



Inferring BGP Blackholing in the Internet

Vasileios Giotsas, Georgios Smaragdakis, Christoph Dietzel,
Philipp Richter, Anja Feldmann, and Arthur Berger

TU Berlin CAIDA MIT DE-CIX Akamai

DDoS Attacks are a Serious Threat

The New York Times


Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool


Leer en español


By NICOLE PERLROTH and DAVID E. SANGER MAY 12, 2017



RELATED COVERAGE


 U.K. Health Service Ignorant Months MAY 12, 2017


 Hacker Leaks Episodes




KrebsOnSecurity Hit With Record DDoS

Wednesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual denial-of-service (DDoS) attack designed to knock the site offline. The attack did succeed thanks to the hard work of the engineers at Akamai, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever seen.






BLOG ADVERTISMENT



ALIEN VAULT



REACT



SC Media UK > News > ICYMI: 1Tb DDoS attack, Krebs dropped, Pippa Middleton, Yahoo!

by SC Staff

[Follow @scmagazineuk](#)

September 30, 2016

ICYMI: 1Tb DDoS attack, Krebs dropped, Pippa Middleton, Yahoo!



In case you missed it this week, our most popular stories included the news of biggest ever DDoS attack, Krebs dropped over other massive DDoS and future queen's younger sister hacked.

Article development led by @comqueue queue.acm.org DOI:10.1145/1897852.1897869

Attacks in Estonia and Georgia highlight key vulnerabilities in national Internet infrastructure.

BY ROSS STAPLETON-GRAY AND WILLIAM WOODCOCK

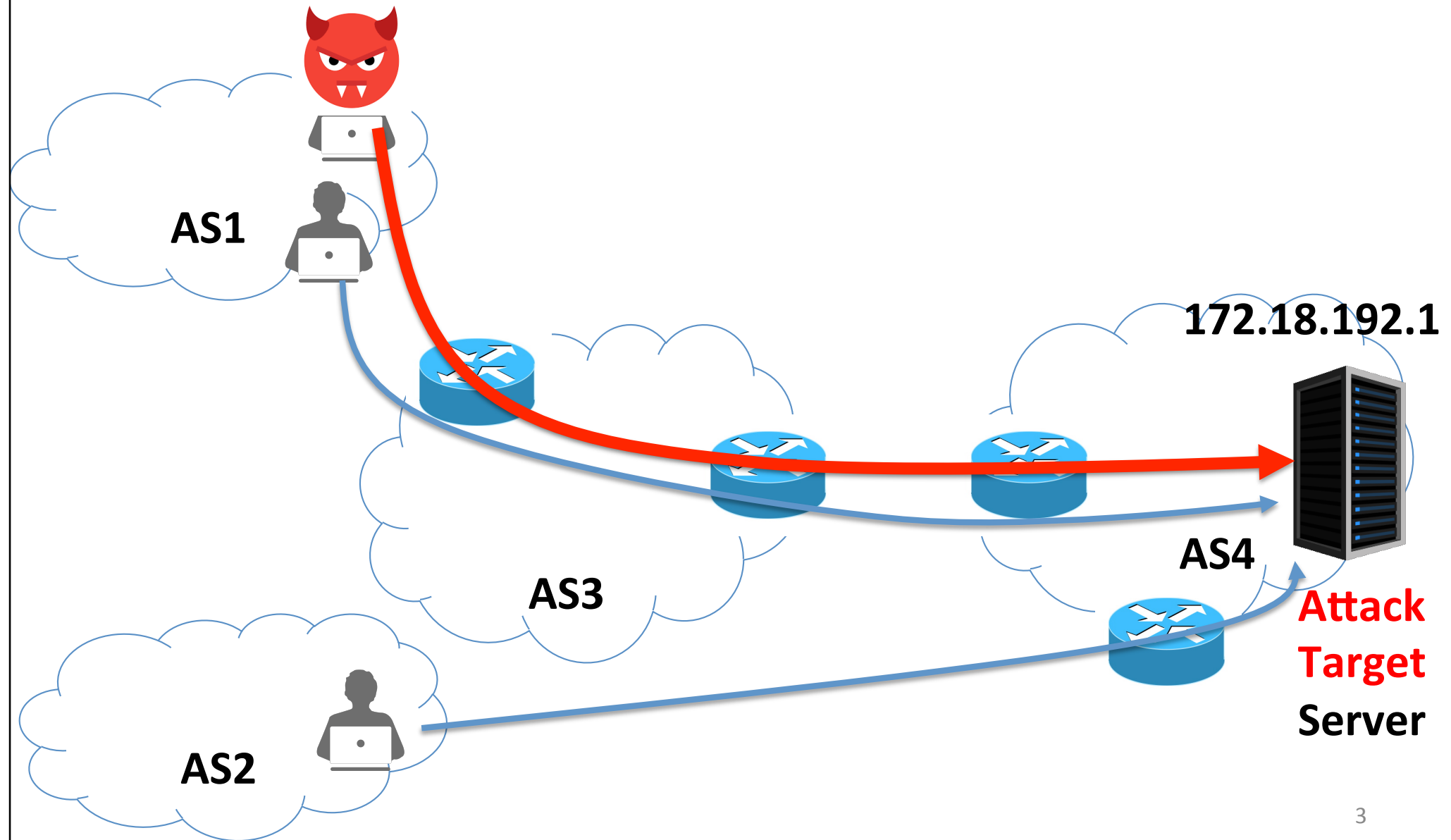
National Internet Defense—Small States on the Skirmish Line

