How much did shutting down McColo help ?

Richard Clayton

CEAS, Mountain View

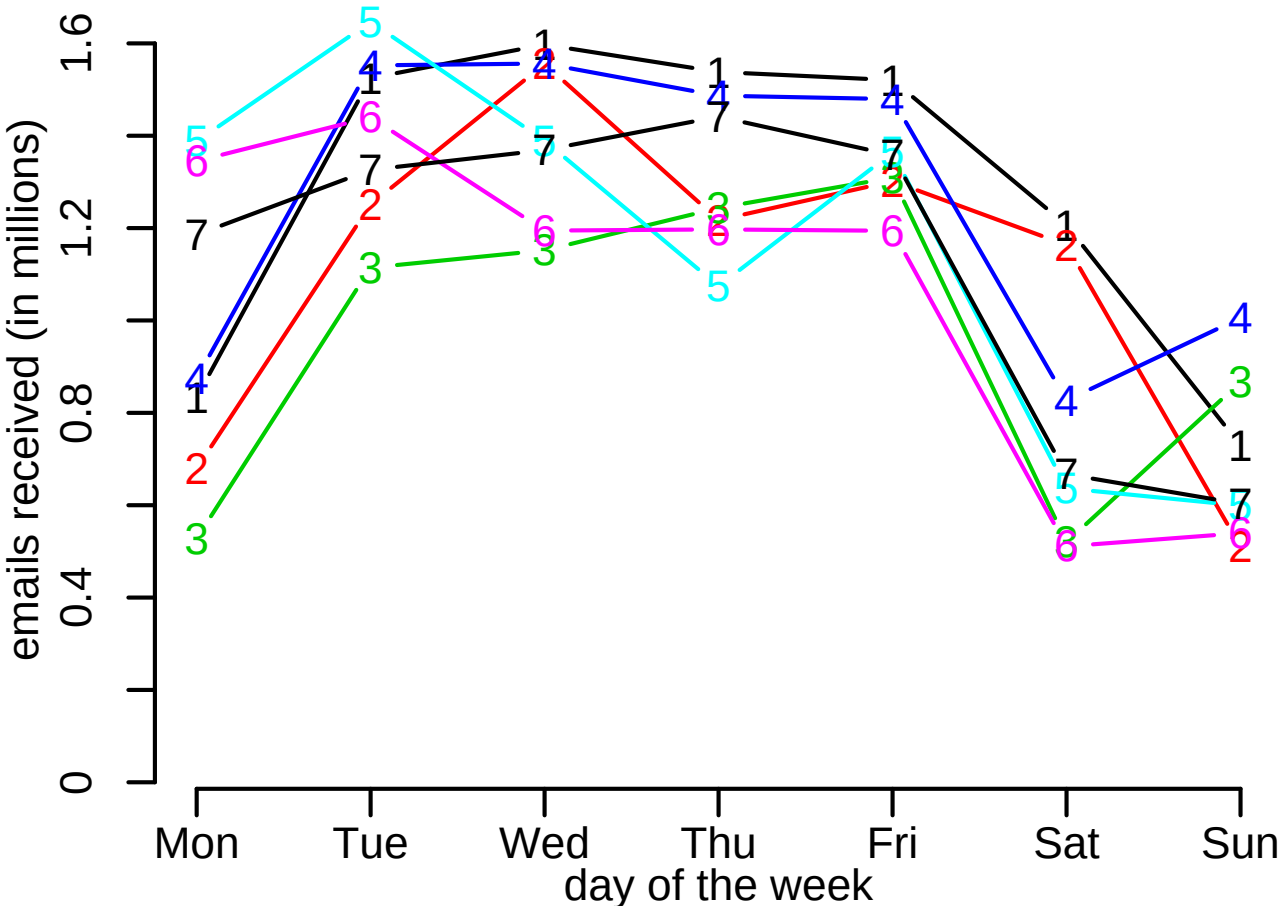
16th July 2009

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

McColo Disconnection

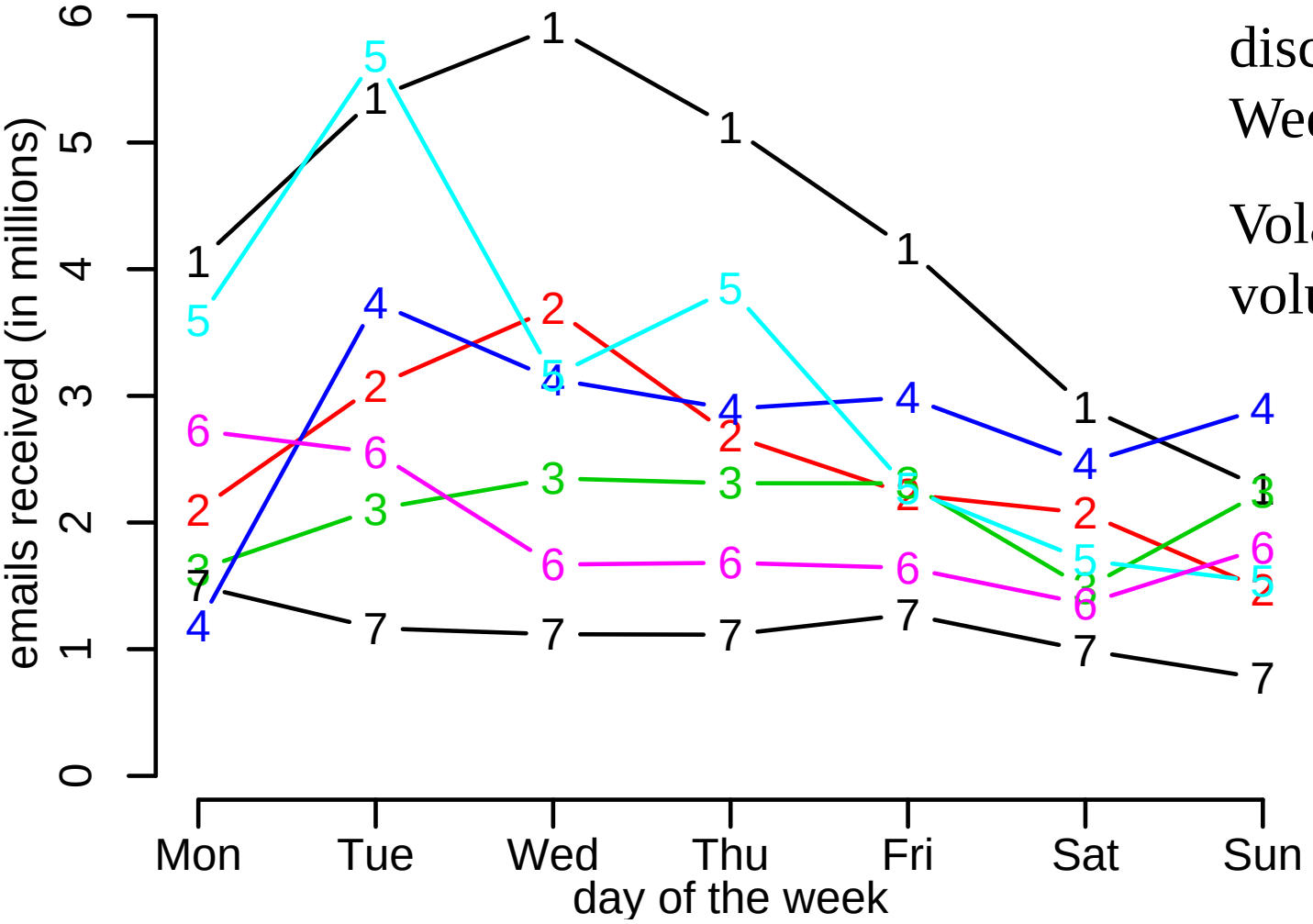
- McColo disconnected Tue 11 Nov 2008
- Took 6 major botnet controllers offline
- Reports suggested spam dropped by 2/3rds
- BUT was this “hard to block spam”
  - we all cheer!
- OR maybe it was “easy to block spam”
  - we all yawn

Dataset



- Seven weeks of email data
- Medium-sized UK ISP with *c.*150K customers
- Fairly consistent pattern of non-spam email (except Mondays)

