Vérifier des téléchargements d'analyse de fichier sur l'ESA

Contenu

Introduction

Ce document décrit comment déterminer si des fichiers qui sont traités par la protection avancée de malware (AMP) sur l'appliance de sécurité du courrier électronique de Cisco (ESA) sont envoyés pour l'analyse de fichier, et aussi ce que le fichier journal associé d'AMP fournit.

Déterminez si des connexions sont téléchargées pour l'analyse de fichier

Avec le fichier l'analyse est activée, les connexions qui sont balayées par réputation de fichier peuvent être envoyées pour classer l'analyse pour l'analyse approfondie. Ceci fournit le de plus haut niveau de la protection contre le zéro-jour et les menaces visées. L'analyse de fichier est seulement disponible quand le filtrage de réputation de fichier est activé.

Employez les types de fichier options afin de limiter les types de fichiers qui pourraient être envoyés au nuage. Les fichiers spécifiques qui sont envoyés sont toujours basés sur des demandes du nuage de services d'analyse de fichier, qui vise ces fichiers pour lesquels l'analyse supplémentaire est nécessaire. L'analyse de fichier pour les types de fichier particuliers pourrait être désactivée temporairement où le nuage de services d'analyse de fichier atteint la capacité.

> Remarque: Référez-vous aux critères de fichier pour des services de protection avancés de malware pour le document Cisco de Produits de sécurité du contenu de Cisco pour le plus à jour et les informations complémentaires.

> Remarque: Veuillez examiner les notes de mise à jour et le guide utilisateur pour la révision spécifique d'AsyncOS qui fonctionne sur votre appliance, car les types de fichier d'analyse de fichier peuvent varier basé sur la version d'AsyncOS.

Types de fichier qui peuvent être envoyés pour l'analyse de fichier :

- Les types de fichier suivants peuvent actuellement être envoyés pour l'analyse : (Toutes les releases qui prennent en charge l'analyse de fichier) Windows Executables, des fichiers par exemple .exe, .dll, .sys, et .scr.Format PDF d'Adobe (PDF), Microsoft Office 2007+ (XML ouvert), Microsoft Office 97-2004 (VIEILLE), Microsoft Windows/DOS exécutable, d'autres types de fichier potentiellement malveillants.Types de fichier que vous avez sélectionnés pour le téléchargement page sur d'Anti-malware et de réputation configurations (pour la sécurité Web) ou page des configurations de réputation et d'analyse de fichier (pour la sécurité du courrier électronique.) Le support initial inclut le PDF et les fichiers de Microsoft Office.(Début dans AsyncOS 9.7.1 pour la sécurité du courrier électronique) si vous avez sélectionné les autres types de fichier potentiellement malveillants option, la Microsoft Office classe avec les extensions suivantes enregistrées dans le format XML ou MHTML : ade, ADP, ADN, accdb, accdr, accdt, accda, mdb, BDC, mda, mdn, mdt, mdw, forces de défense principale, mde, accde, maman, maq, mars, tapis, maf, ldb, laccdb, documentation, point, docx, docm, dotx, dotm, docb, xls, xlt, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, PPT, pot, PPS, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml, et xml.

  Remarque: Si le chargement au service d'analyse de fichier dépasse la capacité, quelques fichiers ne peuvent être analysés même si le type de fichier est sélectionné pour l'analyse et le fichier serait autrement habilité à l'analyse. Vous recevrez une alerte quand le service ne peut pas temporairement traiter des fichiers d'un type particulier.

Mettre en valeur les informations importantes :

