**Suricata - Feature #2198**

Extend the DNS parser to accept `dns_response` keyword in signatures

08/03/2017 07:01 AM - Anonymous

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
</tbody>
</table>

**Description**

For A and AAAA records it would be interesting to match on the IP received from the DNS resolver. In particular this could be useful to check for potentially sink-holed domains.

**Related issues:**

- Related to Feature #2448: Add additional buffers for DNS Responses
  - New

**History**

#1 - 08/04/2017 04:09 PM - Andreas Herz
- Tracker changed from Bug to Feature
- Target version changed from 70 to TBD

Since you assigned yourself, do you want to submit that?

#2 - 08/09/2017 03:06 AM - Anonymous

Andreas Herz wrote:

> Since you assigned yourself, do you want to submit that?

Yes, it is in the pipeline.
Do you want me to focus on a Rust implementation?

#3 - 08/10/2017 03:39 PM - Andreas Herz

Depends on what you prefer, IMHO it would be nice to have it in Rust.

#4 - 02/16/2018 03:26 PM - Jason Ish
- Related to Feature #2448: Add additional buffers for DNS Responses added

#5 - 05/24/2019 08:13 AM - Andreas Herz
- Assignee changed from Anonymous to Stian Bergseth

#6 - 09/27/2019 11:03 AM - Victor Julien
- Assignee changed from Stian Bergseth to Community Ticket