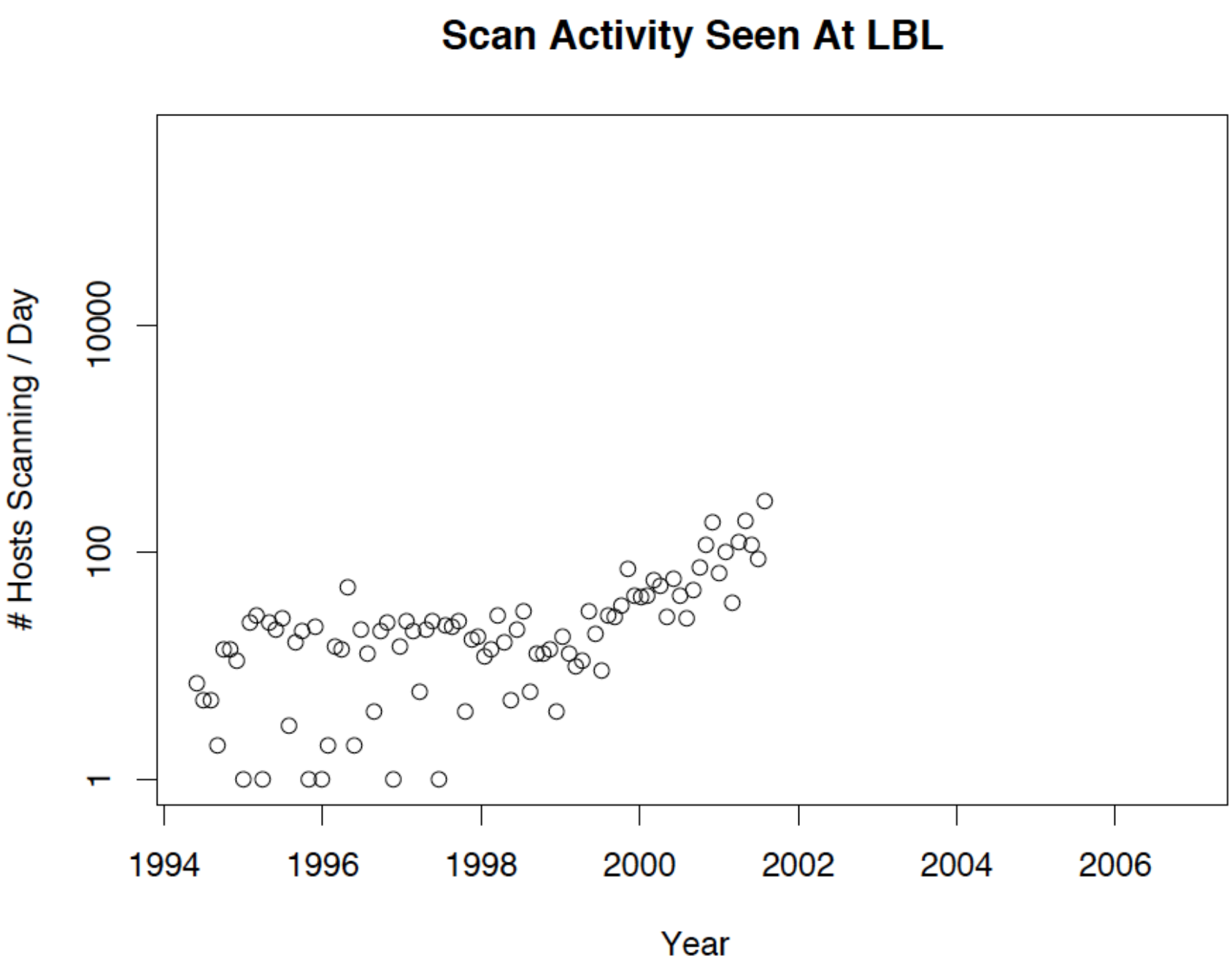
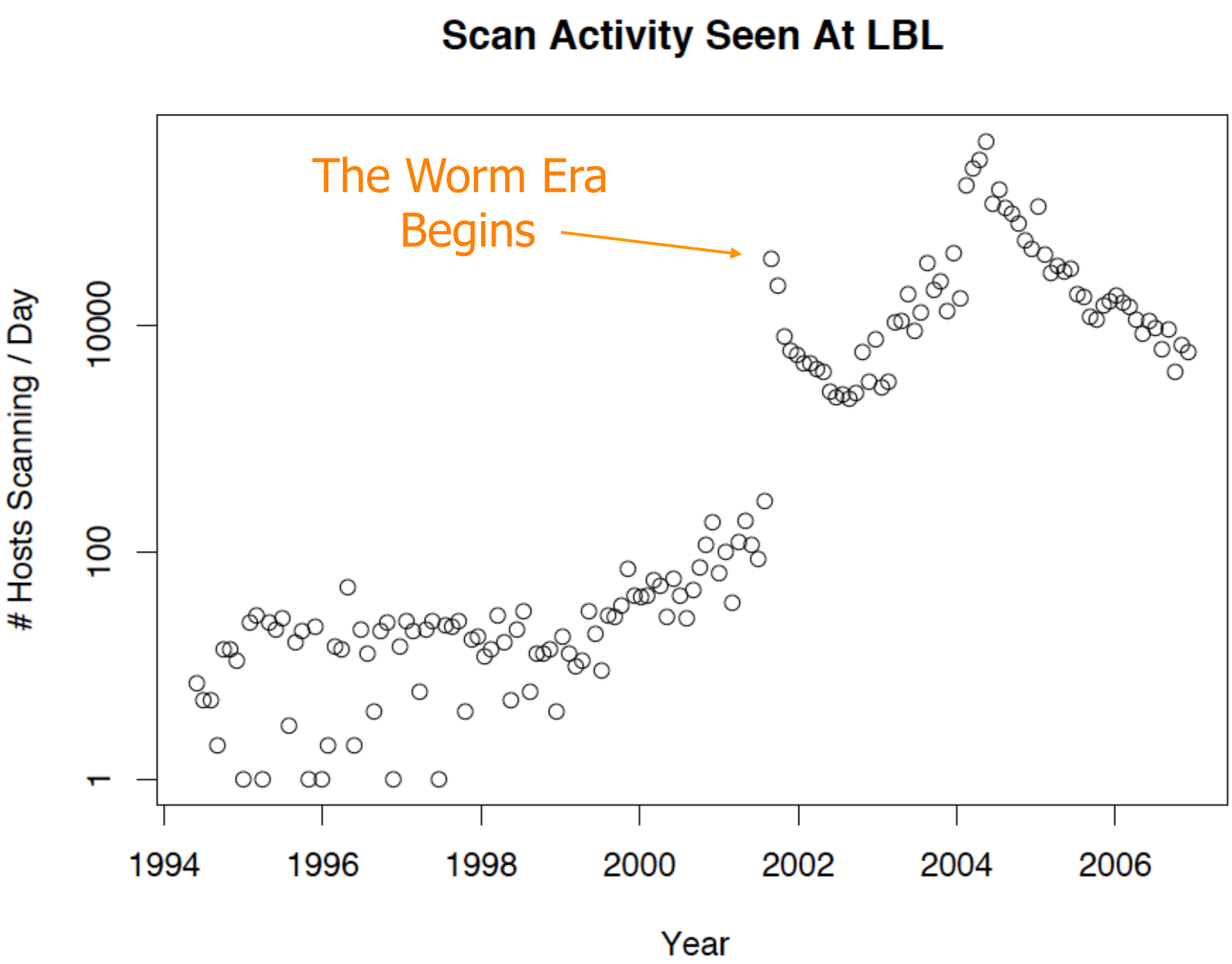
