Comment envoyer un message témoin pour assurer l'engine d'antivirus balaye sur une appliance de sécurité du courrier électronique de Cisco (l'ESA)

Contenu

Introduction

Ce document décrit comment envoyer un message témoin pour s'assurer que l'antivirus de Sophos ou engine d'antivirus de McAfee balaye sur une appliance de sécurité du courrier électronique de Cisco (ESA).

Comment envoyer un message témoin pour assurer l'engine d'antivirus balaye sur une appliance de sécurité du courrier électronique de Cisco (l'ESA)

En envoyant un message témoin avec une charge utile virale de test par l'ESA, nous pouvons engine déclencher de Sophos ou de McAfee antivirus. Avant d'exécuter les étapes répertoriées dans ce document, vous devrez installer votre stratégie entrante ou de mail sortant et configurer la stratégie de messagerie pour avoir la baisse d'antivirus ou pour mettre en quarantaine les messages infectés par virus. Ce document utilise code ASCII fourni d'EICAR (www.eicar.org) qui simulera un virus de test comme connexion :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

> **Note**: Par EICAR : *Ce fichier de test a été fourni à EICAR pour la distribution comme « fichier de test standard d'antivirus EICAR », et il répond à tous les critères répertoriés ci-dessus. Il est sûr de passer autour, parce que ce n'est pas un virus, et n'inclut aucun fragment de code viral. La plupart des Produits réagissent à lui comme si c'étaient un virus (cependant ils le signalent typiquement avec un nom évident, tel que le « EICAR-POIDs du commerce-test »).*

Créez un fichier TXT

Utilisant la chaîne ASCII ci-dessus, créez un fichier de .txt et placez la chaîne comme écrit comme corps du fichier. Vous pourrez envoyer ce fichier comme connexion dans votre message témoin.

Envoi du message témoin

Selon la façon dont vous travaillez, vous pouvez envoyer le message témoin par les diverses manières ESA. Deux méthodes d'exemple sont par l'intermédiaire d'UNIX CLI utilisant la **messagerie** ou d'Outlook (ou de toute autre application de messagerie électronique).

UNIX CLI

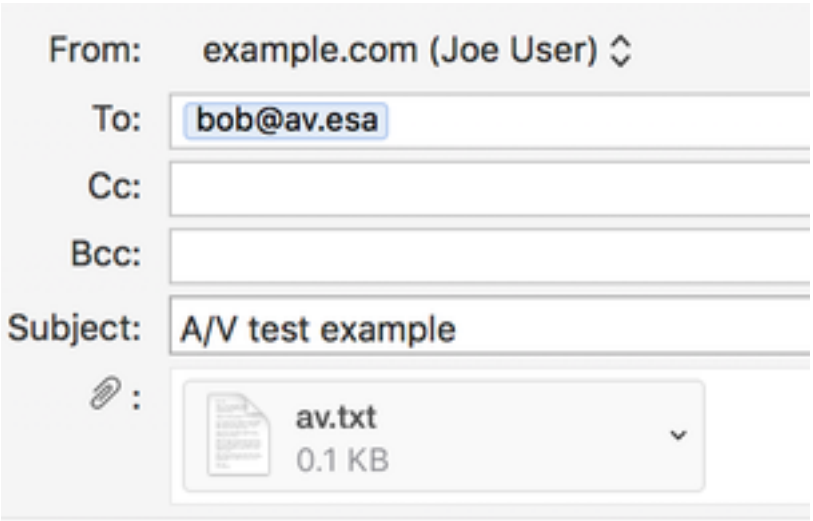
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

Votre environnement Unix devra être correctement installé pour envoyer ou transmettre par relais la messagerie par votre ESA.

Outlook

Utilisant un Outlook (ou une application de messagerie électronique différente), vous avez deux choix en envoyant code ASCII : 1) utilisant le fichier créé de .txt, 2) pâte directe de la chaîne ASCII dans le corps du message.

Utilisant le fichier de .txt comme connexion :



TEST MESSAGE w/ ATTACHMENT

Utilisant la chaîne ASCII dans le corps du message :


```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Votre Outlook (ou toute autre application de messagerie électronique) devra être correctement installé pour envoyer ou transmettre par relais la messagerie par votre ESA.

Vérification

Sur l'ESA CLI, utilisez les **mail_logs de queue de** commande avant d'envoyer le message témoin. Tout en observant la messagerie se connecter vous verra le message est balayé et attrapé par McAfee en tant que « VIRAL » :

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa>
Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com>'
Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment'
Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt'
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file'
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok:  Message 49 accepted'
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
```

Le même message envoyé et balayé par Sophos :

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
```

```
Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa>
Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com>'
Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment'
Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt'
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test'
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok:  Message 50 accepted'
Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done
Wed Sep 13 11:44:29 2017 Info: DCID 240 close
```

Sur ce laboratoire ESA, « des messages infectés par virus » sont configurés pour mettre en quarantaine pour la « action appliquée au message » sur la stratégie particulière de messagerie. L'action sur votre ESA peut varier, basé sur la mesure prise pour les messages infectés par virus manipulés par l'antivirus sur votre stratégie de messagerie.

Informations connexes

- Support et documentation techniques - Cisco Systems