Руководство FireAMP к исключениям на Windows

Содержание

Введение

Этот документ предоставляет рекомендацию по тому, как найти обнаруженные файлы и описывает процесс для исключения их. При выполнении AMP Cisco для Оконечных точек (также известный как FireAMP) на компьютере вы могли бы испытать проблему производительности на приложении или на самом компьютере. Это могло бы произойти из-за чрезмерных операций чтения-записи, разбивки на страницы или журналирования. Это может вызвать проблемы с приложениями, которые требуют исключительных индексов файла, таких как приложение базы данных или создание отчетов о программном обеспечении.

> **Внимание. :** Исключение уменьшает вашу зону уверенного приема. При исключении папки или файла FireAMP не просматривает в той папке. Во избежание исключения чрезмерных файлов необходимо быть определенными, когда это возможно.

Как найти обнаруженные файлы

Когда вы хотите исключить файлы, можно проявить широкий подход или записать очень определенное исключение с подстановочным знаком для покрытия просто файла, на который влияют. Этот документ запускается с основной идентификации каталогов Microsoft Windows.

C : файлы \Program

Большинство приложений установлено в этом каталоге. Эта папка часто является

источником для действия файла в системе и является основным вниманием. Cisco будет в поисках приложений базы данных и других антивирусных программ, а также собственного программного обеспечения или программного обеспечения для внутреннего пользования.

C : данные \Program

Этот каталог иногда используется, чтобы кэшировать или хранить временные файлы. В этой папке вы могли бы заметить много действий, которые зависят от приложений.

C : \Users

Этот каталог принимает различные каталоги пользователя, такие как рабочий стол, документы, загрузки и appdata. appdata папка универсально используется для временных файлов, интернет- файлов просмотра, истории, и так далее.

> **Внимание. :** Из-за количества файлов и данных, которые загружены в этом каталоге, необходимо быть осторожными, когда вы задаете исключение и пытаетесь быть максимально определенными для соответствия с "безопасными" файлами.

C : \Windows

Этот каталог имеет системные файлы. Вы обычно не должны исключать много из этого каталога, поскольку он обрабатывается набором исключения по умолчанию. Вы могли бы хотеть исключить эту папку для кэширования, такого как кэширование для Системный менеджер конфигурации центра (SCCM) и файлы журнала Windows.

Поддерживаемые типы исключения

Угроза: Это - название угрозы, которая не изолирована. Любой файл, который инициирует определенное название угрозы, не был бы изолирован. Примером является `Вин. Вредоносное ПО. PDF`

Путь: Это - размещение системы отдельного файла. Здесь можно использовать определенный путь, такой как `C:\Program Files\Cisco`, или можно использовать постоянный специальный список ID элемента (CSIDL).

> **Примечание:** CSIDL является встроенной переменной, которая распознана Windows и может быть полезной в сценариях, где путь мог находиться на других буквах диска. Примером является `CSIDL_PROGRAM_FILES\Cisco`. Данный пример покрывает `C:\Program Files\Cisco` и `D:\Program Files\Cisco`. CSIDLs только работают в исключениях Пути. См. документацию по Windows для полного списка доступного CSIDLs.

Подстановочный знак: Этот тип должен использоваться каждый раз, когда подстановочный знак (*) желаем в рамках исключения. Пример: `C : \Program Files\Cisco\*.tmp`

Расширение файла: Это - простое исключение для расширения файла типа файла. `Пример. текст`.

Когда исключить

Признак

Если вы выполняете FireAMP и испытываете проблемы производительности с системой или с определенным приложением, это могло быть индикацией относительно отсутствия ответа на ввод пользователя, низкой производительности автоматического процесса, сбоев или ошибок. Иногда отображения приложения определенная ошибка.

Проверка

Для определения файлов или каталогов, которые просмотрены и как часто, выполните эти действия:

Шаг 1: Первый шаг должен генерировать диагностический пакет и извлечь его. Это 7zip, архивируют, и требует, чтобы приложение извлекло его.

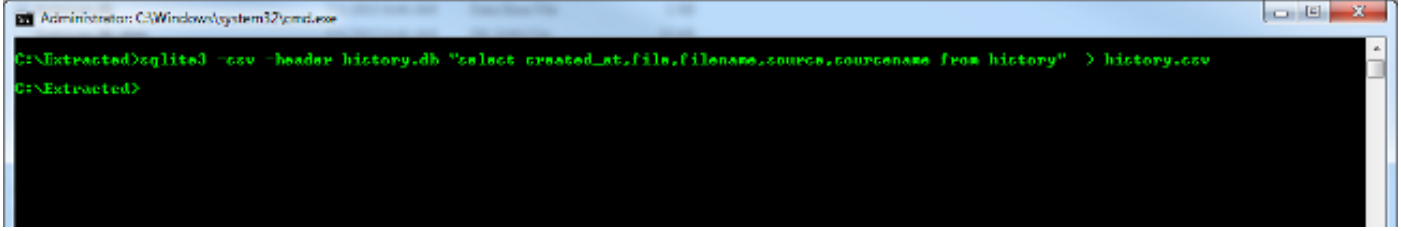
Шаг 2: Действие второе должно обратиться `к history.db` файлу от файла диагностики.

