

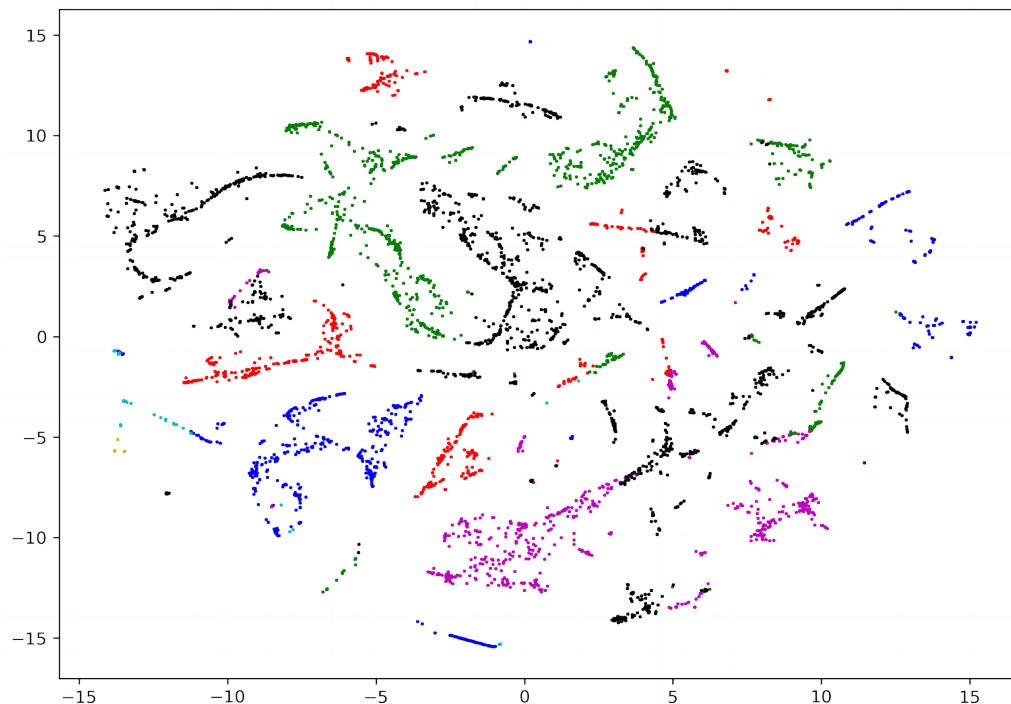
DNS provoz .CZ

Co prozradí BigData

Petr Černohouz • petr.cernohouz@nic.cz • 20. 06. 2017
Bedřich Košata • bedrich.kosata@nic.cz

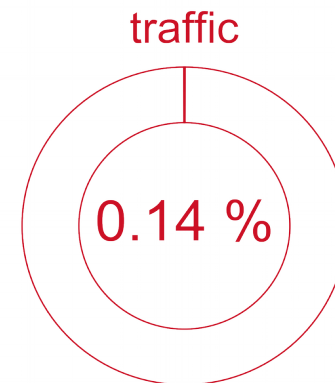
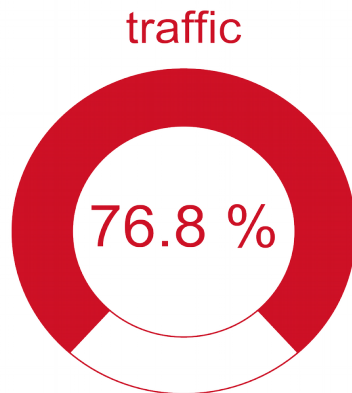
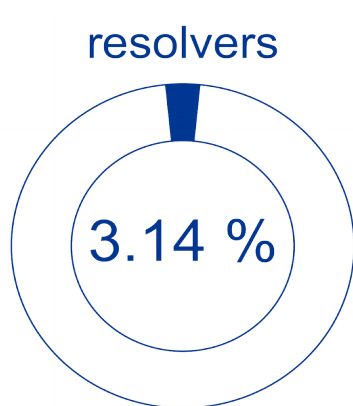
Zkoumaná data

- 1,3 milionu domén
- Období Q1 2017
 - 10 000 dotazů/s
 - 8,5 milionů unikátních IP adres (resolverů)
 - 775 milionů unikátních qnames



