Blackholing at IXPs

On the Effectiveness of DDoS Mitigation in the Wild

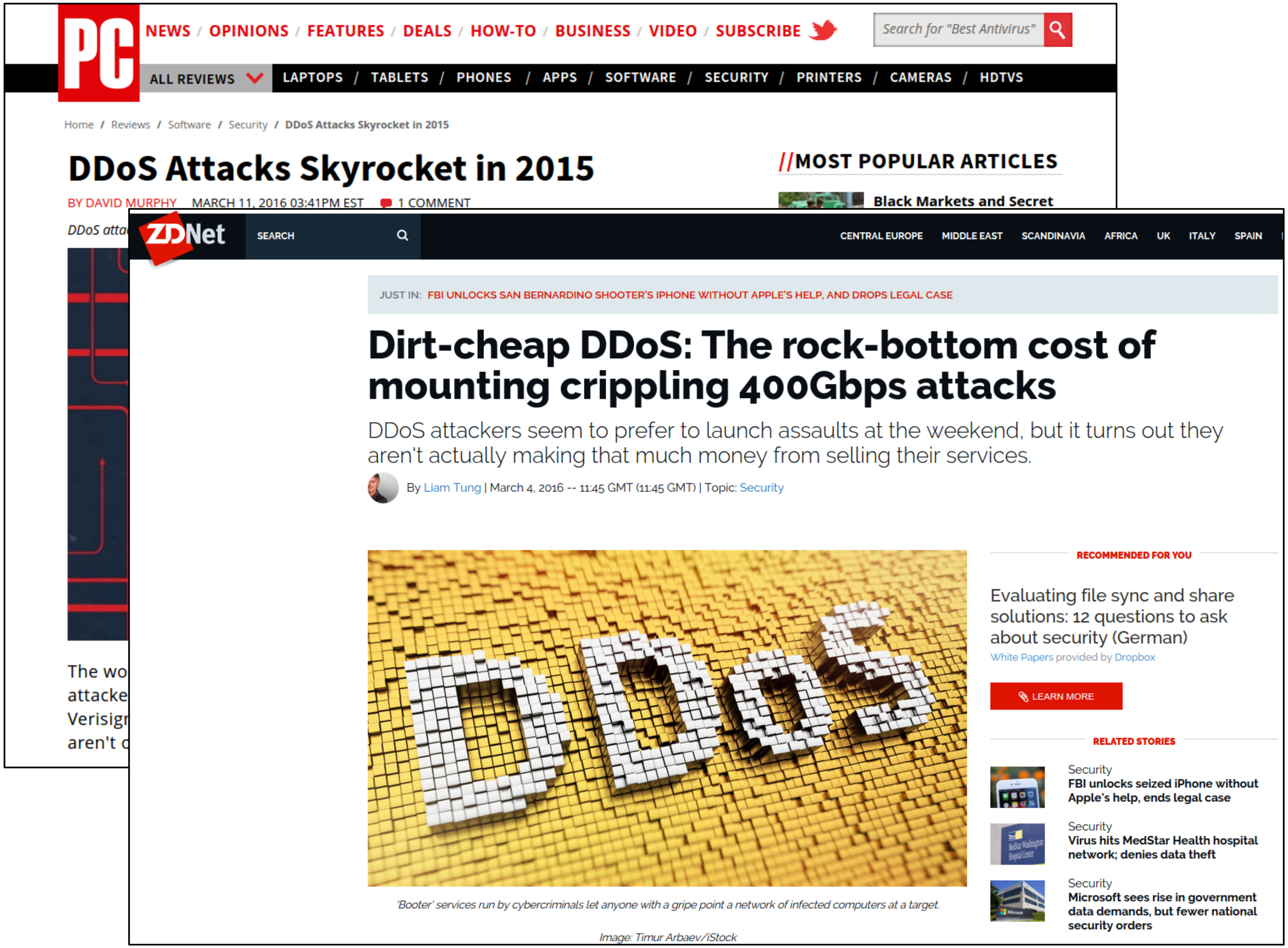
NANOG 67

Christoph Dietzel [1,2], Anja Feldmann [1], Thomas King [2]

[1] INET, TU Berlin

[2] R&D, DE-CIX

DDoS Attacks Remain a Serious Threat



PC
NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / VIDEO / SUBSCRIBE
Search for "Best Antivirus"
ALL REVIEWS
LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY / PRINTERS / CAMERAS / HDTVS
Home / Reviews / Software / Security / DDoS Attacks Skyrocket in 2015

DDoS Attacks Skyrocket in 2015

BY DAVID MURPHY   MARCH 11, 2016 03:41PM EST   1 COMMENT

DDoS atta

The wo
attacke
Verisign
aren't c

//MOST POPULAR ARTICLES
Black Markets and Secret
ZDNet
SEARCH
CENTRAL EUROPE
MIDDLE EAST
SCANDINAVIA
AFRICA
UK
ITALY
SPAIN

JUST IN: FBI UNLOCKS SAN BERNARDINO SHOOTER'S IPHONE WITHOUT APPLE'S HELP, AND DROPS LEGAL CASE

Dirt-cheap DDoS: The rock-bottom cost of mounting crippling 400Gbps attacks

DDoS attackers seem to prefer to launch assaults at the weekend, but it turns out they aren't actually making that much money from selling their services.

By Liam Tung | March 4, 2016 -- 11:45 GMT (11:45 GMT) | Topic: Security

'Booter' services run by cybercriminals let anyone with a gripe point a network of infected computers at a target.

Image: Timur Arbaev/iStock

RECOMMENDED FOR YOU

Evaluating file sync and share solutions: 12 questions to ask about security (German)

White Papers provided by Dropbox

RELATED STORIES

Security
FBI unlocks seized iPhone without Apple's help, ends legal case

Security
Virus hits MedStar Health hospital network; denies data theft

Security
Microsoft sees rise in government data demands, but fewer national security orders

What is Blackholing?

