Documentation for ExeFilter version 1.1.0

Table of Contents

1 Foreword

ExeFilter is a content analysis software which is designed to filter files and e-mails, in order to only accept controlled, static and harmless contents. The main goal is to improve protection of sensitive information systems by enforcing a strict policy based on a white list of file formats. It also provides filtering features to detect or remove all active content in files (binary executable files, scripts, macros, embedded objects, exploits, ...).

Translation of the software and this documentation from French to English is in progress. Some parts are not translated yet.

2 License

ExeFilter is released as open-source software under CeCILL v2 license:

ExeFilter is a software to filter files, e-mails or web pages, in order to remove any active content and protect sensitive systems.

Authors:

- Philippe Lagadec (PL) - philippe.lagadec(a)laposte.net

- Arnaud Kerréneur (AK) - arnaud.kerreneur(a)dga.defense.gouv.fr

- Tanguy Vinceleux (TV) - tanguy.vinceleux(a)dga.defense.gouv.fr

3 Download

Here are the required files to install and use ExeFilter.

3.1 Prerequisites

3.1.1 Operating system

ExeFilter has been initially developed on Windows. It is also compatible with other systems such as Linux and MacOSX. However some features are not available or equivalent on all systems yet.

3.1.2 Python interpreter

A recent Python interpreter is necessary (version 2.5 or newer is recommended):

- For most systems, Python is available on http://www.python.org
- For Windows, there is also an alternative version ActivePython which includes a few additional modules such as pywin32: http://www.activestate.com/Products/activepython

Note: For now ExeFilter is not compatible with the future Python version 3.0 which brings significant changes in the language.

3.1.3 Python Win32 Extensions (pywin32)

On Windows, the pywin32 module is necessary: http://sourceforge.net/projects/pywin32/

3.2 ExeFilter

The official website of the ExeFilter project is http://admisource.gouv.fr/projects/exefilter.

3.3 Additional tools

ExeFilter features may be extended by installing and configuring additional tools:

3.3.1 ClamAV Antivirus and PyClamd

ExeFilter may use the ClamAV antivirus to scan all files. For this ClamAV must be installed and configured in “daemon” mode (clamd), and then the PyClamd module must be installed:

- ClamAV: http://www.clamav.net/
- PyClamd: http://www.decalage.info/python/pyclamd (This page also provides a few instructions to configure clamd on Windows)

1.1.1 F-Prot Antivirus

F-Prot antivirus may be used to scan files, and it can also be used to improve VBA macros removal from MS Office documents. Currently ExeFilter only supports F-Prot v3 and v6 on Windows to scan files, and F-Prot v3 to remove macros.

- http://www.f-prot.com/

4 Installation

ExeFilter is provided as a Zip archive, which must simply be extracted in a directory.

If ExeFilter is to be imported as a module in other Python scripts, it is useful to store its directory in the "site-packages" folder of the Python interpreter. Here are a few typical locations for that folder:

- On Windows: c:\Python25\Lib\site-packages
- On Linux: /usr/lib/python2.5/site-packages
- On MacOSX: /Library/Python/2.5/site-packages

4.1 Default encoding

To avoid potential runtime errors due to Unicode and encodings, it may be useful to create or update a file named **sitecustomize.py** in the site-packages folder with the following lines in order to set the default encoding:

```
import sys
sys.setdefaultencoding('latin_1')
```

Note: In the current ExeFilter version, the support for Unicode filenames only works on Windows. Significant changes will be necessary to fix it on other platforms.

4.2 First use

To test ExeFilter, open a shell (on Unix) or a CMD.exe window (on Windows), and simply launch the script without any argument to display the banner and list available options:

- On Windows: `ExeFilter.py`
- On Unix: `python ExeFilter.py`

5 Use

ExeFilter may be used in two ways:

- As a script from the command line (shell)
- As a Python module imported in another Python script.

5.1 ExeFilter as a script

Launched as a script from a shell, ExeFilter analyzes and filters a group of files and/or directories and stores the result in a destination directory. Source files and/or directories are specified as arguments (separated by spaces) on the command line, and destination is set using the “-d”option:

```
ExeFilter <sources> -d <destination>
```

Example:

```
ExeFilter D:\exefilter\incoming F:\download\test.zip -d D:\exefilter\result
```

5.1.1 Logs

By default ExeFilter creates two log files in the subdirectory “log\journaux” each time it is launched:

- A security log which contains a summary of analyzed files.
- A debug log which stores more technical details (useful in case of errors).