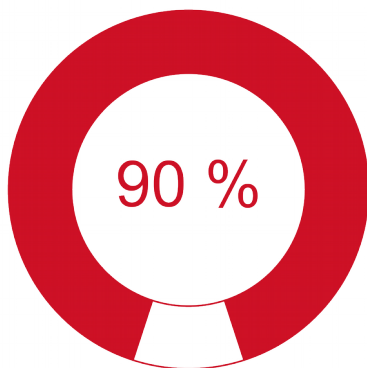
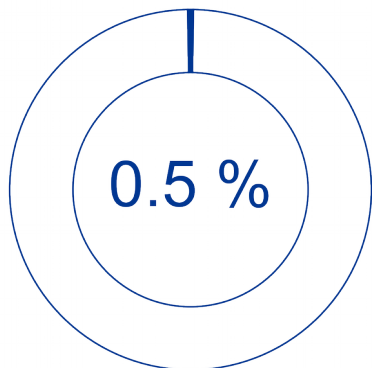
Resolvery

- 3,14 % aktivních každý den
 - Generují 76,8 % provozu
- 50,9 % aktivních pouze 1 den
 - 0,14 % provozu

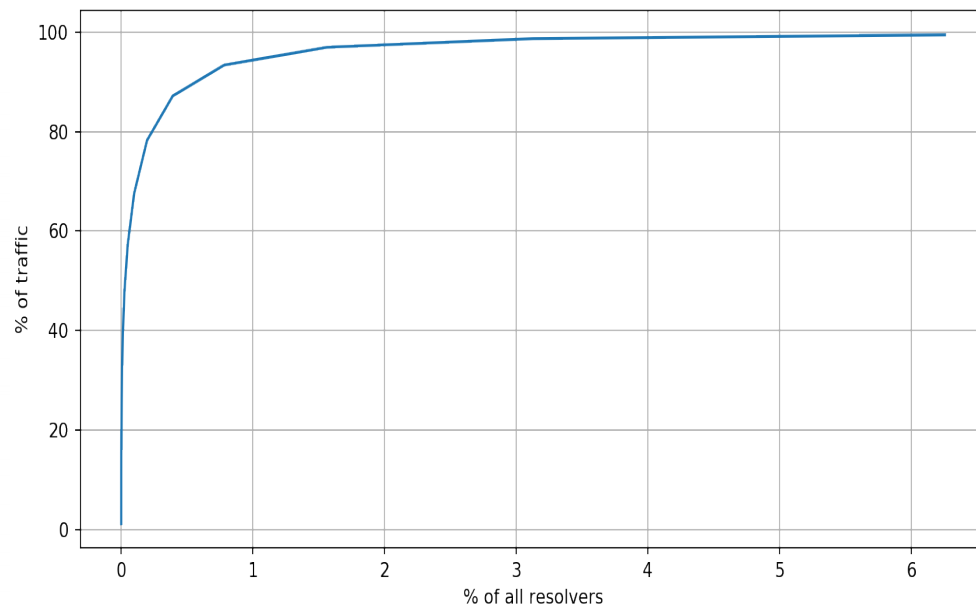


Resolvery

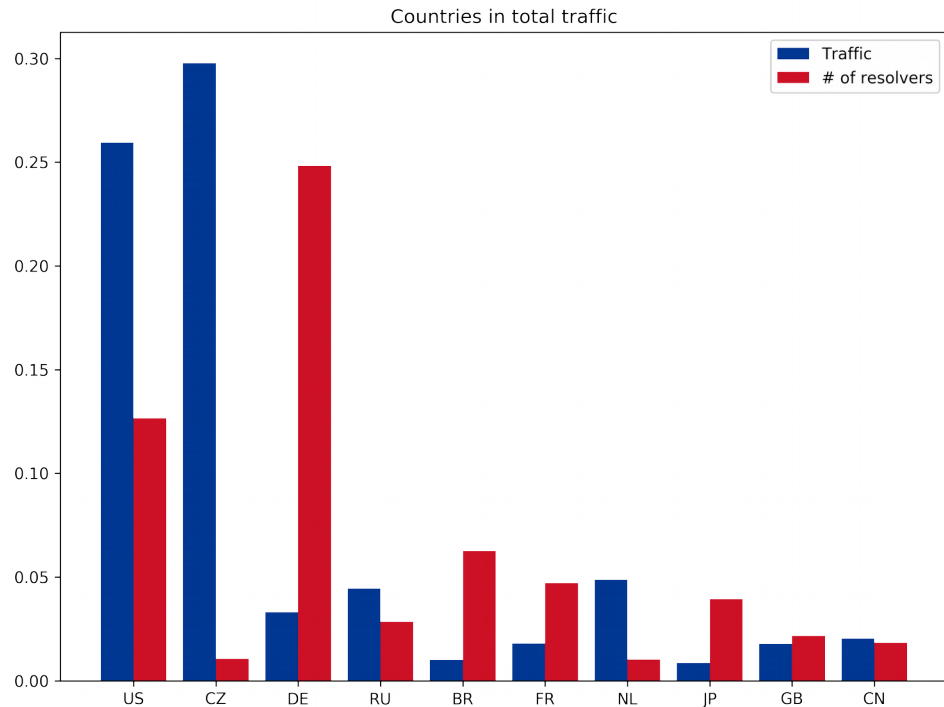
- 0,5 % největších generuje 90 % provozu
- Ne vždy jsou vidět každý den resolvers



