Analyse de fichier ESA par des procédures de vérification d'AMPÈRE

Contenu

Introduction

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

Contribué par Robert Sherwin, ingénieur TAC Cisco.

Déterminez si des fichiers sont téléchargés pour l'analyse

Quand l'analyse de fichier est activée, des fichiers pourraient être automatiquement envoyés dans tout l'AMPÈRE au nuage 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 information les informations complémentaires.

Ces types de fichier peuvent actuellement être envoyés pour l'analyse :

- Toutes les releases qui prennent en charge l'analyse et le Windows Executables de fichier, comme : fichiers **.exe**, **.dll**, **.sys**, et **.scr**.
- 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.

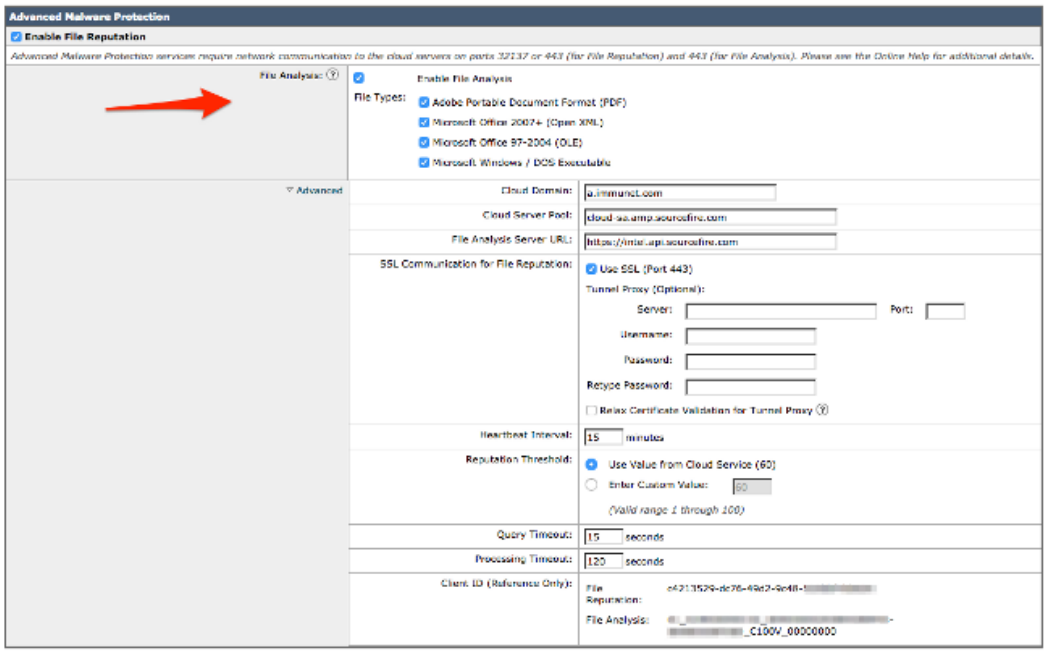
Remarque: Si le chargement au service d'analyse de fichier dépasse la capacité, quelques fichiers ne pourraient pas être analysés, même si le type de fichier est sélectionné pour l'analyse. Vous recevez une alerte quand le service ne peut pas temporairement traiter des fichiers d'un type particulier.

Voici quelques informations importantes :

- Les critères de taille de fichier est établis dynamiquement par le service en fonction d'analyse de fichier sur des tendances en cours de menace, et il peut changer à tout moment. Les modifications de critères les prennent effet automatiquement ; ainsi vous n'êtes pas requis de ne prendre aucune mesure.
- Si un fichier a été récemment téléchargé de n'importe quelle source, le fichier n'est pas téléchargé de nouveau. Afin d'obtenir les résultats d'analyse de fichier pour ce fichier, recherchez **SHA-256 de la** page d'enregistrement d'analyse de fichier.
- Les tentatives d'appareils de télécharger le fichier une fois ; si le téléchargement n'est pas réussi (par exemple, en raison des problèmes de Connectivité), le fichier ne pourrait pas être téléchargé. Si la panne est due à une surcharge de serveur d'analyse de fichier, le téléchargement est tenté une fois de plus.

