Guia de FireAMP às exclusões em Windows

Índice

Introdução

Este documento fornece uma diretriz em como encontrar detectou arquivos e descreve um processo para exclui-los. Quando você dirige Cisco AMP para os valores-limite (igualmente conhecidos como FireAMP) em um computador, você pôde experimentar o problema de desempenho em um aplicativo ou no computador próprio. Isto pôde ocorrer devido às operações, à paginação, ou ao gerencio de leitura/gravação excessivo. Isto pode causar edições com aplicativos que exigem os identificadores de arquivo exclusivos, tais como o software do aplicativo de base de dados ou do relatório.

> **Caution**: A exclusão reduz sua área de cobertura. Quando você exclui um dobrador ou um arquivo, FireAMP não faz a varredura dentro desse dobrador. A fim evitar a exclusão de arquivos excessivos, você deve ser específico sempre que possível.

Como encontrar arquivos detectados

Quando você quer excluir arquivos, você pode tomar uma aproximação larga ou escrever uma exclusão muito específica com um convite a fim cobrir apenas um arquivo afetado. Este documento começa com uma identificação básica de diretórios de Microsoft Windows.

Arquivos de C:\Program

A maioria dos aplicativos são instalados neste diretório. Este dobrador é frequentemente a fonte para a atividade de arquivo no sistema e é o foco preliminar. Cisco estará na vigia para aplicativos de base de dados e os outros programas de antivirus assim como software do proprietário ou da em-casa.

Dados de C:\Program

Este diretório é usado às vezes para pôr em esconderijo ou armazenar arquivos temporário. Neste dobrador, você pôde observar muitas atividades que são dependentes dos aplicativos.

C:\Users

Este diretório acomoda várias pastas de usuário, tais como o desktop, os documentos, as transferências, e o appdata. O dobrador do appdata é usado universalmente para arquivos temporário, arquivos da consultação do Internet, história, e assim por diante.

> **Caution**: Devido ao número de arquivos e de dados que são transferidos neste diretório, você deve ser cuidadoso quando você especifica uma exclusão, e tenta dever o mais específico possível combinar os arquivos “seguros”.

C:\Windows

Este diretório tem os arquivos de sistema. Você geralmente não precisa de excluir muito deste diretório enquanto é segurado pelo grupo da exclusão do padrão. Você pôde querer excluir este dobrador para pôr em esconderijo, tal como pôr em esconderijo para arquivos de registro do gerenciador de configuração (SCCM) e do Windows de System Center.

Tipos apoiados da exclusão

Ameaça: Este é o nome de uma ameaça que não quarantined. Nenhum arquivo que provocar um nome particular da ameaça não quarantined. Um exemplo é `Win.Malware.PDF`

Caminho: Este é um local de sistema do arquivo único. Aqui você pode usar um trajeto específico tal como `C:\Program Files\Cisco`, ou você pode usar a lista especial constante do artigo ID (CSIDL).

> **Note**: Um CSIDL é uma variável incorporado que seja reconhecida por Windows e possa ser útil nas encenações onde um trajeto poderia residir em letras da unidade diferentes. Um exemplo é `CSIDL_PROGRAM_FILES \ Cisco`. Este exemplo cobre `C:\Program Files\Cisco` e `D:\Program Files\Cisco`. Trabalho de CSIDLs somente em exclusões do trajeto. Refira a documentação de Windows para uma lista completa de CSIDLs disponível.

Convite: Este tipo deve ser usado sempre que um convite (*) é desejado dentro da exclusão. Por exemplo: `C:\Program Files\Cisco\ *.tmp`

Extensão de arquivo: Esta é uma exclusão simples para uma extensão de arquivo do tipo de arquivo. Um exemplo é `.txt`.

Quando excluir

Sintoma

Se você executa FireAMP e problemas de desempenho da experiência com o sistema ou com um aplicativo específico, esta poderia ser uma indicação da falta da resposta à entrada de usuário, ao desempenho lento de um processo automático, aos impactos, ou aos erros. Às vezes o aplicativo indica um erro específico.

Verificação

A fim determinar os arquivos ou os diretórios que são feitos a varredura e como frequentemente, siga estas etapas:

Passo 1: A primeira etapa é gerar o pacote diagnóstico e extrai-lo. Este é um arquivo 7zip e exige um aplicativo extrai-lo.

