SwiNOG #30
4 November 2016
Gurtenpark, Bern, Switzerland

The DNS Toolkit

All the fun one can have with DNS

Jeroen Massar
massar@fsi.io

FARSIGHT SECURITY

FARSIGHT SECURITY

Farsight Security, Inc.

- https://www.farsightsecurity.com
- Founded by Dr. Paul Vixie and Dr. Paul Mockapetris
- Team based in US, Canada, Poland and Switzerland
- Security defense and insight based on DNS
- Projects:
  - SIE (Security Information Exchange)
  - DNSDB (DNS Database)
  - NOD (Newly Observed Domains)
  - Domain Sentry, Brand Sentry
  - and more…
- This Talk:
  - RRL – Response Rate Limiting
  - DNS Query Collection (Logging, PassiveDNS, dnstap)
  - DNSDB – DNS Database
  - NOD – Newly Observed Domains

FARSIGHT SECURITY

Anti-Spoof: Where are your MANRS?

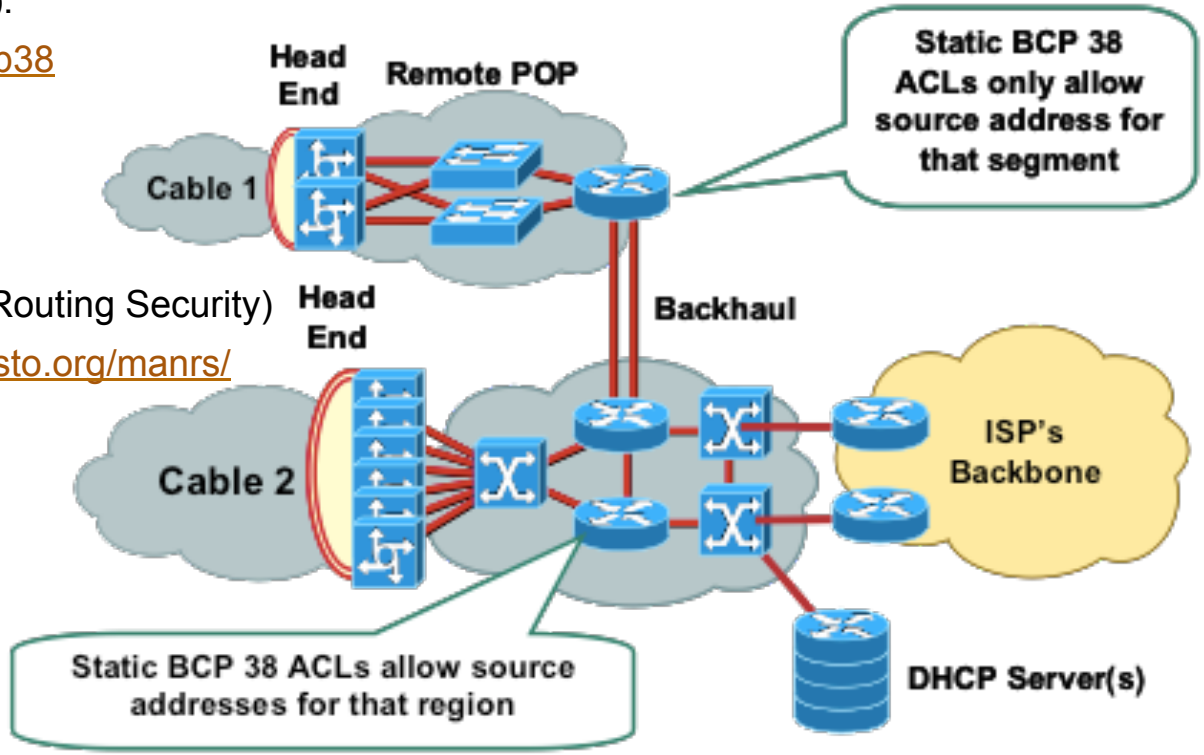
Good old BCP38 (year 2000):

- http://tools.ietf.org/html/bcp38
- http://www.bcp38.info

MANRS

(Mutually Agreed Norms for Routing Security)

