Kdo se moc ptá

Analýza unikátních DNS dotazů

Martin Kunc • martin.kunc@nic.cz • 24. 11. 2017

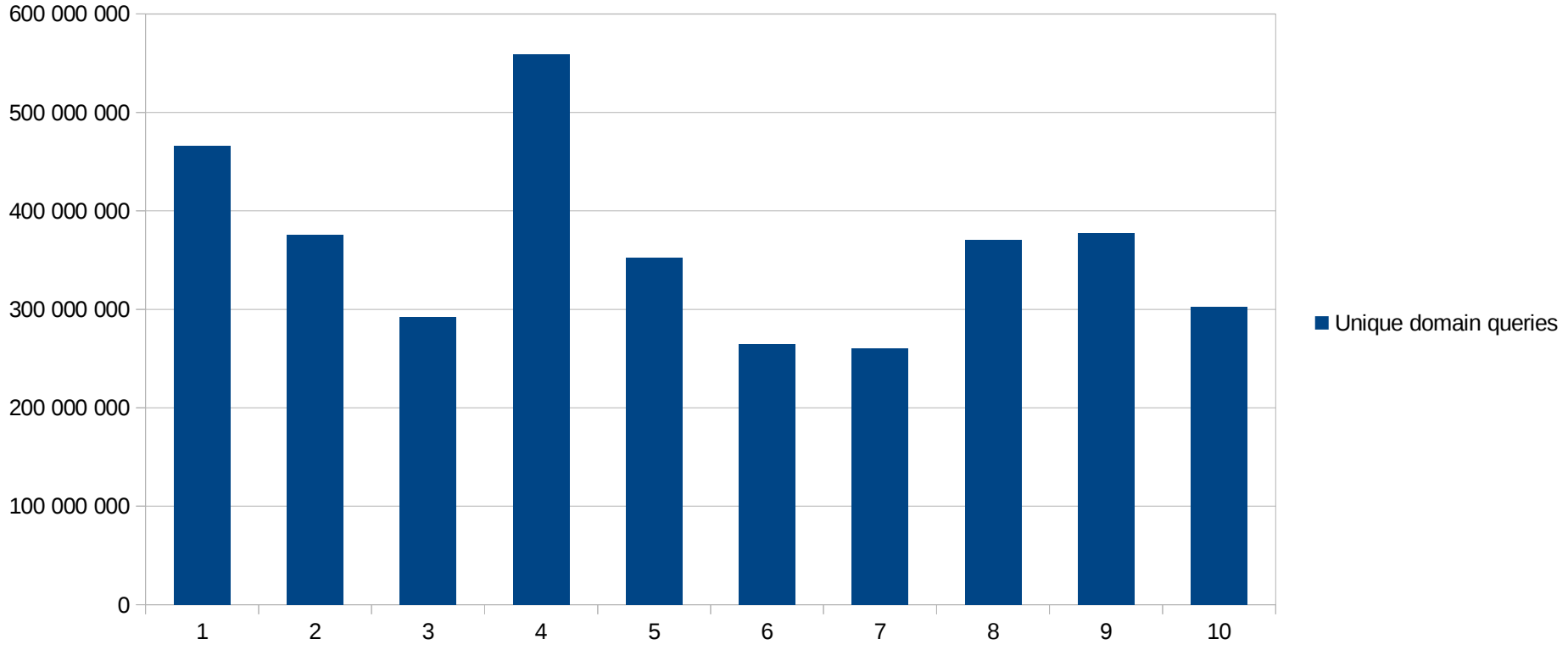
Systém Adam

- Advanced DNS Analytics and Measurement
- Entrada
  - Hadoop
  - Apache Impala
  - Apache Parquet

Celkový počet domén .cz

- 1 306 172 .cz domén (23.11.2017)

Počet dotazů na unikátní domény letos



Kdo se tedy ptá?

- Velcí hráči (co se počtu dotazů týče)
  - Georgia Institute of Technology (Gatech)
  - Yandex
  - Amazon
  - XS4ALL
  - DomainTools, LLC

GATECH

- Zeptáme se

  part of our Active DNS project.

