Test Advanced Malware Protection (AMP) ESA

Contenu

Introduction

Ce document décrit comment tester et vérifier les fonctionnalités AMP (Advanced Malware Protection) de l'appliance de sécurité de la messagerie Cisco (ESA).

Test d'AMP sur l'ESA

Avec la version 8.5 d'AsyncOS pour l'ESA, AMP effectue des analyses de réputation des fichiers et des analyses de fichiers afin de détecter les programmes malveillants dans les pièces jointes.

Touches de fonction

Pour implémenter AMP, vous devez disposer d'une clé de fonction valide et active pour la réputation des **fichiers** et l'**analyse des fichiers** sur votre ESA. Visitez **Administration système > Touches de fonction** sur l'interface utilisateur graphique ou utilisez **des touches de fonction** sur l'interface de ligne de commande afin de vérifier les clés de fonction.

Services de sécurité

Afin d'activer le service à partir de l'interface utilisateur graphique, accédez à **Services de sécurité > Réputation et analyse des fichiers**. À partir de l'interface de ligne de commande, vous pouvez

exécuter **ampconfig**. Envoyez et confirmez vos modifications à la configuration.

Stratégies de messagerie entrante

Une fois que vous avez activé le service, ce service doit être lié à une stratégie de courrier entrant.

1. Accédez à **Politiques de messagerie > Politiques de messagerie entrante**.
2. Sélectionnez votre **stratégie par défaut** ou votre stratégie préconfigurée si nécessaire. La colonne **Advanced Malware Protection** de la page Incoming Mail Polices s'affiche.
3. Sélectionnez le lien **Désactivé** pour la colonne, puis **Activer la réputation de fichier** et **Activer l'analyse de fichier** sur la page d'options.
4. Vous pouvez apporter d'autres améliorations à la configuration de l'analyse des messages, des actions pour les pièces jointes non analysables et des actions pour les messages identifiés positivement, si nécessaire.
5. Envoyez et confirmez vos modifications à la configuration.

Tester

Àce stade, votre stratégie de messagerie entrante est activée pour analyser et détecter les programmes malveillants. Vous devez disposer d'un véritable exemple de programme malveillant avec lequel tester. Si vous avez besoin d'exemples valides, visitez la page de téléchargement de l'Institut Européen de Recherche Antivirus (eicar).

> **Attention** : Cisco ne peut être tenu responsable lorsque ces fichiers ou votre scanner AV associés à ces fichiers causent des dommages à votre ordinateur ou à votre environnement réseau. VOUS TÉLÉCHARGEZ CES FICHIERS À VOS PROPRES RISQUES. Téléchargez ces fichiers uniquement si vous êtes suffisamment sûr dans l'utilisation de votre scanner AV, des paramètres de l'ordinateur et de l'environnement réseau. Ces renseignements sont fournis à titre de courtoisie à des fins de test et de reproduction.

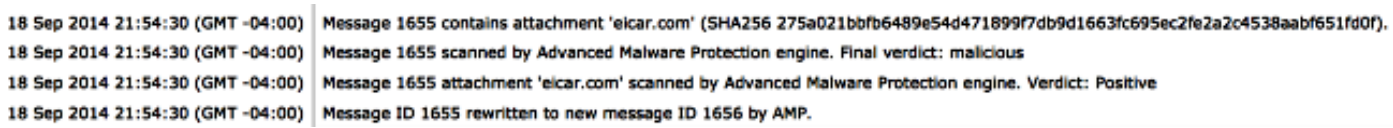
Avec l'utilisation d'un compte de messagerie préconfiguré valide, envoyez la pièce jointe via votre ESA et le traitement normal. Vous pouvez utiliser l'interface CLI de l'ESA et **tail mail_logs** afin de surveiller le courrier au fur et à mesure qu'il traite. L'ID de message (MID) apparaît dans les journaux de messagerie. La sortie similaire à celle-ci s'affiche :

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
```

```
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

L'exemple précédent montre qu'AMP a détecté la pièce jointe du programme malveillant et **a abandonné** en tant qu'action finale par défaut.

