A Day in the Life of a DNS Resolver
DNS OARC
Amsterdam, May 2015

Bruce Van Nice

Yuriy Yuzifovich

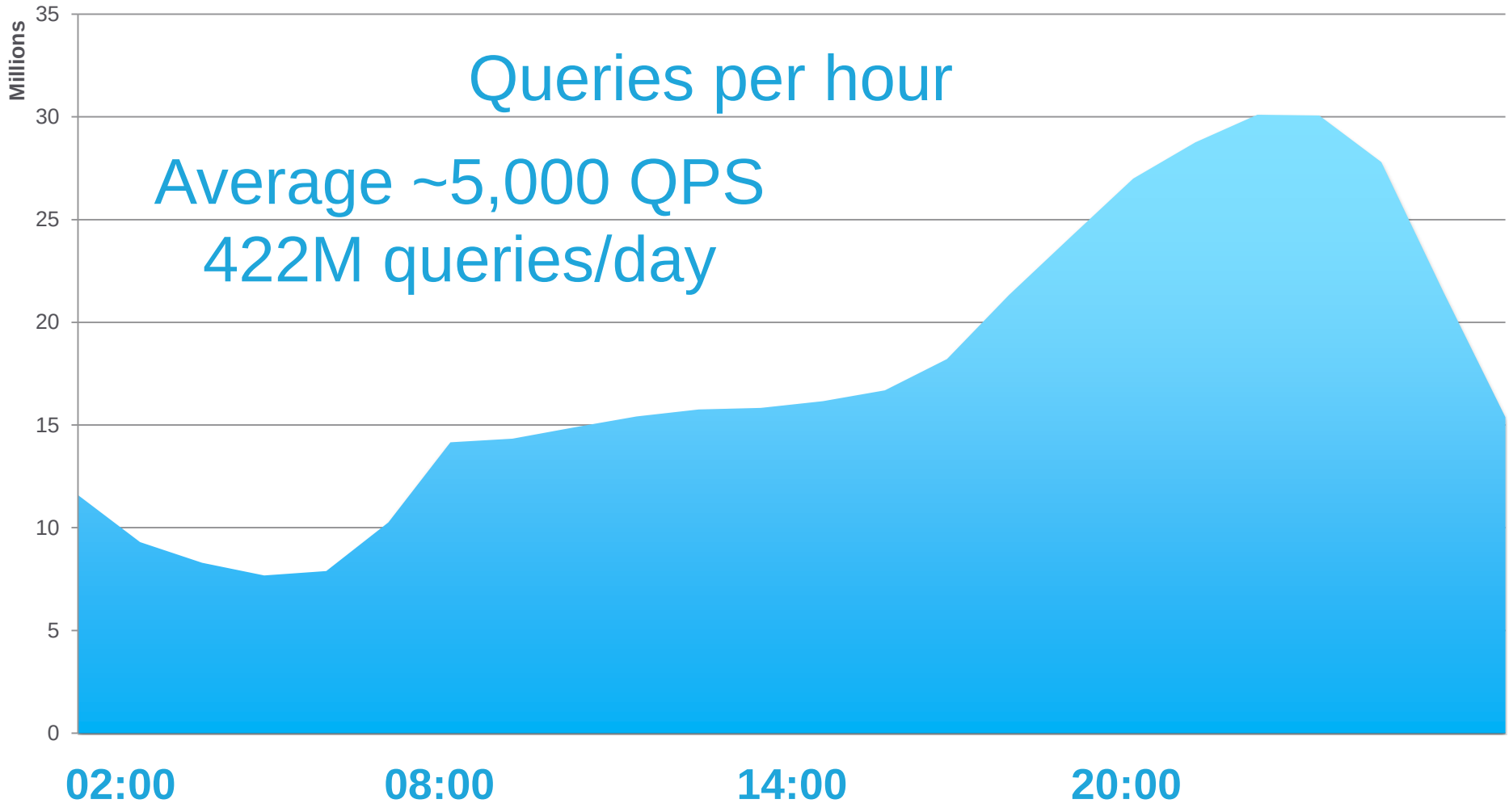
Introduction

- 24 hours traffic from European resolver
  - Consumer broadband
  - ~1 open dns resolver per 200 users
- Data mostly coverings incoming queries
  - Some response data for attacks
- Matching against threat lists
  - Identify DDoS related traffic
  - Bot activity

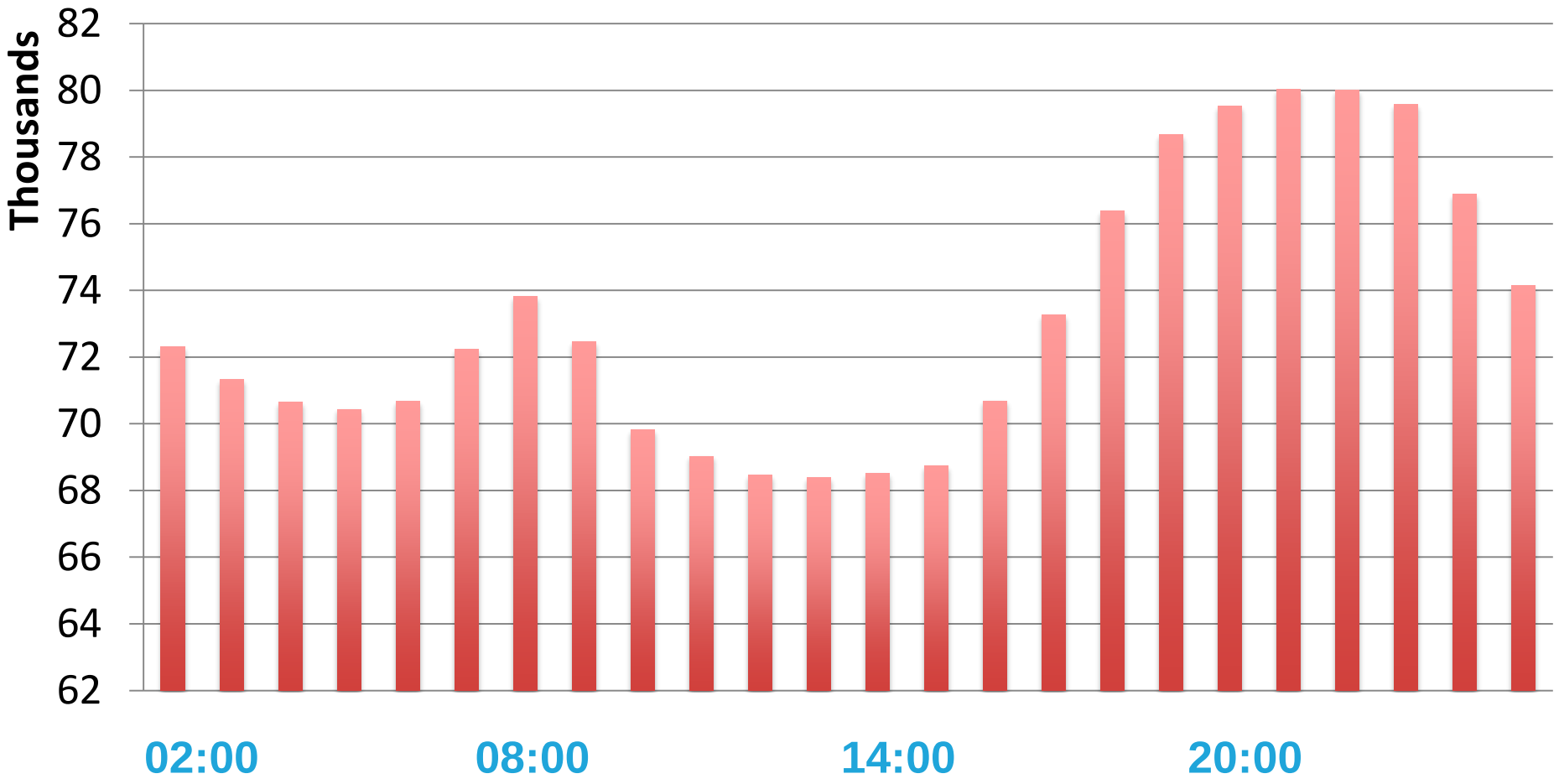
Method

- Processed 24 hours of logs
- Initial filtering for most active domains:
  - DDoS related
  - Known malicious domains
  - Some Query Types
  - Some Flags
- Secondary filtering
  - Higher resolution data per-second activity for attacks

