Using a DNS Response Policy Zone to protect against malware

UKNOF-39
17 January 2018

James Richards
Nominet

DNS Response Policy Zone

RPZ Basics

Blocking and Whitelisting

Monitoring and Analysis

RPZ Basics

Response Policy Zone

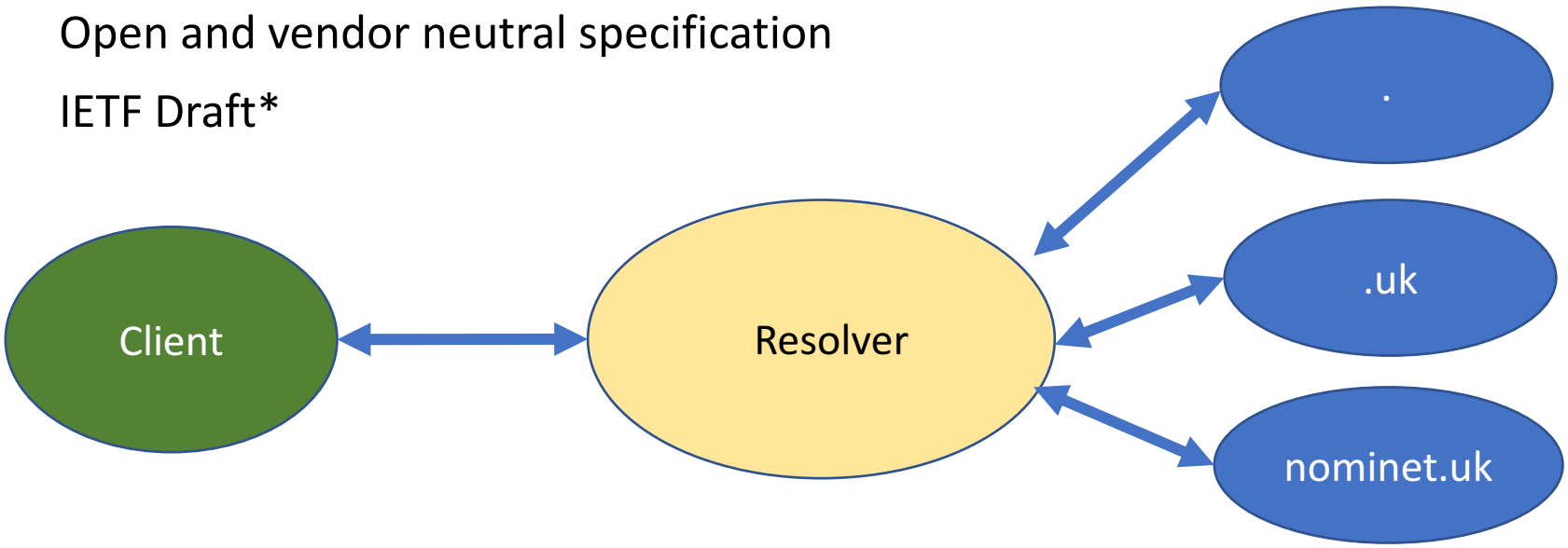
Allows policy to be applied to DNS queries

Recursive resolver (normally)

