Documentation pour ExeFilter version 1.1.0

Sommaire

1 A propos

ExeFilter est un logiciel d'analyse de contenu conçu pour filtrer des fichiers ou des courriels, afin de ne laisser passer que des contenus maîtrisés, statiques et inoffensifs. L'objectif principal est d'améliorer la protection de systèmes d'information particulièrement sensibles, en réduisant le risque de laisser entrer du code malveillant sous toutes ses formes (exécutables binaires, scripts, macros, objets inclus, exploits, ...).

ExeFilter permet d'appliquer une politique de filtrage stricte, pour n’accepter que certains formats de fichiers connus et maîtrisés. La correspondance entre le nom des fichiers (en particulier leur extension) et leur structure interne est vérifiée. Tout contenu actif comme un fichier exécutable, une

macro ou un script peut être bloqué ou nettoyé (cf. [SSTIC03] et [SSTIC04]). L'analyse est récursive si des formats conteneurs sont détectés (archives ZIP, TAR, e-mails, …).

Ce module est conçu de façon générique, afin de pouvoir l'employer pour diverses applications: filtrage de supports amovibles, protocoles HTTP, FTP, SMTP, …

Aujourd'hui des filtres ont été créés pour analyser les formats les plus usuels : TXT, HTML, PDF, DOC, XLS, PPT, RTF, JPG, GIF, MP3, AVI, ZIP, …

ExeFilter est développé intégralement en langage Python, ce qui permet d'assurer une très bonne portabilité et la possibilité d'étendre facilement ses fonctionnalités et les formats pris en charge.

Ce projet est développé par le CELAR depuis 2004, et diffusé comme logiciel libre sous licence CeCILL v2 depuis mars 2008. Cf. [SSTIC06] pour une présentation plus détaillée.

Cette version libre est actuellement en phase de développement. Certaines fonctions ne sont pas encore parfaitement finalisées et testées. Il est donc déconseillé de l'employer sur un système en production pour l'instant.

2 Licence

Le logiciel ExeFilter est diffusé en tant que logiciel libre sous licence CeCILL v2 :

ExeFilter est un logiciel qui permet de filtrer des fichiers, courriels ou pages web, afin de supprimer tout code exécutable et tout contenu potentiellement dangereux en terme de sécurité informatique.

Auteurs:

- 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 Téléchargement

Voici les différents fichiers nécessaires pour installer et utiliser ExeFilter.

3.1 Pré-requis

3.1.1 Système d'exploitation

ExeFilter est initialement développé pour Windows. Il est également compatible avec d'autres systèmes comme Linux et MacOSX, cependant quelques fonctionnalités ne sont pas encore disponibles ou équivalentes dans tous les cas.

3.1.2 Interpréteur Python

Tout d'abord, un interpréteur Python suffisamment récent (version 2.5 ou supérieure recommandée) est nécessaire:

- Pour la plupart des systèmes, Python est disponible sur le site http://www.python.org
- Pour Windows, il existe aussi une version alternative ActivePython qui inclut quelques modules complémentaires comme pywin32: http://www.activestate.com/Products/activepython

Note: pour l'instant ExeFilter n'est pas compatible avec la future version Python 3.0 qui induit des modifications significatives dans le langage.

3.1.3 Extensions Win32 pour Python (pywin32)

Sous Windows, le module pywin32 est nécessaire: http://sourceforge.net/projects/pywin32/

3.1.4 module Path

Le module path est employé pour simplifier la gestion des fichiers et répertoires. Une version est fournie avec ExeFilter, l'original se trouve à l'adresse
http://www.jorendorff.com/articles/python/path/

3.2 ExeFilter

Le site officiel du projet ExeFilter est http://admisource.gouv.fr/projects/exefilter.

3.3 Outils complémentaires

Il est possible d'étendre certaines fonctionnalités d'ExeFilter en installant des outils complémentaires:

3.3.1 Antivirus ClamAV et PyClamd

ExeFilter peut exploiter l'antivirus ClamAV afin d'analyser chaque fichier. Pour cela il faut tout d'abord installer et configurer ClamAV en mode « daemon » (clamd), puis installer le module PyClamd:

- ClamAV: http://www.clamav.net/
- PyClamd: http://www.decalage.info/python/pyclamd (cette page inclut également quelques instructions pour configurer clamd sous Windows)

3.3.2 Antivirus F-Prot

L'antivirus F-Prot peut être employé pour analyser les fichiers, et il peut aussi être utilisé pour améliorer significativement le nettoyage des macros dans les documents Office. Actuellement ExeFilter prend en charge les versions 3 et 6 de F-Prot comme antivirus, et uniquement la version 3 pour le nettoyage de macros. Seule la version Windows est supportée pour l'instant.