`history.db` файл является файлом базы данных SQLite, который отслеживает все обнаруженные файлы FireAMP. Каждая строка включает расположение, имя файла, SHA файла, исходный файл и исходный SHA. Источник является файлом, который создал/обратился сам файл. Это позволяет нам видеть, как приложение вело себя и что оно сделало.

В данном примере команда SQLite3 используется для преобразования базы данных истории в файл Отделенного запятой значения (CSV).

- Загрузите предварительно скомпилированные двоичные файлы SQLite3 для своей операционной системы.
- Извлеките пакет Диагностики FireAMP с приложением такой как 7zip.
- Перейдите к извлеченной диагностической папке и найдите `history.db` файл в рамках каталога `C_\Program Files\Sourcefire\fireAMP\`.
- В терминале или командной строке, вызовите двоичные файлы SQLite3, которые вы загрузили, и предоставьте `history.db` файлу эту команду. (Эта команда предполагает, что SQLite3 находится в местоположении, заданном в ваших переменных среды для вашей операционной системы, или это должно быть размещено в диагностической папке.)

```
sqlite3 -csv -header history.db "select created_at,file,filename,source,sourcename
from history" > history.csv
```



Если команда будет успешна, вы не будете видеть подтверждение или выводить.

Если подведенная команда, уверена, что вы задали местоположение двоичных файлов SQLite3. Если вы видите какие-либо другие сообщения в отношении `history.db` файла, вы, возможно, должны были бы очистить эти четыре файла истории от главного компьютера, на который влияют, в то время как сервис остановлен, который позволяет ему генерировать новый набор файлов в следующий раз, когда сервис запущен.

Шаг 3: Как только Файл csv генерировался, можно открыть его с предпочтительным приложением по работе с электронными таблицами. Приложения, такие как Microsoft Excel могли бы позволить вам преобразовывать Файл csv в таблицу, которая позволяет вам фильтровать/сортировать. Рассмотрите документацию microsoft для того, как использовать Excel.

Основные столбцы для использования:

- **имя файла:** Это поле показывает, что файл просмотрен FireAMP.
- **sourcename**: Это поле показывает процесс или исполняемый файл , который захватил маркер (чтение-запись и так далее). Эти данные используются, чтобы определить, обрабатываются ли файлы доверяемым приложением или иначе.
- **created_at**: Это - метка времени на событии для обнаружения файла.