5.1.2 Reports

By default ExeFilter creates two report files in the subdirectory “log\rapports” which may be useful for the end user to see which files were accepted, cleaned or blocked. Both reports contain the same information, one is HTML and the other is XML.

5.1.3 Archive

The current version stores a copy of each filtered file in an archive directory named “archivage”. It will be possible to disable this feature in future versions.

5.2 ExeFilter comme module Python

ExeFilter peut être employé comme module afin de l'intégrer dans un script ou une application écrits en langage Python. Il est ainsi possible d'utiliser son moteur de filtrage pour analyser tout type de protocole transportant des fichiers ou des contenus similaires: HTTP, SMTP, FTP, etc. La seule limitation actuelle est qu'ExeFilter ne peut filtrer que des fichiers stockés sur disque et non en mémoire.

Pour cela, la fonction principale est « transfert() » dans le module ExeFilter.py. Se reporter au code source du module pour le détail des paramètres à employer.

Voici un exemple simple d'utilisation, reprenant les mêmes paramètres que précédemment:

```
import ExeFilter, Politique
# On crée d'abord une politique par défaut:
pol = Politique.Politique()
# On peut lire la config depuis un fichier:
```

```
pol.lire_config('exefilter.cfg')
# liste des répertoires/fichiers à analyser:
sources = ['D:\\exefilter\\depot', 'F:\\download\\test.zip']
# répertoire destination:
dest = 'D:\\exefilter\\resultat'
# Lancement du transfert pour analyser/filtrer les fichiers:
ExeFilter.transfert(sources, dest, pol=pol)
```

6 Configuration – Administration

ExeFilter est fourni avec une configuration par défaut, ce qui permet de tester rapidement l'outil. Il est cependant possible d'adapter cette configuration au système et aux besoins.

La configuration d'ExeFilter est constituée de deux parties: les paramètres du logiciel, et la politique de filtrage.

- Paramètres: configuration générale du logiciel (chemins des répertoires pour les journaux et rapports, antivirus utilisés, etc.)
- Politique de filtrage: formats de fichiers autorisés et options pour chacun des formats. Il peut être utile de se reporter à [SSTIC03] pour décider quels formats autoriser ou non.

Ces deux parties peuvent être fournies sous la forme d'un ou deux fichiers au format « ini ».

6.1 Créer un nouveau fichier de configuration

Le script ExeFilter dispose d'une option pour créer un nouveau fichier de configuration avec les paramètres par défaut:

```
ExeFilter -n <fichier.cfg>
```

Le fichier obtenu contient à la fois les paramètres et la politique de filtrage. Il peut être utilisé tel quel ou bien séparé en deux fichiers distincts suivant les besoins. La section « [ExeFilter] » contient les paramètres, tandis que les sections « [Filtre_xxx] » contiennent les options pour chaque format de fichier.

6.2 Utiliser un fichier de configuration

Pour employer un fichier de configuration avec le script ExeFilter, utiliser les options -c et/ou -p (ces deux options ont une fonction identique mais permettent de séparer la configuration en deux fichiers si besoin):

```
ExeFilter -c <config.cfg> -p <politique.cfg> <source> -d <destination>
```

6.3 Paramètres disponibles

Le script ExeFilter dispose d'une option pour créer une page HTML listant tous les paramètres disponibles, leur description détaillée et leur valeur par défaut:

```
ExeFilter -e <fichier.html>
```

Voici la liste des paramètres disponibles:

Code Paramètre	Nom	Description	Valeur	Valeur par défaut
section [ExeFilter]				
antivirus_clamd	Utiliser l'antivirus ClamAV (serveur clamd)	Utiliser la version serveur de l'antivirus ClamAV (clamd) pour analyser les fichiers acceptes. Clamd doit tourner en tant que service sur la machine locale.	0	False
antivirus_fpcmd	Utiliser l'antivirus F-Prot 3 (fpcmd)	Utiliser la version ligne de commande de l'antivirus F-Prot 3 (fpcmd) pour analyser les fichiers acceptes. Attention cela peut degrader significativement les performances.	0	False
antivirus_fpscan	Utiliser l'antivirus F-Prot 6 (fpscan)	Utiliser la version ligne de commande de l'antivirus F-Prot 6 (fpscan) pour analyser les fichiers acceptes. Attention cela peut degrader significativement les	0	False

