Suricata - Feature #3298
Create a config flag in the DNS logger to limit events to only the ones in the custom field
11/01/2019 04:14 PM - Stian Bergseth

<table>
<thead>
<tr>
<th>Status:</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jason Ish</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>low</td>
</tr>
</tbody>
</table>

Label: 

Description
I am currently running Suricata with the following YAML for dns logging:

```yaml
  - dns:
    custom: [a, aaaa, cname]
```

But even with this Suricata logs big zone transfers if any of the records contains A,AAAA or Cname it will log all of it. In big AD environments this will create JSON blobs that are quite big.

History

#1 - 11/01/2019 04:31 PM - Stian Bergseth
Output from suricata --dump-config

```
$ suricata --dump-config | grep dns
outputs.1.eve-log.types.4 = dns
outputs.1.eve-log.types.4.dns = (null)
outputs.1.eve-log.types.4.dns.custom = (null)
outputs.1.eve-log.types.4.dns.custom.0 = a
outputs.1.eve-log.types.4.dns.custom.1 = aaaa
outputs.1.eve-log.types.4.dns.custom.2 = cname
```

#2 - 11/01/2019 04:34 PM - Stian Bergseth
eve.json output from the same host

```
"proto": "TCP",
"dns": {,
  "version": 2,
  "type": "answer",
  "id": 51890,
  "flags": "S400",
  "qr": true,
  "aa": true,
  "rrname": "90.254.202.209.in-addr.arpa",
  "rrtype": "PTR",
  "rcode": "NOERROR",
  "answers": [,
   {
    "rrname": "90.254.202.209.in-addr.arpa",
    "rrtype": "PTR",
    "ttl": 3600,
    "rdata": "advertising.lycos.at"
   },
  ],
```

#3 - 11/02/2019 08:49 AM - Victor Julien
- Status changed from New to Feedback
- Assignee set to Jason Ish

If I understand correct it is unclear if this is a missing feature or a bug in the existing implementation?
I guess it depends a bit. I was under the impression that only the specified lookups/responses in the custom field would be logged (A,AAAA,CNAME in this case), but when DNS response/requests are grouped it will also log other types of DNS records if there is at least one A/AAAA/CNAME in there.

So depending on your point of view on this, is it a bug with the custom field? Or if not, it is a new feature?

In eve dns v2, what is logged depends on the request type. You limit it, so you could only log requests/responses where the type is of "A", and so on. Of course the response can contain a whole lot more than A records.

Also, the v2 output does not support custom. Try "types" (see https://suricata.readthedocs.io/en/suricata-5.0.0/output/eve/eve-json-output.html#dns). Perhaps custom should be a hidden alias for types as this could be a common mistake for people upgrading from older versions.

Stian: Can you retest after changing "custom" to "types"?