» Operational technique to counter DDoS attacks

» Triggered directly by IP owners through BGP

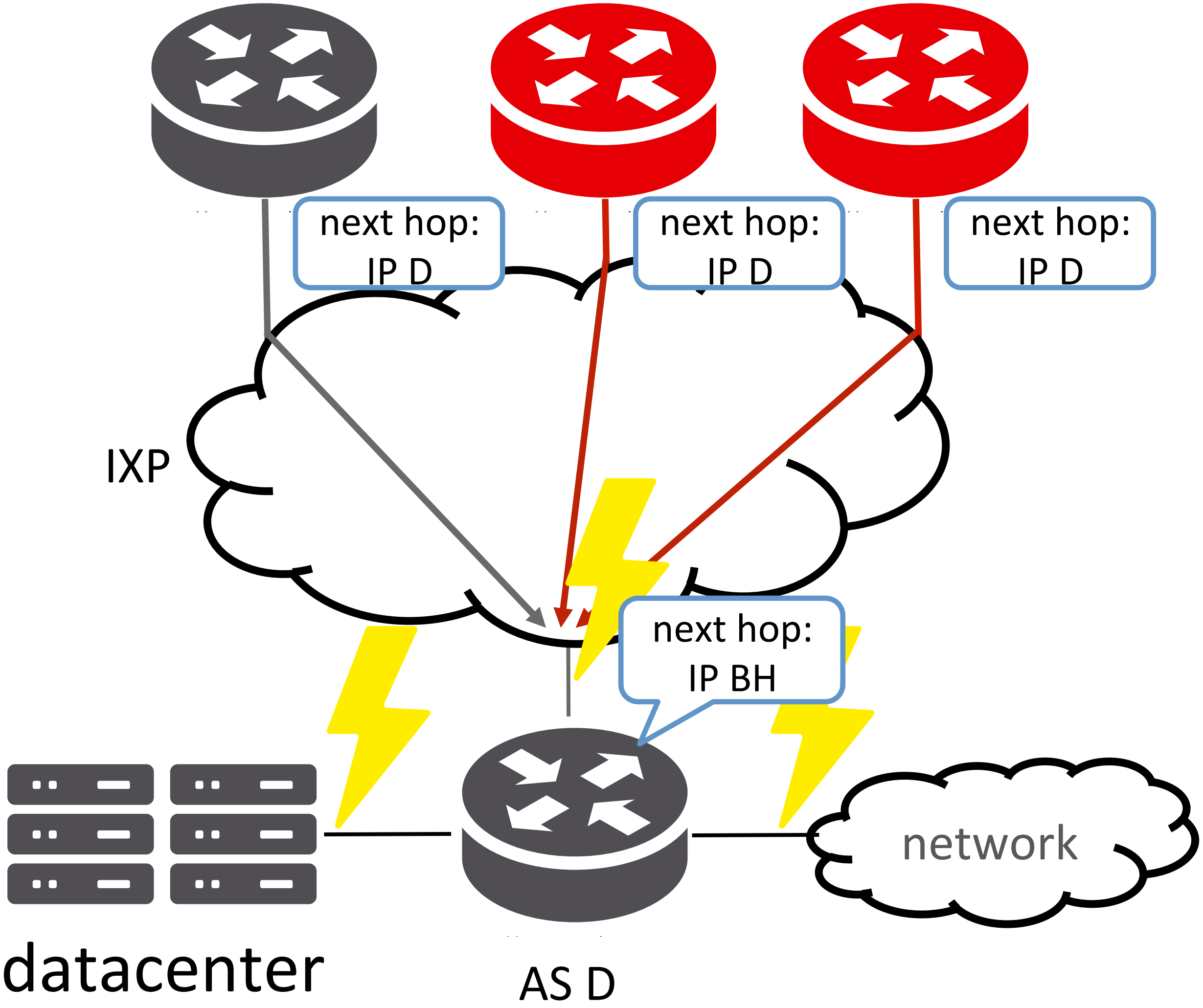
» Last resort to protect upstream/peering link or own network

» Since a few years also at IXPs (DE-CIX, MSK-IX, NETIX, NIX-CZ, …)