- https://www.activednsproject.org
- Nabídli odebrání ze scan listu

Yandex

- m.j. vyhledávač
- Nejzajímavější aktivita
- Velké množství dotazů na unikátní domény

Yandex

- m.j. vyhledávač
- Stejně se zeptáme – Defaultní odpověď...

```
not an attack, but the routine activity of one of
our service bots, which is a part of our web
search engine Yandex.com/Yandex.ru
```

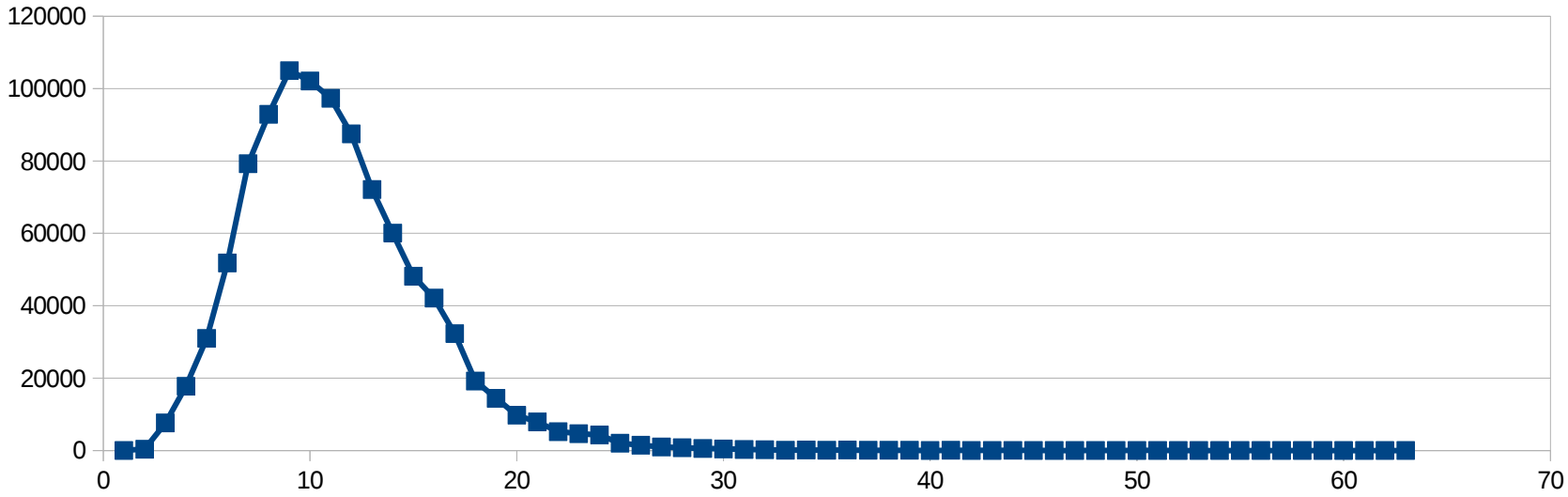
- Čím je zajímavý?

Yandex

- Významnější DNS resolvery cca 500 000 až 1 000 000 unikátních qname denně
  - Např: neco.cz ale i neco.neco.cz
- Yandex?
  - Např i 4 771 534

