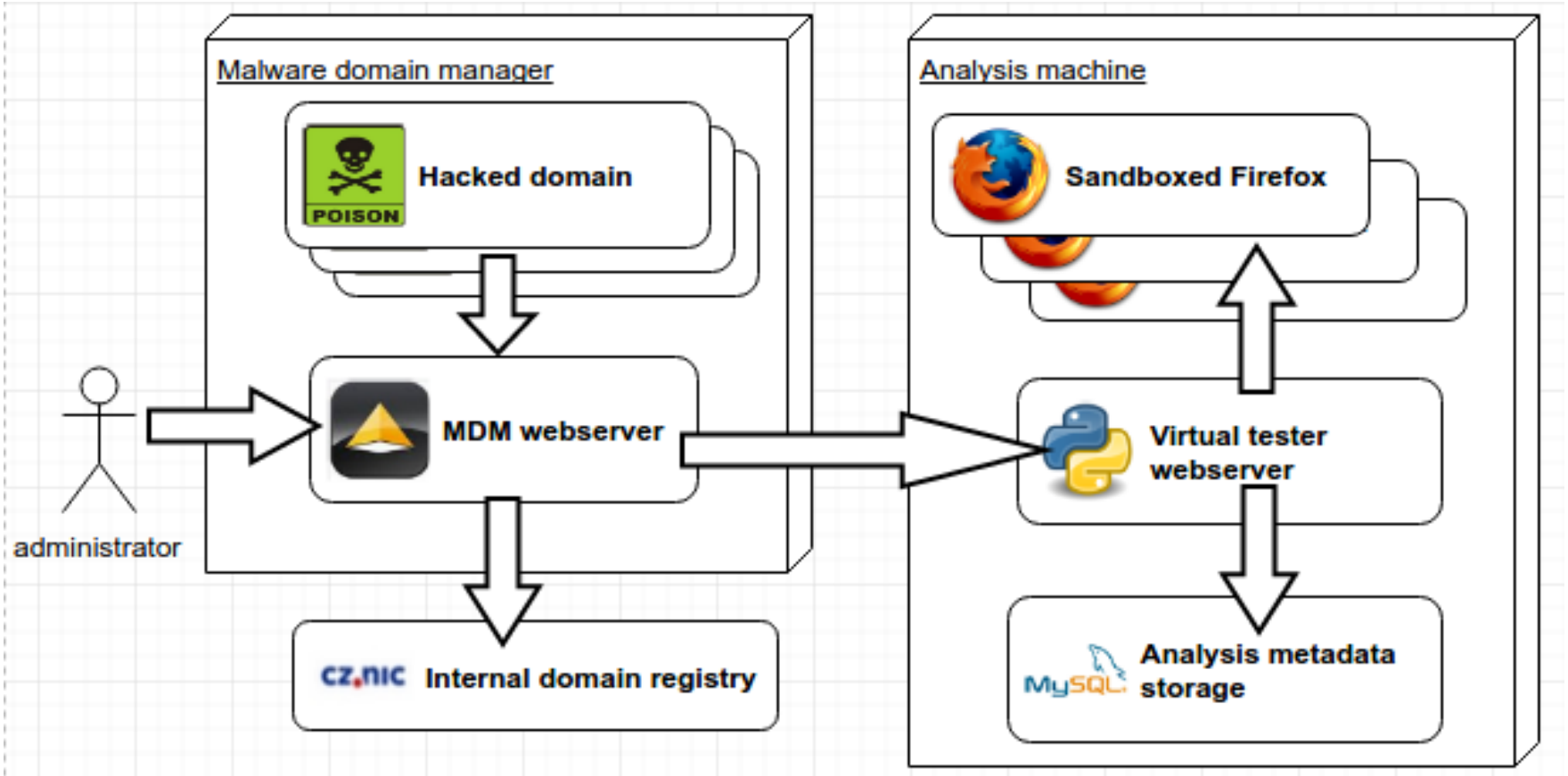
Hledání malware

na 10 000 doménách

Edvard Rejthar • edvard.rejthar@nic.cz • 15. 11. 2018

CZ.NIC | SPRÁVCE DOMÉNY CZ

MDMaug interface



Mdmaug

ostravskykompot.cz
adrealinvest.cz
femalelife.cz
foppapedretti-monad.cz
bubbleways.cz
modry-mauricius.cz

analyze

Multiple URLs

Cache max age:

No cache
Yesterday
Week
Any cache
Max days

Google Safebrowsing

PDNS

Geoip

Autoprune

Creation spree

6:46 PM Scan for pastingroup.cz already exists.

Requests 1279... / 11000 (684 s)

4 threads

6 s bdvyskovicka178.cz
✓ pastingroup.cz
✓ cestakeklidu.cz
✓ i-superstore.cz
✓ hydraulika-praha.cz
11 s mandalia.cz
✓ dido.cz
17 s agenturahledajici.cz
✓ delticom.cz
✓ netflix.cz
✓ tvojemistax.cz
19 s praguepictures.cz
✓ prodejnemovitosti-trebic.cz
✓ rockovyslunovrat.cz
✓ 21 s bezdratovakancela
✓ skodaci.cz
✓ kaznet.cz

02.10.2018 06:34 - 09.10.2018 06:34

aggregate

http://bezdratovakancelar.cz

09.10.2018 18:45

n/a **bezdratovakancelar.cz**

- / →

n/a **www.bezdratovakancelar.cz**

89.221.213.28

- / →
- /wp-json/
- /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.0.1
- /wp-content/themes/Divi/style.css?ver=3.0.106
- /wp-includes/css/dashicons.min.css?ver=4.9.8
- /wp-content/plugins/jetpack/css/jetpack.css?ver=5.9
- /wp-includes/js/jquery/jquery.js?ver=1.12.4 →
- /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
- /wp-content/plugins/duracelltomi-google-tag-manager/js/gtm4wp-form-move-tracker.js?ver=1.7.2 →
- /wp-content/cache/et/global/et-divi-customizer-global-15375435650506.min.css
- /wp-content/uploads/2018/03/bezdratova-logo-480.png

Bezdrátová kancelář.cz

Kontakt

Martin LÉVAY
00420 605 279 984
Po-Pá 10-16 hodin
martin@levay.cz

Bankovní spojení:
č.ú. 2800701891/2010
variabilní symbol použijte vaše telefonní číslo

iPhone

MacBook

iCloud

WiFi

Whitelists

- Add-on hard coded URL
  - Internal redirect http://localhost/redirect/
  - http://www.google.com/adsense/ , http://clients1.google.com/ocsp , https://safebrowsing.google.com/safebrowsing/ , https://safebrowsing-cache.google.com/safebrowsing/
  - https://fbstatic-a.akamaihd.net/rsrc.php
  - https://tiles.services.mozilla.com/
- SQL 2nd domain

  15 domén
  - ocsp.pki.goog (3972 záznamů), google.com, gstatic.com, googlesyndication.com, google-analytics.com, google.cz, googleapis.com, googleadservices.com
  - cloudfront.net, doubleclick.net, mozilla.com, w3.org, digicert.com
  - mozilla.net, mozilla.org
- prefs.js

  detectportal.firefox.com (10942 záznamů)

Stats – 10 997 domains

- origins (7 522) × 3rd parties (8 206) × ip combinations: 43 996
  - incl. origins × 3rd parties: 36 931

Stats – 10 997 domains

- origins (7 522) × 3rd parties (8 206) × ip combinations: 43 996
  - incl. origins × 3rd parties: 36 931
- redirects to ‚www‘: 2 577
- another 3rd redirects: 95

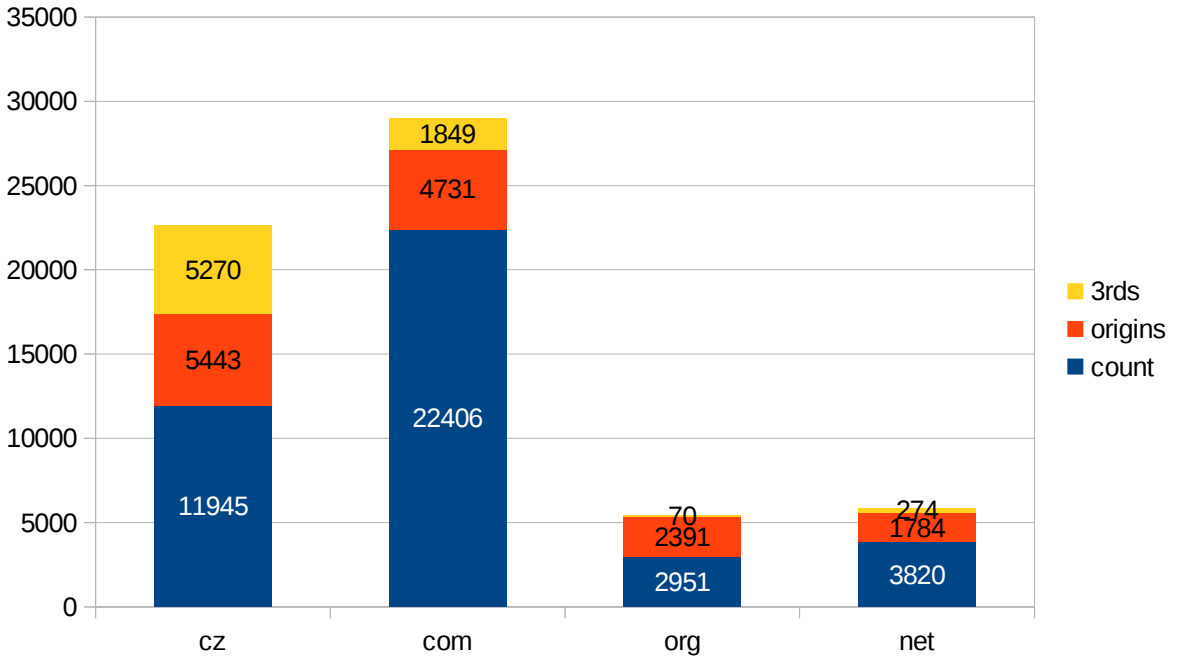
Stats – 10 997 domains

- origins (7 522) × 3rd parties (8 206) × ip combinations: 43 996
  - incl. origins × 3rd parties: 36 931
- redirects to ‚www‘: 2 577
- another 3rd redirects: 95
  - www3, w1, w17
  - img, static, cdn, media
  - admin
  - api, files, geo, legacy
  - jmeno.prijmeni.cz, public.relations.cz
  - 4th domains: www.fotbal

