Dictionary Attack on .NA®

An Analysis with Open Source Tools

Dr Eberhard W Lisse

Namibian Network Information Centre (Pty) Ltd

2014-03-24

Outline

What's This All About?

- Dictionary Attack on .AS reported
  - Was .NA® affected?
- BIND9 Log Files
  - PERL Script
  - MySQL Database
  - WHOIS Refinement
- Contact the Secondaries
- R Analysis
- Contact the Perpetrator...

Software Used

Open Sauce

- BIND9
  - v9.4.2-P2.1 on UBUNTU 8.04 LTS
  - v9.8.1-P1 on UBUNTU 12.04.4 LTS
- MySQL v5.6.16
- PERL v5.16.2
- R v3.0.2/3
- LyX v2.1.0beta2
  - BEAMER v2013/12/02
  - KNITR 1.5

Hardware

Off the Shelf

- Pentium 4 (1GB)
  - Name Server
- Pentium (Dual Core 2GB)
  - MySQL
- iMac (i7 16 GB)
  - R
  - LyX

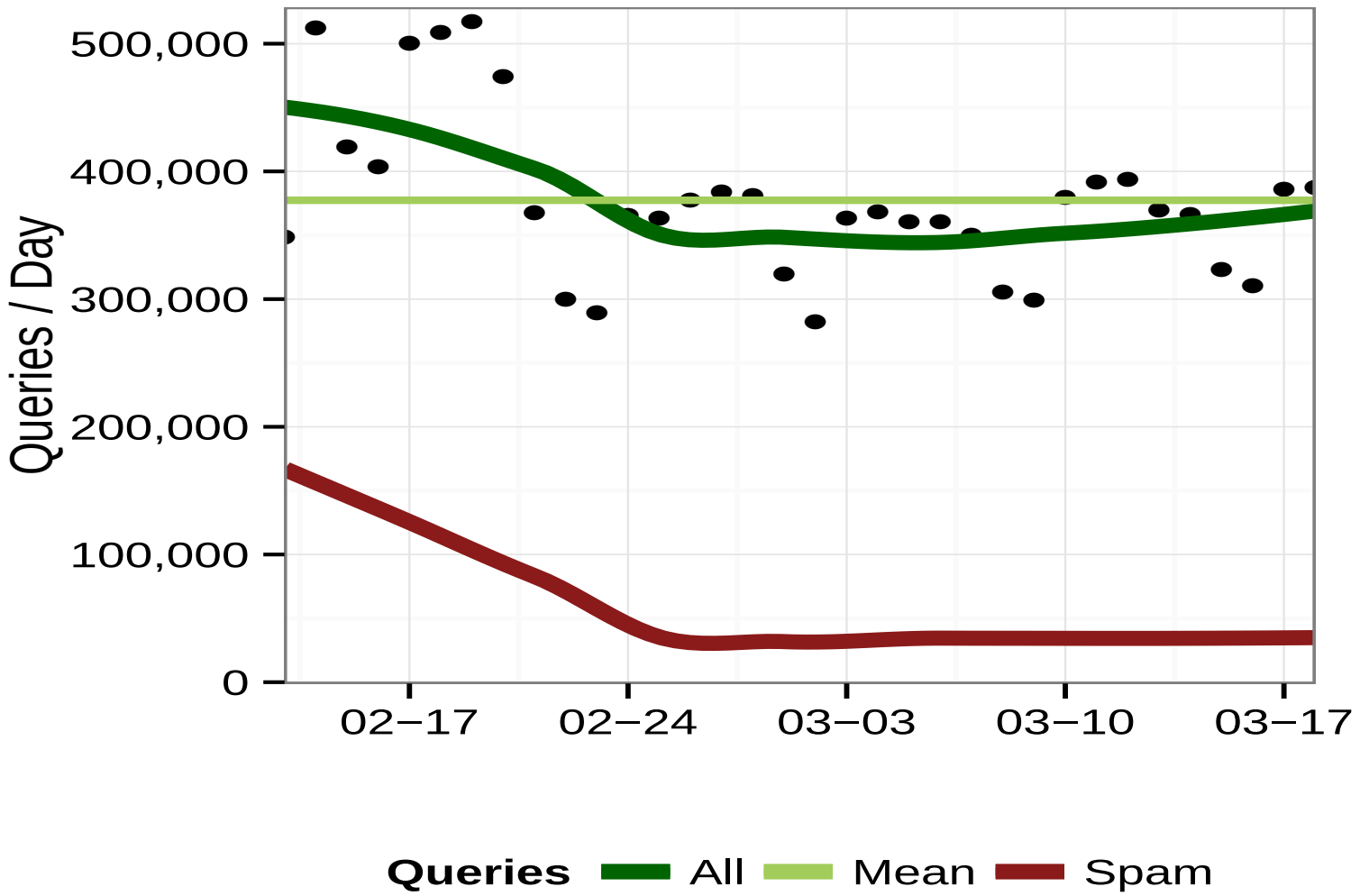
Results

2014-03-19 10:26

First Day	2014-02-13
Last Day	2014-03-18
Days	33
Queries	12899047
Mean	390880

Queries/second	
Minimum	0
Maximum	344
Mean	4.7
Median	4

Smoothed Scatterplot



Involved Networks

CIDR Block	Query Count
Other Blocks	10790391
74.125.0.0/16	803774
176.9.0.0/16	365839
144.76.0.0/16	247880
88.198.0.0/16	209519
192.221.0.0/16	185287
5.9.0.0/16	90900
64.142.0.0/17	59493
193.231.224.0/20	39189
193.231.100.0/24	36220
208.76.24.0/22	28359
193.226.61.0/24	24096
85.214.7.0/24	18100

