Evidence of Bitsquatting in COM/NET Queries

Duane Wessels

February, 2012

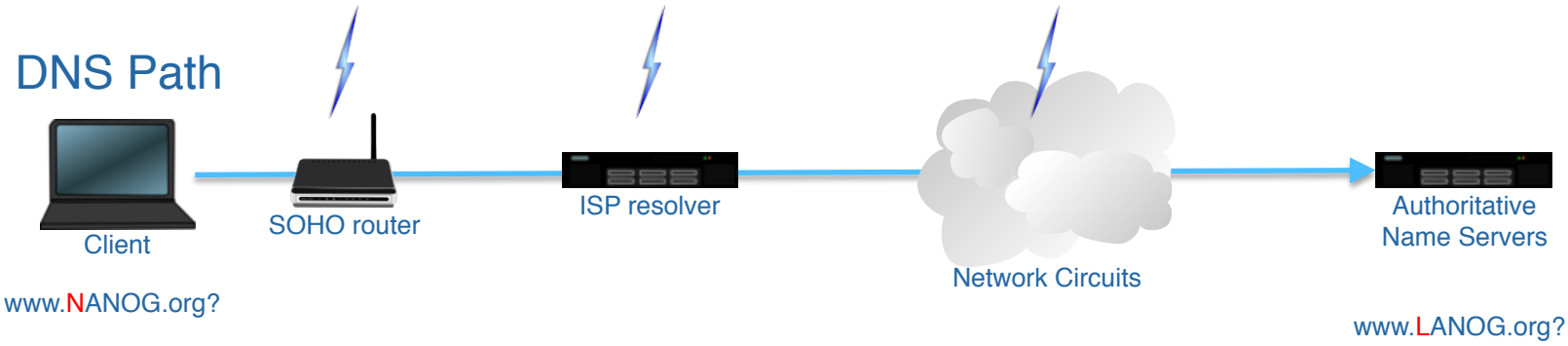
VERISIGN

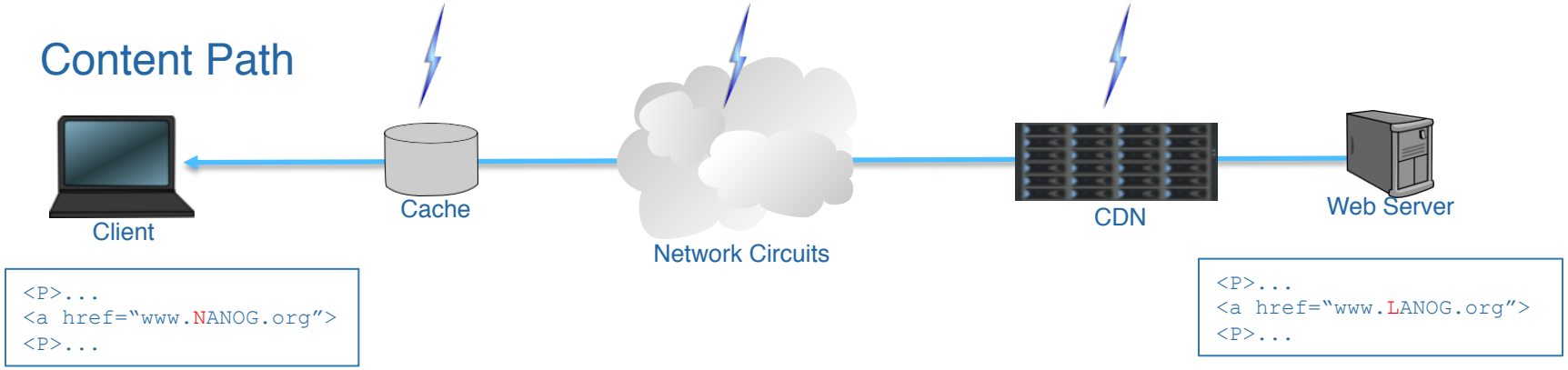
Motivation

- Artem Dinaburg wrote about “bitsquatting” mid-2011 [1]
- Bit-level errors in domain names result in misdirected traffic.
  - MICROSOFT.COM -> MICROSMFT.COM
  - GOOGLE.COM -> GOOG|E.COM
  - MSFT.NET -> M3FT.NET
  - FACEBOOK.COM -> FAKEBOOK.COM
- Bit-level errors might occur in RAM, on Disk, or during transmission

[1] http://www.hakim.ws/BHUS2011/materials/Dinaburg/BH_US_11_Dinaburg_Bitsquatting_WP.pdf

Bitsquatting





Dinaburg's Numbers

- 52,317 bitsquat requests for 31 domains over 221 days
  - 7.6 per domain per day
- 96% of bit errors happened prior to DNS resolution.
  - HTTP Host header matches DNS query name