Gatech vs Yandex

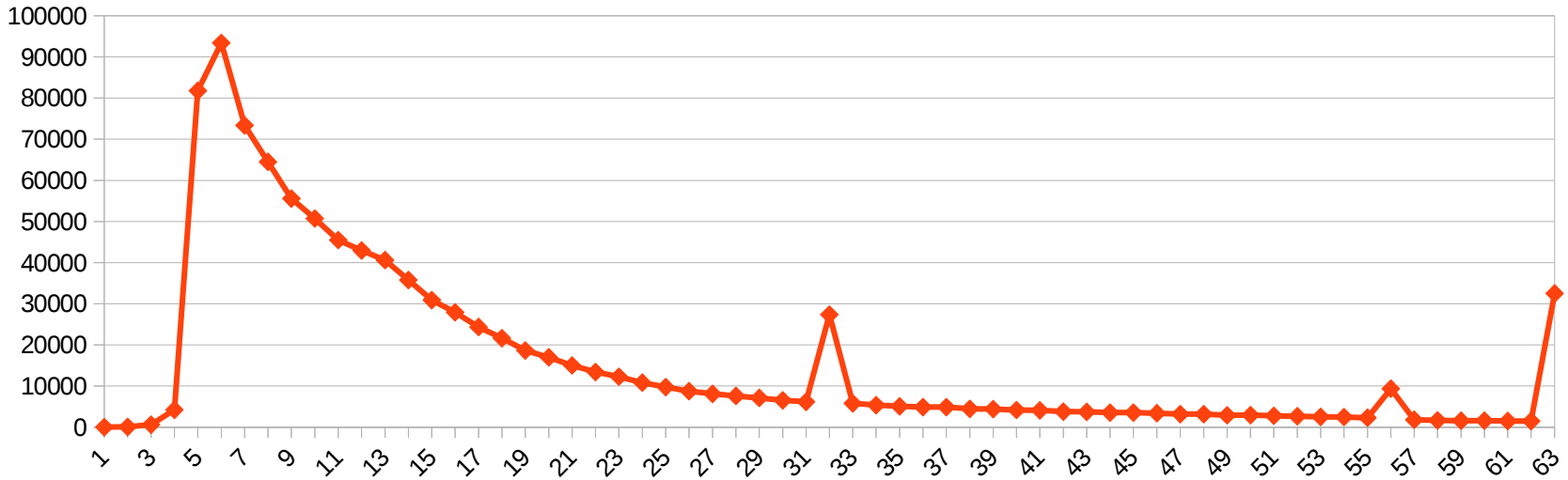
- Gatech:



- jakoby-ceska-domena.cz

Gatech vs Yandex

- Yandex (jedna IP) + abecedně:



- vdc9x7ps0.cz

Yandex

- Yandex
- 12.1.2017
- Od uypelf5z878xj9yezyerx.cz
- Po vectisoft.cz
- Abecedně

Yandex

- 23.12.2016 – 11.1.2017
- 54 852 534 unikátních qname
- 54 755 113 unikátních domén
  - .cz celkem ~1,3 mil. omén
- Z jedné IP