		performances.		
clamd_port	Port du serveur antivirus clamd	En general le serveur clamd tourne sur le port 3310.	3310	3310
clamd_serveur	Adresse IP ou nom du serveur antivirus clamd	En general le serveur clamd tourne sur la meme machine: localhost.	localhost	localhost
fpcmd_executable	Exécutable de l'antivirus F-Prot 3 (fpcmd)	Emplacement du fichier fpcmd de l'antivirus F-Prot 3	c:\Program Files\FRISK Software\ F-PROT Antivirus for Windows\fpcmd.exe	c:\Program Files\FRISK Software\ F-PROT Antivirus for Windows\fpcmd.exe
fpscan_executable	Exécutable de l'antivirus F-Prot 6 (fpscan)	Emplacement du fichier fpscan de l'antivirus F-Prot 6	c:\Program Files\FRISK Software\ F-PROT Antivirus for Windows\fpscan.exe	c:\Program Files\FRISK Software\ F-PROT Antivirus for Windows\fpscan.exe
journal_debug	Ecrire un journal technique de débogage	Le journal technique contient les évènements détaillés des transferts, pour un débogage en cas de problème.	1	True
journal_securite	Ecrire un journal sécurité dans un fichier	Le journal sécurité décrit synthétiquement les évènements concernant la sécurité des transferts.	1	True
journal_syslog	Envoyer un journal sécurité par syslog	Le journal sécurité décrit synthétiquement les évènements concernant la sécurité des transferts. Syslog permet de centraliser ces journaux par le réseau sur un serveur	0	False
port_syslog	Port syslog (numéro de port UDP)	Numéro de port UDP du serveur syslog: 514 pour un serveur syslog standard.	514	514
rep_archives	Répertoire des fichiers archivés	Répertoire où sont archivés tous les fichiers transférés	archivage\	archivage\
rep_journaux	Répertoire des fichiers journaux	Répertoire où sont stockés tous les fichiers journaux	log\journaux\	log\journaux\
rep_rapports	Répertoire des fichiers rapports	Répertoire où sont stockés tous les fichiers rapports	log\rapports\	log\rapports\
rep_temp	Répertoire des fichiers temporaires	Répertoire où sont stockés tous les fichiers temporaires	temp\	temp\
serveur_syslog	Serveur syslog (nom ou adresse IP)	Nom ou adresse IP du serveur syslog qui centralise les journaux sécurité.	localhost	localhost
taille_archives	Taille maximale des archives (en octets)	Taille maximale du répertoire où sont archivés tous les fichiers transférés	10000000000	10000000000
taille_temp	Taille maximale du répertoire temporaire (en octets)	Taille maximale du répertoire où sont stockés tous les fichiers temporaires	10000000000	10000000000
section [Filtre_AVI]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_BMP]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_Excel]				
detecter_ole_pkg	Détecter les objets OLE Package	Détecter les objets OLE Package, qui peuvent contenir des fichiers ou des commandes.	1	True
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
macros_fpcmd	Utiliser F-Prot 3 pour supprimer	Utiliser l'antivirus F-Prot 3 (fpcmd) pour supprimer toutes les macros VBA	0	False

	les macros	des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.		
macros_fpscan	Utiliser F-Prot 6 pour supprimer les macros	Utiliser l'antivirus F-Prot 6 (fpscan) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_win32	Utiliser l'API Win32 pour supprimer les macros	Utiliser les fonctions de Windows pour supprimer toutes les macros VBA des documents. Cette methode est rapide mais ne couvre que Word et Excel, et ne fonctionne que sous Windows.	1	True
supprimer_macros	Supprimer les macros	Supprimer toutes les macros VBA des documents. Voir aussi les parametres macros_xxx pour choisir la methode employee. Si aucune methode n'est active, une methode simple sera employee. Cette methode est portable et rapide, mais ne couvre que Word et Excel.	1	True
section [Filtre_GIF]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_HTML]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_JPEG]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_MP3]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_PDF]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
supprimer_embeddedfile	Supprimer les fichiers inclus	Supprimer tout fichier inclus, qui peut camoufler du code executable.	1	True
supprimer_fileattachment	Supprimer les fichiers attaches	Supprimer tout fichier attache, qui peut camoufler du code executable.	1	True
supprimer_javascript	Supprimer le code Javascript	Supprimer tout code Javascript, qui peut declencher des actions a l'insu de l'utilisateur.	1	True
section [Filtre_PNG]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_Powerpoint]				
detecter_ole_pkg	Détecter les objets OLE Package	Détecter les objets OLE Package, qui peuvent contenir des fichiers ou des commandes.	1	True
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
macros_fpcmd	Utiliser F-Prot 3 pour supprimer les macros	Utiliser l'antivirus F-Prot 3 (fpcmd) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_fpscan	Utiliser F-Prot 6 pour supprimer les macros	Utiliser l'antivirus F-Prot 6 (fpscan) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False