Stats – 10 997 domains

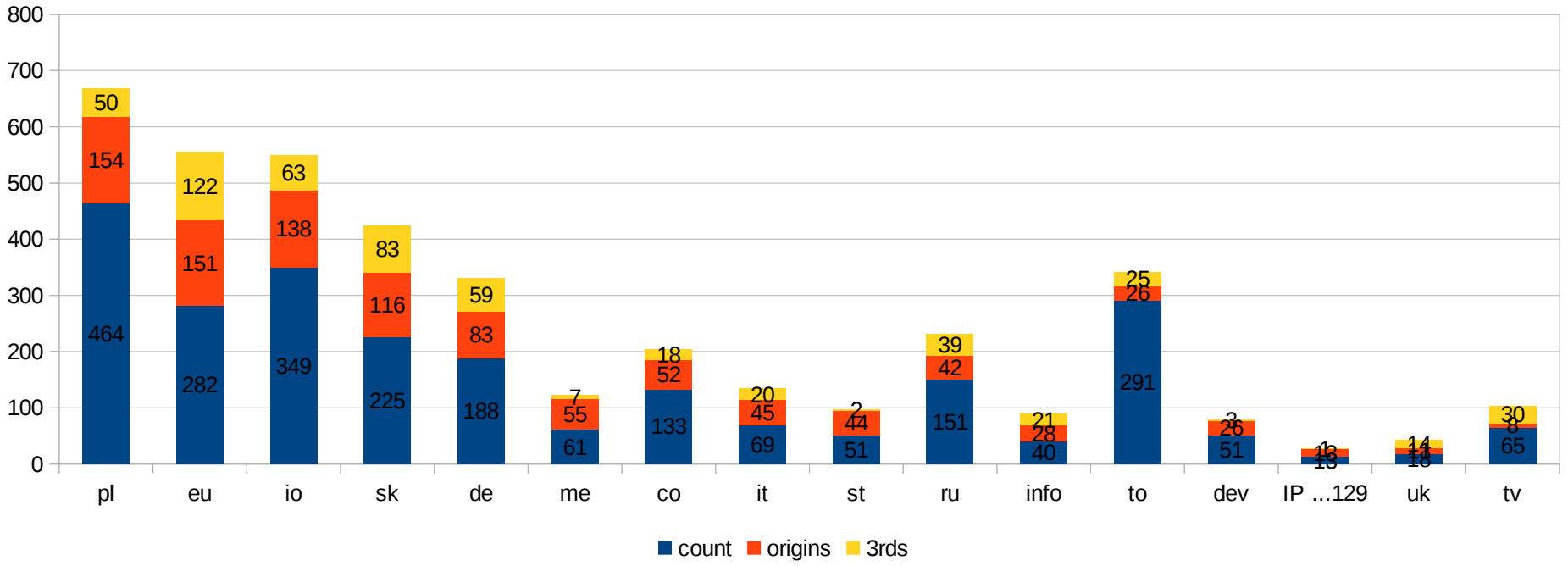
- origins (7 522) × 3rd parties (8 206) × ip combinations: 43 996
  - incl. origins × 3rd parties: 36 931
- redirects to ‚www‘: 2 577
- another 3rd redirects: 95
  - www3, w1, w17
  - img, static, cdn, media
  - admin
  - api, files, geo, legacy
  - jmeno.prijmeni.cz, public.relations.cz
  - 4th domains: www.fotbal
- timeouts: à 1400, without redirects: à 2000, redirect to self only: 593

Group by TLD charts



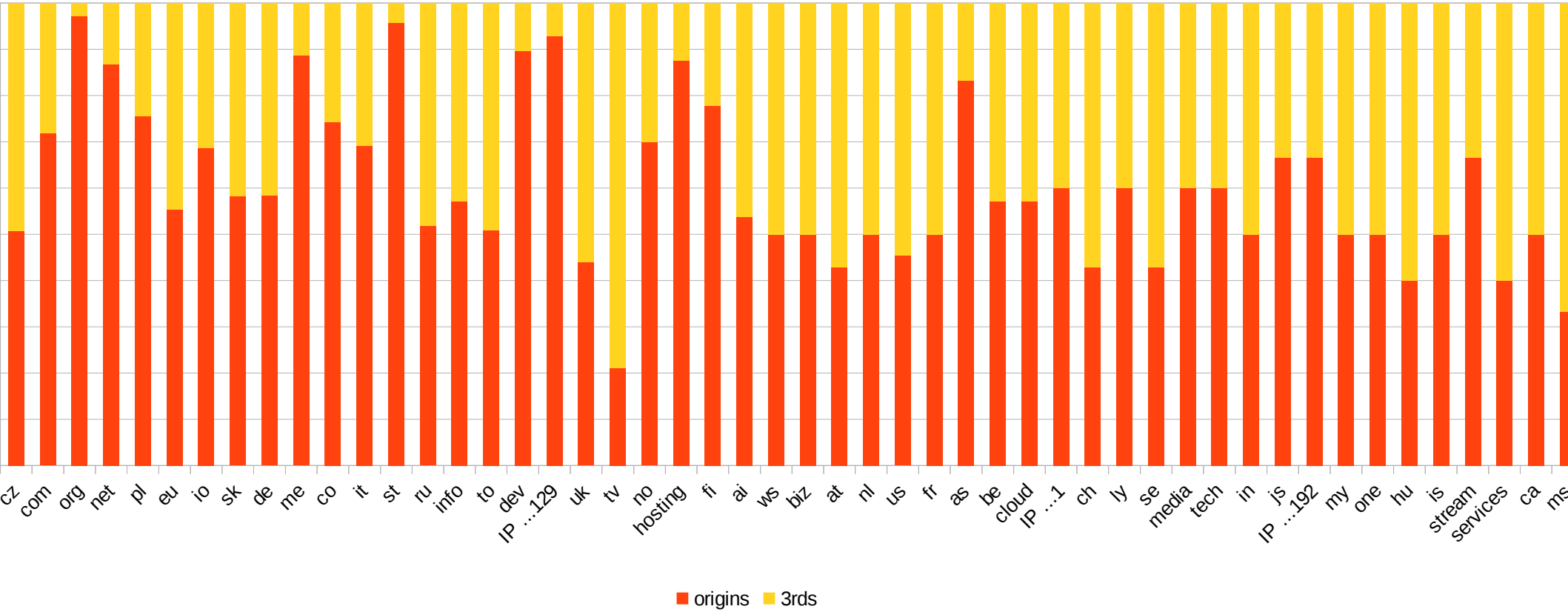
TLD	count	origins	3rds
cz	11945	5443	5270
com	22406	4731	1849
org	2951	2391	70
net	3820	1784	274
pl	464	154	50
eu	282	151	122
io	349	138	63
sk	225	116	83
de	188	83	59
me	61	55	7
co	133	52	18
it	69	45	20
st	51	44	2
ru	151	42	39