Allows the ‘bad’ to be blocked

Open and vendor neutral specification

IETF Draft*



*https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00

Response Policy Zone

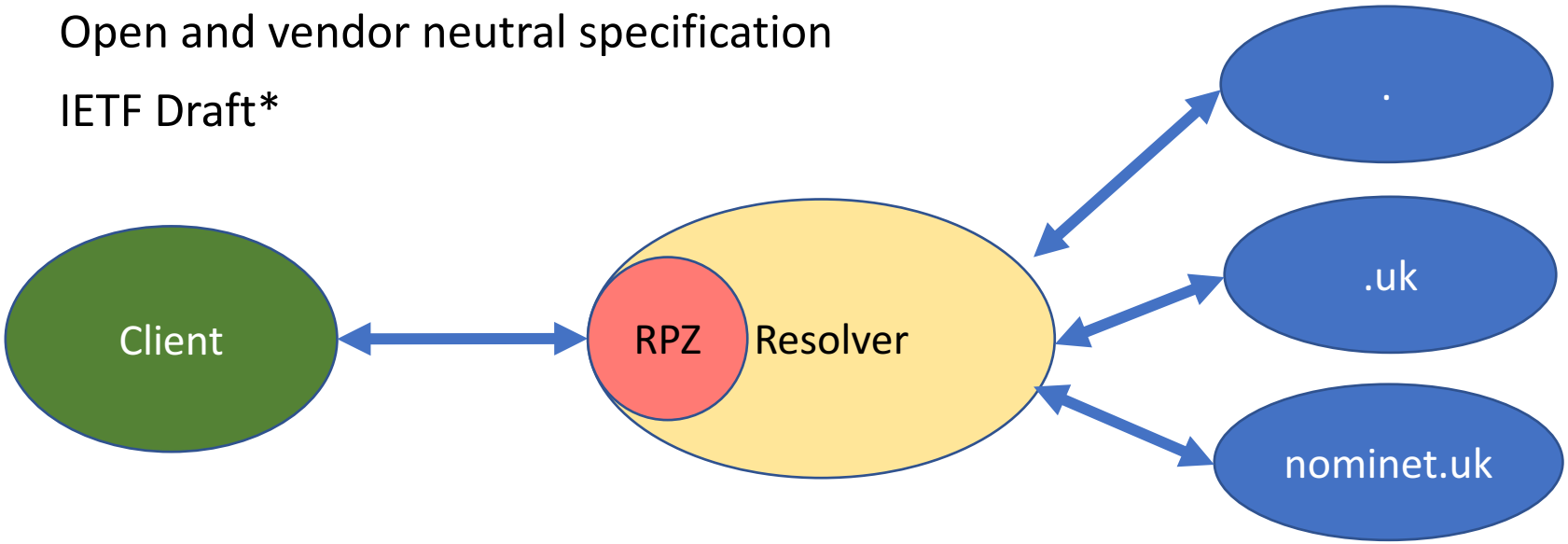
Allows policy to be applied to DNS queries

Recursive resolver (normally)

Allows the ‘bad’ to be blocked

Open and vendor neutral specification

IETF Draft*



‘db.myrpz’ zone: nominet.uk IN A 127.0.0.7

Response Policy Zone

Standard recursive DNS:

```
james$ dig nominet.uk
...
;; QUESTION SECTION:
;nominet.uk.                    IN      A

;; ANSWER SECTION:
nominet.uk.             300     IN      A       104.20.15.61
nominet.uk.             300     IN      A       104.20.14.61
...
```

Response Policy Zone

Resolver with RPZ turned on:

```
james$ dig nominet.uk
...
;; QUESTION SECTION:
;nominet.uk.                    IN      A

;; ANSWER SECTION:
nominet.uk.             5       IN      A       127.0.0.7

;; AUTHORITY SECTION:
myrpz.                  300     IN      NS      LOCALHOST.
...
```

