Documentation for ExeFilter version 1.1.3

1 Foreword

ExeFilter is a content analysis tool and framework 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, ...).

Table of Contents

2 License

ExeFilter is released as open-source software under the 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.

Copyright DGA/CELAR 2004-2008

Copyright NATO/NC3A 2008-2010 (PL changes after v1.1.0)

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

This software is governed by the CeCILL license under French law and abiding by the rules of distribution of free software. You can use, modify and/ or redistribute the software under the terms of the CeCILL license as circulated by CEA, CNRS and INRIA at the following URL "http://www.cecill.info". A copy of this licence is also provided in the attached files Licence_CeCILL_V2-fr.html et Licence_CeCILL_V2-en.html.

As a counterpart to the access to the source code and rights to copy, modify and redistribute granted by the license, users are provided only with a limited warranty and the software's author, the holder of the economic rights, and the successive licensors have only limited liability.

In this respect, the user's attention is drawn to the risks associated with loading, using, modifying and/or developing or reproducing the software by the user in light of its specific status of free software, that may mean that it is complicated to manipulate, and that also therefore means that it is reserved for developers and experienced professionals having in-depth computer knowledge. Users are therefore encouraged to load and test the software's suitability as regards their requirements in conditions enabling the security of their systems and/or data to be ensured and, more generally, to use and operate it in the same conditions as regards security.

The fact that you are presently reading this means that you have had knowledge of the CeCILL license and that you accept its terms.

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, Solaris 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: **Python version 2.6 or 2.5 is recommended**. Python version 3.x is not supported yet, because it brings significant changes in the language.

- 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

3.1.3 Python Win32 Extensions (pywin32)

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

3.2 *ExeFilter*

The official website of the ExeFilter project is http://www.decalage.info/exefilter.

3.3 *Additional tools*

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

3.3.1 Ruby

The Ruby interpreter is required when using some optional features such as the Origami engine in the PDF filter. **Ruby 1.8.x** is recommended: http://www.ruby-lang.org/en/downloads/

3.3.2 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)

3.3.3 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

Important note: as of version 1.1.3, using "setup.py install" to install ExeFilter in the site-packages directory is not yet supported.