Group by TLD charts

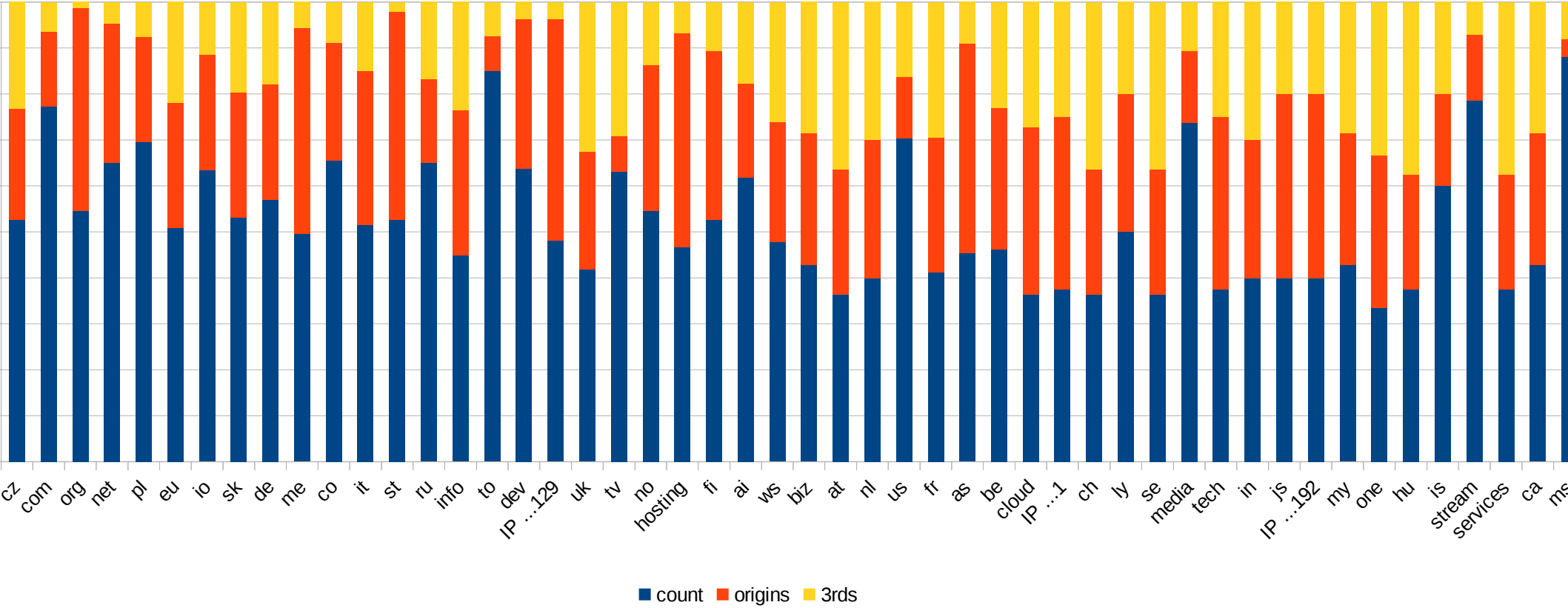


CZ.NIC | SPRÁVCE DOMÉNY CZ

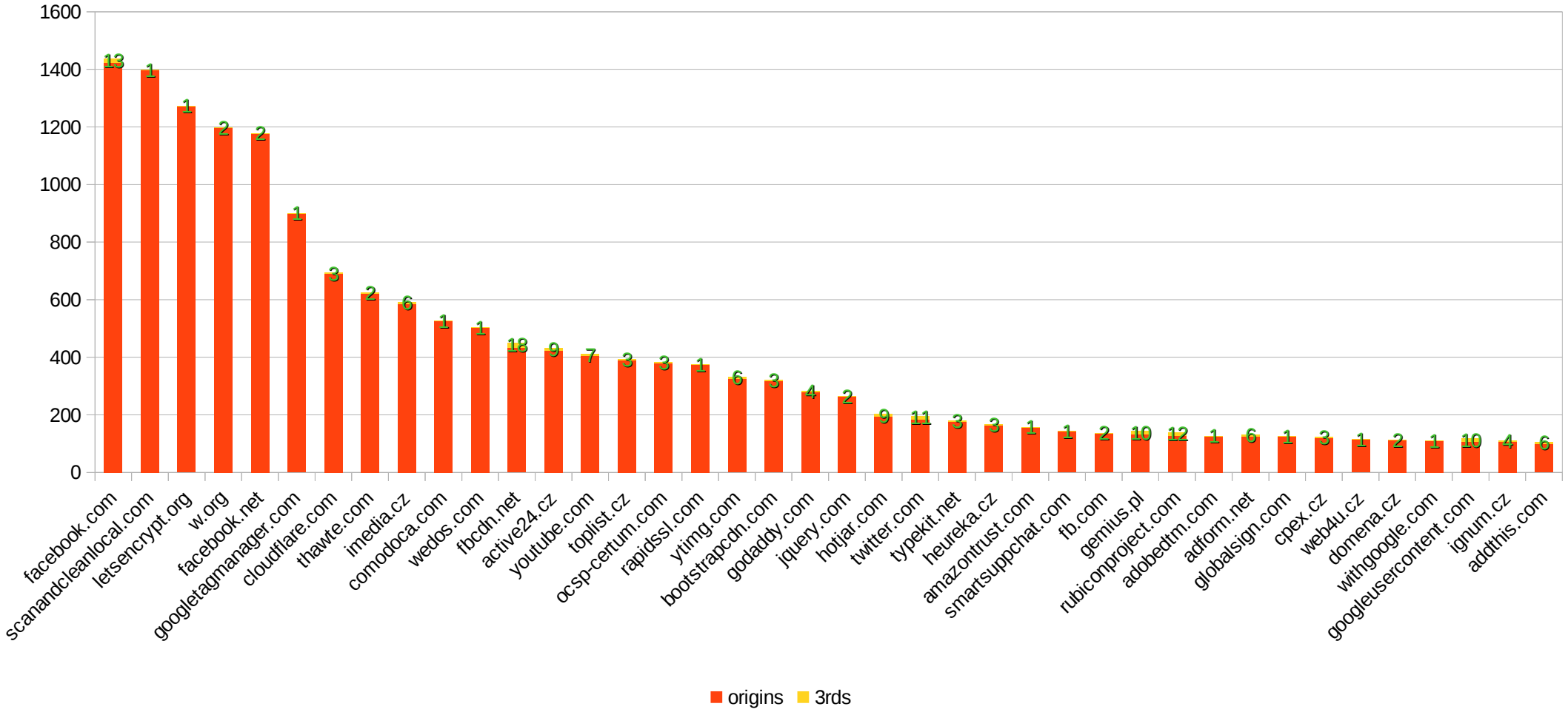
Group by TLD charts (percent)



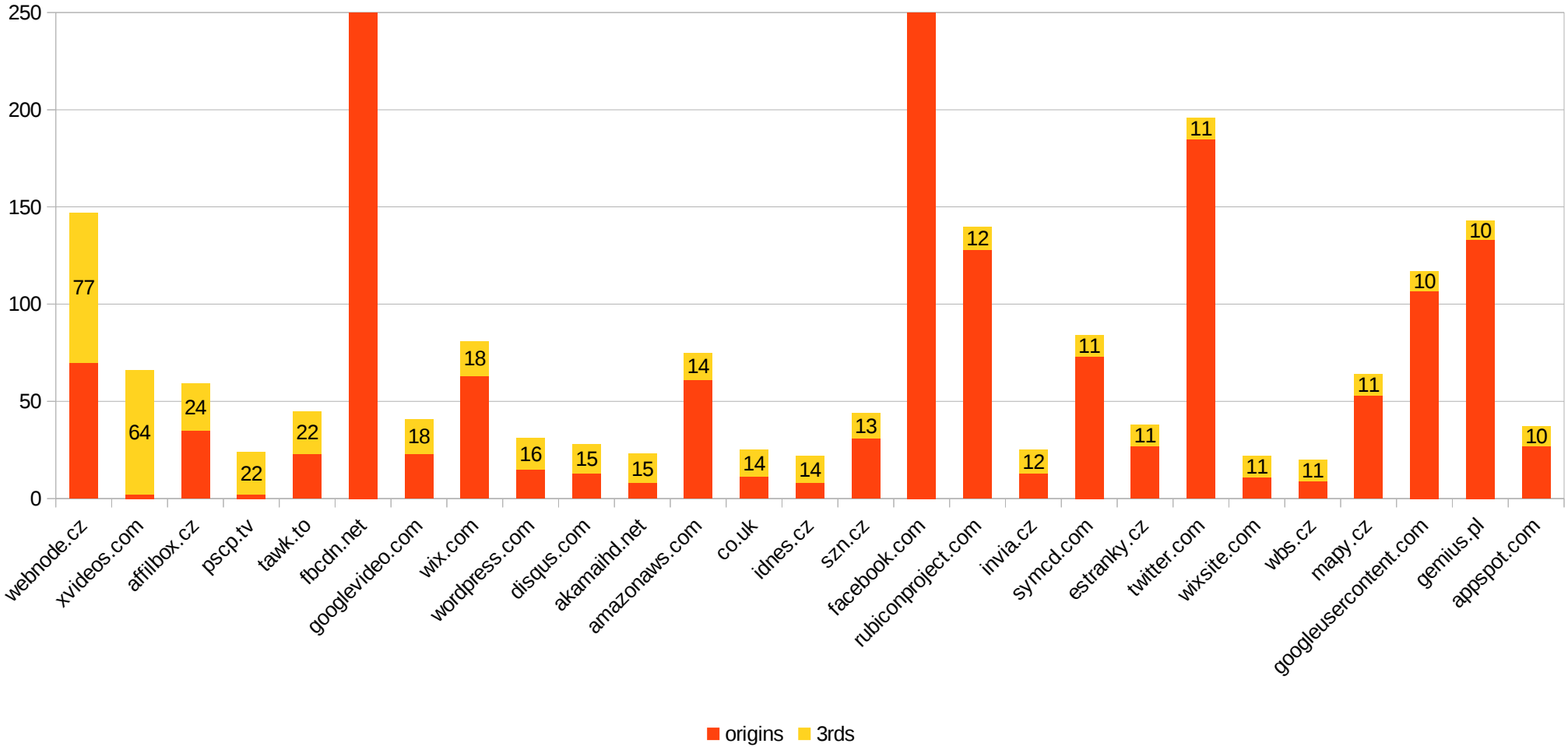
Group by TLD charts (percent)



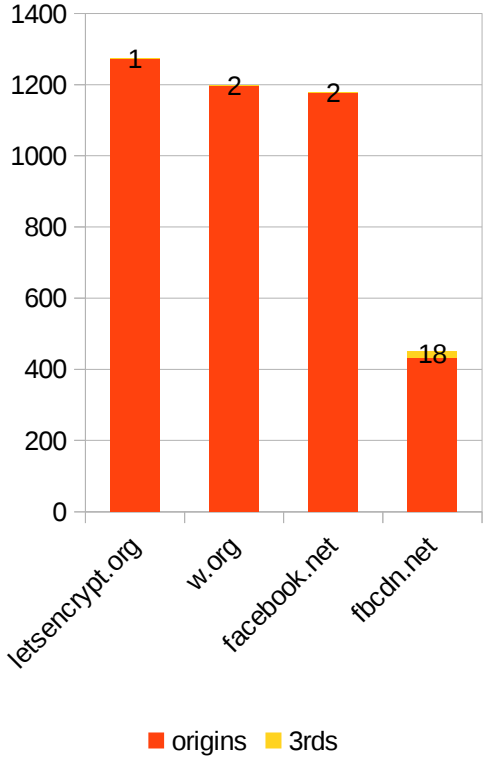
Group by 2nd LD (order by origins count)