- Podíl resolverů na celkovém provozu



Země odkud se resolvery ptají



- Porovnání s doménou .nz
 - 7 z 10 zemí stejných
 - .de a .fr – větší podíl resolverů než provozu

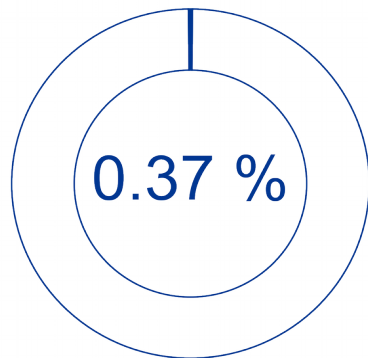


Qnames

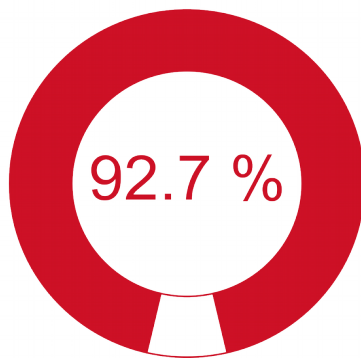
- 0,37 % dotazováno každý den

- Generuje 92,7 % provozu

qnames



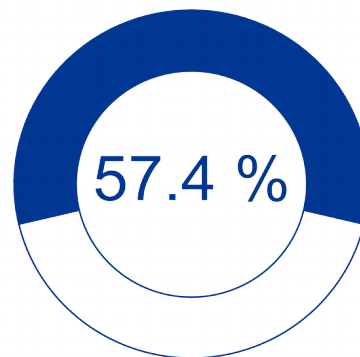
traffic



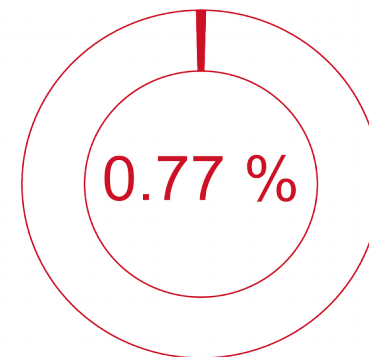
- 57,4 % dotazováno pouze jeden den

- Generuje 0,77 % provozu

