Test de protection de malware avancé par ESA (AMP)

Contenu

Introduction

Ce document décrit comment tester et vérifier les caractéristiques avancées de protection de malware (AMP) de l'appliance de sécurité du courrier électronique de Cisco (ESA).

AMP de test sur l'ESA

Avec la release d'AsyncOS 8.5 pour l'ESA, l'AMP exécute des balayages de réputation de fichier et l'analyse de fichier afin de détecter le malware dans des connexions.

Touches de fonction

Afin d'implémenter l'AMP, vous devez avoir une touche de fonction valide et active pour la **réputation de fichier** et **classer l'analyse** sur votre ESA. Visitez les **touches de fonction de système Administration>** sur le GUI, ou employez les **featurekeys** sur le CLI, afin de vérifier les touches de fonction.

Services de sécurité

Afin d'activer le service du GUI, naviguez vers des **Services de sécurité > la réputation et l'analyse de fichier**. Du CLI, vous pouvez exécuter l'**ampconfig**. Soumettez et commettez vos modifications à la configuration.

Stratégies de messagerie entrante

Une fois que vous avez activé le service, vous devez avoir ce service attaché à une stratégie de messagerie entrante.

1. Naviguez **pour envoyer par mail des stratégies > des stratégies de messagerie entrante**.
2. Sélectionnez votre **stratégie par défaut** ou stratégie préconfigurée comme nécessaire. La colonne **avancée de protection de malware** sur la messagerie entrante maintient l'ordre des affichages de page.
3. Sélectionnez le lien de **handicapés** pour la colonne, et **activez la réputation de fichier** et **activez l'analyse de fichier** sur la page options.
4. Vous pouvez faire toute autre amélioration de configuration à la lecture de message, aux actions pour les connexions ONU-analysables, et aux actions pour les messages franchement identifiés, comme nécessaire.
5. Soumettez et commettez vos modifications à la configuration.

Test

Àce moment, votre stratégie de messagerie entrante est activée balayer et détecter le malware. Vous devez avoir un véritable échantillon de malware avec lequel pour tester. Si vous avez besoin d'exemples valides, rendez visite à l'institut européen pour la page (eicar) de téléchargements de recherches d'antivirus d'ordinateur.

> **Attention** : Cisco ne peut pas être jugé responsable quand ces fichiers ou votre scanner poids du commerce en combination avec ces fichiers endommagent n'importe quel votre ordinateur ou environnement de réseau. VOUS TÉLÉCHARGEZ CES FILES À VOS RISQUES ET PÉRILS. Téléchargez ces fichiers seulement si vous êtes suffisamment sécurisé dans l'utilisation de votre scanner, de paramètres de votre ordinateur, et d'environnement de réseau poids du commerce. Ces informations sont données comme courtoisie pour des buts de test et de reproduction.

Avec l'utilisation d'un valide un compte de messagerie préconfiguré, envoient la connexion par votre ESA et traitement normal. Vous pouvez utiliser le CLI de l'ESA, et les **mail_logs de queue** afin de surveiller la messagerie en tant qu'elle traite. Vous verrez l'ID de message (MID) répertorié dans les logs de messagerie. La sortie semblable à ceci 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 prouve que l'AMP a détecté la connexion de malware et **a chuté** comme mesure finale par valeurs par défaut.

Les mêmes détails sont également vus dans le message dépistant du GUI :

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 de fournir le malware franchement identifié, ou d'autres options avancées dans la configuration d'AMP des stratégies de messagerie entrante, vous pourriez voir cette messagerie traiter des résultats :

```
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
```

Le verdict de réputation est encore positif pour le **MALWARE** comme affiché. L'action réécrite est

