Passive DNS

Using the DNS for fun and profit

Alexandre Dulaunoy

November 28, 2014

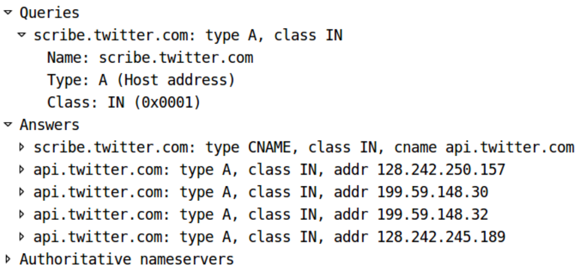
Domain Name Space and Structure 1/3

- The domain name space is structured in a tree.
- The DNS root zone is at the top and provide information on how to reach top-level domains (ccTLD, gTLD).
- Security is limited and DNSSEC is not currently largely deployed.

Name Servers Roles 2/3

- Authoritative name server
  - Give answers about domain name configured by the local name administrator.
- Recursive and caching name server
  - They recursively lookup domains by querying and caching to/from authoritative name server.
- It's recommended to keep separated the authoritative name server from the recursive name server.

DNS Protocol 3/3



```
▿ Queries
  ▿ scribe.twitter.com: type A, class IN
      Name: scribe.twitter.com
      Type: A (Host address)
      Class: IN (0x0001)
▿ Answers
  ▹ scribe.twitter.com: type CNAME, class IN, cname api.twitter.com
  ▹ api.twitter.com: type A, class IN, addr 128.242.250.157
  ▹ api.twitter.com: type A, class IN, addr 199.59.148.30
  ▹ api.twitter.com: type A, class IN, addr 199.59.148.32
  ▹ api.twitter.com: type A, class IN, addr 128.242.245.189
▹ Authoritative nameservers
```

- DNS uses UDP or TCP over port 53. The core element for the DNS procotol is the RR (Resource Record). Each record is composed of various fields: NAME, TYPE, CLASS, TTL, RDLENGTH and RDATA.

DNS and Security?

- Everyone relies on DNS on Internet even malware.
- Can we monitor DNS passively to discover malware infection or limiting its impact?
  - First passive DNS implemented in 2004 by Florian Weimer.
  - Discovering of malware fast-flux domains, malicious domains/IP, hijacked domains...
  - Privacy is critical when doing passive DNS.

DNS and Security - Quick Workshop

- From simple DNS monitoring (tshark -r capture.cap -n -Tfields -e dns.qry.name) to dnscap (https://github.com/adulau/dnscap).
- Can you use the DNS queries/answers for network forensic analysis (use the initial pcap file)?
- Using Passive DNS services and how this can help for network forensic analysis

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`

Bibliography

- DNS and BIND, Fifth Edition, Cricket Liu, Paul Albitz.
- Passive Monitoring of DNS Anomalies, Bojan Zdrnja , Nevil Brownlee , and Duane Wessels.
- Passive DNS - Common Output Format `https://datatracker.ietf.org/doc/draft-dulaunoy-kaplan-passive-dns-cof/`

Q and A

- Thanks for listening.