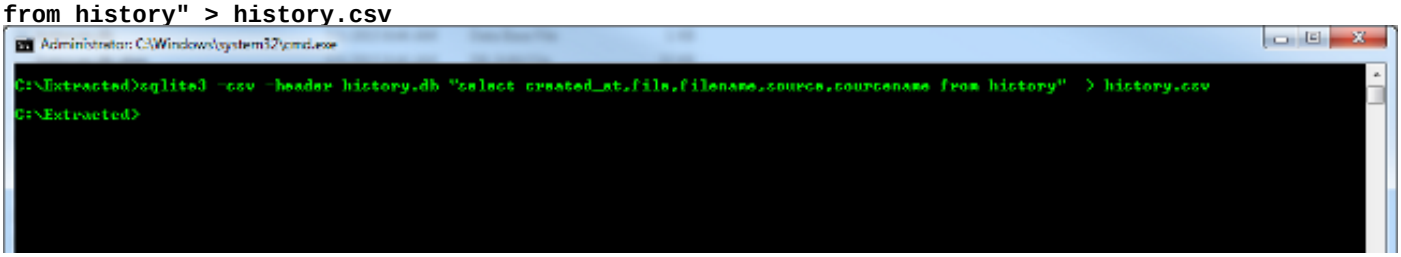
Passo 2: O segundo passo é alcançar o `arquivo history.db do` arquivo de diagnóstico.

`O arquivo history.db` é um arquivo da base de dados de SQLite que se mantenha a par de todo o FireAMP detecte arquivos. Cada fileira inclui a disposição, o nome de arquivo, o arquivo SHA, o arquivo de origem, e a fonte SHA. A fonte é o arquivo que criou/alcançou o arquivo próprio. Isto deixa-nos ver como o aplicativo se comportou e o que fez.

Neste exemplo, o comando SQLite3 é usado a fim converter o base de dados da história em um arquivo do Comma Separated Value (CSV).

- Transfira o binário SQLite3 PRE-compilado para seu sistema operacional.
- Extraia o pacote diagnóstico de FireAMP com um aplicativo tal como 7zip.
- Navegue ao dobrador diagnóstico extraído e encontre o `arquivo history.db` dentro do C_ `\ arquivos de programa \ Sourcefire \ fireAMP \ diretório`.
- Dentro de um terminal ou de um comando prompt, chame o binário que SQLite3 você transferiu e forneça o `arquivo history.db` este comando. (Este comando o supõe que SQLite3 está em um lugar especificado em seus variáveis de ambiente para seu sistema operacional, ou precisa de ser colocado dentro do dobrador diagnóstico.)

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



Você não verá a confirmação ou output se o comando é bem sucedido.

Se o comando falhou, seja certo que você especificou o lugar do binário SQLite3. Se você vê quaisquer outras mensagens com respeito ao `history.db arquivar`, você pôde precisar de cancelar os quatro arquivos históricos da máquina host afetada quando o serviço for parado, que permite que gerencia um grupo fresco de arquivos o serviço é começado a próxima vez que.

Passo 3: Uma vez que o arquivo CSV foi gerado você pode abri-lo com seu aplicativo de planilha preferido. Os aplicativos tais como Microsoft Excel puderam permitir que você converta o arquivo CSV a uma tabela, que lhe permitisse filtrar/tipo. Reveja a documentação Microsoft para que como use Excel.

As colunas preliminares a usar-se são:

- **nome de arquivo**: Este campo mostra que o arquivo está feito a varredura por FireAMP.
- **sourcename**: Este campo mostram o processo ou executável que agarrado o punho (read/write e assim por diante). Estes dados são usados a fim determinar se os arquivos estão segurados por um aplicativo confiado ou de outra maneira.
- **created_at**: Este é o timestamp no evento para a detecção do arquivo.