qnames



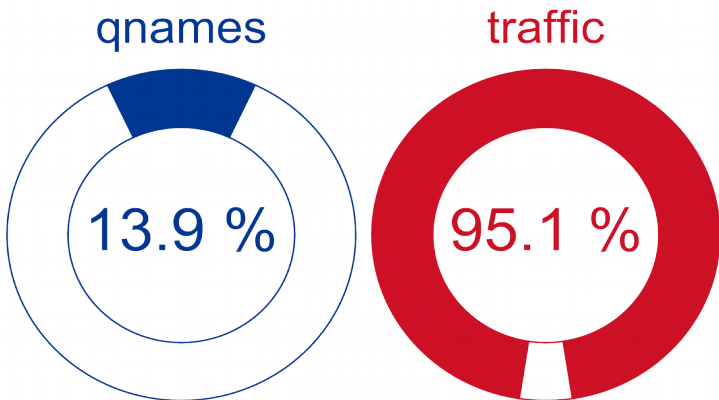
traffic



Qnames – návratové hodnoty

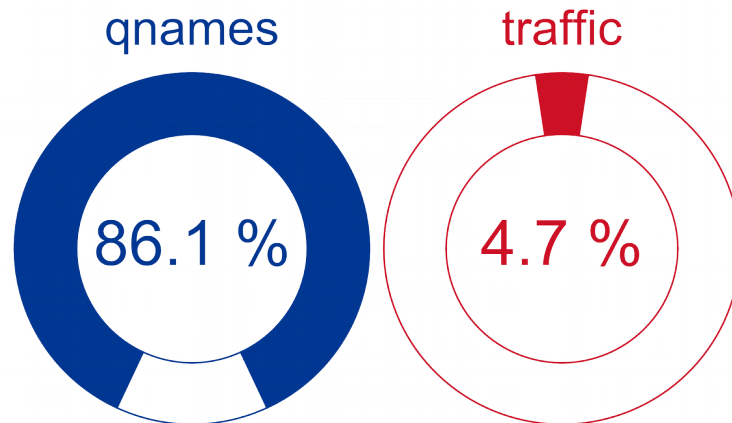
- NOERROR – 13,9 %

- 95,1 % provozu



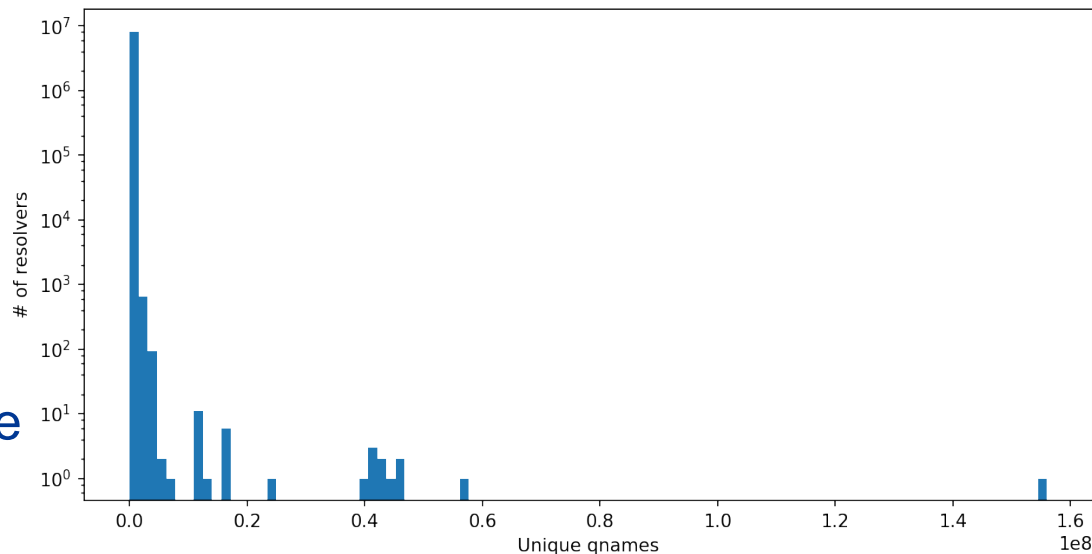
- NXDOMAIN – 86,1 %

- 4,7 % provozu



Zajímavá čísla – všechny resolvers

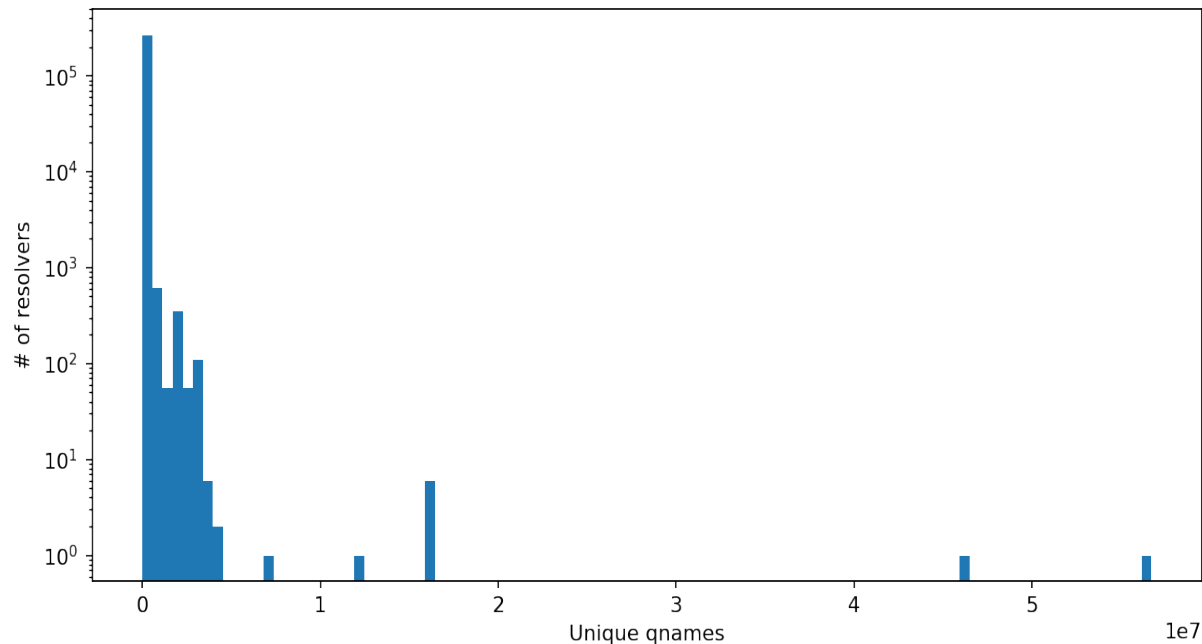
- Unikátní qnames/resolver
 - Median: 3
 - Percerntil 90: 50
 - Percentil 99: 5 633
 - Maximum: 155 996 471
 - Amazon AWS EC2 instance