- https://www.routingmanifesto.org/manrs/



RRL: Response Rate Limiting

FARSIGHT SECURITY

- Large DDoS attacks are common and big as amplification factor is large, as large number of open DNS recursors, large number of networks that allow spoofing (recent attacks with Mirai where btw not spoofed – do you NetFlow?)
- NTP is not alone, SNMP and DNS…
- RRL Limits the number of ***unique responses*** returned by a DNS server per e.g. IPv4 /24, or IPv6 /48
- RRL makes informed decision, simple IP-based rate limiting would just *randomly drop* queries
- Implemented in: NSD, BIND, Knot, more coming
- Design & Implementation: Paul Vixie & Vernon Schryver
- More details: http://www.redbarn.org/dns/ratelimits

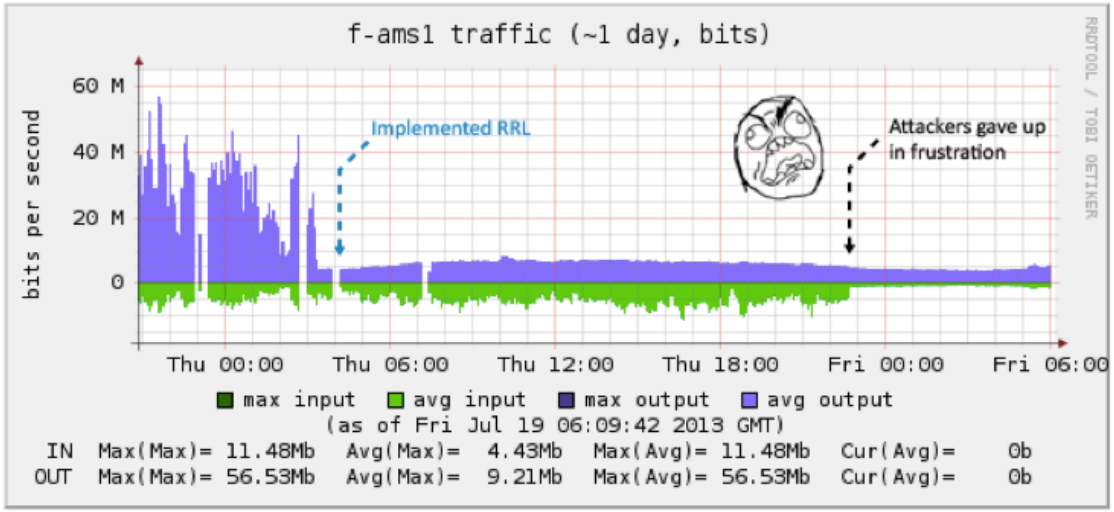
RRL: Example BIND & Knot

BIND

```
rate-limit {
        responses-per-second 200;
        window 2;
    };
```

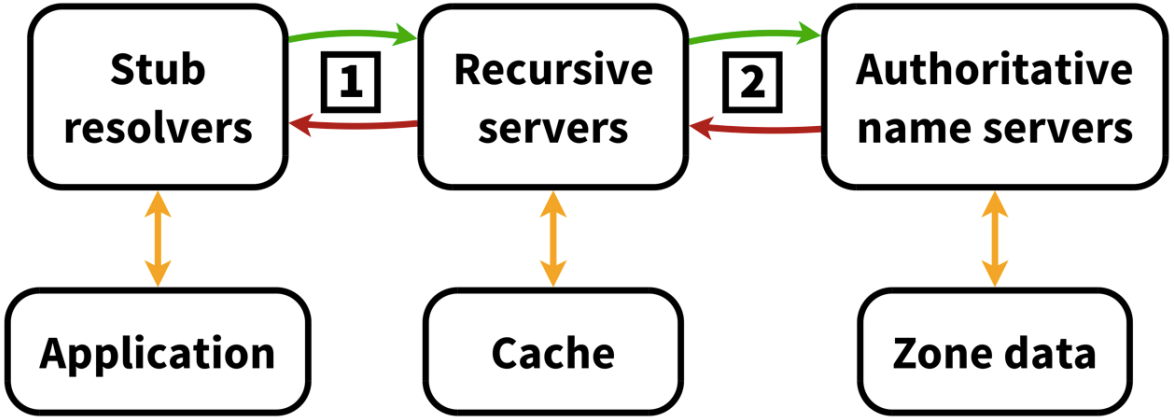
Knot

```
server:
    rate-limit: 200
    rate-limit-slip: 2
```



DNS Query Collection: Why?