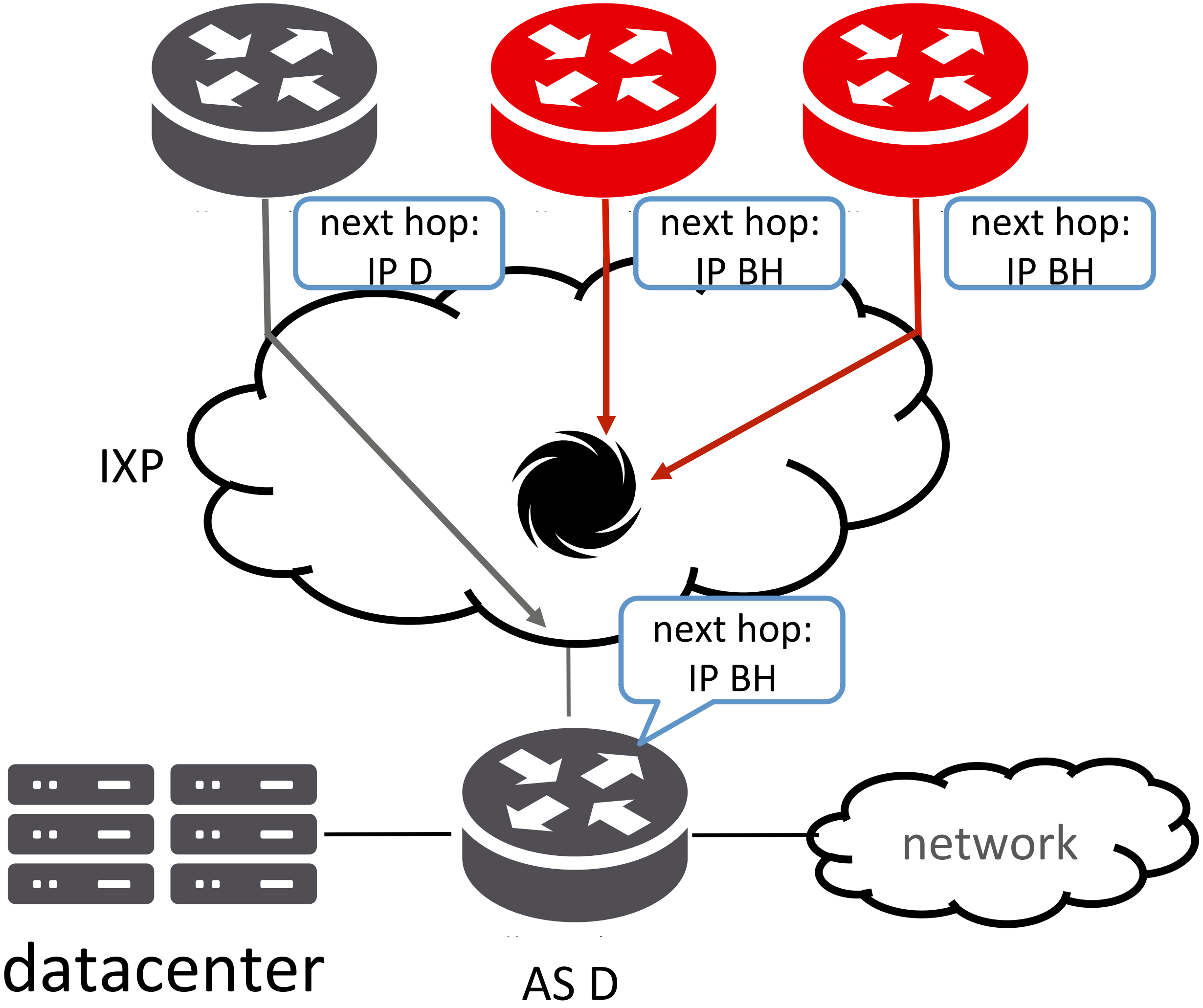
Blackholing – Brief History

- Late 1980s: used on a per device basis
- 2002: within ASes
- 2005 – 2007: major ISPs offer blackholing as a service
- **2010: First IXPs adopt the concept**

Recap – Blackholing at IXPs



Recap – Blackholing at IXPs

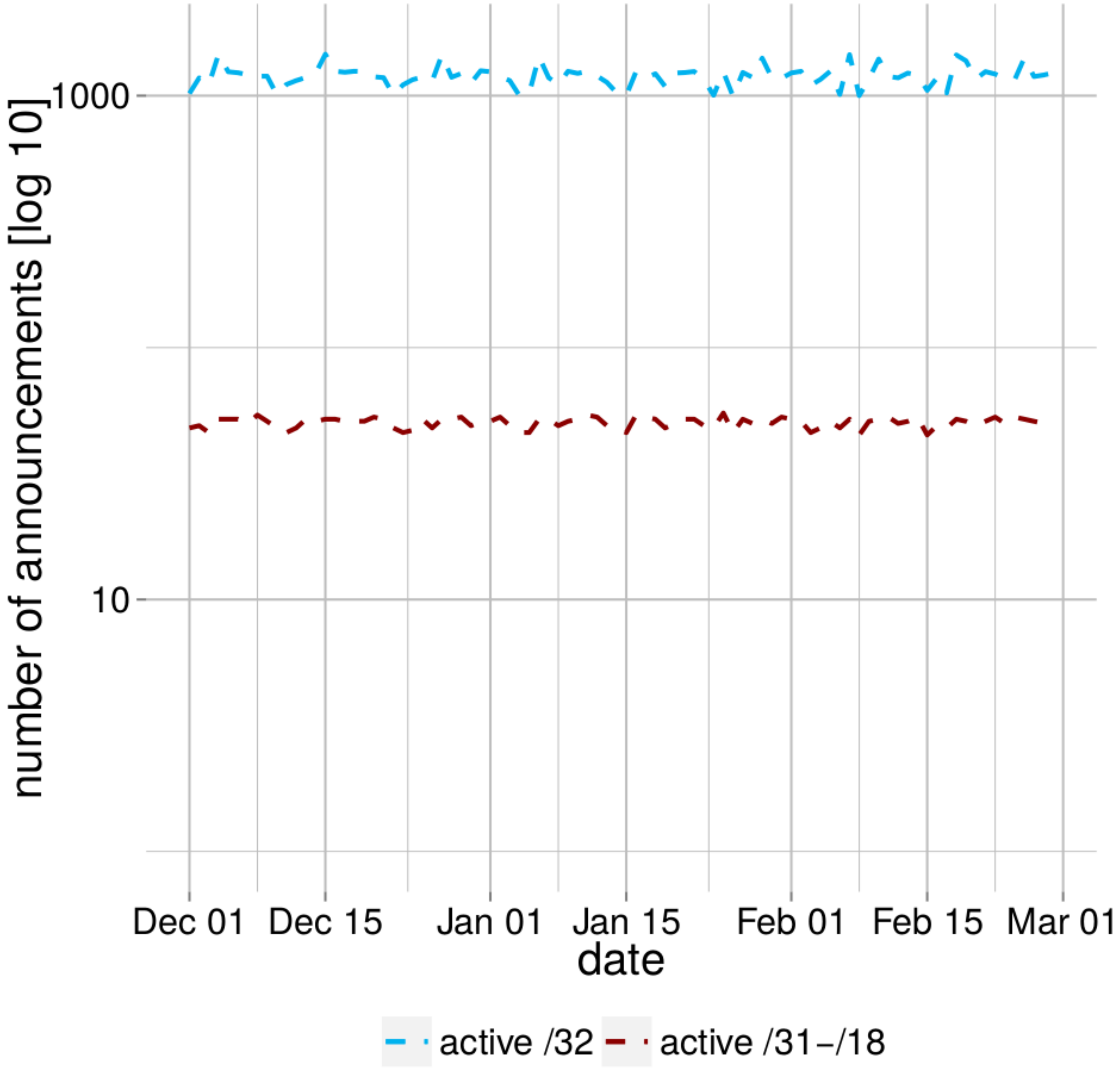


Is it frequently used and how is it used?