Different answer

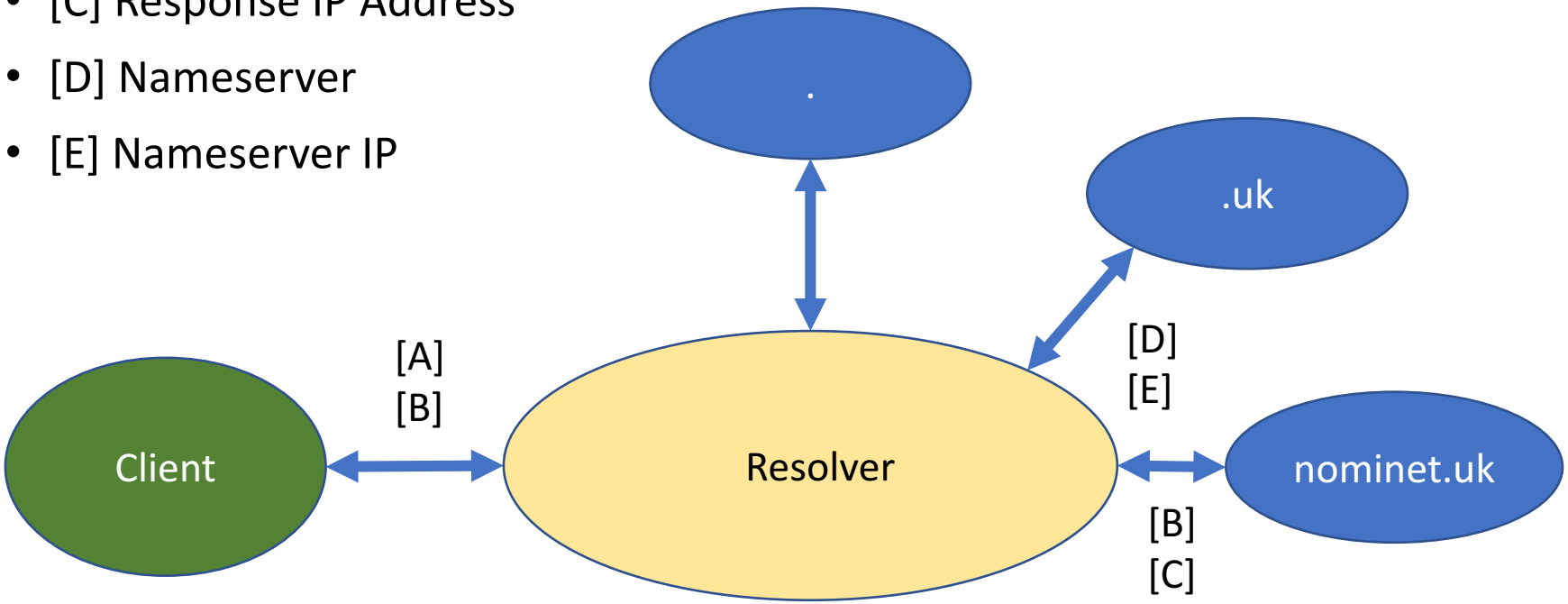
Different TTL

Provided by
our RPZ

Configuring an RPZ

RPZ can be triggered by:

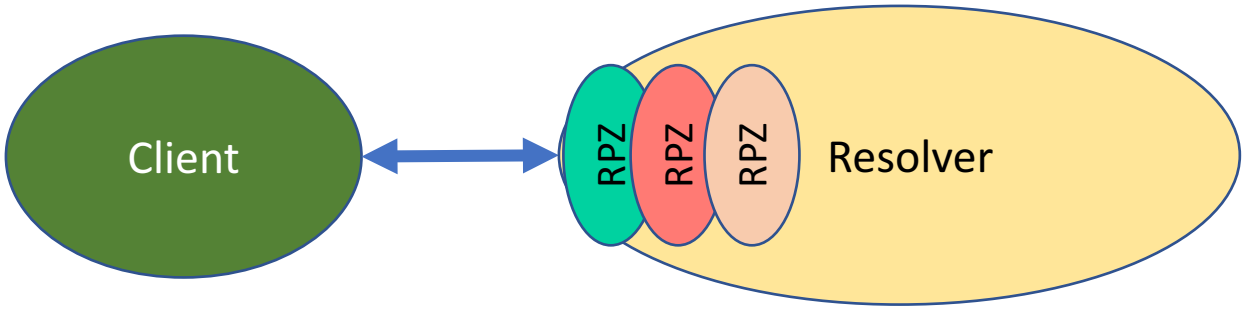
- [A] Client IP Address
- [B] Query Name
- [C] Response IP Address
- [D] Nameserver
- [E] Nameserver IP