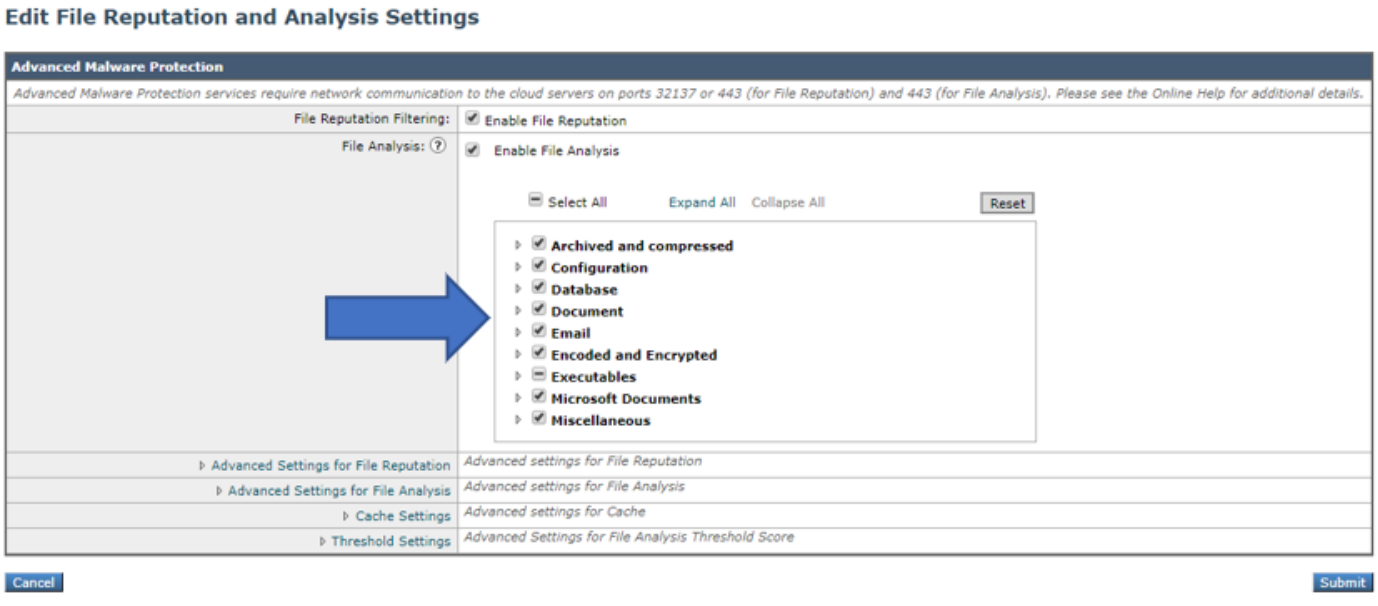
- Si un fichier a été récemment téléchargé de n'importe quelle source, le fichier ne sera pas téléchargé de nouveau. Pour des résultats d'analyse de fichier pour ce fichier, recherchez le SHA-256 de la page d'enregistrement d'analyse de fichier.
- L'appliance essayera une fois de télécharger le fichier ; si le téléchargement n'est pas réussi, par exemple en raison des problèmes de Connectivité, le fichier ne peut être téléchargé. Si la panne était parce que le serveur d'analyse de fichier a été surchargé, le téléchargement sera tenté une fois de plus.

Configurez l'AMP pour l'analyse de fichier

Par défaut, quand un ESA est d'abord activé et a établir encore une connexion à l'updater de Cisco, le SEUL type de fichier d'analyse de fichier répertorié sera les fichiers exécutables de « Microsoft Windows/DOS ». Vous devrez permettre à une mise à jour de service pour se terminer avant d'être laissé pour configurer les types de fichier supplémentaires. Ceci sera reflété dans le fichier journal d'updater_logs, vu en tant que « fireamp.json » :

```
Sun Jul 9 13:52:28 2017 Info: amp beginning download of remote file
"http://updates.ironport.com/amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp successfully downloaded file
"amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp applying file "amp/1.0.11/fireamp.json/default/100116"
```

Pour configurer l'analyse de fichier par l'intermédiaire du GUI, naviguez vers des **Services de sécurité > la réputation de fichier et l'analyse > éditent des paramètres généraux…**



Afin de configurer l'AMP pour l'analyse de fichier par l'intermédiaire du CLI, écrivez l'**ampconfig > la commande setup** et le mouvement par l'assistant de réponse. Vous devez sélectionner **Y** quand vous êtes présenté avec cette question : **Voulez-vous modifier les types de fichier pour l'analyse de fichier ?**

```
myesa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]>

Would you like to use File Analysis? [Y]>

File types supported for File Analysis:

1. Archived and compressed [selected]
2. Configuration [selected]
3. Database [selected]
4. Document [selected]
5. Email [selected]
6. Encoded and Encrypted [selected]
7. Executables [partly selected]
8. Microsoft Documents [selected]
9. Miscellaneous [selected]
```

```
Do you want to modify the file types selected for File Analysis? [N]> y

Enter comma separated serial numbers from the "Supported" list. Enter "ALL" to select all
"currently" supported File Types.
[1,2,3,4,5]> ALL

Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.
```

Basé sur cette configuration, les types de fichier qui sont activés sont sujets à l'analyse de fichier, comme applicable.