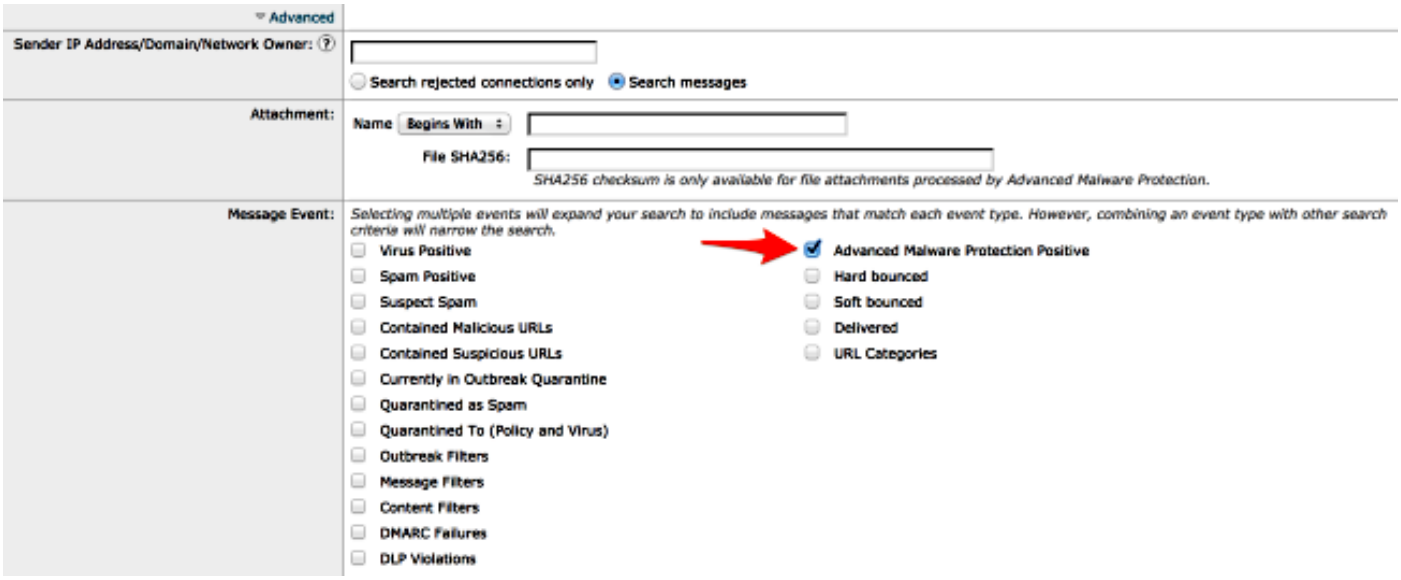
par actions de modification de message et ajouter de champ objet de au début **[AVERTISSANT : MALWARE DÉTECTÉ]**.

Un fichier propre, ou un fichier qui n'a pas été identifié au temps de traitement comme malware, a ce verdict écrit aux logs de messagerie :

```
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
```

