# Filtrage de messagerie charrié par ESA

## Contenu

[Introduction](#)
[Problème](#)
[Solution](#)
[Appliquez les filtres](#)
[Mesures supplémentaires](#)

## Introduction

Ce document décrit un problème qui est produit sur l'appliance de sécurité du courrier électronique de Cisco (ESA) quand le Spam et l'email frauduleux entre dans le réseau.

## Problème

Les fraudeurs tentent de personnifier l'email. Quand l'email personnifie (des significations d'être de) un membre de votre personnel de société, il peut être particulièrement trompeur et a le potentiel d'entraîner la confusion. Afin d'essayer de résoudre ce problème, les administrateurs d'email pourraient tenter de bloquer la messagerie d'arrivée qui semble commencer de la société (messagerie *charriée*).

Il pourrait sembler logique que si vous bloquez la messagerie d'arrivée de l'Internet qui a l'adresse de retour de société dans le nom de domaine, il résout le problème. Malheureusement, quand vous bloquez la messagerie de cette façon, il peut également bloquer l'email légitime en même temps. Considérez ces exemples :

- Un employé voyage et utilise un fournisseur de services Internet (ISP) d'hôtel qui réoriente d'une manière transparente tout les trafic de Protocole SMTP (Simple Mail Transfer Protocol) aux serveurs de messagerie ISP. Quand la messagerie est envoyée, il pourrait sembler que il passe directement par le serveur SMTP d'entreprise, mais il est envoyé réellement par un tiers serveur SMTP avant qu'il soit livré à l'entreprise.

- Un employé s'abonne à une liste de discussion d'email. Quand des messages sont envoyés à la liste d'email, ils sont retournés à tous les abonnés, apparemment du créateur.

- Un système externe est utilisé afin de surveiller la représentation ou l'accessibilité des périphériques externe-visibles. Quand une alerte se produit, l'email a le nom de domaine de société dans l'adresse de retour. Les fournisseurs de services tiers, tels que le WebEx, font ceci assez fréquemment.

- En raison d'une erreur provisoire de configuration réseau, la messagerie de l'intérieur de la société est envoyée par l'intermédiaire de l'auditeur d'arrivée, plutôt que l'auditeur sortant.

- Quelqu'un en dehors de la société reçoit un message ce ils expédient de nouveau dans la

société avec un agent d'utilisateur de messagerie (messagerie) lignes de cette en-tête d'utilisations de nouvelles plutôt que l'en-tête d'origine.

- Une application basée sur Internet, telle que les **pages d'expédition de** Federal Express ou l'**email de** Yahoo **cette** page d'**article**, crée la messagerie légitime avec une adresse de retour qui redésigne la société.  La messagerie est légitime et a une adresse source de l'intérieur de la société, mais elle ne commence pas de l'intérieur.

Ces exemples prouvent que si vous bloquez la messagerie d'arrivée basée sur l'information de domaines, elle peut avoir comme conséquence les faux positifs.

# Solution

Cette section décrit les actions recommandées que vous devriez exécuter afin de résoudre ce problème.

## Appliquez les filtres

Afin d'éviter la perte de messages électroniques légitimes, ne bloquez pas la messagerie d'arrivée basée sur l'information de domaines. Au lieu de cela, vous pouvez étiqueter le champ objet de ces types de messages pendant qu'ils entrent dans le réseau, qui indique au destinataire que les messages sont potentiellement modifiés. Ceci peut être accompli avec des filtres de message ou avec les filtres satisfaits.

La stratégie de base pour ces filtres est de vérifier les lignes vers l'arrière-aiguës d'en-tête de corps (des données est le plus important), aussi bien que l'expéditeur d'enveloppe RFC 821. Ces lignes d'en-tête le plus généralement sont affichées dans les messageries et sont celles qui sont le plus susceptibles d'être modifiées par une personne frauduleuse.

Le filtre de message dans l'exemple suivant affiche comment vous pouvez étiqueter les messages qui sont potentiellement personnifiés. Ce filtre exécute plusieurs actions :

- Si le champ objet a déjà **« {probablement modifié} »** dans lui, alors une autre copie n'est pas ajoutée par le filtre. C'est important quand des réponses sont incluses dans le flux des messages, et un champ objet pourrait se déplacer par le mail gateway plusieurs fois avant qu'un thread de message soit complet.

- Ce filtre recherche l'expéditeur d'enveloppe ou de l'en-tête qui a une adresse qui finit dans le nom de domaine **@yourdomain.com. Il** est important de noter que messagerie-de la recherche est automatiquement ne distinguant pas majuscules et minuscules, mais de - la recherche d'en-tête n'est pas. Si le nom de domaine est trouvé dans l'un ou l'autre d'emplacement, le filtre s'insère « **{probablement modifié} » à l'**extrémité du champ objet.

Voici un exemple du filtre :

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
```

```
        strip-header("Subject");
        insert-header("Subject", "$Subject {Possibly Forged}");
    }
}
```

## Mesures supplémentaires

Puisqu'il n'y a aucun moyen simple d'identifier la messagerie charriée de la messagerie légitime, il n'y a aucune manière d'éliminer le problème entièrement. Par conséquent, Cisco recommande que vous activiez la lecture d'anti-Spam d'IronPort (IPAS), qui efficacement identifie la messagerie frauduleuse (phishing) ou le Spam et le bloque franchement. L'utilisation de ce scanner d'anti-Spam, une fois ajoutée aux filtres décrits dans la section précédente, fournit les meilleurs résultats sans perte d'email légitime.

Si vous devez identifier les emails frauduleux qui entrent dans votre réseau, alors considérez l'utilisation de la technologie de la messagerie identifiée par clés de domaine (DKIM) ; il exige plus d'installation, mais c'est une bonne mesure contre le phishing et les emails frauduleux.

> Remarque: Pour plus d'informations sur des filtres de message, référez-vous au **guide utilisateur d'AsyncOS** sur la page de support d'appareils de sécurité du courrier électronique de Cisco.