What is the impact on traffic?

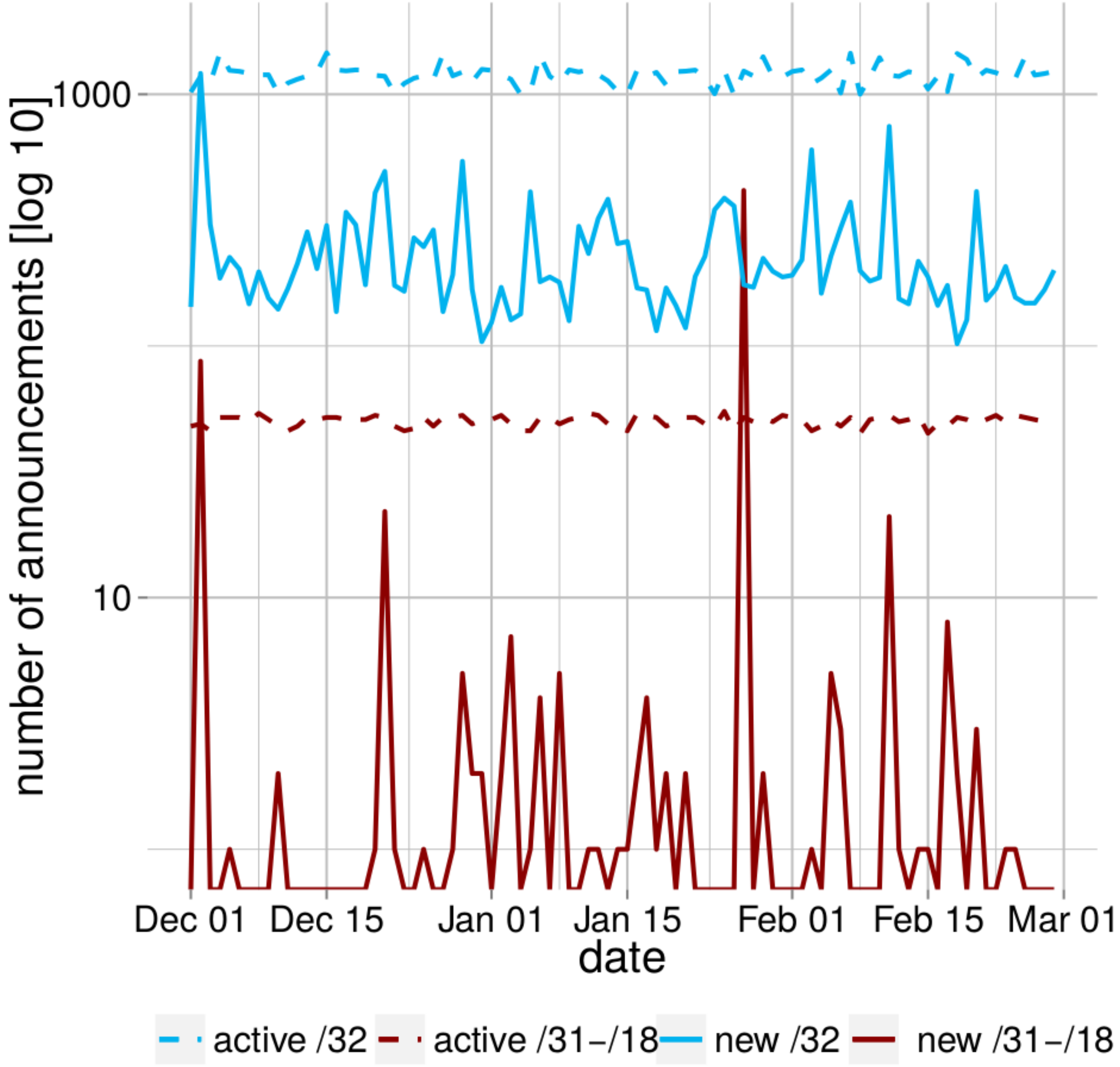
How can we improve blackholing?

Blackholing Usage Analysis – Active Announcements



- About 23,000 announcements
- Stable number of active /32 blackholes (~1200)
- Also stable number of less specifics /31 - /18 (~50)
- **What about new announcements?**

