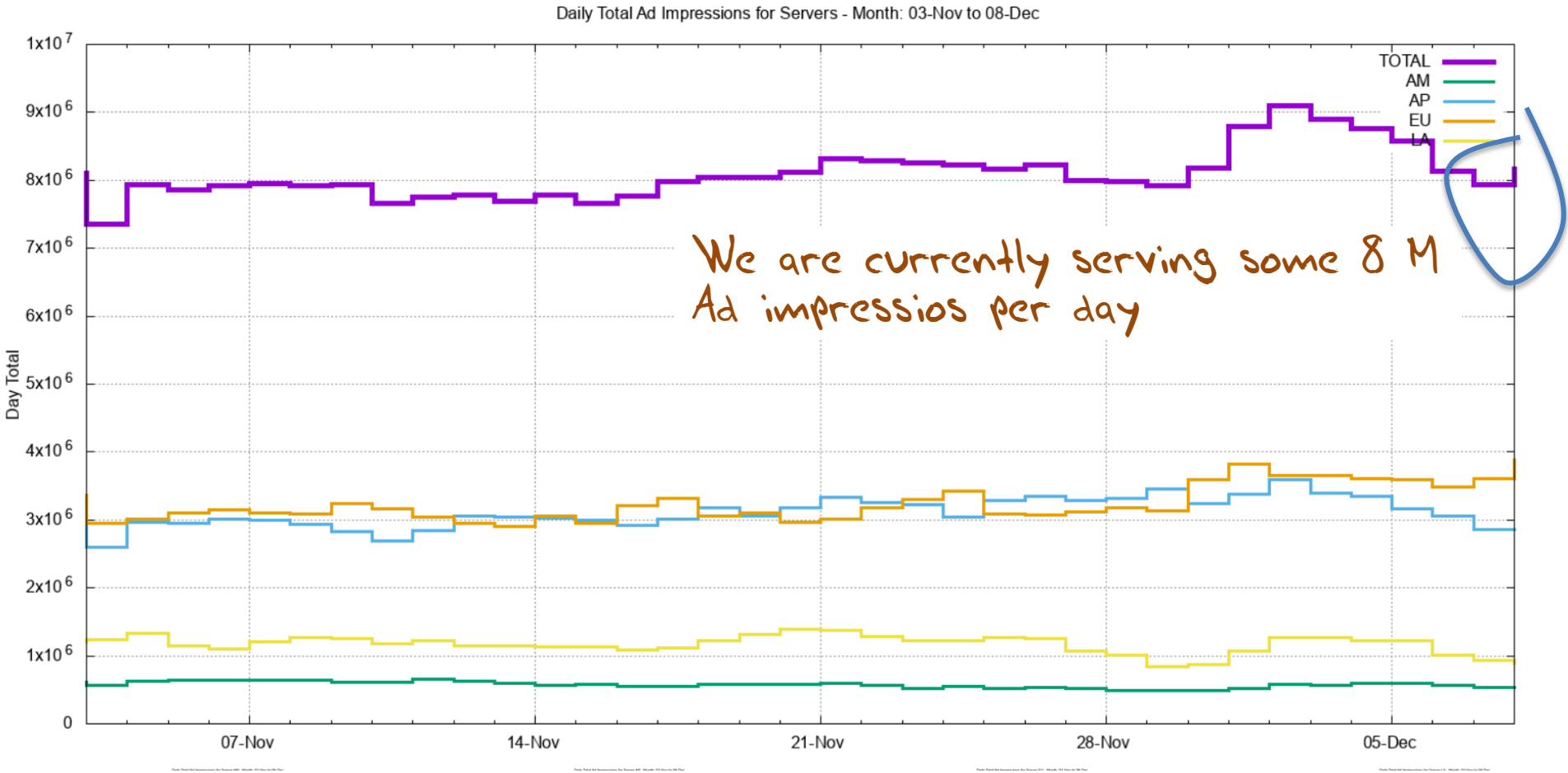
# Abuse of the DNS

# What we do:

Run an online advertisement with an embedded measurement script

- The script caused the browser to fetch a number of 1x1 ‘blots’
- To ensure that we had a clear view of the actions of the user and the DNS resolvers they use, we used unique URL labels.

# Ad Impressions per Day



# URL Load

- We are generating some 24 million DNS queries for “unique” DNS names per day
- And similarly performing some 24 million HTTP blot fetches for “unique” URLs per day

# "Unique"?

What is meant by "**unique**"?

- The DNS name is queried by a single endpoint once and only once(*) – never again!

  (And the name includes a subfield of the time it was created)

- Which means that we should see one query for the name at the authoritative name server

* Well not quite, 25% of the time its queried twice, and sometimes more, but its all triggered by a single resolution action initiated by the endpoint – all these queries are clustered together in time

# What do we see?

```
1575763200.052782 client 2001:558:fe00:c:69:252:228:155#28173: query: 0di-ua3a8f5b9-c233-s1575763198-i00000000-0.am.dotnxdomain.net
1575763200.107703 client 2001:1890:1ff:9c5:12:121:117:117#59964: query: 0du-results-uffc468d4-c233-s1575763190-i6cf3ec1f-0.am.dotnx
1575763200.116616 client 2600:387:2:807::f#2425: query: 0du-results-ufa9c53fd-c233-s1575763189-i6b4de8b7-0.am.dotnxdomain.net. IN A
1575763200.170904 client 76.96.24.3#38686: query: 0ds-u7dc476e7-c233-s1575763199-i00000000-0.am.dotnxdomain.net. IN A -ED () 0 327
1575763200.237990 client 76.96.24.7#37373: query: 0di-u7dc476e7-c233-s1575763199-i00000000-0.am.dotnxdomain.net. IN AAAA -ED () 0 3
1575763200.256426 client 144.160.112.7#31949: query: 06u-udd090ee9-c233-s1552588424-i6b4dd023-0.am.dotnxdomain.net. IN A -ED () 0 1
1575763200.286878 client 144.160.112.7#39678: query: 06u-udd090ee9-c233-s1552588424-i6b4dd023-0.am.dotnxdomain.net. IN AAAA -ED ()
1575763200.324318 client 107.77.253.241#36892: query: 0du-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN A -ED () 0
1575763200.324671 client 107.77.253.240#37953: query: 0du-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN AAAA -ED ()
1575763200.329448 client 2600:387:6:983::16#5656: query: 04u-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN A -ED ()
1575763200.329884 client 107.77.253.241#1154: query: 04u-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN AAAA -ED ()
```

Name ‘creation’ time

Query time

# What do we see?

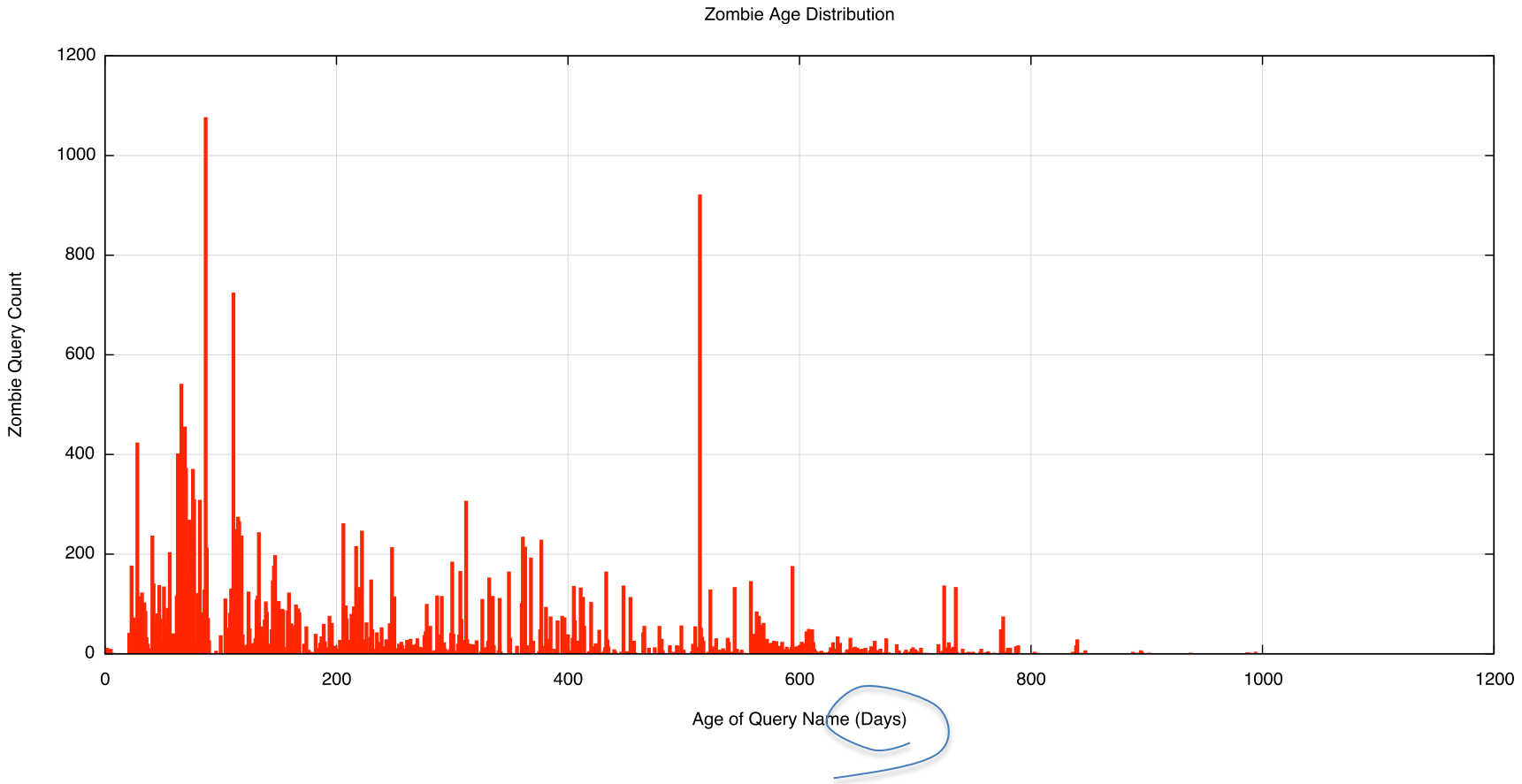
```
1575763200.052782 client 2001:558:fe00:c:69:252:228:155#28173: query: 0di-ua3a8f5b9-c233-s1575763198-i00000000-0.am.dotnxdomain.net
1575763200.107703 client 2001:1890:1ff:9c5:12:121:117:117#59964: query: 0du-results-uffc468d4-c233-s1575763190-i6cf3ec1f-0.am.dotnx
1575763200.116616 client 2600:387:2:807::f#2425: query: 0du-results-ufa9c53fd-c233-s1575763189-i6b4de8b7-0.am.dotnxdomain.net. IN A
1575763200.170904 client 76.96.24.3#38686: query: 0ds-u7dc476e7-c233-s1575763199-i00000000-0.am.dotnxdomain.net. IN A -ED () 0 327
1575763200.237990 client 76.96.24.7#37373: query: 0di-u7dc476e7-c233-s1575763199-i00000000-0.am.dotnxdomain.net. IN AAAA -ED () 0 3
1575763200.256426 client 144.160.112.7#31949: query: 06u-udd090ee9-c233-s1552588424-i6b4dd023-0.am.dotnxdomain.net. IN A -ED () 0 1
1575763200.286878 client 144.160.112.7#39678: query: 06u-udd090ee9-c233-s1552588424-i6b4dd023-0.am.dotnxdomain.net. IN AAAA -ED ()
1575763200.324318 client 107.77.253.241#36892: query: 0du-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN A -ED () 0
1575763200.324671 client 107.77.253.240#37953: query: 0du-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN AAAA -ED ()
1575763200.329448 client 2600:387:6:983::16#5656: query: 04u-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN A -ED ()
1575763200.329884 client 107.77.253.241#1154: query: 04u-uacb2983c-c233-s1575763200-i6b4dfd37-0.am.dotnxdomain.net. IN AAAA -ED ()
```

Old queries

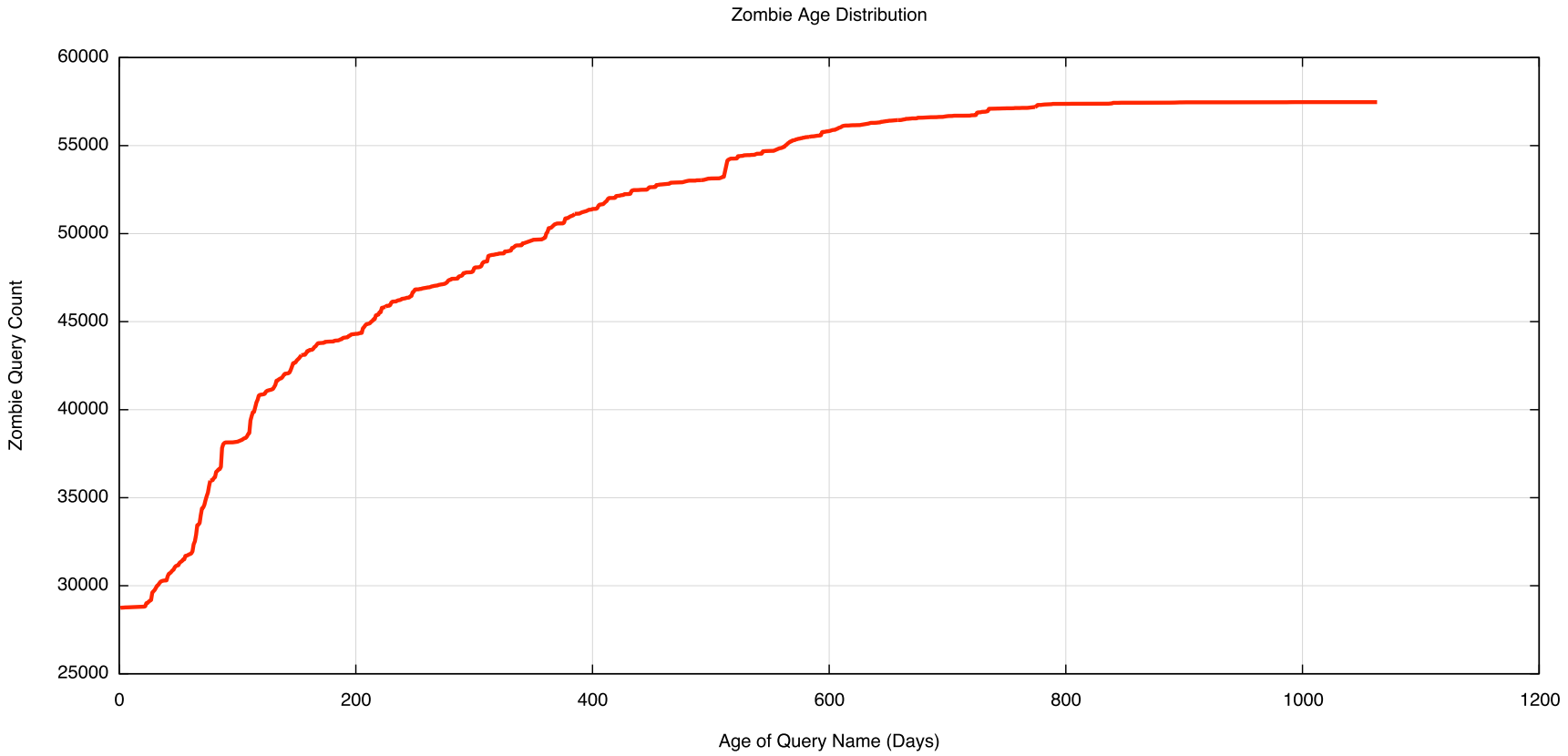
Name ‘creation’ time

Query time

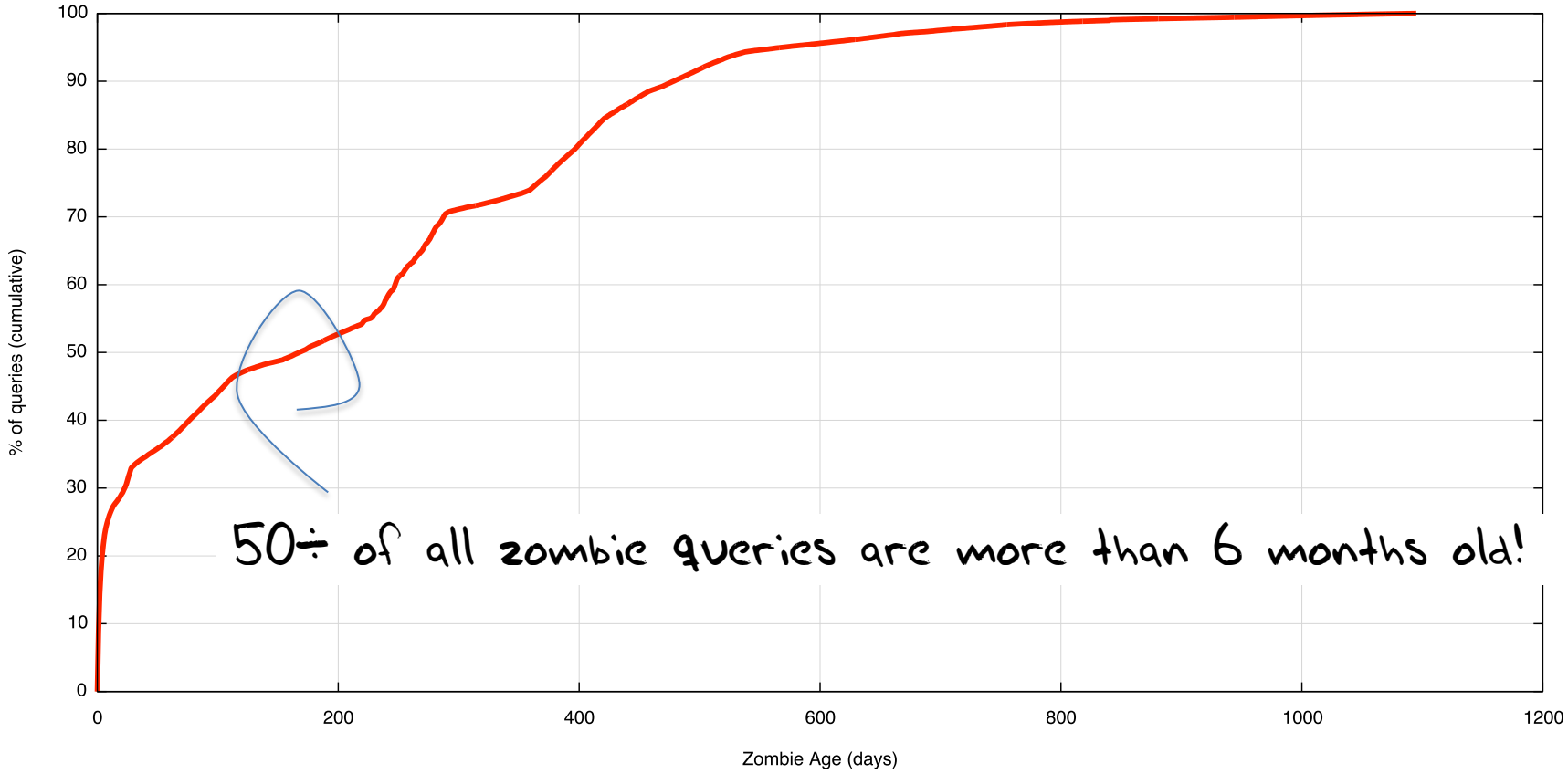
# One Day, One DNS Server



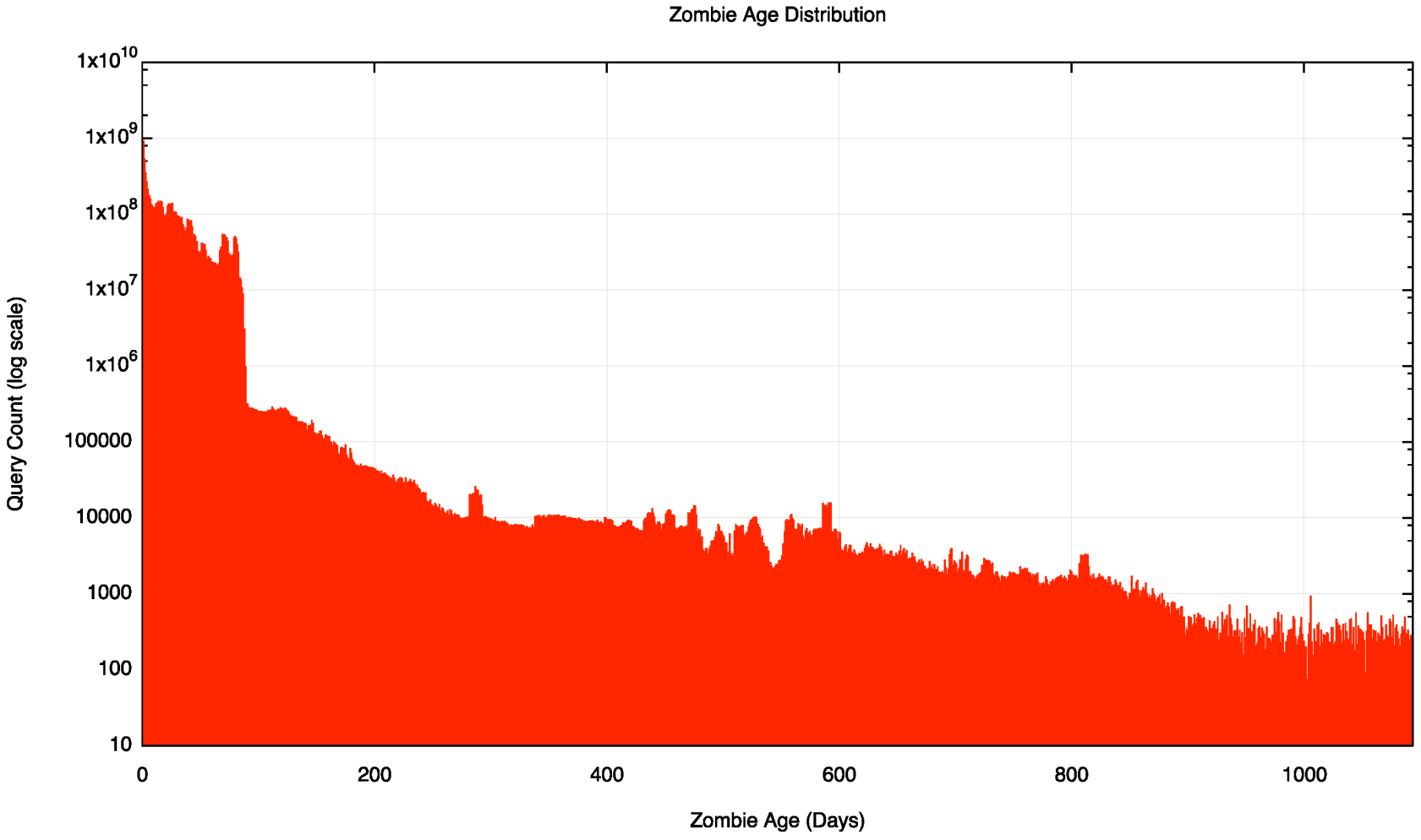
# One Day, One DNS Server



# 60 Days, All DNS Servers



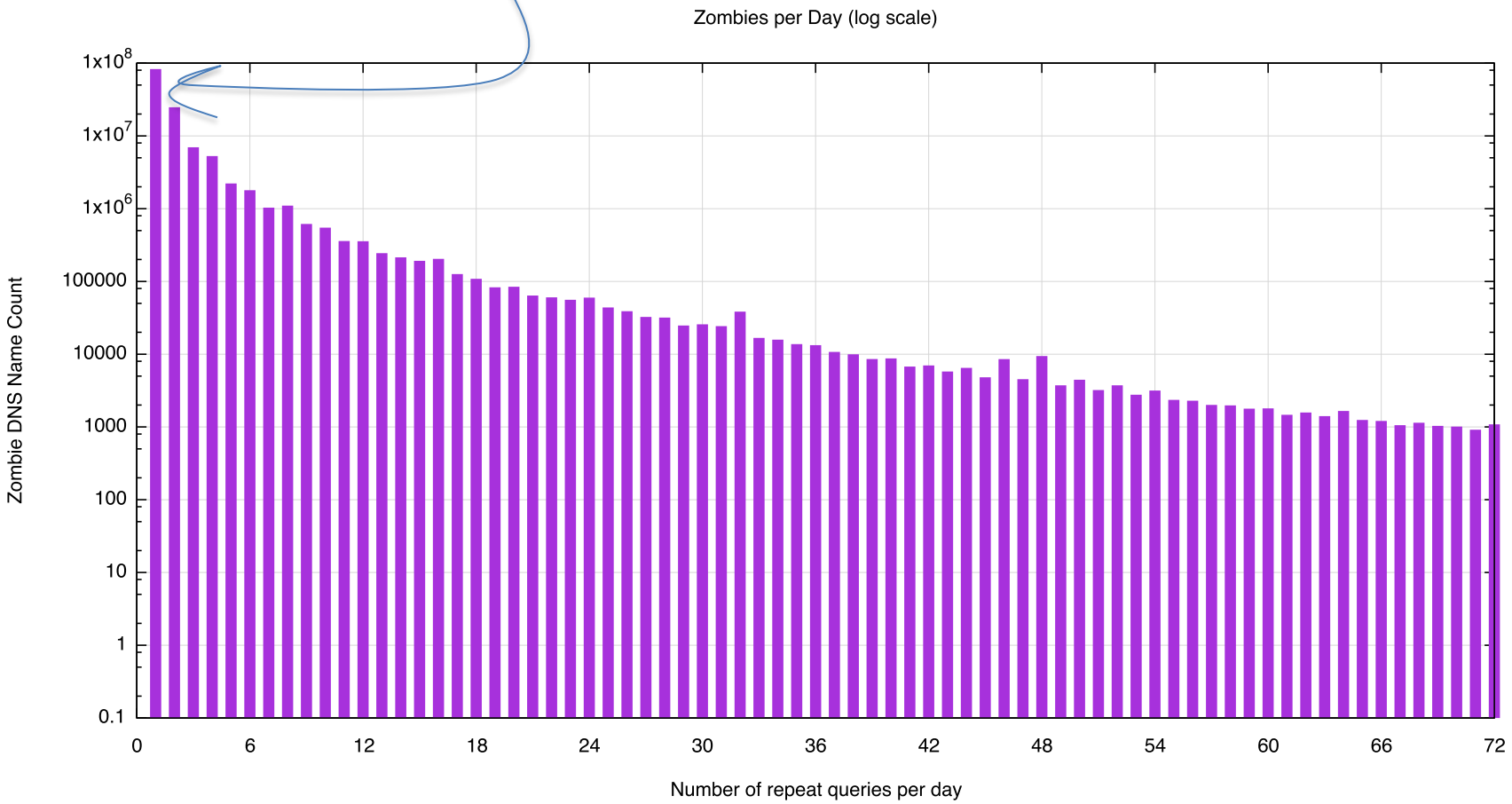
# 180 Days, All DNS Servers



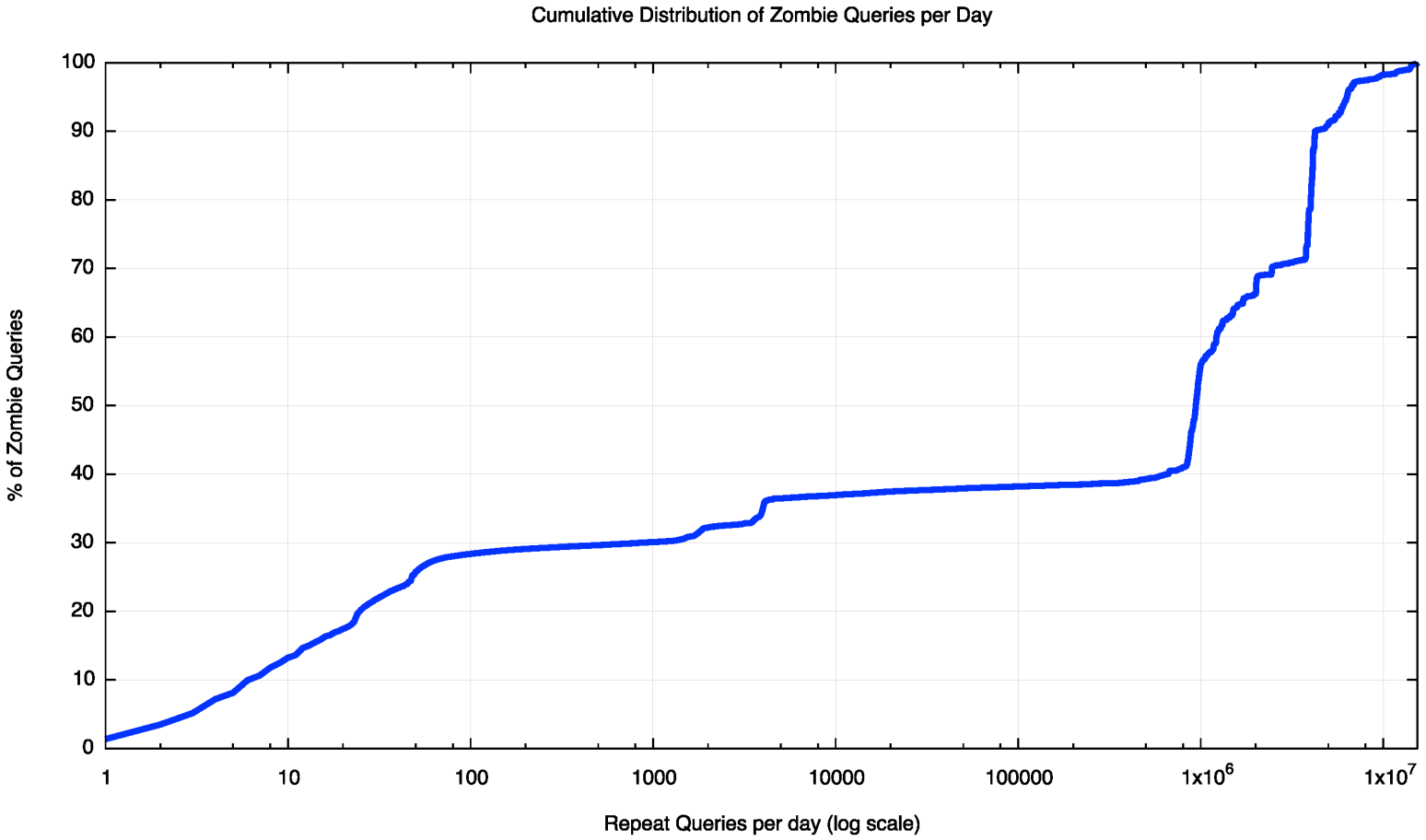

44,733,946,408 DNS queries, of which 11,274,142,797 are zombies – a 25% zombie rating!

# Zombie Queries per day

2/3 of all queries occur once per day



# Zombie Repeats per day



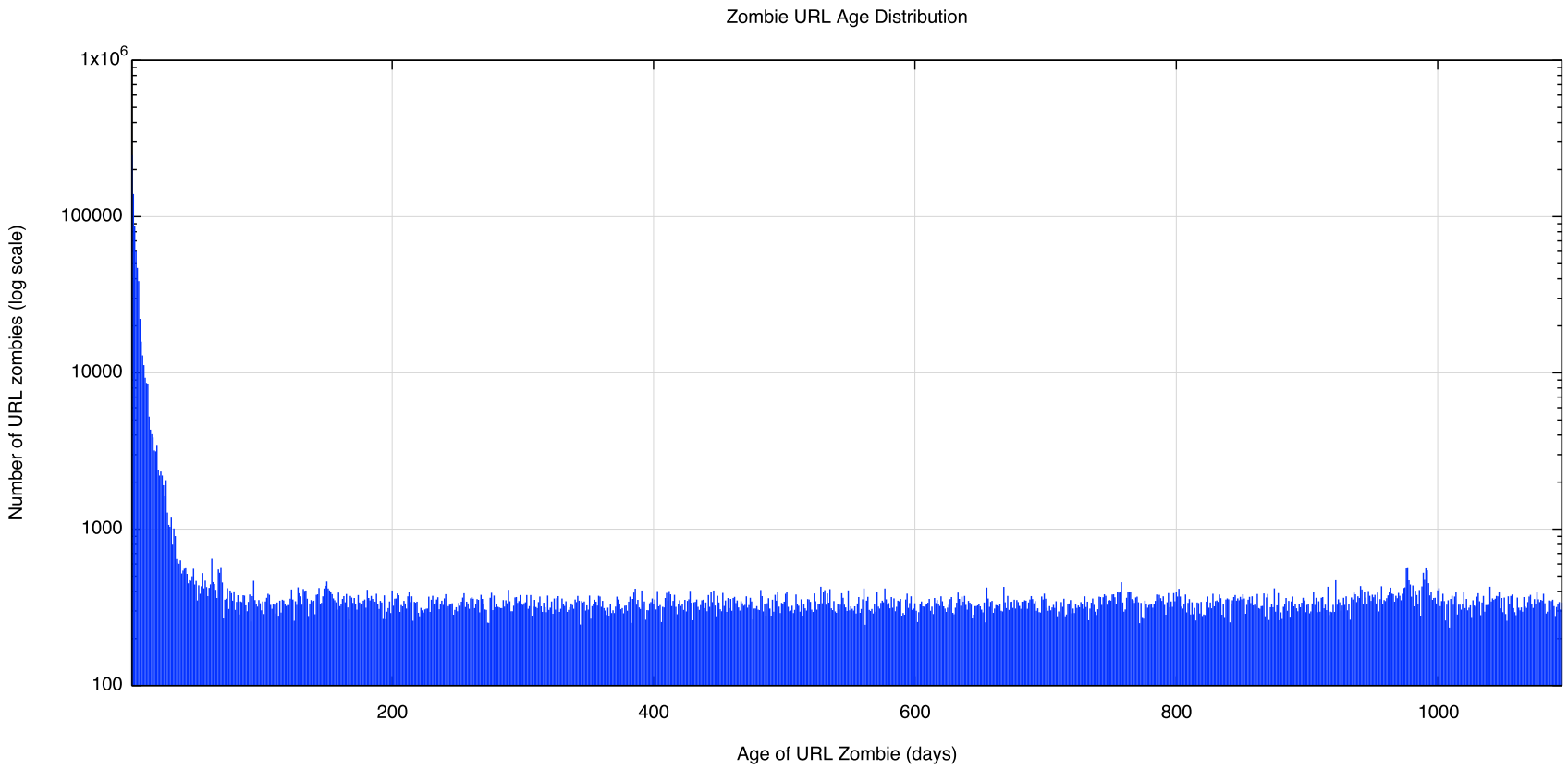
# What is causing this?

Is this the result of a collection of deranged DNS recursive resolvers with an obsession about never forgetting a thing?

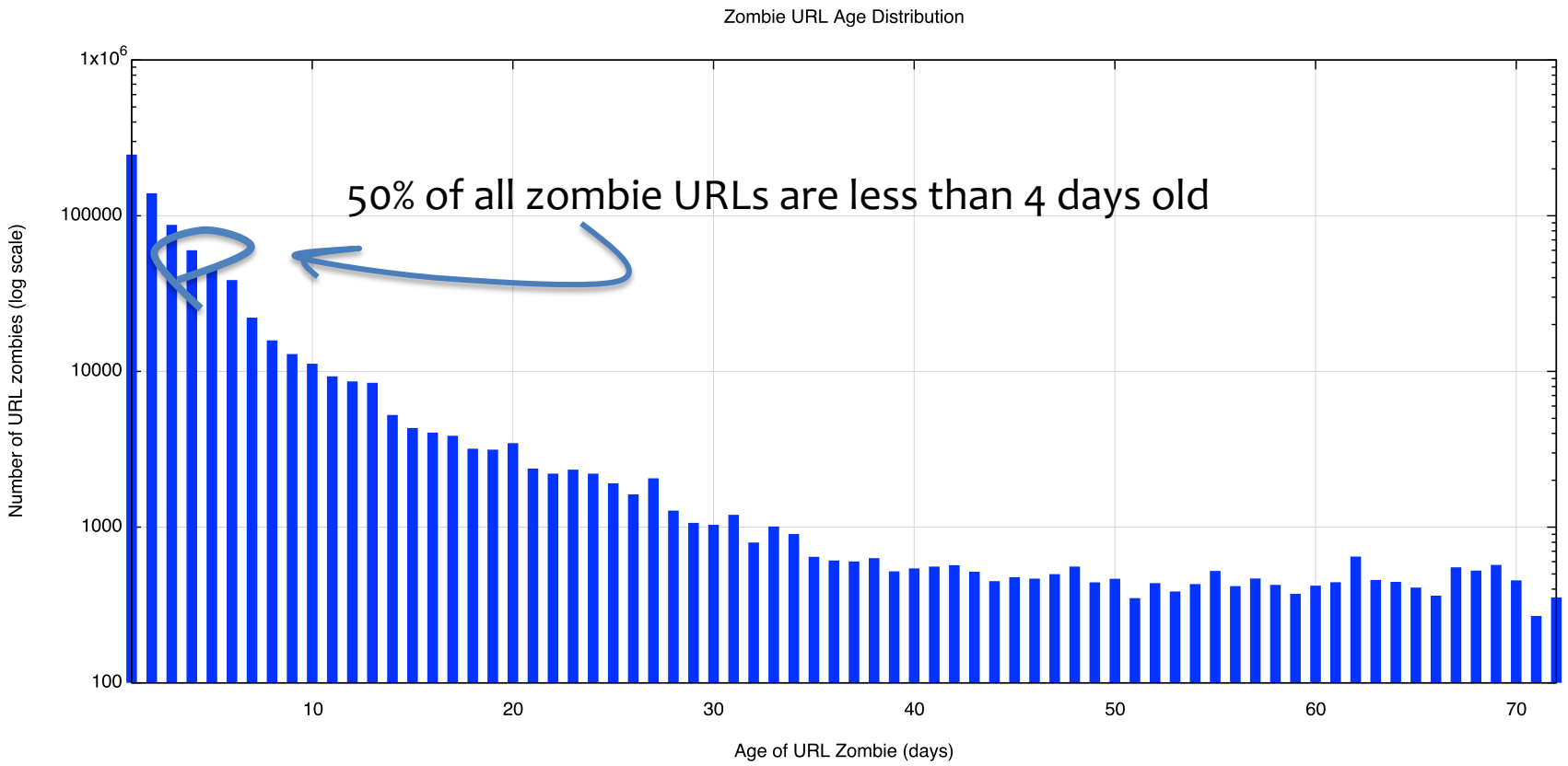
Or web proxies that just have too much time (and space) on their hands and want to fill all that space with a vast collection of identical 1x1 pixel gifs?

Let's look at web zombies …

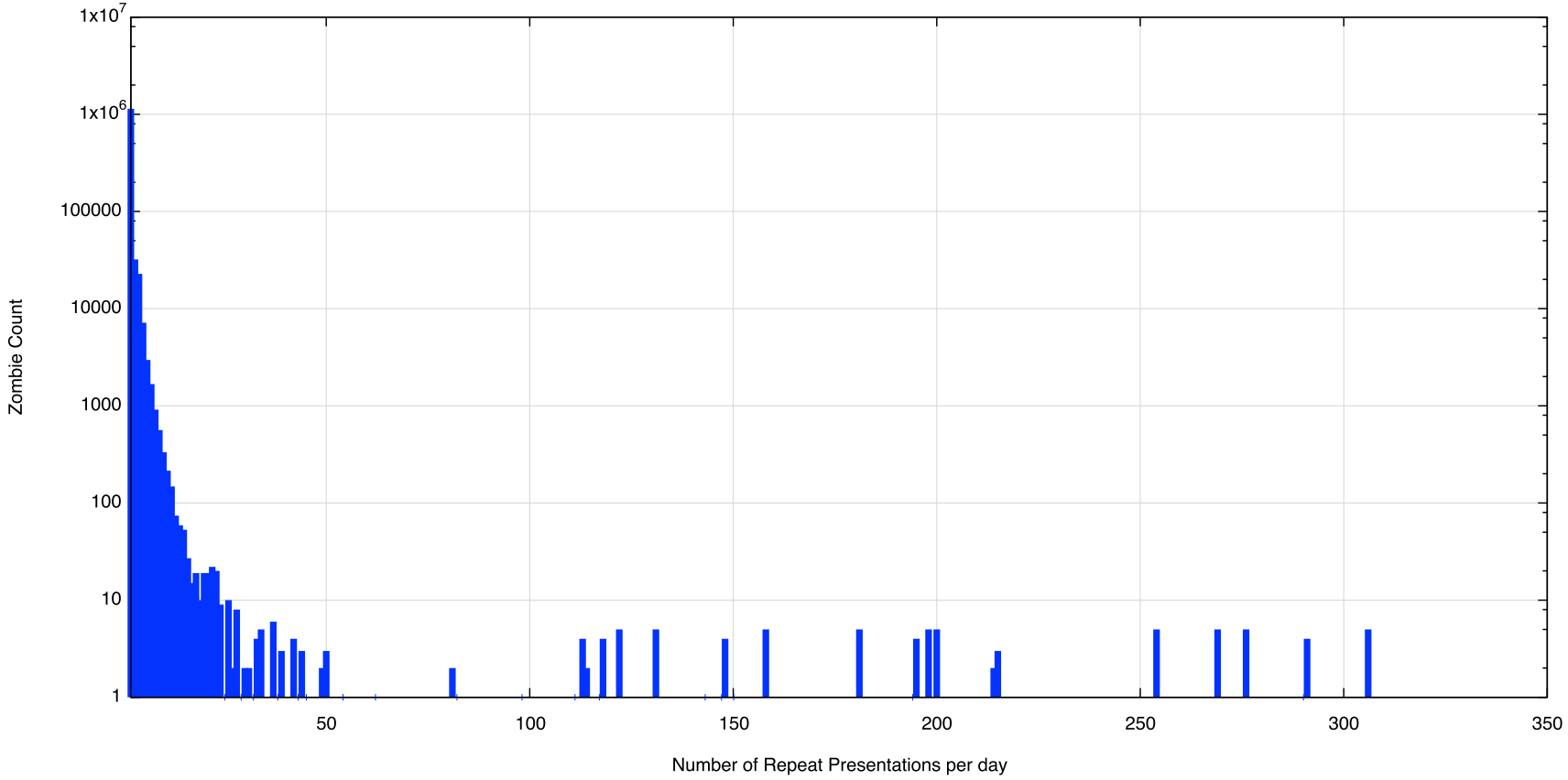
# Zombie URL Age Distribution



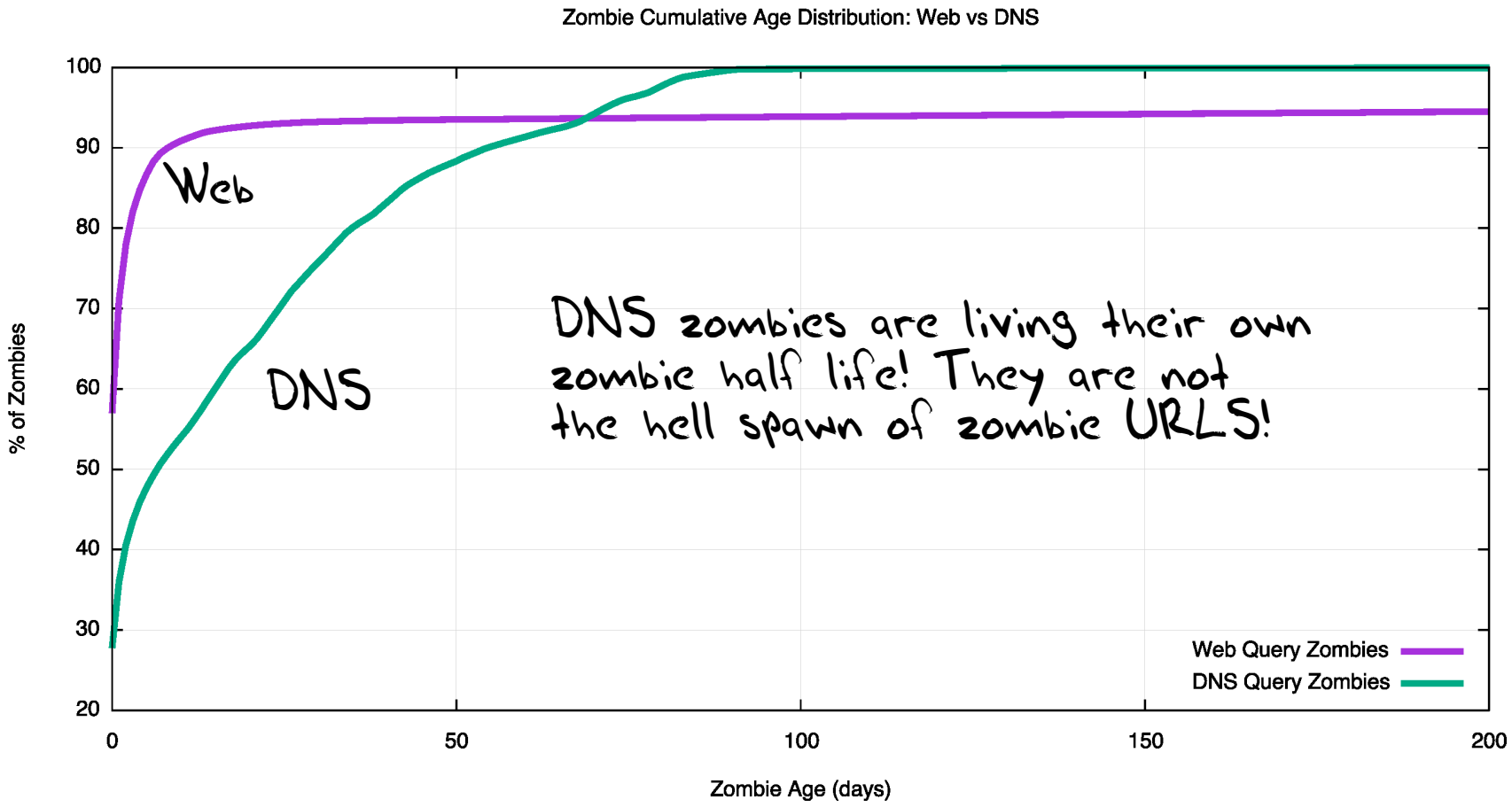
# Zombie URL Age Distribution



# Zombie URL Repeats



# DNS vs URLs

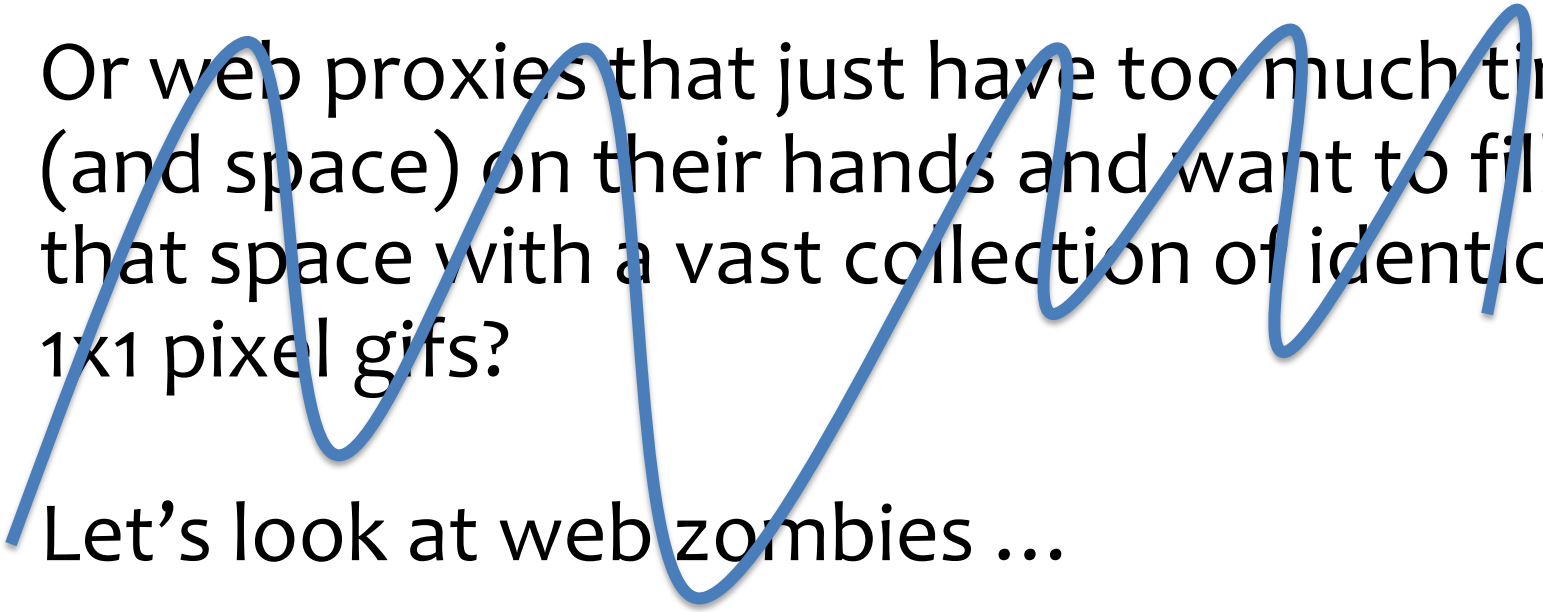

Zombie Cumulative Age Distribution: Web vs DNS
% of Zombies
Zombie Age (days)
100
90
80
70
60
50
40
30
20
0
50
100
150
200
Web
DNS
DNS zombies are living their own zombie half life! They are not the hell spawn of zombie URLS!
Web Query Zombies
DNS Query Zombies

# What is causing this?

Is this the result of a collection of deranged DNS recursive resolvers with an obsession about never forgetting a thing?

Or web proxies that just have too much time (and space) on their hands and want to fill all that space with a vast collection of identical 1x1 pixel gifs?

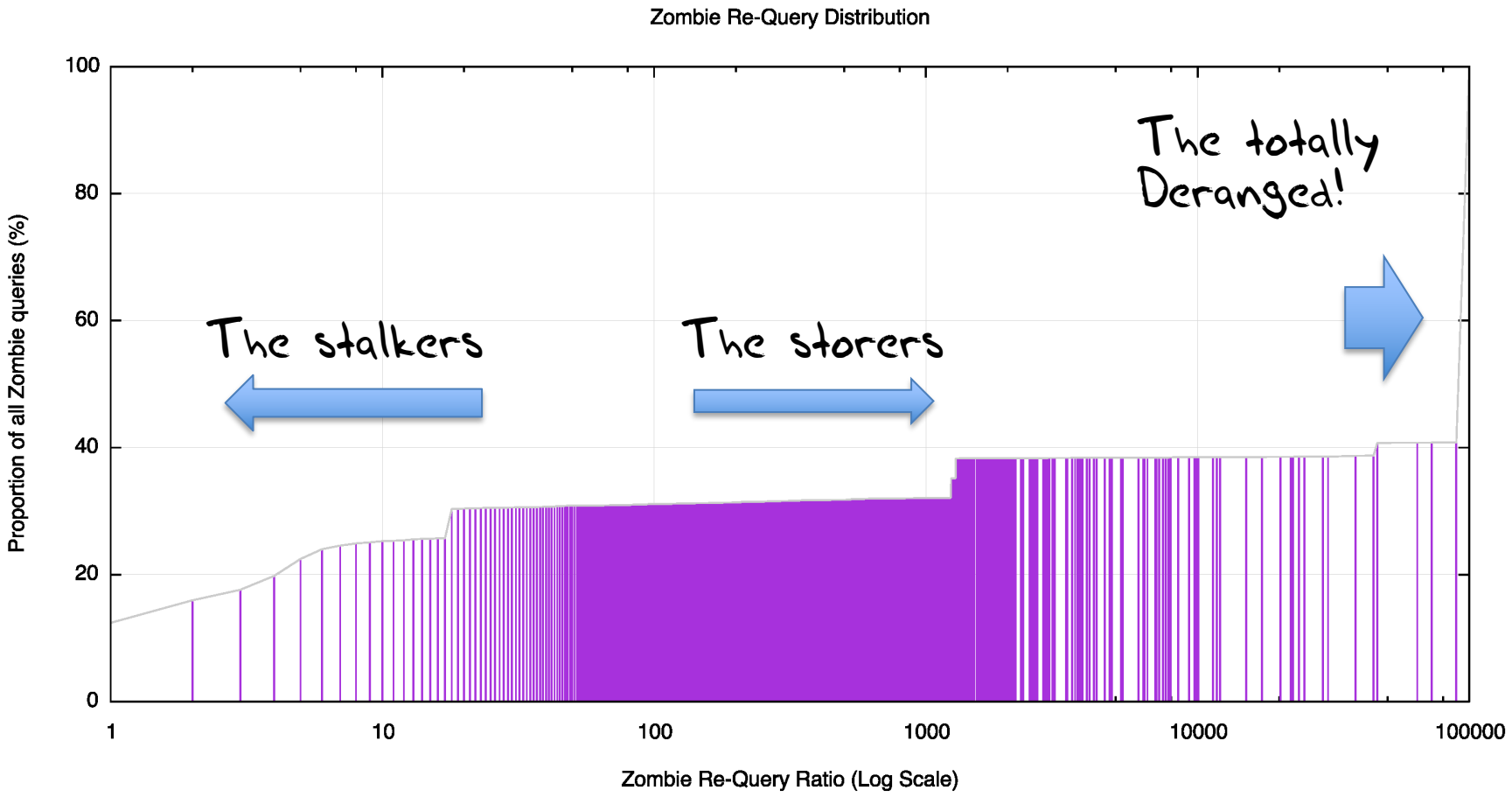
Let's look at web zombies …



# Who Are These Deranged Resolvers?

| Resolver | Current | Zombie | Ratio | ASN | CC | AS Name |
|---|---|---|---|---|---|---|
| 186.151.28.130 | 3,978,931 | 4,610,444,812 | 1,158 | 14754 | GT | Telgua, Guatemala |
| 87.236.233.178 | 14,124,423 | 1,006,797,893 | 71 | 35656 | JO | JUNET Jordanian Universities, Jordan |
| 74.205.176.249 | 9,868,204 | 870,945,137 | 88 | 53618 | CA | ADITY-OSH - Aditya Birla Minacs, Canada |
| 204.184.141.253 | 35,034,545 | 594,314,499 | 16 | 2572 | US | Missouri Research and Edu., United States |
| 38.229.33.65 | 7 | 573,038,416 | 81,862,630 | 23028 | US | Team Cymru Inc. United States |
| 80.246.0.3 | 1,486,712 | 379,724,419 | 255 | 21391 | DZ | TDA-AS,DZ Algeria |
| 80.246.0.2 | 2,041,670 | 373,155,047 | 182 | 21391 | DZ | TDA-AS,DZ Algeria |
| 87.236.232.5 | 5,697,987 | 255,364,280 | 44 | 35656 | JO | JUNET Jordanian Universities, Jordan |
| 74.205.162.254 | 1,975,978 | 200,821,246 | 101 | 14214 | CA | MINACS - Minacs Inc, Canada |
| 38.229.33.67 | 11 | 128,929,881 | 11,720,898 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.68 | 2 | 109,905,028 | 54,952,514 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.100 | 3 | 90,637,788 | 30,212,596 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.99 | 3 | 67,436,258 | 22,478,752 | 23028 | US | Team Cymru Inc, United States |
| 200.195.185.205 | 93,986 | 39,623,754 | 421 | 14868 | BR | COPEL Telecom S.A. Brazil |
| 167.102.229.10 | 1,632,910 | 17,868,074 | 10 | 27026 | US | Network Maryland, US United States |
| 54.183.221.9 | 13 | 17,637,567 | 1,356,735 | 16509 | US | AMAZON-02 - Amazon.com, United States |
| 54.183.144.165 | 59 | 17,331,749 | 293,758 | 16509 | US | AMAZON-02 - Amazon.com, United States |
| 192.235.48.69 | 3,259,591 | 12,759,627 | 4 | 14813 | BB | Columbus Telecommunications, Barbados |

