Identificazione dell'origine di un'infezione interna

Sommario

Introduzione

Questo documento descrive come identificare l'origine di un'infezione interna in Cisco Umbrella.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Umbrella

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Attività botnet di report del server DNS interno

Se si rileva una grande quantità di traffico imprevisto o di traffico identificato da malware/botnet registrato su una delle reti o dei siti in Umbrella Dashboard, è possibile che un host interno sia infetto. Poiché è probabile che le richieste DNS passino attraverso un server DNS interno, l'IP di origine della richiesta viene sostituito con l'IP del server DNS, il che rende difficile tenere traccia di un firewall.

In questo caso, non è possibile utilizzare il dashboard Umbrella per identificare l'origine. Tutte le richieste possono essere registrate sull'identità di rete.

Fasi successive

È possibile eseguire alcune operazioni, ma senza altri prodotti di sicurezza in grado di tenere traccia automaticamente di questo comportamento, il principale consiste nell'utilizzare i registri nel server DNS per individuare l'origine delle richieste e quindi eliminare l'origine.

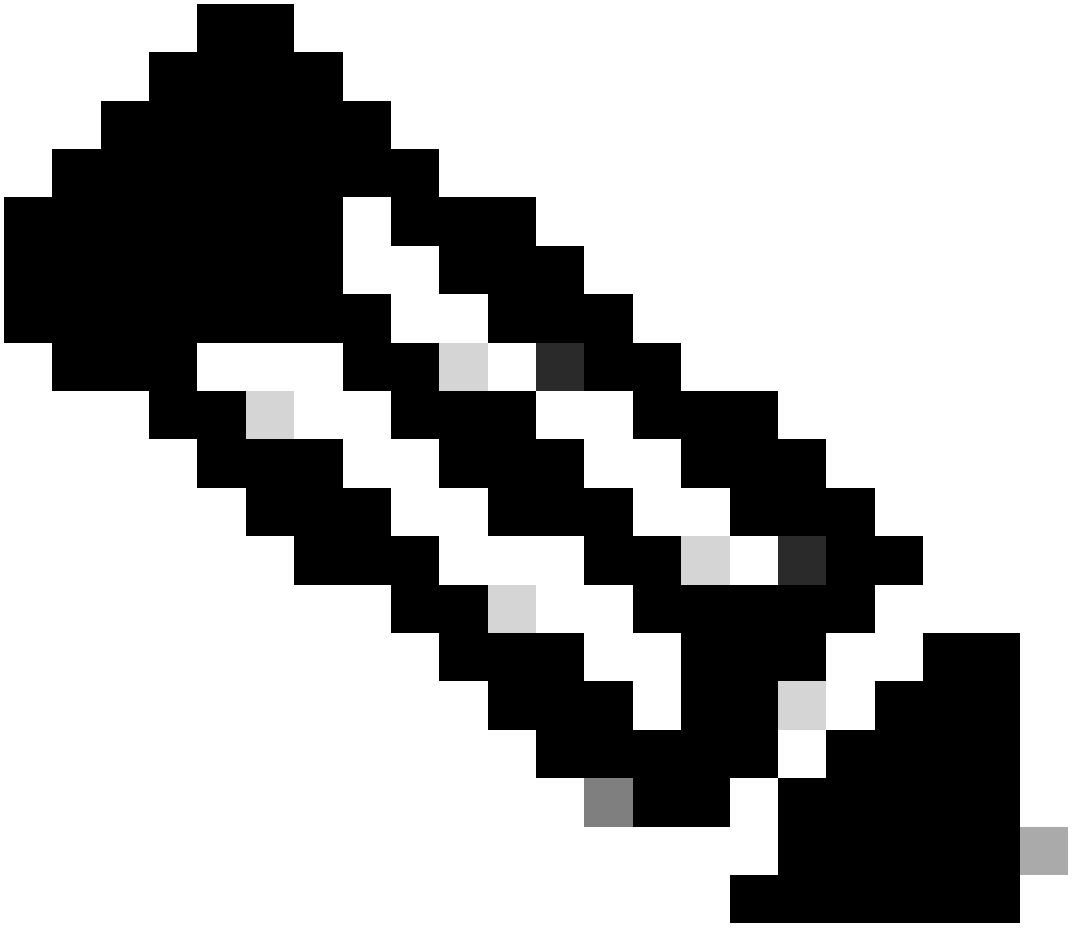
Umbrella consiglia di eseguire l'appliance virtuale (VA) che, tra gli altri vantaggi, può fornire visibilità a livello di host di tutto il traffico DNS sulla rete interna e individuare rapidamente questo tipo di problema.