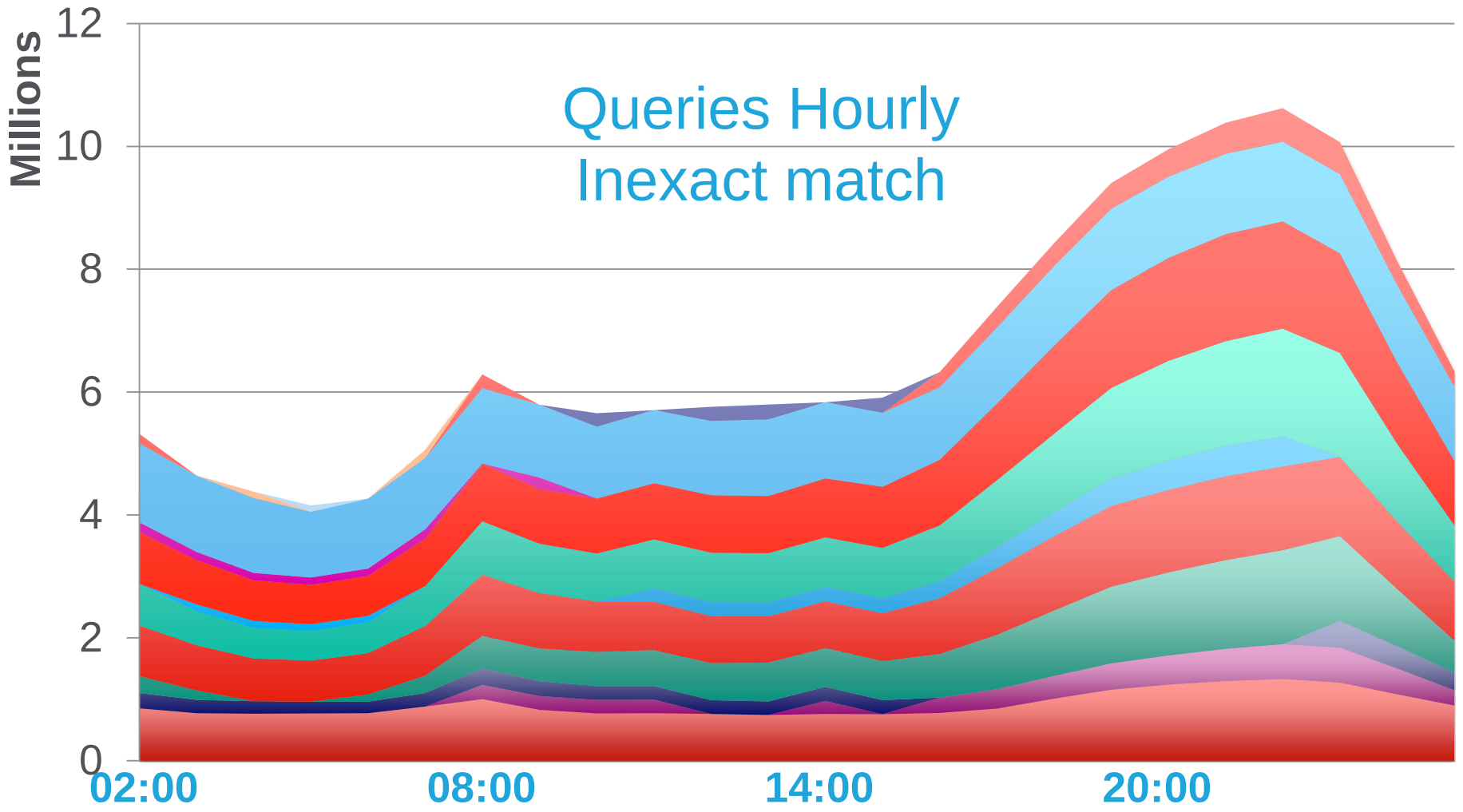
24 Hour Trend (excludes malicious traffic)



