DNS Log File Analysis: The Things you can find (V2.0)

Stephen Deerhake

AS Domain Registry

ICANN-49 TechDay– Singapore 2014

Acknowledgements

- “V2.0” as this is a somewhat expanded version of a talk on this subject that I gave at the recently concluded APLTD meeting in Kuala Lumpur last month.
- Don Hollander – for suggesting the title of this presentation, and providing me the opportunity to initially present at the APTLD meeting.
- Dr. Eberhard Lesse – for taking my Perl scripts to a new level, providing guidance, and for furthering the investigation.

American Samoa – .AS

- AS = American Samoa
- Unique amongst Populated US Territorial possessions:
  -- both unincorporated and unorganized
- Result: A higher degree of autonomy than that enjoyed by other US Territorial possessions
- Only inhabited US territory south of the equator (population around 60K)

Background of .AS Registry

- Established in 1997; predates ICANN
- Currently in excess of 17K domains
- High entry price point (USD $100 for a registration, which is a 2 year registration)
- Free Registration/Renewal if registrant is "on-island"

Background of .AS Registry (cont.)

- Breakdown of Registrations
  - Local ("on-island") registrations
    - Mostly local businesses, but some individuals
  - Brand protection
    - Mostly US "Fortune 500" Corporations and their brand marks (Coca Cola,etc.)
  - Norwegian and Danish Corporate Names
    - "a/s" – joint stock company

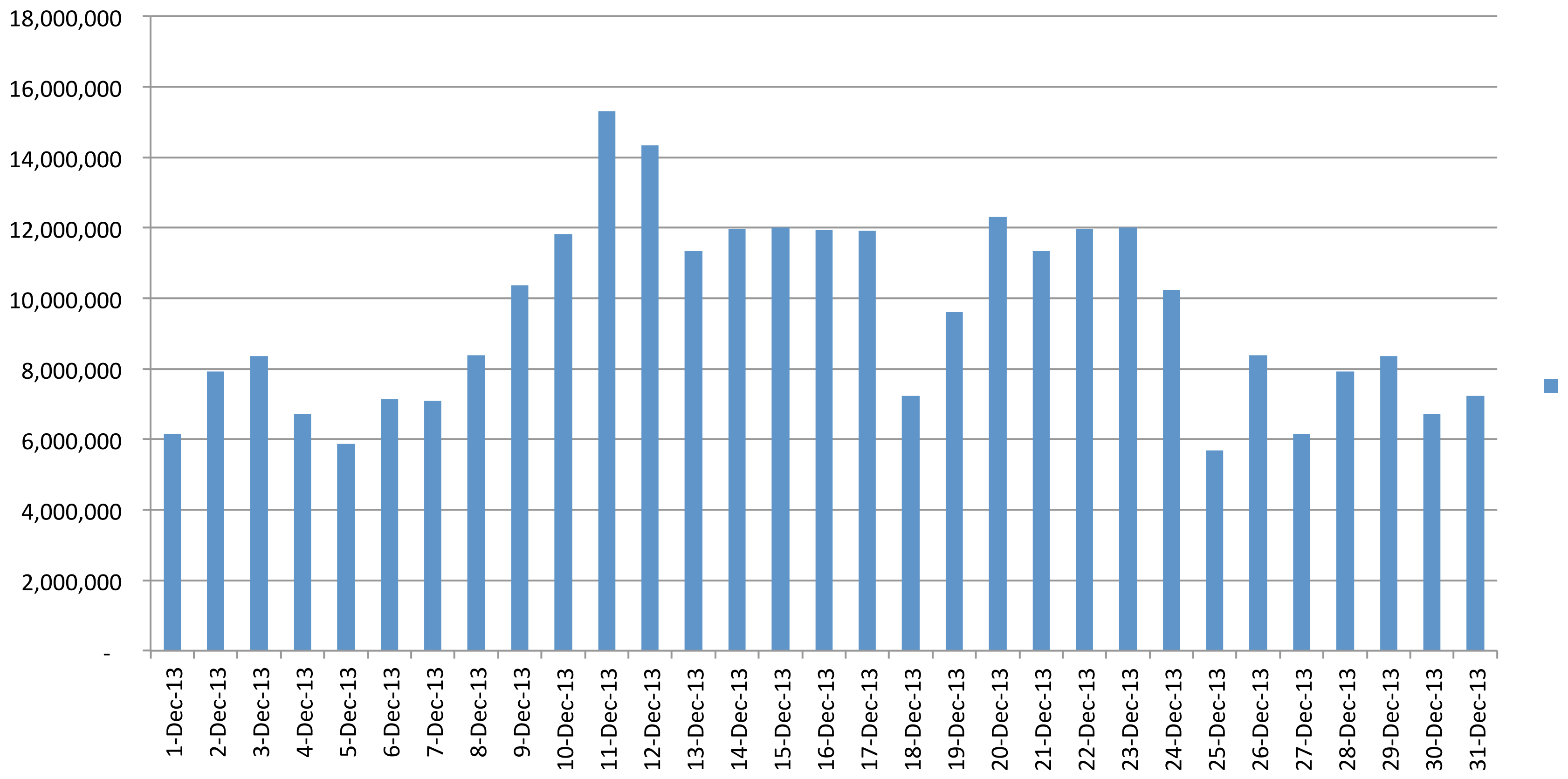
Background of .AS Registry (cont.)