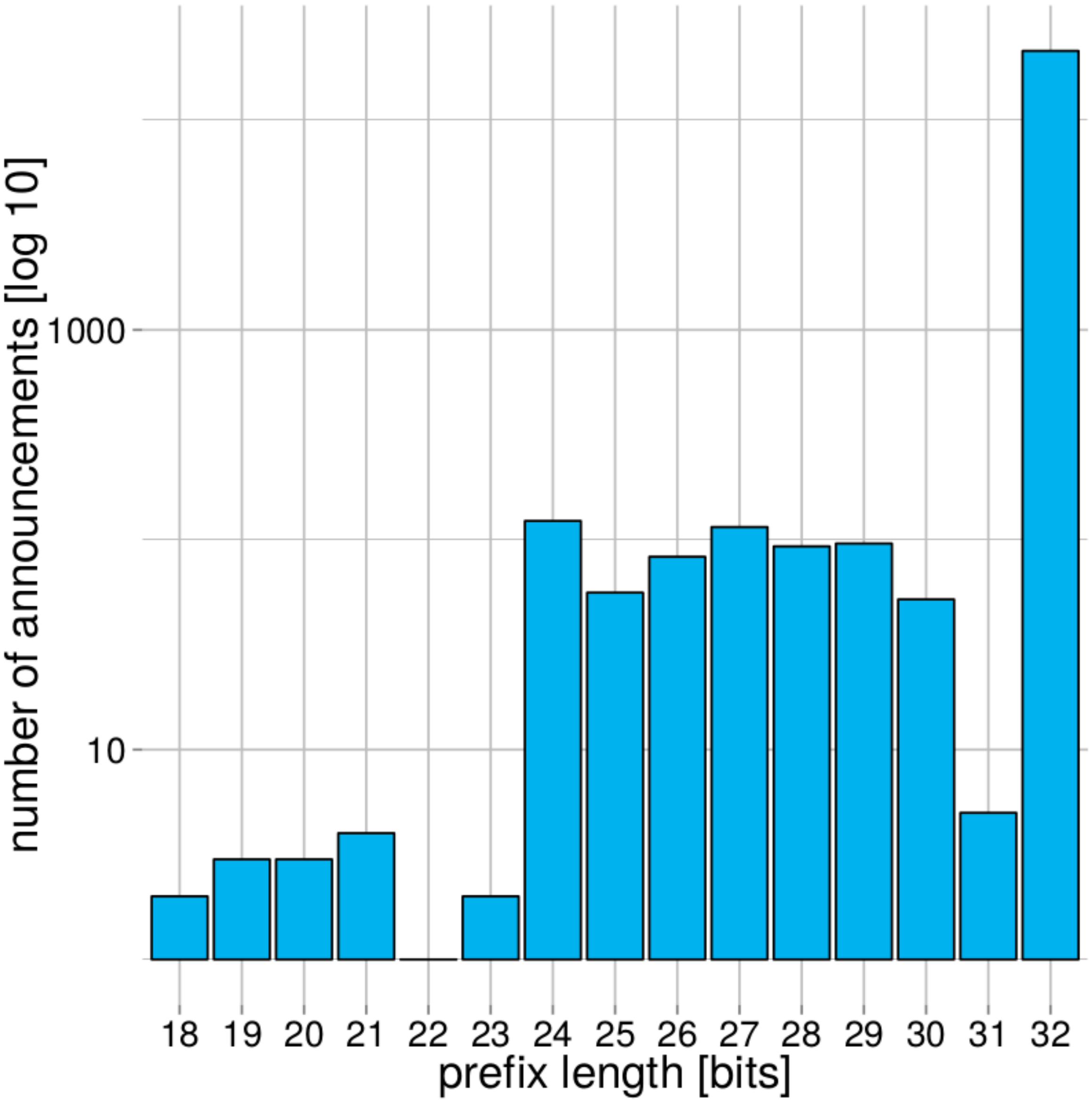
Blackholing Usage Analysis – New Announcements



- High variance in new announcements
- Spikey less specifics (/31 - /18)
- Blackholing is indeed widely used!
- **But which prefix sizes?**

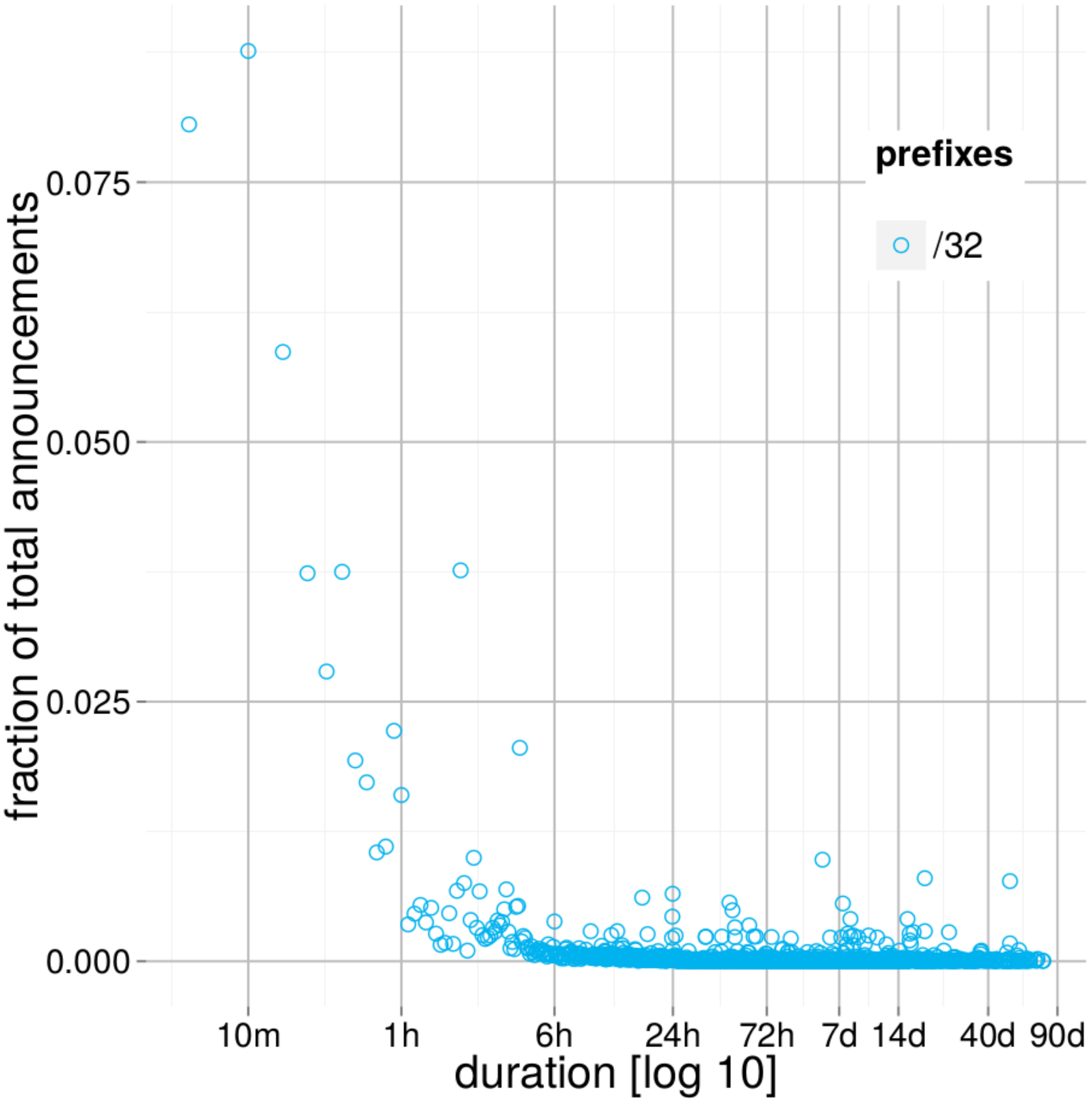
Blackholing Usage Analysis – Prefix Length