IP Count by Hour



Top 10 “Normal” Domains Queried per Hour

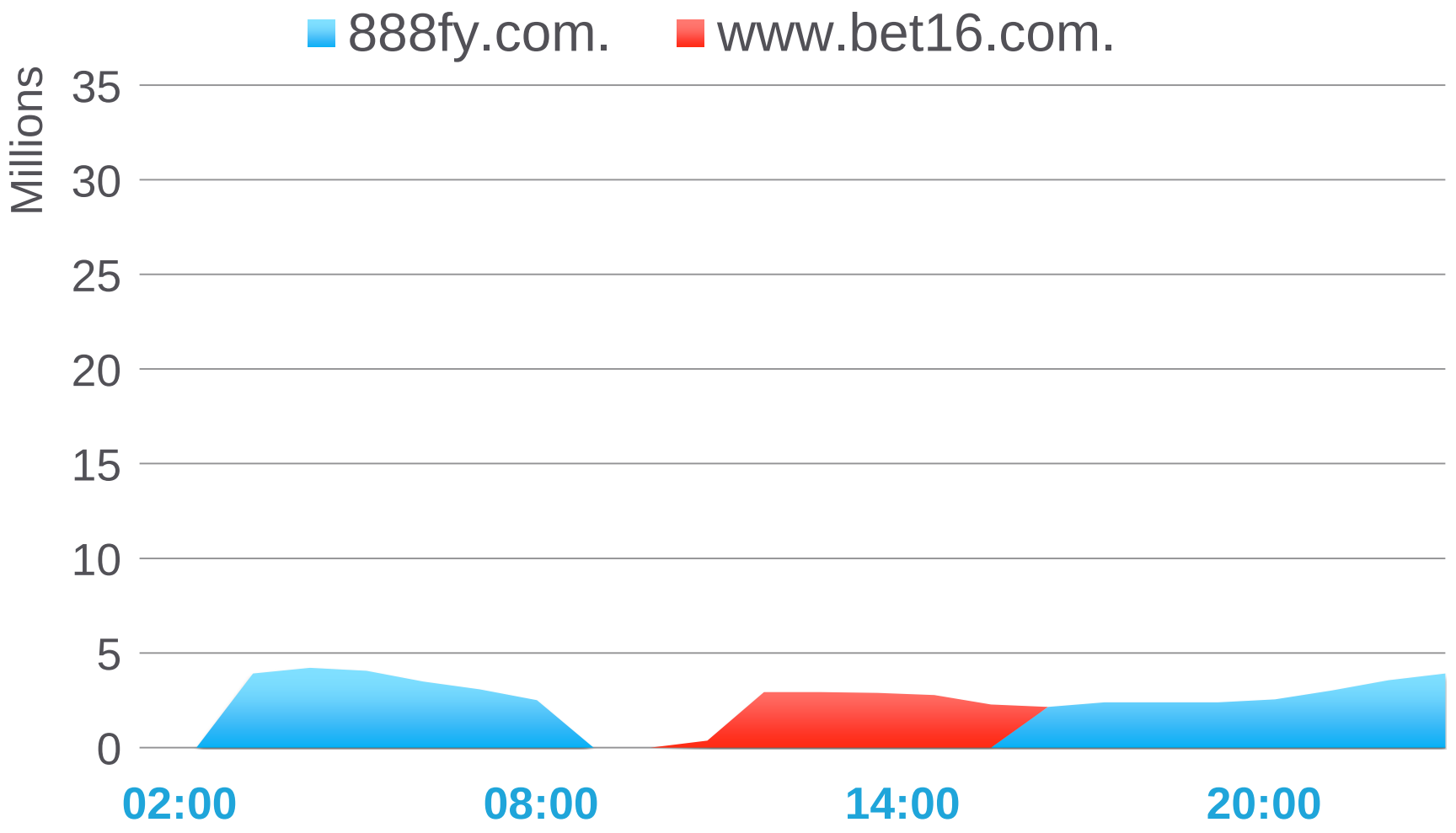


Building Threat Lists

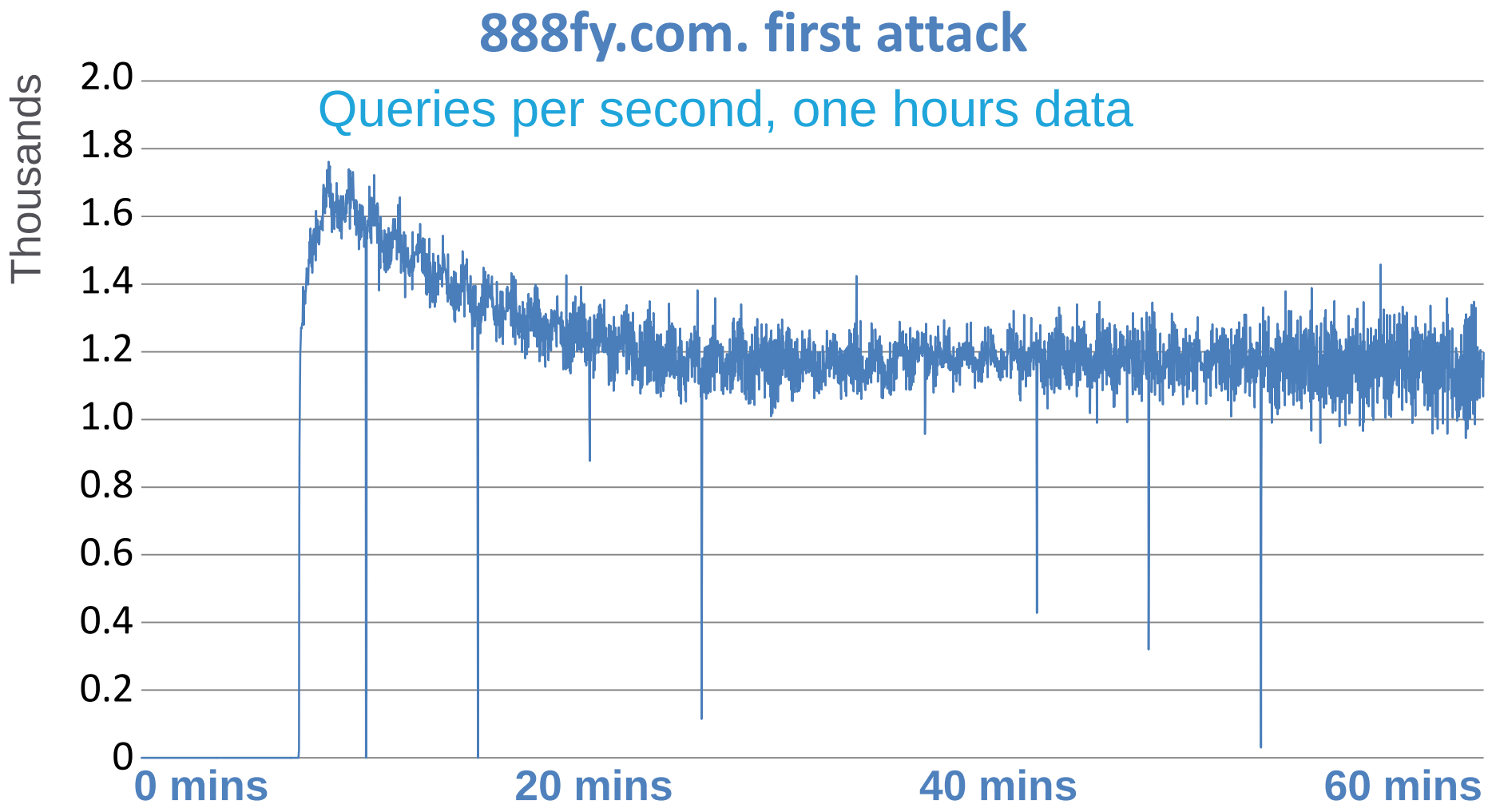
- Worldwide provider data
- Other sources
  - Open source lists
  - Commercial lists
  - Other network data
  - Other threat data
- Extensive Validation
  - Various reputation checks
  - Sometimes manual checks

What goes in here?