4.1 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`**

4.2 Unicode support - Default encoding issues

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')
```

As of version 1.1.2, ExeFilter uses a known "hack" to change the default encoding at runtime, so that you do not have to create the sitecustomize.py file.

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

5 Usage

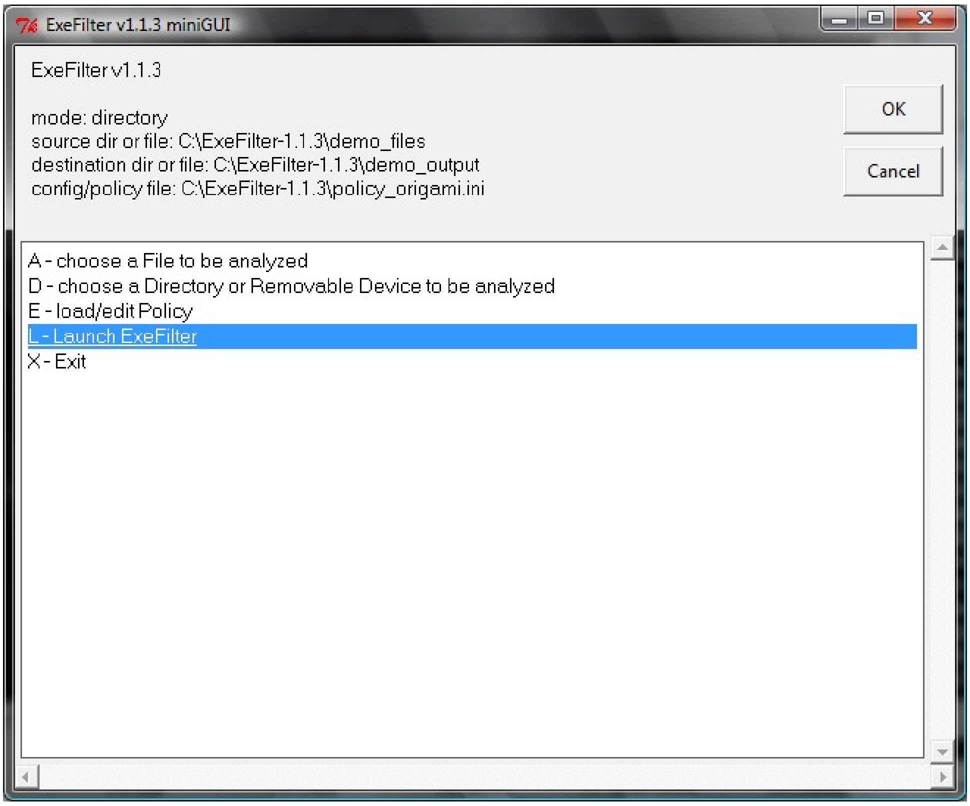
ExeFilter may be used in several ways:

- As a tool with a graphical interface.
- As a tool from the command line (shell).
- As a Python package imported into another Python application.
- As a custom filter in Clearswift MailSweeper, an e-mail security software.

5.1 ExeFilter mini GUI

Since version 1.1.3, ExeFilter is provided with a minimal graphical user interface. It is based on EasyGUI/TkInter so that is does not require the installation of additional GUI libraries such as wxPython or wxGTK. The look and feel is minimal, however all the main features of ExeFilter are available.

Launch **exefilter_minigui.py** either by double-clicking on the file or from the command-line. From the main menu it is possible to choose either a single file to be analysed or a folder (such as a removable device). For a quick test, choose the "demo_files" folder as source, and "demo_output" as destination.



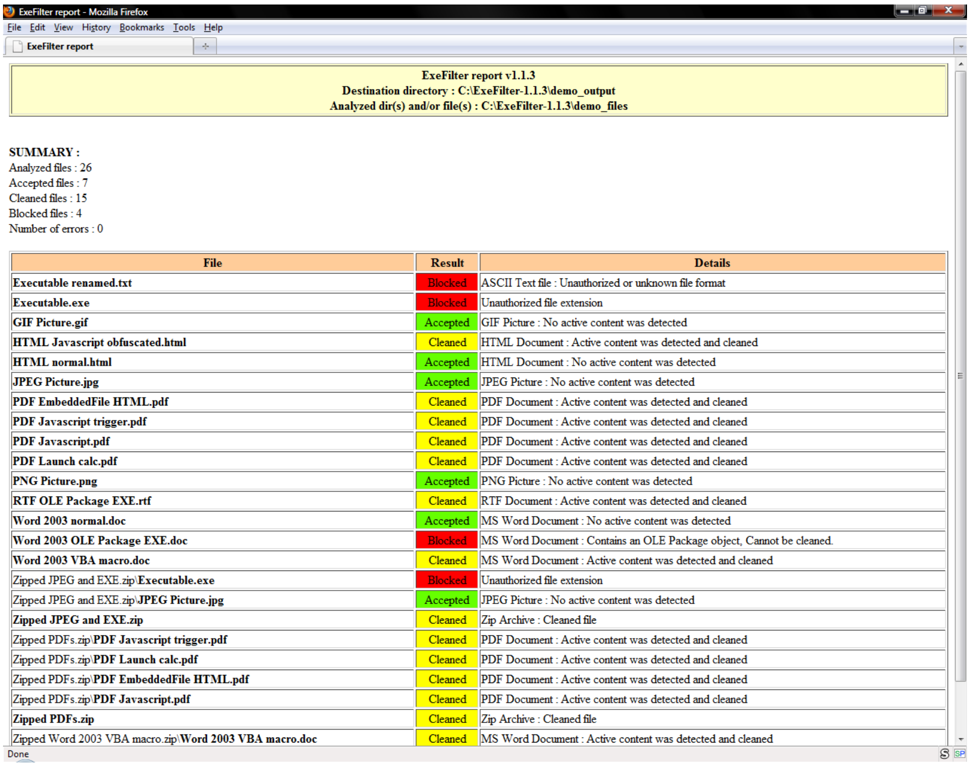
ExeFilter v1.1.3

mode: directory
source dir or file: C:\ExeFilter-1.1.3\demo_files
destination dir or file: C:\ExeFilter-1.1.3\demo_output
config/policy file: C:\ExeFilter-1.1.3\policy_origami.ini

ExeFilter v1.1.3 miniGUI
OK
Cancel
A - choose a File to be analyzed
D - choose a Directory or Removable Device to be analyzed
E - load/edit Policy
L - Launch ExeFilter
X - Exit

Then choose "Launch ExeFilter" to scan and sanitize the selected file or folder.

When the analysis is finished, the HTML report is displayed in the default browser, showing the result for each file:

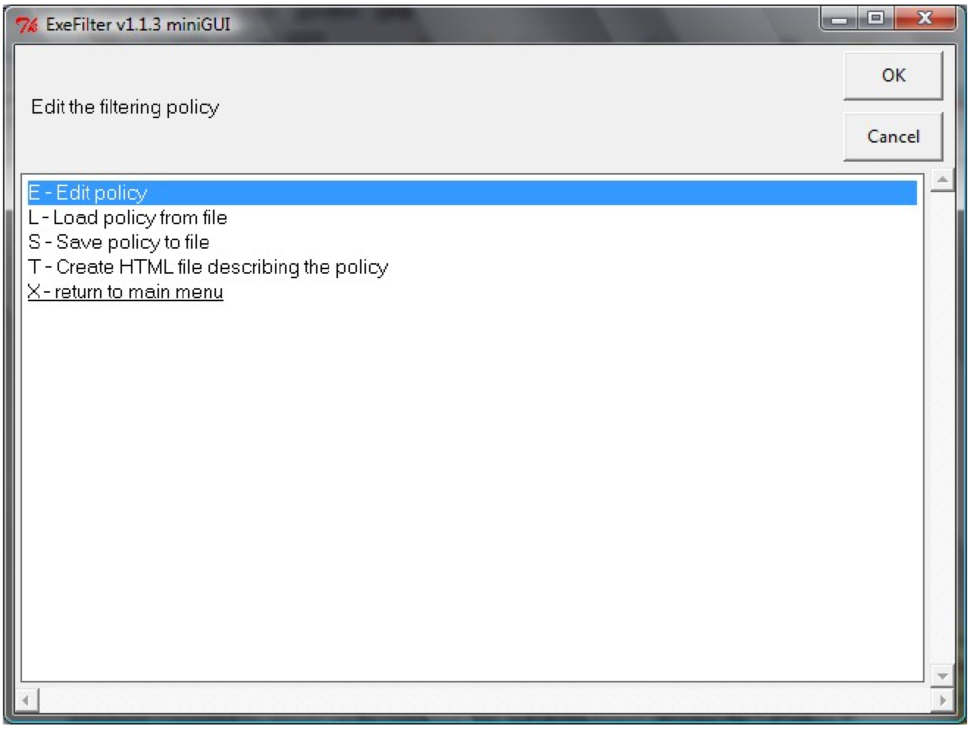

ExeFilter report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ExeFilter report
