Configurer l'analyse antivirus ESA après la suppression de la pièce jointe

Table des matières

[Introduction](#)

[Informations générales](#)

[Énoncé du problème](#)

[Environnement](#)

[Recommandation](#)

[Pourquoi la suppression des pièces jointes ne suffit pas](#)

[Informations connexes](#)

Introduction

Ce document décrit si l'analyse antivirus reste nécessaire après la suppression des pièces jointes sur le dispositif de sécurité de la messagerie Cisco (ESA).

Informations générales

L'analyse antivirus doit rester activée sur l'appliance de sécurité de la messagerie Cisco (ESA) même lorsque les règles de suppression des pièces jointes sont activées, car la suppression des pièces jointes ne supprime pas de manière fiable tout le contenu malveillant de chaque structure de message.

Énoncé du problème

Les administrateurs peuvent supposer que la suppression des pièces jointes élimine les risques liés aux programmes malveillants et rend l'analyse antivirus inutile. Ce document explique pourquoi l'analyse antivirus doit toujours être utilisée après la suppression des pièces jointes.

Environnement

Ce guide s'applique aux e-mails entrants et sortants traités par l'appliance de sécurisation de la messagerie Cisco (ESA).

Recommandation

L'analyse antivirus est requise pour les messages même lorsque les règles de suppression des pièces jointes sont activées sur l'appliance de sécurité de la messagerie Cisco (ESA).

Maintenez l'analyse antivirus activée pour tous les flux de messages applicables après la configuration des stratégies de suppression des pièces jointes.

- Analyser les e-mails entrants car le contenu malveillant peut rester dans les parties des messages qui ne sont pas supprimées par les règles de suppression des pièces jointes.
- Analyser les e-mails sortants car les messages peuvent toujours contenir des programmes malveillants après le traitement de suppression des pièces jointes.
- Attendez-vous à ce que les règles de suppression des pièces jointes réduisent les risques et non remplacent l'analyse antivirus.



Remarque : Résultat escompté : la suppression des pièces jointes peut réduire l'exposition à certaines menaces basées sur des fichiers, mais une analyse antivirus est toujours nécessaire pour détecter le contenu malveillant qui reste dans le message. Portée : ce guide indique si l'analyse antivirus est toujours requise après la suppression des pièces jointes ; il ne décrit pas toutes les fonctions de détection des programmes malveillants sur ESA.

Pourquoi la suppression des pièces jointes ne suffit pas

La suppression des pièces jointes réduit le risque, mais ne l'élimine pas.

- L'attachement n'est pas une définition technique stricte.
- ESA évalue les pièces MIME définies par RFC, et non un objet de pièce jointe universel.
- Les messages peuvent être construits de manière à contourner la logique de suppression des pièces jointes, car le terme « pièce jointe » n'est pas une définition technique précise.
- Étant donné que le contenu des e-mails peut être structuré dans différents formats MIME, les règles de suppression des pièces jointes ne suppriment pas de manière fiable tout le contenu malveillant.
- Les messages sortants peuvent toujours contenir des programmes malveillants.

Informations connexes

Pour plus d'informations, consultez :

- Descriptions des actions de filtre de message ESA
- Utilisation des filtres de messages

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.