Configuring an RPZ

Actions that can be taken:

- Local Data — RPZ specified resource record — (UKPDNS - Block Page IP)
- NXDOMAIN — Respond with NonExistent Domain — (Perhaps ‘best’ option...?)
- DROP — Timeout
- NODATA — Empty answer
- TCP-ONLY — Try again over TCP
- PASSTHRU — <logging>



Blocking and Whitelisting

Types of Security Threat

Imitating a known site

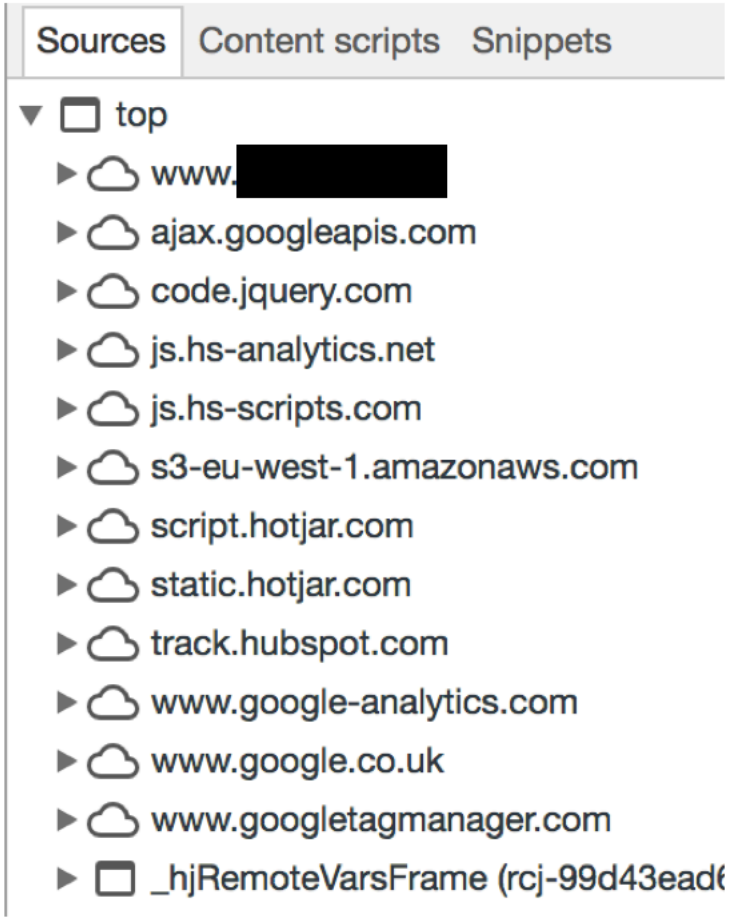
Compromised content (e.g. JavaScript, etc)

Exploit Kit Servers

Command and Control (C2) including Domain Generating Algorithms (DGAs)

- ofdhiydrrttpblp[.]com
- puciftnfkplcbhp[.]net
- bowjjxxnhkyvygk[.]biz

roomthirteen.net (‘suppobox’) [1]
airbus.com (‘virut’) [2]



Sources: [1] Bambenek Consulting
[2] DGArchive

Security Feeds

UKPDNS uses both commercial and open source intelligence feeds

List of feeds on dnsrpz.info:

Provider	Service
DissectCyber	rpzone.us
FarsightSecurity	Newly Observed Domains and example
InfoBlox	DNS firewall
SpamHaus	Several of their popular blocklists are available via RPZ. Article Pricing
SURBL	Data Feed
SWITCH	SWITCH DNS Firewall
ThreatStop	DNS firewall and announcement

Test the feed in PASSTHRU mode

There is variety in the types of malware each feed protects against

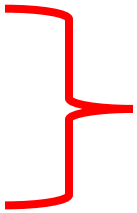
Whitelisting

Consider whitelisting:

- Critical Organisational Internal Domains
- Critical Content Distribution Networks
- Internet Hosted Apps
- Updates and Internet Infrastructure
- Specific Network Ranges
- Search Engines

Top Domains

- Alexa Top Domains
- Majestic Million
- and others



Be careful. “Bad” domains still appear on these lists!

