Le Spam entre par l'appliance de sécurité du courrier électronique de Cisco (ESA) dans votre organisation

Contenu

Introduction

Ce document décrit cinq méthodes que les emails de Spam peuvent écrire votre organisation.

Méthodes

1. Messagerie légitime de message/vente

Le message légitime a été choisi dedans par l'utilisateur ou leur nom a été vendu à une autre organisation. Dans le premier cas l'utilisateur devra prendre des mesures pour se désabonner de la liste. Si c'est ce dernier, soumettez le message de nouveau à spam@access.ironport.com ainsi des définitions de courrier indésirable peuvent être mises à jour globalement, améliorant le débit global de capture de Spam de votre ESA. L'activation de la messagerie de vente à la stratégie de messagerie entrante peut aider à changer la perception de ce message « lançant sur le marché » au-dessus du « Spam ».

2. L'anti-Spam n'est pas mis à jour correctement

L'anti-Spam est désactivé ou la touche de fonction a expiré. Pour vérifier et voir si l'anti-Spam met à jour, allez à **GUI > Services de sécurité > anti-Spam d'IronPort**. Dans ce panneau vous devriez voir les mises à jour aux positionnements de règles ou l'engine dans les 6 dernières heures. Également de cet onglet au dessus vous pouvez s'assurer que le service d'anti-Spam est activé. Pour l'examen de l'état de touche de fonction vous pouvez aller à l'onglet > à la touche de fonction d'administration système à vérifier le statut de la clé d'anti-Spam.

3. Filtre de stratégie ou de message de messagerie

Le Spam peut entrer dans votre organisation si l'engine de Sécurité d'anti-Spam est désactivée pour un expéditeur ou un récepteur spécifique par stratégie de messagerie de client. Une autre manière d'ignorer le filtrage spam est par l'intermédiaire de message filtre (CLI : commande de **filtres**).

4. Stratégie de flux de courrier

Un message est classifié utilisant l'ICID du message. Dans cette situation il est probable que la fonctionnalité de sécurité d'anti-Spam soit arrêtée, qui ignore la stratégie de messagerie. Vous pouvez déterminer ceci en regardant les logs de messagerie, dans les logs que vous le premier besoin de passer en revue l'ICID pour comprendre dans quel SenderGroup le message a été classé. Là de l'examen de la stratégie associée de flux de courrier. Si vous avez un grand nombre d'entrées dans votre WhiteList, vous pouvez devoir passer en revue certains des messages qui obtiennent dedans de voir s'ils étaient balayés par l'engine de courrier indésirable. Ouvrez les en-têtes d'un message et recherchez le X-IronPort-Spam d'en-tête, la présence de cette en-tête signifie que le message est passé par l'engine.

5. Le message est Spam

Le message est Spam réel. Vous avez confirmé le message a été balayé par l'engine de courrier indésirable utilisant la fonctionnalité de suivi de message (dans le message dépistant, recherchez le « CAS »). Si le verdict de cas est négatif et vous considérez le message pour être Spam, soumettez le premier message à spam@access.ironport.com. Ceci pourrait être un cas d'une nouvelle menace de Spam juste étant libérée ou d'une menace plus ancienne qui re-a été machinée.

Le traitement des envois de Spam est un automatique et le processus manuel et là n'est aucun feedback pour votre envoi spécifique. À un point quelconque vous pouvez contacter Cisco TAC et demander une évaluation et une réponse.