- Mainly /32 announcements (97%)
- /24 - /31 account for 2.5%
- 9 announcements for < /24
- More specific acceptance needed
- **Announced for how long?**



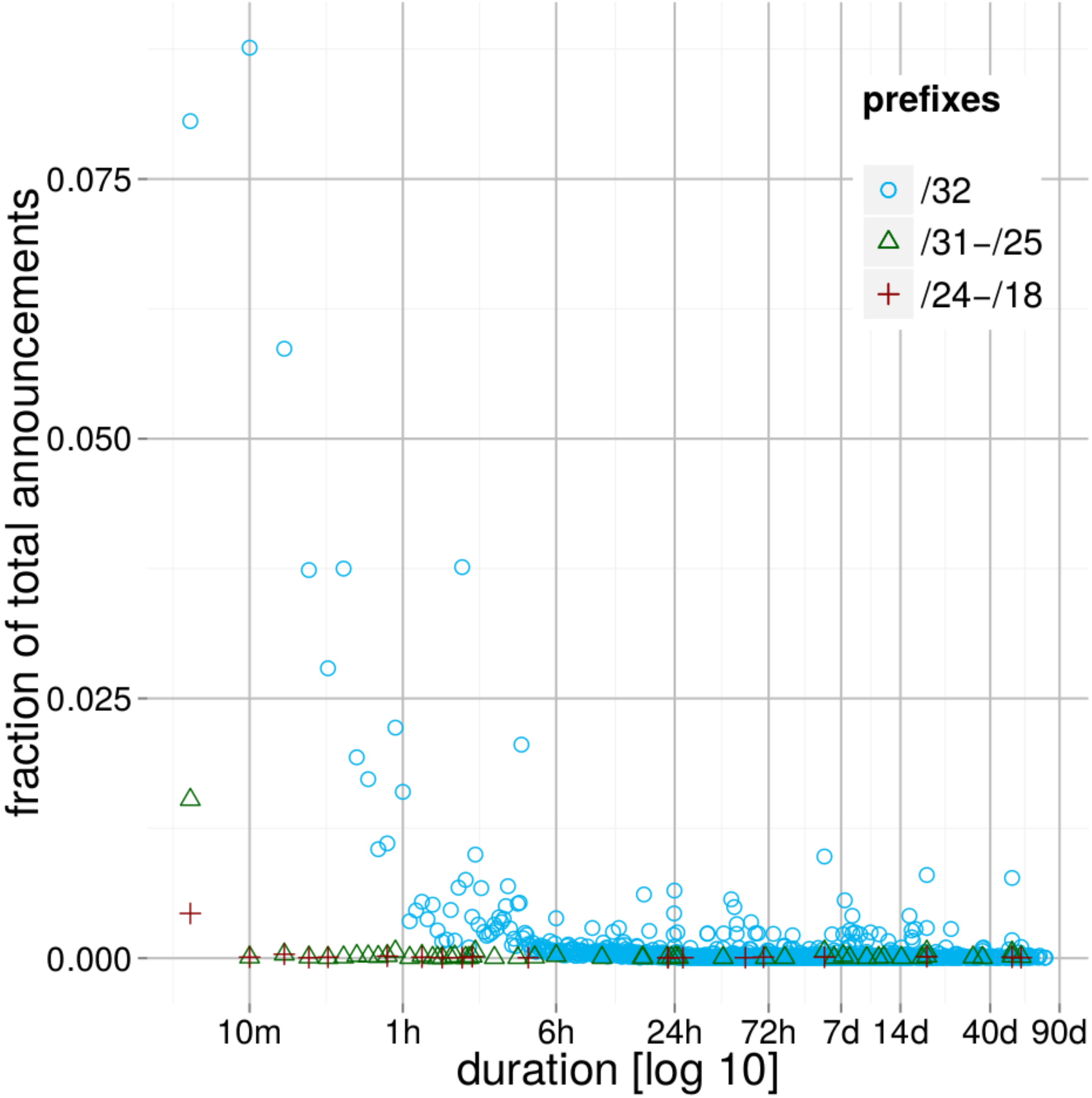
Blackholing Usage Analysis – Active Duration

- Active duration per prefix (/32)
- Majority is short-lived (~50% <= 3 hours)
- Longest observed announcement 76.31 days



Blackholing Usage Analysis – Active Duration

- Majority is short-lived
- Also very long living announcements
- **Could be the same prefix?!**