- Useful for determining what sites are visited/looked-up
- Can indicate that a client in the network is connecting to a known C&C Botnet when using DNS – collect, analyze and know!
- Above the recursor: does not collect PII as one does not see Stub's IP address



1) below, 2) above – the recursor

DNS Query Collection: Query Logging

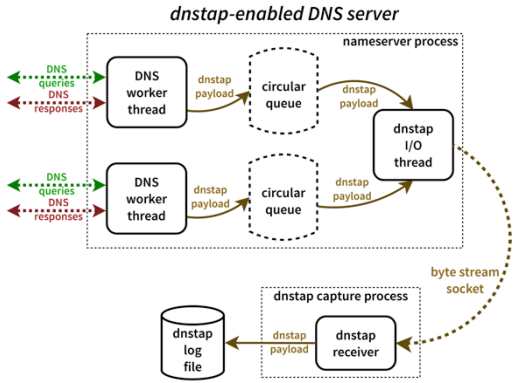
- DNS Server logs queries to disk (file or syslog)
- Slows DNS server itself down as syslog/file-writing is typically a blocking operation
- Text-based, thus requires formatting/parsing and the overhead of ASCII
- Lose all details not logged at that time (DNSSEC flags, cache miss/hit, etc)

DNS Query Collection: Passive DNS

- Use a hub/mirror-port etc. to sniff the interface of the DNS server collection DNS responses
- Full packet details, which need to be parsed
- Requires TCP reassembly and UDP fragment reassembly
- No performance impact on the actual DNS server
- Can be done below and above the recursive

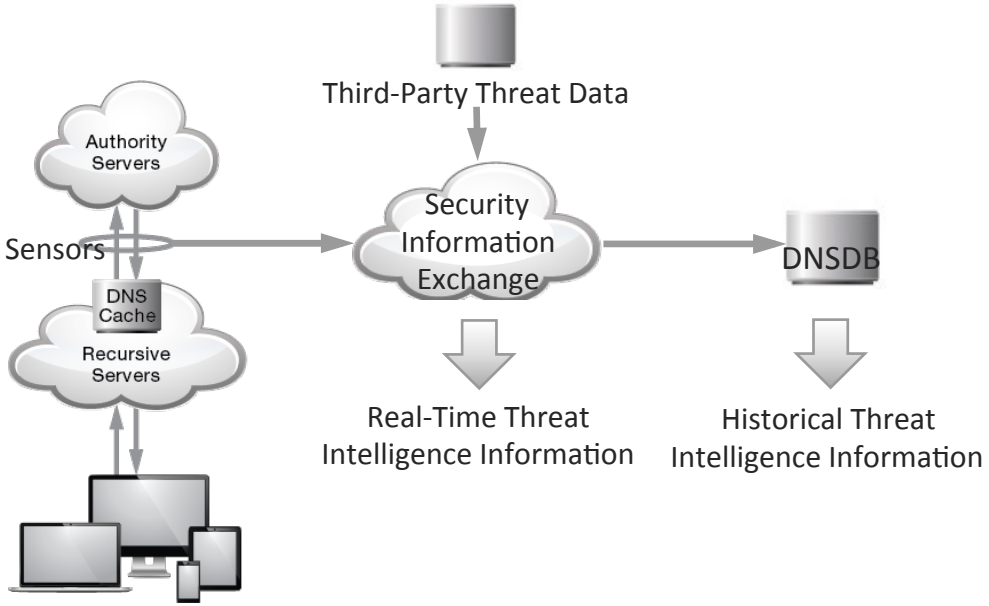
DNS Query Collection: dnstap

- The best of Query Logging + Passive DNS: dnstap
- Patch the DNS server to support logging using dnstap
- Duplicates the internal parsed DNS format message
- Uses circular queues & non-blocking logging techniques: minimal performance hit on DNS server
- Implemented in BIND, Unbound, Knot DNS and more
- Documentation / Tutorials / Mailinglist / Code: http://www.dnstap.info
- Design & Implementation: Robert Edmonds

