Suricata - Feature #2563
Add dump of all headers in http eve-log
08/03/2018 01:13 PM - Maurizio Abba

Status: Closed
Priority: Normal
Assignee: Maurizio Abba
Category: Target version: 5.0beta1
Effort: low
Difficulty: low

Description
A patch adding a list of json objects with the list of HTTP headers encountered for that transaction in the two object "request_headers" and "response_headers".

The direction of the information (i.e., whether we want to log only HTTP request headers, only HTTP response headers, or both) is set via configuration key "dump-all-headers".

We introduced two limits to avoid potential memory exhaustion caused by very long http headers. This limit is hardcoded to 256 bytes for HTTP header name and 2048 for http header value.

The resulting list of http headers will be in this form:

"http": {
   "request_headers": [
      {
         "name": "User-Agent",
         "value": "Wget/1.13.4 (linux-gnu)"
      },
      {
         "name": "Accept",
         "value": "*/*
      },
   ],
   "response_headers": [
      {
         "name": "Date",
         "value": "Wed, 25 Mar 2015 15:40:41 GMT"
      },
      {
         "name": "Server",
         "value": "Apache"
      },
      {
         "name": "Last-Modified",
         "value": "Wed, 25 Mar 2015 15:38:48 GMT"
      },
      {
         "name": "ETag",
         "value": ""34000d-c3-5121eb20b238d"
      }
   ],
}

Note that the dump-all-headers is disabled by default, meaning that by default the fields will not be present.

Related issues:
Related to Task #2685: SuriCon 2018 brainstorm New

History
#1 - 08/13/2018 08:54 PM - Andreas Herz
https://github.com/OISF/suricata/pull/3443

#2 - 11/17/2018 12:41 AM - Maurizio Abba
v3 https://github.com/OISF/suricata/pull/3548

#3 - 11/21/2018 09:12 AM - Victor Julien
- Target version set to 5.0beta1

#4 - 11/21/2018 09:12 AM - Victor Julien
- Status changed from New to Assigned

#5 - 11/21/2018 09:12 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#6 - 02/13/2019 10:53 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/pull/3639