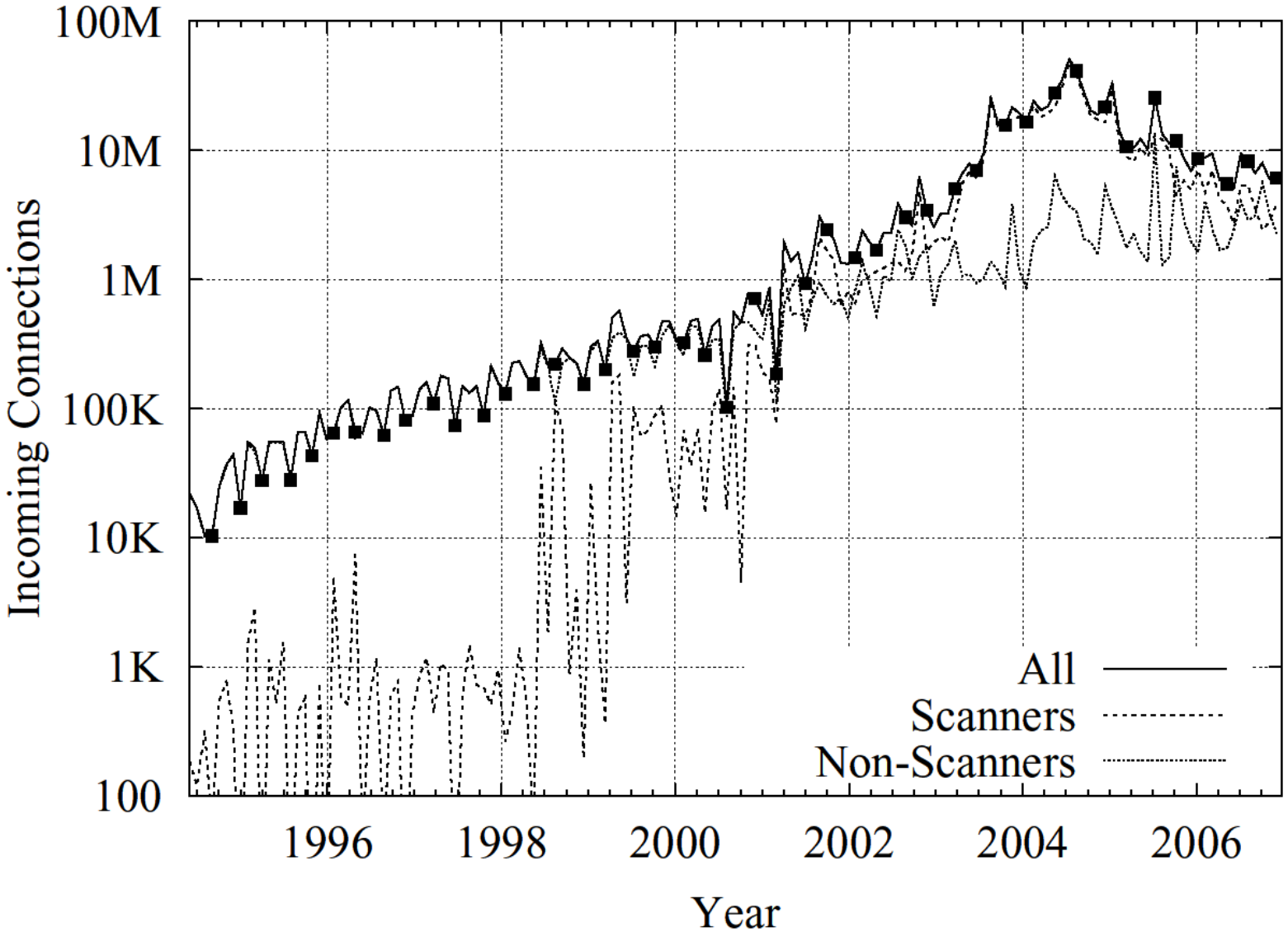
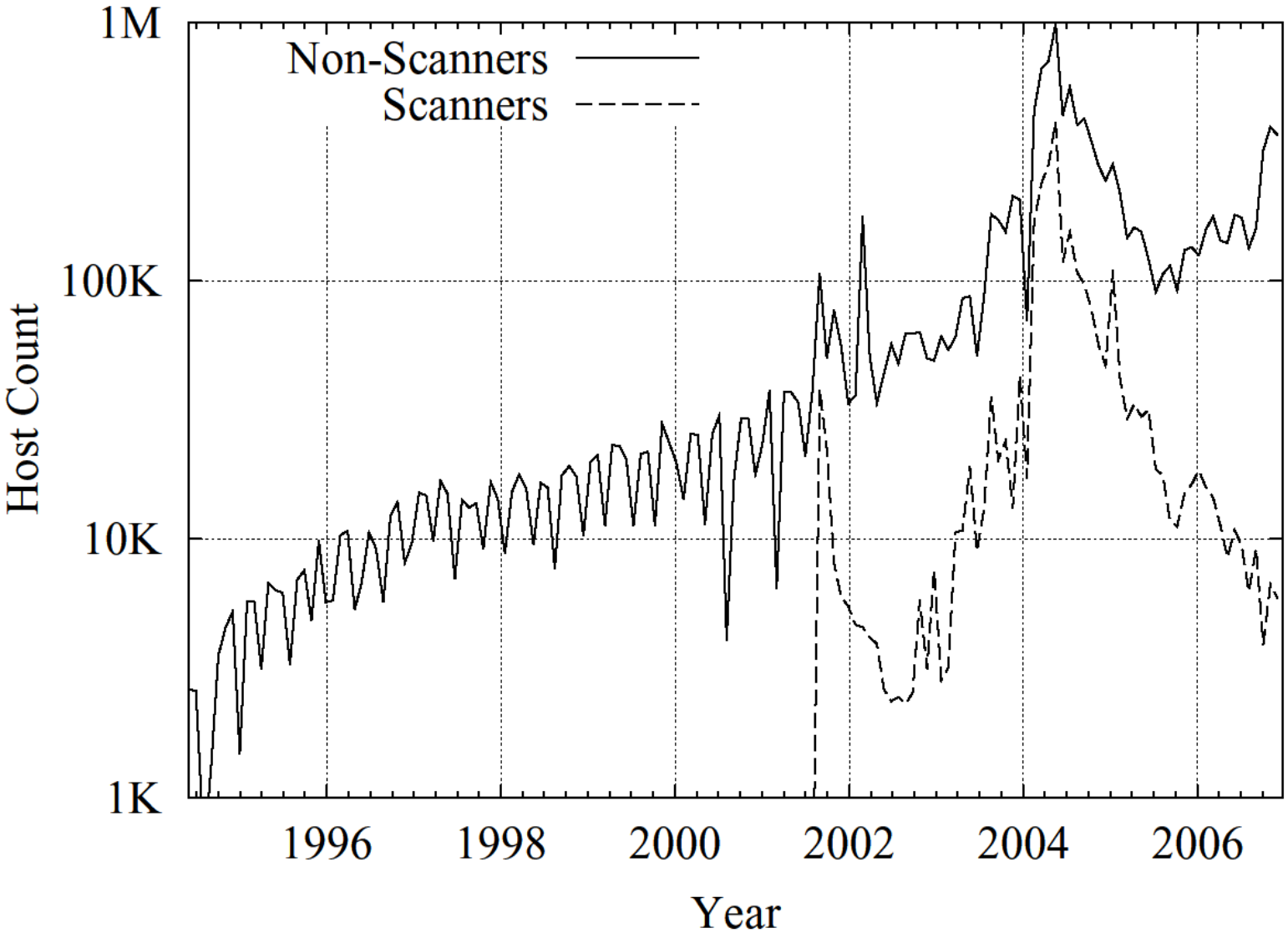

