

How to build a scalable passive DNS using a key/value data structure "designed" in 5 minutes



CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy

February 17, 2012

DNS and Security?

- Everyone relies on DNS on Internet and often your friendly malware
- Can we monitor passively DNS 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 and DNS don't mixup very well (in other words, it sucks)
 - What are the changes of a DNS record over time?

The 5 minutes "design"

- I'm lazy, the dirty job of DNS decoding is done by ISC dnscap tool
- I hate slow disk access, the database must stay in memory
- I hate large piece of code, the implementation must be modular and having less than 5K LOC (↓ trash and rewrite cost)
- I hate those bloody legal documents, we keep only the DNS answers (no queries or source IP addresses stored)

A sample DNS answer

- ▼ 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

The 5 minutes Redis data structure

