L'ESA éprouve une tempête du rebond (NDR)

Contenu

Introduction

Ce document décrit un problème rencontré où votre appliance de sécurité du courrier électronique (ESA) éprouve une tempête de rebond et offre une solution au problème.

Informations générales

Une tempête de rebond est un effet secondaire d'un travail de Joe ou d'une rétrodiffusion de Spam d'email.

Le travail de Joe

Un travail de Joe est une attaque de Spam qui emploie des données et des objectifs charriés d'expéditeur pour ternir la réputation de l'expéditeur apparent et/ou pour inciter les destinataires à agir contre l'expéditeur apparent.

Rétrodiffusion

Une rétrodiffusion est un effet secondaire de Spam d'email, des virus, et des vers où les serveurs de mail qui reçoivent le Spam et toute autre messagerie envoient des avis de non-livraison à un interlocuteur innocent. Ceci se produit parce que l'expéditeur d'enveloppe de premier message est modifié afin de contenir l'adresse e-mail de la victime. Puisque ces messages n'ont pas été sollicités par les destinataires, sont essentiellement semblables entre eux, et sont livrés en quantité en vrac, ils qualifient comme email publicitaire non sollicité ou Spam. En soi, les systèmes qui génèrent la rétrodiffusion d'email peuvent devenir énumérés sur de diverses listes noires de système de noms de domaine (DNSBLs) et être en violation des conditions d'utilisation de fournisseurs d'accès Internet.

Problème

Votre ESA éprouve une tempête de rebond où il y a un déluge des messages injectés dans l'ESA. Les pics de compte de connexion entrante pendant une telle attaque. L'appliance pourrait développer une sauvegarde de workqueue. Afin de vérifier si l'appliance est sujette à une telle attaque, grep que la messagerie se connecte pour la messagerie de l'adresse. Rebonds (états de non-livraison - NDRs) ont une messagerie vide d'enveloppe d'adresse.

```
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: <>
```

Une appliance qui est sujette à une tempête de rebond aura la majorité des messages avec la messagerie d'enveloppe de l'adresse du « **<>** ».

Solution

Il y a un certain nombre d'options de gérer une tempête de rebond.

Vérification de rebond

Afin de combattre ces attaques mal dirigées de rebond, AsyncOS inclut la vérification de rebond de Cisco. Une fois activée, cette caractéristique étiquette l'adresse d'expéditeur d'enveloppe pour des messages envoyés par l'intermédiaire de l'ESA. Le destinataire d'enveloppe pour n'importe quel avis de non-livraison reçu par l'ESA est alors vérifié la présence de cette balise. Quand des avis de non-livraison légitimes sont reçus, la balise qui a été ajoutée à l'expéditeur d'enveloppe que l'adresse est retirée et le rebond est fournie au destinataire. Des avis de non-livraison qui ne contiennent pas la balise peuvent être manipulés séparément.

AsyncOS considère des rebonds comme messagerie avec une messagerie nulle d'adresse (**<>**). Des messages qui sont des adresses telles que mailer-daemon@example.com ou postmaster@example.com ne sont pas considérés des rebonds par le système et ne sont pas sujets à la vérification de rebond.

Configurez l'adresse de vérification de rebond étiquetant des clés

L'adresse de vérification de rebond étiquetant répertorier de clés affiche que votre clé et tout en cours unpurged vous introduit l'a utilisé dans le passé. Afin d'ajouter une nouvelle clé, terminez-vous ces étapes :

1. À la page de **vérification de stratégies >** de **rebond de messagerie**, cliquez sur New la **clé**.
2. Écrivez une chaîne de texte et cliquez sur Submit.
3. Commettez vos modifications.

Purger des clés

Vous pouvez purger votre vieille adresse étiquetant des clés si vous sélectionnez une règle pour

purger du menu déroulant et cliquez sur la **purge.**

Configurez les configurations de vérification de rebond de Cisco

Les configurations de vérification de rebond déterminent quelle action de prendre quand un rebond non valide est reçu.

- Choisissez les **stratégies de messagerie** > la **vérification de rebond**.
- Cliquez sur Edit les **configurations**.
- Sélectionnez si rejeter des rebonds non valides ou ajouter une en-tête faite sur commande au message. Si vous voulez ajouter une en-tête, écrivez le nom et la valeur d'en-tête.
- Sur option, activez les exceptions intelligentes. Cette configuration permet les messages entrants et les avis de non-livraison générés par des serveurs de messagerie interne à exempter automatiquement du procédé de vérification de rebond (même lorsqu'un auditeur simple est utilisé pour entrant et le mail sortant).
- Soumettez et commettez vos modifications.

Configurez la vérification de rebond de Cisco avec le CLI

Vous pouvez employer les commandes de **bvconfig** et de **destconfig** dans le CLI afin de configurer la vérification de rebond. Ces commandes sont discutées dans le guide de référence de Cisco AsyncOS CLI.

Cisco rebondissent la vérification et la configuration du cluster

La vérification de rebond fonctionne en configuration du cluster tant que les deux appliances de Cisco utilisent la même « clé de rebond. » Quand vous utilisez la même clé, l'un ou l'autre de système devrait pouvoir recevoir un bounceback légitime. La balise/clé modifiées d'en-tête n'est pas spécifique à chaque appliance de Cisco.

Filtre de messagerie

Si vous ne pouvez pas utiliser la vérification de rebond parce que vous utilisez les appliances distinctes pour la réception et la livraison, vous pouvez installer un filtre de message afin de bloquer les messages qui ont une messagerie vide d'adresse.

Bloc de messagerie

Puisque ces avis de non-livraison auront très probablement une adresse réceptive d'enveloppe inexistante, vous pouvez des adresses non valides de bloc par l'intermédiaire de la validation réceptive de Protocole LDAP (Lightweight Directory Access Protocol) de conversation afin d'aider inférieur l'incidence de tels messages.