Les mêmes détails sont également visibles dans le suivi des messages depuis l'interface utilisateur graphique :



Si vous choisissez de fournir des programmes malveillants identifiés positivement ou d'autres options avancées dans la configuration AMP à partir des stratégies de messagerie entrante, vous pouvez voir le résultat suivant :

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

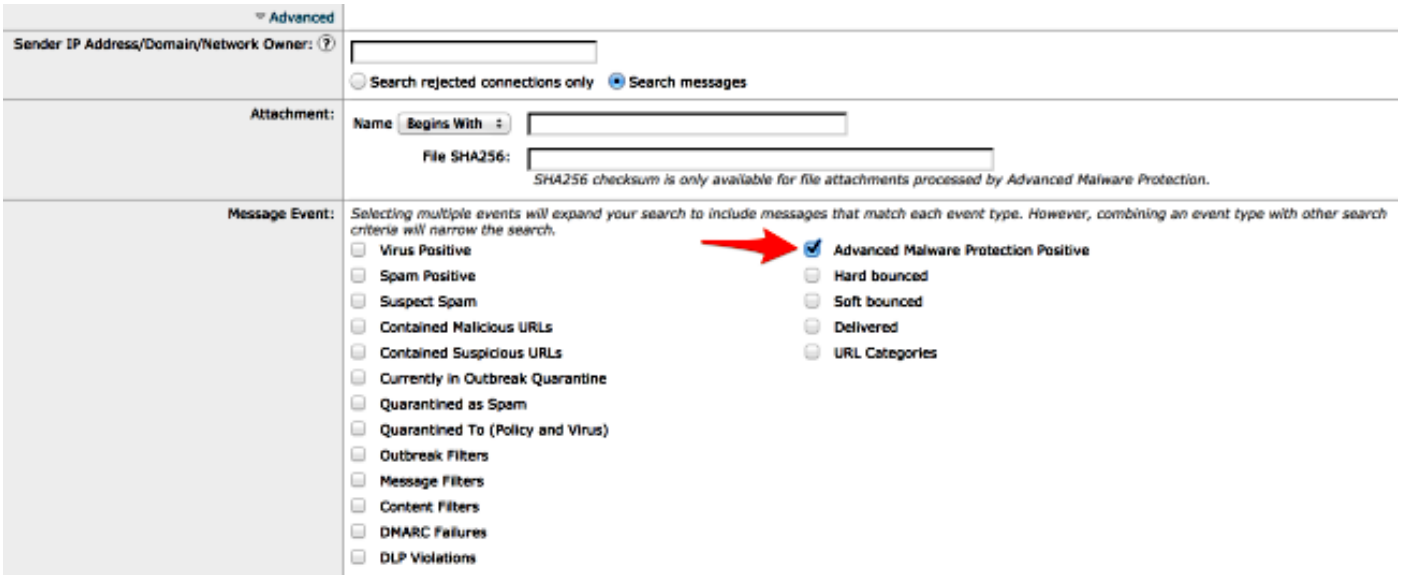
Le verdict de réputation reste positif pour **MALWARE** comme indiqué. L'action réécrite est conforme aux actions de modification du message et à la ligne d'objet en attente de **[AVERTISSEMENT : MALWARE DÉTECTÉ]**.

Un fichier propre ou un fichier qui n'a pas été identifié au moment du traitement comme étant un programme malveillant, a ce verdict écrit dans les journaux de messagerie :

