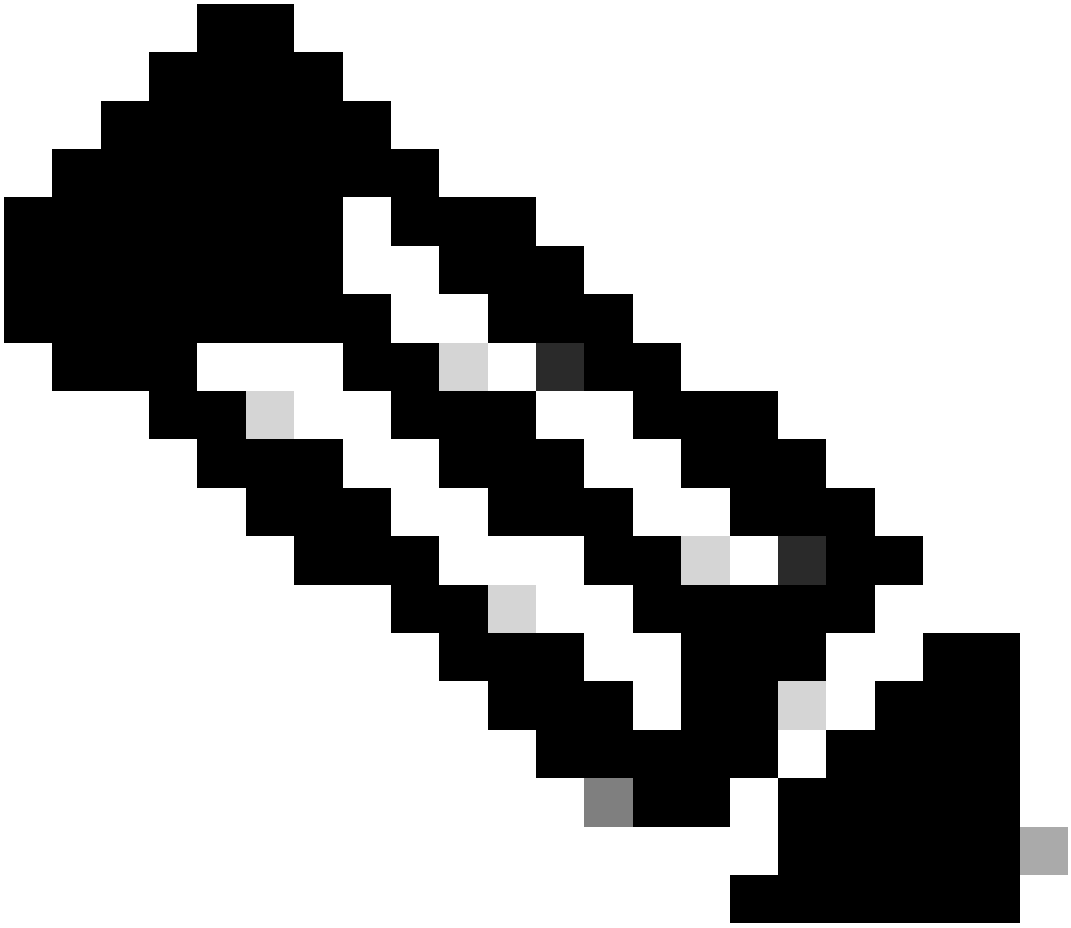
A Umbrella normalmente recomenda a execução do Virtual Appliance (VA) que, entre outros benefícios, pode dar visibilidade em nível de host de todo o tráfego DNS na rede interna e identificar rapidamente esse tipo de problema.

No entanto, o Umbrella Support às vezes identifica problemas em que um host interno que não está apontando DNS para os VAs está infectado e enviando solicitações DNS através de um servidor DNS do Windows. Como nesse cenário obviamente não há como o VA ver a solicitação DNS (e, portanto, seu endereço IP de origem), todas as consultas DNS que passam por esse servidor DNS podem ser registradas na rede ou no site.

Considerações sobre os sistemas operacionais anteriores ao servidor 2016

No entanto, em sistemas operacionais anteriores ao Server 2016, essas informações não são registradas por padrão. Você precisa ativá-lo manualmente para poder capturar os dados. Notavelmente, para 2012r2, você pode instalar o hotfix da Microsoft para obter esse nível de registro disponibilizado para você.

Para outros sistemas operacionais e para obter mais informações sobre como configurar o log de depuração no servidor DNS, este artigo da Microsoft fornece uma visão geral das opções e do uso.



Note: A configuração e o uso dessas opções não se enquadram no escopo do suporte Umbrella.

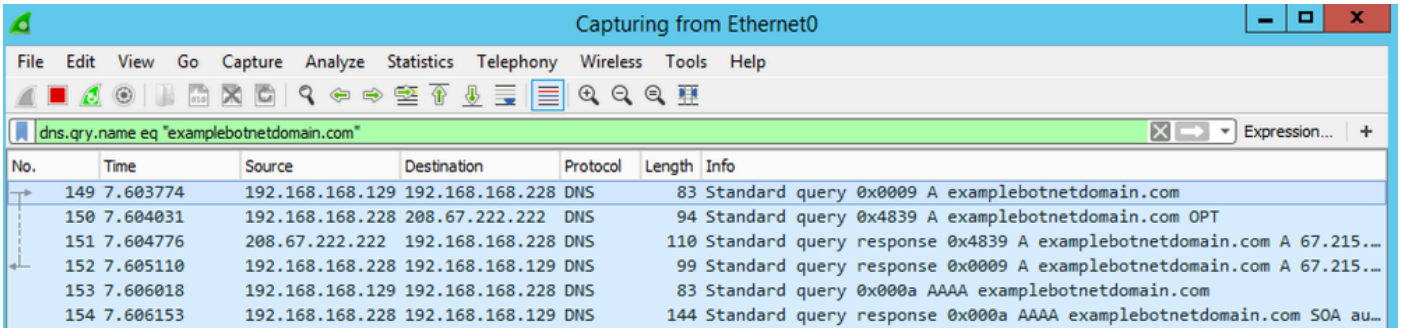
Opções adicionais

Você pode executar uma captura do Wireshark com um filtro restante em execução procurando DNS e o Umbrella de destino está fazendo login no painel. Em seguida, você poderá ter visibilidade suficiente para encontrar a origem da solicitação.

Por exemplo, essa captura executada em um servidor DNS mostra o cliente (192.168.168.129) fazendo a solicitação ao servidor DNS (192.168.168.228), em seguida, o servidor DNS fazendo a consulta aos servidores Umbrella Anycast (208.67.222.222), obtendo uma resposta e atendendo isso de volta ao cliente.

Uma sugestão de filtro seria algo como:

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



exemplo de botnetdomain.png

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.