ENOG-7

27 May 2014

Moscow Marriott Grand Hotel, Moscow, Russia

A watchful eye on DNS

Jeroen Massar, Farsight Security, Inc.
massar@fsi.io

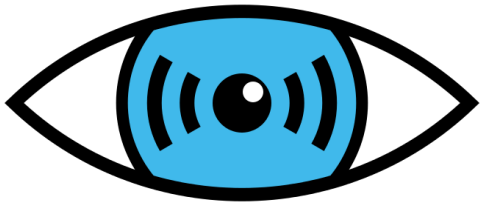
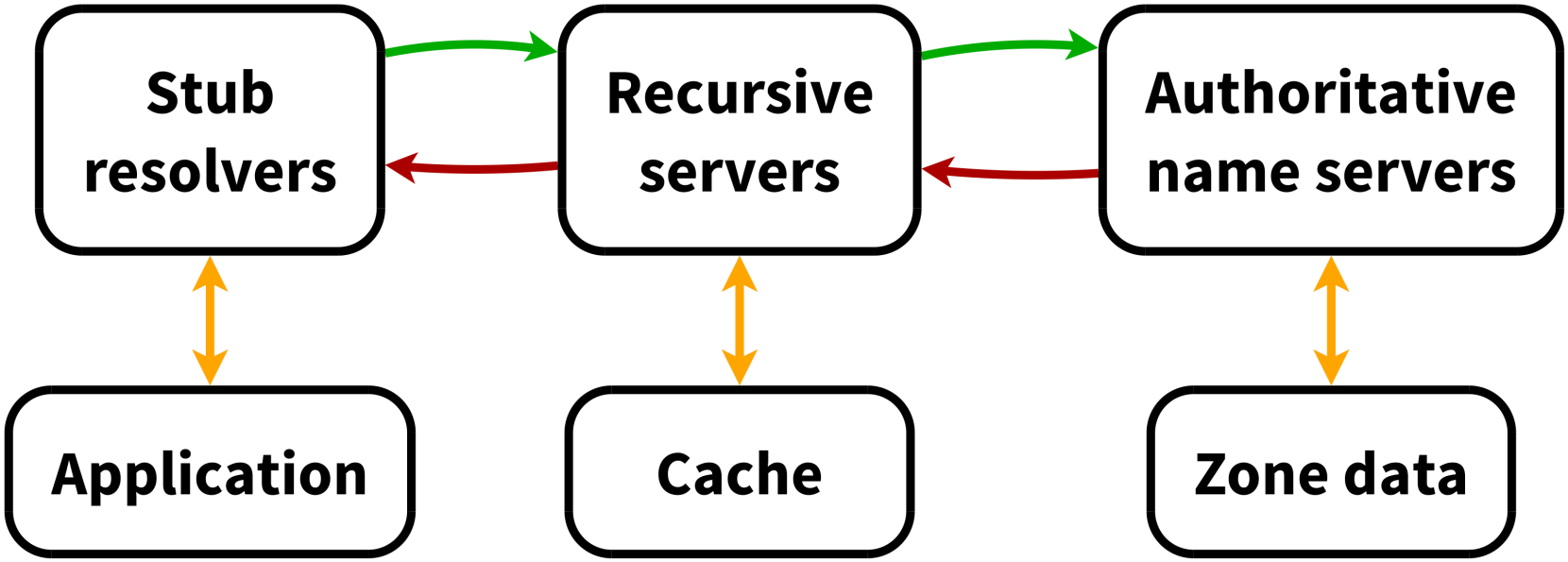


Image: http://www.wwfblogs.org/climate/sites/default/files/kremlin.jpg

Farsight Security, Inc.