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

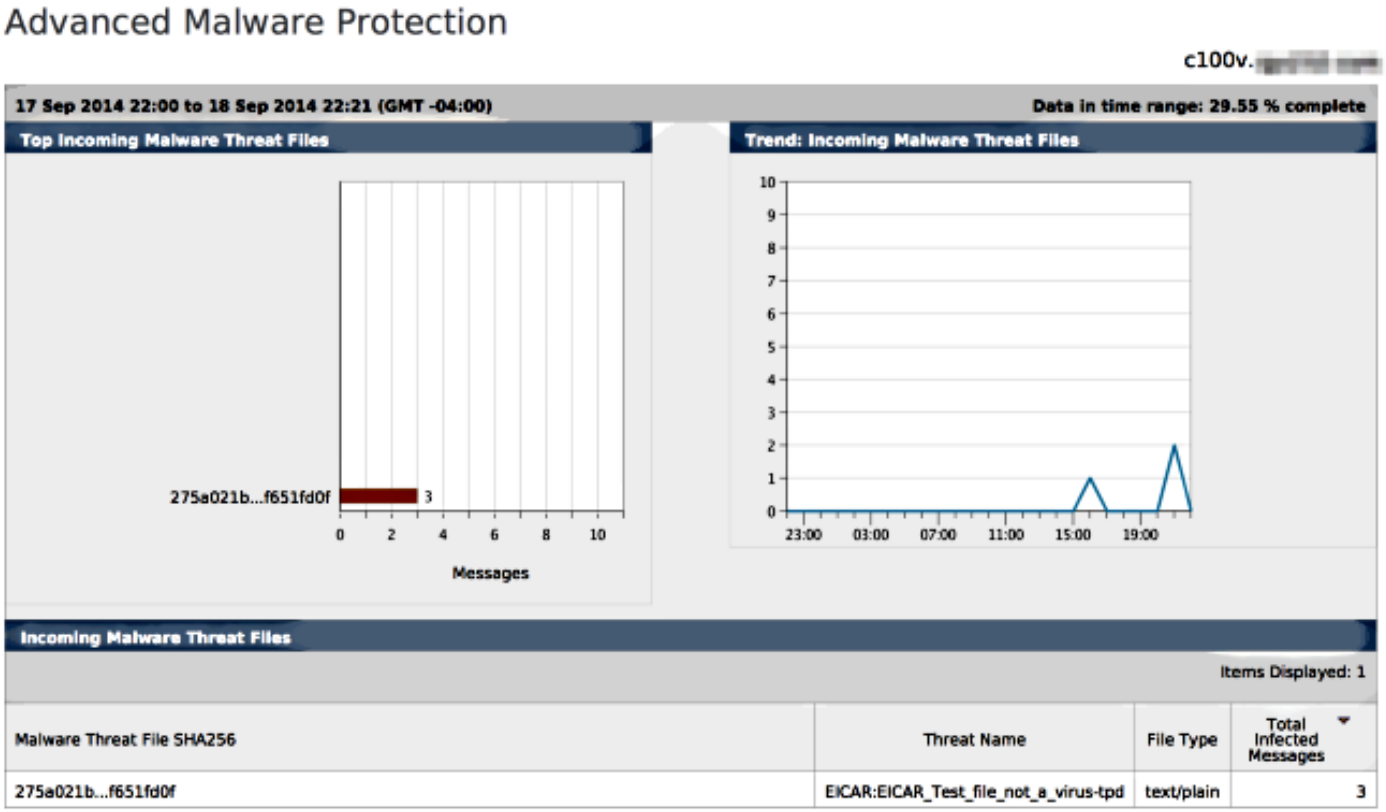
Suivi avancé des messages AMP+

Également dans l'interface utilisateur graphique, lorsque vous utilisez le suivi des messages et le menu déroulant Avancé, vous pouvez choisir de rechercher un message positif Advanced Malware Protection directement :



Rapports avancés sur la protection contre les programmes malveillants

Àpartir de l'interface graphique de l'ESA, vous pouvez également voir le suivi des rapports pour les messages identifiés positivement via AMP. Naviguez jusqu'à **Monitor > Advanced Malware Protection** et modifiez l'intervalle de temps si nécessaire. Vous pouvez maintenant voir la même chose avec les exemples précédents pour les entrées :



Dépannage

Si vous ne voyez pas de fichier de programme malveillant réel connu qui est analysé positivement par AMP, consultez les journaux de messagerie afin de vous assurer qu'un autre service n'a pas pris d'action sur le message et/ou la pièce jointe avant qu'AMP n'analyse le message.

Dans l'exemple précédent utilisé, lorsque l'antivirus Sophos est activé, il intercepte et agit sur la pièce jointe :

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

Les paramètres de configuration antivirus Sophos de la stratégie de messagerie entrante sont définis pour **supprimer** les messages infectés par un virus. Dans ce cas, AMP n'est jamais joint pour analyser ou agir sur la pièce jointe.

Ce n’est pas toujours le cas. Il peut être nécessaire d'examiner les journaux de messagerie et les ID de message (MID) pour s'assurer qu'un autre service OU qu'un filtre de contenu/message n'a pas pris d'action contre le MID avant le traitement AMP et qu'une action a été atteinte.

Informations connexes

- Cisco Email Security Appliance - Guides de l'utilisateur final
- Support et documentation techniques - Cisco Systems