# Three Zombie Factories



# The Stalkers

| Resolver | Current | Zombie | Ratio | ASN | CC | AS Name |
|---|---|---|---|---|---|---|
| 38.229.33.65 | 7 | 573,038,416 | 81,862,630 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.68 | 2 | 109,905,028 | 54,952,514 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.100 | 3 | 90,637,788 | 30,212,596 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.99 | 3 | 67,436,258 | 22,478,752 | 23028 | US | Team Cymru Inc, United States |
| 38.229.33.67 | 11 | 128,929,881 | 11,720,898 | 23028 | US | Team Cymru Inc, United States |
| 199.91.135.162 | 0 | 5,519,461 | 5,519,461 | 27471 | US | Blue Coat Systems, Inc, United States |
| 212.142.63.183 | 0 | 2,472,109 | 2,472,109 | 6830 | NL | LGI-UPC Liberty Global Operations, Netherlands |
| 212.142.48.75 | 0 | 2,401,930 | 2,401,930 | 6830 | NL | LGI-UPC Liberty Global Operations, Netherlands |
| 54.193.90.244 | 1 | 1,480,634 | 1,480,634 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.193.58.86 | 0 | 1,479,066 | 1,479,066 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.193.65.165 | 0 | 1,423,147 | 1,423,147 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.183.221.9 | 13 | 17,637,567 | 1,356,735 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.193.7.134 | 0 | 842,849 | 842,849 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 218.241.99.50 | 0 | 713,779 | 713,779 | 24151 | CN | China Internet Network Information Center, China |
| 54.215.202.77 | 0 | 372,889 | 372,889 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.215.190.109 | 0 | 365,598 | 365,598 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.215.215.191 | 0 | 361,804 | 361,804 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.193.83.224 | 0 | 361,474 | 361,474 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.219.130.114 | 0 | 345,080 | 345,080 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.183.145.224 | 0 | 338,949 | 338,949 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 54.193.11.144 | 0 | 334,725 | 334,725 | 16509 | US | AMAZON-02 - Amazon.com, Inc, United States |
| 220.128.227.81 | 0 | 326,208 | 326,208 | 3462 | TW | HINET Data Communication Business Group, Taiwan |
| 59.120.57.250 | 0 | 323,403 | 323,403 | 3462 | TW | HINET Data Communication Business Group, Taiwan |
| 86.82.68.237 | 0 | 321,396 | 321,396 | 1136 | NL | KPN, Netherlands |
| 64.89.232.86 | 0 | 317,115 | 317,115 | 17204 | US | Nominum, Inc, United States |

# The Storers (and the totally deranged!)

| Resolver | Current Uniques | Current Repeats | Zombie Uniques | Zombie Repeats | Zombie Repeat Ratio | ASN | CC | AS Name |
|---|---|---|---|---|---|---|---|---|
| 74.205.176.249 | 3,238 | 10,501,108 | 724 | 876,780,601 | 1,211,023 | 53618 | CA | Aditya Birla Minacs Worldwide, Canada |
| 204.184.141.253 | 2,495 | 35,034,545 | 572 | 600,739,995 | 1,050,244 | 2572 | US | MOREnet, United States |
| 186.151.28.130 | 926 | 3,978,931 | 6,462 | 4,704,634,886 | 728,046 | 14754 | GT | Telgua, Guatemala |
| 74.205.162.254 | 345 | 2,167,441 | 411 | 202,079,128 | 491,676 | 14214 | CA | MINACS – Minacs, Canada |
| 87.236.233.178 | 8,201 | 14,435,262 | 3,094 | 1,019,572,525 | 329,532 | 35656 | JO | JUNET Jordanian Universities, Jordan |
| 209.173.47.77 | 136 | 495,700 | 11 | 3,338,108 | 303,464 | 18474 | US | Aeneas Internet Services, United States |
| 115.249.45.34 | 37 | 265,058 | 12 | 3,154,574 | 262,881 | 18101 | IN | Reliance Communications, India |
| 200.195.185.205 | 74 | 93,986 | 218 | 40,534,251 | 185,936 | 14868 | BR | COPEL Telecom, Brazil |
| 195.53.128.4 | 215 | 70,442 | 1 | 138,326 | 138,326 | 31418 | ES | SOGECABLE, Spain |
| 50.203.18.22 | 223 | 1,946,242 | 6 | 668,671 | 111,445 | 7922 | US | Comcast, United States |
| 197.215.152.195 | 13,830 | 37,012,512 | 1,408 | 142,438,304 | 101,163 | 37558 | LY | LITC, Libya |
| 201.94.158.33 | 98 | 347,644 | 17 | 1,522,810 | 89,577 | 28625 | BR | Terremark do Brasil, Brazil |
| 38.95.167.66 | 75 | 242,166 | 6 | 436,269 | 72,711 | 174 | US | Cogent Communications, United States |
| 46.174.164.4 | 93 | 785,915 | 6 | 435,973 | 72,662 | 39742 | UA | ITM IT-MARK, Ukraine |
| 167.102.229.7 | 612 | 99,122 | 58 | 3,729,929 | 64,309 | 27026 | US | NETWORKMARYLAND, United States |
| 87.236.232.5 | 54,998 | 5,819,430 | 5,634 | 258,275,972 | 45,842 | 35656 | JO | JUNET Jordanian Universities, Jordan |
| 217.108.239.47 | 12 | 55,886 | 39 | 1,731,390 | 44,394 | 3215 | FR | AS3215 Orange, France |
| 217.108.239.58 | 68 | 57,215 | 39 | 1,727,063 | 44,283 | 3215 | FR | AS3215 Orange, France |
| 167.102.229.10 | 6,823 | 1,634,688 | 505 | 19,286,366 | 38,190 | 27026 | US | NETWORKMARYLAND, United States |
| 67.51.123.126 | 57 | 239,777 | 5 | 150,976 | 30,195 | 7385 | US | Integra Telecom, United States |
| 89.207.162.2 | 670 | 16,443 | 1 | 28,921 | 28,921 | 41383 | GB | WOLASN Wolseley, United Kingdom |
| 187.7.128.5 | 0 | 0 | 18 | 444,244 | 24,680 | 8167 | BR | Brasil Telecom, Brazil |
| 41.63.166.180 | 14 | 4,696 | 4 | 94,524 | 23,631 | 36907 | AO | TVCaboAngola, Angola |
| 216.195.101.101 | 189 | 358,403 | 9 | 201,797 | 22,421 | 33481 | US | BELWAVE COMMUNICATIONS, United States |
| 212.118.102.114 | 94 | 223,292 | 3 | 66,067 | 22,022 | 34397 | SA | Cyberia Riyadh, Saudi Arabia |
| 200.111.157.10 | 41 | 53,333 | 183 | 3,690,776 | 20,168 | 6471 | CL | ENTEL, Chile |
| 12.13.190.116 | 14 | 1,890 | 8 | 137,972 | 17,246 | 7018 | US | ATT-INTERNET4, United States |
| 98.142.39.194 | 19 | 484,707 | 2 | 30,221 | 15,110 | 25899 | US | LS Networks, United States of America |
| 200.3.214.69 | 5 | 3,536 | 16 | 193,635 | 12,102 | 17126 | CL | E-money, Chile |
| 84.17.5.235 | 42 | 195,941 | 13 | 152,705 | 11,746 | 8359 | RU | MTS MTS PJSC, Russian Federation |