**Suricata - Feature #776**

**Add smtp_envelope and smtp_header keywords**

03/12/2013 04:55 AM - David André

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>low</td>
</tr>
<tr>
<td>Label:</td>
<td>Beginner</td>
</tr>
</tbody>
</table>

**Description**

Add smtp_envelope and smtp_header keywords.

The envelope is composed of communication before the DATA segment (example at [http://en.wikipedia.org/wiki/SMTP#SMTP_transport_example](http://en.wikipedia.org/wiki/SMTP#SMTP_transport_example)) and the header is the part of the email content before there is the mail body (which should be anything between DATA and the first occurrence of CR LF CR LF).

The idea is to allow rules searching for email addresses, mail user-agents, etc., while not matching on the same pattern(s) being discussed in an email body.

**History**

#1 - 03/12/2013 05:16 AM - Victor Julien

I have some test code for this, let me try to find it and see if it in usable shape.

#2 - 10/16/2013 01:35 AM - Christophe Vandeplas

Email subject and attachment names are also very interesting keywords

Do consider that data need to be normalized as the data:

- can be split in multiple lines

#3 - 10/26/2013 10:21 AM - Victor Julien

- Target version set to TBD

#4 - 01/01/2016 06:16 PM - Andreas Herz

- Assignee set to OISF Dev

#5 - 07/17/2018 08:33 AM - Victor Julien

- Assignee changed from OISF Dev to Anonymous
- Effort set to medium
- Difficulty set to low

#6 - 02/23/2019 10:11 PM - Andreas Herz

- Assignee set to Community Ticket

#7 - 09/25/2019 07:26 PM - Victor Julien

- Label Beginner added