DESPITE THE GLOBAL and borderless nature of the Internet's underlying protocols and driving philosophy, there are significant ways in which it remains substantively territorial. Nations have policies and laws that govern and attempt to

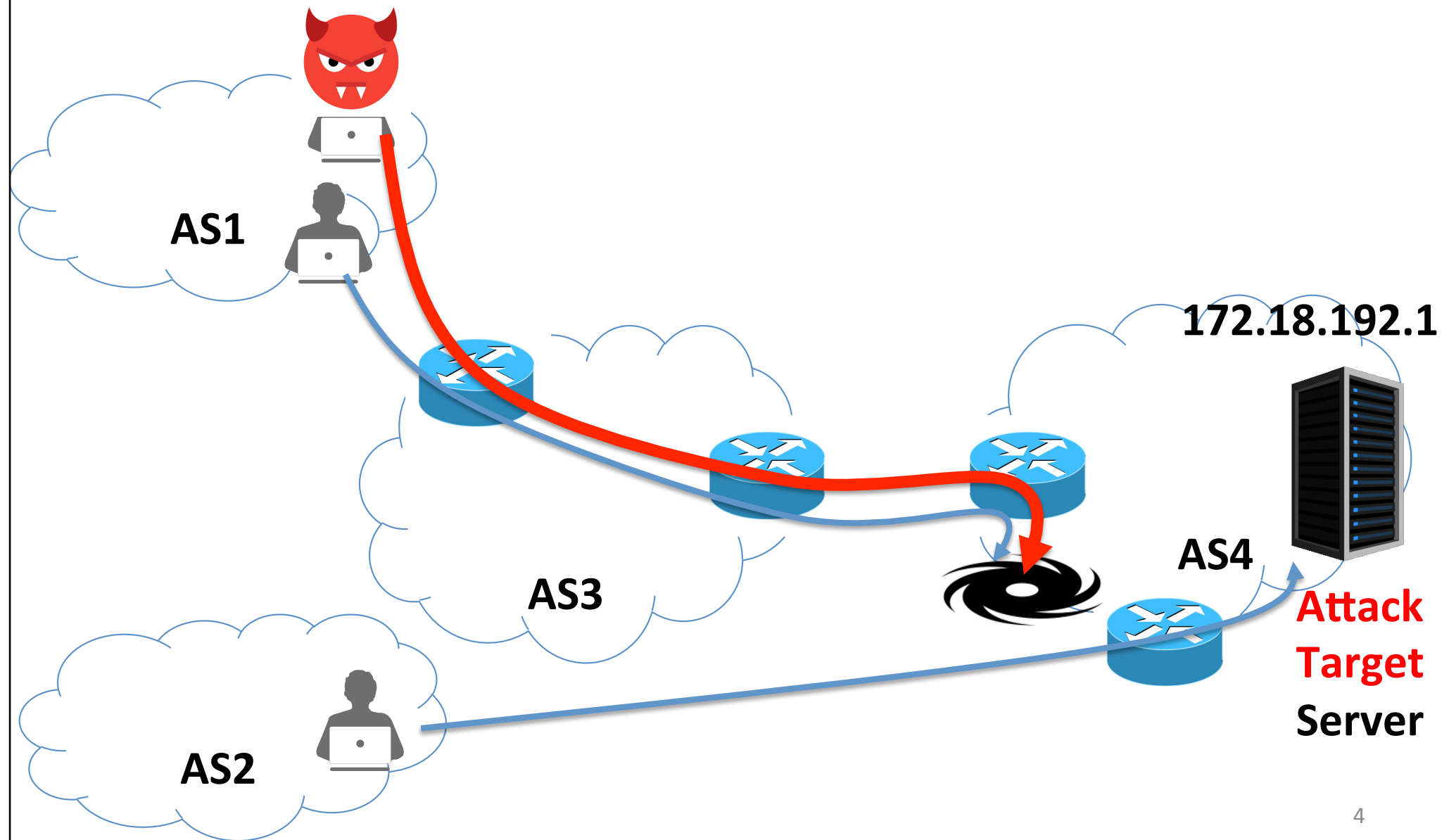


and commercial activity and influence. This is far less palpable than a nation's physical territory or even than "its air" or "its water"—one could, for example, establish by treaty how much pollution Mexican and American factories might contribute to the atmosphere along their shared border, and establish metrics and targets fairly objectively. Cyberspace is still a much wilder frontier, difficult to define and measure. Where