- So we are a “dull” Registry…
  - Not a likely candidate for “short-term” registrations due to initial registration costs (USD $100)
  - Mostly
    - Brand protection
    - On-island businesses
    - Norwegian/Danish Corporations

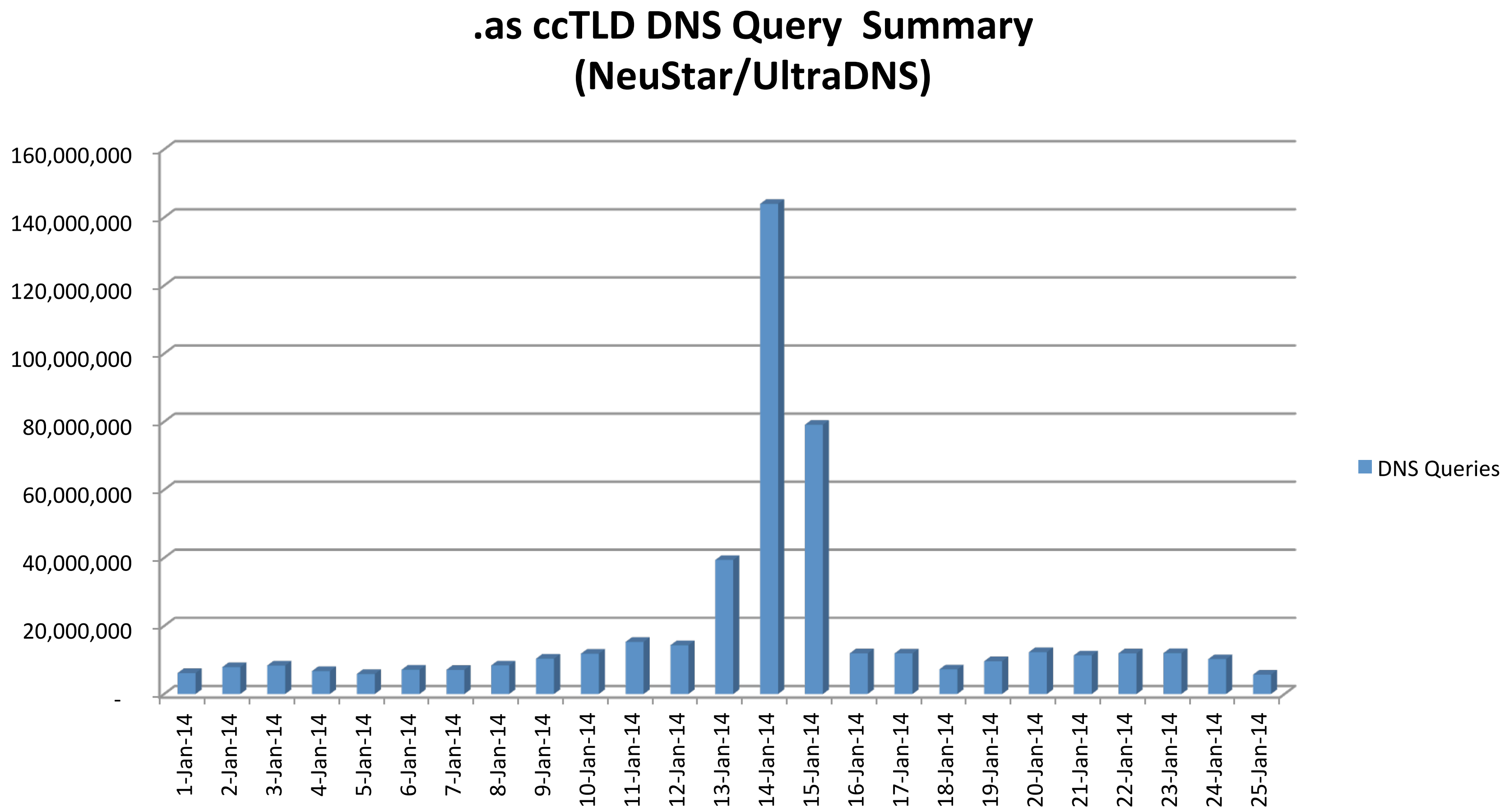
DNS Set Up

- The root zone entries have evolved over time…
- Current situation:
  - 7 distinct entries in the root
  - 1 entry under the direct control of the Registry

A Typical Month of DNS Inquiries



January 2014



What was this Spike About?

- Not detected until “after the fact”
- Vast bulk of the traffic was handled by NeuStar/UltraDNS
- No operational impact on the Registry

Data Sources

- No data available from NeuStar/UltraDNS
- Raw log files from our locally controlled name server
- Dropped log files into a single SQL (Postgres) table on local (slow) hardware

A little SQL…

```
select
client_ip, count(*)
from dns_log
group by client_ip
having count(*)>50000
order by 2 desc;
```

Showed the Issue at Hand…

```
client_ip        |  count
-----------------+-----------
46.4.113.114     | 36,588,331
208.80.194.120   |    610,093
207.102.138.158  |    213,959
69.9.6.68        |    141,830
189.1.87.5       |     97,600
64.142.100.122   |     79,789
110.20.42.46     |     64,797
216.239.45.74    |     59,796
200.155.38.1     |     55,729
208.76.26.4      |     50,479
