Проверка аналитических загрузок файла на ESA

Содержание

Введение

Этот документ описывает, как определить, передаются ли файлы, которые обработаны посредством Усовершенствованной вредоносной защиты (AMP) на Cisco Email Security Appliance (ESA), за анализом файла, и также что предоставляет связанный файл журнала AMP.

Определите, загружены ли прикрепления для анализа файла

С Файлом включен Анализ, прикрепления , которые просмотрены Репутацией Файла, могут быть переданы Анализу Файла для дальнейшего анализа. Это предоставляет высший уровень защиты от нулевого дня и предназначенных угроз. Когда фильтрация Репутации Файла включена, анализ файла только доступен.

Используйте опции File Types для ограничения типов файлов, которые могли бы быть переданы Облаку. Определенные файлы, которые передаются, всегда на основе запросов от Аналитического Облака сервисов Файла, которое предназначается для тех файлов, для которых необходим дополнительный анализ. Когда Аналитическое Облако сервисов Файла достигает емкости, анализ файла для определенных типов файла мог бы быть отключен временно.

> **Примечание:** См. Критерии Файла для Усовершенствованной Вредоносной Службы защиты для Документа Cisco продуктов Безопасности содержания Cisco для большинства современных данных и дополнительных сведений.

> **Примечание:** Рассмотрите Комментарии к выпуску и Руководство пользователя для определенного пересмотра AsyncOS, который работает на вашем устройстве, поскольку Аналитические типы файла Файла могут варьироваться на основе версии AsyncOS.

Типы файла, которые могут быть переданы за анализом файла:

- Следующие типы файла могут в настоящее время передаваться за анализом: (Все версии, что Анализ файла поддержки) Windows Executables, например .exe, .dll, .sys, и .scr файлы.Переносимый формат документа (PDF) Adobe, Microsoft Office 2007 + (Открытый XML), Microsoft Office 97-2004 (OLE), Microsoft Windows / Исполняемый файл DOS, Другие потенциально злонамеренные типы файла.Типы файла, которые вы выбрали для загрузки на странице настроек Антивируса и Репутации (для веб-Безопасности) или странице настроек Репутации и Анализа Файла (для Безопасности электронной почты.) Первичная поддержка включает файлы Microsoft Office и PDF.(Начинающийся в AsyncOS 9.7.1 для Безопасности электронной почты), Если вы выбрали Другую потенциально злонамеренную опцию типов файла, файлы Microsoft Office со следующими расширениями, сохраненными в формате MHTML или XML: ade, автоматическая обработка, adn, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdt, mdw, mdf, mde, accde, mam, maq, синяк, циновка, maf, ldb, laccdb, doc, точка, docx, docm, dotx, dotm, docb, xls, xlt, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, горшок, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, MHT, mhtm, mhtml, и xml.

  Примечание: Если загрузка на Аналитическом сервисе Файла превышает емкость, некоторые файлы не могут быть проанализированы, даже если бы тип файла выбран для анализа, и файл иначе имел бы право на анализ. Когда сервис будет временно неспособен обработать файлы определенного типа, вы получите предупреждение.

Выделение важных замечаний:

- Если файл был недавно загружен из какого-либо источника, файл не будет загружен снова. Для результатов анализа файла для этого файла ищите SHA 256 от Аналитической страницы создания отчетов Файла.
- Устройство попытается однажды загрузить файл; если загрузка не успешна, например из-за неполадок подключения, файл не может быть загружен. Если сбой состоял в том, потому что аналитический сервер файла был перегружен, загрузка будет предпринята еще раз.