Logs d'AMP d'examen pour l'analyse de fichier

Quand des connexions sont balayées par réputation de fichier ou classent l'analyse sur l'ESA, elles sont enregistrées dans le log d'AMP. Afin de passer en revue ce log pour toutes les actions d'AMP, exécutez l'**Ampère de queue du** CLI de l'ESA, ou déplacez-vous par l'assistant de réponse pour la **queue** ou la commande de **grep**. La commande de **grep** est utile si vous connaissez le fichier spécifique ou d'autres détails que vous désirez rechercher dans le log d'AMP.

Voici un exemple :

```
mylocal.esa >  tail amp

Press Ctrl-C to stop.
Tue Aug 13 17:28:47 2019 Info: Compressed/Archive File: sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac MID = 1683600, Extracted File: File Name =
'[redacted].pdf', File Type = 'application/pdf', sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac, Disposition = LOWRISK, Response received from =
Cloud, Malware = None, Analysis Score = 0, upload_action = Recommended to send the file for
analysis
Thu Aug 15 13:49:14 2019 Debug: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Thu Aug 15 13:49:14 2019 Debug: Response received for file reputation query from Cloud. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

> Remarque: Des versions plus anciennes d'AsyncOS afficheraient « amp_watchdog.txt » dans les logs d'AMP. C'est un fichier de SYSTÈME D'EXPLOITATION qui est affiché toutes les dix minutes dans les logs. Ce fichier fait partie de la keep-alive pour l'AMP et peut être sans risque ignoré. Ce fichier est démarrer masqué dans AsyncOS 10.0.1 et plus nouveau.

> Remarque: Des versions plus anciennes d'AsyncOS se connecteront la balise d'upload_action a trois valeurs qui est définie pour que le téléchargement classe le comportement d'analyse.

Les trois réponses pour l'action de téléchargement sur AsyncOS plus ancien :

- « upload_action = 0" : Le fichier est connu au service de réputation ; n'envoyez pas pour l'analyse.
- « upload_action = 1" : Envoyez
- « upload_action = 2" : Le fichier est connu au service de réputation ; n'envoyez pas pour l'analyse

Les deux réponses pour l'action de téléchargement sur la version 12.x d'AsyncOS et en avant :

- le « upload_action = a recommandé d'envoyer le fichier pour l'analyse »
- **Le débogage se connecte seulement :** le « upload_action = a recommandé de ne pas envoyer le fichier pour l'analyse »

Cette réponse dicte si un fichier est envoyé pour l'analyse. De nouveau, il doit répondre aux critères des types de fichier configurés afin de pour être avec succès soumis.

Explication des balises d'action de téléchargement

```
"upload_action = 0": The file is known to the reputation service; do not send for analysis.
```

Pour "0," ceci signifie que le fichier « n'est pas nécessaire pour être envoyé pour le téléchargement ». Ou, une meilleure manière de le regarder est, le fichier *peut* être envoyée pour que le téléchargement classe l'analyse *s'il y a lieu*. Cependant, si le fichier n'est pas exigé alors le fichier n'est pas envoyé.

```
"upload_action = 2": The file is known to the reputation service; do not send for analysis
```

Pour "2," que c'est un strict « n'envoyez pas » le fichier pour le téléchargement. Cette action est finale et décisive, et le traitement d'analyse de fichier est fait.

Exemples de scénarios

Cette section décrit les scénarios possibles dans lesquels des fichiers sont téléchargés pour l'analyse correctement ou ne sont pas dus téléchargé à une raison spécifique.

Fichier téléchargé pour l'analyse

AsyncOS plus ancien :

Cet exemple affiche un fichier DOCX qui répond aux critères et est étiqueté avec l'**upload_action = 1.** Dans la prochaine ligne, le **fichier téléchargé pour l'**Algorithme de hachage sûr (SHA) d'**analyse** est aussi bien enregistré au log d'AMP.