- http://www.farsightsecurity.com
- CEO: Dr. Paul Vixie
- Team based in US, Canada and Switzerland
- Security defense and insight based on DNS
- Major projects:
  - SIE (Security Information Exchange)
  - DNSDB (DNS Database)

Simplified DNS Overview



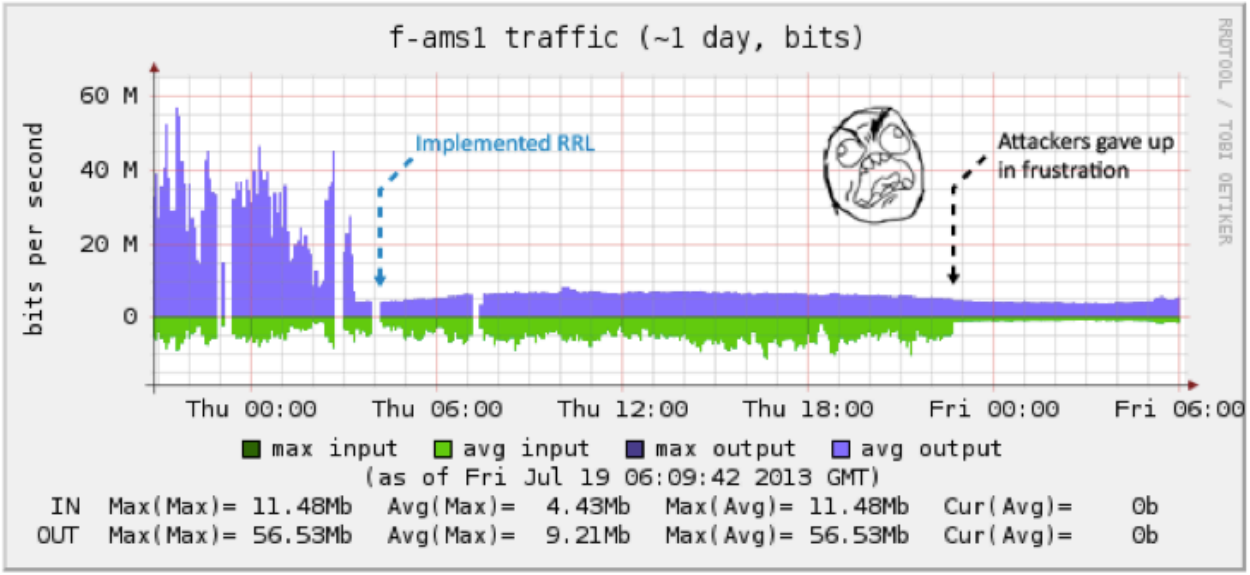
Response Rate Limiting (RRL)

- NTP DDoS attacks are common and big as amplification factor is large, large number of open recursors, large number of networks that allow spoofing
- RRL Limits the number of ***unique responses*** returned by a DNS server per eg 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
- Credits: Paul Vixie & Vernon Schryver
- More details: http://www.redbarn.org/dns/ratelimits

RRL Example

BIND Configuration in options section of configuration:

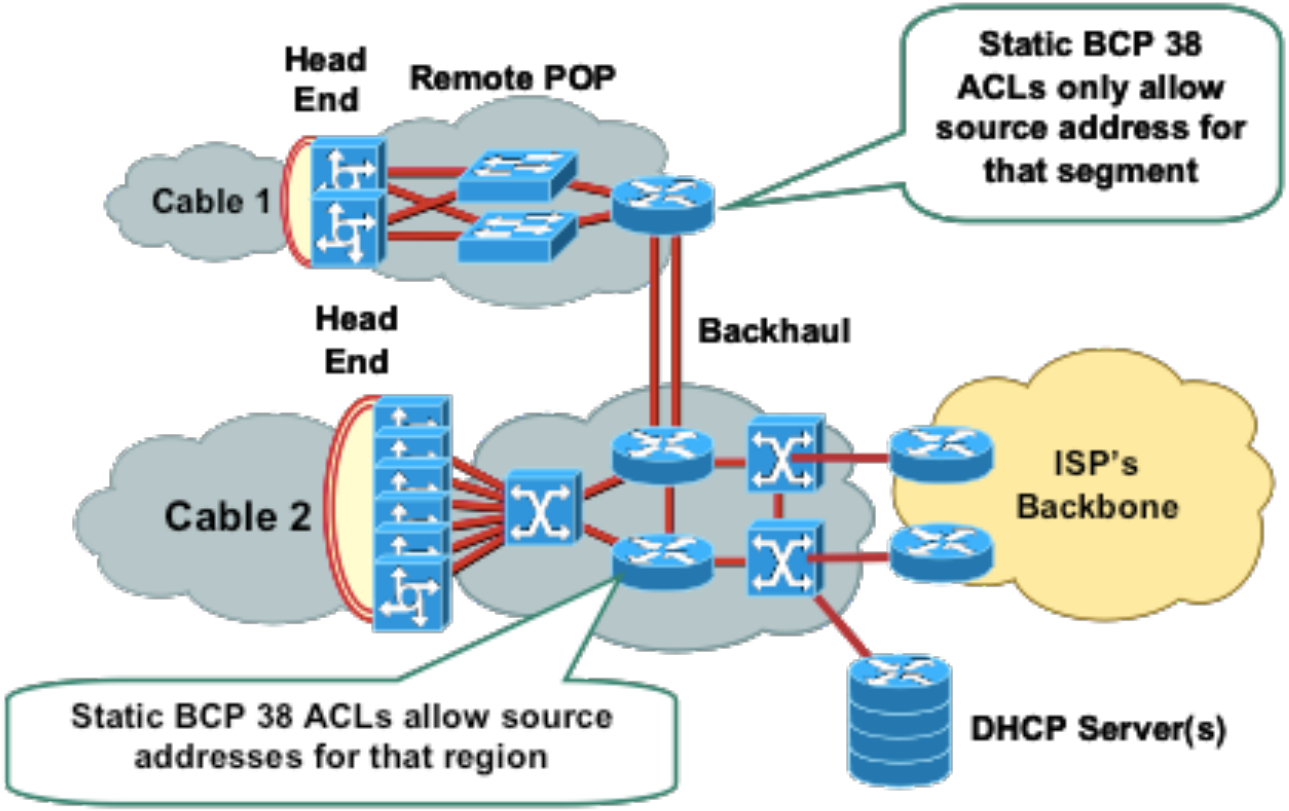
```
rate-limit {
                responses-per-second 15;
                window 5;
        };
```



Graph courtesy of Peter Losher / ISC F-Root, when they enabled RRL on their Amsterdam node

BCP38

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



Response Policy Zone (RPZ)