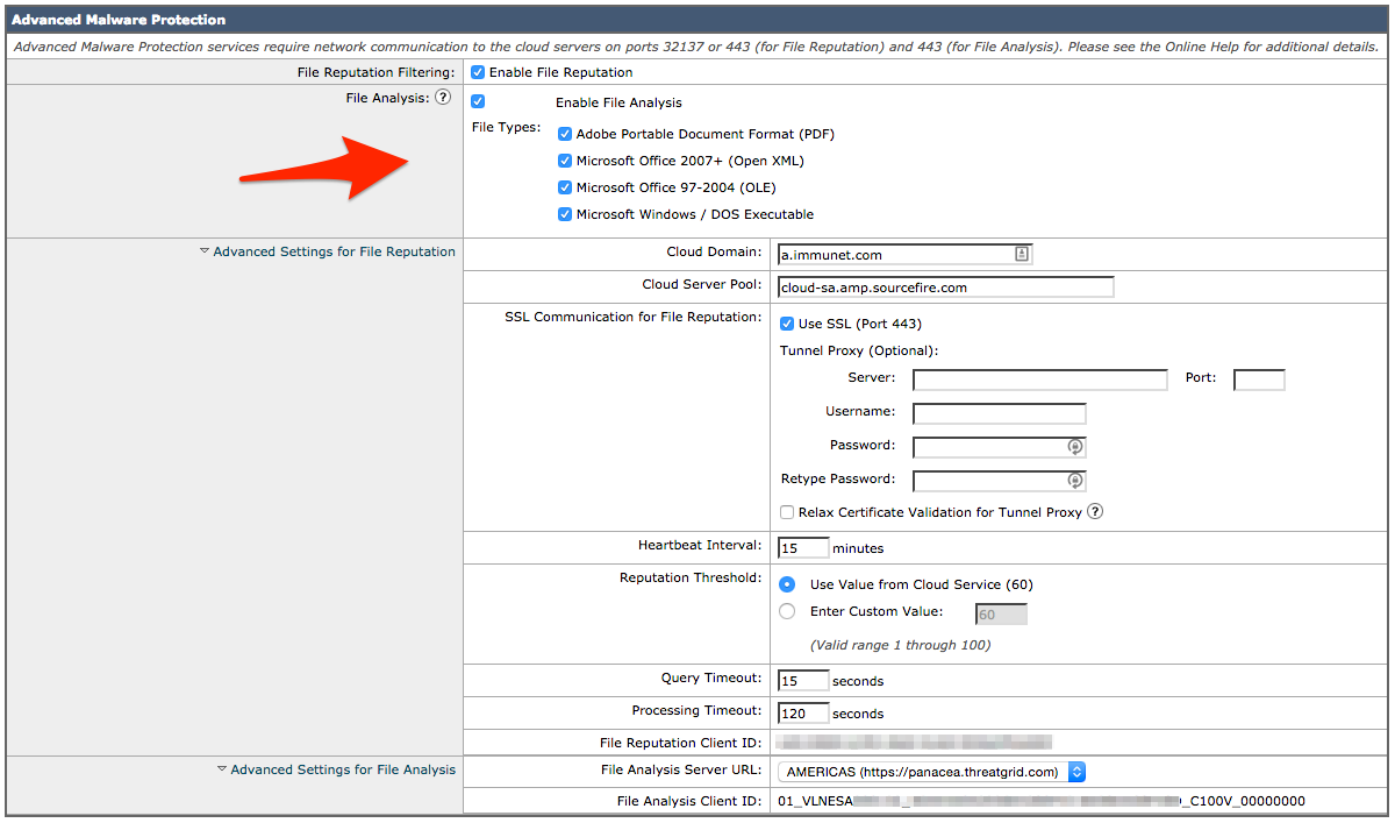
Настройте AMP для анализа файла

По умолчанию, когда ESA сначала включен и должен все же установить соединение со средством обновления Cisco, Аналитическим перечисленным типом файла Файла ONLY будет "Microsoft Windows / Исполнимые файлы" DOS. Необходимо будет позволить сервисному обновлению завершать до того, чтобы быть позволенным настроить дополнительные типы файла. Это будет отражено в updater_logs файле журнала, рассмотренном как "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"
```

К Анализу файла конфигурации через GUI перейдите к **Сервисам безопасности>, Репутация Файла и Анализ> Редактируют Глобальные параметры...**



Для настройки AMP для Анализа Файла через CLI введите **ampconfig>** команда **настройки** и переместитесь через мастера ответа. Когда вам предоставляют этот вопрос, необходимо выбрать **Y**: **вы хотите модифицировать типы файла для Анализа Файла?**