supprimer_macros	Supprimer les macros	Supprimer toutes les macros VBA des documents. Voir aussi les parametres macros_xxx pour choisir la methode employee. Si aucune methode n'est active, une methode simple sera employee. Cette methode est portable et rapide, mais ne couvre que Word et Excel.	1	True
section [Filtre_Project]				
detecter_ole_pkg	Détecter les objets OLE Package	Détecter les objets OLE Package, qui peuvent contenir des fichiers ou des commandes.	1	True
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
macros_fpcmd	Utiliser F-Prot 3 pour supprimer les macros	Utiliser l'antivirus F-Prot 3 (fpcmd) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_fpscan	Utiliser F-Prot 6 pour supprimer les macros	Utiliser l'antivirus F-Prot 6 (fpscan) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
supprimer_macros	Supprimer les macros	Supprimer toutes les macros VBA des documents. Voir aussi les parametres macros_xxx pour choisir la methode employee. Si aucune methode n'est active, une methode simple sera employee. Cette methode est portable et rapide, mais ne couvre que Word et Excel.	1	True
section [Filtre_RTF]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_Texte]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
section [Filtre_Visio]				
detecter_ole_pkg	Détecter les objets OLE Package	Détecter les objets OLE Package, qui peuvent contenir des fichiers ou des commandes.	1	True
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
macros_fpcmd	Utiliser F-Prot 3 pour supprimer les macros	Utiliser l'antivirus F-Prot 3 (fpcmd) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_fpscan	Utiliser F-Prot 6 pour supprimer les macros	Utiliser l'antivirus F-Prot 6 (fpscan) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
supprimer_macros	Supprimer les macros	Supprimer toutes les macros VBA des documents. Voir aussi les parametres macros_xxx pour choisir la methode employee. Si aucune methode n'est active, une methode simple sera employee. Cette methode est portable et rapide, mais ne couvre que Word et Excel.	1	True
section [Filtre_WAV]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True

section [Filtre_Word]				
detecter_ole_pkg	Détecter les objets OLE Package	Détecter les objets OLE Package, qui peuvent contenir des fichiers ou des commandes.	1	True
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True
macros_fpcmd	Utiliser F-Prot 3 pour supprimer les macros	Utiliser l'antivirus F-Prot 3 (fpcmd) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_fpscan	Utiliser F-Prot 6 pour supprimer les macros	Utiliser l'antivirus F-Prot 6 (fpscan) pour supprimer toutes les macros VBA des documents. Cette methode est lente mais fiable pour Word, Excel et Powerpoint.	0	False
macros_win32	Utiliser l'API Win32 pour supprimer les macros	Utiliser les fonctions de Windows pour supprimer toutes les macros VBA des documents. Cette methode est rapide mais ne couvre que Word et Excel, et ne fonctionne que sous Windows.	1	True
supprimer_macros	Supprimer les macros	Supprimer toutes les macros VBA des documents. Voir aussi les parametres macros_xxx pour choisir la methode employee. Si aucune methode n'est active, une methode simple sera employee. Cette methode est portable et rapide, mais ne couvre que Word et Excel.	1	True
section [Filtre_Zip]				
format_autorise	Format autorisé	indique si ce format est autorisé ou non par la politique de filtrage	1	True

7 Contribuer au projet ExeFilter

ExeFilter est un logiciel libre, il est donc très important de contribuer au projet pour qu'il puisse progresser. Il existe de nombreuses possibilités pour apporter de l'aide.

7.1 Contact

Dans tous les cas, voici les adresses à utiliser pour contacter l'équipe du projet:

- Philippe Lagadec: philippe.lagadec(a)laposte.net
- Arnaud Kerréneur: arnaud.kerreneur(a)dga.defense.gouv.fr

7.2 Signaler des erreurs

Si vous détectez une anomalie de fonctionnement, une incompatibilité ou bien un fichier qui est bloqué ou accepté à tort, merci de nous transmettre tous les détails nécessaires.