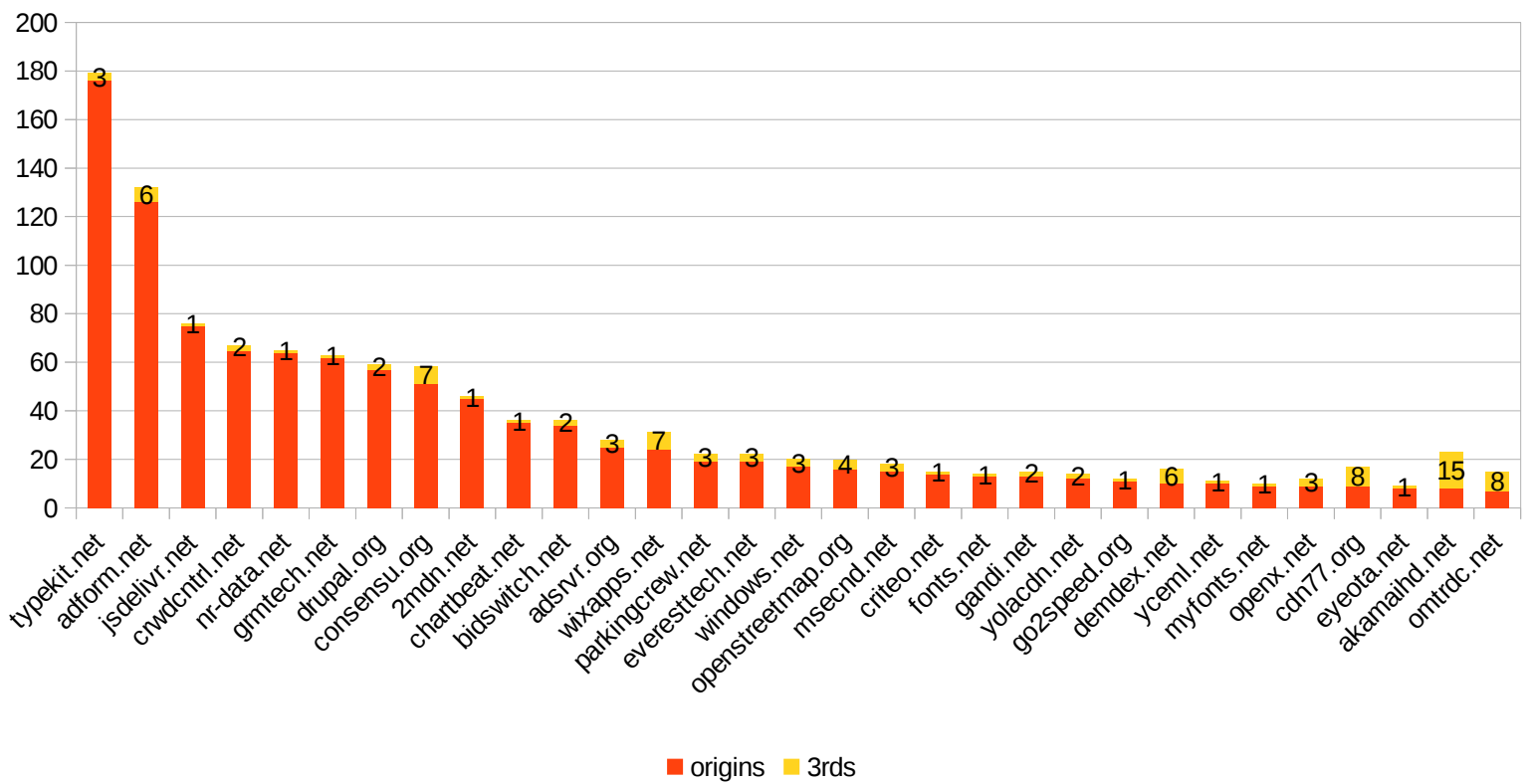


Group by 2nd LD (order by 3rd parties count)



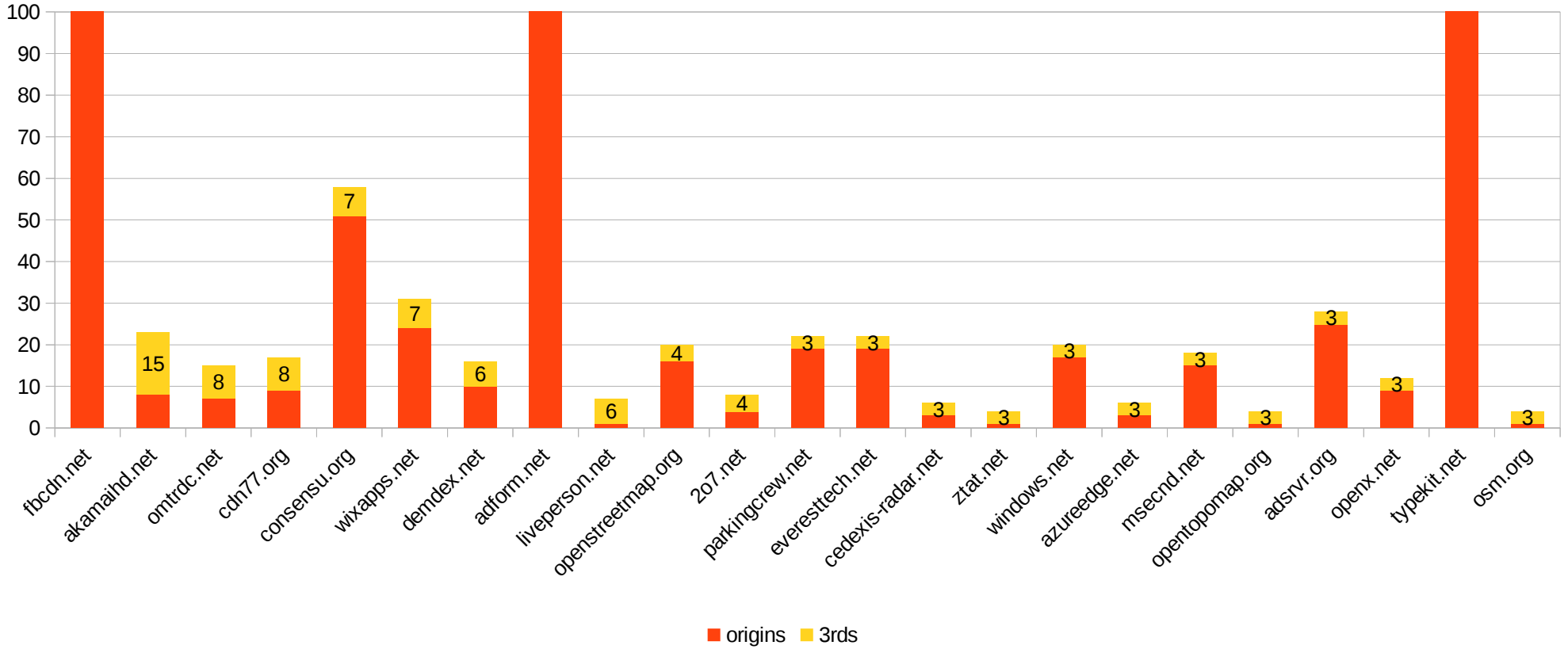
TLD .org, .net (order by origins count)



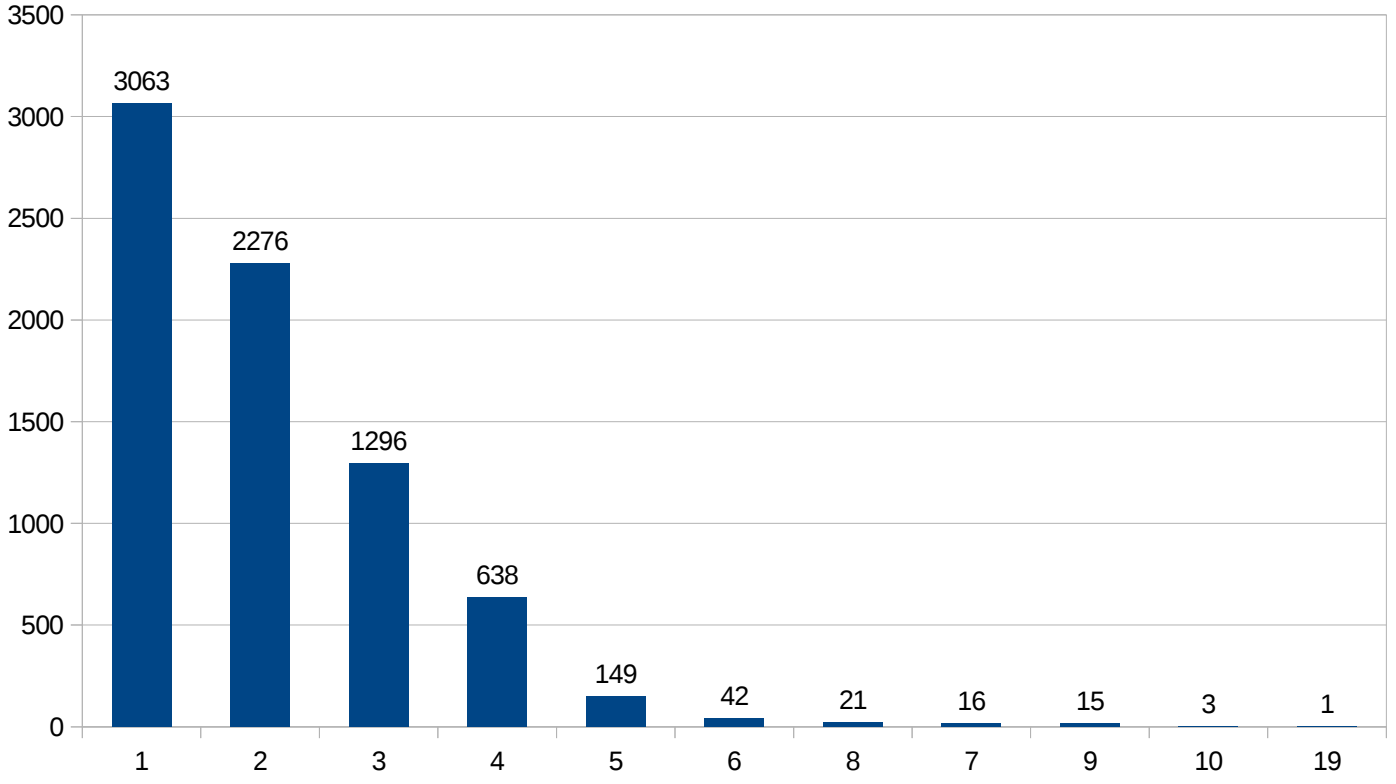


CZ.NIC | SPRÁVCE DOMÉNY CZ

TLD .org, .net (order by 3rd parties count)



