Analyzing and Mitigating Privacy
with the DNS Root Service

Wes Hardaker
USC/ISI
<hardaker@isi.edu>
Last Year I Pondered:
Can you avoid asking questions?

.TLD
Parent DNS

Example.TLD
Outsourced Child DNS

ISP Resolver

ISP

NS

Data

Primary Service (eg https)

More DNS Anonymous

Less DNS Anonymous
Which Led Me To More Questions

• Does query leakage really reveal anything?
  – What does (e.g.) the root see about me?
• Does traffic analysis reveal anything?
• Does temporal analysis reveal anything?

• How much protection do solutions offer?
  – TLS?
  – Query minimization?
• What offers full protection?
DNS Query Leaking to the Roots

Clients → ISP → Resolver → DNS Infrastructure

Cache:
- com
- example.com

www.example.com?
DNS Query Leaking to the Roots

Clients

ISP

QName Minimization

Multiple DNS cache entries:
- com
- example.com

Encryption

DNS Infrastructure

Root

com

www.example.com

org

eicann

example
DNS Query Leaking to the Roots

What if you don’t trust them either?

Clients

ISP

DNS Infrastructure

Resolver

QName Minimization

Encryption

Cache
- com
- example.com
Experiment Plan and Data

- Two residences
  - Recursive resolvers
  - Static IP
  - Willingness
  - Providing ground truth

- An authoritative server
  - B-Root
  - **One month** of query data: 2017, Jan.

- Bulk global analysis
  - Quick analysis
## Data Statistics

<table>
<thead>
<tr>
<th></th>
<th>Residence 1</th>
<th>Residence 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Packets</td>
<td>52191</td>
<td>2049</td>
</tr>
<tr>
<td>IPv6 Packets</td>
<td>27675</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>79866</td>
<td>2049</td>
</tr>
</tbody>
</table>
Analysis Types

- RRTYPE
- Geographical
- Temporal
- Special Name

- Warning: Results coming next at firehose rate

*(don’t try this at home)*
RES1 RRTYPE Analysis

RRTYPEs Seen

- **IPv4**
- **IPv6**

---

<table>
<thead>
<tr>
<th>RRTYPE</th>
<th>IPv4 Count</th>
<th>IPv6 Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IXFR</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXFR</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNSKEY</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRV</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MX</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SOA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TXT</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AAAA</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---

The chart illustrates the number of RRTYPEs seen for both IPv4 and IPv6. Each RRTYPE is represented by a bar, with the height indicating the count for that specific RRTYPE.
RES1 RRTYPE Analysis

RRTYPEs Seen

12251 Requests:
- TXT: hostname.bind
- TXT: id.server
- TXT: version.bind
- TXT: version.server
RES1 RRTYPE Analysis

SOA queries and responses per hour
TXT queries and responses per hour
RES1 RRTYPE Analysis

SOA queries and responses per hour
TXT queries and responses per hour

RIPE Atlas Probe? *(yes!)*

... Let's remove this root (.) clutter
RES1 RRTYPE Analysis – Non Root

This graph has no queries for root-zone data (i.e. no “.” queries)
RES1 RRTYPE Analysis – Non Root

Non-Root RRTYPEs

Mail server on network?

12 Requests: _domainkey records

Yes!
RES1 RRTYPE Analysis – Smaller

Smaller Quantity, Non-Root, RRTYPEs Seen

IPv4 120
IPv6 110

DS 0
IXFR 1
AXFR 1
SRV 1
MX 1
NS 4
SOA 120
RES1 RRTYPE Analysis – Smaller

Smaller Quantity, Non-Root, RRTYPEs Seen

DNS Server Characteristics:
Validating (DS)
Master or Slave (IXFR, AXFR)
Yes! Yes!
RES2 RRTYPE Analysis

Interesting: there is no IPv6 Deployed in RES2!
RES2 RRTYPE Analysis

Smaller Quantity, Non-Root, RRTYPEs Seen
RES2 RRTYPE Analysis

Internal network Address leakage:

10.0.0.38

Yes!
RES2 RRTYPE Analysis

Smaller Quantity, Non-Root, RRTYPEs Seen

Internal network Name leakage:

QNAME: “g2”

Yes! confirmed hostname
RES2 RRTYPE Analysis

Smaller Quantity, Non-Root, RRTYPEs Seen

Internal network Name leakage:

QNAME: “g2”

Ask yourself:
Would QName Min Have Helped?
RES1 Geographical Analysis

Heat Map: Most popular CC-TLDs
RES1 Geographical Analysis

Heat Map: Most popular CC-TLDs

Lots of communication with China and Russia?

No! Fail! – SPAM
RES2 Geographical Analysis

Heat Map: Most popular CC-TLDs
RES2 Geographical Analysis

Heat Map: Most popular CC-TLDs

Lots of communication with Australia?

