**Suricata - Feature #960**

**persistent TCP resets**

09/13/2013 11:11 AM - Victor Julien

<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>medium</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
</tbody>
</table>

Currently when the reject keyword is being used we send a single RST packet. If that is lost, ignored or discarded, the flow might just continue. Making the active response ineffective.

This is not a problem in IPS mode, where we drop as well as reset. The flow stores a drop flag and new packets coming in on that flow will also be dropped.

So in IDS mode, we need a better way of dealing with this. One way would be to set a flow flag as well and send more resets if more packets come in on the same flow.

We'd have to be careful of course. We should probably only do this on established TCP connections and on events generated by inspecting the reassembled stream and the app layer state. Otherwise the risk of us sending (loads of) RSTs based on injected packets might be too great.

<table>
<thead>
<tr>
<th>History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 - 01/01/2016 06:13 PM - Andreas Herz</td>
<td>Assignee set to OISF Dev</td>
</tr>
<tr>
<td>#2 - 07/17/2018 08:43 AM - Victor Julien</td>
<td>Assignee changed from OISF Dev to Anonymous</td>
</tr>
<tr>
<td></td>
<td>Effort set to medium</td>
</tr>
<tr>
<td></td>
<td>Difficulty set to medium</td>
</tr>
<tr>
<td>#3 - 02/23/2019 10:13 PM - Andreas Herz</td>
<td>Assignee set to Community Ticket</td>
</tr>
</tbody>
</table>