Scan Activity Seen At LBL
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year


Scan Activity Seen At LBL
The Worm Era
Begins
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year

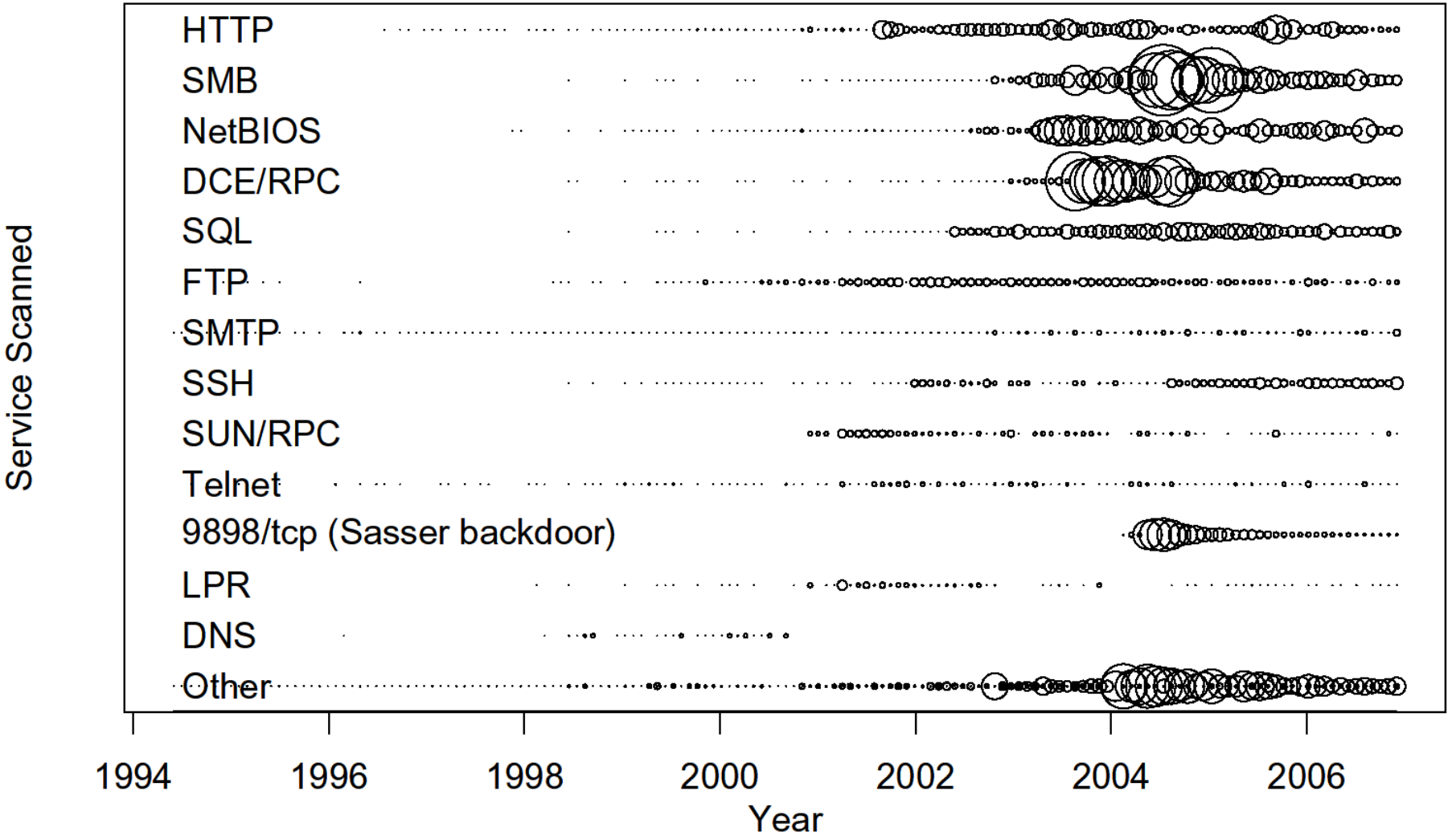
Scanning Activity Seen @ LBNL

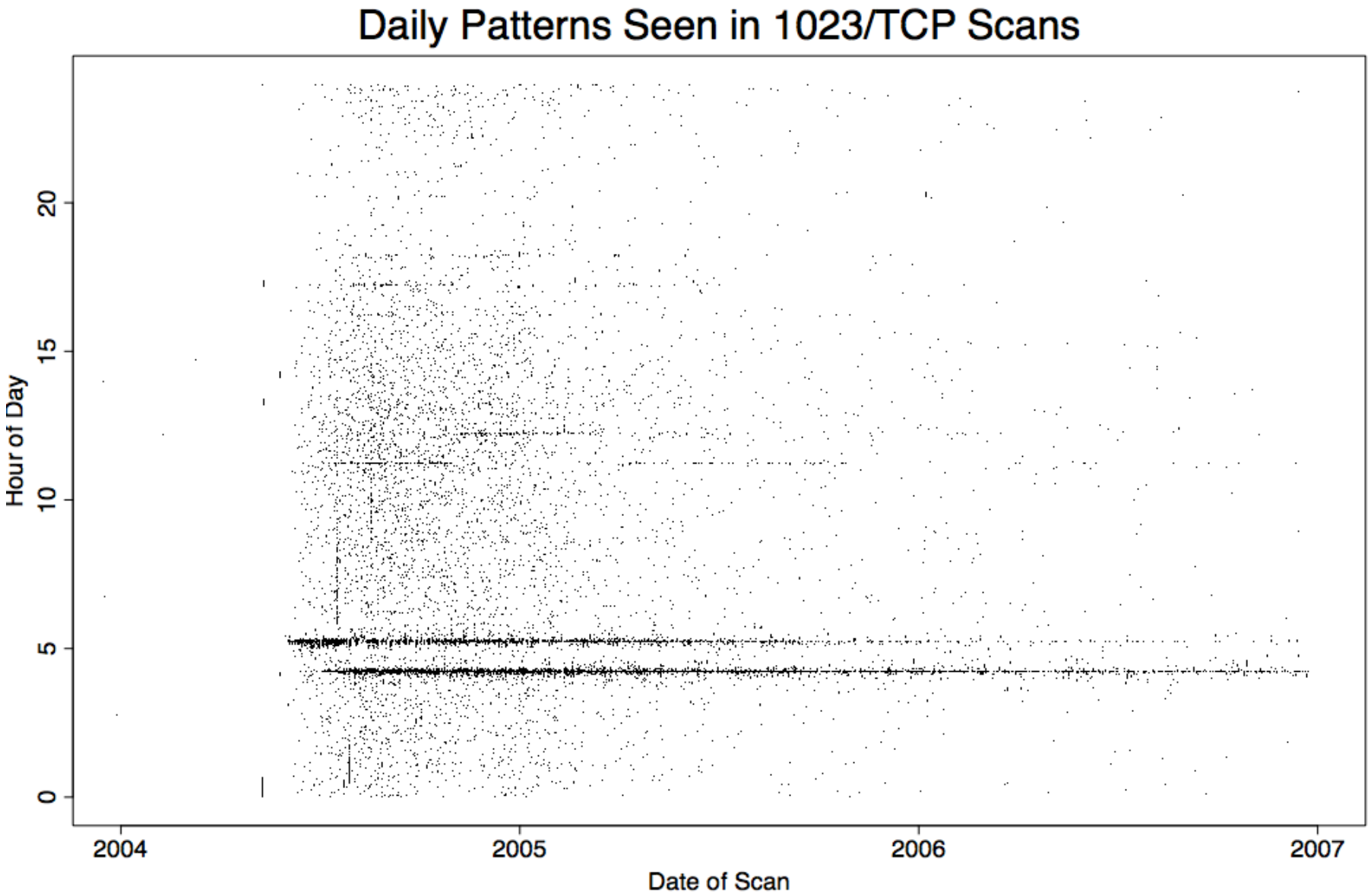


Scanning Hosts Seen @ LBNL

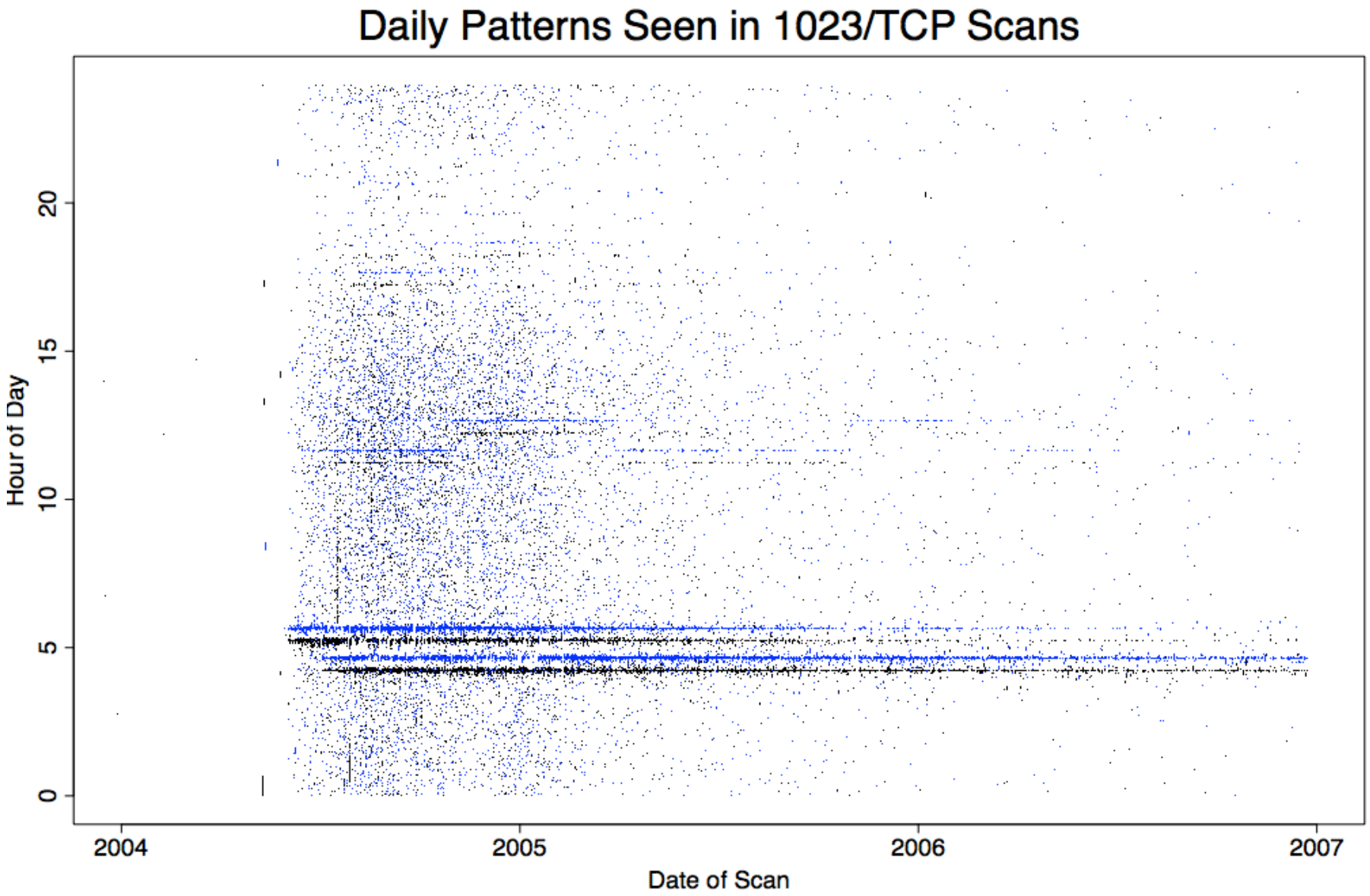