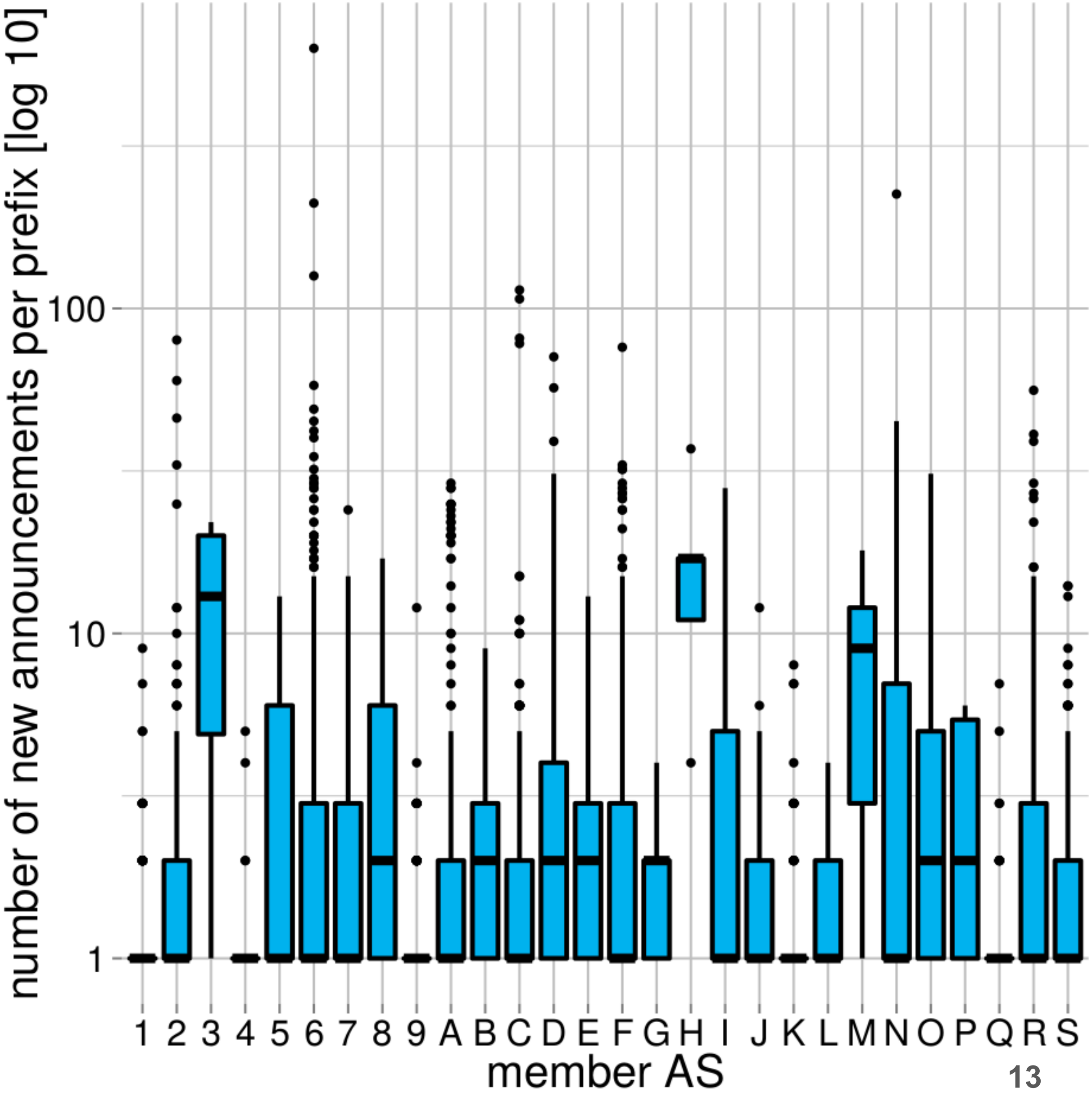


Blackholing Usage Analysis – Re-Announcements per Prefix

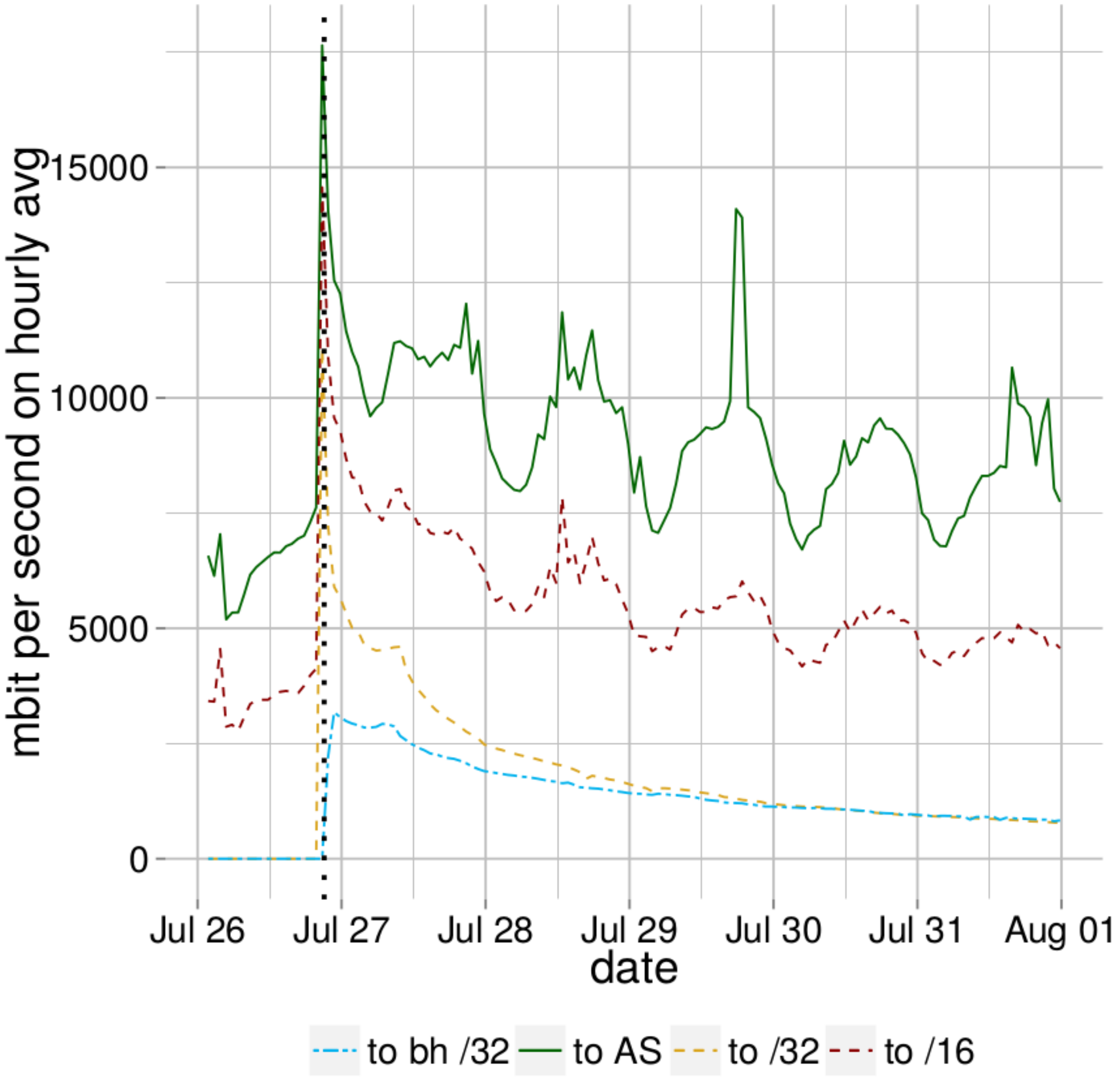
- 7,864 unique prefixes

- Most prefixes announced once (10%), or between two and three times (15%)

