Commande de quarantaine ESA/CES une fois diminué par des plusieurs services

Contenu

Introduction

Ce document décrit le comportement des périphériques des appareils de sécurité du courrier électronique de Cisco (ESA) et de la sécurité du courrier électronique de nuage (CES) quand un email est signalé par des plusieurs services pour mettre en quarantaine et l'écoulement FO l'email par le reste du pipeline d'email.

Conditions préalables

Exigences

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur Cisco ESA avec la version d'AsyncOS 12.1.0.

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 en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les emails qui traverse Cisco ESA et des périphériques de CES pour filtrer suit le pipeline de file d'attente de travail d'email. Le pipeline est statique et s'il y a de plusieurs actions des plusieurs services définis pour signaler un email pour les quarantaines, il ne suit pas la commande selon le pipeline ; au lieu de cela, l'ESA/CES le met en quarantaine avec sa propre commande.

> Remarque: Les emails aux lesquels sont signalés avec des actions réglées (mesure finale) auront la priorité immédiate et quittent le traitement de file d'attente de travail.

Qu'arrive à l'email une fois diminué par des plusieurs services pour la quarantaine ?

L'email est donné la priorité dans la quarantaine de l'attaque de virus de stratégie (PVO) d'abord. Il n'y a aucune commande spécifique dans laquelle la quarantaine de stratégie il entre pendant que le PVO répertorie chaque autre quarantaine que l'email est également tenu dedans. Après que l'email soit libéré sur une des quarantaines PVO, on le tient dans toutes les quarantaines respectives à signaler dedans.

Après que l'email ait été relâché (manuellement ou par le temporisateur où l'action par défaut est placée de relâcher) les emails puis écrivent la quarantaine de Spam. Quand l'email est relâché de la quarantaine de Spam, il des transverses dans la livraison s'alignent pour la livraison finale ensuite.

> Remarque: Un email qui est supprimé outre d'une quarantaine PVO, enlèvera l'email de tout l'ultérieur le met en quarantaine s'est tenu dedans aussi bien.

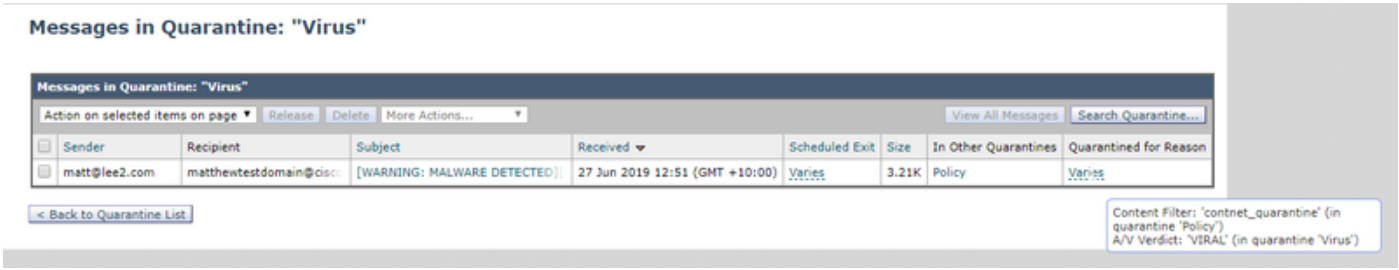
- Des messages libérés des quarantaines de stratégie et de virus sont rebalayés par l'antivirus, la protection avancée de malware, et les engines de graymail.
- Des messages libérés de la quarantaine d'épidémie sont rebalayés par l'anti-Spam, l'antivirus, et les engines d'AMP.
- Des messages libérés de la quarantaine d'analyse de fichier sont rebalayés pour des menaces.
- Des messages avec des connexions sont rebalayés par le service de réputation de fichier sur la release des quarantaines de stratégie, de virus, et d'épidémie.

Injection initiale d'email avec le filtrage fait par l'ESA. Dans cette sortie vous voyez qu'elle est signalée par la quarantaine de Spam, quarantaine de virus, et quarantaine de stratégie :

```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with AV EICAR and other triggers'
Thu Jun 27 12:51:15 2019 Info: MID 378951 ready 3292 bytes from <matt@lee2.com>
Thu Jun 27 12:51:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim verdict using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: MID 378951 using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:51:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:51:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:51:15 2019 Info: MID 378951 attachment 'testAV.txt'
Thu Jun 27 12:51:15 2019 Info: MID 378951 URL https://ihaveabadreputation.com has reputation -
9.3 matched Condition: URL Reputation Rule
Thu Jun 27 12:51:15 2019 Info: MID 378951 Custom Log Entry:  - Match whole word filter
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Policy" (content
filter:contnet_quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Virus" (a/v verdict:VIRAL)
Thu Jun 27 12:51:15 2019 Info: Message finished MID 378951 done
Thu Jun 27 12:51:15 2019 Info: ICID 391696 close
```