- 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

BIND configuration options to enable 3 RPZ feeds:

```
response-policy {
        zone "dns-policy.vix.com";
        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

DNS Query collection

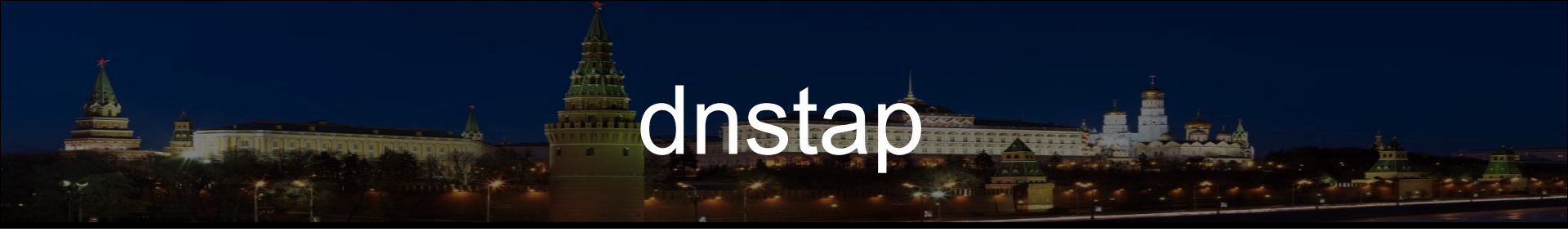
- Useful for determining what sites are visited/looked-up
- Can indicate that a client in the network is connecting to a known C&C Botnet when using DNS

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

Passive DNS

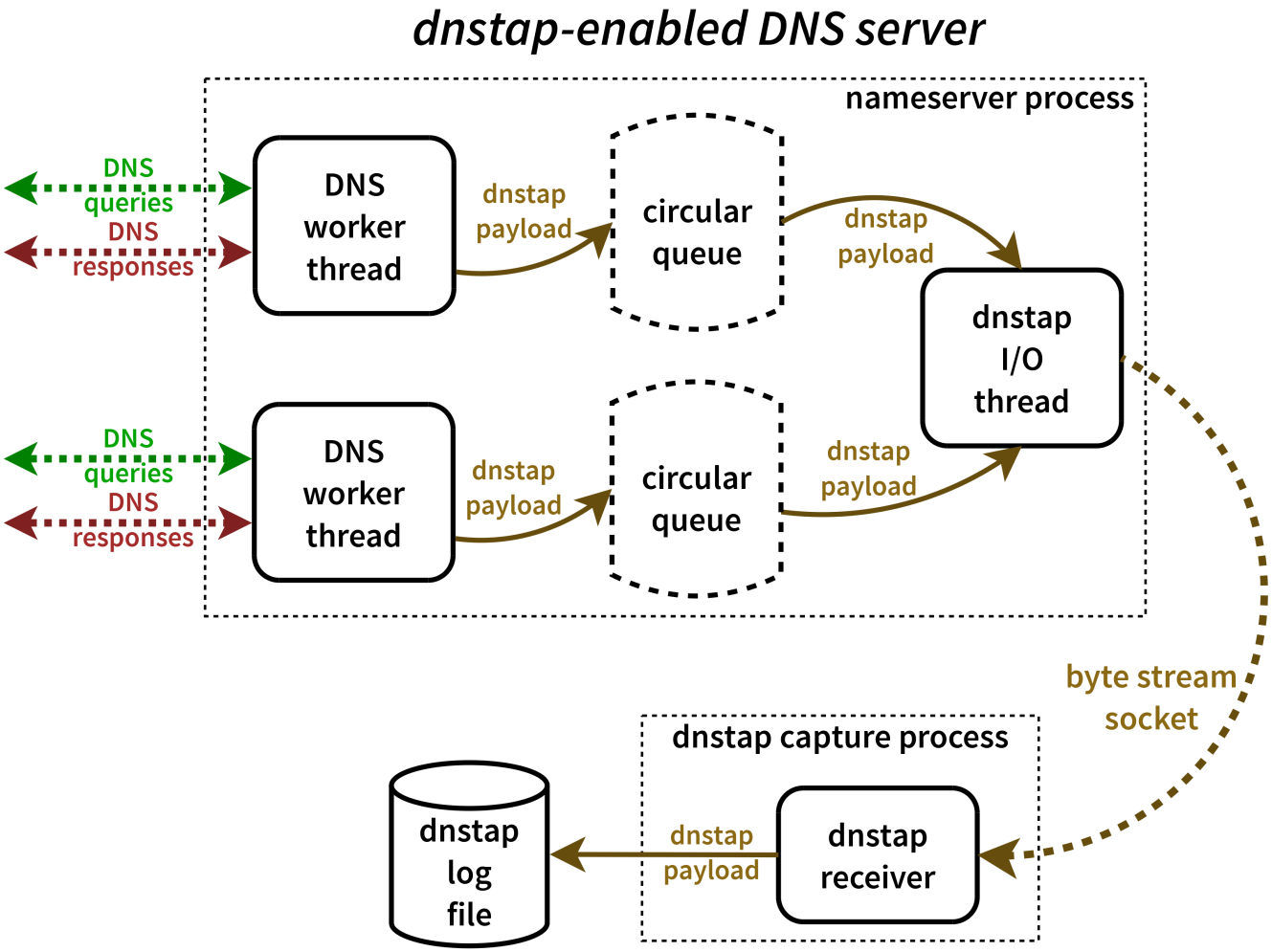
- Use a hub/mirror-port etc to sniff the interface of the DNS server collection DNS responses
- Full packet details, which need to be parsed
- Requires TCP reassembly and UDP fragment reassembly
- No performance impact on the actual DNS server
- Can be done below and above the recursive



dnstap

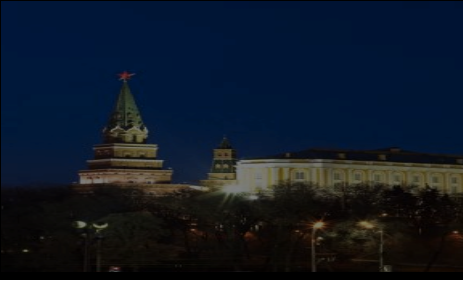
- The best of Query Logging + Passive DNS: dnstap
- Patch the DNS server to support logging using dnstap
- Duplicates the internal parsed DNS format message
