Windows での除外に関する FireAMP ガイド

目次

概要

この資料は方法でガイドラインを検出するファイルを見つける提供し、それらを除くためにプロセスを説明したものです。 コンピュータのエンドポイント（別名 FireAMP）のための Cisco AMP を実行するとき、アプリケーションまたはコンピュータ自体のパフォーマンス上の問題に直面するかもしれません。 これは余分な読み書きオペレーション、ページング、または日誌に記すことが原因で発生するかもしれません。 これは排他的なファイル ハンドルを必要とするデータベース アプリケーションまたはレポート ソフトウェアのようなアプリケーションにおいての問題を引き起こす場合があります。

> **注意**： 除外はカバレッジ 領域を減らします。 フォルダかファイルを除くとき、FireAMP はそのフォルダの内でスキャンしません。 余分なファイルの除外を避けるために、可能な限り特定であるはずです。

検出するファイルを見つける方法

ファイルを除きたいと思うとき広いアプローチを行うか、またはちょうど影響を受けたファイルをカバーするためにワイルドカードとの極めて特殊な除外を書くことができます。 この資料は Microsoft Windows ディレクトリの基本的な識別から開始します。

C:\Program ファイル

アプリケーションのほとんどはこのディレクトリにインストールされています。 このフォルダは頻繁にシステムのファイル アクティビティにおける出典で、プライマリ フォーカスです。 Cisco はデータベース アプリケーションおよび他の抗ウイルスプログラム、また独自または社内ソフトウェアのための眺望にあります。

C:\Program データ

時々このディレクトリがテンポラリファイルをキャッシュするか、または保存するのに使用されています。 このフォルダでは、アプリケーションに依存している多くのアクティビティに注意するかもしれません。

C:\Users

このディレクトリはデスクトップ、文書、ダウンロードおよび appdata のようなさまざまなユーザ の フォルダを、取り扱います。 appdata フォルダはテンポラリファイルのためにユニバーサル、ファイルを、履歴参照する、インターネット等使用されます。

> **注意**： 除外を注意する規定 するはずで、「安全な」ファイルを一致するためにできるだけ特定であることを試みますときこのディレクトリでダウンロードされるデータおよびファイルの数が原因で。

C:\Windows

このディレクトリにシステム ファイルがあります。 デフォルト除外 セットによって処理されると同時に一般にこのディレクトリから多くを除く必要はありません。 、システム センター コンフィギュレーションマネージャ (SCCM) および Windows ログファイルのためのキャッシングのようなキャッシュのためのこのフォルダを除きたいと思うかもしれません。

サポートされた除外型

脅威: これは検疫されない脅威の名前です。 どのファイルでも特定の脅威名前を引き起こす検疫されません。 例は `Win.Malware.PDF` です

[Path]： これは単一 ファイル システム口ケーションです。 ここでは `C:\Program Files\Cisco` のような特定のパスを使用できますまたは一定した特別な項目 ID リスト (CSIDL) を使用できます。

> **注:** CSIDL は Windows によって認識され、パスが異なるドライブレターに常駐する可能性があるシナリオで役立ちます組み込み変数です。 例は `CSIDL_PROGRAM_FILES \ Cisco` です。 この例は `C:\Program Files\Cisco` および `D:\Program Files\Cisco` カバーします。 CSIDLs パス 除外の作業だけ。 利用可能 な CSIDLs の詳細なリストのための Windows ドキュメントを参照して下さい。

ワイルドカード: この型はワイルドカードが除外の内で (*) 望まれる時はいつでも使用する必要があります。 次に、例を示します。 `C:\Program Files\Cisco\ *.tmp`

ファイル拡張子: これはファイルタイプのファイル拡張子のための簡単な除外です。 例は `.txt` です。

いつ除くか

症状

FireAMP を実行し、システムまたは特定のアプリケーションにおいてのパフォーマンス上の問題に直面する場合、これはユーザインプットへの応答の欠如、自動化 された プロセスの低いパフォーマンス、クラッシュ、またはエラーの示す値である可能性があります。 時々アプリケーションは特定のエラーを表示する。

確認

頻繁にかどのようにスキャンされる、そして判別するためにファイルをかディレクトリ、次の手順に従って下さい:

ステップ 1： 第一歩は診断パッケージを生成し、得ることです。 これは 7zip アーカイブで、アプリケーションをそれを得るように要求します。

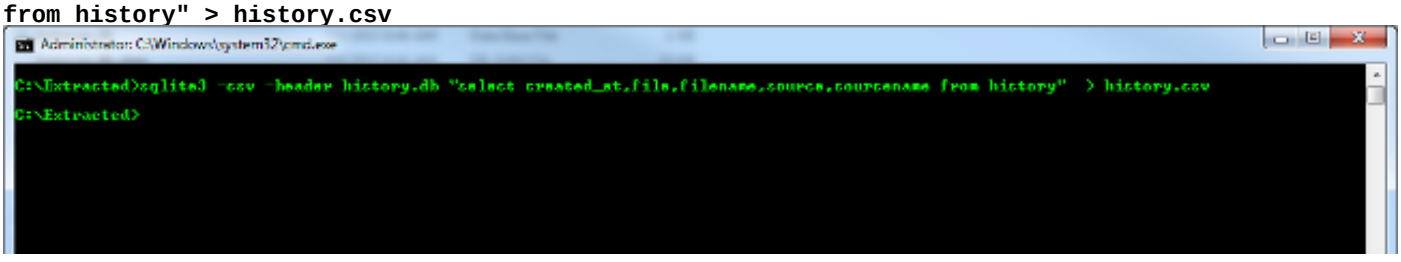
ステップ 2： 第2ステップは診断ファイルから `history.db` アクセスすることです。

`history.db` FireAMP によって検出するファイルすべてを把握する SQLite データベース ファイルです。 各行は開封、ファイル名、ファイル SHA、原始ファイルおよび出典 SHA が含まれています。 出典はファイル自体を作成したり/アクセスしたファイルです。 これは私達がアプリケーションがどのように作動し、ことをしたか見ることを可能にします。

この例では Comma Separated Value（CSV）ファイルに履歴データベースを変換するために、SQLite3 コマンドは使用されます。

- オペレーティング システムのための前コンパイルされた SQLite3 バイナリをダウンロードして下さい。
- 7zip のようなアプリケーションの FireAMP 診断パッケージを得て下さい。
- 得られた診断フォルダにナビゲート し、C_ \ \ Sourcefire \ fireAMP \ディレクトリ内の `history.db` 見つけて下さい。
- ターミナルかコマンド プロンプトの中では、ダウンロードした呼出し、このコマンドを `history.db` 与えて下さい SQLite3 バイナリを。（このコマンドは SQLite3 がオペレーティング システムのための環境変数で規定 される 位置にまたはあるかことそれを診断フォルダの内に置かれる必要があります仮定します。）

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



コマンドが正常である場合確認を見ないか、または出力します。

コマンドが失敗した場合、SQLite3 バイナリの位置を規定 したことをことを確かめて下さい。`history.db` に関して他のどのメッセージも表示される場合、それが次にサービスが開始する新しい一組のファイルを生成するようにするサービスが停止する間、影響を受けたホスト マシンからの 4 つの活動記録 ファイルをクリアする必要があるかもしれません。

ステップ 3： CSV ファイルが生成されたら優先 する スプレッドシート アプリケーションとそれを開くことができます。 Microsoft Excel のようなアプリケーションは/並べ替えフィルタリングするために与える表に CSV ファイルを変換することを可能にするかもしれません。 Excel を使用する方法に関するマイクロソフトのドキュメンテーションを参照して下さい。

使用するべきプライマリ カラムは次のとおりです:

- **ファイル名**: このフィールドはファイルが FireAMP によってスキャンされることを示します。
- **sourcename**: このフィールドはハンドル（読み書き等）をつかんだ実行可能モジュールかプロセスを示します。 このデータはファイルが信頼アプリケーションによってまたは他では処理されるかどうか判別するために使用されます。
- **created_at**: これはファイルの検出のためのイベントのタイムスタンプです。

