Suricata - Feature #2486

Task # 4380 (Assigned): tracking: improvements to bits, ints, vars

prefilter/fast_pattern logic for flowbits

04/14/2018 06:43 PM - Jason Williams

Status: In Progress
Priority: Normal
Assignee: Victor Julien
Category: 
Target version: 7.0rc1
Effort:
Difficulty:

Description:

It would be useful to have a way to indicate that a rule with a flowbit check should only be checked in the event that the set flowbit appears in the flow.

This could reduce the number of checks on signatures with poor fast_pattern candidates and time spent matching only to throw away the match because the flowbit was not present.

For example:

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CURRENT_EVENTS HTTP POST Form Observed After Successful Credential Theft"; flowbits:isset,ET.genericphish; file_data; content:"method=|22|post|22|"; nocase; sid:123; rev:1;)
```

This rule can be very useful for generic phish detection, but because the only content we're looking for is the post, we incur lots and lots of checks as thats the only available match for fast_pattern

Related issues:
Related to Task #2685: SuriCon 2018 brainstorm
Related to Task #3288: Suricon 2019 brainstorm
Related to Task #4097: Suricon 2020 brainstorm

History

#1 - 04/24/2018 10:06 PM - Andreas Herz
- Target version set to TBD

#2 - 11/21/2018 11:39 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien

I think this can be done with some limitations. Since prefilter runs before the actual rules, it could FN if one of the rules sets a flowbit after the prefilter has run.

A simple solution could be to simply limit the prefilter support to flowbits that are set in one direction, and checked in the other direction.

Another more complex setup could be that when setting a flowbit the rules that depend on it (and use it as a prefilter) are added to the rule 'candidate' list. Here the rule order would probably have to be taken into account.

#3 - 11/21/2018 11:39 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#4 - 11/05/2019 09:37 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#5 - 11/05/2019 09:50 AM - Victor Julien
At Suricon 2019 there was still interest for this.
#6 - 11/14/2020 02:26 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added

#7 - 11/16/2020 12:18 PM - Victor Julien
- Target version changed from TBD to 7.0rc1

#8 - 03/06/2021 08:06 AM - Victor Julien
- Parent task set to #4380

#9 - 10/11/2021 02:09 PM - Victor Julien
- Status changed from Assigned to In Progress