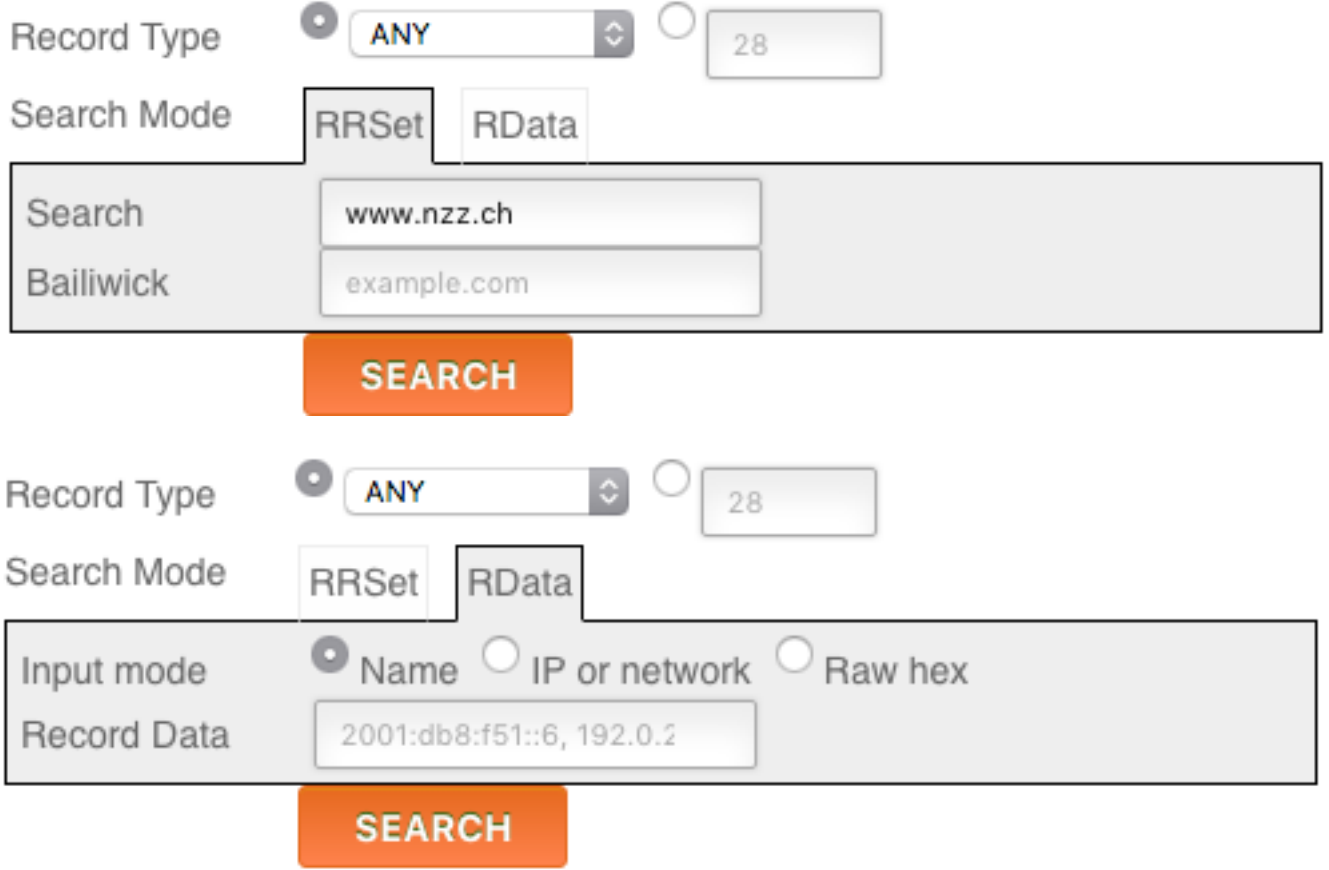


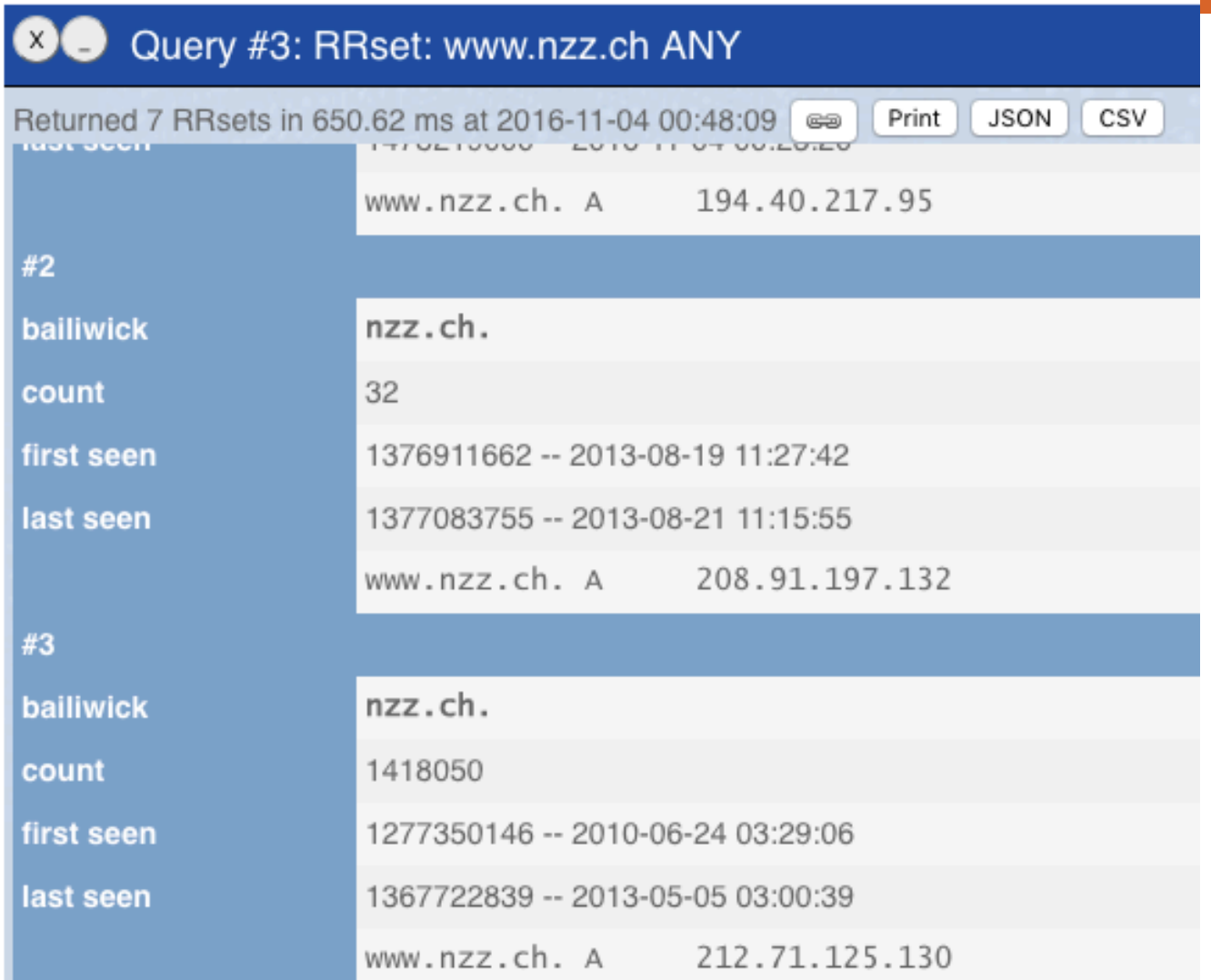
DNSDB: The DNS Database

- Central repository from Passive DNS collectors data
- Web-based query interface @ http://www.dnsdb.info
- API (http://api.dnsdb.info) access for integration in various investigative tools
  - dnsdb-query (Python)
  - dnsdb_c (C ☺)
  - Maltego
  - Splunk
- DNSDB Export: On-premise