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

4 Installation

ExeFilter est pour l'instant fourni simplement sous la forme d'une archive Zip. Pour l'installer il suffit de décompresser cette archive dans le répertoire voulu.

S'il est prévu d'employer ExeFilter en tant que module importé dans un script Python, il est utile de placer le répertoire ExeFilter dans le dossier site-packages de l'interpréteur Python. Voici quelques emplacements typiques pour ce dossier:

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

4.1 Default encoding

Pour éviter certaines erreurs d'exécution dues à la prise en charge d'Unicode, il est utile de créer ou compléter un fichier **sitecustomize.py** dans le dossier site-packages de l'interpréteur Python avec les lignes suivantes:

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

Note: Dans la version actuelle d'ExeFilter, le support des noms de fichiers Unicode ne fonctionne correctement que sous Windows. Des modifications importantes sont prévues pour améliorer la portabilité sur les autres systèmes.

4.2 Première utilisation

Pour tester le bon fonctionnement d'ExeFilter, ouvrir un shell (sous Unix) ou une fenêtre CMD.exe (sous Windows) et lancer simplement le script sans option pour afficher la bannière et les options disponibles:

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

Ensuite, pour vérifier que le filtrage fonctionne correctement, une série de fichiers est fournie dans un répertoire TESTS. La commande suivante permet de recopier ces fichiers dans le répertoire Resultats en appliquant la politique de filtrage par défaut:

```
ExeFilter.py TESTS -d Resultats
```

La liste des fichiers analysés peut ensuite être consultée dans un rapport HTML situé dans le répertoire log/rapports.

En cas d'anomalie, le répertoire log/journaux contient des journaux plus détaillés. Il peut également être utile de refaire le même test en mode “debug” grâce à l'option -v, et vérifier ensuite le journal:

```
ExeFilter.py TESTS -d Resultats -v
```

5 Utilisation

ExeFilter peut être utilisé de deux façons:

- Comme script depuis la ligne de commande (shell)
- Comme module Python importé dans un autre script.

5.1 ExeFilter comme script

Lancé comme script depuis un shell, ExeFilter permet d'analyser et filtrer un ensemble de fichiers et/ou de répertoires, et de recopier le résultat dans un répertoire destination. Les fichiers et/ou répertoires sources sont simplement spécifiés comme arguments sur la ligne de commande en les séparant par des espaces, et la destination est indiquée par l'option « -d » :

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

Exemple:

```
ExeFilter D:\exefilter\depot F:\download\test.zip -d D:\exefilter\resultat
```

5.1.1 Journaux

Par défaut, ExeFilter crée deux fichiers journaux dans le sous-répertoire « log\journaux » à chaque exécution:

- Un journal sécurité qui contient un résumé des fichiers filtrés.
- Un journal technique de débogage qui fournit de nombreux détails sur le filtrage en cas d'anomalie.

Il est possible de changer leur emplacement ou de les désactiver en modifiant les paramètres du fichier de configuration. Il est aussi possible de journaliser vers un serveur syslog. (cf. chapitre configuration)

5.1.2 Rapports

Par défaut, ExeFilter crée deux fichiers rapports dans le sous-répertoire « log\rapports » à chaque exécution:

- Un rapport au format HTML qui contient un résumé des fichiers filtrés destiné à l'utilisateur qui a demandé le transfert.
- Un rapport au format XML contenant les mêmes informations, destiné à être visualisé dans une interface graphique.

Il est possible de changer leur emplacement ou de les désactiver en modifiant les paramètres du fichier de configuration. (cf. chapitre configuration)

5.1.3 Archivage

La version actuelle d'ExeFilter archive une copie de chaque fichier analysé dans un répertoire « archivage », dont la taille totale est limitée. Dans une future version il sera possible de désactiver cette fonctionnalité.

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 Références

- [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 Historique du document

date	version	auteur	modifications
2008-03-03	1	P. Lagadec	Création du document