Inconsistent behavior with 'only_stream' flow keyword

03/31/2016 12:21 PM - Zach Rasmor

In testing some Suricata rules with RDP pcap, I seem to have uncovered inconsistent behavior with the 'only_stream' flow keyword. My original testing was with rules invoking luajit scripts, but the behavior occurs even without luajit scripts, so I have removed them from these rules for simplicity:

Say I want to alert on all streams flowing to port 3389. This rule will not fire. I believe this to be a bug.

```
alert tcp any any -> any 3389 (msg:"RDP connection request"; flow:to_server, established, only_stream; sid:15; rev:1;)
```

```
$ tail -1 /var/log/suricata/suricata-stats.log | jq .stats.detect
{
  "alert": 0,
  "alert_delta": 0
}
```

However, if I change 'only_stream' to 'no_stream' to alert on every packet flowing to port 3389, this rule does fire. And it fires A LOT.

```
alert tcp any any -> any 3389 (msg:"RDP connection request"; flow:to_server, established, no_stream; sid:15; rev:1;)
```

```
$ tail -1 /var/log/suricata/suricata-stats.log | jq .stats.detect
{
  "alert": 3333875,
  "alert_delta": 1380607
}
```

But finally, if I switch back to 'only_stream', but tighten the rule to add a content field that checks the first byte of the payload, the rule fires.

```
alert tcp any any -> any 3389 (msg:"RDP connection request"; flow:to_server, established, only_stream; content:"|03|"; offset:0; depth:1; sid:15; rev:1;)
```

```
$ tail -1 /var/log/suricata/suricata-stats.log | jq .stats.detect
{
  "alert": 363,
  "alert_delta": 363
}
```

I could possibly submit pcap privately (pending approval), but I imagine that this bug wouldn't be hard to reproduce for other traffic.

History

#1 - 09/08/2016 02:37 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 02/18/2019 10:59 PM - Andreas Herz
Do you still see the issue with recent suricata versions?
Hi, we're closing this issue since there have been no further responses. If you think this bug is still relevant, try to test it again with the most recent version of suricata and reopen the issue. If you want to improve the bug report please take a look at https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Reporting_Bugs