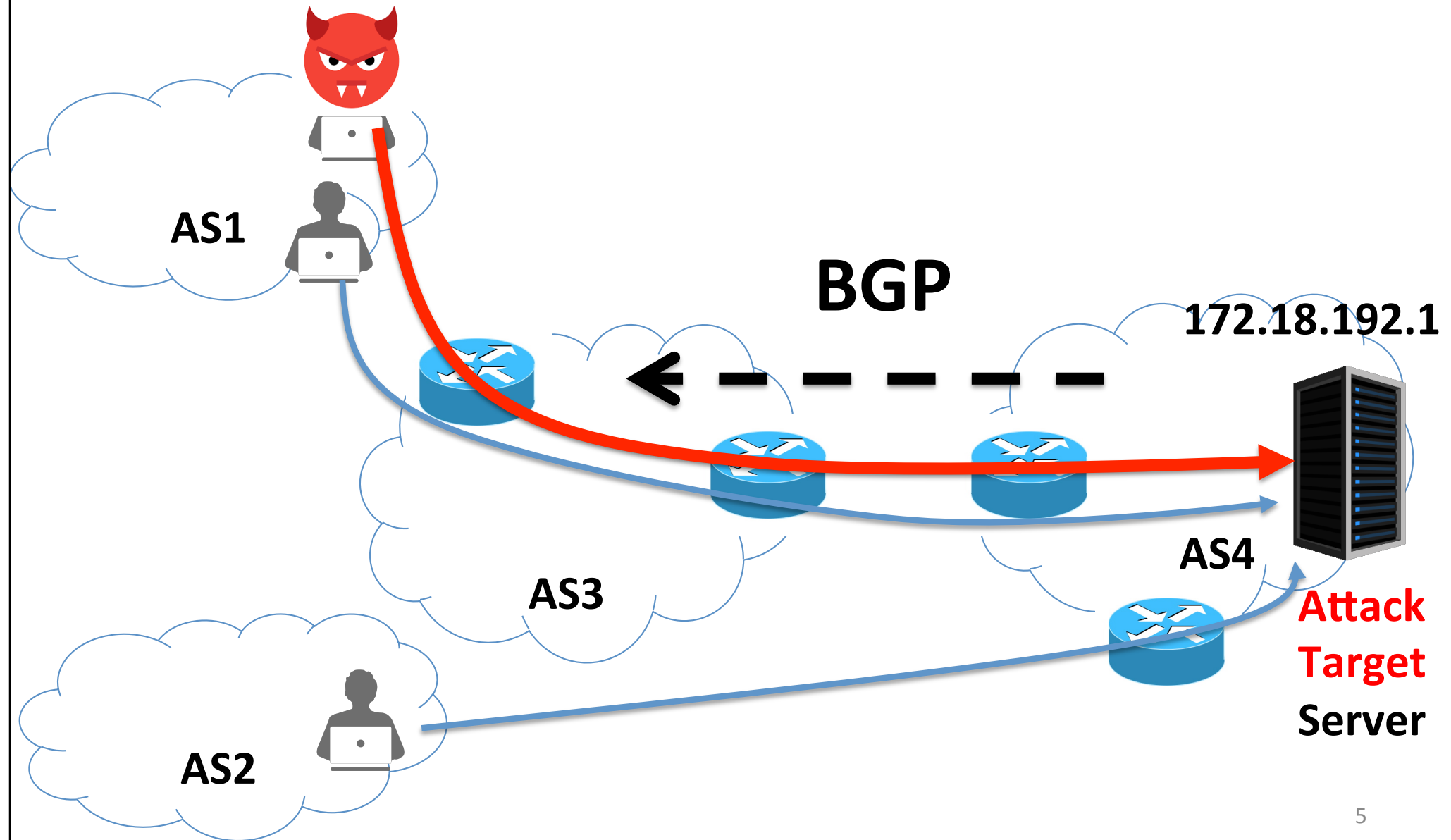
Networks under Attack