Configurez l'AMPÈRE pour l'analyse de fichier

Afin de configurer l'AMPÈRE pour 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'AMPÈRE 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


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. Adobe Portable Document Format (PDF) [selected]
2. Microsoft Office 2007+ (Open XML) [selected]
3. Microsoft Office 97-2004 (OLE) [selected]
4. Microsoft Windows / DOS Executable [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]> 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 balayés et envoyés pour l'analyse, comme applicable.

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

Quand les fichiers applicables sont analysés par AMPÈRE, ils sont enregistrés dans le log d'AMPÈRE. Afin de passer en revue ce log pour toutes les actions d'AMPÈRE, sélectionnez la commande d' **Ampère de queue** dans le CLI, 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'AMPÈRE.

Voici un exemple :

```
myesa.local> tail amp

Press Ctrl-C to stop.
Mon Feb 2 14:45:35 2015 Info: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:45:35 2015 Info: Response received for file reputation query from Cache.
File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None,
Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe2
7e95b245f82, upload_action = 1
Mon Feb 2 14:55:35 2015 Info: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:55:35 2015 Info: Response received for file reputation query from Cache.
File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None,
Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe2
7e95b245f82, upload_action = 1
Mon Feb 2 15:05:35 2015 Info: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 15:05:35 2015 Info: Response received for file reputation query from Cache.
File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None,
Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe2
7e95b245f82, upload_action = 1
```

Le fichier d' **amp_watchdog.txt** est affiché toutes les dix minutes dans les logs. Ce fichier fait partie de la keep-alive pour l'AMPÈRE.

Les fichiers étant traité pour la réputation, ils ont l' **upload_action** étiquetés à la fin de la requête de réputation de fichier. Il y a trois réponses pour l'action de téléchargement :

```
"upload_action = 0": The file is known to the reputation service; do not send
 for analysis.
"upload_action = 1": Send
"upload_action = 2": The file is known to the reputation service; do not send
 for analysis
```

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.

Exemples de scénarios

Cette section décrit trois scénarios possibles dans lesquels des fichiers sont téléchargés pour l'analyse correctement, ou n'est pas due téléchargé à une raison spécifique.

Fichier téléchargé pour l'analyse

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'AMPÈRE.

```
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 = 754e3e13b2348ffd9c701bd3d8ae9
6c5174bb8ebb76d8fb51c7f3d9567ff18ce, upload_action = 1
Thu Jan 29 08:32:21 2015 Info: File uploaded for analysis. SHA256: 754e3e13b2348ffd9c7
01bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce
```

Fichier non téléchargé pour l'analyse due au type de fichier

Cet exemple affiche un fichier zip qui est analysé par AMPÈRE et étiqueté avec l' **upload_action = 1** ajouté au log de réputation de fichier, mais l'analyse de fichier d'AMPÈRE ne prend en charge pas des fichier zip. Par conséquent, il n'y a pas un SHA enregistré au log d'AMPÈRE pour ce fichier.

```
Wed Jan 28 08:21:43 2015 Info: File reputation query initiating. File Name =
'Sample_Malware_Files.zip', MID = 852, File Size = 272703 bytes, File Type =
application/zip
Wed Jan 28 08:21:45 2015 Info: Response received for file reputation query from Cloud.
```

```
File Name = 'Sample_Malware_Files.zip', MID = 852, Disposition = unscannable, Malware
= None, Reputation Score = 0, sha256 = 0edf4cbf86a3345ca930f1bcc37344b1d95e9f4e9d9da7
53339cefeff03df810, upload_action = 1
```

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

Cet exemple affiche un fichier PDF qui est analysé par AMPÈRE 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 = 00b32c3428362e39e4df2a0c3e0950947c147781fdd
3d2ffd0bf5f96989bb002, upload_action = 2
```

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 (AMPÈRE)**
- **Support et documentation techniques - Cisco Systems**

Date du fichier PDF généré: 16 décembre 2015

http://www.cisco.com/cisco/web/support/CA/fr/112/1128/1128628_118796-technote-esa-00.html