Contenu

Introduction

Ce document décrit comment permettre à la caractéristique de la prévention d'attaque de récolte de répertoire (DHAP) sur l'appliance de sécurité du courrier électronique de Cisco (ESA) afin d'empêcher des attaques de récolte de répertoire (DHAs).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- AsyncOS

Composants utilisés

Les informations dans ce document sont basées sur toutes les versions d'AsyncOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Un DHA est une technique qui est utilisée par des spammers afin de localiser les adresses e-mail valides. Il y a deux techniques principales qui sont utilisées afin de générer les adresses des cibles ce DHA :

- Le spammer crée une liste de toutes les combinaisons possibles des lettres et numéro, et puis ajoute le nom de domaine.

- Le spammer utilise une attaque par dictionnaire standard avec la création d'une liste qui de cartels de terrain communal des prénoms, des noms de famille, et des initiales.

Le DHAP est une caractéristique prise en charge sur les appliances de sécurité du contenu de Cisco qui peuvent être activées quand la validation d'acceptation de Protocole LDAP (Lightweight Directory Access Protocol) est utilisée. La caractéristique DHAP maintient le nombre d'adresses réceptives non valides d'un expéditeur donné.

Une fois qu'un expéditeur franchit un seuil administrateur-défini, l'expéditeur est considéré être non approuvé, et la messagerie de cet expéditeur est bloquée sans la condition requise de conception de réseaux (NDR) ou la génération de code d'erreur. Vous pouvez configurer le seuil basé sur la réputation de l'expéditeur. Par exemple, les expéditeurs non approuvés ou méfiants peuvent avoir un seuil du bas DHAP, et les expéditeurs de confiance ou honorables peuvent avoir un seuil de la haute DHAP.

Enable DHAP

Afin d'activer la caractéristique DHAP, naviguez **pour envoyer par mail les stratégies >** le **Tableau d'accès au hôte (CHAPEAU) du** GUI d'appareils de sécurité du contenu et pour sélectionner des **stratégies de flux de courrier**. Choisissez la stratégie que vous souhaitez éditer de la colonne de **nom de stratégie**.

Le CHAPEAU a quatre règles d'accès de base qui sont utilisées afin d'agir sur des connexions des serveurs distants :

- **ACCEPT** : La connexion est reçue, et l'acceptation d'email est limitée plus loin par les configurations d'auditeur. Ceci inclut le Tableau réceptif d'Access (pour les auditeurs publics).

- **ANOMALIE** : La connexion est au commencement reçue, mais le client que les tentatives de se connecter reçoit un message d'accueil 4XX ou 5XX. Aucun email n'est reçu.

- **TCPREFUSE** : La connexion est refusée au niveau de TCP.

- **RELAIS** : La connexion est reçue. La réception pour n'importe quel destinataire est permise et n'est pas contrainte par le Tableau réceptif d'Access. La signature de clés de domaine est disponible seulement sur des stratégies de flux de courrier de relais.

Dans la section de **limites de flux de courrier de la** stratégie sélectionnée, la découverte et a placé la configuration de la **prévention d'attaque de récolte de répertoire (DHAP)** en plaçant les destinataires non valides maximaux par heure. Vous pouvez également choisir de personnaliser les destinataires non valides maximaux par code d'heure et

Vous devez répéter cette section afin de configurer DHAP pour des stratégies supplémentaires.

Assurez-vous que vous soumettez et commettez tous les changements du GUI.

> Remarque: Cisco recommande que vous utilisiez un nombre maximal entre cinq et dix pour le **nombre maximal de destinataires non valides par heure d'une** configuration de **serveur distant**.

Remarque: Pour information les informations complémentaires, référez-vous au **guide utilisateur d'AsyncOS** sur le portail de support de Cisco.