Passive DNS - Common Output Format

Current state of the Internet-Draft

CIRCL
Computer Incident
Response Center
Luxembourg

CERT.at

TLP:WHITE

alexandre.dulaunoy@circl.lu
kaplan@cert.at

February 11, 2014

Background and History

- In 2005, Florian Weimer described Passive DNS replication at the 17th FIRST annual conference
- Nowadays Passive DNS software are created[1] and used worldwide
- In 2011, we started to work on a common output format for Passive DNS systems at the FIRST annual conference
- After discussions with many authors of passive DNS, version 02 of the internet-draft is published

[1] To our knowledge, there are more than 15 software implementations

Main objectives of the internet-draft

- 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

```
{"count": 868, "time_first": 1298398002, "rrtype": "A", "rrname": "www.terena.org", "rdata": "192.87.30.6", "time_last": 1383124252}
{"count": 89, "time_first": 1383729690, "rrtype": "CNAME", "rrname": "www.terena.org", "rdata": "godzilla.terena.org", "time_last": 1391517643}
{"count": 110, "time_first": 1298398002, "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`

Future works

- IETF 89 London to review the internet-draft with the dnsop WG
- Incorporate all the comments and feedback from recently discovered Passive DNS (servers/clients) developers
- Expand the sample implementations to help developers to support the format
- An internet-draft for the query interface to Passive DNS systems is under preparation

Contact

- `https://datatracker.ietf.org/doc/draft-dulaunoy-kaplan-passive-dns-cof/`
- Don't hesitate to contact us. Feedback and updates are welcomed:
- alexandre.dulaunoy@circl.lu - CIRCL
- kaplan@cert.at - CERT.at
- paul@redbarn.org - Farsight Security, Inc
- henry@stern.ca - Farsight Security, Inc.