

Team CIRCL

<https://www.d4-project.org/>

2019/03/29

Alexandre Dulaunoy

d4-lo

- CIRCL (and other CSIRTs) have their own passive DNS<sup>1</sup> collection mechanisms
- Current **collection models** are affected with DoH<sup>2</sup> and centralised DNS services
- DNS answers collection is a tedious process
- **Sharing Passive DNS stream** between organisation is challenging due to privacy

---

<sup>1</sup><https://www.circl.lu/services/passive-dns/>

<sup>2</sup>DNS over HTTPS

- Improve **Passive DNS collection diversity** by being closer to the source and limit impact of DoH (e.g. at the OS resolver level)
- Increasing diversity and **mixing models** before sharing/storing Passive DNS records
- Simplify process and tools to install for **Passive DNS collection by relying on D4 sensors** instead of custom mechanisms
- Provide a distributed infrastructure for mixing streams and filtering out the sharing to the validated partners

- analyzer-d4-passivedns<sup>3</sup> is an analyzer for a D4 network sensor. The analyser can process data produced by D4 sensors (in passivedns CSV format<sup>4</sup>)
- Ingest these into a **Passive DNS server** which can be queried later to search for the Passive DNS records
- The lookup server (using on redis-compatible backend) is a Passive DNS REST server compliant to the Common Output Format<sup>5</sup>

---

<sup>3</sup><https://github.com/D4-project/analyzer-d4-passivedns>

<sup>4</sup><https://github.com/gamlinux/passivedns>

<sup>5</sup><https://tools.ietf.org/html/draft-dulaunoy-dnsop-passive-dns-cof-04>

d4-overview.pdf

# COMMON OUTPUT FORMAT

- **Consistent naming of fields across Passive DNS software**  
based on the most common Passive DNS implementations
- Minimal set of fields to be supported
- Minimal set of optional fields to be supported
- Way to add "additional" fields via a simple registry mechanism (IANA-like)
- Simple and easily parsable format
- A gentle reminder regarding privacy aspects of Passive DNS

# SAMPLE OUTPUT WWW.TERENA.ORG

```
1 {"count": 868, "time_first": 1298398002, "rrtype": "A", "
   rrtype": "A", "rrname": "www.terena.org", "rdata": "192.87.30.6", "
   time_last": 1383124252}
2 {"count": 89, "time_first": 1383729690, "rrtype": "CNAME",
   "rrtype": "CNAME", "rrname": "www.terena.org", "rdata": "godzilla.terena.
   org", "time_last": 1391517643}
3 {"count": 110, "time_first": 1298398002, "rrtype": "AAAA",
   "rrtype": "AAAA", "rrname": "www.terena.org", "rdata": "2001:610:148:dead
   ::6", "time_last": 136670845}
```

## MANDATORY FIELDS

- **rrname** : name of the queried resource records
  - ▶ JSON String
- **rrtype** : resource record type
  - ▶ JSON String (interpreted type of resource type if known)
- **rdata** : resource records of the query(ied) resource(s)
  - ▶ JSON String or an array of string if more than one unique triple
- **time\_first** : first time that the resource record triple (rrname, rrtype, rdata) was seen
- **time\_last** : last time that the resource record triple (rrname, rrtype, rdata) was seen
  - ▶ JSON Number (epoch value) UTC TZ



## OPTIONAL FIELDS

- **count** : how many authoritative DNS answers were received by the Passive DNS collector
  - ▶ JSON Number
- **bailiwick** : closest enclosing zone delegated to a nameserver served in the zone of the resource records
  - ▶ JSON String

## ADDITIONALS FIELDS

- **sensor\_id** : Passive DNS sensor information
  - ▶ JSON String
- **zone\_time\_first** : specific first/last time seen when imported from a master file
- **zone\_time\_last**
  - ▶ JSON Number
- Additional fields can be requested via <https://github.com/adulau/pdns-qof/wiki/Additional-Fields>

- **Mixing models for passive DNS stream** (for privacy) in next version of D4 core server
- Interconnecting private D4 sensor networks with other D4 sensor networks (sharing to partners filtered stream)
- Previewing dataset collected in D4 sensor network and providing **open data stream** (if contributor agrees to share under specific conditions)

# GET IN TOUCH IF YOU WANT TO JOIN/SUPPORT THE PROJECT, HOST A PASSIVE DNS SENSOR OR CONTRIBUTE

- Collaboration can include research partnership, sharing of collected streams or improving the software.
- Contact: [info@circl.lu](mailto:info@circl.lu)
- <https://github.com/D4-Project> -  
[https://twitter.com/d4\\_project](https://twitter.com/d4_project)