TLDs count



CZ.NIC | SPRÁVCE DOMÉNY CZ

TLDs count

tlds_count	tlds
19	com,net,be,dk,uk,pl,cz,it,au,sk,de,ca,fr,in,hk,sg,nl,ie,my
10	net,com,co,org,fi,eu,de,cz,pl,io
10	io,com,eu,de,cz,net,co,st,org,pl
10	com,co,uk,nl,ro,net,de,cz,hu,it
9	net,org,com,eu,ai,de,cz,st,pl
9	net,com,eu,cz,de,co,st,org,pl
9	com,net,cz,sk,org,eu,ru,de,io
9	net,com,eu,de,cz,co,st,org,pl
9	com,co,net,eu,de,cz,it,org,pl
9	cz,com,tv,io,net,pl,us,me,org
9	com,co,org,net,eu,cz,de,st,pl
9	com,org,eu,cz,de,net,co,st,pl
9	com,net,eu,de,cz,co,st,org,pl

19× TLD champion

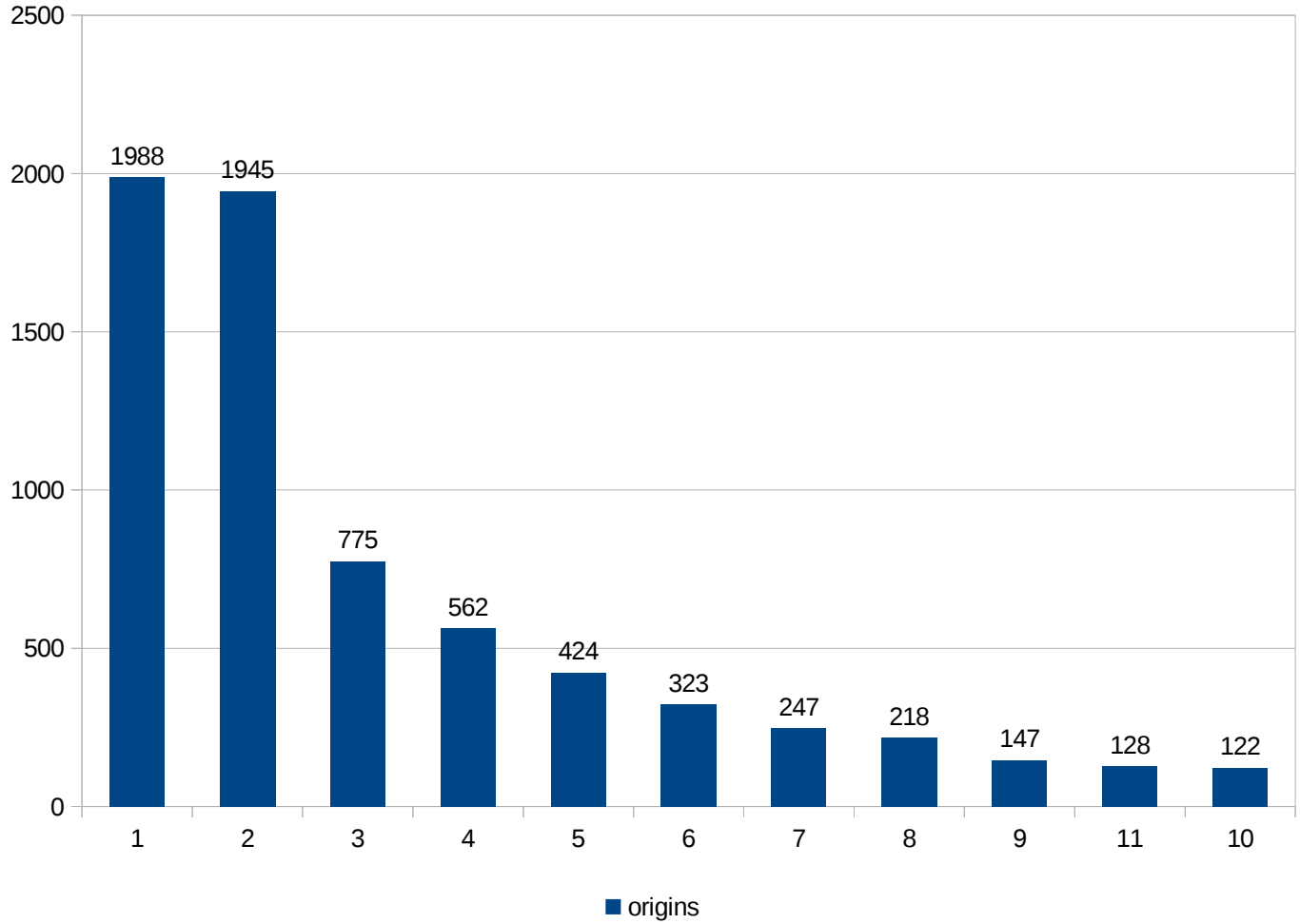
×	host	ip
10	hello.staticstuff.net	2400:cb00:2048:1::6810:7888
4	static-cdn.responsetap.com	13.32.99.132
4	cdn.siteimprove.net	143.204.101.11
4	s.trustpilot.com	143.204.101.7
4	siteimproveanalytics.com	2606:4700:20::6819:8976
4	static-ssl.responsetap.com	13.32.99.240
4	insights.hotjar.com	13.32.99.26
3	ocsp.affirmtrust.com	2a02:26f0:dc:2ac::1b01
3	try.abtasty.com	2a02:26f0:40:29f::1eae
3	win.staticstuff.net	198.145.13.11
2	accdn.lpsnmedia.net	2a03:6400:16:0:178:249:101:99
2	dcinfos.abtasty.com	52.215.65.63

VCE
ÉNY CZ

2	www.google.co.uk	2a00:1450:400e:806::2003
2	www.google.com.my	2a00:1450:400e:806::2003
2	www.google.fr	2a00:1450:400e:806::2003
2	ssl.comodo.com	2a02:1788:4fd:cd::c742:cdf2
2	www.google.de	2a00:1450:400e:806::2003
2	www.google.nl	2a00:1450:400e:806::2003
2	www.google.com.hk	2a00:1450:400e:806::2003
2	www.google.ca	2a00:1450:400e:806::2003
2	lpcdn.lpsnmedia.net	2a03:6400:10:0:178:249:97:98
2	www.google.sk	2a00:1450:400e:806::2003
2	www.google.com.sg	2a00:1450:400e:806::2003
2	www.google.dk	2a00:1450:400e:806::2003
2	www.google.co.in	2a00:1450:400e:806::2003
2	eu2.siteimprove.com	52.58.236.177
2	static.hotjar.com	147.75.205.155
2	www.google.pl	2a00:1450:400e:806::2003
2	www.google.ie	2a00:1450:400e:806::2003