Done

ExeFilter report v1.1.3
Destination directory : C:\ExeFilter-1.1.3\demo_output
Analyzed dir(s) and/or file(s) : C:\ExeFilter-1.1.3\demo_files

SUMMARY :
Analyzed files : 26
Accepted files : 7
Cleaned files : 15
Blocked files : 4
Number of errors : 0

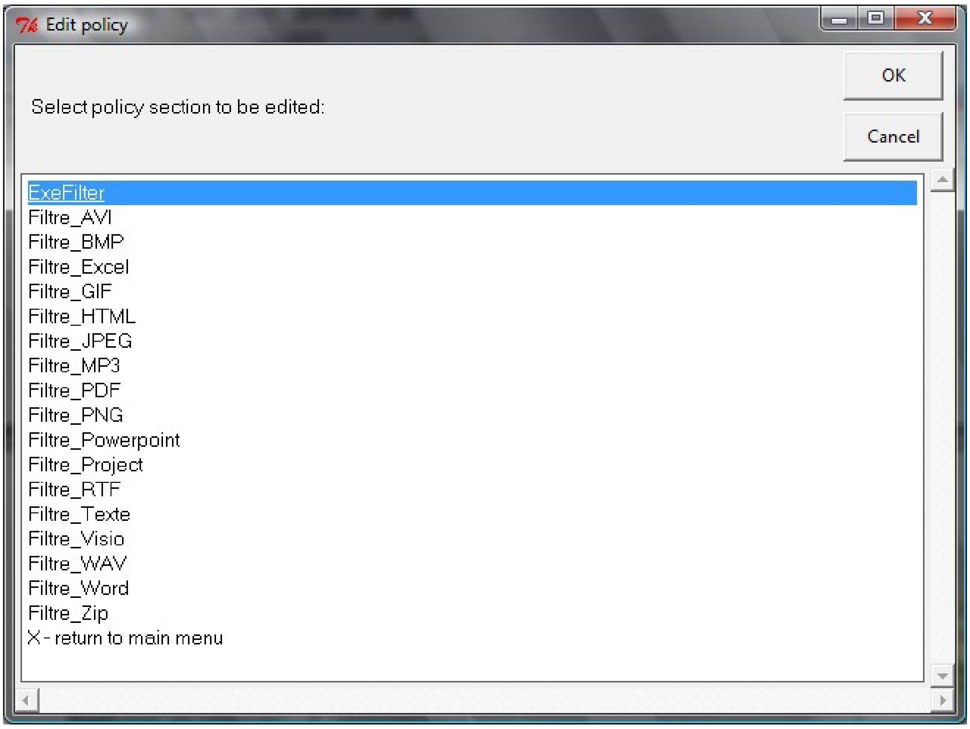
File	Result	Details
Executable renamed.txt	Blocked	ASCII Text file : Unauthorized or unknown file format
Executable.exe	Blocked	Unauthorized file extension
GIF Picture.gif	Accepted	GIF Picture : No active content was detected
HTML Javascript obfuscated.html	Cleaned	HTML Document : Active content was detected and cleaned
HTML normal.html	Accepted	HTML Document : No active content was detected
JPEG Picture.jpg	Accepted	JPEG Picture : No active content was detected
PDF EmbeddedFile HTML.pdf	Cleaned	PDF Document : Active content was detected and cleaned
PDF Javascript trigger.pdf	Cleaned	PDF Document : Active content was detected and cleaned
PDF Javascript.pdf	Cleaned	PDF Document : Active content was detected and cleaned
PDF Launch calc.pdf	Cleaned	PDF Document : Active content was detected and cleaned
PNG Picture.png	Accepted	PNG Picture : No active content was detected
RTF OLE Package EXE.rtf	Cleaned	RTF Document : Active content was detected and cleaned
Word 2003 normal.doc	Accepted	MS Word Document : No active content was detected
Word 2003 OLE Package EXE.doc	Blocked	MS Word Document : Contains an OLE Package object, Cannot be cleaned.
Word 2003 VBA macro.doc	Cleaned	MS Word Document : Active content was detected and cleaned
Zipped JPEG and EXE.zip**Executable.exe**	Blocked	Unauthorized file extension
Zipped JPEG and EXE.zip**JPEG Picture.jpg**	Accepted	JPEG Picture : No active content was detected
Zipped JPEG and EXE.zip	Cleaned	Zip Archive : Cleaned file
Zipped PDFs.zip**PDF Javascript trigger.pdf**	Cleaned	PDF Document : Active content was detected and cleaned
Zipped PDFs.zip**PDF Launch calc.pdf**	Cleaned	PDF Document : Active content was detected and cleaned
Zipped PDFs.zip**PDF EmbeddedFile HTML.pdf**	Cleaned	PDF Document : Active content was detected and cleaned