Lessons Learned

There is some very cool stuff out there

- Perl
  - CPAN
- MySQL
- R
  - CRAN
- LyX
  - Knitr
  - Beamer

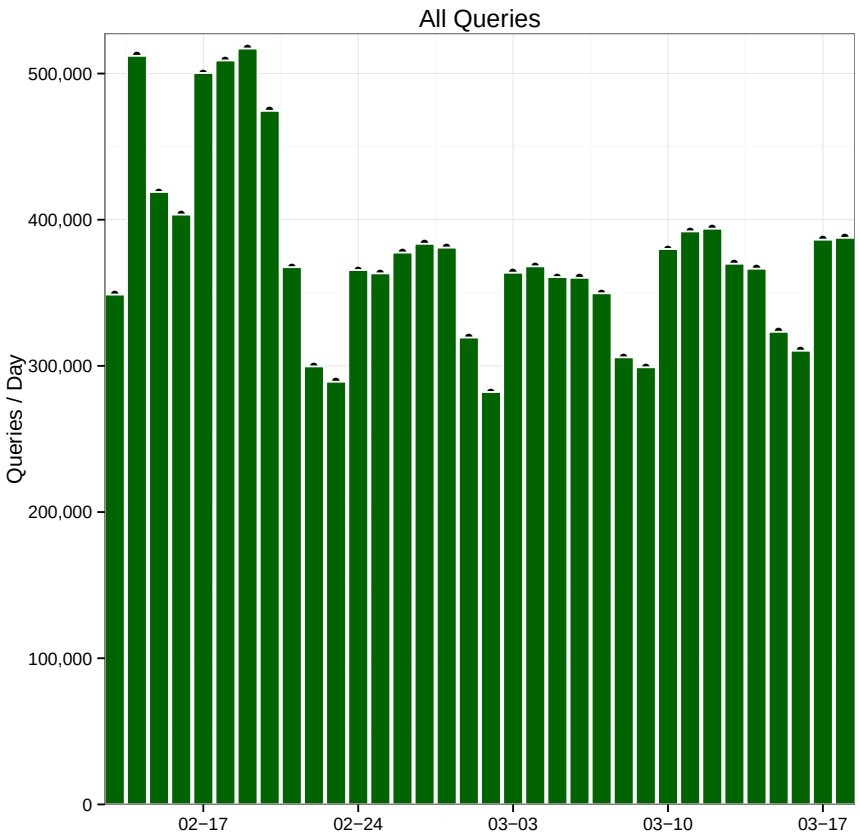
Lessons Learned

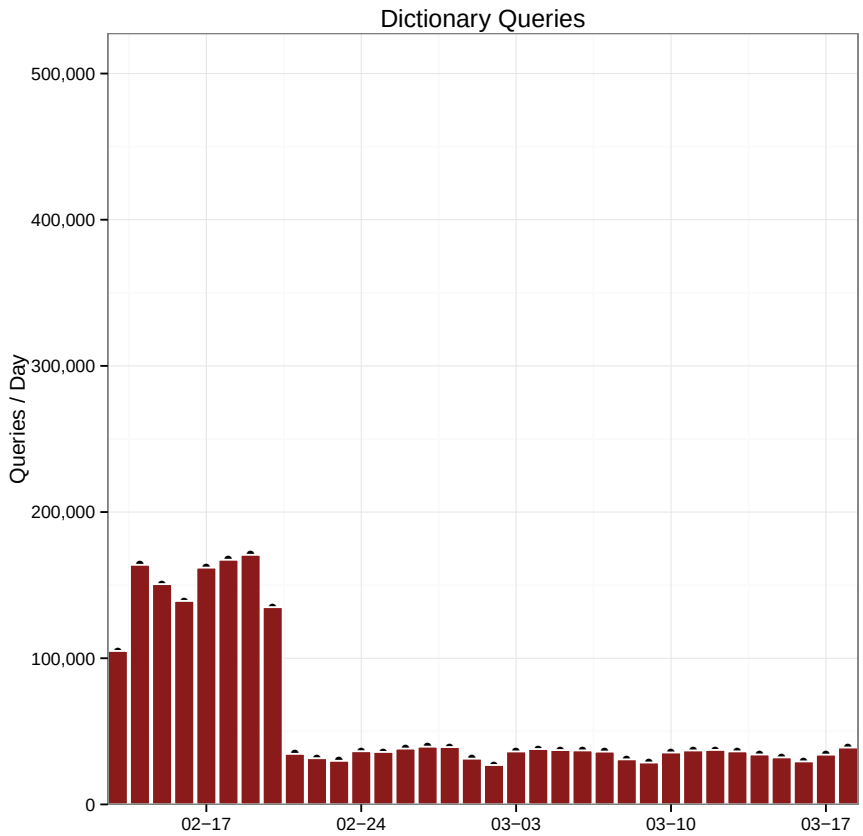
Anycasting is the Key

- Ticket Systems are inflexible
  - So are Call Agents
- German Perpetrators don't like the words
  - Urheberrechtsverletzung
  - Staatsanwalt
- German Hosters don't like
  - Störerhaftung
  - Beihilfe
  - Access Control Lists

Lessons Learned

Can You Spot 2?





Further Work

Dictionary Attack

Request	CIDR Block
0-0-5.org.na	192.221.0.0/16
0-0-8.org.na	192.221.0.0/16
0-0-a.org.na	74.125.0.0/16
0-0-b.co.na	193.231.224.0/20
0-0-c.org.na	193.231.224.0/20
0-0-d.org.na	74.125.0.0/16
0-0-g.org.na	74.125.0.0/16

Further Work

Business Intelligence

- Automate Log Transfer to MySQL
  - Named Pipes?
    - Regular Expressions?
  - Modify Bind?
- SQL to Identify Dictionary Attacks
  - Soundex?
- Identify CIDR Blocks