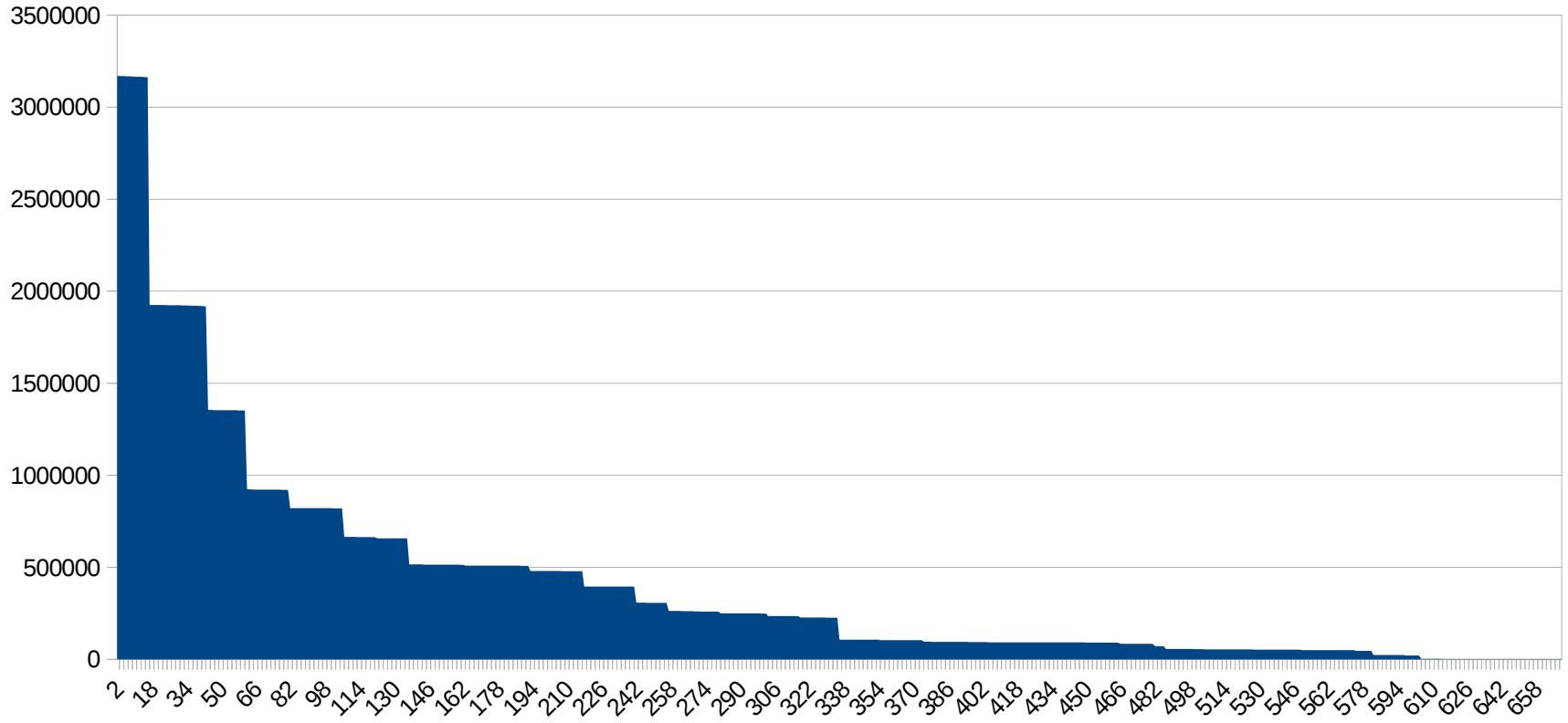
Yandex IP nebyla jedinná

535 693 588

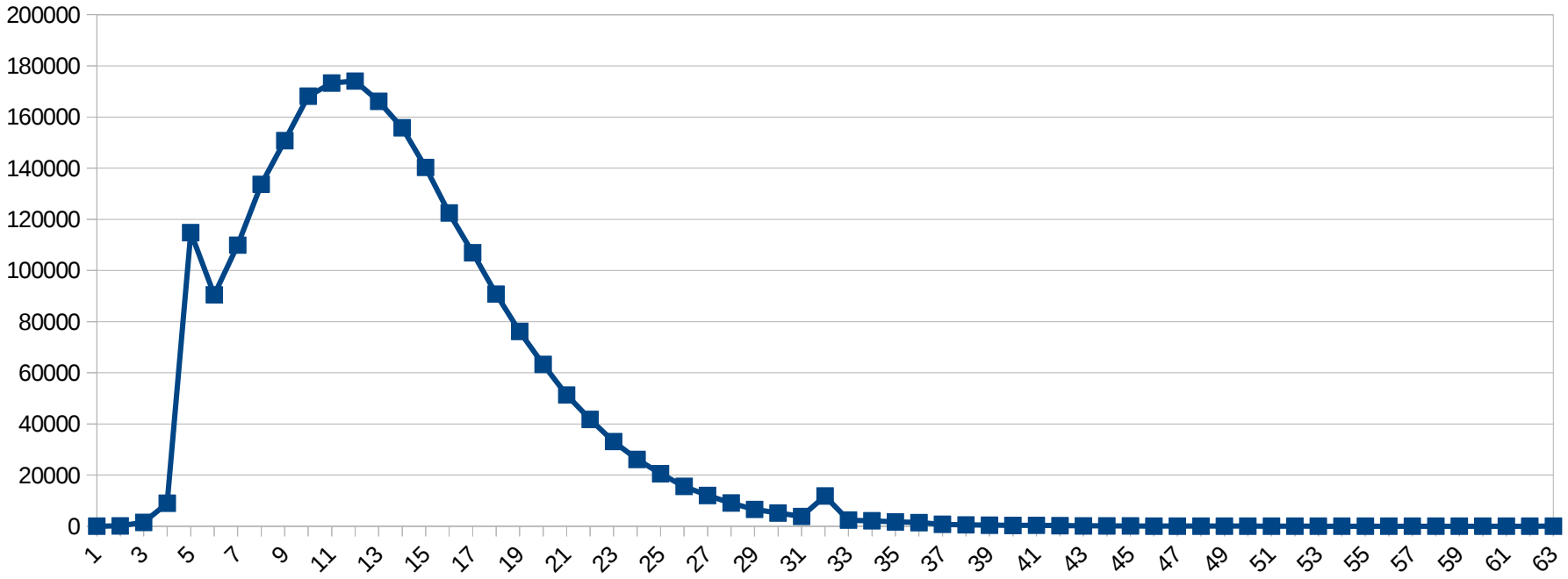
A co Google?