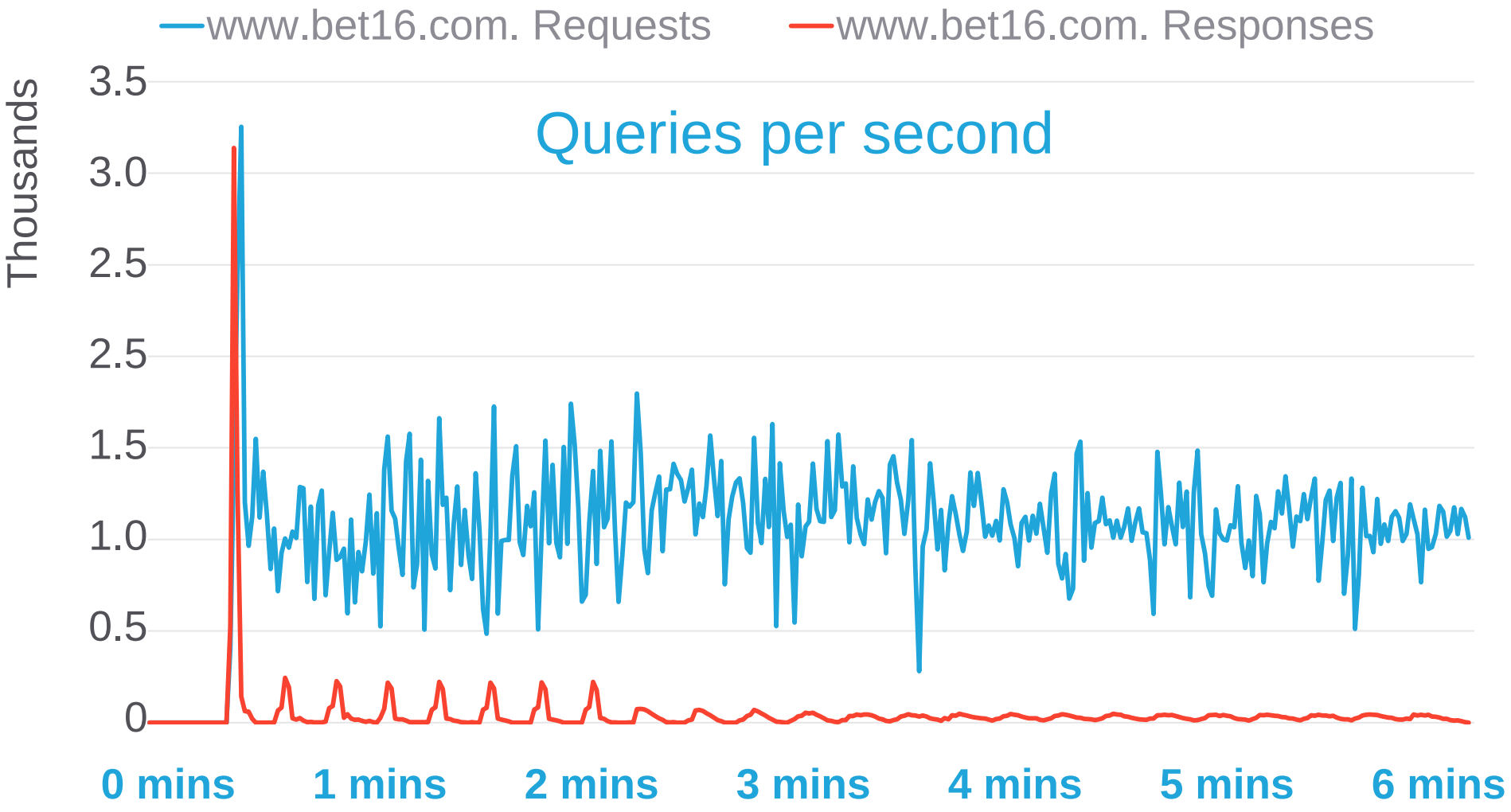
Random Subdomains



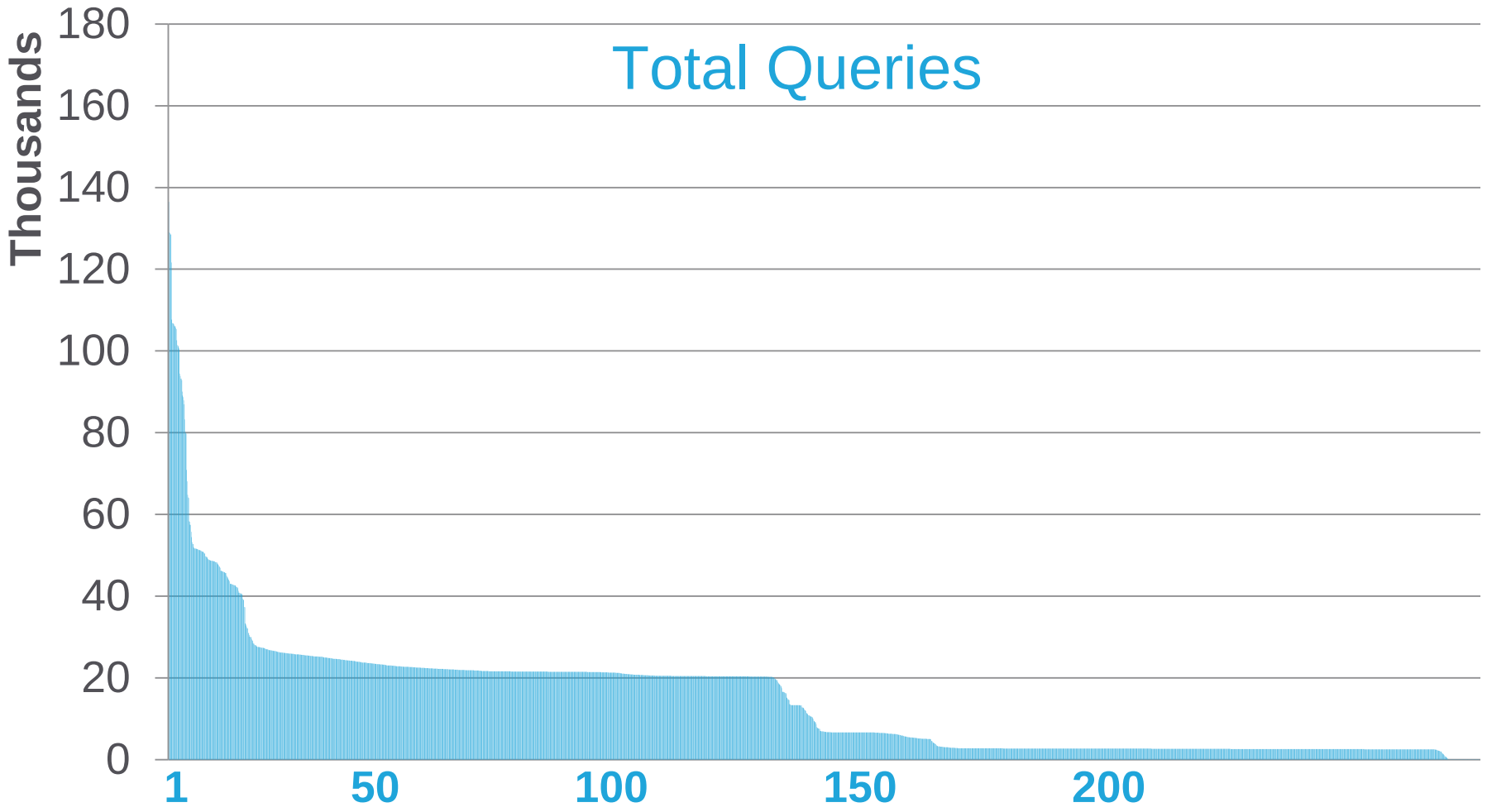
An Hour In the Life



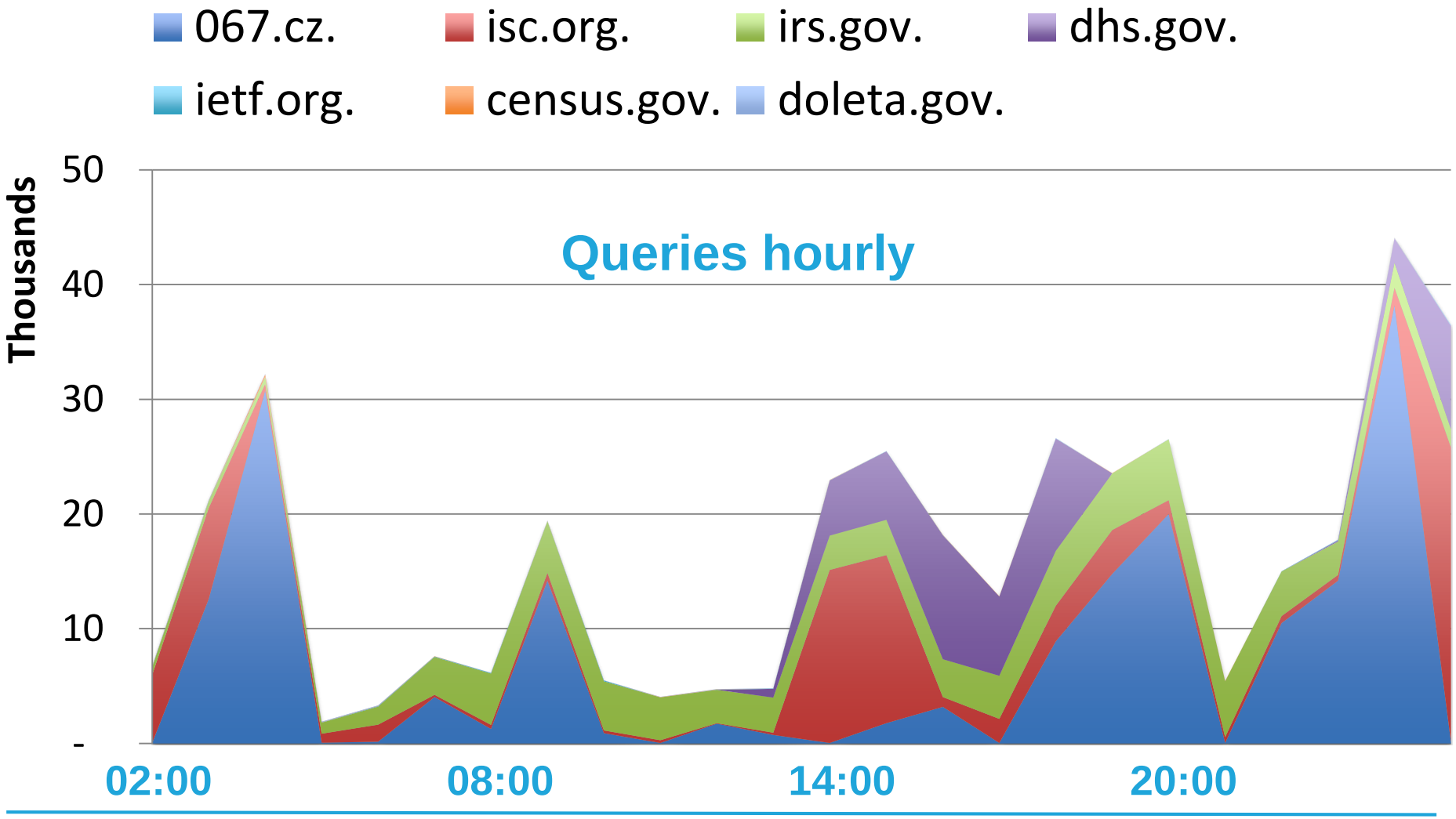
6 Mins in the Life…



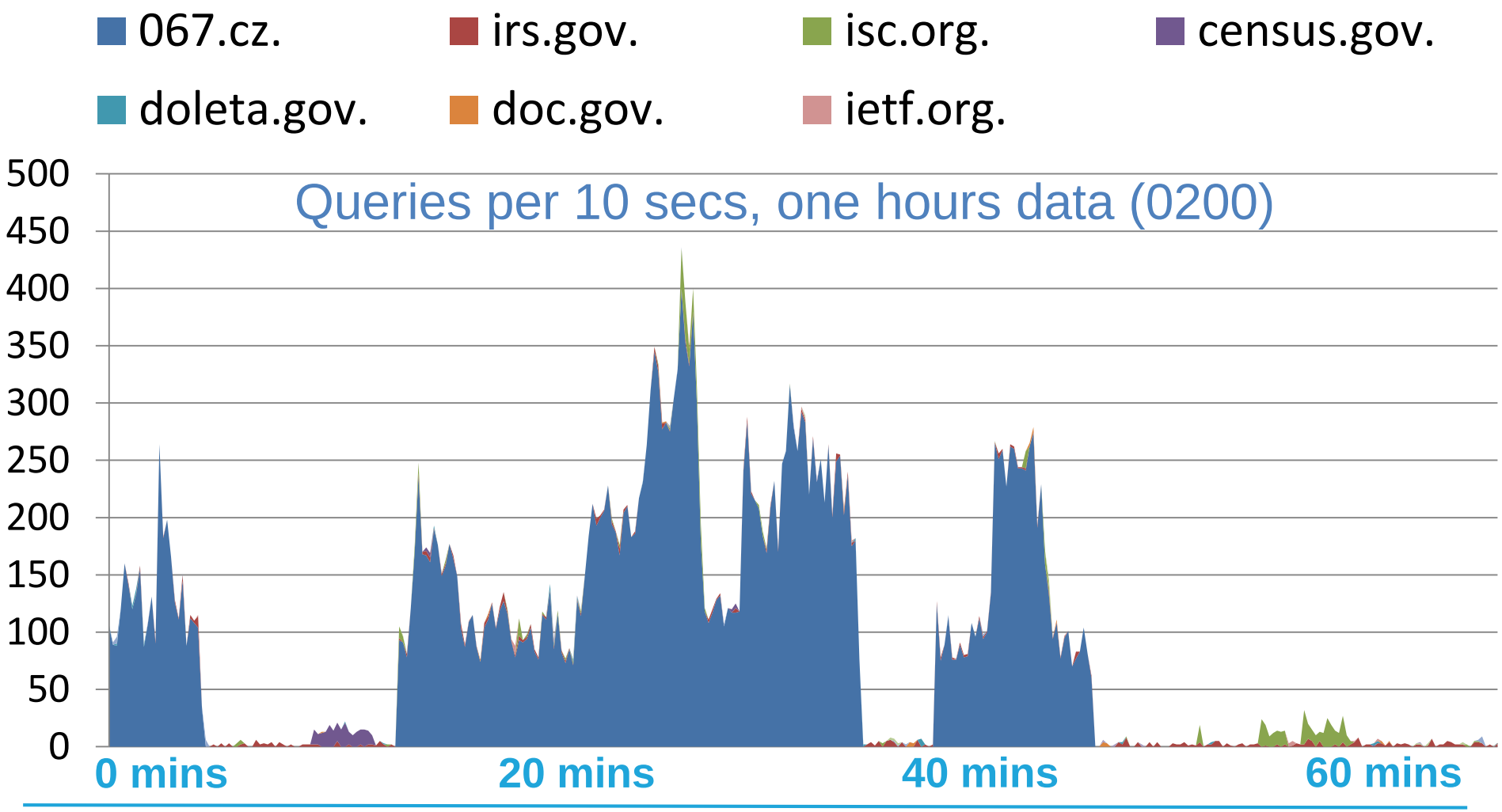
IPs Querying for Random Subdomains



DNS Amplification Queries



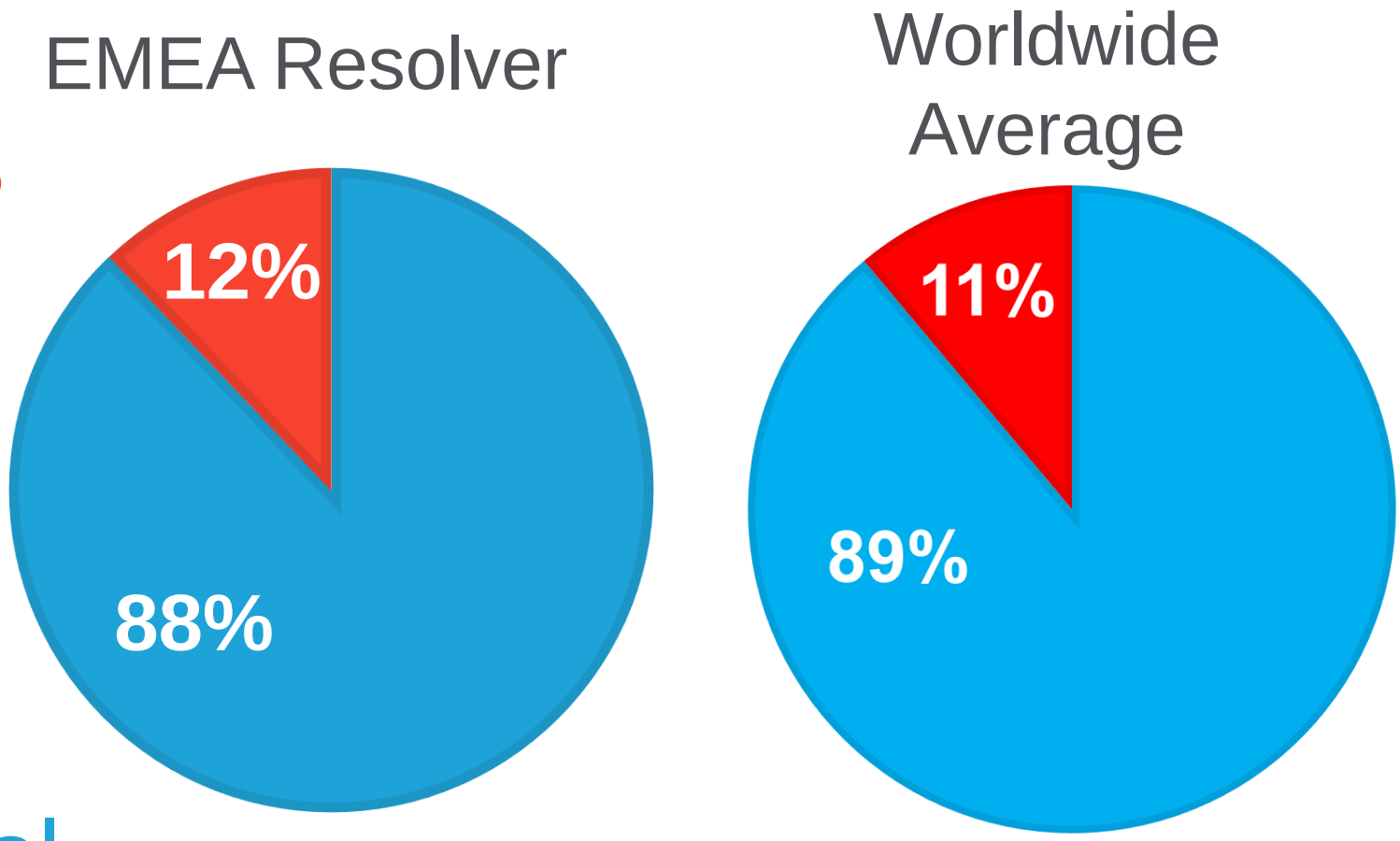
DNS Amplification Queries



Summary “Day in the Life”
Overall Queries Seen at a Resolver

DDoS

Normal

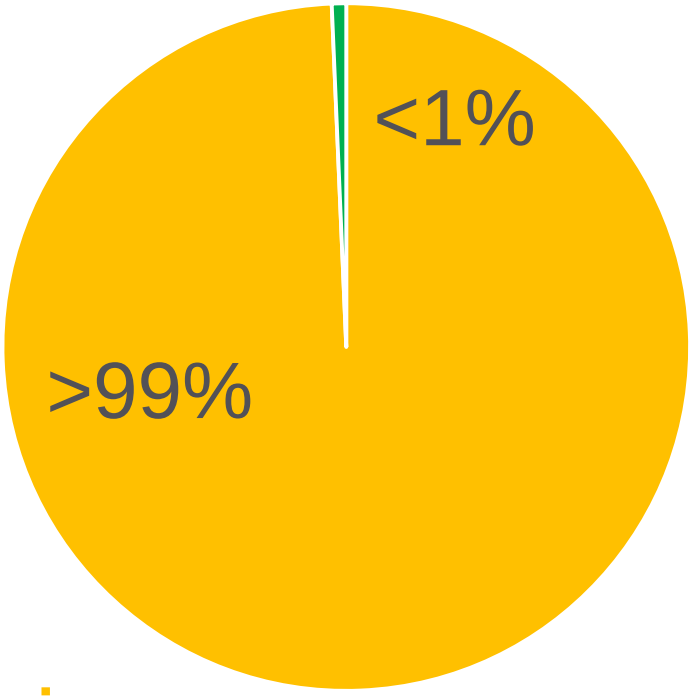


Typical Day in The Life
DDoS Queries Seen at a Resolver

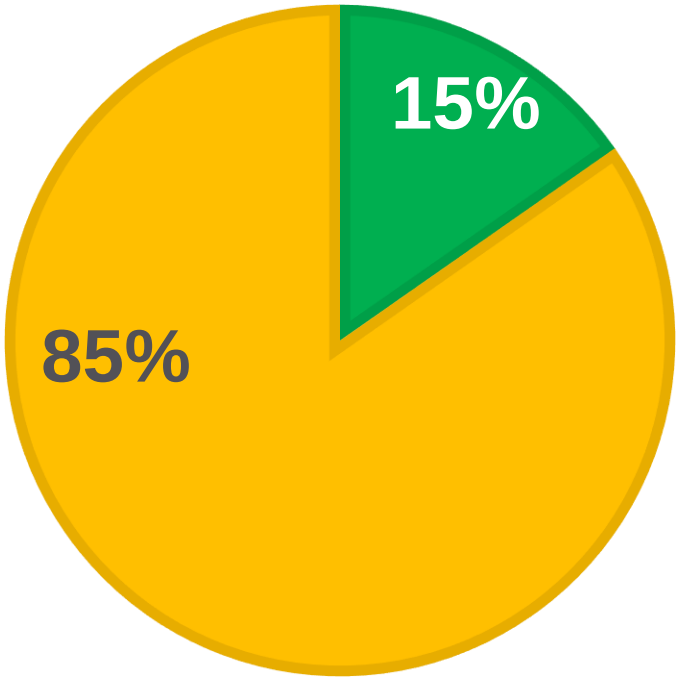
Amplifi-
cation

Random
Subdomain

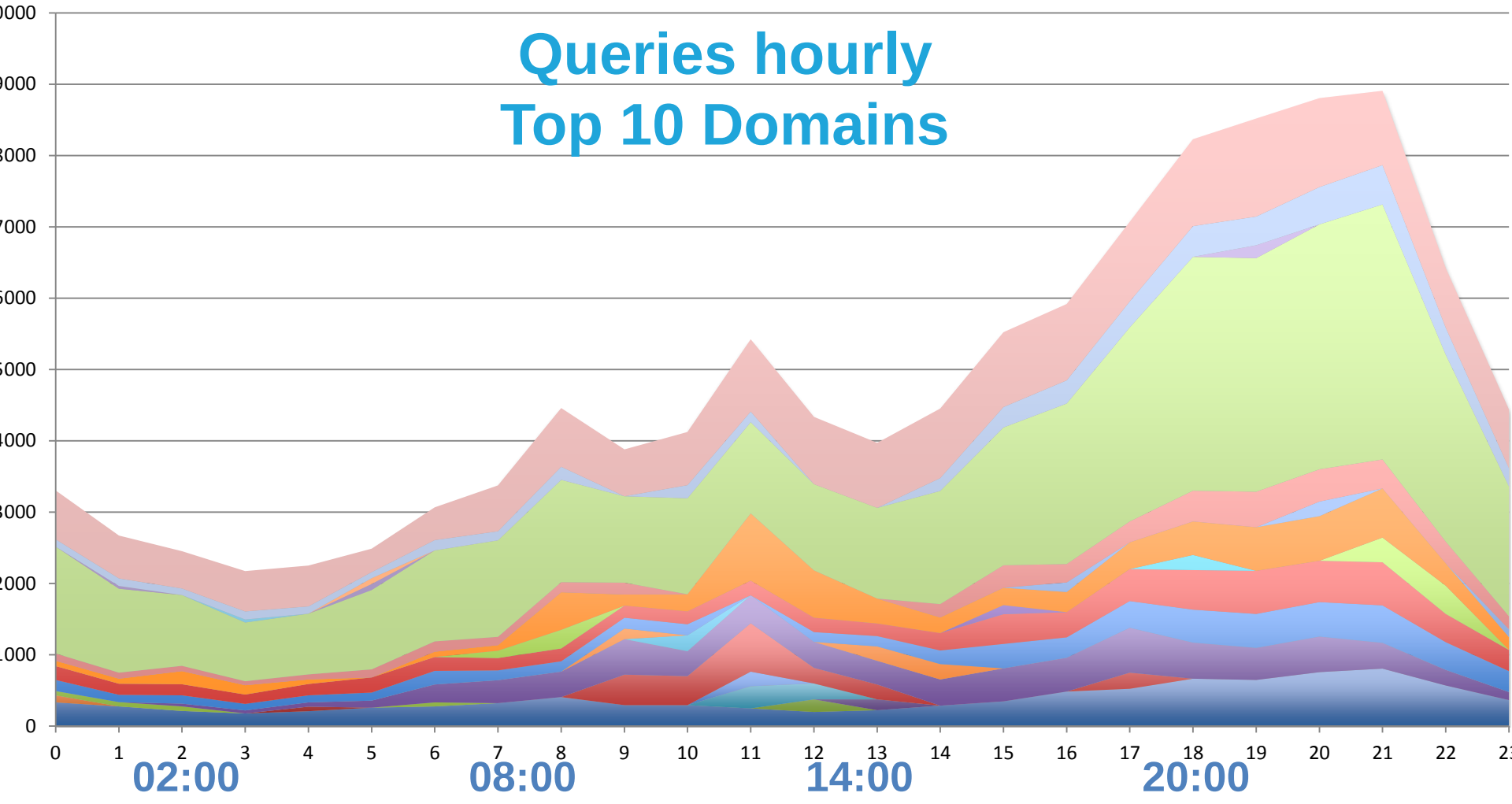
