Suricata - Feature #3549
Add MQTT parser
03/26/2020 04:35 PM - Sascha Steinbiss

Status: In Review
Priority: Normal
Assignee: Sascha Steinbiss
Category: Protocol
Target version: 6.0.0rc1
Effort: 

Description
It would probably be useful if Suricata had more support for IoT related protocols, such as MQTT. Zeek has support for that (https://docs.zeek.org/en/current/scripts/policy/protocols/mqtt/main.zeek.html) and it seems to be used in some popular contexts, such as The Things Network.

Both detailed logging (to gather information about communicating parties and publisher/subscriber relationships, potentially allowing to implement anomaly detection on top of that) and indicator based detection (via rules) would be needed to gain visibility into such network activity.

History
#1 - 04/13/2020 11:28 PM - Jason Ish
- Status changed from New to In Review

Initial pull request: https://github.com/OISF/suricata/pull/4733

#2 - 05/12/2020 09:34 AM - Victor Julien
- Assignee set to Sascha Steinbiss
- Target version set to 6.0.0rc1