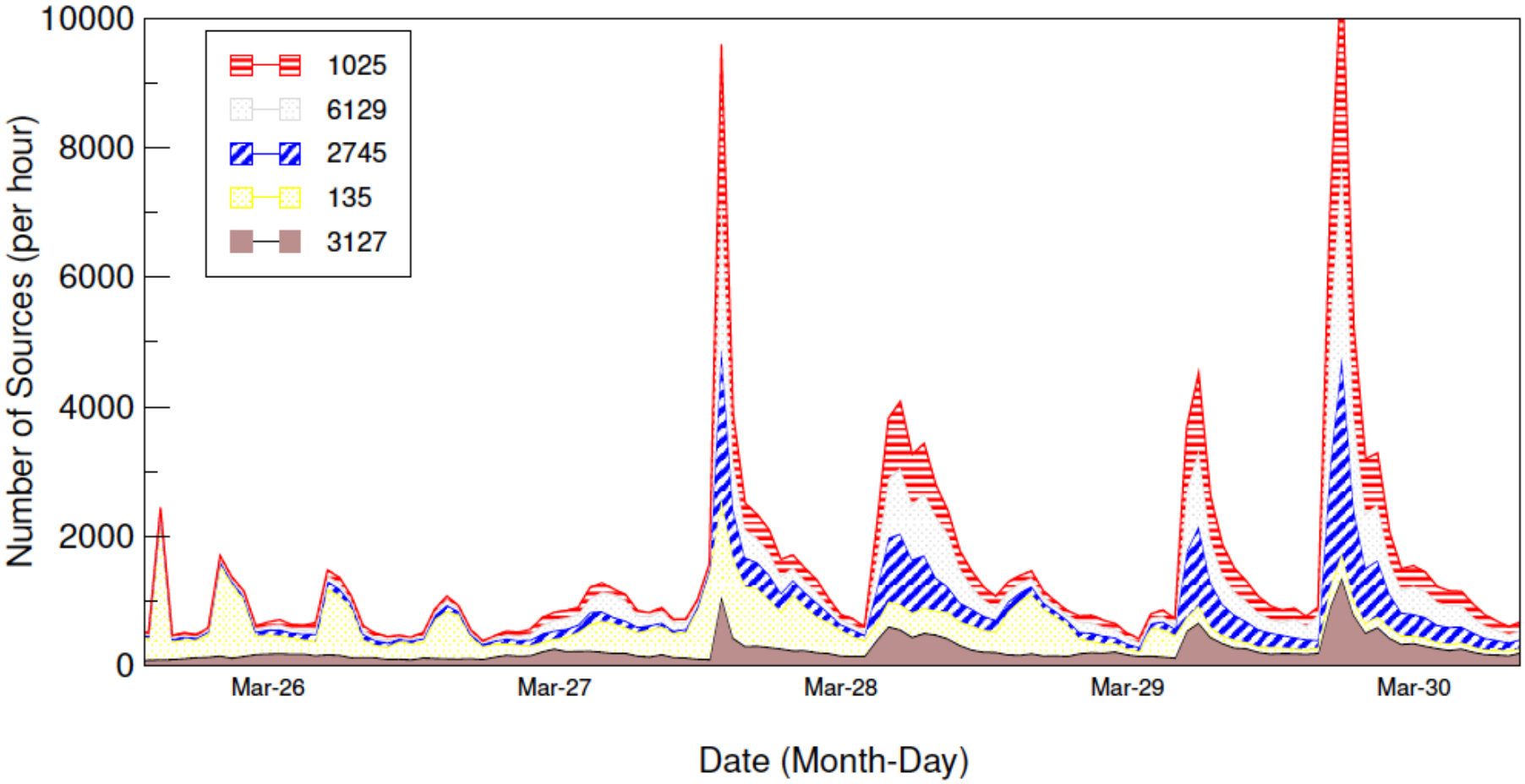
Services Scanned Over Time



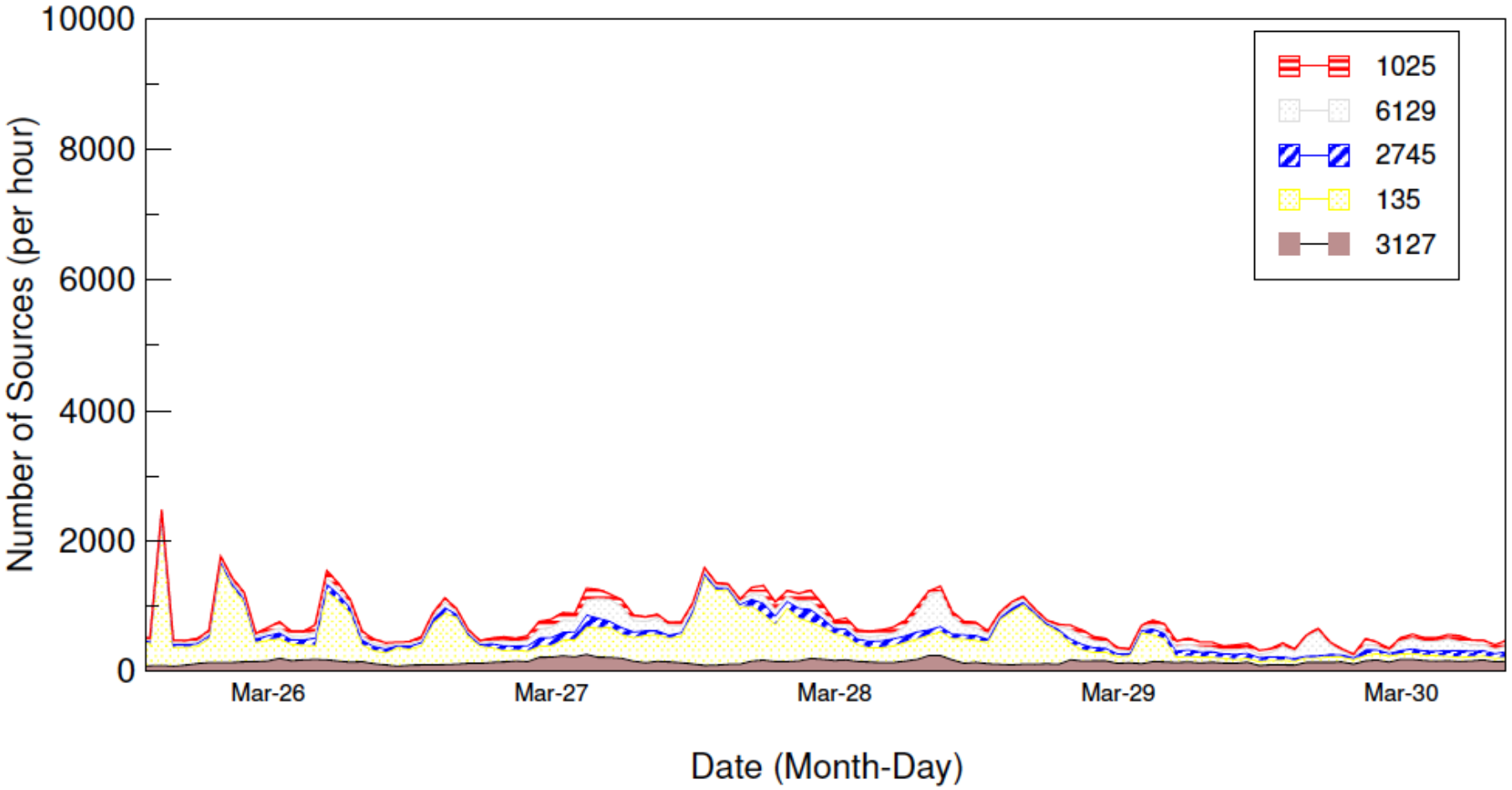


/16 at LBL, sampled 1-in-1K