EMEA
Resolver



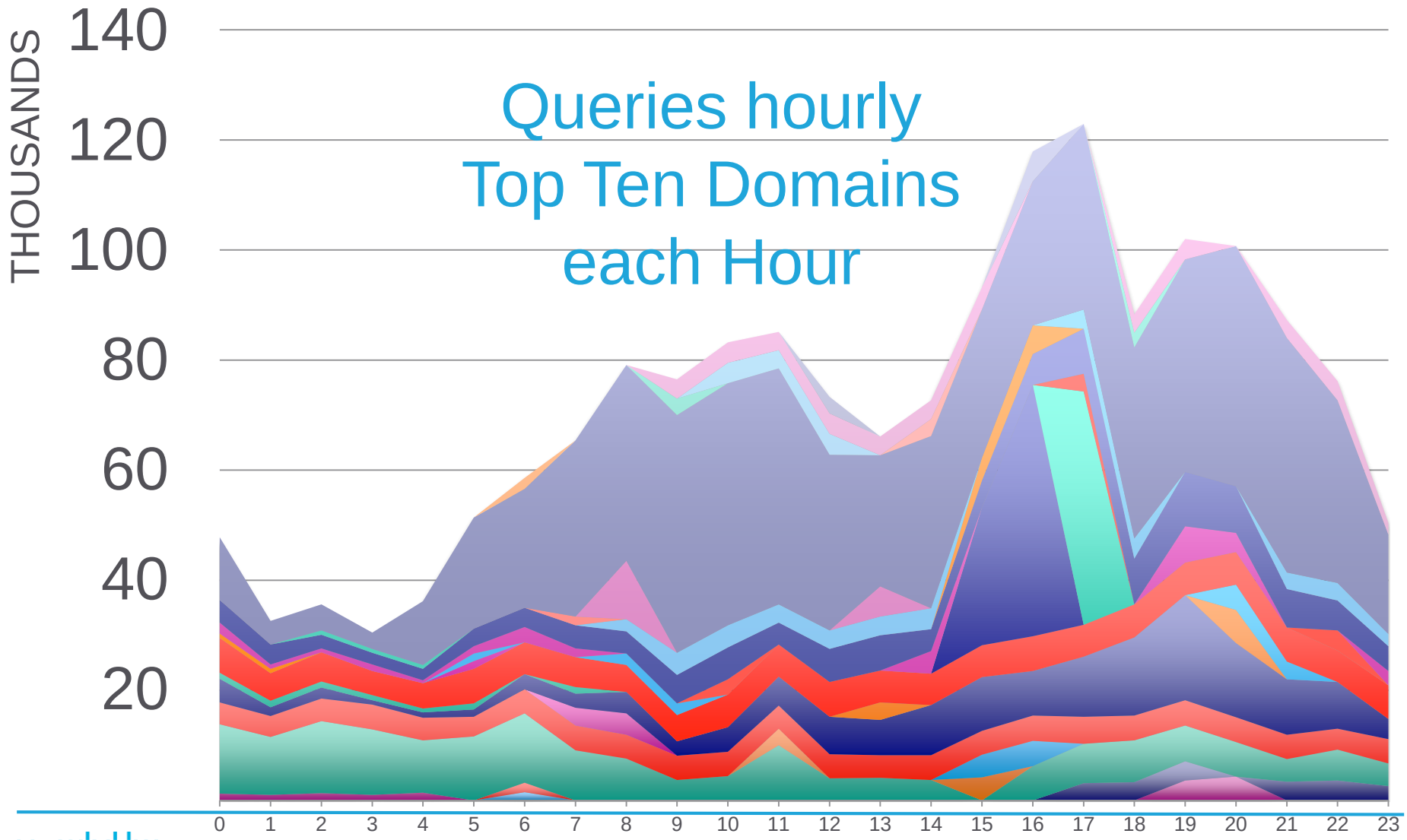
Worldwide
Average



ANY Queries


Queries hourly
Top 10 Domains
0000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
02:00
08:00
14:00
20:00

