Tester la protection avancée contre les programmes malveillants sur l'appliance de sécurité

Table des matières

[Introduction](#)

[Informations générales](#)

[Test d'AMP sur le ESA](#)

[Touches de fonction](#)

[Services de sécurité](#)

[Stratégies de messages entrants](#)

[Essai](#)

[Suivi avancé des messages AMP+](#)

[Rapports Advanced Malware Protection](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment tester et vérifier les fonctions avancées de protection contre les programmes malveillants (AMP) sur l'appliance de sécurisation de la messagerie Cisco (ESA).

Informations générales

Avant de commencer, vérifiez que les touches de fonction File Reputation et File Analysis sont actives et qu'AMP est activé dans une stratégie de messages entrants. Cette procédure permet de vérifier que l'ESA analyse les pièces jointes et applique l'action attendue, telle que la suppression ou la réécriture, en cas de détection d'un programme malveillant. Confirmez les résultats dans mail_logs pour les entrées de verdict AMP et dans l'interface utilisateur graphique dans Message Tracking and Monitor > Advanced Malware Protection.

Test d'AMP sur le ESA

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

Touches de fonction

Pour mettre en oeuvre AMP, vous devez disposer d'une clé de fonction ESA valide et active pour File Reputation et File Analysis. Visitez Administration système > Touches de fonction sur l'interface graphique utilisateur ou utilisez feature keys sur l'interface de ligne de commande pour vérifier les touches de fonction.

Services de sécurité

Pour activer le service à partir de l'interface utilisateur graphique, accédez à Services de sécurité > File Reputation and Analysis. À partir de l'interface de ligne de commande, vous pouvez exécuter ampconfig. Envoyez et validez vos modifications dans la configuration.

Stratégies de messages entrants

Une fois le service activé, vous devez l'associer à une stratégie de messages entrants.

1. Accédez à Politiques de messagerie > Politiques de messages entrants.
2. Sélectionnez votre stratégie par défaut ou une stratégie préconfigurée selon vos besoins. La colonne Advanced Malware Protection de la page Stratégies de messages entrants s'affiche.
3. Sélectionnez le lien Disabled pour la colonne, puis Enable File Reputation et Enable File Analysis 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, le cas échéant.
5. Envoyez et validez vos modifications dans la configuration.

Essai

Votre stratégie de messages entrants est désormais activée pour analyser et détecter les programmes malveillants. Vous devez disposer d'un véritable échantillon de programme malveillant pour le tester. Si vous avez besoin d'exemples valides, visitez la page de téléchargement de l'Institut Européen pour la Recherche Informatique Antivirus (Eicar).

⚠ Attention : Cisco ne peut être tenu responsable lorsque ces fichiers ou votre scanner AV associé 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 sécurisé à l'aide de votre scanner AV, des paramètres de votre ordinateur et de votre environnement réseau. Ces informations sont fournies à titre gracieux à des fins de test et de reproduction.

Envoyez la pièce jointe via votre ESA et effectuez un traitement normal à l'aide d'un compte de messagerie électronique préconfiguré valide. Vous pouvez utiliser l'interface de ligne de commande de l'ESA et tail mail_logs pour surveiller le courrier pendant qu'il est traité. Vous pouvez voir l'ID de message (MID) répertorié dans les journaux de messagerie. Le résultat similaire à celui-ci affiche :

<#root>

```
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 l'a abandonnée en tant qu'action finale conformément aux paramètres par défaut.

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

18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 contains attachment 'eicar.com' (SHA256 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f).
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 scanned by Advanced Malware Protection engine. Final verdict: malicious
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 attachment 'eicar.com' scanned by Advanced Malware Protection engine. Verdict: Positive
18 Sep 2014 21:54:30 (GMT -04:00)	Message ID 1655 rewritten to new message ID 1656 by AMP.

Si vous choisissez d'envoyer des programmes malveillants identifiés positivement ou d'autres options avancées dans la configuration AMP à partir des stratégies de messages entrants, vous pouvez voir ce résultat de traitement du courrier :

```
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
```

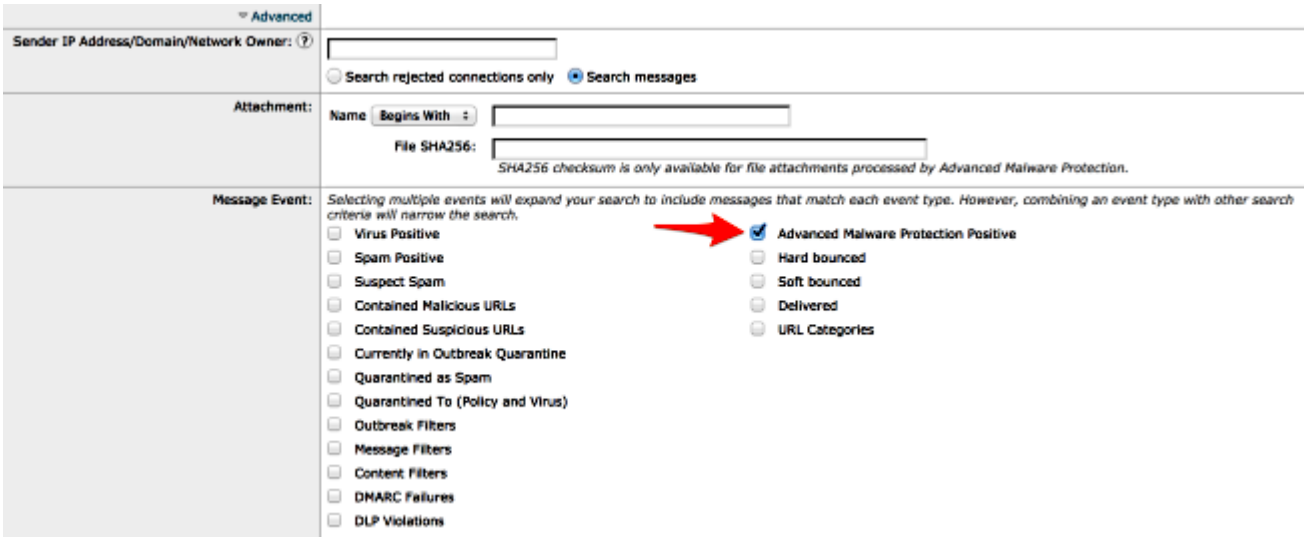
Le verdict de réputation est toujours positif pour le MALWARE comme indiqué. L'action réécrite est conforme aux actions de modification du message et à la ligne d'objet qui précède [AVERTISSEMENT : PROGRAMME MALVEILLANT DÉTECTÉ].

Un fichier sain, ou un fichier qui n'a pas été identifié au moment du traitement comme 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
```