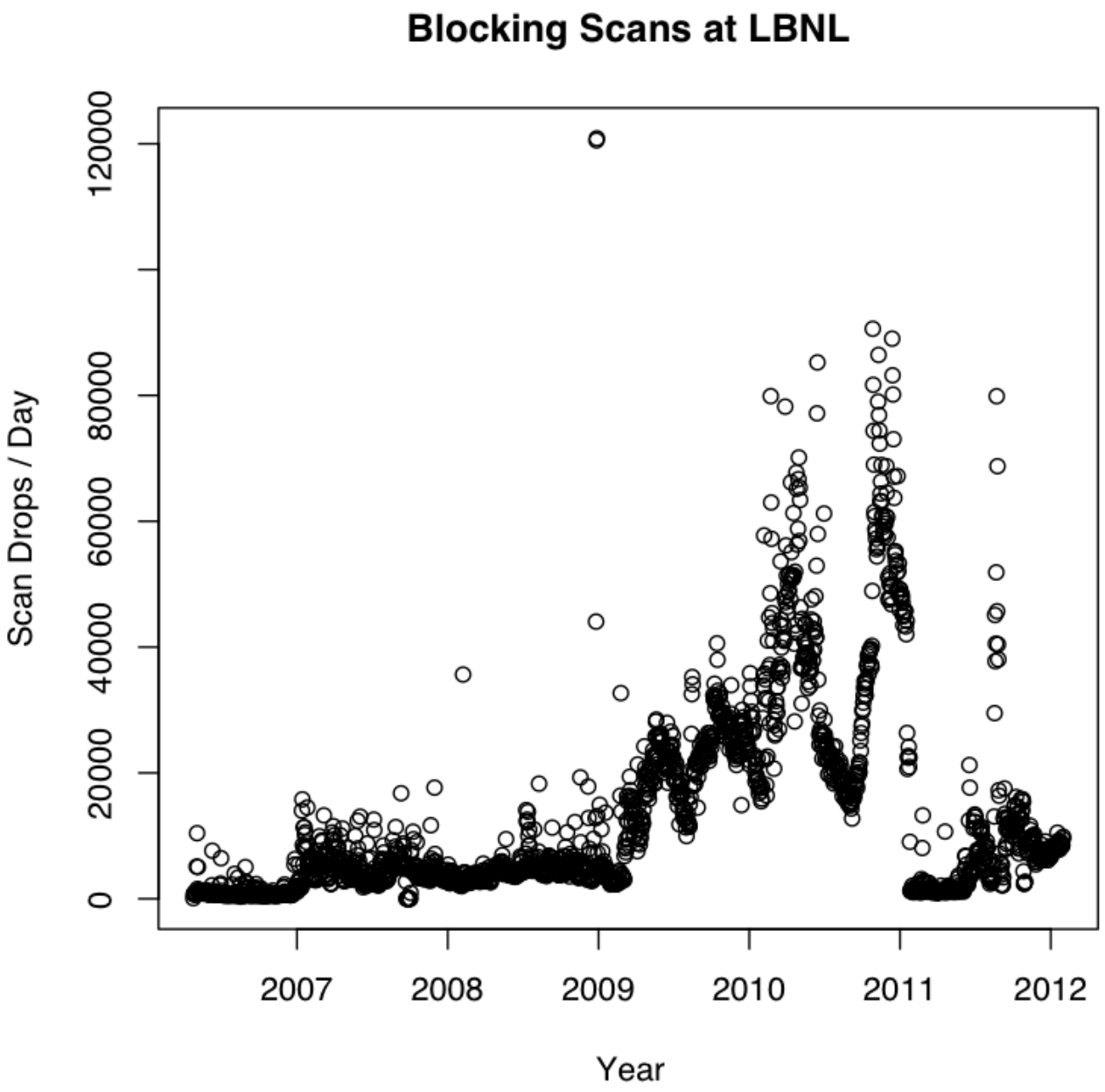

Daily Patterns Seen in 1023/TCP Scans
Hour of Day
0
5
10
15
20
2004
2005
2006
2007
Date of Scan
/16 at LBL, sampled 1-in-1K
2nd /16, sampled 1-in-1K