Other Malicious Activity – Bots Malware



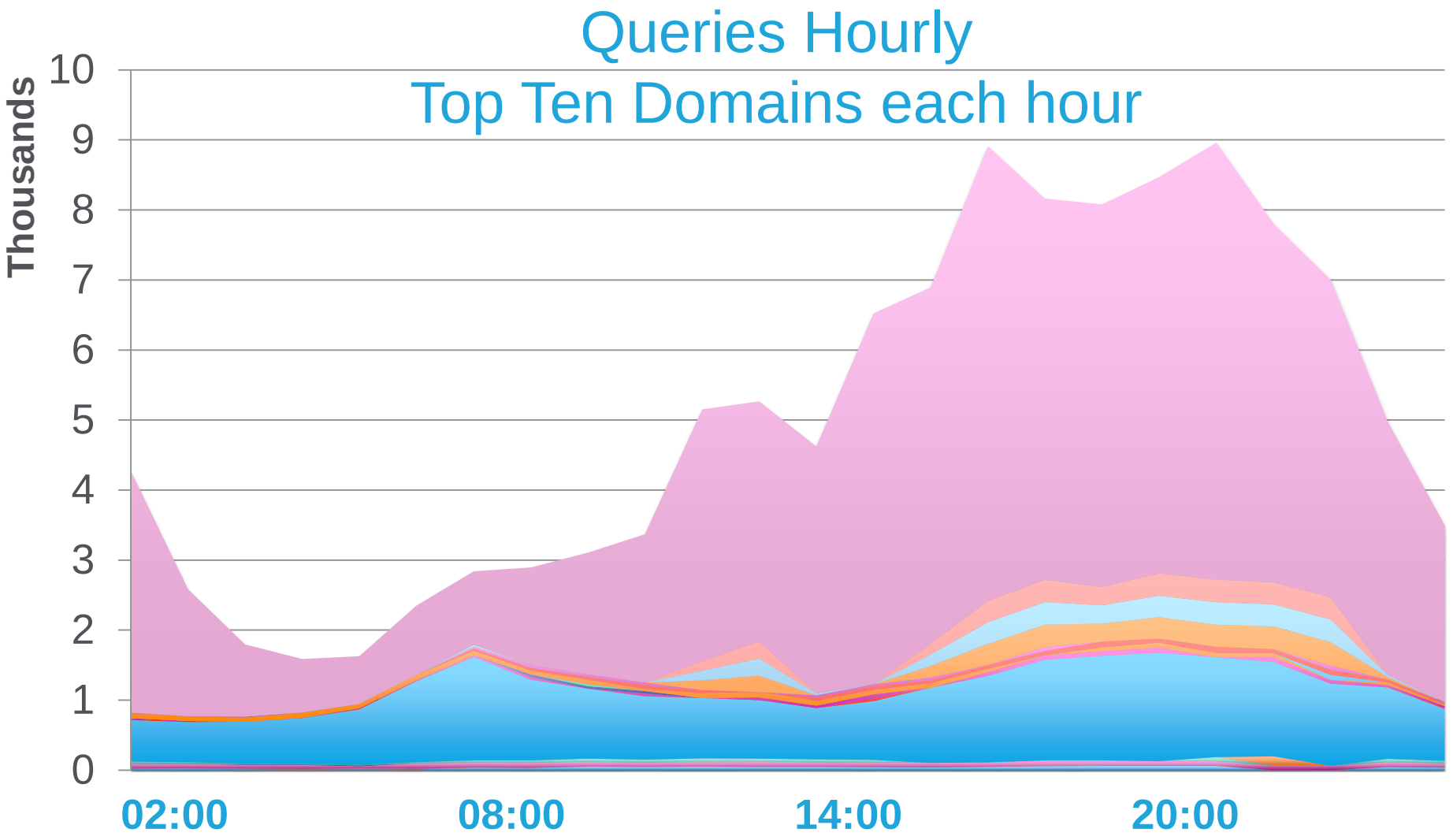
nominum

DDoS Bot Gateway

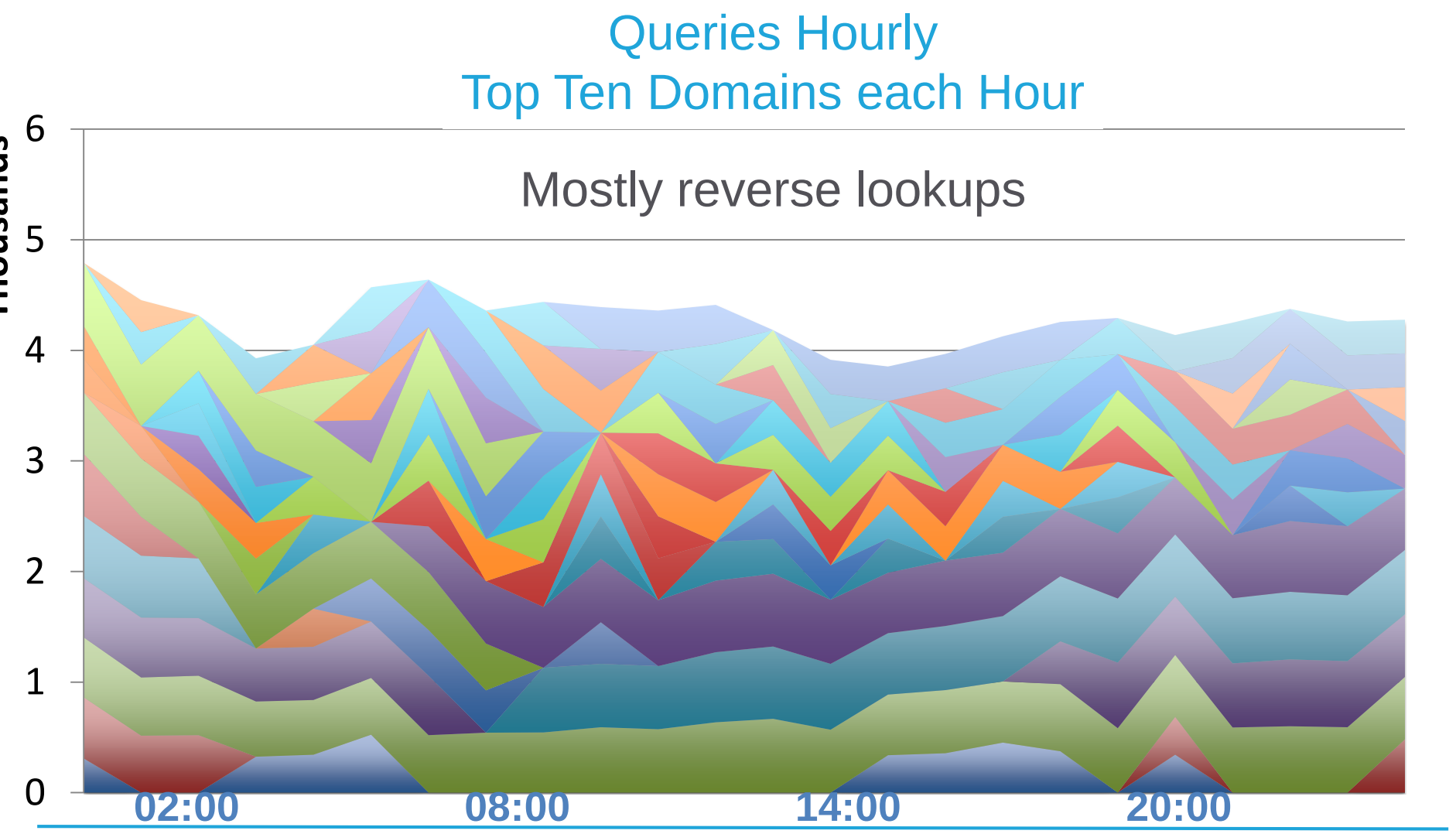
Queries – Top 20 non-attack domains queried
Lots of AV updates!

1. 1.courier-sandbox-push-apple.com.akadns.net.
2. a1363.dscg.akamai.net.
3. a568.d.akamai.net.
4. e10088.dspb.akamaiedge.net.
5. crl.microsoft.com.
6. fe2.update.microsoft.com.
7. fe2.update.microsoft.com.akadns.net.
8. nexus.officeapps.live.com.
9. Iprep1.zyxel.ctmail.com.
10. Iprep2.zyxel.ctmail.com.
11. Iprep3.zyxel.ctmail.com.
12. Iprep4.zyxel.ctmail.com.
13. Iprep5.zyxel.ctmail.com.
14. ipres.1.geo.ctmail.com.
15. ipres.2.geo.ctmail.com.
16. ipres.3.geo.ctmail.com.
17. ipres.4.geo.ctmail.com.
18. ipres.5.geo.ctmail.com.
19. liveupdate.symantec.d4p.net.
20. liveupdate.symantecliveupdate.com.

Other Query Types: MX

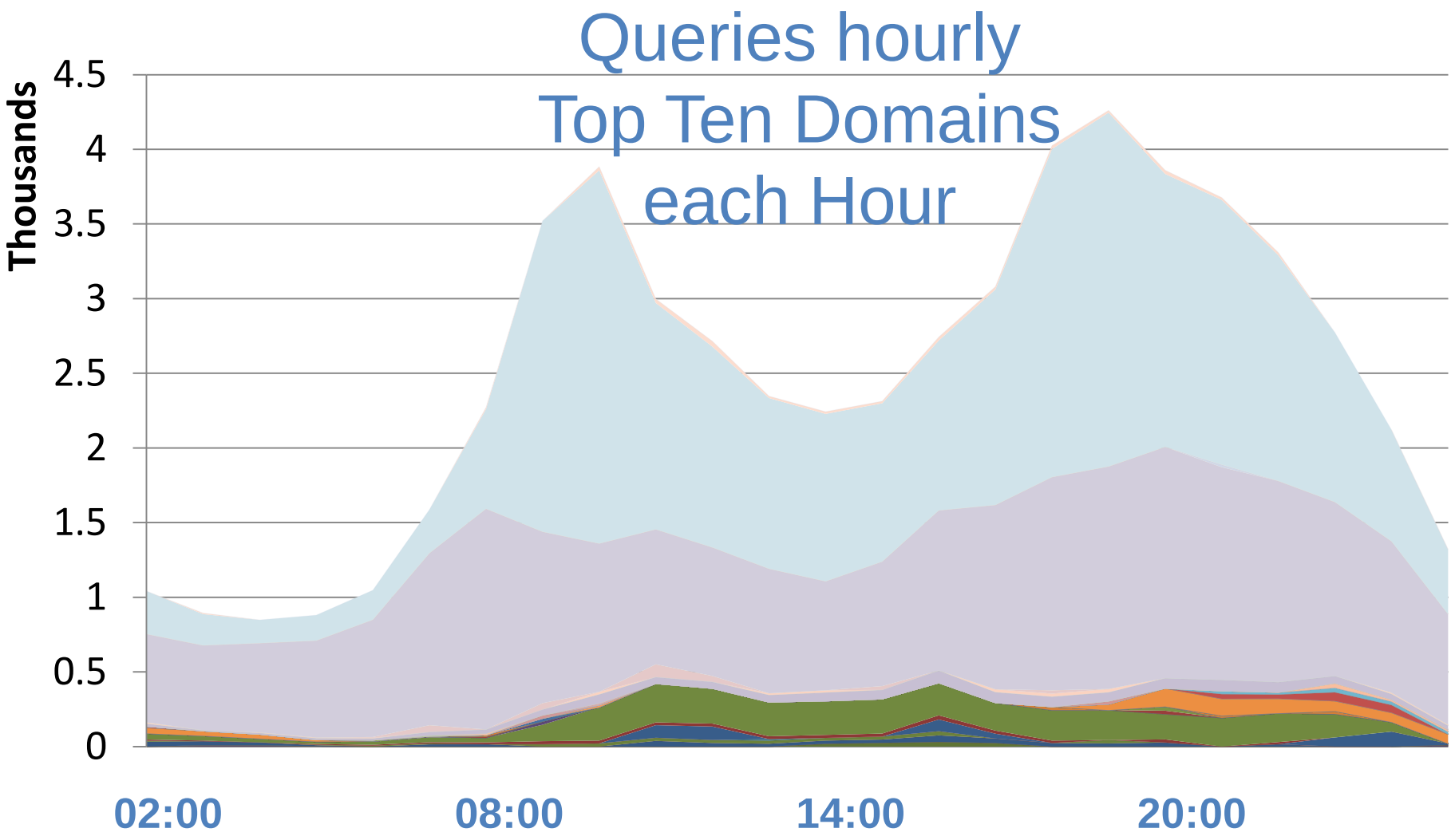


Queries with DO Bit Set



nominum

Queries Over TCP



Summary

A Day in the Life of a DNS Resolver

"Normal" queries - 423 million

Random subdomain queries - 58 million

Amplification queries - 392 thousand

Bot/malware - 18 thousand

ANY - 116 thousand

MX – 121 thousand

DO bit set – 102 thousand

TCP – 60 thousand