# Installation Guide

FOR THE **VAMSOFT PDF SPAM AGENT 1.0 BETA R6**

# Introduction

The *Vamsoft PDF Spam Agent* is an External Agent for ORF version 2.1 and newer versions that improves ORF by PDF spam detection capabilities.

Version 1.0 Beta R6 is an updated agent release that recognizes most of the latest PDF spam varieties. Note that the PDF spam phenomenon is new and changes rapidly. Due to the design of the PDF Spam Agent, it may quickly lose effectiveness without being updated. Be sure to visit

http://www.vamsoft.com/vspdfspam

or

news://news.vamsoft.com/orf.ee.3rdparty

regularly for the latest version and/or community updated versions of the PDF Spam Agent. We also publish announcements about updates in the News section of our website. Subscribe to the vamsoft.com news RSS feed (URL: http://www.vamsoft.com/rssnews.asp) using a news aggregator (Microsoft Internet Explorer 7, Mozilla Firefox, GreatNews, etc.) to track the news automatically.

### WHAT IS PDF SPAM?

“PDF Spam” is the common name for unsolicited emails that utilizes attached PDF documents (often with embedded images) for the payload, typically stock tips.

### HOW DOES THE PDF SPAM AGENT WORK?

The agent checks for specific properties of 9+ different types of PDF spam emails. If the email is identified as one of these types, it is reported as suspected PDF spam.

### UPDATES

The PDF spam phenomenon is new and changes rapidly. Due to the design of the PDF Spam Agent, it may quickly lose effectiveness without being updated. Be sure to check the PDF Spam Agent webpage (http://www.vamsoft.com/vspdfspam/) often or subscribe to the vamsoft.com news RSS feed (URL: http://www.vamsoft.com/rssnews.asp) using a news aggregator (Microsoft Internet Explorer 7, Mozilla Firefox, GreatNews, etc.) to track the update news automatically.

### FALSE POSITIVES

The agent tests the email for several different characteristics of PDF spam. Due to the heuristic nature of PDF spam detection, some emails may be falsely identified as PDF spam (false positive), e.g. emails with a single PDF attachment containing a scanned document, created in an old version of Adobe Acrobat or some PDFs generated by web scripts. As of writing this, we have not discovered any false positives, however.

## Prerequisites

**IMPORTANT:** This software requires the *Microsoft .NET 2.0 Runtime* and also the *.NET 1.1 Runtime*. If you do not have these already installed, download and install them from the link below.

.NET Runtime 2.0
http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

.NET Runtime 1.1
http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en

## Upgrading From Previous Versions

If you have a previous version installed (*1.0 Beta R1-R5*), please delete your current PDF Spam Agent definition using the ORF Administration Tool. Select *Configuration / Filtering - On Arrival / External Agents*, select the *Vamsoft PDF Spam Agent* definition and click the *Delete* button.

When installing the new version, you can safely overwrite your previous agent files with the new ones.

## Installation

### 1. DOWNLOAD THE PACKAGE

Download the *Vamsoft PDF Spam* package from:

http://www.vamsoft.com/vspdfspam/

### 2. EXTRACTING FILES

Extract the package contents into an arbitrary local directory on your server. We recommend to extract the files to:

*\Program Files\Vamsoft\PDFSpamAgent*

This guide will use this path in the further examples.

### 3. IMPORTING THE AGENT DEFINITION

Follow the instructions below to import the agent definition.

1. Start the *ORF Administration Tool*.
2. Select *Configuration* | *Import* | *External Agent Definitions* from the menu.
3. Select the \*Program Files\Vamsoft\PDFSpamAgent\agentdef\vspdfspam.xml* agent definition file in the dialog and click *Open*.
4. Click *Ok* in the *Importing Agent Definitions* dialog.
5. Configure the agent below as described in the next section.

## Configuration

### 1. CHECKING THE EXTERNAL AGENT TEST STATUS

The agent will work only if the External Agents test is enabled and properly configured. Make sure that:

- The External Agent Test is enabled on the *Configuration / Tests / Tests* page.
- *Path for temporary email files* points to a valid and existing directory on the *Configuration / Filtering – On Arrival / External Agents* page.