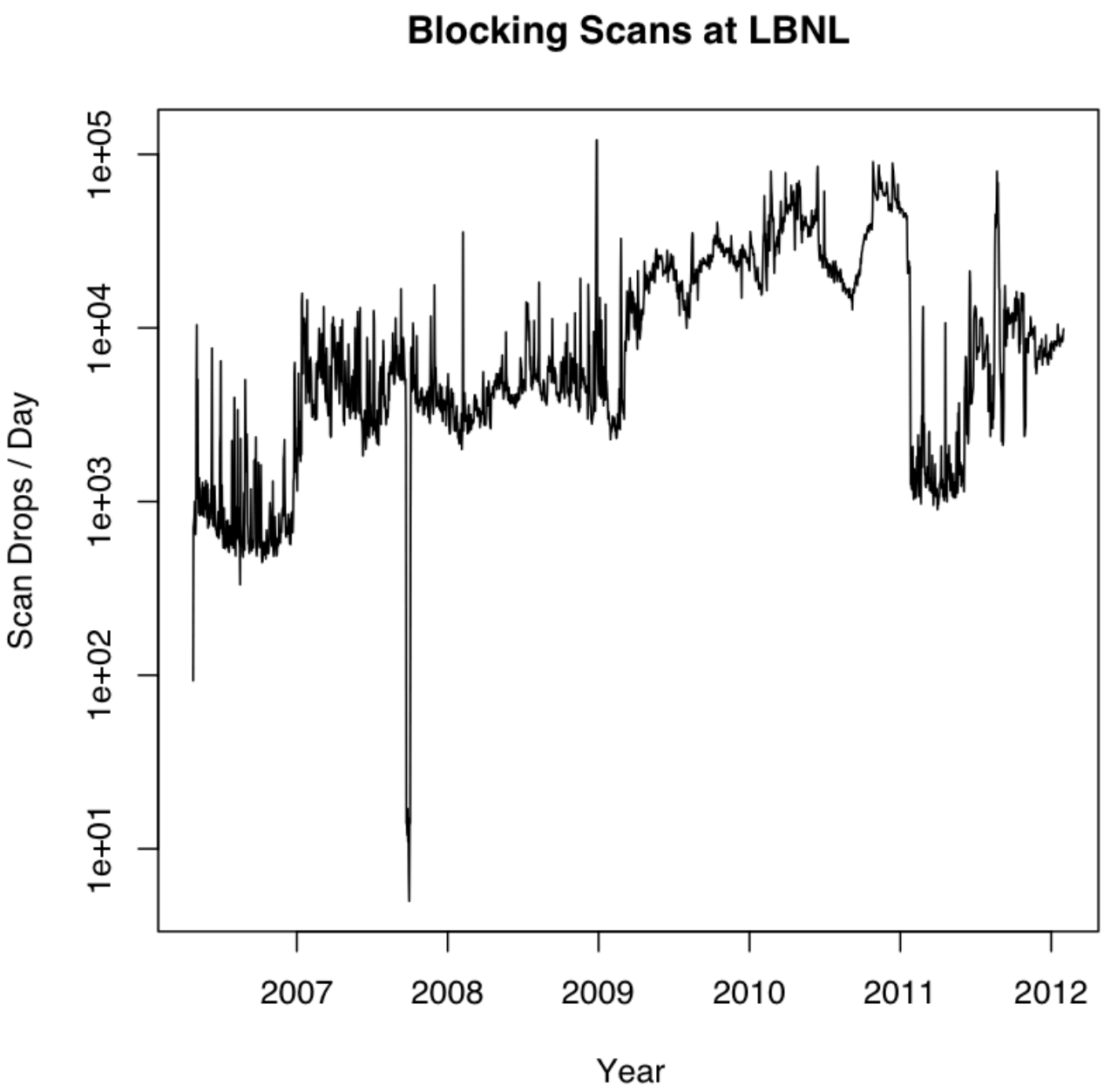


(a) Agobot Sources: UW I

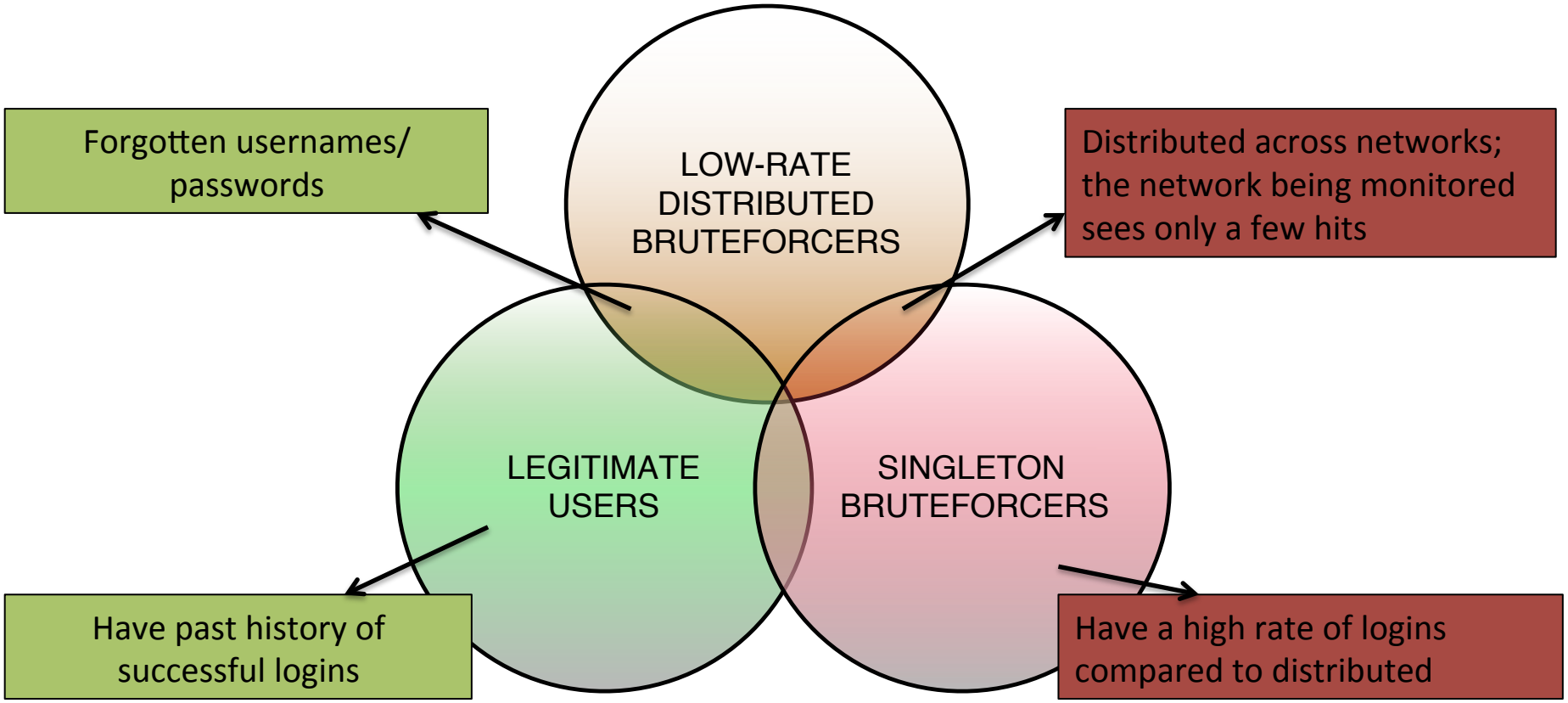


(b) Agobot Sources: UW II


Blocking Scans at LBNL
Scan Drops / Day
0
20000
40000
60000
80000
120000
2007
2008
2009
2010
2011
2012
Year


Blocking Scans at LBNL
Scan Drops / Day
1e+01
1e+02
1e+03
1e+04
1e+05
2007
2008
2009
2010
2011
2012
Year

User Populations



Characteristics overlap of legitimate users and bruteforcers

Dataset

- SSH *syslog* login records collected at Lawrence Berkeley National Laboratory (LBNL)
  - LBNL has two /16 address blocks

Time Span	Jan 2005 – Dec 2012
SSH servers	2,243
