Problemi di coesistenza della sicurezza DNS Umbrella con Broadcom WSS su macOS

Sommario

Problema

Il modulo Umbrella non intercetta il traffico DNS su macOS quando coesiste con Broadcom WSS (Web Security Service). Quando l'agente WSS è configurato per intercettare porte Web specifiche come 80 e 443, la funzionalità di protezione DNS Umbrella non riesce a acquisire tutte le query DNS. Tuttavia, quando WSS è disabilitato, Umbrella riprende l'intercettazione del traffico DNS come previsto. Quando il servizio WSS è abilitato, Umbrella elabora solo determinate query DNS, anziché tutto il traffico DNS intercettato.

Ambiente

- Sistema operativo: macOS
- Modulo di sicurezza DNS Cisco Umbrella
- Agente Broadcom WSS (Web Security Service)
- Agente WSS configurato per intercettare le porte Web 80 e 443

Risoluzione

Questo problema è stato analizzato e determinato come una limitazione dell'architettura di macOS in cui la sicurezza DNS non può coesistere con WSS nell'architettura macOS corrente. Questa limitazione si applica sia alle soluzioni di protezione DNS Infoblox che Cisco Umbrella.

Analisi tecnica

La causa principale è correlata alle limitazioni del proxy DNS macOS:

- A causa delle limitazioni di macOS, nel sistema può essere attivo un solo proxy DNS alla volta
- Se i resolver DNS sono associati a interfacce UutunX o a resolver inseriti tramite proxy, macOS risolve i DNS all'interno del tunnel, non tramite Umbrella
- Quando un altro NEDnsProxyProvider è attivo sul sistema su macOS, Umbrella non intercetta il traffico DNS

Comandi diagnostici

Per verificare quale resolver DNS ha la priorità su macOS, utilizzare il comando seguente:

```
scutil --dns
```

Questo comando mostra quale resolver è contrassegnato come: Ambito, Supplementare o Interfaccia: utunX, che consente di identificare i conflitti del proxy DNS.

Opzioni per la soluzione

Per gli ambienti macOS, WSS continuerà a intercettare DNS senza agenti DNS separati. Per procedere con la copertura della sicurezza DNS, un'opzione sarebbe quella di implementare per supportare un'architettura di bypass passivo. Con questo approccio, il provider ignora completamente il flusso, consentendo l'elaborazione del traffico come se il provider non fosse attivo.

Causa

Il problema è causato dalle limitazioni dell'architettura macOS in cui solo un NEDnsProxyProvider può essere attivo sul sistema alla volta. Quando sono installati sia Umbrella DNS Security che Broadcom WSS, competono per il controllo proxy DNS, facendo sì che WSS abbia la priorità e impedendo a Umbrella di intercettare il traffico DNS. Si tratta di una limitazione fondamentale dello stack di rete macOS e influisce su tutte le soluzioni di sicurezza DNS, non solo su Cisco Umbrella.

Contenuto correlato

- Supporto tecnico Cisco e download

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).