No! Fail!
aridns.net.au – Unknown
RES1: Temporal Analysis – by hour
RES1: Temporal Analysis – by hour

Household sleeping period? TZ offset 6-8 from GMT?
Yes! (7)
RES2: Temporal Analysis – by hour

![Bar chart showing hours of the day with data points from 0 to 23. The chart indicates peak activity between 12 and 17 hours.]
RES2: Temporal Analysis – by hour

Household sleeping period? TZ offset 4-6 from GMT?

Yes! (4)
RES1: Temporal Analysis – by day

Traffic per Day

Total traffic for 28 days divided across 7 weekdays
RES1: Temporal Analysis – by day

**Fail:** Typical 5-workday pattern not discernible

Would likely work for some places though?
RES2: Temporal Analysis – by day

Traffic per Day

Total traffic for 28 days divided across 7 weekdays
Fail: Typical 5-workday pattern not discernible

Would likely work for some places though?
RES1 Names containing “_”

- _adsp._domainkey.ihjqljmo.cc.
- _adsp._domainkey.linkedin.chi.namibia.na.
- _adsp._domainkey.newsbank.club.
- _adsp._domainkey.till.name.
- _adsp._domainkey.user1-computer.i-did-not-set-mail-host-address--so-tickle-me.
- _adsp._domainkey.uzps.co.sy.
- _adsp._domainkey.xstreamues.trade.
- _minecraft._tcp.10.0.0.18.
- _minecraft._tcp.10.0.0.2.
- _minecraft._tcp.73.41.83.66.
- dkim._domainkey.speedbring.win.
- libglesv1_cm.so.
- mesmtp._domainkey.mad.paris.
- _xmpp-server._tcp.pandion.im.
- postfix._domainkey.luffy.cx.
- testglxgetprocaddress_genentry.sh.
- testpatchentrypoints_gldispatch.sh.

Internal Addresses!
Minecraft player!
Jabber User!
Mitigation Options

1) DNS Query Name minimization
   - Send only partial queries

2) TLS-based DNS encryption
   - Encrypt against man-in-the-middle

3) LocalRoot – RFC7706
   - Slave the root zone
   - Eventually slave others
https://localroot isi.edu/

Server List

<table>
<thead>
<tr>
<th>Administrative Name</th>
<th>Address</th>
<th>TSIG</th>
<th>Enabled</th>
<th>Active</th>
<th>Delete</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>my cool TSIG key: p9ibZHNqKlqxHbtav5OU6g==</td>
<td>✔️️</td>
<td>❌️️</td>
<td></td>
<td>[get config]</td>
</tr>
</tbody>
</table>

Add a New Server

(Click on the enabled buttons to toggle)

Servers will not be listed active until an hour after an initial AXFR has been seen.

© Copyright 2017 by USC/ISI.
Configuration Generator

Select from the following parameters to change the configuration code generated below:

Full recursive resolver configuration

Your generated bind configuration for 10.0.0.2 at 10.0.0.2 is:

```plaintext
// TSIG keys

key "my_cool_TSIG_key" {
  algorithm hmac-sha256;
  secret  "p9lbZHNgkJkxHbtav5OU6g==";
};

// upstream servers to transfer from

server 128.9.36.81 { keys { "my_cool_TSIG_key"; }; } // localroot.isi.edu

// The slave definition for the root zone
// includes all servers we can transfer data from
```

https://localroot.isi.edu/
**Mitigation Option Comparison**

<table>
<thead>
<tr>
<th>Analysis Method</th>
<th>Qname Min.</th>
<th>TLS</th>
<th>LocalRoot / 7706</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Version</td>
<td>N</td>
<td>N</td>
<td>P</td>
</tr>
<tr>
<td>RRType</td>
<td>Y</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Geographical</td>
<td>N</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Temporal</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>TLD</td>
<td>N</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>SLD</td>
<td>Y</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>PSL</td>
<td>Y</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Special Names</td>
<td>Y</td>
<td>P</td>
<td>Y</td>
</tr>
</tbody>
</table>

Conclusions:

Note: We only touched the tip of the analysis iceberg

1) Qname Minimization doesn’t help geographical and temporal analysis
2) Encryption only works against MiM – not against parental DNS servers
3) The only way to truly be private: **don’t ask any questions!!**

https://localroot.isi.edu/
LocalRoot: Don’t Ask Questions

LocalRoot enabled

(RIPE atlas)

https://localroot.isi.edu/
Conclusions

- QName Minimization and TLS only go so far
  - Traffic analysis discloses other sensitive data
  - You still need to trust the parent hierarchy
- More data studies are needed
  - (great thanks to Robert Story for his residence data)
- Distributed naming and push models win

- [https://localroot.isi.edu/](https://localroot.isi.edu/)
  - Solves much of this, but only for the root (*currently*)
  - Cost: bandwidth and memory