Total spam volume

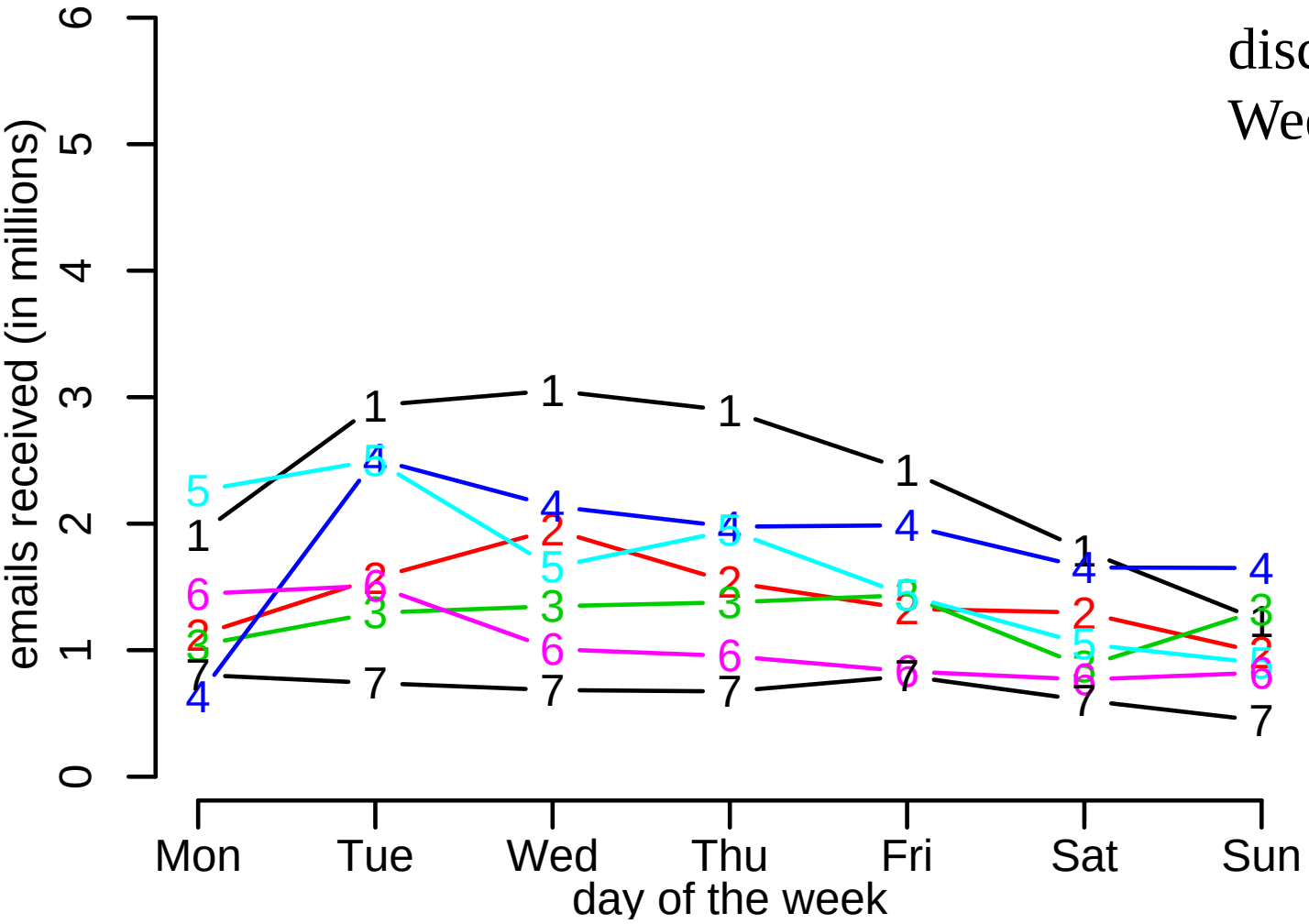


McColo was disconnected Week 6 (Tue)

