对排除的FireAMP指南在Windows

目录

简介

本文提供一个指南关于怎样查找检测的文件并且描述进程排除他们。当您管理终端的(亦称FireAMP)时思科安培在计算机，您也许遇到性能问题在应用程序或在计算机。这也许发生由于额外的读/写操作，传呼或者连接。这能导致与要求不包括文件句柄的应用程序的问题，例如数据库应用程序或报告软件。

> **警告**：排除减少您的覆盖区域。当您排除文件夹或文件时， FireAMP不在该文件夹内扫描。为了避免额外的文件排除，您应该特定若情况许可。

如何查找检测的文件

当您要排除文件时，您能采取一清楚的方法或写入非常详细的排除以通配符为了报道一个受影响的文件。本文从Microsoft Windows目录的一基本识别开始。

C:\Program文件

大多应用程序在此目录安装。此文件夹经常是個的来源在系统并且是主要介绍。思科在监视数据库应用程序和其他反病毒程序以及所有权或者机构内部的软件。

C:\Program数据

此目录有时用于缓存或存储临时文件。在此文件夹中，您也许注意依靠应用程序的很多活动。

C:\Users

此目录适应多种用户文件夹，例如桌面、文档、下载和appdata。appdata文件夹全体地使用临时文件，浏览文件的互联网，历史记录，等等。

> **警告：**由于在此目录下载文件和数据的数量，您应该小心，当您指定排除时，并且设法尽可能具体地将匹配“安全”文件。

C:\Windows

此目录有系统文件。当由默认排除集，处理您通常不需要从此目录排除。您也许要排除缓存的此文件夹，例如系统中心配置管理器(SCCM)和Windows日志文件的高速缓冲存储。

支持的排除类型

威胁：这是没有被检疫威胁的名称。触发一特定的威胁名称的任何文件不会检查。示例是`Win.Malware.PDF`

路径：这是单个文件系统位置。这里您能使用一个特定路径例如`C:\Program Files\Cisco`，或者您能使用不变特殊项目标识列表(CSIDL)。

> **注意**：CSIDL是由Windows认可，并且可以是有用的在方案路径在不同的盘符可能驻留的一内置的变量。示例是`CSIDL_PROGRAM_FILES \`。此示例包括`C:\Program Files\Cisco`和`D:\Program Files\Cisco`。在路径排除的仅CSIDLs工作。可用的CSIDLs详尽列表的参考的窗口文档。

通配符： 必须使用此类型，每当通配符(*)在排除内希望。例如：`C:\Program Files\Cisco\*.tmp`

文件扩展：这是文件类型文件扩展的简单排除。示例是`.txt`。

什么时候排除

症状

如果运行FireAMP并且遇到性能问题用系统或与一特定应用程序，这可能是缺乏对用户输入的答复，性能低下自动化进程，失败或者错误的征兆。有时应用程序显示一个特定错误。

验证

为了确定被扫描，并且的文件或目录多么频繁地，请遵从这些步骤：

步骤 1：第一步将生成诊断程序包和解压缩它。这是7zip存档并且要求应用程序解压缩它。

步骤 2：第二步将访问`history.db`从诊断文件。

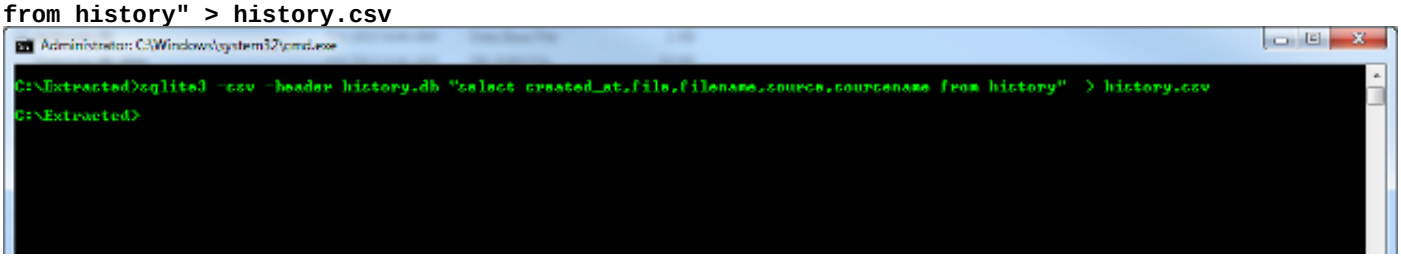
`history.db`是记录所有FireAMP检测文件的SQLite数据库文件。每行包括处理、文件名、文件SHA、源文件和来源SHA。来源是创建/访问文件的文件。这让我们发现应用程序如何运转，并且什

么。

在本例中， SQLite3命令用于为了转换历史记录数据库到逗号分隔的值(CSV)文件。

- 下载您的操作系统的PRE编译SQLite3二进制。
- 解压缩与一应用程序的FireAMP诊断程序包例如7zip。
- 导航到解压缩的诊断文件夹并且查找在C_ \\ Sourcefire \ fireAMP \history.db。
- 在终端或prompt命令内，请呼叫您下载的SQLite3二进制并且提供history.db此命令。(此命令假设， SQLite3在您的您的操作系统的环境变量指定的位置或者它需要在诊断文件夹内被放置。)

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



如果命令是成功的，您将看不到确认或输出。

如果命令失败，请务必您指定SQLite3二进制的位置。如果关于history.db看到任何其他消息，您也许需要清除从受影响的主机的四份历史文件，当服务被终止时，允许它生成新套文件服务下次开始。

步骤 3： 一旦CSV文件生成您能打开它与您的首选的电子表应用程序。应用程序例如Microsoft Excel也许允许您转换CSV文件到表，给您过滤/排序。参阅如何的Microsoft文档能使用Excel。