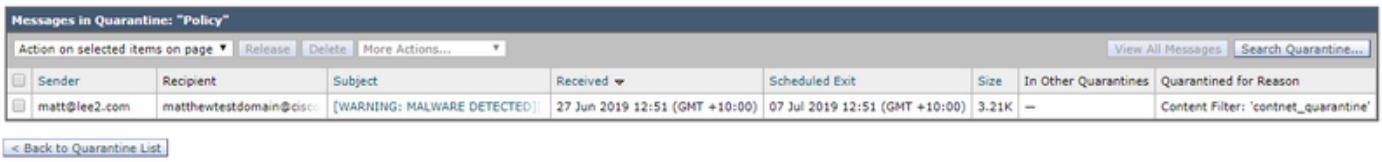
Une fois étudié à l'intérieur de la quarantaine, de l'email tenu dans la quarantaine PVO que vous

avez marquée êtes vu, aussi bien que de toutes autres quarantaines elle diminue pour être dedans.



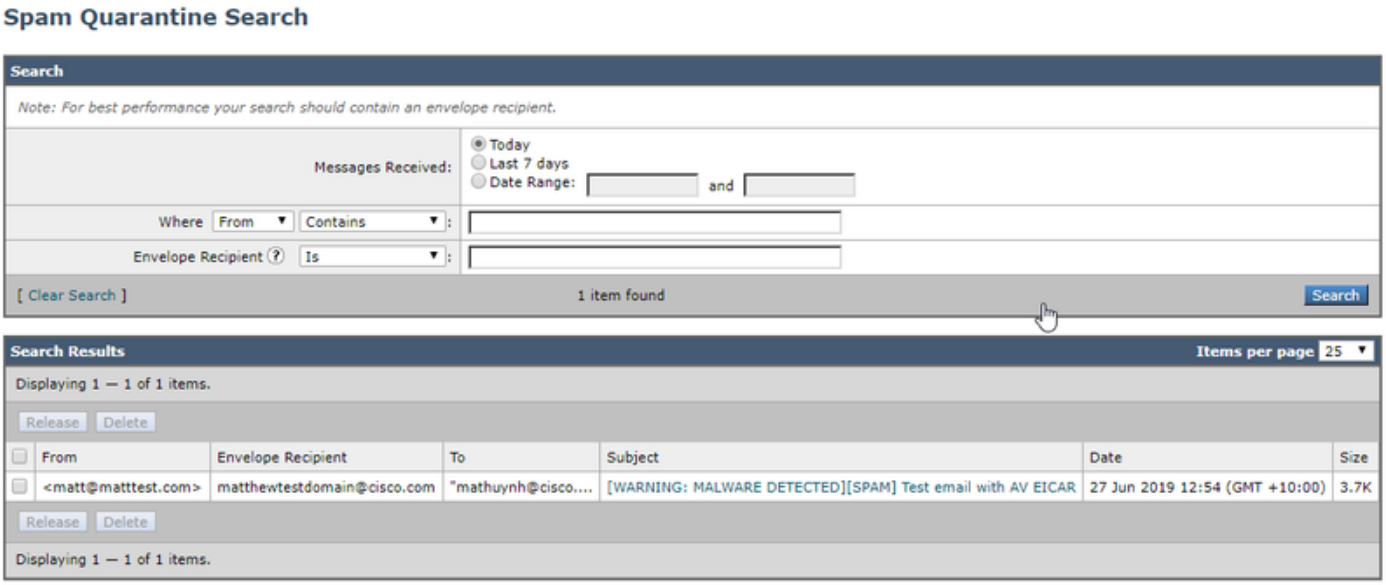
Après qu'il libère de cette quarantaine, il se connecte cet événement dans vos **mail_logs** et réfléchit sur les autres quarantaines aussi bien qu'il n'est plus disponible dans l'autre quarantaine.

```
Thu Jun 27 12:52:59 2019 Info: MID 378951 released from quarantine "Virus" (manual) t=104
```



Libérez-le hors de la quarantaine PVO qui demeure permettent aux emails pour voyager à la quarantaine signalée de Spam ensuite.

```
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from quarantine "Policy" (manual) t=180
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from all quarantines
Thu Jun 27 12:54:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:54:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:54:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:54:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:54:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:54:15 2019 Info: MID 378951 queued for delivery
Thu Jun 27 12:54:15 2019 Info: RPC Delivery start RCID 13914 MID 378951 to local IronPort Spam
Quarantine
Thu Jun 27 12:54:15 2019 Info: ISQ: Quarantined MID 378951
Thu Jun 27 12:54:15 2019 Info: RPC Message done RCID 13914 MID 378951
Thu Jun 27 12:54:15 2019 Info: Message finished MID 378951 done
```



Là sur la version finale de la quarantaine de Spam, l'email est destiné à la file d'attente de la livraison.

```
Thu Jun 27 12:55:33 2019 Info: Start MID 378952 ICID 0 (ISQ Released Message)
Thu Jun 27 12:55:33 2019 Info: ISQ: Reinjected MID 378951 as MID 378952
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 From: <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 Subject '[WARNING: MALWARE DETECTED][SPAM] Test email
with AV EICAR'
Thu Jun 27 12:55:33 2019 Info: MID 378952 ready 9661 bytes from <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 queued for delivery
```

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems