Suricata - Bug #221

signature does not alert or drop

07/27/2010 02:11 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Pablo Rincon</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>1.0.1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

this signature can be used to drop http connections:

```
drop tcp any any -> any 80 (msg:"Snort_Inline is blocking the http link"; sid:1; content:"/";)
```

but this signature can't be:

```
drop tcp any any -> any 80 (msg:"Snort_Inline is blocking the http link"; sid:1;)
```

so for some reason we need a content match to be able to match.

I suspect somehow the setting of the SIG_FLAG_PAYLOAD flag in a signature has something to do with it.

Please add a unittest on the matching itself and confirm that the patch properly drops.

**History**

#1 - 07/28/2010 07:53 AM - Pablo Rincon
- File 0001-Fix-for-bug221-avoid-considering-sig-as-decoder-even.patch added
- Status changed from New to Feedback

Hi, I have attached a patch that avoid flagging the sig as "decoder event only", so now it gets grouped correctly and properly triggered. Anyway, we need to flag signatures with something to tell that they have "decoder event" checks. And later update the function that tells if it's a decoder event only sig or not.

#2 - 07/29/2010 03:01 AM - Victor Julien
- Status changed from Feedback to Closed
- % Done changed from 0 to 100

Applied your patch but made some modifications to actually check if the sig contains a decoder event keyword.

**Files**

0001-Fix-for-bug221-avoid-considering-sig-as-decoder-even.patch  2.29 KB  07/28/2010  Pablo Rincon