使用的主要的列是：

- **文件名**：此字段显示文件由FireAMP扫描。
- **sourcename** ：此字段显示获取把柄的进程或可执行(读/写等等)。此数据用于为了确定文件是否由委托应用程序处理或。
- **created_at** ：这是在事件的时间戳文件的检测的。

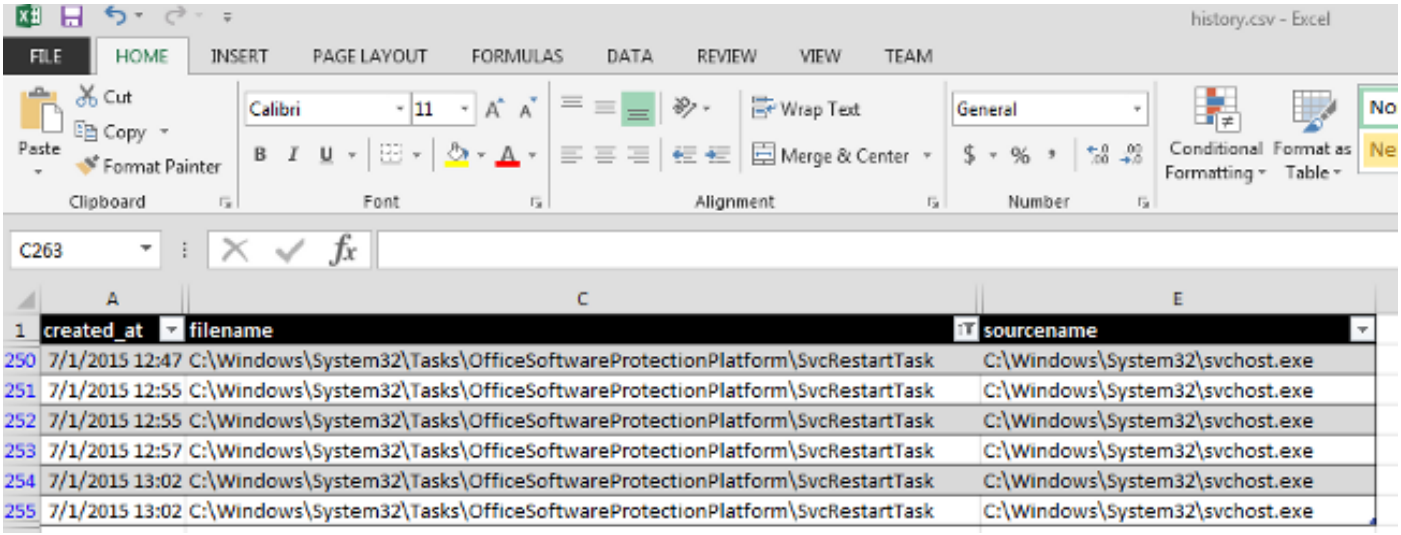
故障排除

这时有两三个选项：

- 如果遇到了性能问题，您能由是被扫描的时间戳的**created_at**排序表和看到多数近期事件。您能向后浏览检测和工作为了发现发生什么。
- 您能为也许由FireAMP最近已经影响了的应用程序也搜索或浏览。

什么您要寻找是某事类似重复被扫描也许有不同的SHA值的同一个文件。您也要查看文件类型为了发现这是否是预料之中的行为。

在本例中，文件被搜索了“办公室”。结果表示文件， FireAMP在文件名或路径扫描了有词“办公室”。您能也看到被处理对应的文件的来源进程该。



	A	C	E
1	created_at	filename	sourcename
250	7/1/2015 12:47	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe
251	7/1/2015 12:55	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe
252	7/1/2015 12:55	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe
253	7/1/2015 12:57	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe
254	7/1/2015 13:02	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe
255	7/1/2015 13:02	C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask	C:\Windows\System32\svchost.exe

在本例中， FireAMP扫描与微软办公软件服务涉及的一个文件。如果要排除此，您可能创建简单路径排除例如显示的那个此处：

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

有时，排除不是那么直接的。偶然地您在其他区域看到象这样的活动例如，

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

例如，请说有测试应用程序该缓存对与一个特定文件名的appdata目录。您能排除某事与教名。

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

此示例排除临时应用程序的缓存文件。然而，因为互联网缓存文件作为下载/镜像在此目录，可能驻留您不要排除临时文件夹。您能也缩小目录到测验文件夹，然而应用程序也许连接到互联网，或者有不危害性能也不可能潜在是开放的冒险的其他缓存文件。通配符用于排除此。

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

您看到，通配符(*)用于占任何东西在字母和小点之间在文件名。此通配符排除匹配此表达式的所有文件。这是示例您如何能缩小排除为了防止许多种风险。

您能也使用通配符完整路径名。这是一相似的示例;

```
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
```

通配符排除-排除在路径和文件名可以表示的通配符表达式可以完成。即，如果文件名是不变，然后它是最佳“限制条件”通配符到一个特定路径。 因此，如果AIM.exe在C:\Program文件总是存在(x86)*\AIM.EXE在所有子目录将查找。

在您查找您的希望的FireAMP排除后，您在您的控制板能遵从在此条款列出的步骤为了实现他们和执行测试。

版本5.0+

在版本5.0+中，個不再是登录的`history.db`被扫描的文件的新的结构和路径在historyex.db查找`Python`脚本，不支持由Cisco技术支持中心(TAC)，在CiscoSupport公共中是可用的。在Linux环境，脚本能转换historyex.dbto(CSV)文件。它允许您查看排除的活动。

相关文档

- 在FireAMP配置与管理排除
- 查看在v5.0+的文件扫描
- 技术支持和文档 - Cisco Systems