Zajímavá čísla – aktivní resolvers

- Resolvery aktivní denně

- Median: 701
- Percentil 90: 21 373
- Percentil 99: 289 373
 - Jen 0,5 % maxima
- Max: 56 725 350
 - ns1.vodafone.ie



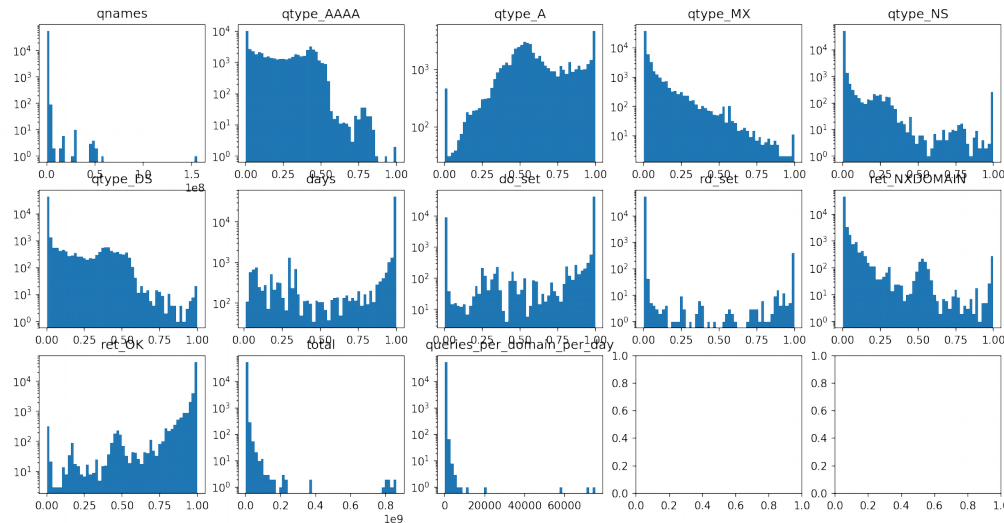
Hledání okrajových případů

- Definice „standardního“ profilu dotazů
- Resolvery budou mít normální rozložení
- Čím dále od středu, tím podezřelejší
- Tudy ne!
- Veškerý provoz z Q1 2017
- Resolvery s více než 100k dotazy
 - 57 000 resolverů (0,7 %)
 - 92,3 % provozu
- Každý resolver popsán vektorem metrik



Hledání okrajových případů – data

- 13 metrik
 - Poměr Qtypes – A, AAAA, MX, NS, DS
 - Poměr Rcodes – NOERROR, NXDOMAIN
 - Poměr RD a DO bitů
 - Počet dotazů, unikátních Qnames, dnů aktivity, dotazů/doménu/den



Jak dále?

- Pokus najít standardní chování
- Definování „odchylky“ od normálu
- Hledání situací, kdy resolvers vybočují ve více kritériích
- Machine learning

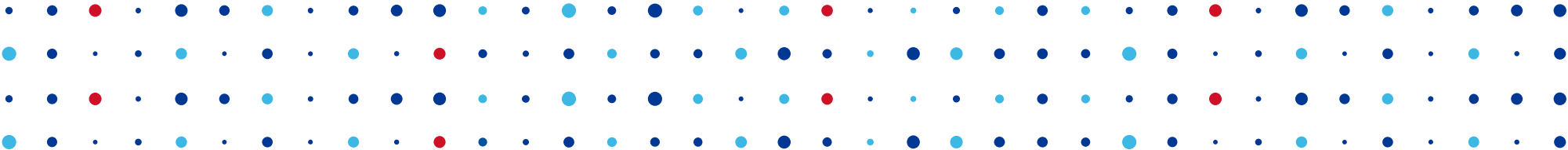


Zdroj: <https://xkcd.com/1838/>



Dotazy?





Děkuji za pozornost

Petr Černohouz • petr.cernohouz@nic.cz
Bedřich Košata • bedrich.kosata@nic.cz