Volatility and volume reduce

Spam removed by filters

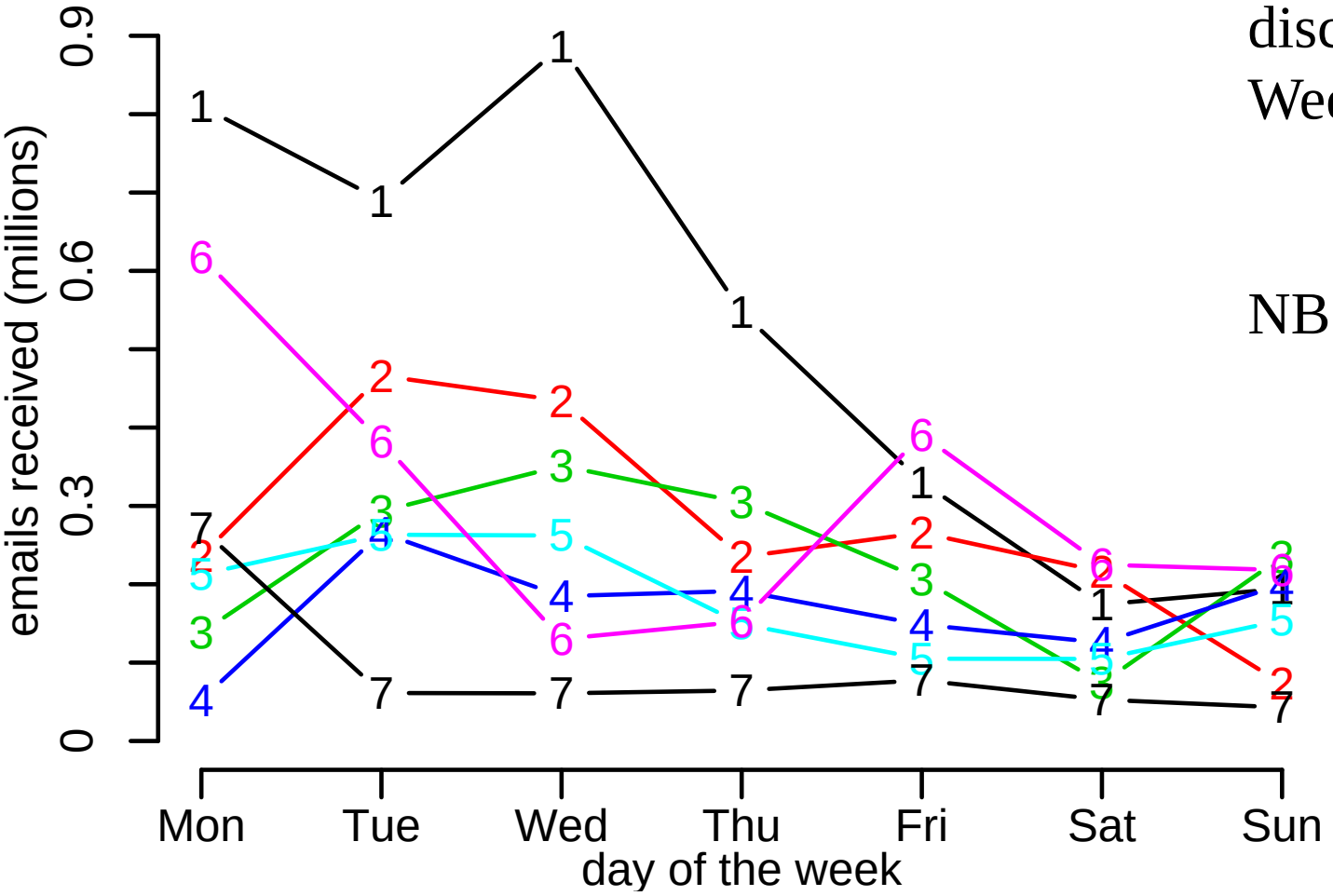
McColo was disconnected Week 6 (Tue)



Impact on filter usage

- Filters are an expensive way to block spam
- Before disconnection 32% to 56% of spam could be dealt with prior to the filters
- After disconnection a more consistent 43% could be dealt with prior to the filters (but of course there was less spam overall)