- Uses circular queues & non-blocking logging techniques: minimal performance hit on DNS server
- Implemented in Bind, Unbound, Knot DNS and more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

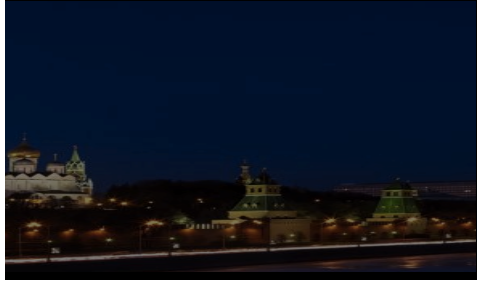
DNSTap Big Overview



DNS Database (DNSDB)

- Central repository from Passive DNS collectors data
- Web-based query interface
- API access for integration in various investigative tools
- http://www.dnsdb.info / http://api.dnsdb.info





Returned 3 RRsets in 0.06 seconds.

bailiwick	**cisco.com.**
count	84476
first seen	2013-01-13 04:35:10 -0000
last seen	2014-04-06 09:51:13 -0000
`cisco.com.`	`A` `72.163.4.161`

bailiwick	**cisco.com.**
count	1
first seen	2012-03-12 21:30:34 -0000
last seen	2012-03-12 21:30:34 -0000
`cisco.com.`	`A` `172.19.25.68`
`cisco.com.`	`A` `198.133.219.25`

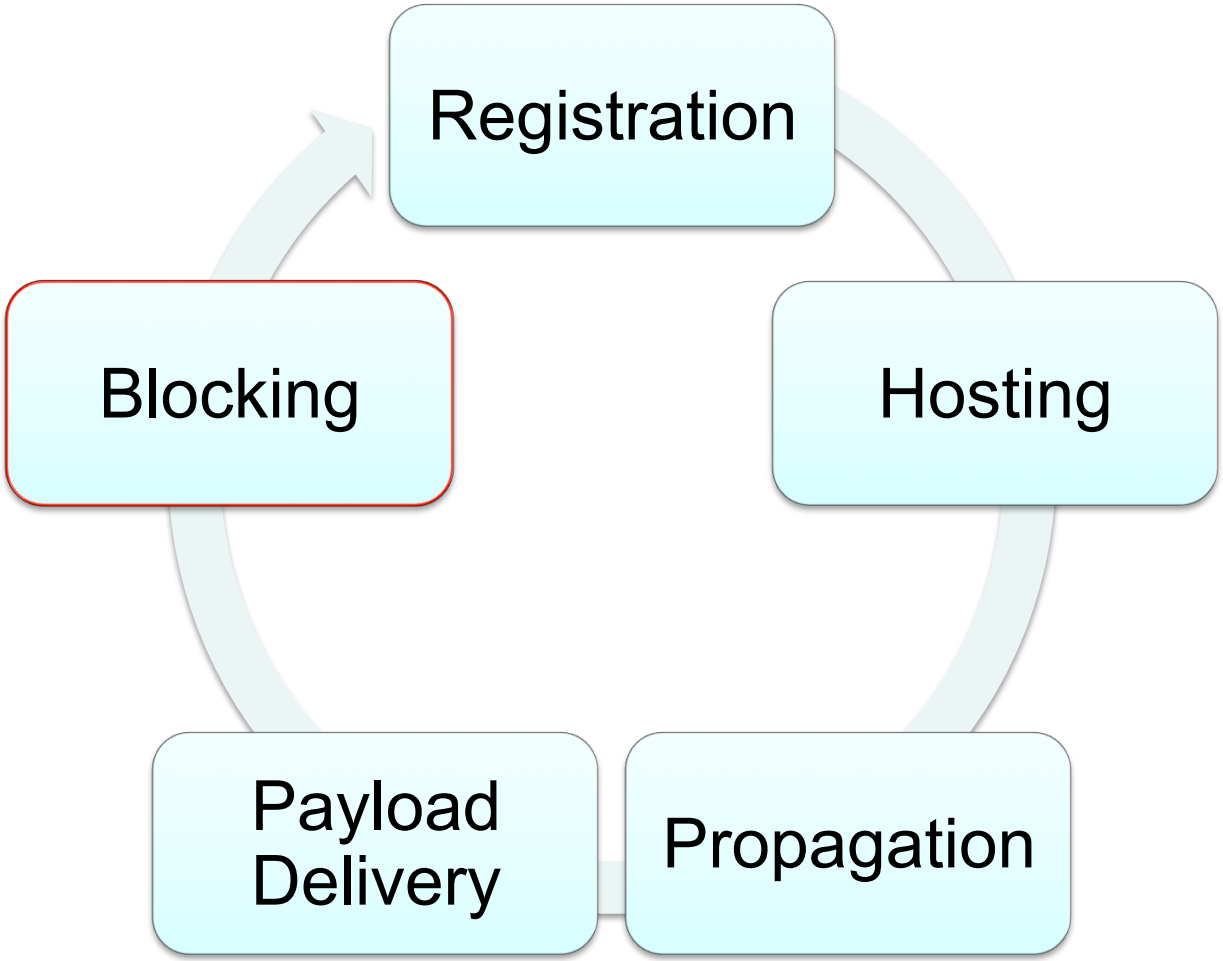
bailiwick	**cisco.com.**
count	150120
first seen	2010-06-24 04:48:14 -0000
last seen	2013-01-13 04:16:48 -0000
`cisco.com.`	`A` `198.133.219.25`

Rdata results for **ANY/198.133.219.25**

