L'ESA attraversa una tempesta

Sommario

Introduzione

In questo documento viene descritto un problema riscontrato in un ambiente in cui Email Security Appliance (ESA) genera un problema che può essere risolto.

Premesse

Una tempesta di rimbalzo è un effetto collaterale di un lavoro joe o un backscatter di spam e-mail.

Joe Job

Un lavoro joe è un attacco di spam che utilizza dati falsificati del mittente e mira a macchiare la reputazione del mittente apparente e/o indurre i destinatari a prendere provvedimenti contro il mittente apparente.

Retrodiffusione

Un backscatter è un effetto collaterale della posta indesiderata, dei virus e dei worm in cui i server di posta elettronica che ricevono la posta indesiderata e altri messaggi inviano messaggi di rimbalzo a una parte innocente. Questo si verifica perché il mittente della busta del messaggio originale viene contraffatto per contenere l'indirizzo e-mail della vittima. Poiché questi messaggi non sono stati sollecitati dai destinatari, sono sostanzialmente simili tra loro e vengono consegnati in grandi quantità, possono essere considerati come posta indesiderata o spam. Di conseguenza, i sistemi che generano backscatter e-mail possono essere elencati in varie DNSBL (Domain Name System Blacklists) e violare i Termini di servizio dei provider di servizi Internet.

Problema

La vostra ESA sperimenta una tempesta di rimbalzi dove c'è una valanga di messaggi iniettati nell'ESA. Il numero di connessioni in ingresso aumenta durante un attacco di questo tipo. L'accessorio potrebbe sviluppare un backup della coda di lavoro. Per verificare se l'accessorio è soggetto a un attacco di questo tipo, leggere i log di posta per l'indirizzo **Da** posta. I messaggi di mancato recapito (rapporti di mancato recapito) hanno un indirizzo **Da** busta vuoto.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Un accessorio soggetto a uragani avrà la maggior parte dei messaggi con l'indirizzo **Da** busta di '**<>**'.

Soluzione

Ci sono diverse opzioni per gestire una tempesta.

Verifica Rimbalzo

Per combattere questi attacchi di bounce indirizzati in modo errato, AsyncOS include Cisco Bounce Verification. Se abilitata, questa funzione associa l'indirizzo del mittente della busta ai messaggi inviati tramite l'ESA. Il Destinatario della busta per ogni messaggio di rimbalzo ricevuto dall'ESA viene quindi controllato per verificare la presenza di questo tag. Quando vengono ricevuti messaggi di mancato recapito legittimi, il tag aggiunto all'indirizzo del mittente della busta viene rimosso e il rimbalzo viene consegnato al destinatario. I messaggi di rimbalzo che non contengono il tag possono essere gestiti separatamente.

AsyncOS considera i rimbalzi come posta con un indirizzo **From di** posta null (**<>**). I messaggi provenienti da indirizzi quali mailer-daemon@example.com o postmaster@example.com non sono considerati messaggi in uscita dal sistema e non sono soggetti alla verifica dei rimbalzi.

Configura chiavi di tag indirizzo verifica rimbalzo

L'elenco Chiavi di tag indirizzo verifica rimbalzo mostra la chiave corrente e tutte le chiavi non eliminate utilizzate in passato. Per aggiungere una nuova chiave, procedere come segue:

1. Nella scheda **Criteri di posta** > **Verifica Rimbalzo** fare clic su **Nuova chiave**.
2. Immettere una stringa di testo e fare clic su **Invia**.
3. Eseguire il commit delle modifiche.

Rimozione delle chiavi

Se si seleziona una regola per la rimozione dal menu a discesa e si fa clic su **Rimuovi, è** possibile rimuovere le vecchie chiavi di tag degli indirizzi.

Configura impostazioni di verifica dei rimbalzi Cisco

Le impostazioni di verifica del rimbalzo determinano l'azione da eseguire quando viene ricevuto un rimbalzo non valido.

- Scegli **Criteri di posta** > **Verifica Rimbalzo**.
- Clic **Modifica impostazioni**.
- Scegliere se rifiutare i rimbalzi non validi o aggiungere un'intestazione personalizzata al messaggio. Se si desidera aggiungere un'intestazione, immettere il nome e il valore dell'intestazione.
- Facoltativamente, abilitare le eccezioni intelligenti. Questa impostazione consente l'esenzione automatica dall'elaborazione della verifica dei messaggi in arrivo e dei messaggi in uscita generati dai server di posta interni, anche quando viene utilizzato un solo listener per la posta in arrivo e in uscita.
- Inviare e confermare le modifiche.

Configurazione della verifica dei rimbalzi di Cisco con la CLI

Èpossibile usare i comandi **bvconfig** e **destconfig** nella CLI per configurare la verifica del rimbalzo. Questi comandi sono descritti nella Cisco AsyncOS CLI Reference Guide.

Verifica dei rimbalzi e configurazione del cluster Cisco

La verifica del rimbalzo funziona in una configurazione cluster purché entrambe le appliance Cisco utilizzino la stessa "chiave di rimbalzo". Quando si utilizza la stessa chiave, entrambi i sistemi devono essere in grado di accettare un rimbalzo legittimo. Il tag o la chiave dell'intestazione modificata non è specifica di ciascun accessorio Cisco.

Filtro posta

Se non è possibile utilizzare la verifica dei rimbalzi perché si utilizzano dispositivi separati per la ricezione e la consegna, è possibile impostare un filtro messaggi per bloccare i messaggi con indirizzo **Da** vuoto.

Blocco posta

Poiché è molto probabile che questi messaggi in uscita abbiano un indirizzo destinatario della busta inesistente, è possibile bloccare gli indirizzi non validi tramite la convalida del destinatario LDAP (Lightweight Directory Access Protocol) di conversazione per ridurre l'impatto di tali messaggi.