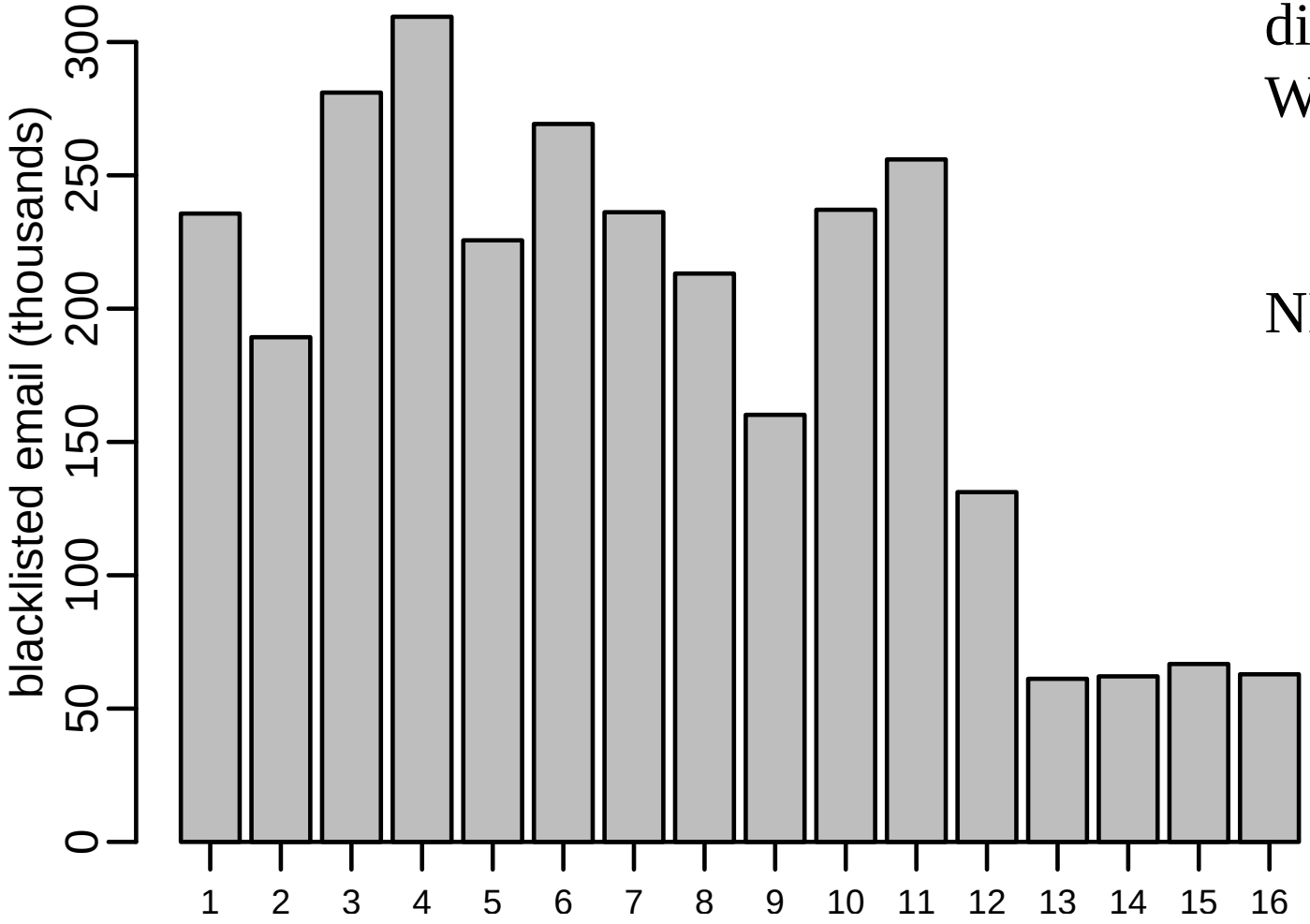
Spam to unknown addresses



McColo was disconnected Week 6 (Tue)

NB: new scale

Spam from blacklisted IPs



McColo was disconnected Week 6 (Tue)

NB: new scale

Recap

- Non-spam fairly constant
- After disconnection event
  - less volatility and lower overall spam volumes
  - higher (or some days lower) proportion of spam reached content filters
  - “unknown address” rule much less effective
  - blacklisting IPs much less effective
- So disconnection Good, but some ISPs will have been less impressed than others

How much did shutting down McColo help ?

http://www.lightbluetouchpaper.org/