```

46.4.113.114

- > 36 million queries over a 36 hr period
- Traced back to Dresden, DE
- Victim or Attacker? (Current opinion: Attacker)

Analysis of the Attack

- Three distinct phases:
  - Code development
    - Began on 6 January 2014
    - Sporadic log entries
  - Code test
    - Switched from “A” to “NS” retrievals
  - Full on Attack
    - Started 14 January 2014 at 18.55 GMT
    - Lasted almost two days; then abruptly stopped

Dictionary Contents

- Both English and non-English strings
- Numeric and alpha-numeric strings as well
- Almost no evidence of repeated queries

How successful was the Attack?

- From an NS record harvesting perspective…
  - REASONABLY SUCCESSFUL
  - > 60% of the zone file was harvested

How successful was the Attack?

- From an efficiency perspective…
  - Not very efficient
  - >36 Million queries for 11K domains

Consequences

- > 60% of zone file was successfully stolen
- NO “whois” data was stolen
- No operational issues with the Registry during the attack

On Going…

- Looking at impact on other Registries
- Debating whether or not to engage LE
- Looking at implementing Response Rate Limiting (RRL)
- Would like to review data held by NeuStar/ UltraDNS
- Looking at implementing real-time monitoring on local authoritative name server

Questions?

- Stephen Deerhake: sdeerhake@nic.as