Passive DNS SIG updates

SIG chairs:

Aaron Kaplan aaron@lo-res.org

Alexandre Dulaunoy alexandre.dulaunoy@circl.lu

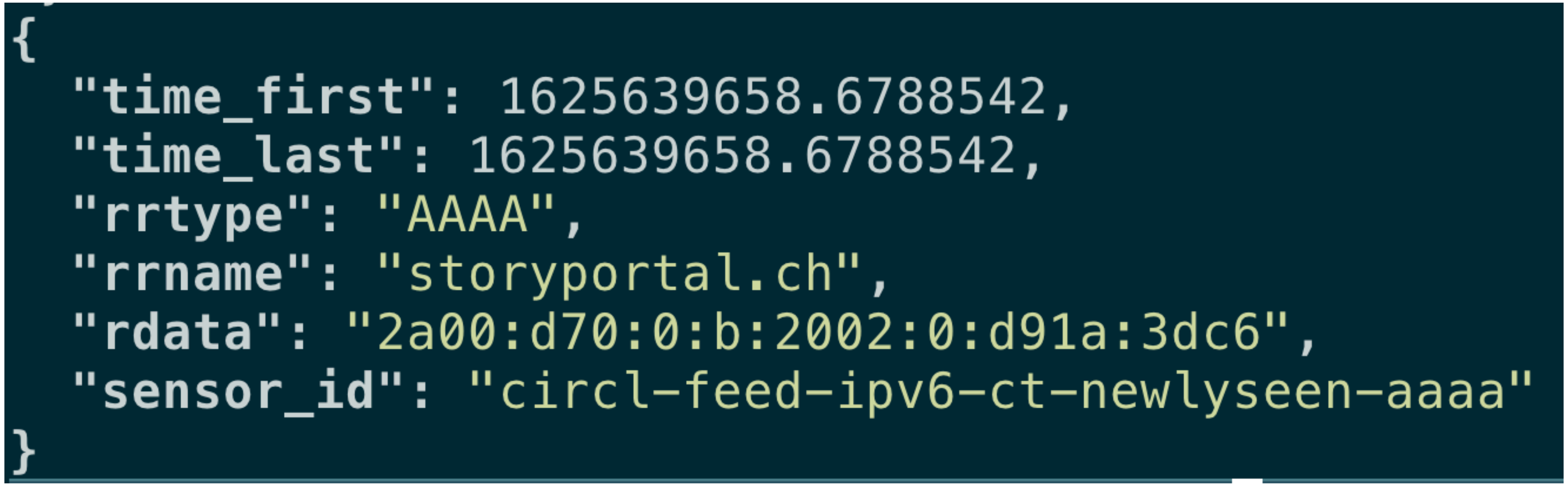
Paul Vixie vixie@sie-europe.net

History

- Passive DNS – what is it?
- At around 2009/2010 multiple implementations
- Every pDNS server seens only a part of the whole DNS traffic
- Idea: create a **C**ommon **O**utput **F**ormat **(COF)** for querying different pDNS servers
- Get together Paul Vixie, Henry Stern, Alexandre Dulaunoy, Aaron Kaplan → SIG created
- Nine version iteratons of the standard

Example COF message

- It’s a simple JSON format, contains the most relevant fields.
- Interchangeable !
- Example:



```
{
  "time_first": 1625639658.6788542,
  "time_last": 1625639658.6788542,
  "rrtype": "AAAA",
  "rrname": "storyportal.ch",
  "rdata": "2a00:d70:0:b:2002:0:d91a:3dc6",
  "sensor_id": "circl-feed-ipv6-ct-newlyseen-aaaa"
}
```

Status quo

Standard

- We are an **”active internet draft (individual submission in DNSOP)”.**
- https://datatracker.ietf.org/doc/draft-dulaunoy-dnsop-passive-dns-cof/
- Sending to the editor

Tools

- Tool to query different servers (**`dnsdbq`**): https://github.com/dnsdb/dnsdbq
- MISP module: cof2misp: import pDNS into MISP
- Used for streaming JTAN the result of DNS resolutions
- Standard widely deployed amongst pDNS server operators
- Inclusion into D4 (CIRCL)

Summary - status quo

- Standard is **STABLE** ✓ Sending to the editor
- It is used and usable ✓
- Implemented by:
  - Farsight / Domaintools
  - CIRCL pDNS
  - CERT.at
  - Balboa
  - D4 project
  - mnemonic
  - **You**? → we would like to hear from you! PR to https://github.com/adulau/pdns-qof

Future

- DNSTAP 2 COF: in the making

- Standardize RESTful API endpoint specs (== the query)?
- Standardize sensor to DB format?
- Make a sensor to DB sharing “switch”

- **Your ideas?**

Contact

- Mail the SIG chars
- In FIRST’s **slack**: **#passive-dns-sig**