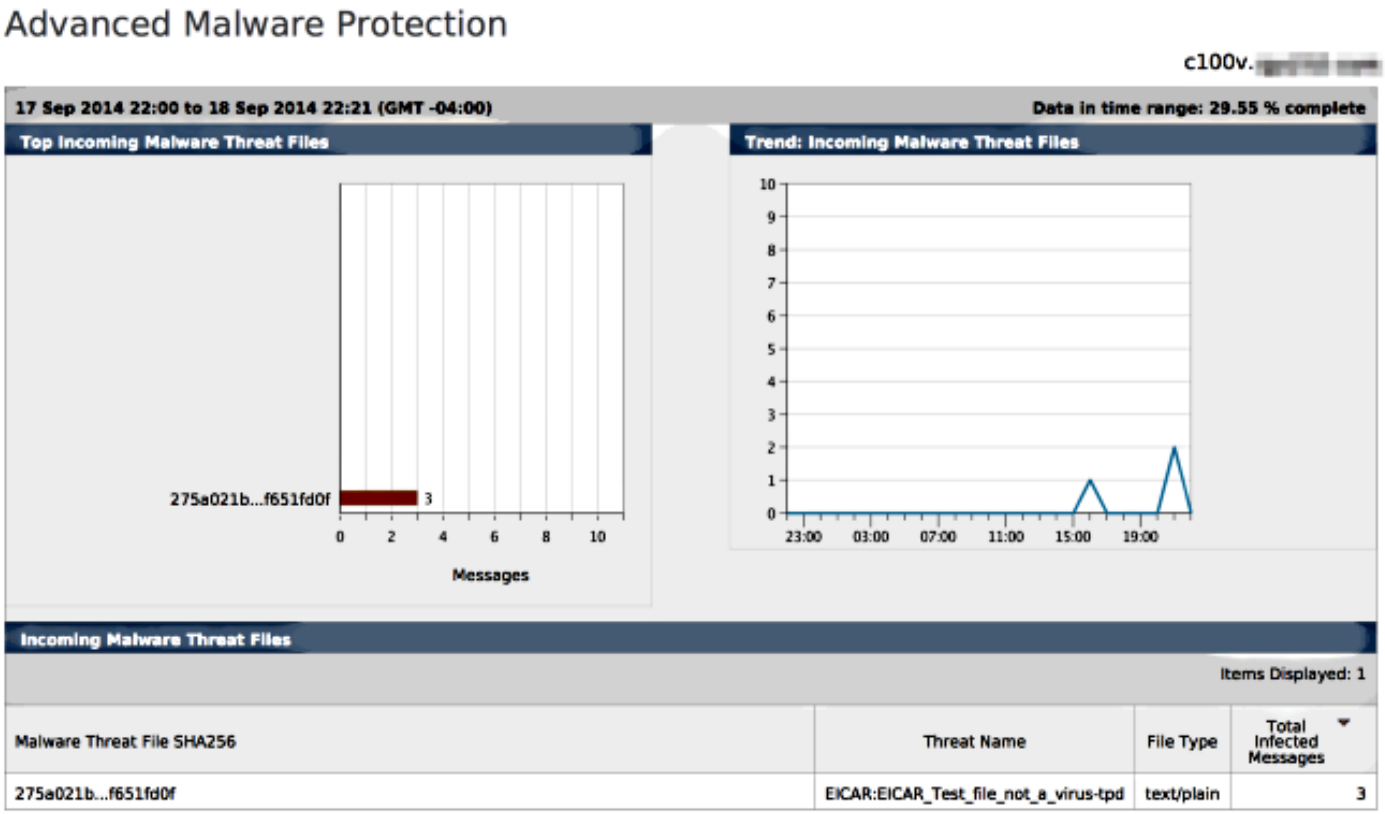
Message avancé dépistant pour des messages AMP+

Également du GUI, quand vous utilisez le cheminement de message et le menu déroulant avancé, vous pouvez choisir de rechercher un message positif de protection avancée de malware directement :



États avancés de protection de malware

Du GUI ESA, vous également voyez que l'état dépistant pour les messages franchement identifiés par AMP. Navigate **pour surveiller > a avancé la protection de malware** et modifiez la plage de temps comme nécessaire. Vous voyez maintenant semblable, avec les exemples précédents pour l'entrée :



Dépanner

Si vous ne voyez pas connue, le véritable fichier de malware qui est franchement analysé par AMP, passent en revue la commande de logins de messagerie pour s'assurer qu'un autre service n'a pas agi sur le message et/ou la connexion avant que l'AMP ait balayé le message.

De l'exemple plus tôt utilisé, quand l'antivirus de Sophos est activé, il réellement attrape et agit sur la connexion :

```
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 d'antivirus de Sophos sur la stratégie de messagerie entrante sont placés **pour chuter** pour les messages infectés par virus. Dans ce cas, l'AMP n'est jamais atteint pour balayer ou agir sur la connexion.

Ce n'est pas toujours le cas. Un examen de la messagerie se connecte et les id de message (MIDS) pourraient être nécessaires afin de s'assurer qu'un autre service OU un filtre de contenu/message n'a pas agi contre le MID avant l'AMP traitant et une action ont été atteints.

Informations connexes

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