- Outliers spread from 10 to 100, max 623



Case Study - Impact on Traffic

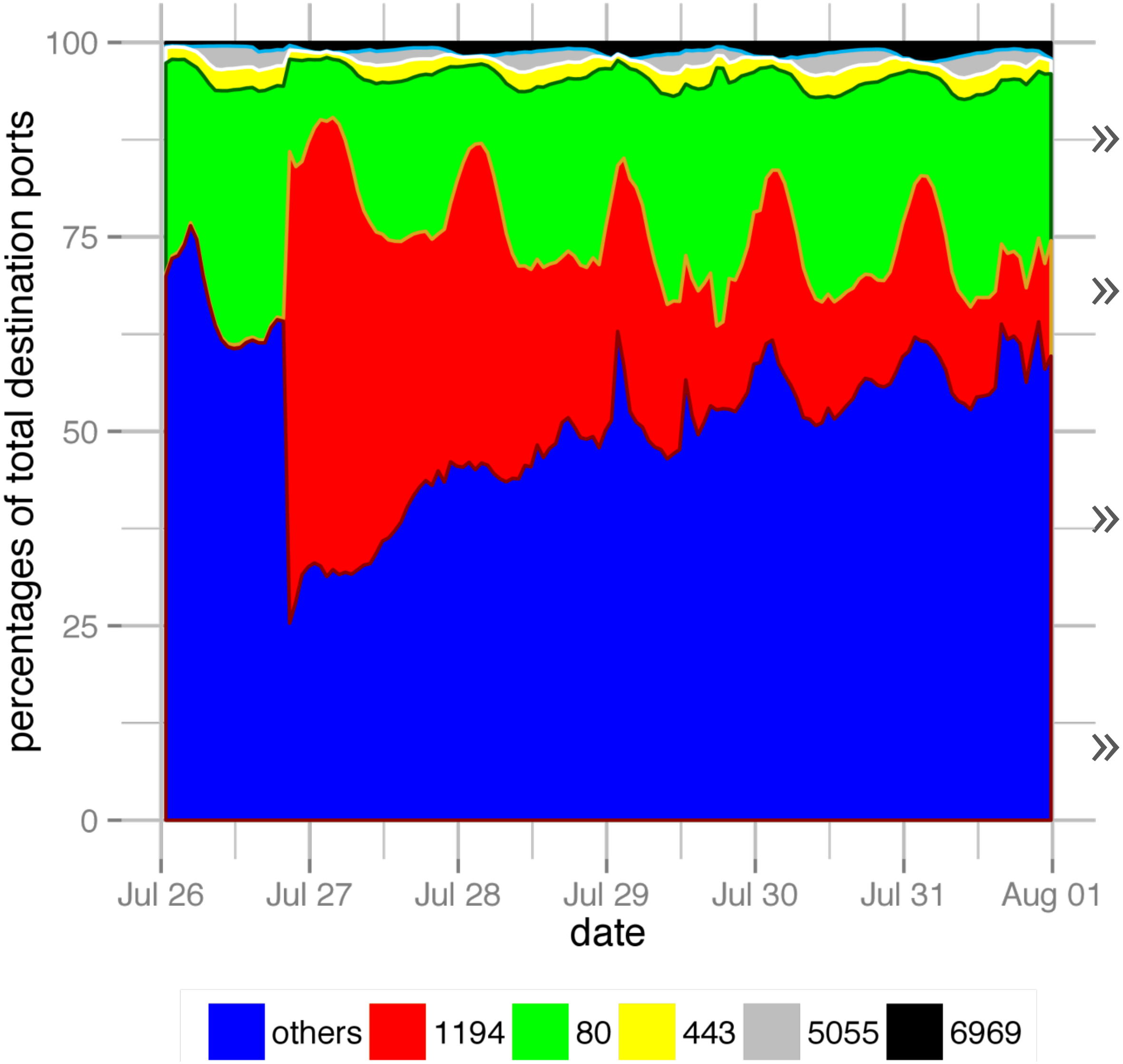


» Traffic for one /32

» Traffic rises up to 17.6 Gbit/s

» Traffic is reduced by one third

Case Study - Impact on Traffic



- Effectiveness indicator
- Port mix of customer port traffic
- Port 1194 (OpenVPN) share increases to ~50%
- Blackhole takes effect, port mix converges to initial distribution

Summary

» 23,000 announced blackholes (over a three month period)

» Stable number of 1200 active blackholes

» Observed least specific was a /18

» Very diverse announcement patterns (frequency, duration, …)

» Succeeds in mitigating large DDoS attacks

Full paper at http://www.net.t-labs.tu-berlin.de/papers/DFK-BIXPO-16.pdf

Future Work

- Acceptance of /32 blackholing announcements
- Standardized triggering
- Blackholing traffic monitoring
- Fine-grained blackholing

Security Considerations

- BGP communities can be altered (RPKI/BGPSec won’t help)
  - Strict filtering [RFC7454]
- DDoS attack through blackholing?
  - Strict filtering [RFC7454]
- Resource exhaustion attack against router
  - No known defense

Standardized Triggering of Blackholing

- Well-defined community for triggering blackholing
- First version of Internet Draft available [2]
- Extended beyond IXPs and more Operational Recommendations added
- Will become RFC status this year

[2] https://tools.ietf.org/html/draft-ymbk-grow-blackholing-01

Comments? Questions?

christoph@inet.tu-berlin.de