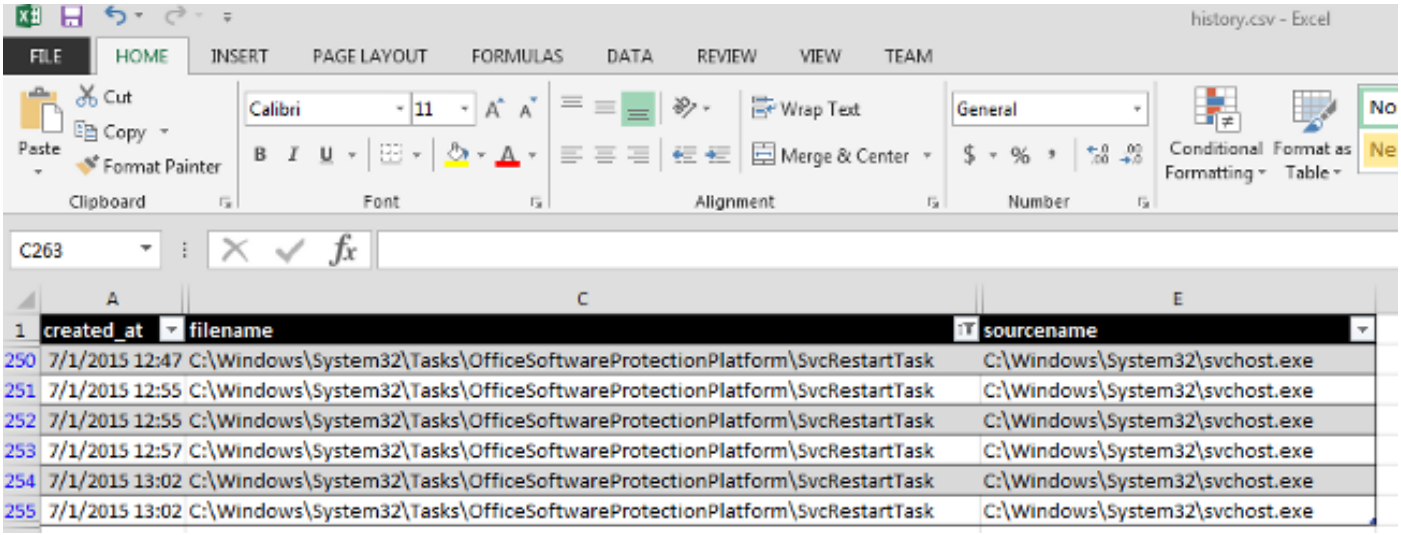
Устранение неполадок

На этом этапе существует несколько опций:

- Если вы просто испытали проблему производительности, можно сортировать таблицу **created_at**, который является просмотренной меткой времени, и посмотрите новые события. Можно просмотреть обнаружения и работать назад для наблюдения то, что произошло.
- Можно также искать или искать приложения, на которые, возможно, недавно повлиял FireAMP.

То, что вы хотите искать, является чем-то как тот же файл, который неоднократно просматривается, который мог бы иметь другие значения SHA. Вы также хотите посмотреть на тип файла, чтобы видеть, является ли это нормальным поведением.

В данном примере файл искался "офис". Результаты показывают файлы, что FireAMP просмотрел, который имел слово "офис" в имени файла или пути. Можно также видеть, что источник обрабатывает, который обработал соответствующий файл.



В данном примере FireAMP просматривает файл, отнесенный к сервису Microsoft Office. Если вы хотите исключить это, вы могли бы создать исключение простого контура такой как один показанный здесь:

```
C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask
```

Иногда, исключения не таким образом прямые. Иногда вы видите действие как это в других областях такой как,

```
C:\Users\Username\Appdata\
```

Например, SAID там является тестовым приложением что кэши к appdata каталогу с определенным именем файла. Можно исключить что-то с данным именем.

```
C:\Users\Test\Appdata\Temp\cookies
C:\Users\Test\Appdata\Temp\cache
C:\Users\Test\Appdata\Temp\Test\testcachefile20150116.tmp
```

Данный пример исключает файлы кэша для временного приложения. Однако вы не хотите исключать временную папку как интернет-файлы кэша, поскольку загрузки/образы могли находиться в этом каталоге. Можно также сузить каталог к тестовой папке, однако приложение могло бы соединиться с Интернетом также или иметь другие файлы кэша, которые не вредят производительности или могли потенциально быть открыты для риска. Подстановочный знак используется для исключения этого.

```
C:\Users\Test\Appdata\Temp\Test\testcachefile*.tmp
```

Как вы видите, подстановочный знак (*) использовался для составления чего-либо между буквами и точкой в имени файла. Этот подстановочный знак исключает любой файл, который совпадает с этим выражением. Это - пример того, как можно сузить исключения для предотвращения слишком большого количества риска.

Можно также использовать подстановочные знаки для названий полного пути. Вот подобный пример;

```
C:\Users\Test\Appdata\Temp\Test\20150116\cache\testfilecache083022.tmp
C:\Users\Test\Appdata\Temp\Test\20150117\cache\testfilecache092533.tmp
C:\Users\Test\Appdata\Temp\Test\20150118\cache\testfilecache104431.tmp
```

Исключения подстановочного знака - исключения могут быть сделаны на выражении с подстановочными знаками, где могут быть выражены и путь и имя файла. Т.е. если имя файла является постоянным, то лучше “ограничивать” подстановочный знак к определенному пути. Таким образом, если бы AIM.exe всегда существует в C:\Program Files (x86)*\AIM.EXE, посмотрел бы в любом подкаталоге.

После обнаружения желаемых исключений FireAMP можно выполнить действия, перечисленные в этой статье, чтобы внедрить их в информационной панели и выполнить тестирование.

Версия 5.0 +

В Версии 5.0 +, в действия файла больше не входят `history.db`. Новая структура для просмотренных файлов и путей расположена в `historyex.db`. Сценарий питона, не поддерживаемый Центром технической поддержки Cisco (TAC), доступен в Сообществе Cisco Support. На среде Linux сценарий в состоянии преобразовать `historyex.db` в файл Отделенного запятой значения (CSV). Это позволяет вам рассматривать действия для исключений.

Дополнительная документация

- Настройте и управляйте исключениями в FireAMP
- Рассмотрение Просмотров Файла на v5.0 +
- Cisco Systems – техническая поддержка и документация