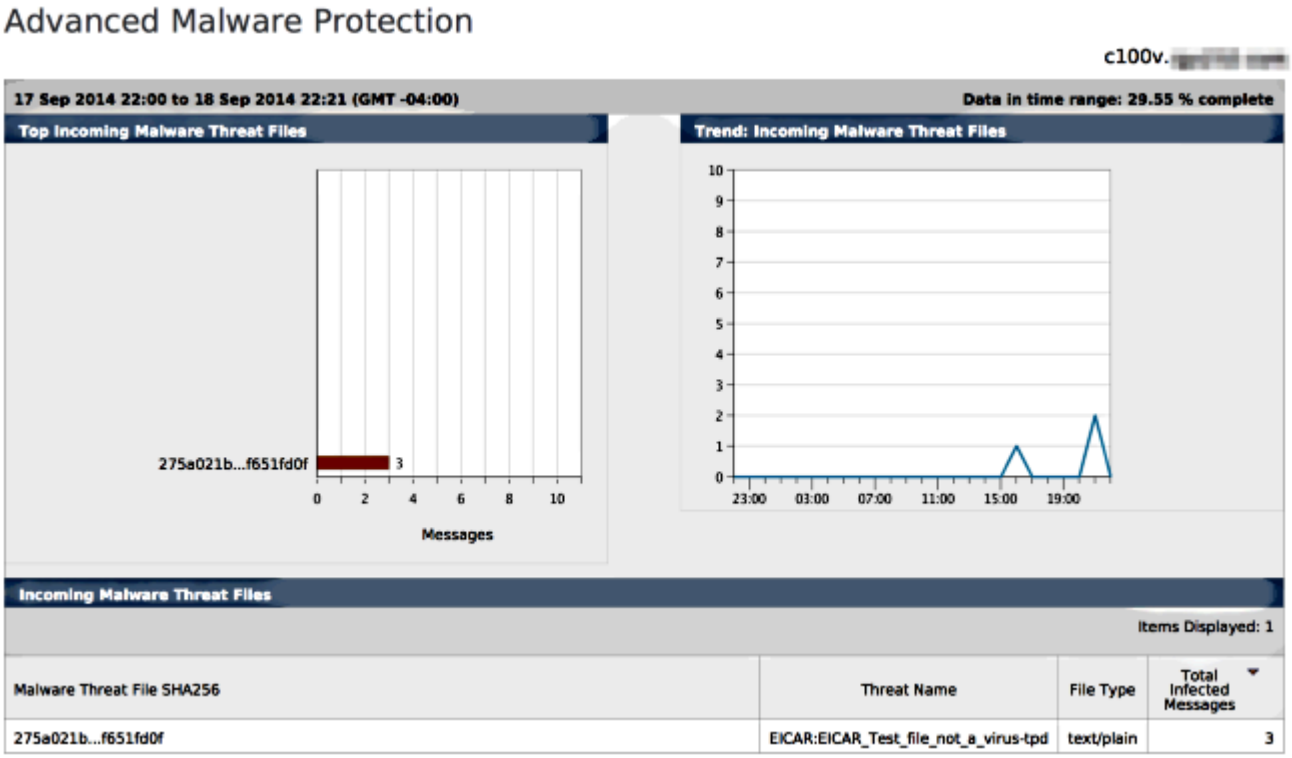
Suivi avancé des messages AMP+

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



Rapports Advanced Malware Protection

L'interface utilisateur graphique de l'ESA permet également d'afficher 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 voyez maintenant des informations similaires, avec les exemples précédents pour la saisie :



Dépannage

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

Dans l'exemple précédent, lorsque Sophos Anti-Virus est activé, il détecte et agit sur la pièce jointe :

<#root>

```
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 de Sophos Anti-Virus de la stratégie de messages entrants sont définis sur Abandon pour les messages infectés par un virus. Dans ce cas, AMP n'est jamais atteint pour analyser ou prendre des mesures sur la pièce jointe.

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

Informations connexes

- Guide des meilleures pratiques pour la protection avancée contre les programmes malveillants sur ESA
- Guide de l'administrateur de Cisco Email Security Appliance - Advanced Malware Protection
- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Assistance et documentation techniques - Cisco Systems

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.