Monitoring and Analysis

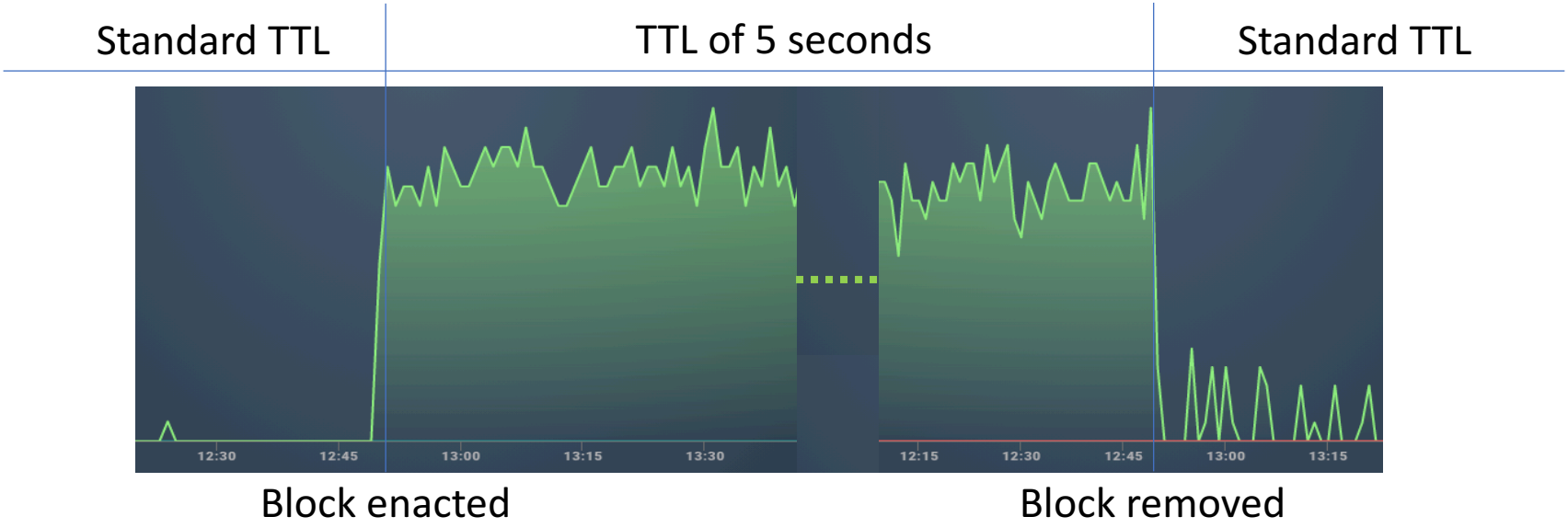
Monitoring and Analysis

May require additional monitoring, e.g. qtype

- IPv4 host = 1 DNS query (A)
- IPv6 host = 2 DNS queries (A, AAAA)

What effect does the RPZ have on cached queries?

- Standard Response TTL = minutes / hours / days
- Blocked Response TTL = seconds



Monitoring and Analysis

Unique Blocked Queries per query name, IP, etc

Unique Blocked Queries per source IP or network

Blocks per intelligence feed source and threat type (C2, exploit kit, cryptominers, etc)

Blocks per registered domain: publicsuffix.org

www.example.uk
example.uk
example.co.uk
example.<dynamic-dns-provider>.net

Summary

- RPZ allows action to be taken on DNS queries
- Whitelist important domains, personalised to your environment
- May need additional DNS monitoring and analysis tools
- Experiment with different feeds for blocking
- Experiment with different traffic measurements
- User interaction is important - have clear policies for block/unblock

Questions ☺