Tuttavia, il supporto Umbrella talvolta identifica problemi in cui un host interno che non punta DNS ai VA è infetto e invia richieste DNS tramite un server DNS Windows. Poiché in questo scenario non è ovviamente possibile che la VA visualizzi la richiesta DNS (e quindi il relativo indirizzo IP di origine), tutte le query DNS che passano attraverso tale server DNS possono essere registrate nella rete o nel sito.

Considerazioni sui sistemi operativi precedenti a Server 2016

Nei sistemi operativi precedenti a Server 2016, tuttavia, queste informazioni non vengono registrate per impostazione predefinita. Per acquisire i dati, è necessario attivarli manualmente. In particolare, per il 2012r2, è possibile installare l'hotfix di Microsoft per ottenere questo livello di registrazione reso disponibile.

Per altri sistemi operativi e per ulteriori informazioni sulla configurazione della registrazione di debug sul server DNS, questo articolo di Microsoft fornisce una panoramica delle opzioni e dell'utilizzo.



Nota: La configurazione e l'utilizzo di queste opzioni non rientrano nell'ambito del supporto Umbrella.

Opzioni aggiuntive

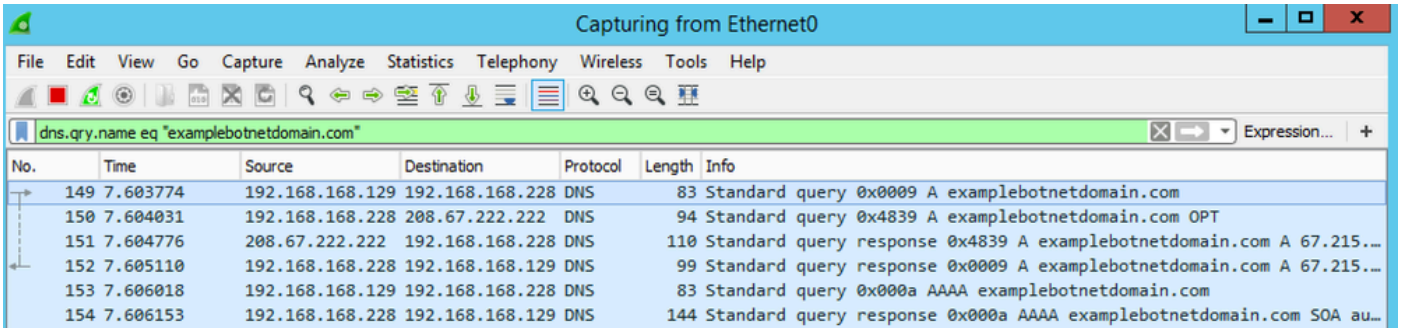
È possibile eseguire un'acquisizione Wireshark con un filtro in esecuzione alla ricerca di DNS e la destinazione Umbrella sta registrando nel dashboard. Sarà quindi possibile disporre di visibilità sufficiente per individuare l'origine della richiesta.

Ad esempio, questa acquisizione eseguita su un server DNS mostra il client (192.168.168.129) che effettua la richiesta al server DNS (192.168.168.228), quindi il server DNS che esegue la query ai server Anycast Umbrella (208.67.222.222), che riceve una risposta e la invia al client.

Un suggerimento sul filtro potrebbe essere simile al seguente:

```
dns.qry.name contains examplebotnetdomain
```

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



esempio di domotnetnet.png

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).