Returned 29 RRs in 0.03 seconds.

cisco-systems.se.	A	198.133.219.25
www.cisco-systems.se.	A	198.133.219.25
cisco.ba0.biz.	A	198.133.219.25
cisco.biz.	A	198.133.219.25
2mul.com.	A	198.133.219.25
www.2mul.com.	A	198.133.219.25
cisco.com.	A	198.133.219.25
www9.cisco.com.	A	198.133.219.25
origin-www.cisco.com.	A	198.133.219.25
conft.com.	A	198.133.219.25
auswan.com.	A	198.133.219.25
tivella.com.	A	198.133.219.25
netsolve.com.	A	198.133.219.25
cisconokia.com.	A	198.133.219.25

Malicious Domains Lifecycle



Newly Observed Domains

- Zone File Access (ZFA) as provided by TLD operator (ICANN Base Registry Agreement)
- ZFA is not available for eg ccTLDs, .mil etc
- ZFA is only published every 24 hours
- Might miss domains that are registered and removed inside that period again (eg domain tasting)
- Hence: look at DNSDB, as it knows what is being queried. If domain not seen for last 10 days: Newly Observed Domain!
- Newly Observed Domains (NOD) are published as RPZ zone

Questions?

Jeroen Massar

massar@fsi.io

http://www.farsightsecurity.com/