```
Thu Jan 29 08:32:18 2015 Info: File reputation query initiating. File Name = 'Lab_Guide.docx',
MID = 860, File Size = 39136 bytes, File Type = application/msword
Thu Jan 29 08:32:19 2015 Info: Response received for file reputation query from Cloud. File Name
= 'Royale_Raman_Lab_Setup_Guide_Beta.docx', MID = 860, Disposition = file unknown, Malware =
None, Reputation Score = 0, sha256 =
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce, upload_action = 1
Thu Jan 29 08:32:21 2015 Info: File uploaded for analysis. SHA256:
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce
```

AsyncOS 12.x et en avant :

Cet exemple affiche un fichier PPTX qui répond aux critères et est étiqueté avec l'**upload_action = recommandé d'envoyer le fichier pour l'analyse**. Dans la prochaine ligne, le **fichier téléchargé pour l'**Algorithme de hachage sûr (SHA) d'**analyse** est aussi bien enregistré au log d'AMP.

```
Thu Aug 15 09:42:19 2019 Info: Response received for file reputation query from Cloud. File Name
= 'ESA_AMP.pptx', MID = 1763042, Disposition = UNSCANNABLE, Malware = None, Analysis Score = 0,
sha256 = 0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, upload_action = Recommended to
send the file for analysis
Thu Aug 15 10:05:35 2019 Info: File uploaded for analysis. SHA256:
0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, file name: ESA_AMP.pptx
```

Fichier non téléchargé pour l'analyse puisque le fichier est déjà connu

AsyncOS plus ancien :

Cet exemple affiche un fichier PDF qui est analysé par AMP avec l'**upload_action = 2** ajoutés au log de réputation de fichier. Ce fichier est déjà connu au nuage et n'est pas exigé pour être téléchargé pour l'analyse, ainsi elle n'est pas téléchargée de nouveau.

```
Wed Jan 28 09:09:51 2015 Info: File reputation query initiating. File Name = 'Zombies.pdf', MID
= 856, File Size = 309500 bytes, File Type = application/pdf
Wed Jan 28 09:09:51 2015 Info: Response received for file reputation query from Cache. File Name
= 'Zombies.pdf', MID = 856, Disposition = malicious, Malware = W32.Zombies.NotAVirus, Reputation
Score = 7, sha256 = 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002,
upload_action = 2
```

AsyncOS 12.x et en avant :

Cet exemple affiche le fichier d'amp_watchdog.txt avec le niveau de débogage de logins d'Ampère appariant l'**upload_action = recommandé de ne pas envoyer le fichier pour l'analyse** ajoutée au log de réputation de fichier. Ce fichier est déjà connu au nuage et n'est pas exigé pour être téléchargé pour l'analyse, ainsi elle n'est pas téléchargée de nouveau.

```
Mon Jul 15 17:41:53 2019 Debug: Response received for file reputation query from Cache. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

Téléchargement d'analyse de fichier journal par l'intermédiaire des en-têtes d'email

Du CLI, avec l'option utilisant le **logconfig de** commande, la sous-option des **logheaders** peut être sélectionnée pour répertorier et se connecter les en-têtes des emails traités par l'ESA. Utilisant « X-AMP-FILE-a téléchargé » l'en-tête, n'importe quand un fichier est téléchargé ou non téléchargé pour l'analyse de fichier sera enregistré aux logs de messagerie de l'ESA.

Regardant la messagerie se connecte, résulte pour des fichiers téléchargés pour l'analyse :

```
Mon Sep 5 13:30:03 2016 Info: Message done DCID 0 MID 7659 to RID [0] [('X-Amp-File-Uploaded',
'True')]
```

Regardant la messagerie se connecte, résulte pour des fichiers non téléchargés pour l'analyse :

```
Mon Sep 5 13:31:13 2016 Info: Message done DCID 0 MID 7660 to RID [0] [('X-Amp-File-Uploaded',
'False')]
```

Informations connexes

- Guides utilisateurs d'AsyncOS
- Critères de fichier pour des services de protection avancés de malware pour des Produits de sécurité du contenu de Cisco
- Test de protection de malware avancé par ESA (AMP)
- Support et documentation techniques - Cisco Systems