Suricata - Feature #2283

turn content modifiers into 'sticky buffers'

11/20/2017 10:01 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: OISF Dev
Category: Target version: 5.0rc1
Effort:
Difficulty:

Label:

Description

Turn all content modifiers into sticky buffers with a `<proto>.<buffer>[.<modifier>]` notation. Support this dot-notation for all existing sticky buffers.

In both cases the existing rule keywords need to keep working for backwards compatibility. New keywords only need to support the new notation.

Some examples:

content:"abc"; http_uri; -> http.uri; content:"abc";
content:"abc"; http_raw_uri; -> http.uri.raw; content:"abc";
content:"abc"; http_client_body; -> http.request_body; content:"abc";
dns_query; content:"abc"; -> dns.query; content:"abc";

Internally, these keywords need to be registered through the 'v2 API', so that they support transforms.

Examples can be found in https://github.com/OISF/suricata/pull/3632

Subtasks:

Feature # 2897: update http_content_type and others to new style sticky buffers
Feature # 2914: modernize tls sticky buffers
Bug # 2915: modernize ssh sticky buffers
Feature # 2930: http_protocol: use mpm and content inspect v2 apis

Related issues:

Related to Task #2309: SuriCon 2017 brainstorm
Related to Task #2685: SuriCon 2018 brainstorm
Related to Feature #2952: modernize http_header_names

History

#1 - 11/20/2017 10:03 AM - Victor Julien
- Assignee set to Jason Williams
- Target version set to 70

#2 - 11/20/2017 10:41 AM - Jason Williams

1. flip the proto to the end

- this complicates the naming a little
- breaks the current "proto_buffer"; naming scheme

uri_http;
header_http;
user_agent_http;

2. use similar naming to 'raw'

- a little more typing
- looks fairly similar to what we already have
3. put sticky at the end

- not a naming convention we have currently

http_uri_sticky;
http_header_sticky;
http_user_agent_sticky;

4. let suricata decide the function of the buffer

- this could possibly complicate the engine's parsing of the rules
  - cleanest

content: "example"; http_uri; (old - modifier)
http_uri; content: "example"; (new - sticky)

#3 - 12/01/2017 05:05 AM - Victor Julien
- Related to Task #2309: SuriCon 2017 brainstorm added

#4 - 04/14/2018 07:46 PM - Jason Williams
After some time thinking about this, perhaps the initial 'http' portion of the buffer name is not needed?

our rule is already 'alert http...'

http_uri; -> uri;
http_user_agent; -> user_agent;
http_referer; -> referer;

#5 - 11/24/2018 09:48 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#6 - 03/04/2019 10:45 AM - Victor Julien
- Description updated

- Assignee changed from Jason Williams to OISF Dev
- Target version changed from 70 to 5.0beta1

#7 - 04/29/2019 09:03 AM - Victor Julien
- Target version changed from 5.0beta1 to 5.0rc1

#8 - 05/06/2019 05:52 AM - Victor Julien
- Status changed from New to Closed

https://github.com/OISF/suricata/pull/3826

#9 - 05/06/2019 05:52 AM - Victor Julien
- Related to Feature #2952: modernize http_header_names added