Zipped PDFs.zip**PDF Javascript.pdf**	Cleaned	PDF Document : Active content was detected and cleaned
Zipped PDFs.zip	Cleaned	Zip Archive : Cleaned file
Zipped Word 2003 VBA macro.zip**Word 2003 VBA macro.doc**	Cleaned	MS Word Document : Active content was detected and cleaned

It is also possible to load or to edit the policy to set parameters for ExeFilter and all the format filters:



Edit the filtering policy

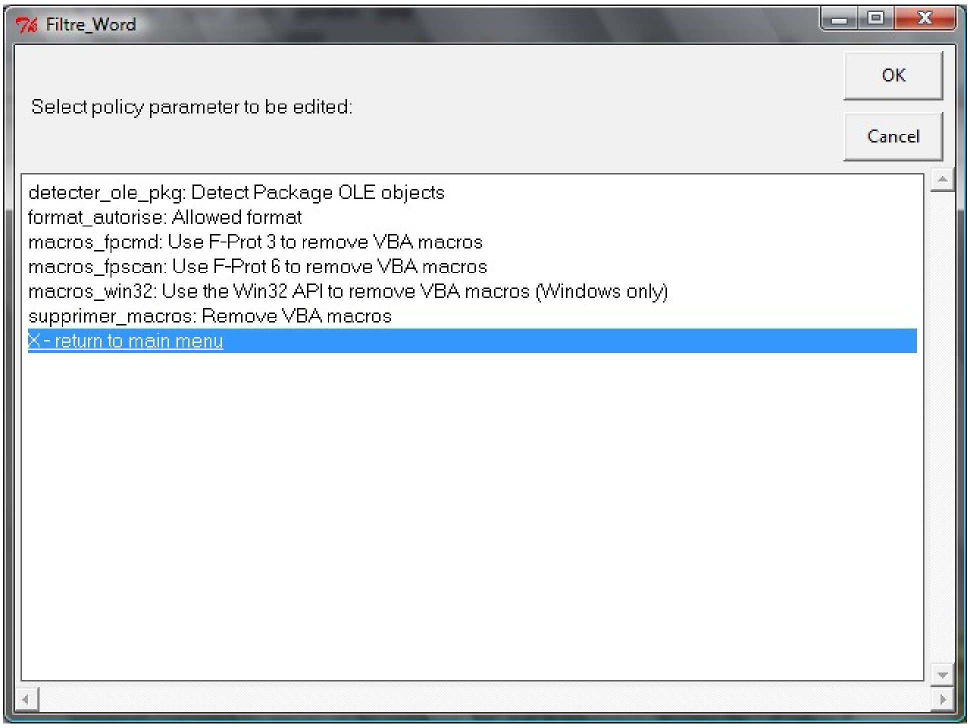
When editing the policy, choose a section to edit it. The ExeFilter section contains the main parameters, while each filter section provides parameters for a specific file format:



Select policy section to be edited:

ExeFilter
Filtre_AVI
Filtre_BMP
Filtre_Excel
Filtre_GIF
Filtre_HTML
Filtre_JPEG
Filtre_MP3
Filtre_PDF
Filtre_PNG
Filtre_Powerpoint
Filtre_Project
Filtre_RTF
Filtre_Texte
Filtre_Visio
Filtre_WAV
Filtre_Word
Filtre_Zip
X - return to main menu

For example the section "Filtre_Word" contains parameters to control how MS Word documents are sanitized:



Select policy parameter to be edited:

detecter_ole_pkg: Detect Package OLE objects
format_autorise: Allowed format
macros_fpcmd: Use F-Prot 3 to remove VBA macros
macros_fpscan: Use F-Prot 6 to remove VBA macros
macros_win32: Use the Win32 API to remove VBA macros (Windows only)
supprimer_macros: Remove VBA macros
X - return to main menu

When the policy is modified, you may then save it to a configuration file, and export it to HTML.

5.2 Using ExeFilter as a command-line tool

Launched as a script from a shell, ExeFilter can scan and sanitize a group of files and/or directories and store the result in a destination directory. Source files and/or directories are specified as arguments (separated by spaces) on the command line, and the destination directory is set using the

“-d”option:

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

For example, in order to analyze all files from a CDROM or a USB stick on drive D: (on Windows) and to copy a sanitized version in the directory C:\import, use the following command:

```
ExeFilter.py D:\ -d C:\import
```

Here is another example with several sources:

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

5.2.1 A quick demo with sample files

ExeFilter is provided with a few sample files located in the demo_files folder.

1. Open each file in the **demo_files** folder, to look at active content (javascript, macros, embedded files, etc). Note: Some samples only work on Windows.
2. On Windows: simply run **DEMO.bat**, or type: **ExeFilter.py demo_files -d demo_output**
3. On Unix/Linux/MacOSX: **python ExeFilter.py demo_files -d demo_output**
4. Then open each file in **demo_output**, and compare results.

5.2.2 Analysing a single file

Since version 1.1.2, it is possible to analyse a single file, and to provide an output filename using the “-o” option:

```
ExeFilter.py <source file> -o <output file>
```

The output file may be the same as the source file: it will be cleaned in place.

5.2.3 Exit code

When finished, ExeFilter returns an exit code (errorlevel) according to the overall result:

- 0: all analysed files are clean.
- 1: all analysed files were blocked.
- 2: some analysed files were cleaned or blocked.
- 3: an unexpected error happened during the analysis.

This should help the integration of ExeFilter into gateways and filtering products.

5.2.4 Forcing the file extension

Since version 1.1.3, it is possible to override the format detection by forcing the file extension with the “-f” option. This may be useful in cases when the file has been renamed, such as when using Mailsweeper as described in the next section. This option can only be used in single file mode with the “-o” option. For example, here is how to force the file extension to “.pdf”:

```
ExeFilter.py -f pdf file0001.tmp -o file0001.out
```

5.2.5 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 analysed files.

- A debug log which stores more technical details (useful in case of errors).

5.2.6 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.

The HTML report is automatically opened in the default web browser after analysis. This action is optional and may be disabled using the batch mode option.

5.2.7 Batch mode

When ExeFilter is used as filtering tool inside another application such as an e-mail gateway, the batch mode option (-b) must be used to avoid displaying the HTML report after each analysis:

```
ExeFilter.py -b <source file> -o <output file>
```

5.2.8 Archive

ExeFilter may store a copy of each filtered file in an archive directory named “archivage”. As of version 1.1.2 this option is disabled by default, and may be enabled in the configuration file.

5.3 Using ExeFilter into Python applications

ExeFilter may be used as a Python package into other applications. It is then possible to use its filtering engine to analyse any protocol involving files or similar content, such as HTTP, SMTP, POP3 or FTP. The current limitation is that ExeFilter can only analyse files stored on disk and not directly in memory yet.

To use ExeFilter as a package, the main function is “transfert()” in the module ExeFilter.py. See the source code for a detailed description of all its parameters.

Here is a minimal script which sanitizes the provided demo files as shown in the previous paragraphs:

```
# import the necessary modules:
import ExeFilter


# call transfert() to analyse and sanitize source dir according to the default
policy:
# (note that source is a list, while destination is a single string)
ExeFilter.transfert(['demo_files'], 'demo_output')
```

Here is another sample script showing how to call ExeFilter with several sources and a custom policy described in a configuration file:

```
# import the necessary modules:
import ExeFilter, Politique


# First, create a default policy object:
pol = Politique.Politique()
# The policy may then be read from a config file (optional):
```

```
pol.lire_config('exefilter.cfg')

# list of directories and files to be analysed:
sources = ['D:\\exefilter\\depot', 'F:\\download\\test.zip']

# destination directory:
dest = 'D:\\exefilter\\result'

# call transfert() to analyze and sanitize source files according to policy:
ExeFilter.transfert(sources, dest, pol=pol)
```

5.4 Using ExeFilter in Clearswift MailSweeper

Warning: this feature is still EXPERIMENTAL, test it carefully before any operational use.

Clearswift Mailsweeper (or MIMEsweeper for SMTP) is a software running on Windows, which purpose is to filter incoming and outgoing e-mails in order to protect company networks. It is possible to create custom filters by providing an executable file that returns specific output codes according to the scan result. Such a filter may be applied to the whole e-mail, to attachments or to specific content types.

Since version 1.1.3, ExeFilter may be used as a custom filter in Mailsweeper. An issue is that when Mailsweeper calls a custom filter to scan an attachment, it uses a temporary file with a random name, and the custom filter has no mean to check the actual extension of the attachment filename. Because ExeFilter relies on the file extension to choose which filter(s) to apply, it is necessary to force that extension, based on the file type detected by Mailsweeper.

For example, here is how to setup Mailsweeper to call ExeFilter to scan and sanitize PDF attachments:

1. Create an Executable scenario
2. The scenario should apply to the content type Document/PDF
3. It should launch:

   ```
   python.exe ExeFilter.py -b -f pdf  %FILENAME% -o %FILENAME%
   ```

4. The returned error code should be taken into account as follows:
   - 0 = the file is clean
   - 1 = the file should be blocked (suspicious content/format)
   - 2 = the file has been cleaned successfully (active content was sanitized)
   - 3 = an error occurred

The same principle can be used to create custom filters for other formats such as MS Word, HTML, etc. Each time the “-f” option must be used to force the file extension corresponding to the content type chosen for the scenario.

Important note: in this case, the filter relies on the file format detection performed by Mailsweeper and not on the one from ExeFilter. Because Mailsweeper only checks the content of the file and not the file extension, format detection may not be 100% accurate.

6 Configuration and Policy

ExeFilter is provided with a default configuration which makes it possible to quickly test the tool. However, it is possible (and recommended) to adapt that configuration to specific needs.

ExeFilter's configuration is made of two parts: global parameters for the software, and the filtering policy.

- **Parameters**: general configuration for the software (paths for reports and logs, antivirus engines, etc)
- **Policy**: allowed file formats, and specific options for each format.

These two parts may be provided in a single configuration file (using the standard INI format), or in two separate files.

6.1 How to create a new configuration file

ExeFilter provides a command-line option "-n" to create a new configuration file with all available parameters and their default values:

```
ExeFilter.py -n <default_config.cfg>
```

The created file contains both global parameters and the filtering policy. Section "[ExeFilter]" contains global parameters, while each section "[Filtre_xxx]" contains specific options for the corresponding file format (which defines the filtering policy).

This file may be used as is, or split into two separate files.

6.2 How to use a configuration file

The option "-c" may be used to specify a configuration file when using ExeFilter as a command-line tool. The option "-p" may be used in addition to specify a second configuration file for the policy. (In practice these two options are the same, they are only provided to allow the separation between parameters and policy.)

Usage:

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

Here is an example:

```
ExeFilter.py -c local_config.ini -p policy_origami.ini demo_files -d demo_out
```

6.3 Available parameters

The option “-e” may be used to create a HTML file describing all available parameters and their default values:

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

Here is the current list of parameters:

Parameter	Name	Description	Value	Default value
section [ExeFilter]				
antivirus_clamd	Use ClamAV antivirus (clamd daemon)	Use the daemon version of the ClamAV antivirus (clamd) to analyze all files after content filtering. For this, clamd must run as a service on the local host.	0	False
antivirus_fpcmd	Use the F-Prot 3 antivirus (fpcmd)	Use the command-line version of the F-Prot 3 antivirus (fpcmd) to scan all files. Warning: this may affect performance significantly.	0	False
antivirus_fpscan	Use the F-Prot 6 antivirus (fpscan)	Use the command-line version of the F-Prot 6 antivirus (fpscan) to scan all files. Warning: this may affect performance significantly.	0	False
archive_after	Archive all files after filtering	To store a copy of each filtered file in an archive directory	0	False
clamd_port	Port of the clamd server	Usually the clamd server listens on port 3310	3310	3310
clamd_serveur	Hostname or IP address of the clamd server	Usually the clamd server runs on the same machine: localhost.	localhost	localhost
fpcmd_executable	Path of the F-Prot 3 executable (fpcmd)	Absolute path of the F-Prot 3 executable (fpcmd / fpcmd.exe)	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	Path of the F-Prot 6 executable (fpscan)	Absolute path of the F-Prot 6 executable (fpscan / fpscan.exe)	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	Write a debug log file	The debug log file contains very detailed technical events about content analysis, for troubleshooting in case of unexpected errors.	1	True
journal_securite	Write a security log file	The security log file contains all main security events which happen during content analysis.	1	True
journal_syslog	Send security events to a syslog server	The security log file contains all main security events which happen during content analysis. This option sends the security log events to a central syslog server.	0	False
port_syslog	Syslog port (UDP port number)	UDP port number used by the syslog server: usually 514 for a standard syslog server.	514	514

Parameter	Name	Description	Value	Default value
rep_archives	Archived files directory	Directory where all the filtered files are archived	archivage\	archivage\
rep_journaux	Logs directory	Directory where all the log files are written	log\journaux\	log\journaux\
rep_rapports	Reports directory	Directory where all the report files are written	log\rapports\	log\rapports\
rep_temp	Temp directory	Directory where all the temporary files are written	temp\	temp\
serveur_syslog	Syslog server (hostname or IP address)	Hostname or IP address of the syslog server to centralize logs.	localhost	localhost
taille_archives	Maximal size for the archive directory (in bytes)	Maximal size of the directory where all archived files are stored.	10000000000	10000000000
taille_temp	Maximal size for the temp directory (in bytes)	Maximal size of the directory where all temporary files are stored.	10000000000	10000000000
section [Filtre_AVI]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_BMP]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_Excel]				
detecter_ole_pkg	Detect Package OLE objects	Detect Package OLE objects, which may contain any file or command line.	1	True
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
macros_fpcmd	Use F-Prot 3 to remove VBA macros	Use the F-Prot 3 antivirus (fpcmd) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_fpscan	Use F-Prot 6 to remove VBA macros	Use the F-Prot 6 antivirus (fpscan) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_win32	Use the Win32 API to remove VBA macros (Windows only)	Use the Win32 API on Windows to remove all VBA macros from documents. This method is fast, but it only covers Word and Excel, and it only works on Windows. This parameter is ignored on other platforms.	1	True
supprimer_macros	Remove VBA macros	Remove/disable all VBA macros from documents. See also macros_xxx parameters to choose which method to use. If no specific method is enabled, a simple method will be used. This simple method is portable and fast, however it only covers Word and Excel files.	1	True
section [Filtre_GIF]				

Parameter	Name	Description	Value	Default value
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_HTML]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_JPEG]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_MP3]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_PDF]				
disable_aa	Disable AA objects (additional actions)	Disable all AA objects, which may trigger active content. (pdfid)	1	True