Valid users	4,364
Mean daily password login attempts	486 ($\sigma \approx 183$)
Mean daily users	116 ($\sigma \approx 32$)
Total attempts using passwords	5.3M (1/4 successes)

Excludes: Key-based logins and readily detectable high-rate brute-forcers.

- Complemented by SSH flow data

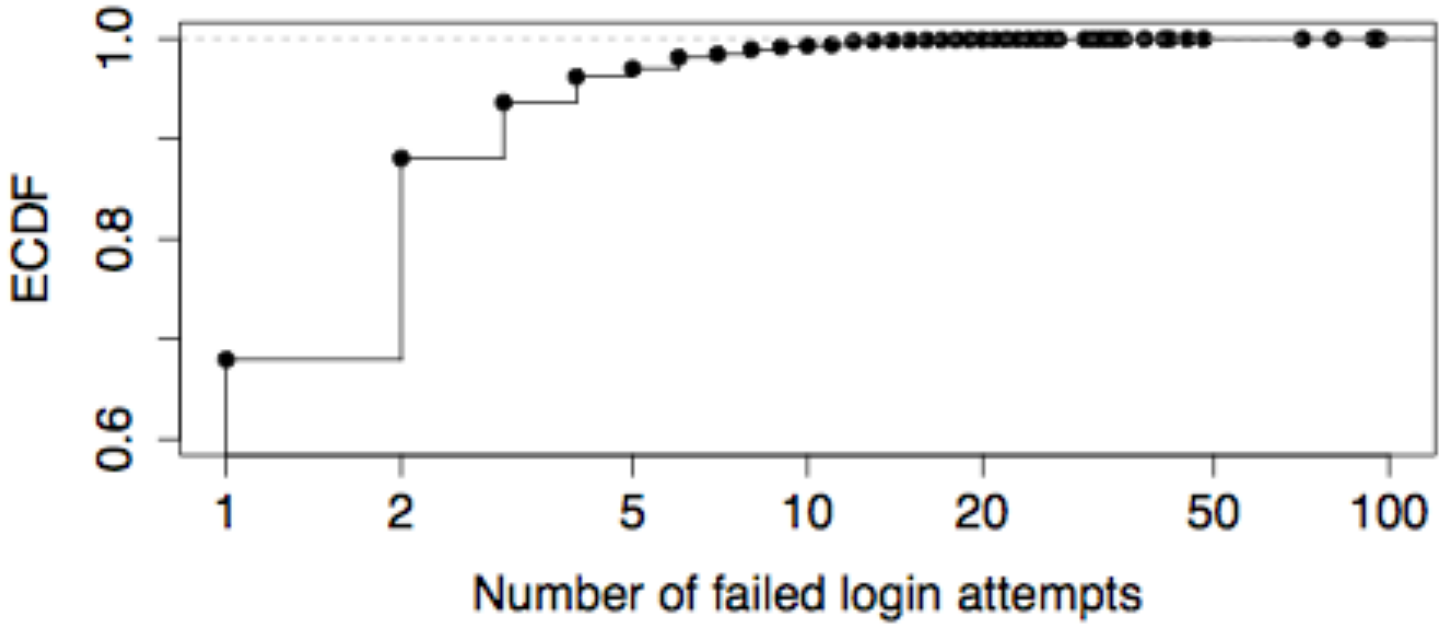


Figure 1: Empirical CDF of the number of failed login attempts per hour until a success for legitimate user login efforts with forgotten or mistyped usernames/passwords.

Aggregate Site Analyzer

Site-wide parameter: Global Failure Indicator (GFI)

- Site-wide # of failed logins per batch of x logins