### 2. SETTING THE AGENT PATH

After importing the agent definition, you will have to set the path for the agent.

1. Select *Configuration / Filtering - On Arrival / External Agents* in the Administration Tool.

2. Select "*Vamsoft PDF Spam Agent*" from the list and click the *Modify* button.

3. Click the ***Run*** tab.

4. Click the ellipsis (...) button on the right of the *Agent Executable* edit box.

5. Select *pdfspamagent.exe* from from *\Program Files\Vamsoft\PDFSpamAgent\bin*.

6. Click *Ok*.

### 2. ENABLING THE AGENT

1. Select *Configuration / Filtering - On Arrival / External Agents* in the Administration Tool.

2. Select "*Vamsoft PDF Spam Agent*" from the list and set the checkbox for it.

3. Apply the configuration changes in the *Configuration | Save and Update Configuration* menu.

## Source Code

### PDF SPAM AGENT SOURCE CODE

You can download the source code (C# 2.0) of the PDF Spam Agent from the link below:

http://www.vamsoft.com/vspdfspam/

The source code is licensed under *GNU Lesser General Public License* (LGPL), which allows you to modify the agent to your requirements and share the modified source code.

The PDF Spam Agent relies on iText#, a free C# port of the open source Java iText library. Learn more about iText# at

http://itextsharp.sourceforge.net/

### DEVELOPMENT SKILLS REQUIRED

Updating the agent for new PDF variants requires entry-level C# 2.0 development skills, but you can probably succeed with a solid background of any modern object oriented language, like C++, Java or Delphi.

### DEVELOPMENT ENVIRONMENT

The agent was created in Microsoft Visual Studio 2005 Professional. You can also compile the project using the command-line *csc* compiler or use the free Microsoft Visual C# 2005 Express Edition IDE, SharpDevelop or your favorite environment.

### BASICS OF EXTERNAL AGENTS

ORF External Agents are basically command-line (console) applications. ORF starts the agent with various parameters (e.g. path to the email MIME source file being checked), wait for the agent process to exit and take the process exit/return code (plus optionally, its output to *stdout* or *stderr*). Based on the agent exit code, ORF performs the actions as specified by the agent definition.

### PDF SPAM AGENT USAGE FROM COMMAND-LINE

The above design makes it very easy to test External Agents, because you can run them from the console, e.g.

```
pdfspamagent -c test.eml
echo Exit Code: %ERRORLEVEL%
```

will check *test.eml* for PDF spam and will write the exit code of the PDF Spam Agent to the console.

### UPDATING THE RECOGNITION ENGINE

The PDF spam recognition engine resides in the *PdfSpamRecognizer.cs* file. *IsTypeXSpam()* static methods are responsible for recognizing specific PDF spam variants, based on the pre-parsed properties of the email and the embedded PDF.

You can extend the recognition engine by adding a new *IsTypeXSpam()* method based on the previous ones and insert the call to new method into the *IsPdfSpamEmail()* static method.

To learn what properties a new variant has, run the agent as

```
pdfspamagent -d test.eml
```

or

*pdfspamagent -d test.pdf*

This will dump the email and PDF properties to the console, helping you to recognize unique properties of the spam variant and constructing a ruleset against them.

### DEFINING NEW RULESETS

We recommend that you define new rulesets very strictly. It is true that a new variant will not be recognized if the spammer changes only one of the properties, but the more strict the ruleset is the less likely the agent catches a legitimate email. So, the more parameters that describe the spam email the better.

## Technical Support

Please contact our technical support using contact options below. Using the Community Forums is recommended (we are active there as well).

Before contacting us, please check the product documentation and the ORF FAQ, you may find a quick answer for your question there.

| | |
|---|---|
| **Email:** | orf-support@vamsoft.com |
| **Community Forums** | http://www.vamsoft.com/forum |
| **Phone:** | (+36) 1 279 2299 |
| **Fax:** | (+36) 1 279 1260 |
| **World Wide Web:** | http://www.vamsoft.com |
| **Postal Address:** | Vamsoft Ltd.<br>Budapest<br>Györök utca 11.<br>H-1113<br>HUNGARY |