disable_embeddedfile	Disable embedded files	Disable all embedded files, which may hide executable code. (simple replace, pdfid)	1	True
disable_fileattachment	Disable attached files	Disable all file attachments, which may hide executable code. (simple replace, pdfid)	1	True
disable_javascript	Disable Javascript	Disable all Javascript code, which may trigger actions without user confirmation. (simple replace, pdfid)	1	True
disable_jbig2decode	Disable JBIG2Decode objects	Disable all JBIG2Decode objects, subject to vulnerabilities in some applications. (pdfid)	0	False
disable_openaction	Disable OpenAction objects	Disable all OpenAction objects, which may trigger active content. (pdfid)	1	True
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
ignore_origami_errors	Ignore PDF parsing errors in Origami engine	The current version of Origami does not support all PDF features, and may block legitimate files. With this option ExeFilter will fall back to the simple replace method in case of error.	1	True
use_origami	Remove active content using Origami engine	Remove all active content using Origami pdfclean engine. (EXPERIMENTAL: not all PDFs are supported yet)	0	False
use_pdfid	Remove active content using pdfid	Remove all active content using pdfid. (EXPERIMENTAL: Effective against obfuscated PDFs)	1	True
use_simple_replace	Remove active content using simple replace	Remove all active content using builtin simple replace method. (Only effective against non obfuscated PDFs)	1	True
section [Filtre_PNG]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_Powerpoint]				

Parameter	Name	Description	Value	Default value
detecter_ole_pkg	Detect Package OLE objects	Detect Package OLE objects, which may contain any file or command line.	1	True
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
macros_fpcmd	Use F-Prot 3 to remove VBA macros	Use the F-Prot 3 antivirus (fpcmd) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_fpscan	Use F-Prot 6 to remove VBA macros	Use the F-Prot 6 antivirus (fpscan) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
supprimer_macros	Remove VBA macros	Remove/disable all VBA macros from documents. See also macros_xxx parameters to choose which method to use. If no specific method is enabled, a simple method will be used. This simple method is portable and fast, however it only covers Word and Excel files.	1	True
section [Filtre_Project]				
detecter_ole_pkg	Detect Package OLE objects	Detect Package OLE objects, which may contain any file or command line.	1	True
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
macros_fpcmd	Use F-Prot 3 to remove VBA macros	Use the F-Prot 3 antivirus (fpcmd) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_fpscan	Use F-Prot 6 to remove VBA macros	Use the F-Prot 6 antivirus (fpscan) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
supprimer_macros	Remove VBA macros	Remove/disable all VBA macros from documents. See also macros_xxx parameters to choose which method to use. If no specific method is enabled, a simple method will be used. This simple method is portable and fast, however it only covers Word and Excel files.	1	True
section [Filtre_RTF]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
supprimer_OLE_Package	Disable Package OLE objects	Disable Package OLE objects, which may contain any executable file or command line.	1	True
section [Filtre_Texte]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_Visio]				
detecter_ole_pkg	Detect Package OLE objects	Detect Package OLE objects, which may contain any file or command line.	1	True

Parameter	Name	Description	Value	Default value
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
macros_fpcmd	Use F-Prot 3 to remove VBA macros	Use the F-Prot 3 antivirus (fpcmd) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_fpscan	Use F-Prot 6 to remove VBA macros	Use the F-Prot 6 antivirus (fpscan) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
supprimer_macros	Remove VBA macros	Remove/disable all VBA macros from documents. See also macros_xxx parameters to choose which method to use. If no specific method is enabled, a simple method will be used. This simple method is portable and fast, however it only covers Word and Excel files.	1	True
section [Filtre_WAV]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
section [Filtre_Word]				
detecter_ole_pkg	Detect Package OLE objects	Detect Package OLE objects, which may contain any file or command line.	1	True
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True
macros_fpcmd	Use F-Prot 3 to remove VBA macros	Use the F-Prot 3 antivirus (fpcmd) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_fpscan	Use F-Prot 6 to remove VBA macros	Use the F-Prot 6 antivirus (fpscan) to remove all VBA macros from documents. This method is slow but efficient for Word, Excel and Powerpoint.	0	False
macros_win32	Use the Win32 API to remove VBA macros (Windows only)	Use the Win32 API on Windows to remove all VBA macros from documents. This method is fast, but it only covers Word and Excel, and it only works on Windows. This parameter is ignored on other platforms.	1	True
supprimer_macros	Remove VBA macros	Remove/disable all VBA macros from documents. See also macros_xxx parameters to choose which method to use. If no specific method is enabled, a simple method will be used. This simple method is portable and fast, however it only covers Word and Excel files.	1	True
section [Filtre_Zip]				
format_autorise	Allowed format	Specifies whether this file format is allowed by the filtering policy or not	1	True

7 How to contribute to the ExeFilter project

ExeFilter is an open-source project. Therefore, it is crucial to contribute to the project so that it can progress. There are many ways to help:

7.1 Contact

In all cases, here are the e-mail addresses to contact the project team:

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

7.2 Report bugs

If you see any unexpected error, an incompatibility or a file which is accepted or blocked whereas it should not, please send us all necessary details.

If possible, here are the useful pieces of information which would help us understand the issue:

- a detailed description of the context (usage mode, type of analyzed content, operating system and version, installed versions of Python and ExeFilter, configuration file, etc)
- file samples to reproduce the error
- debug log files, if possible obtained using the "-v" option with ExeFilter command-line.

7.3 Report a vulnerability

Like any other security software, detecting a vulnerability in ExeFilter is critical. Because ExeFilter contains parsers for various file formats, vulnerabilities are likely to be found.

If you find one, please report it ASAP to the project team, and leave us enough time to fix it before any public disclosure. It is much more responsible to provide users with a security fix before disclosing a vulnerability. The project team will take all reported vulnerabilities very seriously, and will attempt to fix them as soon as possible.

A mailing-list will be created in the future to inform users about new versions and security fixes.

7.4 Test various environments

The project team cannot test ExeFilter in all possible configurations and on all platforms. Reporting that ExeFilter runs fine or not on a specific platform will help the project. Thank you to tell us any successful or failed test, and the corresponding configuration.

Here are the platforms where the latest ExeFilter versions are usually tested:

- Windows Vista with Python 2.6
- MacOSX Leopard (10.5) with Python 2.6
- GNU/Linux Ubuntu with Python 2.6

7.5 Create new filters

It is possible to create new filters to support additional file formats. If you would like to add a new format or to improve an existing filter, the first thing to do is to contact the project team, in order to know if it is already an ongoing task or not.

To develop a new filter, here is a summary of the actions to perform:

1. Determine if it is a **simple filter** (to accept or block files without cleaning) or a **complex filter** (which may modify files to clean them).
2. If it is a simple filter, use one of these existing filters as template: GIF, JPEG, BMP, Text.
3. If it is a complex filter, pick one of these: RTF, PDF, Office.
4. The filter script must be a Python module (.py), starting with “Filtre_”, located in the “Filtres” subfolder.
5. It must contain a class with a name starting with “Filtre_”, which inherits from the class “Filtre.Filtre”.
6. The class must have a class attribute “extensions” which is a list of all file extensions allowed for the format, in lowercase, including a leading dot. For example the MS Word format has the following list: ['.doc', '.dot'].
7. The class must implement a method “reconnait_format” (recognize format) which returns True if the contents of the file match the expected format, or False otherwise. For example, a PDF file is expected to start with “%PDF”.
8. The class must also implement the method “nettoyer” (clean), which analyzes the file structure in depth and removes active content if applicable. This method must return a “Resultat” (result) object, to provide the result of the cleaning process. It must replace the temporary copy of the file by a cleaned version if necessary.
9. If the format is a container, such as an archive, then it is also necessary to create a “Conteneur” (container) class. See Conteneur_ZIP.py for an example.

Note: the ExeFilter API is quite complex and only available in French for now. Therefore, please contact the project team first if you would like to develop a filter.

7.6 Participate in the project development

It is also possible to help the development effort by improving some features or integrating ExeFilter into other applications (HTTP proxy, e-mail server, GUI, etc). Please contact the project team if you would like to submit patches or to join the team.

7.7 Improve documentation

As in any project, documentation is a very important and very difficult task. Any contribution would be greatly appreciated! :-)

8 References

- [CSW08] ExeFilter – a new open-source framework for active content filtering, P. Lagadec, CanSecWest08 conference, http://www.decalage.info/exefilter
- [EUSW10] Fighting PDF malware with ExeFilter, P. Lagadec, EUSecWest 2010 conference, http://www.decalage.info/eusecwest10
- [HACKLU09] Malicious PDF origamis strike back, F. Raynal, G. Delugré, D. Aumaitre, Hack.lu09 conference, http://www.security-labs.org/fred/docs/hack.lu09-origamis-strike-back.pdf
- [SSTIC03] Formats de fichiers et code malveillant (File Formats and Malware), P. Lagadec, SSTIC03 symposium, http://www.decalage.info/fr/sstic03
- [SSTIC04] Filtrage de messagerie et analyse de contenu (E-mail Filtering and Content Analysis), P. Lagadec, SSTIC04 symposium, http://www.decalage.info/fr/sstic04
- [SSTIC06] Diode réseau et ExeFilter (Network Diode and ExeFilter), P. Lagadec, SSTIC06 symposium, http://www.decalage.info/fr/sstic06

9 Changelog

date	version	author	modifications
2008-03-03	1	P. Lagadec	Initial version
2008-03-27	2	P. Lagadec	English translation
2009-11-02	3	P. Lagadec	Updated for version 1.1.2, completed English translation
2009-12-18	4	P. Lagadec	Added the “single file output” option (-o) and exit codes
2010-02-09	5	P. Lagadec	Added the “batch mode” option (-b)
2011-02-07	6	P. Lagadec	Updated for version 1.1.3: mini GUI, -f option, Mailsweeper integration