- **Up to 4% happened during resolution**
  - 0.3 per domain per day

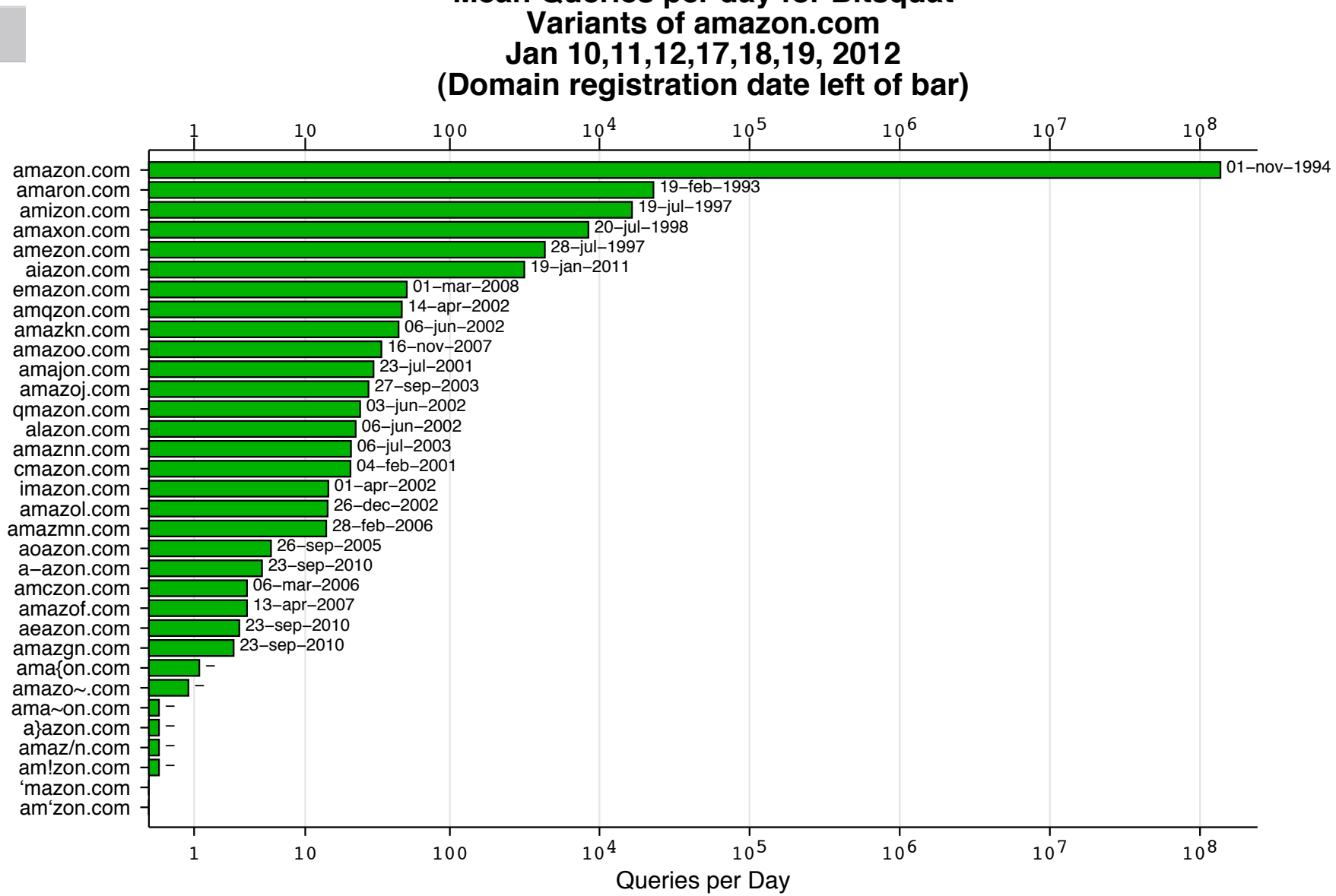
Questions

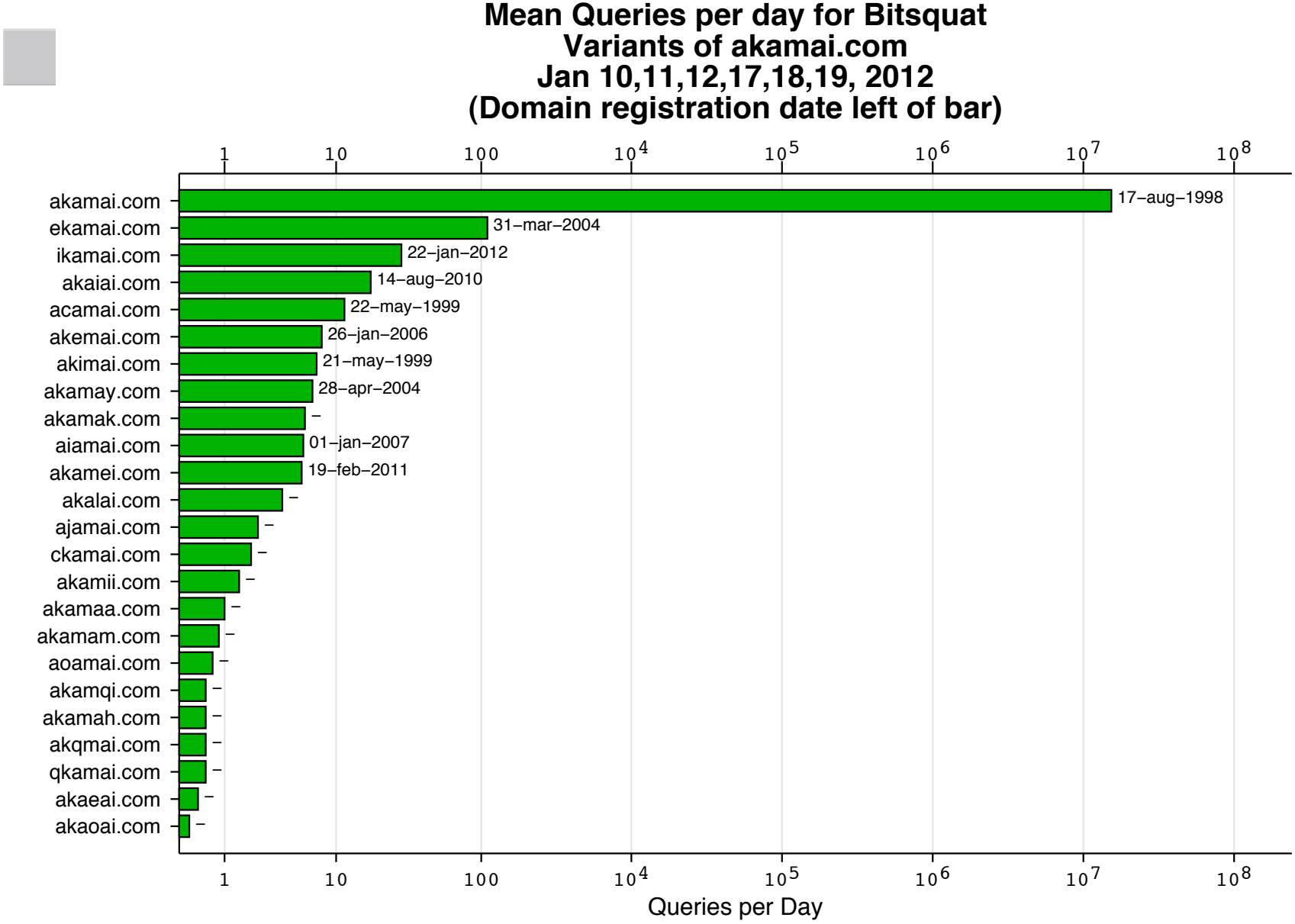
- What evidence does Verisign see of bitsquatting errors?
- If bitsquatting errors are happening, shouldn't they happen to all bits with equal probability?
- Can we tell the difference between bitsquatting and typos?
- Should domain owners be concerned about bitsquatting?

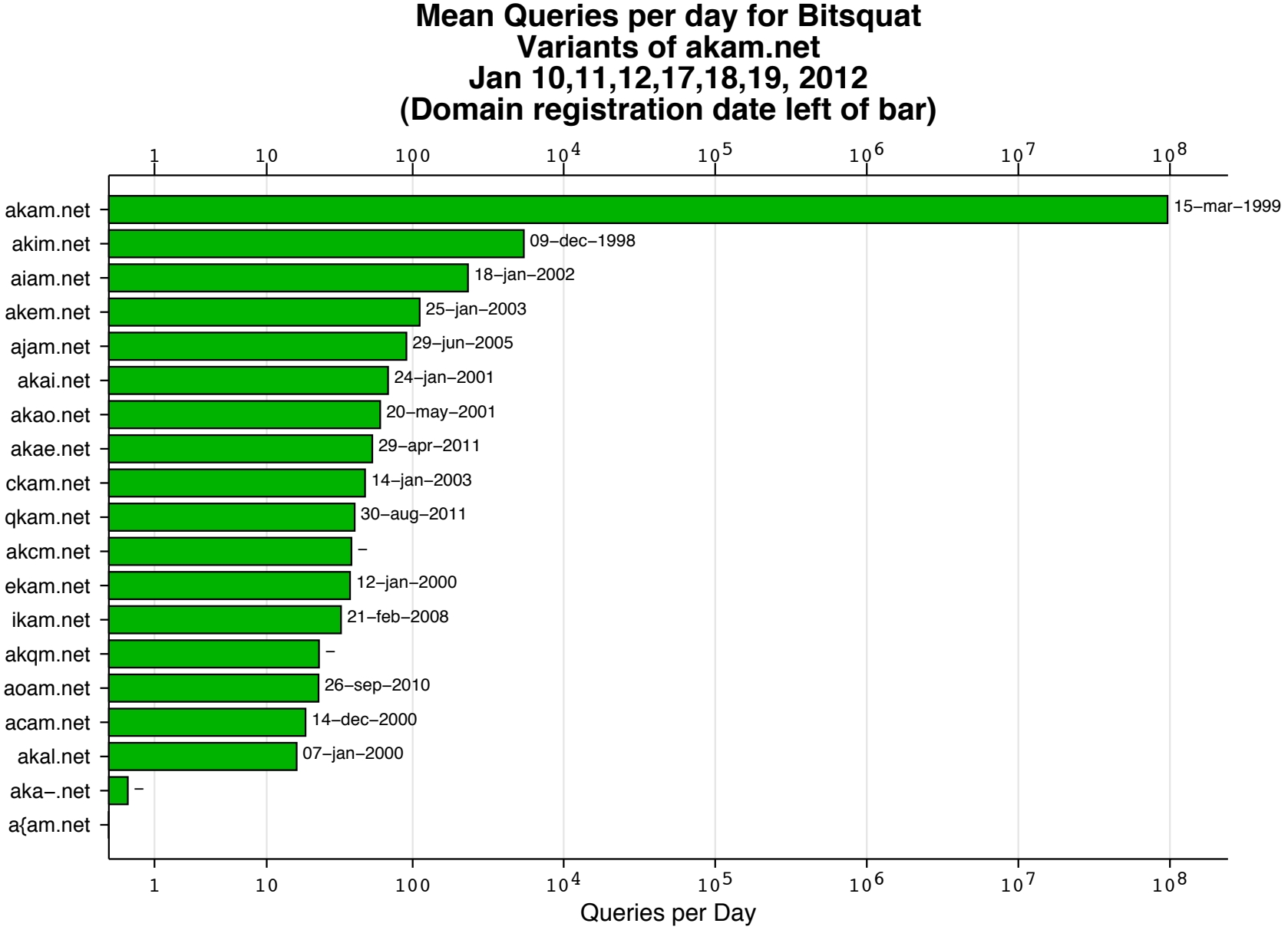
Data

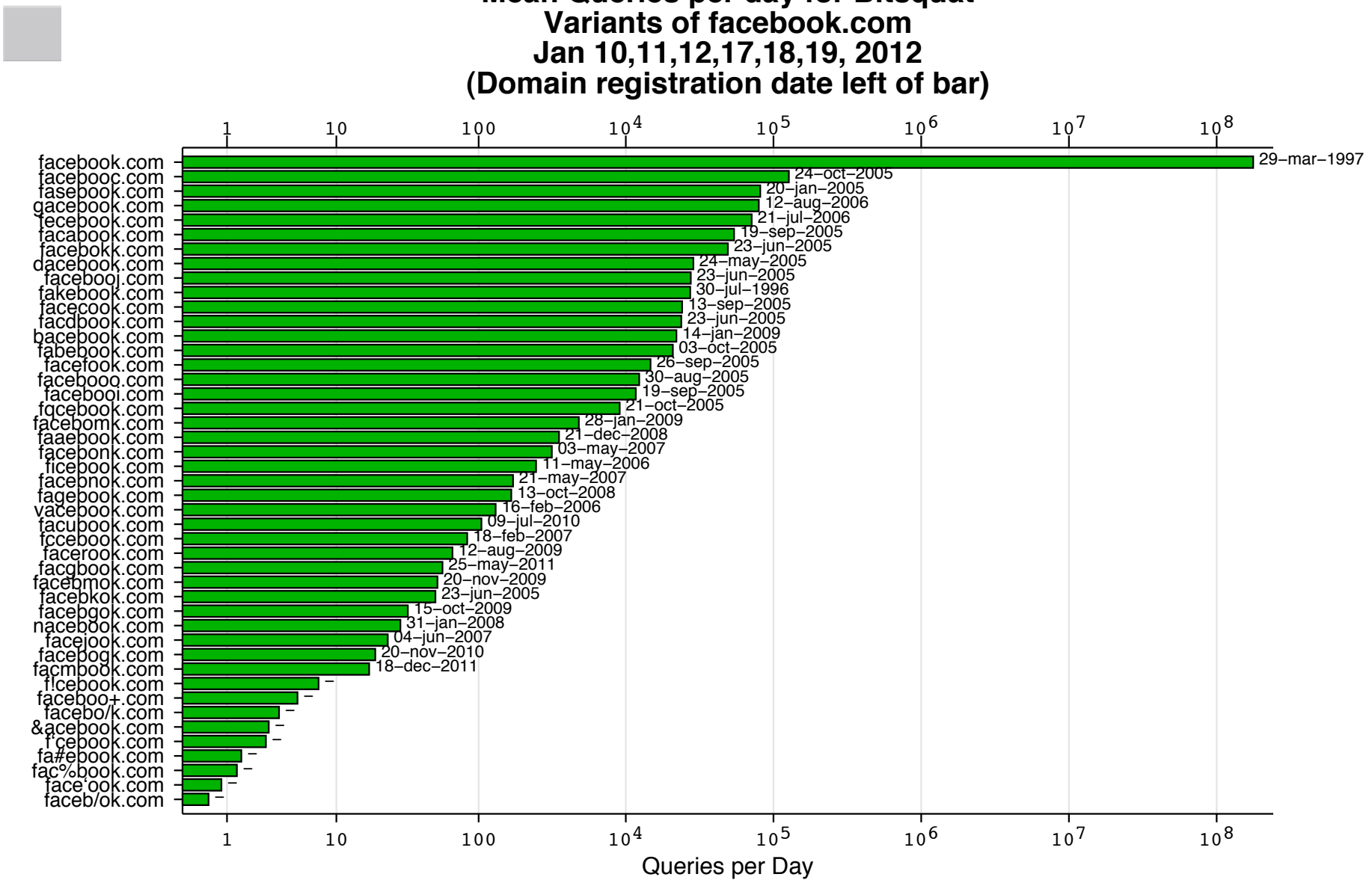
- Queries to com/net name servers over a period of 6 days
  - Jan 10-12, 17-19
- From 4 Verisign sites
  - SFO, IAD, NYC, AMS
- Isolate queries for high-profile brands
  - Microsoft
  - Google
  - Facebook
  - Akamai
  - Amazon
- Analyzed on small Hadoop cluster
- Queries with bad checksums are omitted

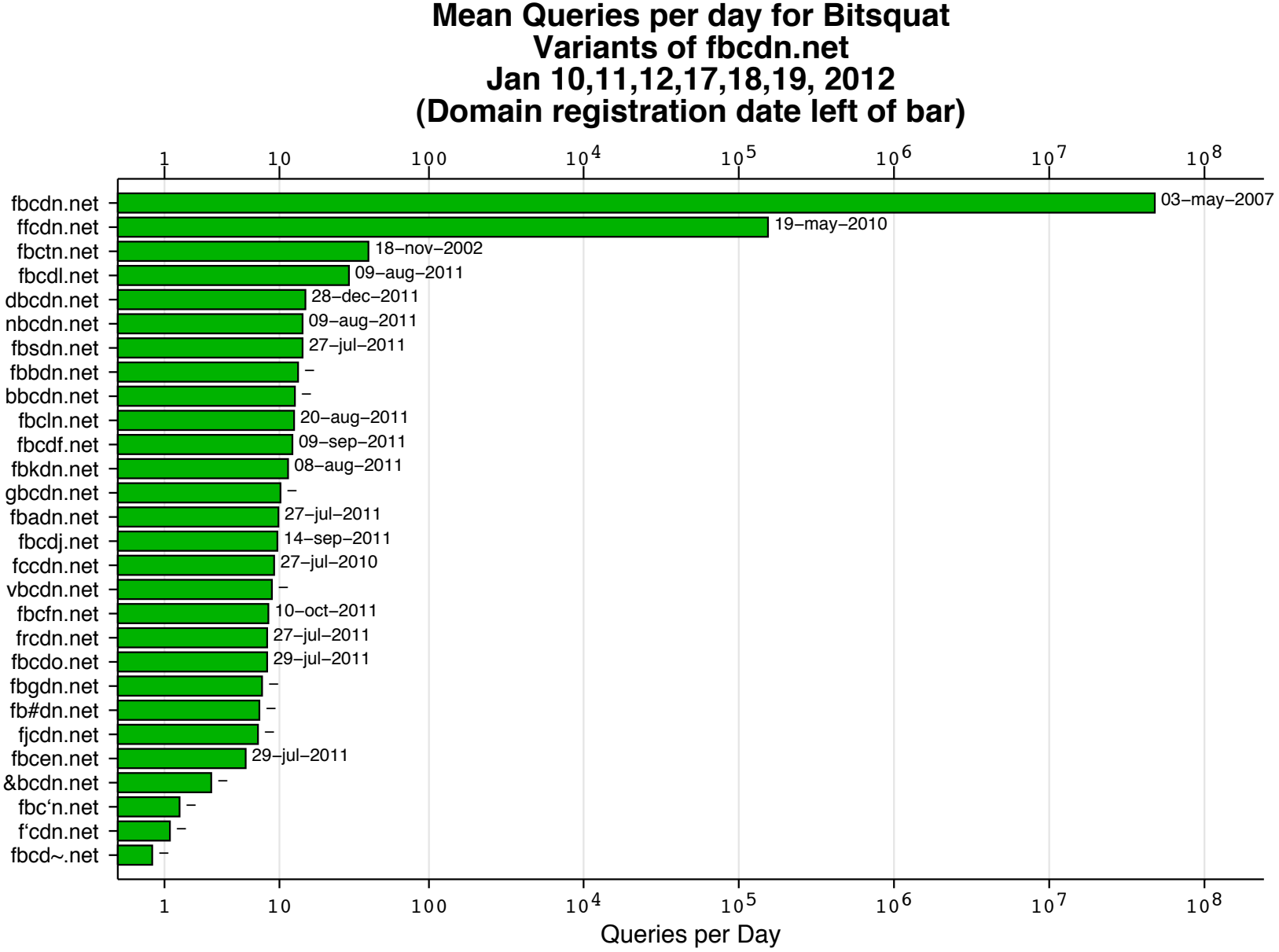
Results

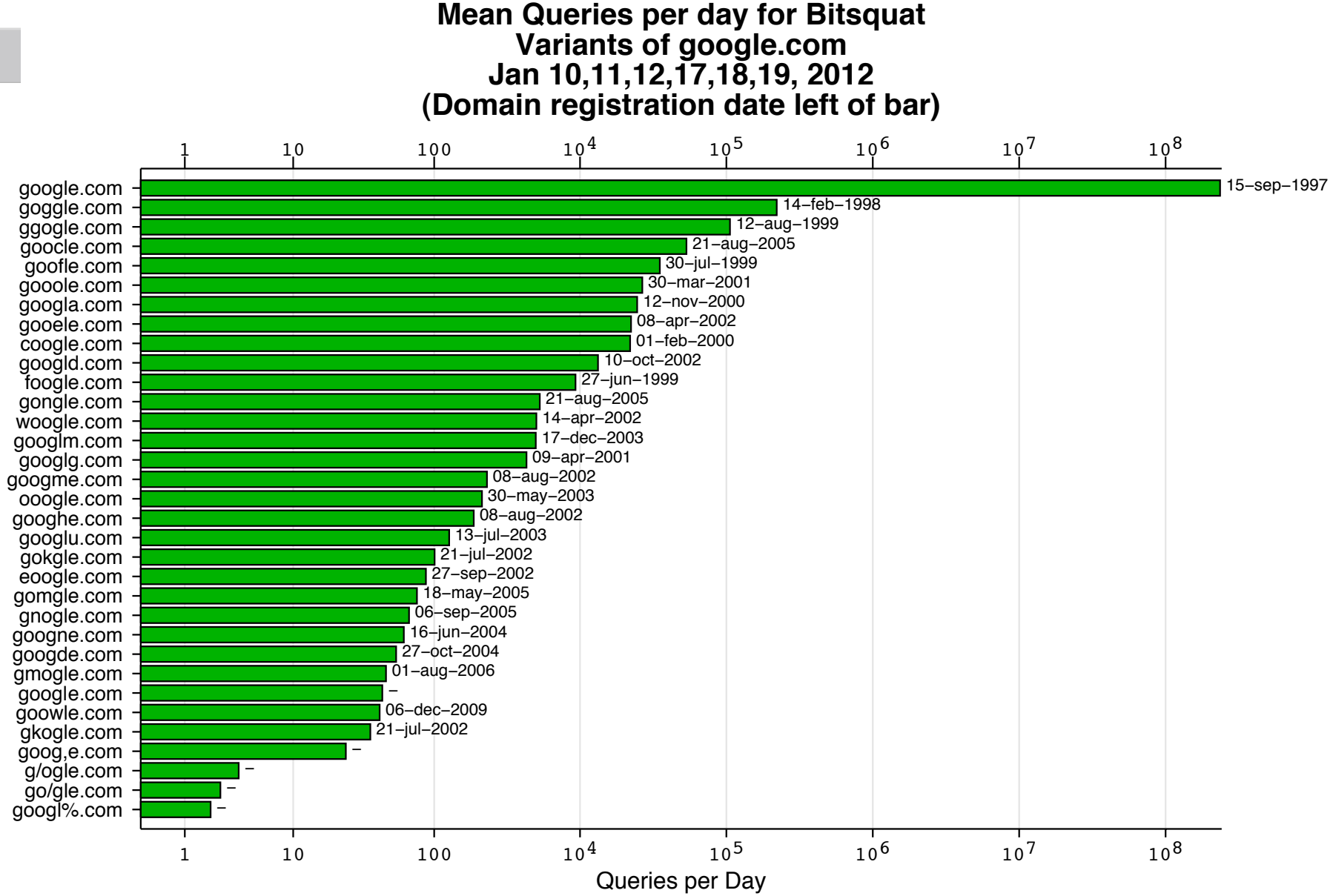

Mean Queries per day for Bitsquat
Variants of amazon.com
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
amazon.com
amaron.com
amizon.com
amaxon.com
amezon.com
aiazon.com
emazon.com
amqzon.com
amazkn.com
amazoo.com
amajon.com
amazoj.com
qmazon.com
alazon.com
amaznn.com
cmazon.com
imazon.com
amazol.com
amazmn.com
aoazon.com
a–azon.com
amczon.com
amazof.com
aeazon.com
amazgn.com
ama{on.com
amazo~.com
ama~on.com
a}azon.com
amaz/n.com
am!zon.com
‘mazon.com
am‘zon.com
01–nov–1994
19–feb–1993
19–jul–1997
20–jul–1998
28–jul–1997
19–jan–2011
01–mar–2008
14–apr–2002
06–jun–2002
16–nov–2007
23–jul–2001
27–sep–2003
03–jun–2002
06–jun–2002
06–jul–2003
04–feb–2001
01–apr–2002
26–dec–2002
28–feb–2006
26–sep–2005
23–sep–2010
06–mar–2006
13–apr–2007
23–sep–2010
23–sep–2010
–
–
–
–
–
Queries per Day

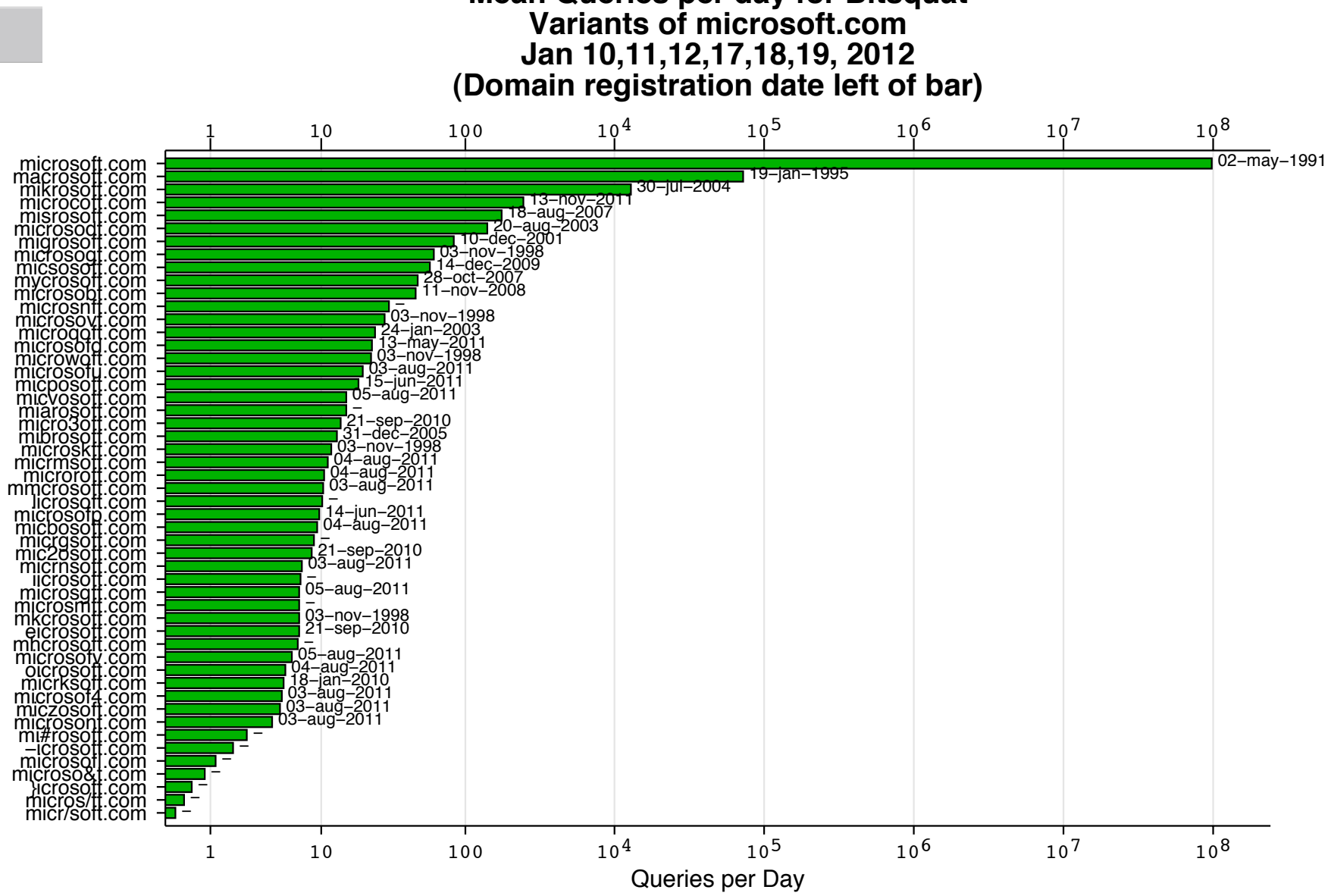

Mean Queries per day for Bitsquat
Variants of akamai.com
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
akamai.com
ekamai.com
ikamai.com
akaiai.com
acamai.com
akemai.com
akimai.com
akamay.com
akamak.com
aiamai.com
akamei.com
akalai.com
ajamai.com
ckamai.com
akamii.com
akamaa.com
akamam.com
aoamai.com
akamqi.com
akamah.com
akqmai.com
qkamai.com
akaeai.com
akaoai.com
17–aug–1998
31–mar–2004
22–jan–2012
14–aug–2010
22–may–1999
26–jan–2006
21–may–1999
28–apr–2004
01–jan–2007
19–feb–2011
Queries per Day

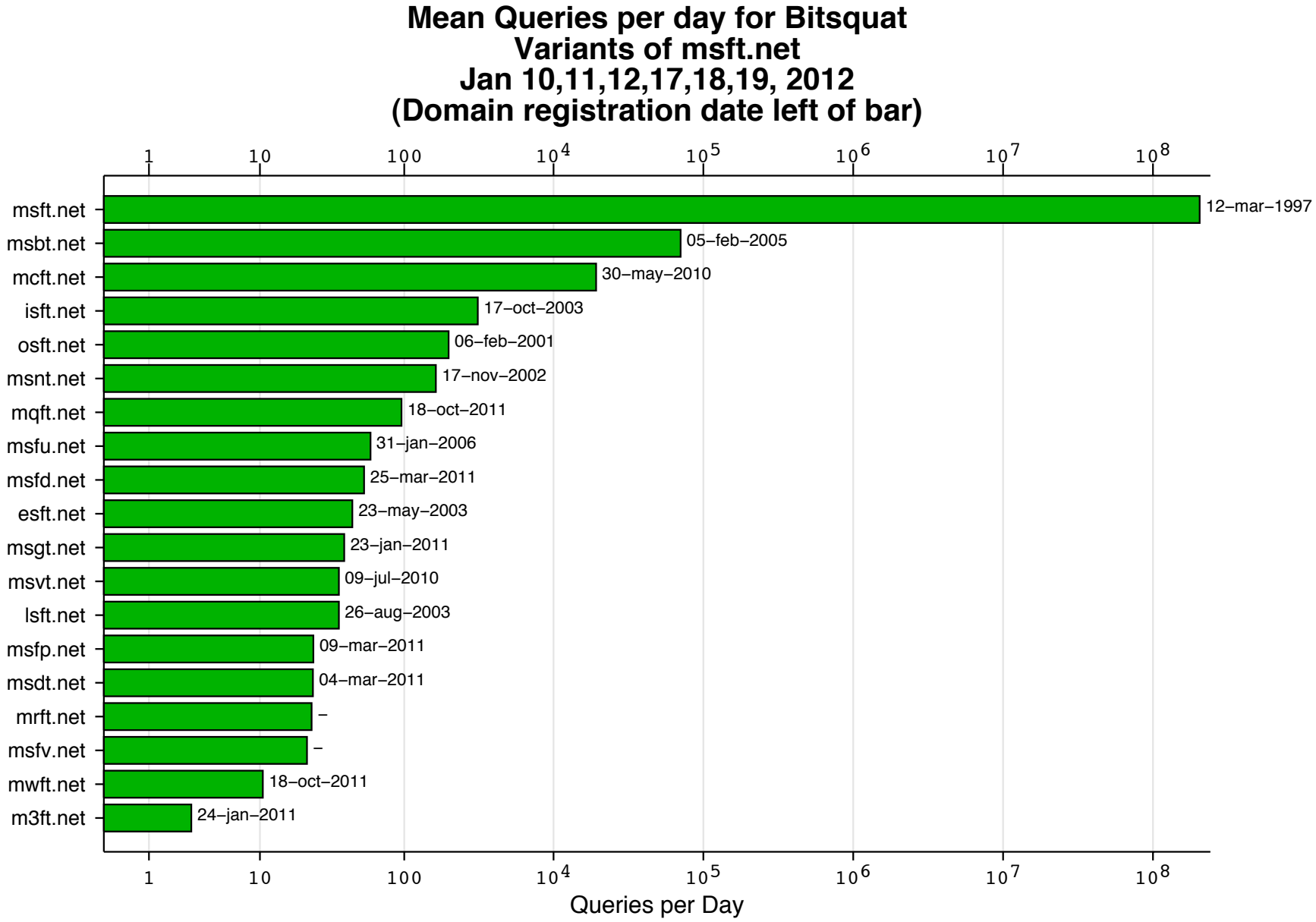

Mean Queries per day for Bitsquat
Variants of akam.net
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
akam.net
akim.net
aiam.net
akem.net
ajam.net
akai.net
akao.net
akae.net
ckam.net
qkam.net
akcm.net
ekam.net
ikam.net
akqm.net
aoam.net
acam.net
akal.net
aka–.net
a{am.net
15–mar–1999
09–dec–1998
18–jan–2002
25–jan–2003
29–jun–2005
24–jan–2001
20–may–2001
29–apr–2011
14–jan–2003
30–aug–2011
–
12–jan–2000
21–feb–2008
–
26–sep–2010
14–dec–2000
07–jan–2000
–
Queries per Day

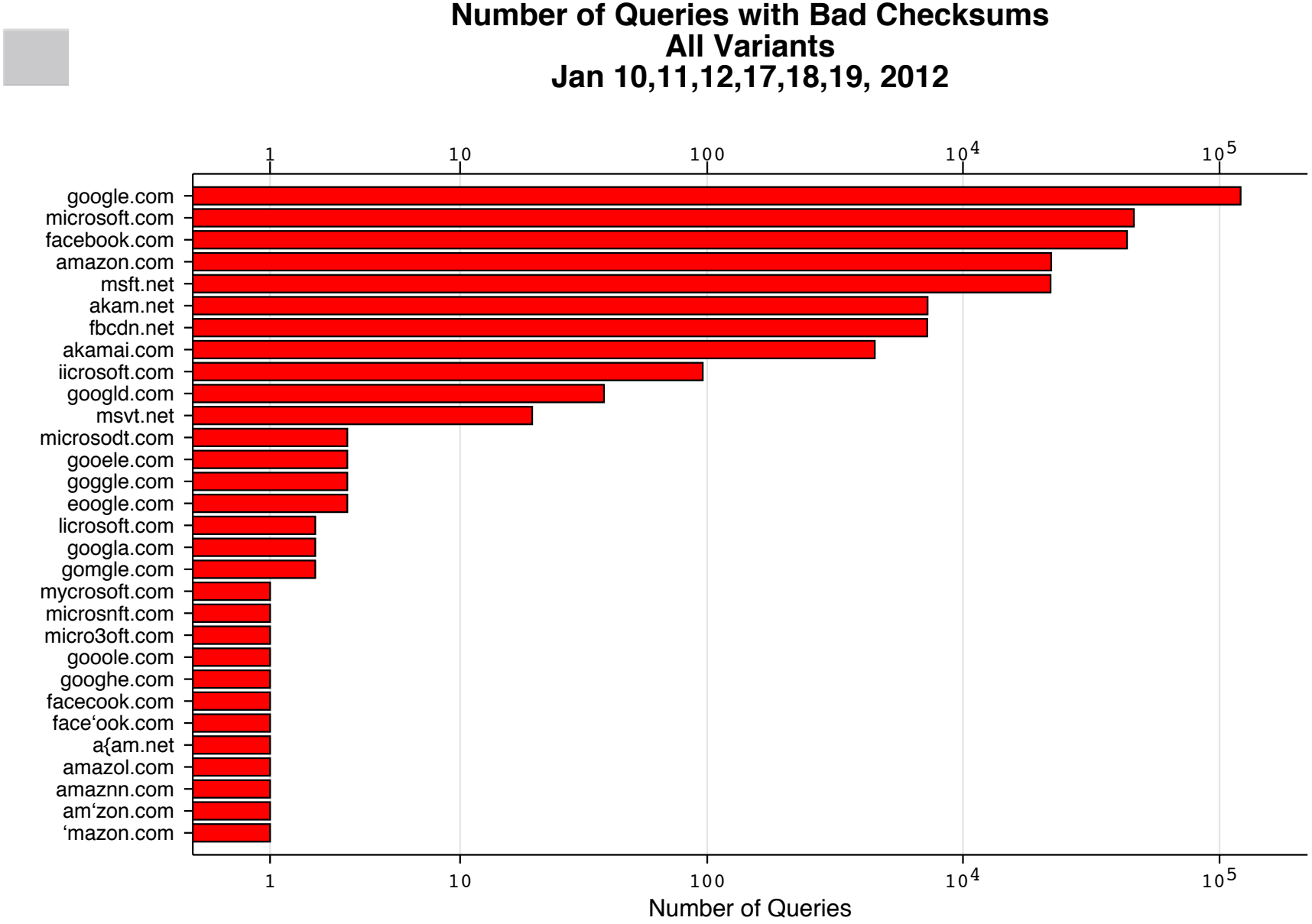

Mean Queries per day for Bitsquat
Variants of facebook.com
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
facebook.com
facebooc.com
fasebook.com
gacebook.com
fecebook.com
facabook.com
facebokk.com
dacebook.com
facebooj.com
fakebook.com
facecook.com
facdbook.com
bacebook.com
fabebook.com
facefook.com
facebooo.com
facebooi.com
fqcebook.com
facebomk.com
faaebook.com
faceponk.com
ficebook.com
facebnok.com
fagebook.com
vacebook.com
facubook.com
fccebook.com
facerook.com
facgbook.com
facebmok.com
facebkok.com
facebgok.com
nacebook.com
facejook.com
facebogk.com
facmbook.com
f!cebook.com
faceboo+.com
facebo/k.com
&acebook.com
f'cebook.com
fa#ebook.com
fac%book.com
face'ook.com
faceb/ok.com
29–mar–1997
24–oct–2005
20–jan–2005
12–aug–2006
21–jul–2006
19–sep–2005
23–jun–2005
24–may–2005
23–jun–2005
30–jul–1996
13–sep–2005
23–jun–2005
14–jan–2009
03–oct–2005
26–sep–2005
30–aug–2005
19–sep–2005
21–oct–2005
28–jan–2009
21–dec–2008
03–may–2007
11–may–2006
21–may–2007
13–oct–2008
16–feb–2006
09–jul–2010
18–feb–2007
12–aug–2009
25–may–2011
20–nov–2009
23–jun–2005
15–oct–2009
31–jan–2008
04–jun–2007
20–nov–2010
18–dec–2011
Queries per Day


Mean Queries per day for Bitsquat
Variants of fbcdn.net
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
fbcdn.net
ffcdn.net
fbctn.net
fbcdl.net
dbcdn.net
nbcdn.net
fbsdn.net
fbbdn.net
bbcdn.net
fbcln.net
fbcdf.net
fbkdn.net
gbcdn.net
fbadn.net
fbcdj.net
fccdn.net
vbcdn.net
fbcfn.net
frcdn.net
fbcdo.net
fbgdn.net
fb#dn.net
fjcdn.net
fbcen.net
&bcdn.net
fbc‘n.net
f‘cdn.net
fbcd~.net
03–may–2007
19–may–2010
18–nov–2002
09–aug–2011
28–dec–2011
09–aug–2011
27–jul–2011
–
–
20–aug–2011
09–sep–2011
08–aug–2011
–
27–jul–2011
14–sep–2011
27–jul–2010
–
10–oct–2011
27–jul–2011
29–jul–2011
–
–
–
29–jul–2011
–
–
–
Queries per Day

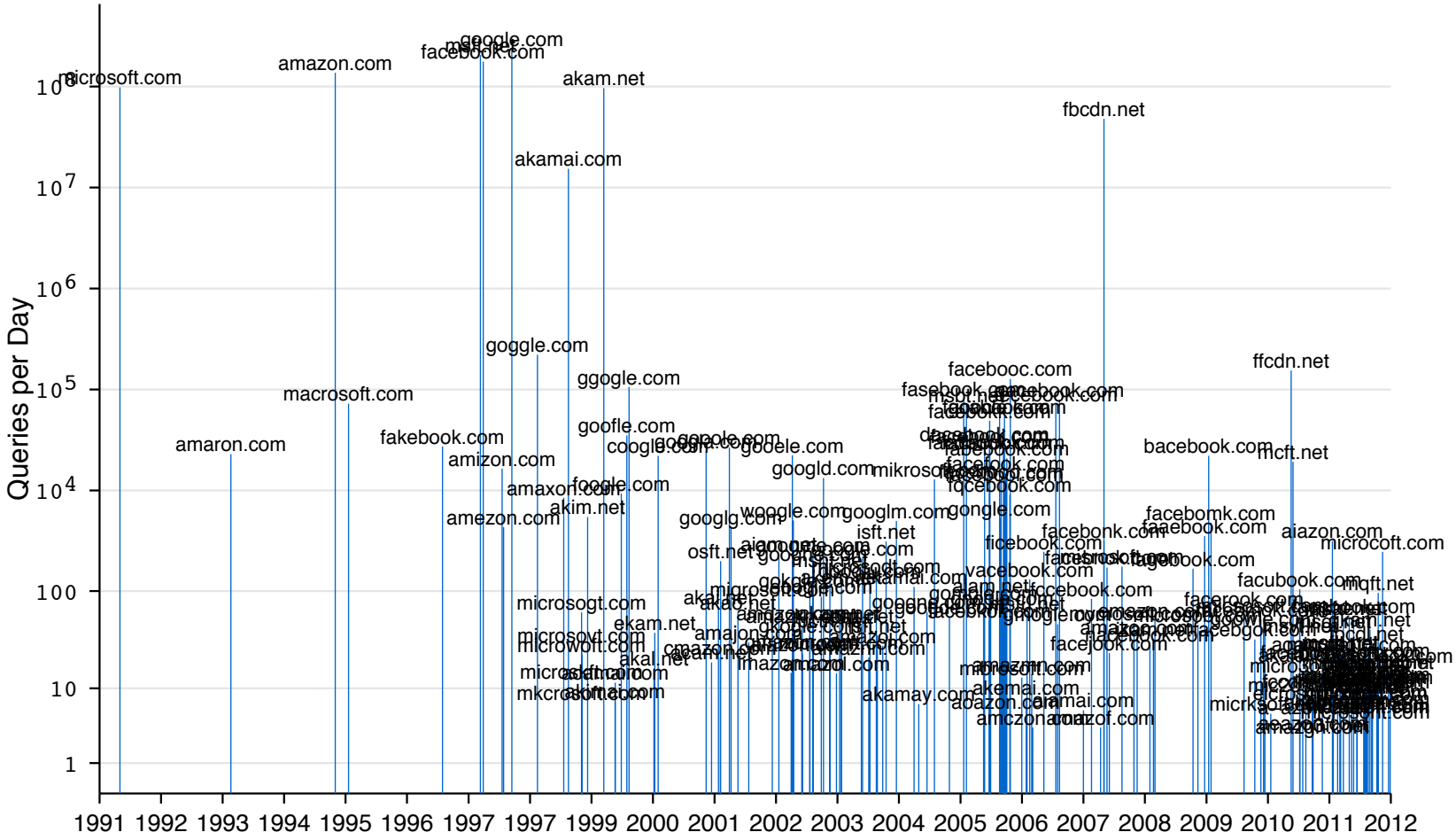

Mean Queries per day for Bitsquat
Variants of google.com
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
google.com
goggle.com
ggogle.com
goocle.com
goofle.com
gooole.com
googla.com
gooele.com
coogle.com
googld.com
foogle.com
gongle.com
woogle.com
googlm.com
googlg.com
googme.com
ooogle.com
googhe.com
googlu.com
gokgle.com
eoogle.com
gomgle.com
gnogle.com
googne.com
googde.com
gmogle.com
google.com
goowle.com
gkogle.com
goog,e.com
g/ogle.com
go/gle.com
googl%.com
15–sep–1997
14–feb–1998
12–aug–1999
21–aug–2005
30–jul–1999
30–mar–2001
12–nov–2000
08–apr–2002
01–feb–2000
10–oct–2002
27–jun–1999
21–aug–2005
14–apr–2002
17–dec–2003
09–apr–2001
08–aug–2002
30–may–2003
08–aug–2002
13–jul–2003
21–jul–2002
27–sep–2002
18–may–2005
06–sep–2005
16–jun–2004
27–oct–2004
01–aug–2006
–
06–dec–2009
21–jul–2002
–
–
–
Queries per Day


Mean Queries per day for Bitsquat
Variants of microsoft.com
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
microsoft.com 02–may–1991
macrosoft.com 19–jan–1995
mikrosoft.com 30–jul–2004
microcoft.com 13–nov–2011
misrosoft.com 18–aug–2007
microsodt.com 20–aug–2003
migrosoft.com 10–dec–2001
microsogt.com 03–nov–1998
micsosoft.com 14–dec–2009
mycrosoft.com 28–oct–2007
mrcrosobt.com 11–nov–2008
microsnft.com –
microsovt.com 03–nov–1998
microgoft.com 24–jan–2003
microsofd.com 13–may–2011
microwoft.com 03–nov–1998
microsofu.com 03–aug–2011
micposoft.com 15–jun–2011
micvosoft.com 05–aug–2011
miarosoft.com –
micro3oft.com 21–sep–2010
mibrosoft.com 31–dec–2005
microskt.com 03–nov–1998
micrmsoft.com 04–aug–2011
microroft.com 04–aug–2011
mmcrosoft.com 03–aug–2011
licrosoft.com –
microsofp.com 14–jun–2011
micbosoft.com 04–aug–2011
micrgsoft.com –
mic2osoft.com 21–sep–2010
micrnsoft.com 03–aug–2011
iicrosoft.com –
microsgft.com 05–aug–2011
microsmft.com –
mkcrosoft.com 03–nov–1998
eicrosoft.com 21–sep–2010
mhcrosoft.com –
microsofv.com 05–aug–2011
oicrosoft.com 04–aug–2011
micrksoft.com 18–jan–2010
microsof4.com 03–aug–2011
miczosoft.com 03–aug–2011
microsont.com 03–aug–2011
mi#rosoft.com –
–icrosoft.com –
microsqft.com –
microso&t.com –
kicrosoft.com –
micros/ft.com –
micr/soft.com –
Queries per Day


Mean Queries per day for Bitsquat
Variants of msft.net
Jan 10,11,12,17,18,19, 2012
(Domain registration date left of bar)
1
10
100
10^4
10^5
10^6
10^7
10^8
msft.net
msbt.net
mcft.net
isft.net
osft.net
msnt.net
mqft.net
msfu.net
msfd.net
esft.net
msgt.net
msvt.net
lsft.net
msfp.net
msdt.net
mrft.net
msfv.net
mwft.net
m3ft.net
12–mar–1997
05–feb–2005
30–may–2010
17–oct–2003
06–feb–2001
17–nov–2002
18–oct–2011
31–jan–2006
25–mar–2011
23–may–2003
23–jan–2011
09–jul–2010
26–aug–2003
09–mar–2011
04–mar–2011
–
–
18–oct–2011
24–jan–2011
Queries per Day


Number of Queries with Bad Checksums
All Variants
Jan 10,11,12,17,18,19, 2012
1
10
100
10^4
10^5
google.com
microsoft.com
facebook.com
amazon.com
msft.net
akam.net
fbcdn.net
akamai.com
iicrosoft.com
googld.com
msvt.net
microsodt.com
gooele.com
goggle.com
eoogle.com
licrosoft.com
googla.com
gomgle.com
mycrosoft.com
microsnft.com
micro3oft.com
gooole.com
googhe.com
facecook.com
face‘ook.com
a{am.net
amazol.com
amaznn.com
am‘zon.com
‘mazon.com
Number of Queries

Number of Queries by Date of Registration



Conclusions

- For some of the most popular domains, bit-level errors during DNS resolution appear to occur very infrequently
  - about once every 10^7 – 10^8 queries
  - Much less often than typos
- Bit-level errors separate from DNS (i.e., in distribution and storage of content) is the more serious problem.
  - Perhaps its time for an HTTP checksum?