Suricata - Bug #5437
'unseen' http midstream packets
07/06/2022 01:57 PM - Juliana Fajardini Reichow

Status: New
Priority: Normal
Assignee: OISF Dev
Category: 
Target version: TBD
Affected Versions: 
Effort: 
Difficulty: 
Label: 

Description

This was raised by a discussion on our Discord server.

Two users reached out because Suri seemed to be randomly omitting payloads from some of the alerts.

Apparently, this is happening because some HTTP midstream packets are not seen by Suri, even if we have `stream.midstream=true`. Wireshark is able to properly tag such traffic as HTTP.

This also leads to Suri not logging associated payload to some alert events in the eve-log, as it doesn't recognize the stream as HTTP.

The rule used by them to generate the alerts was:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC User-Agent known malicious user-agent string - Mirai"; flow:to_server,established; content:"User-Agent|3A| Hello, world"; fast_pattern:only; http_header; metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service HTTP; reference:url,www.virustotal.com/en/file/3908cc1d8001f926031fbeb55c1044448dbc20c979b57c3cb0d9abe7b9789f899d/analysis/; classtype:trojan-activity; sid:58992; rev:1;)
```

History

#1 - 07/08/2022 03:25 PM - Juliana Fajardini Reichow
- Description updated

#2 - 07/08/2022 06:49 PM - Juliana Fajardini Reichow
SV test demonstrating the issue: https://github.com/OISF/suricata-verify/pull/877

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymized-NoPayload.pcap</td>
<td>768 Bytes</td>
<td>07/06/2022</td>
<td>Juliana Fajardini Reichow</td>
</tr>
<tr>
<td>anonymized-Payload.pcap</td>
<td>8.33 KB</td>
<td>07/06/2022</td>
<td>Juliana Fajardini Reichow</td>
</tr>
</tbody>
</table>

07/16/2022