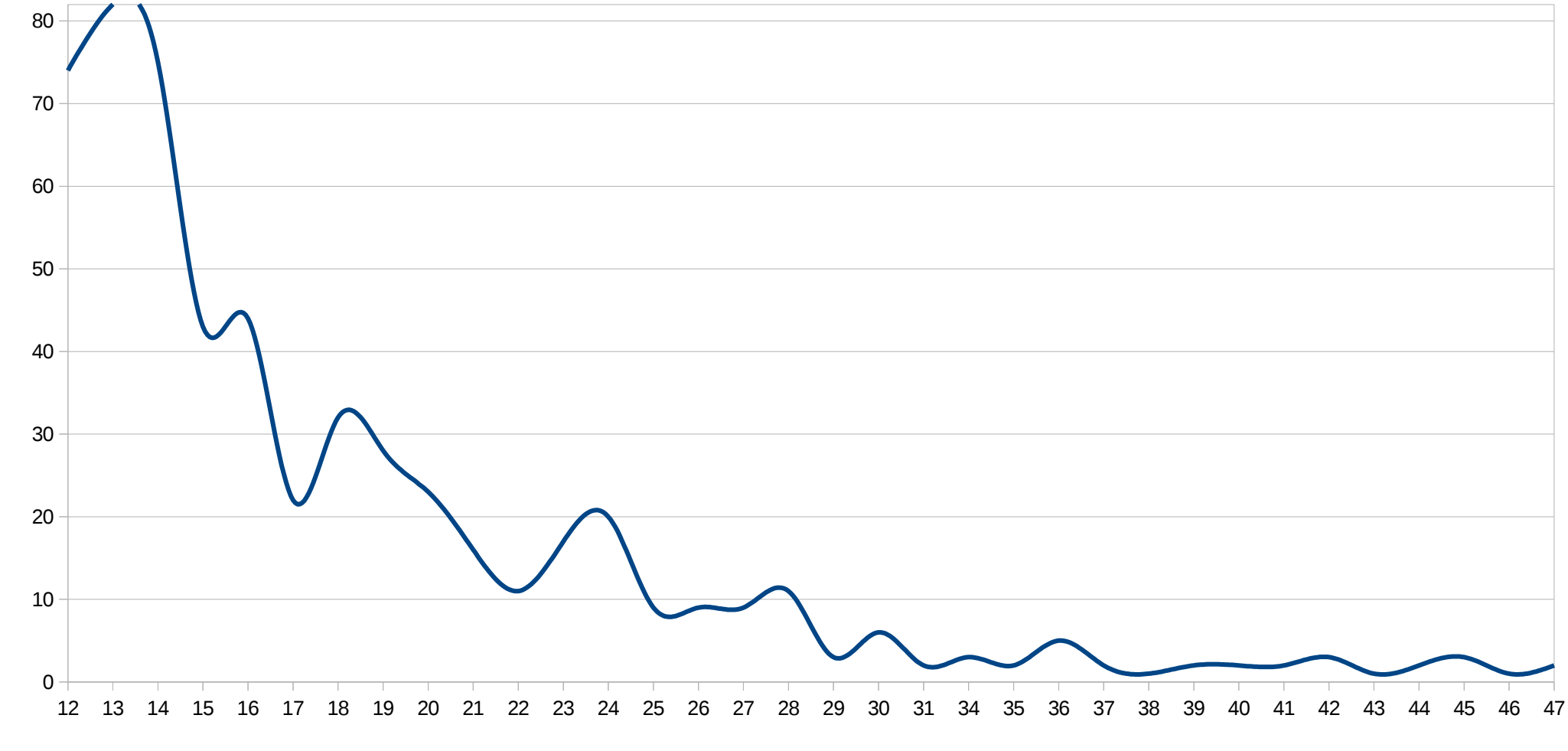
u.heatmap.it
m.addthisedge.com
report-uri.cloudflare.com
www.facebook.com
widget.trustpilot.com
app2.salesmanago.pl
lptag.liveperson.net
connect.facebook.net
vxml4.delacon.com.au
www.youtube.com
bfs.bibbyfs.net
m.addthis.com
dev.visualwebsiteoptimizer.com
lo.v.liveperson.net
tags.liveperson.net
ict.infinity-tracking.net
app.everyonesocial.com
youtube.com
vars.hotjar.com
use.typekit.net
services.postcodeanywhere.co.uk
script.hotjar.com
s7.addthis.com
fb.scanandcleanlocal.com
t.leady.com
my2.siteimprove.com
chatcon5.liveperson.net
track.leady.cz
cdnjs.cloudflare.com
script.crazyegg.com
go.pardot.com
www.dynamicnumbers.mediahawk.co.uk
40691190.lo.cobrowse.liveperson.net
graylog.hotjar.com
gtrk.s3.amazonaws.com
pixel.powerlinks.com
cdn.mouseflow.com
eu3.heatmap.it
cdn.daddyanalytics.com
status.thawte.com
youtu.be
pi.pardot.com
t.leady.cz
i.ctnsnet.com
www.googletagmanager.com
id.siteimprove.com

3rd parties count *(1988 origins ~ 1× 3rd party)*

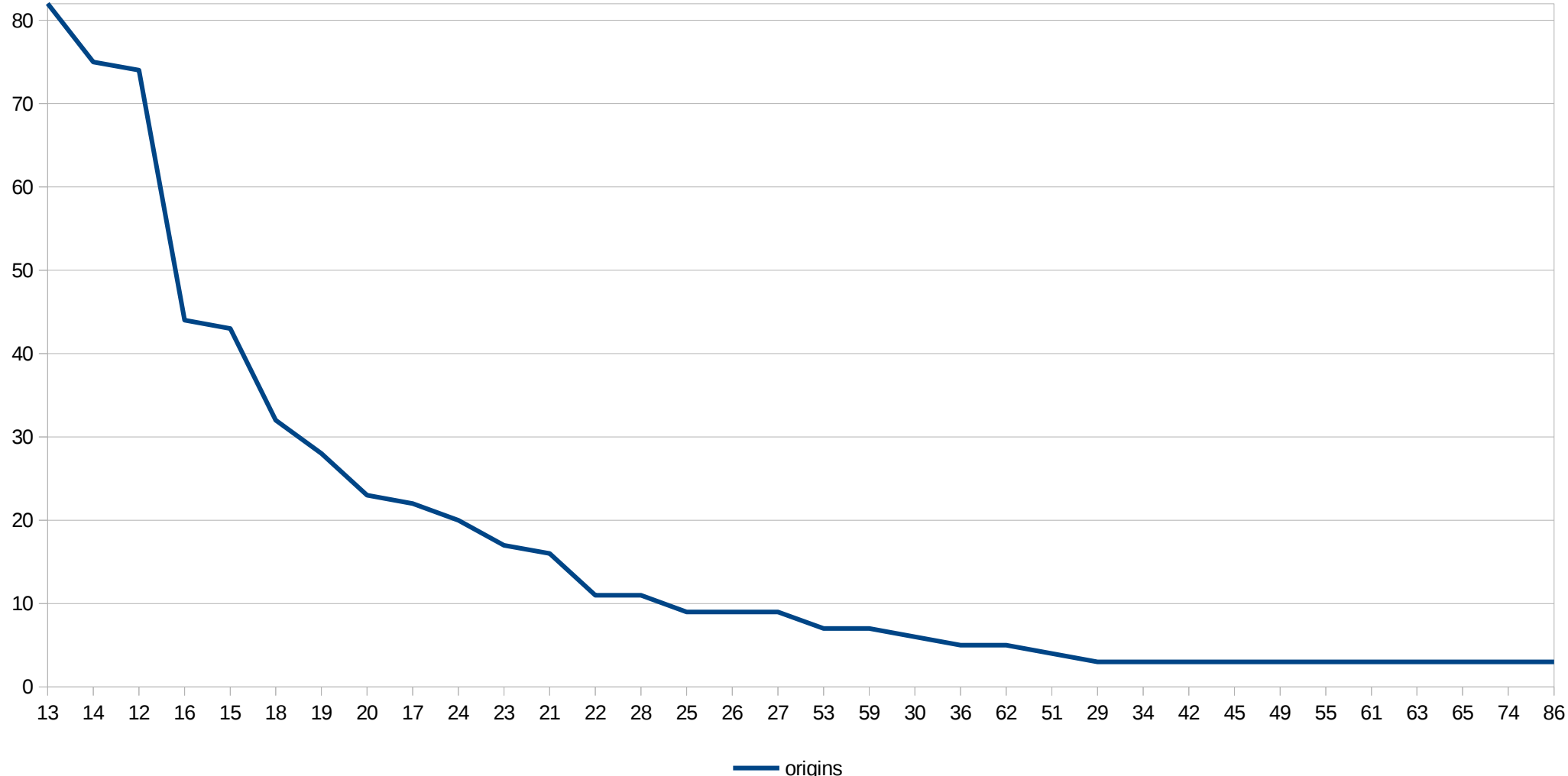


87	1
86	3
85	2
84	1
81	1
78	2
74	3
73	1
72	1
71	2
70	1
69	2
68	2
67	1
66	1
65	3

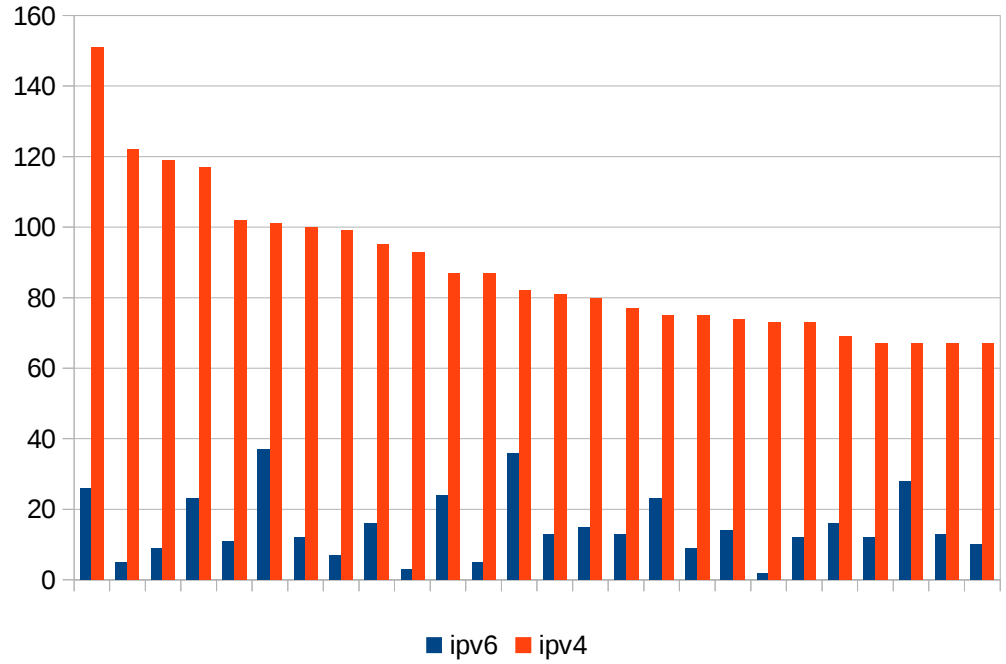
3rd parties count *(82 origins ~ 13× 3rd party)*

