How to detect attacks in the infinite payloads?

08/31/2020 03:49 AM - Zhu Zhu

Status: New
Priority: Normal
Assignee:
Category:
Affected Versions: 5.0.1
Label:

Description
I have the infinite payloads to check and try to match each payload with all ET rules amount is about 40k. I tried with unit test functions to create a full package and also load signatures with unit test functions, however, it is very slow in this situation. Is there any suggestion to resolve my problem?

ps: The suricata version is 5.0.1.

History
#1 - 09/05/2020 09:44 PM - Andreas Herz