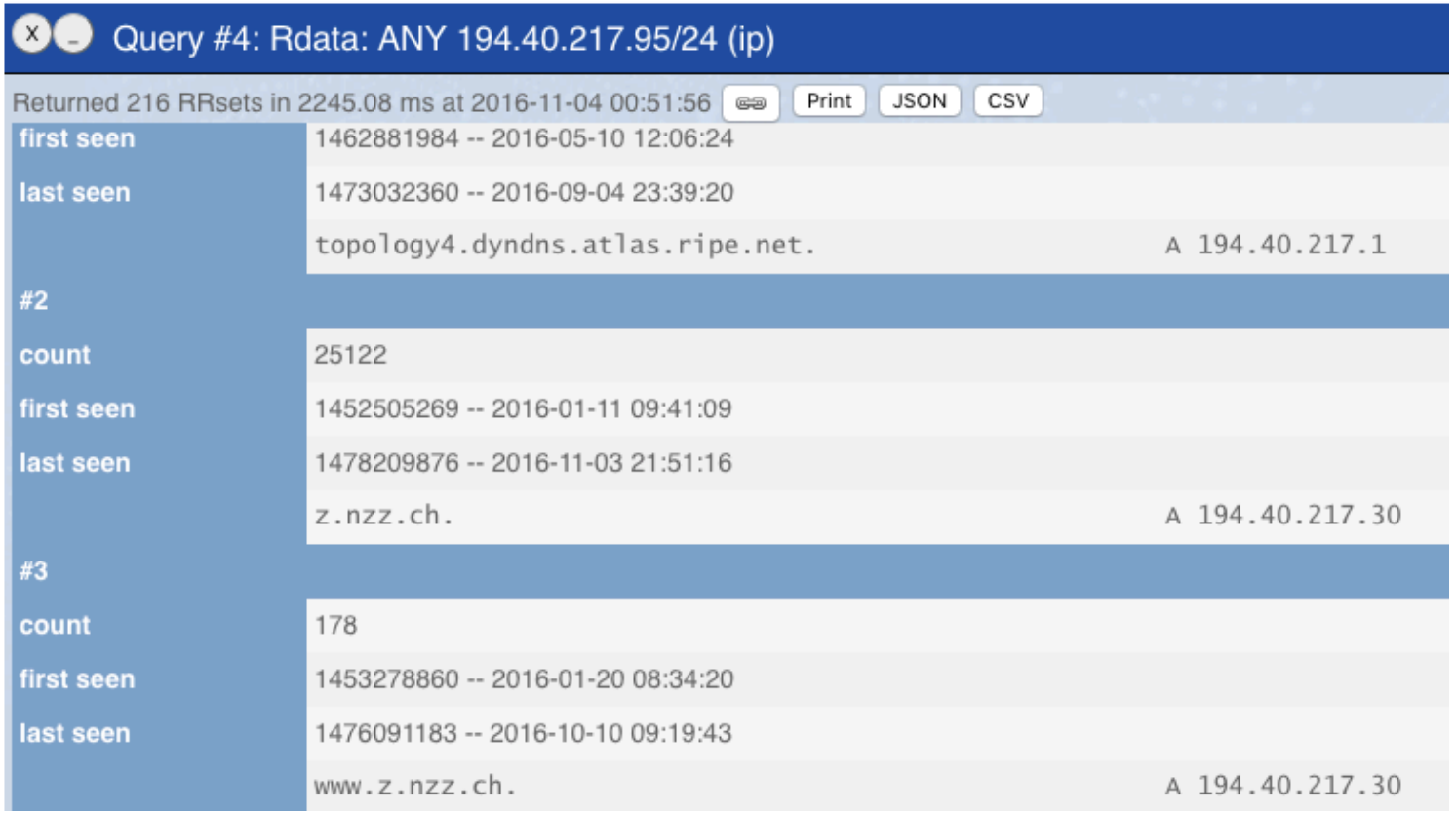


DNSDB Web Interface




Query #3: RRset: www.nzz.ch ANY
Returned 7 RRsets in 650.62 ms at 2016-11-04 00:48:09
Print
JSON
CSV
www.nzz.ch. A 194.40.217.95
#2
bailiwick nzz.ch.
count 32
first seen 1376911662 -- 2013-08-19 11:27:42
last seen 1377083755 -- 2013-08-21 11:15:55
www.nzz.ch. A 208.91.197.132
#3
bailiwick nzz.ch.
count 1418050
first seen 1277350146 -- 2010-06-24 03:29:06
last seen 1367722839 -- 2013-05-05 03:00:39
www.nzz.ch. A 212.71.125.130