Si possible, voici les informations qui sont utiles pour comprendre le problème:

- Une description détaillée des circonstances (mode d'utilisation, type de contenu analysé, système d'exploitation, versions de Python et d'ExeFilter installées, etc.)
- Des échantillons de fichiers permettant de reproduire le problème
- Le journal debug correspondant, si possible en ayant lancé ExeFilter avec l'option « -v ».

7.3 Signaler une vulnérabilité

Comme pour tout logiciel de sécurité, la détection d'une vulnérabilité est primordiale. Dans ce cas, merci de contacter rapidement l'équipe projet avant toute diffusion publique de l'information. Il est préférable de fournir un correctif de sécurité aux utilisateurs avant de publier toute information sur la vulnérabilité.

Une liste de diffusion sera prochainement mise en place pour que les utilisateurs puissent être informés rapidement de chaque nouvelle version et de la diffusion de correctifs de sécurité.

7.4 Tester différents environnements

L'équipe projet ne peut pas tester ExeFilter dans toutes les configurations possibles sur divers systèmes d'exploitation. Merci de nous signaler tout test réussi ou non ainsi que la configuration employée.

Voici pour l'instant les plate-formes testées:

- Windows XP SP2 avec Python 2.5
- Linux Fedora core 8 avec Python 2.5.1
- MacOSX 10.3.9 avec Python 2.5

7.5 Créer de nouveaux filtres

Il est possible de créer de nouveaux filtres pour prendre en charge des formats de fichiers supplémentaires. Si vous souhaitez ajouter un format ou améliorer la prise en charge d'un format existant, la première chose à faire est de contacter l'équipe projet pour savoir s'il n'y a pas déjà un développement en cours pour ce format.

Pour créer un nouveau filtre, voici un résumé des actions à effectuer:

1. identifier s'il s'agit d'un filtre simple (qui accepte ou bloque sans nettoyer) ou d'un filtre complexe (qui peut modifier les fichiers pour les nettoyer).
2. S'il s'agit d'un filtre simple, prendre pour modèle un des filtres suivants: GIF, JPEG, BMP, Texte.
3. S'il s'agit d'un filtre complexe: PDF, RTF, Office.
4. Le fichier doit être un module Python commençant par « Filtre_ », situé dans le sous-répertoire « Filtres » d'ExeFilter.
5. Il doit contenir une classe dont le nom commence par « Filtre_ », qui hérite de la classe « Filtre.Filtre ».
6. Cette classe doit posséder un attribut « extensions » contenant la liste des extensions autorisées pour ce format, en minuscules et incluant un point.
7. Elle doit fournir une méthode « reconnait_format » qui retourne True si la structure interne du fichier correspond au format attendu.
8. Elle doit enfin fournir une méthode « nettoyer » chargée d'analyser le format en profondeur (recherche de contenu actif si applicable). Cette méthode doit retourner un objet Resultat en fonction de l'analyse. Elle peut également modifier la copie temporaire du fichier en cas de nettoyage.

Note: une documentation détaillée des différents modules et classes est disponible au format HTML dans le sous-répertoire « doc ».

7.6 Participer au développement

Il est également possible de participer au développement pour améliorer diverses fonctionnalités ou intégrer ExeFilter dans d'autres applications (proxy HTTP, serveur de messagerie, etc.). Contactez l'équipe projet pour savoir quelles sont les développements déjà prévus et les besoins.

7.7 Participer à la documentation

Comme dans tout projet, la documentation est une tâche très importante et difficile. Tout(e) volontaire est le(la) bienvenu(e).

8 References

- [SSTIC03] Formats de fichiers et code malveillant, P. Lagadec, SSTIC03, http://actes.sstic.org/SSTIC03/Formats_de_fichiers/
- [SSTIC04] Filtrage de messagerie et analyse de contenu, P. Lagadec, SSTIC04, http://actes.sstic.org/SSTIC04/Filtrage_messagerie/
- [SSTIC06] Diode réseau et ExeFilter, P. Lagadec, SSTIC06, http://actes.sstic.org/SSTIC06/Diode_ExeFilter/

9 Changelog

date	version	author	modifications
2008-03-03	1	P. Lagadec	Initial version
2008-03-27	2	P. Lagadec	English translation