```
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. 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]
5. Other potentially malicious file types [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.
```

На основе этой конфигурации типы файла, которые включены, подвергаются Анализу Файла, как применимому.

Журналы AMP анализа для анализа файла

Когда прикрепления просмотрены Анализом Репутации или Файла Файла ESA, они зарегистрированы в журнале AMP. Для рассмотрения этого журнала для всех действий AMP выполните **хвостовой усилитель** от CLI ESA или перемещение через мастера ответа или для **хвоста** или для **команды grep**. **Команда grep** полезна, если вы знаете определенный файл или другие подробные данные, которые вы желаете искать в журнале AMP.

Например:

```
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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, 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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, 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 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

> **Примечание:** Более старые версии AsyncOS отобразили бы "amp_watchdog.txt" в журналах AMP. Это - файл ОС, который отображается каждые десять минут в журналах. Этот файл является частью поддержки активности для AMP и может быть безопасно проигнорирован. Этот файл скрыт, запустившись в AsyncOS 10.0.1 и более новый.

С файлом (файлами), обработанным для репутации, у них есть **upload_action**, помеченный в конце запроса репутации файла. Существует три ответа для действия загрузки:

- "upload_action = 0": файл известен сервису репутации; не посылайте за анализом.
- "upload_action = 1": Send

- "upload_action = 2": файл известен сервису репутации; не посылайте за анализом

Этот ответ диктует, передается ли файл за анализом. Снова, это должно соответствовать критериям настроенных типов файла, чтобы быть успешно отправленным.

Пояснение действия загрузки "0" по сравнению с действием загрузки "2"

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
Для "0", это означает, что файл не "необходим, чтобы быть переданным за загрузкой". Или, лучший способ посмотреть на него , файл *может* быть передан за загрузкой на Анализ Файла *при необходимости*. Однако, если файл *не* требуется тогда, файл не передается.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
Для "2", это - строгое, "не передают" файл за загрузкой. Это действие является окончательным и решающим, и Аналитическая обработка Файла сделана.

Примеры сценариев

В этом разделе описываются возможные сценарии, в которых файлы или загружены для анализа должным образом или не загружены из-за определенной причины.

Файл, загруженный для анализа

Данный пример показывает файл DOCX, который соответствует критериям и помечен с **upload_action = 1**. В следующей строке **Файл, загруженный для аналитического** Защищенного алгоритма хэширования (SHA), зарегистрирован к журналу AMP также.

```
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
```

Файл, не загруженный для анализа, поскольку уже известен файл

Данный пример показывает файл PDF, который просмотрен AMP с **upload_action = 2** добавленных к журналу репутации файла. Этот файл уже известен Облаку и не требуется, чтобы быть загруженным для анализа, таким образом, это не загружено снова.

```
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
```

Анализ Logging File загружает по электронной почте

заголовки

От CLI, с опцией с помощью команды **logconfig**, подпараметр **logheaders** может быть выбран, чтобы перечислить и регистрировать заголовки электронных почт, обработанных через ESA. Использование "X-Amp-File-Uploaded" заголовка, каждый раз, когда файл загружен или не загружен для анализа файла, будет зарегистрировано к почтовым журналам ESA.

При рассмотрении почтовых журналов результаты для файлов загрузили для анализа:

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

Рассмотрение почтовых журналов, результатов для файлов, не загруженных для анализа:

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

Дополнительные сведения

- Руководства пользователя AsyncOS
- Критерии файла для усовершенствованной вредоносной службы защиты для продуктов безопасности содержания Cisco
- Тест Усовершенствованной вредоносной защиты (AMP) ESA
- Cisco Systems – техническая поддержка и документация