- Maximum během února
- 3 170 495 z jedné IP
- 60 IP adres > 1 000 000 unikátních dotazů
- 115 459 342 celkem

A co Google? Víc IP adres



A co Google?


200000
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
1
3
5
7
9
11
13
15
17
19
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51
53
55
57
59
61
63

Amazon?

- Nejzvědavější IP adresa
- 155 990 964 unikátních dotazů během jednoho měsíce (březen)

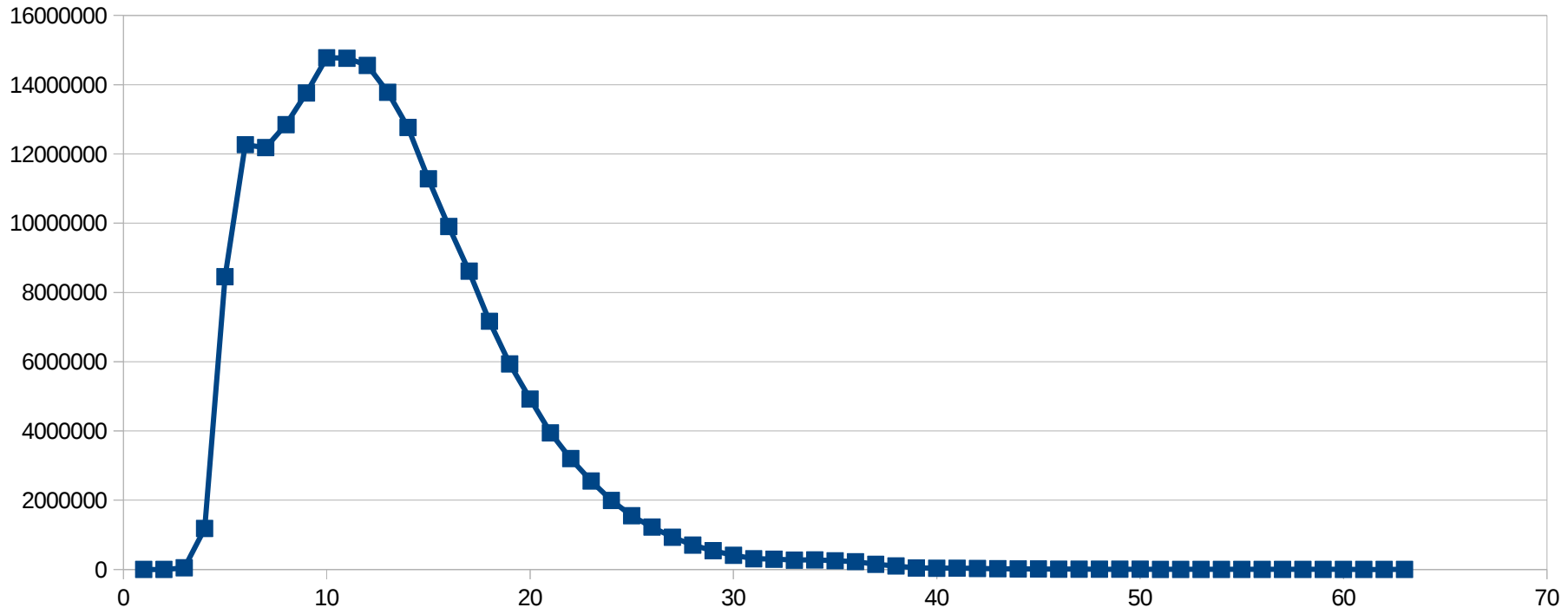
Další zajímavosti

- Časté shluky IP adres – stejný rozsah, vysoký počet dotazů
- Duben – Yandex (první místo)
  - 13 IP adres x 34 000 000 dotazů
- Google jen 2x v prvních 50ti

Další zajímavosti

- DigitalOcean – žádné shluky, IP z různých rozsahů
- Za říjen top 19 IP adres s průměrem 19 000 000 unikátních dotazů
- 198 427 349

DigitalOcean



Děkuji za pozornost

Martin Kunc • martin.kunc@nic.cz