

Backscatter Protection Agent

VERSION 1.1 DOCUMENTATION

Revision: 1.2
Date: February 21, 2011

Introduction

WHAT IS BACKSCATTER?

Backscatter (or “reverse NDR”) attacks occur when a spammer sends large amount of emails in the name of your domain and your email server gets bombed by bounce reports (also called DSNs or NDRs) from legitimate servers.

HOW DOES THIS AGENT HELPS?

The Backscatter Protection Agent can detect backscatter with high accuracy and enables you to throw away the DSNs caused by the forged emails.

Note that this agent will help against DSNs only. Out-Of-Office autoresponses, Challenge/Response anti-spam requests and other type of automated emails may get thru the filtering.

Publishing an SPF policy could also help reducing the amount of backscatter you receive. Read more about this [below](#).

HOW DOES THE AGENT WORK?

The idea behind the agent is that most DSNs contain the original email and this allows the agent to check if the original email is from your network, by examining whether it shows properties unique to your network.

This agent checks specifically for the Message-ID email header, which has a unique format pattern for every network/server. The agent extracts the Message-ID headers from the bounce report, and matches them with your unique pattern. If none of the Message-IDs are like your pattern, the agent reports that the original email was probably from another network—in other words, it's a backscatter DSN.

Before Installation

To start using the agent, you need to find out the Message-ID pattern unique to your network. Read the section below before you start installing the agent.

DETERMINING YOUR MESSAGE-ID PATTERN

During email delivery, typically it is the first server involved in the delivery which assigns a unique *Message-ID* to the email, e.g. a Microsoft® Exchange Server or the IIS SMTP Service. A Message-ID email header looks like this:

Message-ID: <01a901c894aa\$28afcc20\$39fba8c0@domain.local>

The value between < and > is the Message-ID, as shown in the example below:

01a901c894aa\$28afcc20\$39fba8c0@domain.local

We highlighted the `@domain.local` part, because this is what we are going to define a simple regular expression pattern for, which is:

`.*@domain\.local$`

[explained: zero or more (*) arbitrary characters (.), followed by an '@' sign and the literal "domain", a dot character (\.) and the literal "local". No extra characters behind this pattern are allowed (\$)]

In rare cases, your network may have multiple servers with where Message-IDs are generated. In this case, you may have to use a combined pattern:

`.*@(domain1\.local|domain2\.local)$`

[explained: same as before, but a logical OR operation was introduced between the two patterns, using parentheses and the | sign. You can add further subpatterns in this fashion as (subpattern1|subpattern2|subpattern3)]

If your Message-IDs domains differ only in the server name (e.g. `@srv1.domain.local`, `@srv2.domain.local`), you can use a regular expression like:

`.*@.*\.domain\.local$`

[explained: like in the first example, but now we allow zero or more arbitrary characters after the '@' sign and require a dot character before the 'domain.local' literal]

Regular expressions (regex) can be a bit scary at first - if you get lost, feel free to contact us with your Message-ID samples. When writing regexs, consider that many characters have special role in regular expressions. It is recommended that you "escape" any non-alphanumeric letter by placing a backslash in front of them. For example, dot character escaped is `\.`, instead of just `.`.

Now, you need to determine check *your* Message-ID pattern. The easiest way to do this is to send an email *outside your organization* (e.g. to GMail or Hotmail) and check the email source. Outlook shows the email headers (open the email, select *View | Options*). In GMail, use the *Show Original* menu. You can also email us (orf-support@vamssoft.com) and we will tell you what Message-ID we received.

Typically, your Message-ID will contain the internal server name or the local domain name. Consider that special-purpose email software, such as CRM systems, mailing lists, bug trackers and such may assign their own Message-ID to the emails they generate. If you have such software installed on your network, it is recommended to check their Message-ID samples, too.

Installation

1. DOWNLOAD THE PACKAGE

Download the *Vamssoft PDF Spam* package from:

<http://www.vamsoft.com/vsbackscatter/>

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\BackscatterAgent`

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\BackscatterAgent\agentdef\backscatteragent.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. CHECKING THE DSN FILTERING STATUS

ORF has to be configured to allow filtering DSNs. Make sure that the “*Allow filtering Delivery Status Notifications*” box is **checked** on the *Configuration / Global / Miscellaneous* page.

3. 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 Backscatter Protection 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 *backscatteragent.exe* from from *\Program Files\Vamsoft\BackscatterAgent\bin*.

4. CONFIGURING PARAMETERS

Still on the same page, enter your Message-ID pattern.

1. In the “*Parameters*” box, replace the *<msgidpattern>* text with your Message-ID pattern regex. Make sure the regex is between double quotes, e.g. “*.*@domain\.local\$*”.

To learn how to determine your Message-ID pattern, [click here](#).

5. ENABLING THE AGENT

1. Select *Configuration / Filtering - On Arrival / External Agents* in the Administration Tool.
2. Select “*Vamsoft Backscatter Protection Agent*” from the list and set the checkbox for it.
3. Apply the configuration changes in the *Configuration | Save Configuration* menu.

Additional Information

JUST HOW ACCURATE THE AGENT IS?

In our lab test, the agent produced 0.19% false positives on a 1064 bounce-report-only test body. Here, a false positive means a DSN incorrectly classified as backscatter DSN. The false negative rate was 0.66%, i.e. emails that are from backscatter, but are not classified so.

Note that the above figures are for bounce reports only. There is practically no chance for classifying a regular email as backscatter DSN.

False positives typically occur if the network which receives your email rewrites the Message-ID of the email. Another observed case is when the DSN is about another DSN.

OTHER METHODS OF PROTECTING YOURSELF FROM BACKSCATTER

If you have not published an SPF policy yet, do it now and it will help with reducing backscatter. By publishing an SPF policy, you declare which IP addresses may act as outbound email servers for your domain. SPF-compliant email receivers will check your SPF policy and if they find that an email came from an IP address not listed by policy, they will know the sender is forged. Setting up an SPF policy is quite easy. Learn more about SPF at <http://www.openspf.org>.

■ Technical Support

Please contact us <http://www.vamsoft.com/support.asp>.