FARSIGHT SECURITY



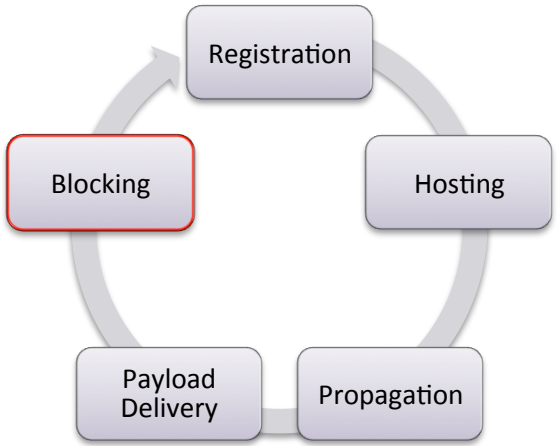
Query #4: Rdata: ANY 194.40.217.95/24 (ip)

Returned 216 RRsets in 2245.08 ms at 2016-11-04 00:51:56 [Print] [JSON] [CSV]

first seen	1462881984 -- 2016-05-10 12:06:24	
last seen	1473032360 -- 2016-09-04 23:39:20	
	topology4.dyndns.atlas.ripe.net.	A 194.40.217.1
#2		
count	25122	
first seen	1452505269 -- 2016-01-11 09:41:09	
last seen	1478209876 -- 2016-11-03 21:51:16	
	z.nzz.ch.	A 194.40.217.30
#3		
count	178	
first seen	1453278860 -- 2016-01-20 08:34:20	
last seen	1476091183 -- 2016-10-10 09:19:43	
	www.z.nzz.ch.	A 194.40.217.30

NOD: Newly Observed Domains

- One can get ‘new’ domains from Zone File Access (ZFA) as provided by TLD operators (as per ICANN Base Registry Agreement)
- But ZFA is not available for e.g. ccTLDs, .mil / .gov and badly managed ones
- ZFA is only published every 24 hours
  - Might miss domains that are registered and removed inside that period again (eg domain tasting)
- With the help of DNSDB, as it knows what is being queried:
  - If domain not seen for last 10 days: Newly Observed Domain!
- NOD is published as RPZ zone, RBL zone or SIE channel 212
  - With RPZ: one can block or CNAME new domains to a safe place
  - Easily Integrate into SpamAssassin and other tools



FARSIGHT SECURITY

RPZ: Response Policy Zones

FARSIGHT SECURITY

- Website with more details: http://www.dnsrpz.info
- Also dubbed “DNS Firewalls”
- Rules are carried in standard DNS zones
- Using IXFR, NOTIFY, TSIG zone updates are distributed automatically and efficiently to stealth secondaries
- Depending on rule, a different response might be returned than the real one

RPZ: Rule Types

Rules:

- If the name being looked up is W.
- If the response contains any IP address in range X.
- If a listed name server name is Y.
- If any returned name server IP address is in range Z.

RPZ: Actions

- Synthesize NXDOMAIN.

```
www.infected.example.@ CNAME .
```

- Synthesize NODATA:

```
www.infected.example.@ CNAME *.
```

- Synthesize an answer.

```
www.infected.example.@ CNAME
www.antivirus.example.
www.malificent.example.@ AAAA 2001:db8::42
```

- Answer with the truth by not having an entry.

RPZ: Examples

FARSIGHT SECURITY

BIND configuration options to enable 4 RPZ feeds:

```
response-policy {
     zone "rpz.deteque.com”;
     zone “rpz.surbl.org”;
     zone “rpz.spamhaus.org”;
     zone “rpz.iidrpz.net”;
};
```

Note that RPZ servers are ACLd, hence need permission of operator to get access to the data

FARSIGHT SECURITY