**Suricata - Feature #3261**

SMTP quoted-printable Decoding of Message Body  

10/17/2019 07:04 PM - Brandon Murphy

<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>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Description**

In attempting to write signatures for a quoted-printable decoded message body (not an attachment) I find that signatures do not fire as expected.

FWIW, I've observed the same issue for base64 encoding of the message body as well. [https://redmine.openinfosecfoundation.org/issues/3260](https://redmine.openinfosecfoundation.org/issues/3260) has been opened to address that.

I have attached a zip that contains pcap, IDS output, rules, etc.

The pcap has two different tcp sessions, one which includes only a quoted-printable message body (tcp.port 44240), and another that includes the same quoted-printable data as an attachment (tcp.port 44242). This was done to validate that quote-printable decoding of SMTP attachments worked and could be triggered via the file_data keyword as expected.

The pcap was captured while using python scripts to read an EML and send it to a python "SMTP Sink". I then used tcprewrite to rewrite the src/dst ips from 127.0.0.1 to something more representative of the traffic I'm attempting to signature.

Please let me know if anything else is required.

**Related issues:**

- Related to Feature #3260: SMTP Base64 Decoding of Message Body  
  - New
- Related to Task #4097: Suricon 2020 brainstorm  
  - New

**History**

#1 - 10/20/2019 08:55 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 10/21/2019 01:58 PM - Victor Julien
- Related to Feature #3260: SMTP Base64 Decoding of Message Body added

#3 - 10/21/2019 01:59 PM - Victor Julien
- Tracker changed from Bug to Feature

See #3260#note-2

#4 - 01/30/2020 11:54 AM - Victor Julien
- Label Protocol added

#5 - 11/14/2020 02:26 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added

**Files**

- quoted-printable_message_body_trbl.zip  
  - 32.5 KB  
  - 10/17/2019  
  - Brandon Murphy