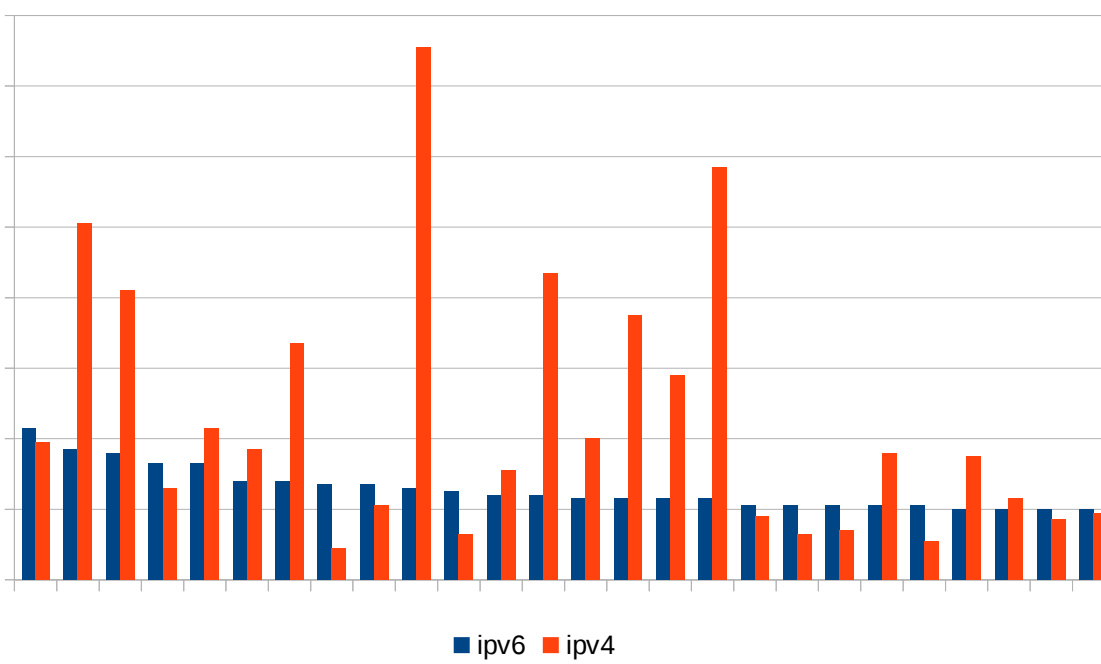


3rd parties count *(82 origins ~ 13× 3rd party)*

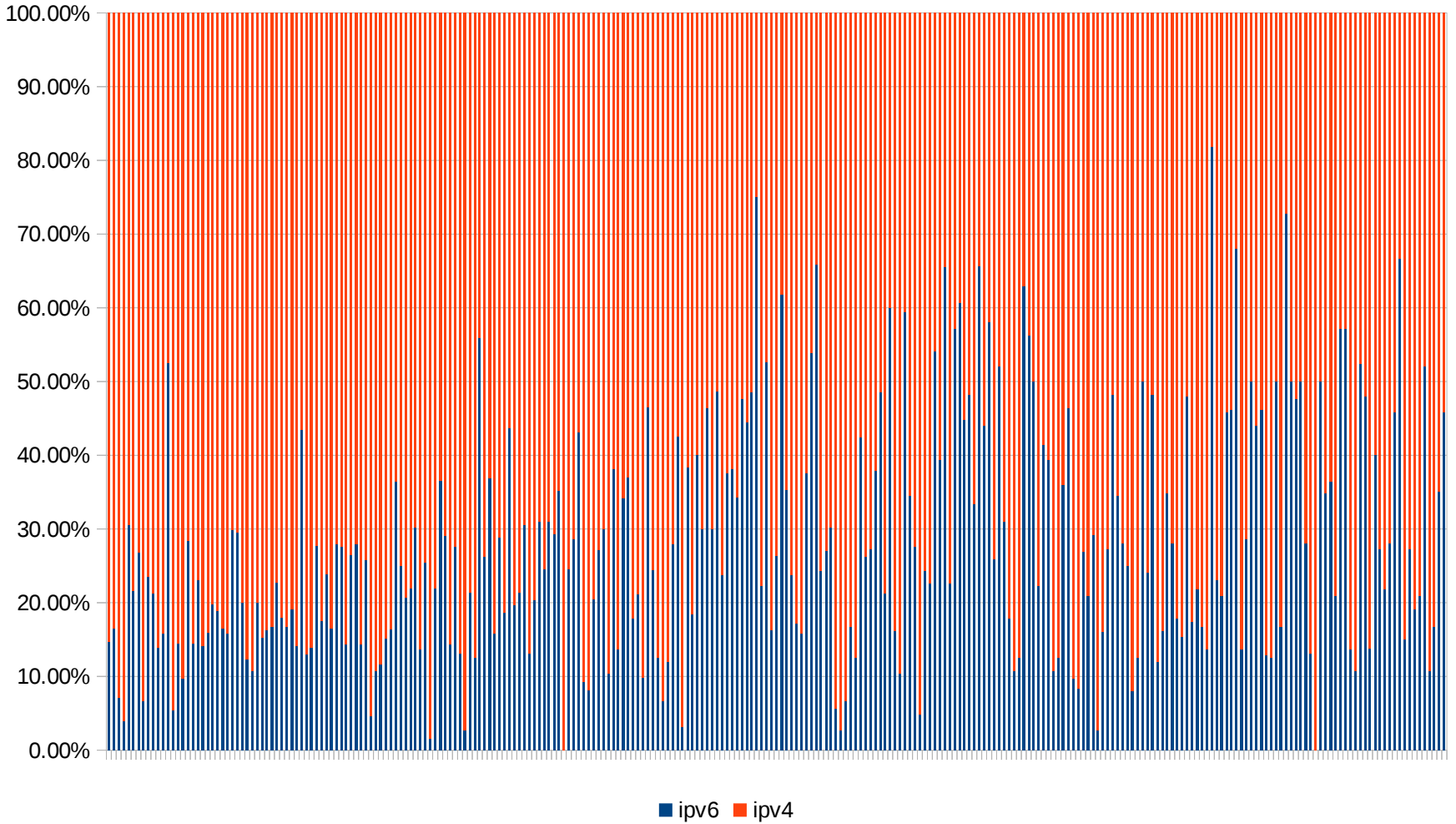


Sort by IPv4 / by IPv6





IPv4 vs IPv6


100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
ipv6
ipv4

Spy module

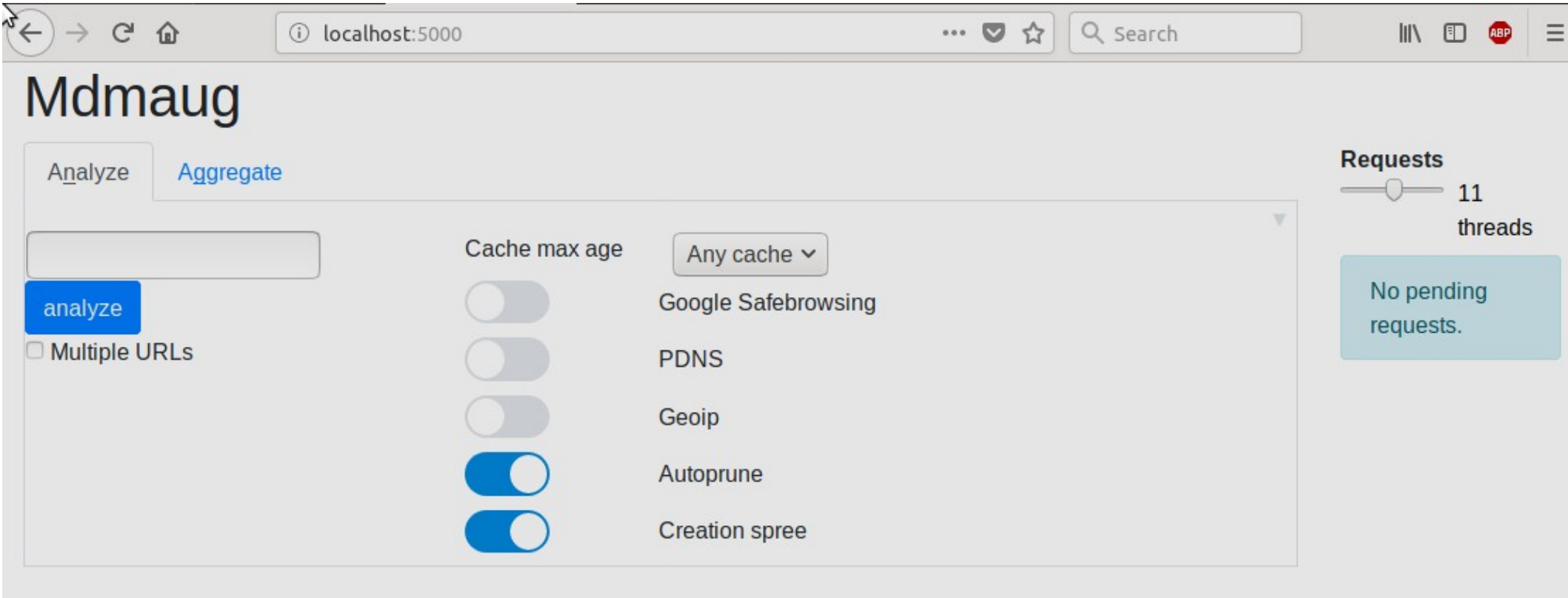
```
var unescape = mdmaugWrapper(unescape);
var mdmaugWrapper = function (fn) {
    var swap = fn;
    return function () {
        mdmaugSquawk(swap.name, arguments);
        return swap.apply(null, arguments);
    };
};
```

