Suricata - Feature #2970

DNS: Parse and extract SOA app layer data from DNS packets

05/07/2019 11:31 AM - Konstantin Klinger

Status: In Review
Priority: Normal
Assignee: Simon Dugas
Category:
Target version: 6.0.0rc1
Effort:
Difficulty:

Label: Protocol

Description
At the moment the DNS parser gives you "SOA" as rrtype, but the related metadata of those SOA records/DNS packets are missing. In the attached pcap you can find the current output.

I would expect something like this (equivalent to the content in Wireshark output):

Answers
suricon.net: type SOA, class IN, mname ns1.siteground199.com
Name: suricon.net
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 21599
Data length: 50
Primary name server: ns1.siteground199.com
Responsible authority's mailbox: root.siteground199.com
Serial Number: 2018092604
Refresh Interval: 86400 (1 day)
Retry Interval: 7200 (2 hours)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 86400 (1 day)

History
#1 - 05/23/2019 10:05 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to TBD

#2 - 01/30/2020 01:35 PM - Victor Julien
- Label Protocol added

#3 - 04/17/2020 02:51 PM - Simon Dugas
I started looking into this: https://github.com/OISF/suricata/pull/4830

#4 - 04/26/2020 11:19 AM - Victor Julien
- Status changed from New to In Review
- Assignee changed from Community Ticket to Simon Dugas
- Target version changed from TBD to 6.0.0rc1

https://github.com/OISF/suricata/pull/4830

Files
soa_record.eve.json  5.54 KB  05/07/2019  Konstantin Klinger
soa_record.pcap  719 Bytes  05/07/2019  Konstantin Klinger