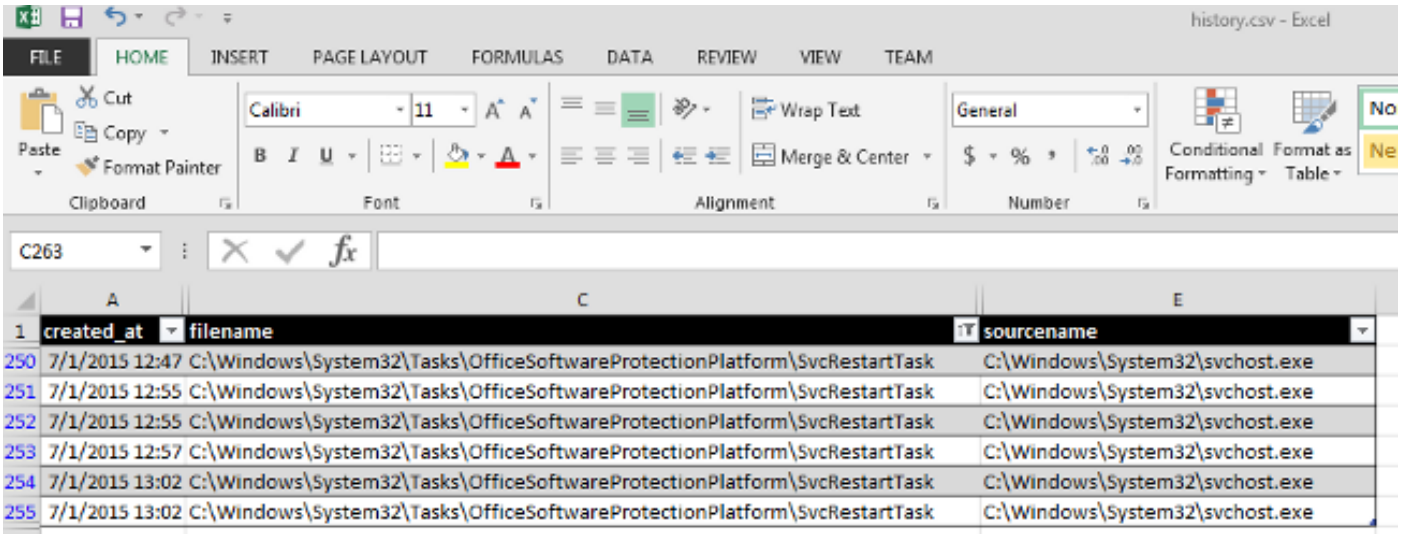
トラブルシューティング

この時点で幾つかのオプションがあります:

- ちょうどパフォーマンス上の問題に直面した場合、スキャンされたタイムスタンプ ソートしである、ほとんどの近況をできます **created_at** によって表を表示。 何が起こったか見るために検出および作業を逆方向に参照できます。
- また FireAMP によって最近影響を与えられるかもしれないアプリケーションを捜すか、または参照できます。

探したいと思う何に繰り返しスキャンされる何かです同じファイルのよう異なる SHA 値があるかもしれない。 またこれが予期された動作であるかどうか見るためにファイルタイプを検知 したいと思います。

この例では、ファイルは「オフィス」を捜されました。 結果は FireAMP がことワード「オフィス」ファイル名かパスで持たれていてスキャンしたことをファイルに示します。 また対応した ファイルを処理した出典 プロセスを表示できます。



この例では、FireAMP は Microsoft Office サービスに関するファイルをスキャンします。 これを除きたいと思う場合ここに示されているもののような簡単なパス 除外を作成する可能性があります:

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

時々、除外はあまり簡単ではないです。 時折他の工リアのこのようなアクティビティをのような

見ます、

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

たとえば特定のファイル名を用いる appdata ディレクトリにキャッシュその試験的応用があることを、言って下さい。 所定の名前と何かを除くことができます。

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

この例は臨時雇用者アプリケーションのためのキャッシュファイルを除きます。 ただしダウンロード/イメージとしてインターネット キャッシュファイルがこのディレクトリに常駐する可能性があるので、臨時雇用者フォルダを除きたいと思いません。 またテスト フォルダにアプリケーションがインターネットに同様に接続するかもしれませんディレクトリを狭くすることができましたりまたは危険にさらすためにパフォーマンスを害を与えないし、可能性としては開くことができなかった他のキャッシュファイルがありますどんなに。 ワイルドカードがこれを除くのに使用されています。

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

見るように、何でもを文字の間で説明し、ファイル名で点を打つのにワイルドカードが（*）使用されました。 この式と一致するこのワイルドカードはファイルを除きます。 これはたくさんのリスクを防ぐためにどのようにの除外を狭くすることができるか例です。

またフルパス名のためにワイルドカードを使用できます。 同じような例はここにあります;

```
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
```

ワイルドカード 除外-除外はパスおよびファイル名が両方表現することができるワイルドカード式でするることができます。 すなわち、ファイル名が一定しているなら、そしてそれ最もよいです「抑制します特定のパスに」ワイルドカードを。 従って C:\Program ファイルで常に存在 する AIM.exe なら（x86)*\AIM.EXE はあらゆるサブディレクトリを検知 します。

望ましい FireAMP 除外を見つけた後、それらをダッシュボードで設定し、テストを行うためにこの技術情報にリストされているステップに従うことができます。

バージョン 5.0+

バージョン 5.0+ では、ファイル アクティビティはもはやログイン された `history.db` ではないです スキャンされたファイルのための新しい構造およびパスは historyex.db にあります Cisco Technical Assistance Center（TAC）によってサポートされないスクリプトは、CiscoSupport コミュニティで利用できます。 Linux 環境で、スクリプトは historyex.dbto を変換 `Comma Separated Value`（CSV）ファイルできます。 それは除外のためのアクティビティを検討することを可能にします。

関連資料

- FireAMP での除外の設定と管理
- v5.0+ のファイル 走査の検討
- テクニカルサポートとドキュメント - Cisco Systems