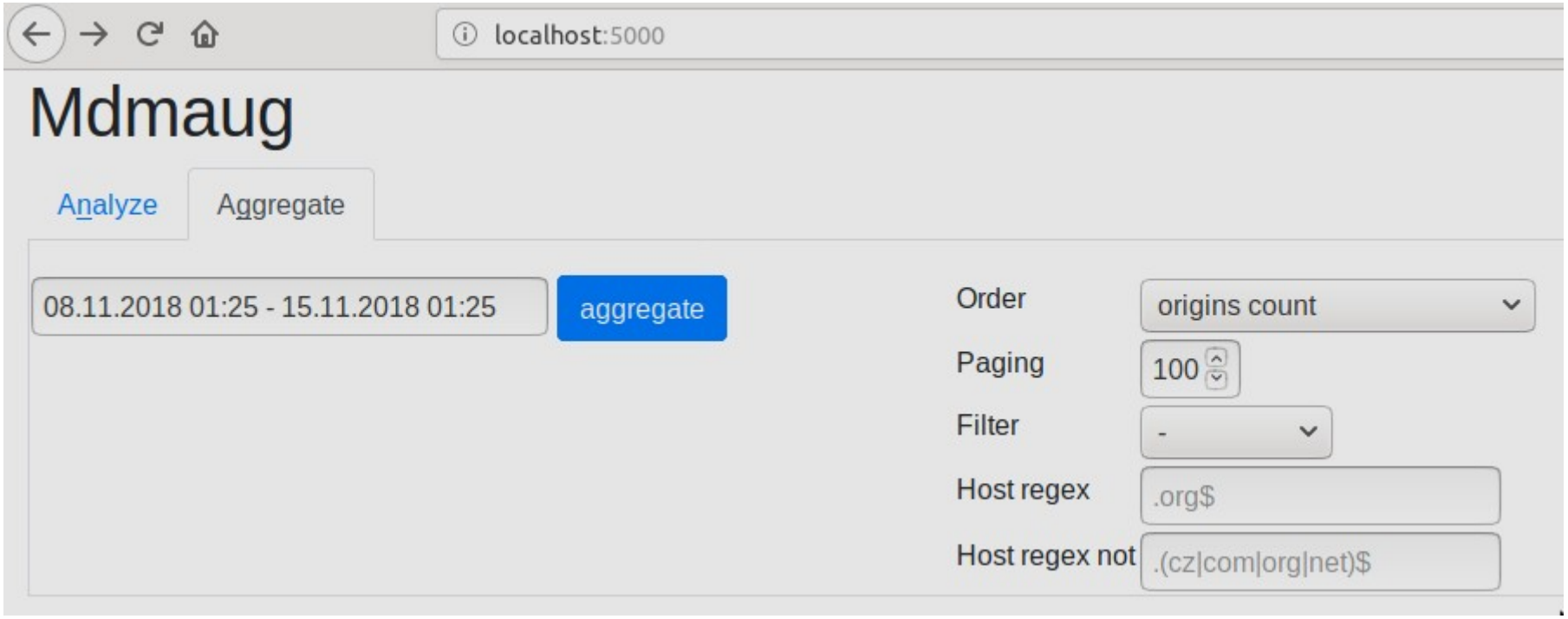
```
document.write = function (str) {
    mdmaugSquawk("document.write", str);
    document.getElementsByTagName("html")[0].innerHTML = str;
};
```

```
var evalClone = window.wrappedJSObject.eval;
var eval = function (cmd) {
    mdmaugSquawk("eval", cmd);
    if (arguments.length > 0) {
        if (arguments[0].indexOf("arguments.callee") != -1) {
            arguments[0] = arguments[0].replace("arguments.callee", arguments.callee.caller.name);
        }
    }
    return evalClone(cmd);
};
```

```
exportFunction(unescape, window.wrappedJSObject, {defineAs: "unescape"});
exportFunction(eval, window.wrappedJSObject, {defineAs: "eval"});
exportFunction(evalClone, window.wrappedJSObject, {defineAs: "evalClone"});
exportFunction(document.write, window.wrappedJSObject, {defineAs: "document.write"});
```

Interface


localhost:5000
Search
Mdmaug
Analyze
Aggregate
analyze
Multiple URLs
Cache max age
Any cache
Google Safebrowsing
PDNS
Geoip
Autoprune
Creation spree
Requests
11
threads
No pending
requests.



CZ.NIC | SPRÁVCE DOMÉNY CZ

Demopage


```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Demo page</title>
</head>
<body>

This page has a lot of suspicious code. It serves as demo for MDMaug scanner.

<iframe src="another-page"></iframe>
<object>strange object</object>
<img src='strange-dir/image-link' onclick='suspicious-js-function' />

<img src="http://example.cz/test">


<script>
    eval("This internal script uses eval.");
    window.location.href +2;
</script>
<script src="demoscript.js"></script>

</body>
</html>
```

cz.nic | SPRÁVCE DOMÉNY CZ

Demopage

http://127.0.0.1:5000/static/demopage.html

05.10.2018 03:26 05.10.2018 03:38

n/a **127.0.0.1**

- :5000/static/demopage.html
- :5000/static/
- :5000
- :5000/static/strange-dir/image-link
- :5000/static/demoscript.js
- :5000/static/another-page
- :5000/favicon.ico
- /static/another-page →
- /static/demopage.html →
- /static/demoscript.js →
- /static/demopage.html spy

eval "This internal script uses eval." ,

eval "This external script has a suspicious eval call"

n/a **example.cz**

93.185.104.64

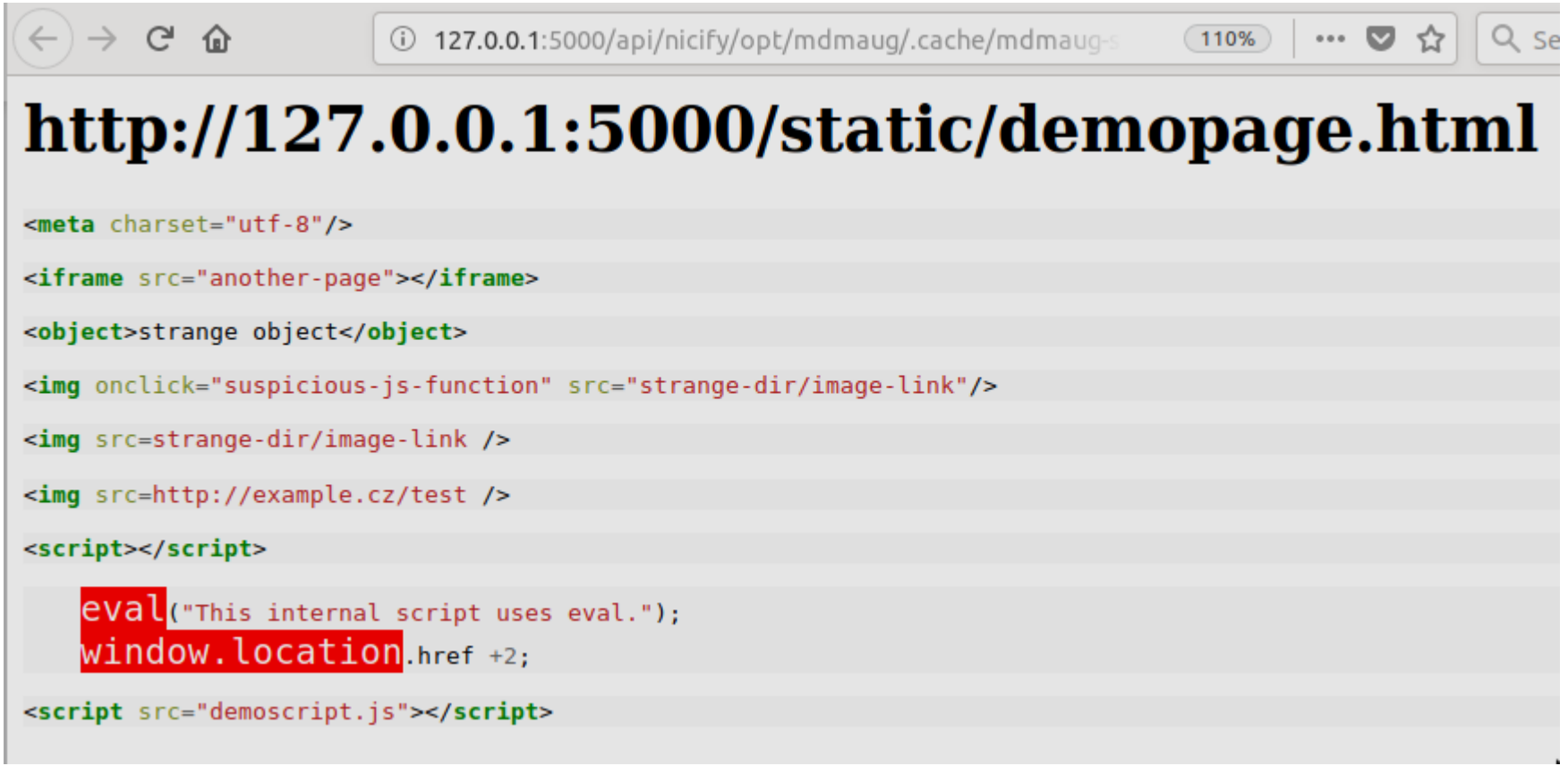
- /test

n/a **pipni.cz**

93.185.104.4 example.cz

- /404

Demopage


127.0.0.1:5000/api/nicify/opt/mdmaug/.cache/mdmaug-s
110%
http://127.0.0.1:5000/static/demopage.html
<meta charset="utf-8"/>
<iframe src="another-page"></iframe>
<object>strange object</object>

<script></script>
eval("This internal script uses eval.");
window.location.href +2;
<script src="demoscript.js"></script>

Installation

```
## Installation

1. Download ```git clone git@gitlab.labs.nic.cz:csirt/mdmaug.git /tmp/mdmaug```
2. Edit mdmaug/lib/config.py
3. You should generate a certificate to `mdmaug/cert-mdmaug.pem`, at least a self-signed one (non
recommended): `openssl req -x509 -newkey rsa:4096 -nodes -out cert-mdmaug.pem -keyout key-mdmaug.pem`
4. Perform installation: ```/tmp/mdmaug/INSTALL```
5. Everything should be located in `/opt/mdmaug`.
6. For testing purposes, launch it under newly created `mdmaug` user:
                                                    `su - mdmaug -c 'python3 -m mdmaug'`
7. Connect in the browser at: https://127.0.0.1:5000
8. Try analysing `https://127.0.0.1:5000/static/demopage.html` on local server
9. For deployment, configure nginx properly to be used with flask
```

Děkuji za pozornost

Edvard Rejthar • edvard.rejthar@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