Comment autoriser les campagnes simulées de plate-forme d'hameçonnage via l'appliance de sécurité de la messagerie Cisco

Contenu

Introduction

Ce document décrit les étapes de configuration de l'appliance de sécurité de la messagerie Cisco (ESA) pour permettre la simulation de campagnes de phishing.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Création de filtres de messages et de contenu sur le ESA.
- Configuration de la table d'accès hôte (HAT).
- Compréhension du pipeline d'e-mails entrants de Cisco ESA.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les plates-formes d'hameçonnage simulées permettent aux administrateurs d'exécuter des campagnes d'hameçonnage dans le cadre d'un cycle de gestion de l'une des plus grandes menaces qui utilise les systèmes de messagerie comme vecteur d'attaques d'ingénierie sociale.

Problème

Lorsque l'ESA n'est pas préparée à de telles simulations, il n'est pas rare que ses moteurs d'analyse arrêtent les messages de campagne d'hameçonnage, ce qui entraîne une défaillance ou une diminution de l'efficacité des simulations.

Solution

> **Attention** : Dans cet exemple de configuration, la stratégie de flux de courrier *TRUSTED* est sélectionnée pour permettre à l'ESA de passer par des campagnes d'hameçonnage simulées de plus grande taille sans aucune limitation. L'exécution de campagnes d'hameçonnage en continu de volume élevé peut avoir un impact sur les performances de traitement des e-mails.

Pour s'assurer que les messages de campagne d'hameçonnage ne sont arrêtés par aucun composant de sécurité de la configuration ESA doit être mis en place.

1. Créer un groupe d'expéditeurs : **GUI > Politiques de messagerie > Vue d'ensemble de HAT** et lier-le à la stratégie de flux de *messages* de *confiance* (vous pouvez également créer une nouvelle stratégie avec des options similaires sous **GUI > Politiques de messagerie > Politiques de flux de messages**).
2. Ajoutez le ou les hôtes d'envoi ou les adresses IP de la plate-forme d'hameçonnage simulée à ce groupe d'expéditeurs. Si la plate-forme d'hameçonnage simulé comporte une large gamme d'adresses IP, vous pouvez ajouter des noms d'hôte partiels à la place ou des plages d'adresses IP, le cas échéant.
3. Commandez le groupe d'expéditeurs au-dessus de votre groupe d'expéditeurs *BLOCKLIST* pour vous assurer qu'il correspond de manière statique plutôt qu'à SBRS.
4. Désactivez toutes les fonctions de sécurité de la stratégie de flux de courrier *TRUSTED* sous **GUI > Politiques de messagerie > Stratégies de flux de courrier > TRUSTED** (ou votre nouvelle stratégie de flux de courrier) :

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

5. **Envoyez ces modifications et confirmez.**

Attention : Dans cet exemple de configuration, la stratégie de flux de courrier *TRUSTED* est sélectionnée pour permettre à l'ESA de passer par des campagnes d'hameçonnage simulées de plus grande taille sans aucune limitation. L'exécution de campagnes d'hameçonnage en continu de volume élevé peut avoir un impact sur les performances de traitement des e-mails.

Pour s'assurer que les messages de campagne d'hameçonnage ne sont arrêtés par aucun composant de sécurité de la configuration ESA doit être mis en place.

1. Créer un groupe d'expéditeurs : **GUI > Politiques de messagerie > Vue d'ensemble de HAT** et lier-le à la stratégie de flux de *messages* de *confiance*.
2. Ajoutez le ou les hôtes d'envoi ou les adresses IP de la plate-forme d'hameçonnage simulée à ce groupe d'expéditeurs. Si la plate-forme d'hameçonnage simulé comporte une large gamme d'adresses IP, vous pouvez ajouter des noms d'hôte partiels à la place ou des plages d'adresses IP, le cas échéant.
3. Commandez le groupe d'expéditeurs au-dessus de votre groupe d'expéditeurs *BLOCKLIST* pour vous assurer qu'il correspond de manière statique plutôt qu'à SBRS.
4. **Envoyez ces modifications et confirmez.**
5. Accédez à la CLI et ajoutez un nouveau filtre de message, **CLI > filtres,** copiez et modifiez la syntaxe et ajoutez le filtre.
6.
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. Ordonner le filtre de message dans la liste pour s'assurer qu'il ne sera pas ignoré par un autre filtre de message au-dessus qui inclut l'action Ignorer les filtres.
8. Appuyez sur la touche Entrée pour revenir à l'invite de commandes principale d'AsyncOS et lancez la commande "**commit**" pour valider les modifications. (ne cliquez pas sur CTRL+C - il effacera toutes les modifications).
9. Accédez à l'**interface utilisateur graphique > Politiques de messagerie > Filtres de contenu entrant**
10. Créez un nouveau filtre de contenu entrant avec la condition ***« Autre en-tête"*** définie pour rechercher l'en-tête personnalisé **« x-sp »** et sa *valeur unique* configurée dans le filtre de message et configurez l'action ***Ignorer les filtres de contenu restants (Action finale)***.
11. Ordonner au filtre de contenu la valeur « 1 » pour s'assurer que les autres filtres n'interviendront pas contre le message d'hameçonnage simulé.
12. Accédez à **GUI > Politiques de messagerie > Politiques de messagerie entrante** et affectez

le filtre de contenu à la stratégie requise.

13. Envoyez et validez les modifications.
14. Exécutez la campagne simulée de plate-forme d'hameçonnage et surveillez les journaux de messagerie/Suivi des messages pour vérifier la correspondance des règles de flux et de stratégie.