Suricata - Feature #2538

dsize keyword improvements

07/16/2018 02:47 PM - Cyrille Barbaux

Status: New
Priority: Normal
Assignee: Community Ticket
Category:
Target version: TBD
Effort: low
Difficulty: medium

Description

Today, dsize is limited to detect if a payload size is smaller, equal or larger than a single value.

In order to improve abnormal packets detection, signatures should be able to:
- Detect if dsize is different than a specified value.
- Allow multiple dsizes in the same signature.

For example, I've got 2 use-cases from real world.

I've got an industrial protocol that uses the same payload size in every packet, let's say 100B. Today, I've got to write 2 rules, one with "dsize<100;" and a second one with "dsize>100;" as multiple dsizes are not allowed in the same signature.

It would be nice to write a single rule with dsize:!100;

Another protocol uses only 2 payload sizes, depending on the packet type, let's use 100B and 150B. I cannot detect the full range of anomaly with the current implementation.

The improvement should allow to write: "dsize:!100; dsize:!150;" or "dsize:!\[100,150\];" in the signature.

History

#1 - 07/16/2018 02:54 PM - Victor Julien
- Subject changed from dsize improvements to dsize keyword improvements
- Assignee set to Anonymous
- Target version set to TBD
- Effort set to low
- Difficulty set to medium

Difficulty is mostly in the interaction with the prefilter functionality.

#2 - 02/23/2019 10:03 PM - Andreas Herz
- Assignee set to Community Ticket