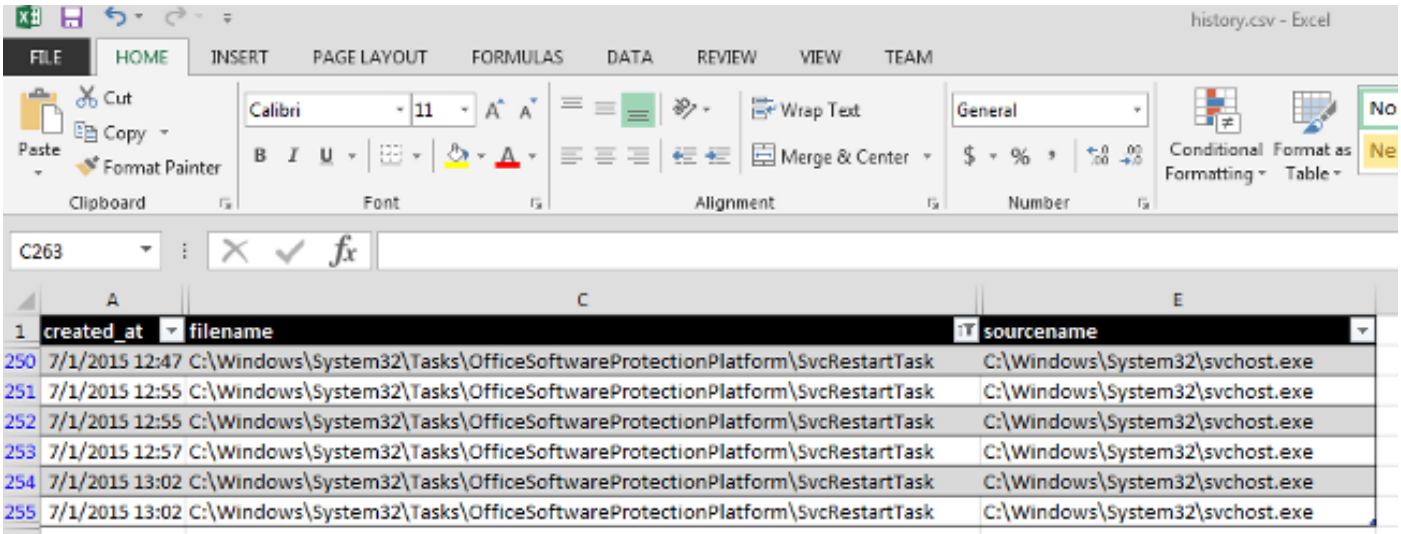
Troubleshooting

Neste momento há um par opções:

- Se você apenas experimentou o problema de desempenho, você pode classificar a tabela pelo **created_at** que é o timestamp feito a varredura e ver a maioria de acontecimentos recentes. Você pode consultar as detecções e o trabalho para trás a fim ver o que aconteceu.
- Você pode igualmente procurar ou consultar para os aplicativos que puderam recentemente ter sido impactados por FireAMP.

O que você quer procurar é algo como o mesmo arquivo que é feito a varredura repetidamente que pôde ter valores diferentes SHA. Você igualmente quer olhar o tipo de arquivo a fim ver se este é comportamento esperado.

Neste exemplo, o arquivo foi procurado pelo “escritório”. Os resultados mostram aos arquivos que FireAMP fez a varredura que tido a palavra “escritório” no nome de arquivo ou no trajeto.
Você pode igualmente ver o processo da fonte que segurou o arquivo correspondente.



Neste exemplo, FireAMP faz a varredura de um arquivo relativo a um serviço do microsoft office. Se você quer excluir este, você poderia criar uma exclusão simples do trajeto tal como essa mostrada aqui:

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

Às vezes, as exclusões não são tão diretas. Ocasionalmente você vê a atividade como este em

outras áreas como,

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

Por exemplo, diga que há um aplicativo de teste esse esconderijos ao diretório do appdata com um nome de arquivo específico. Você pode excluir algo com o nome concedido.

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

Este exemplo exclui arquivos de cache para o aplicativo do temp. Contudo, você não quer excluir o dobrador do temp porque os arquivos de cache do Internet como transferências/imagens poderiam residir neste diretório. Você pode igualmente reduzir para baixo o diretório ao dobrador do teste, porém o aplicativo pôde conectar ao Internet também, ou tem outros arquivos de cache que não prejudicam o desempenho nem poderiam potencialmente estar abertos arriscar. Uma curinga é usada para excluir esta.

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

Como você vê, um convite (*) foi usado para esclarecer qualquer coisa entre as letras e o ponto no nome de arquivo. Este convite exclui todo o arquivo que combinar esta expressão. Este é um exemplo de como você pode reduzir para baixo exclusões a fim impedir demasiado risco.

Você pode igualmente usar curingas para nomes de caminho cheio. Está aqui um exemplo similar;

```
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
```

Exclusões do convite - As exclusões podem ser feitas em uma expressão do convite onde o trajeto e o nome de arquivo possam ser expressados. Isto é, se o nome de arquivo é constante, a seguir ele é o melhor “forçam” o convite a um trajeto específico. Assim se AIM.exe existe sempre em C:\Program arquiva (x86)*\AIM.EXE olharia em todo o sub-diretório.

Depois que você encontra suas exclusões desejadas de FireAMP, você pode seguir as etapas alistadas neste artigo a fim executá-las em seu painel e executar testes.

Versão 5.0+

Na versão 5.0+, as atividades de arquivo são registradas já não em `history.db`. Uma estrutura nova para arquivos feitos a varredura e os trajetos são ficados situada em historyex.db. Um script do `pitão`, não apoiado pelo centro de assistência técnica da Cisco (TAC), está disponível na comunidade de CiscoSupport. Em um ambiente de Linux, o script pode converter o historyex.dbto um arquivo do `Comma Separated Value` (CSV). Permite que você rever as atividades para exclusões.

Documentos relacionados

- Configurar e controle exclusões em FireAMP
- Revendo varreduras de arquivo em v5.0+

- Suporte Técnico e Documentação - Cisco Systems