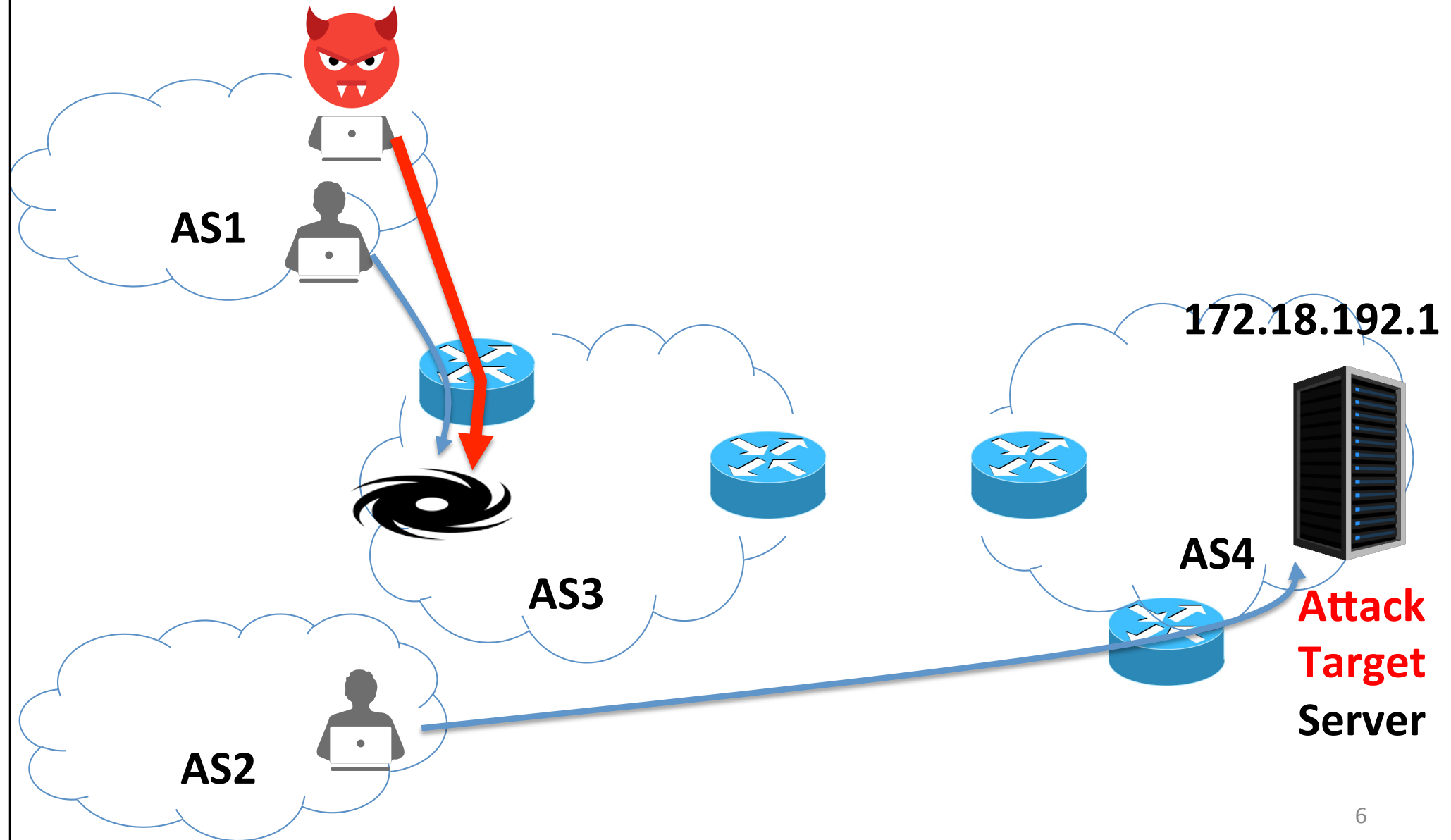
Blackholing



BGP Blackholing



BGP Blackholing



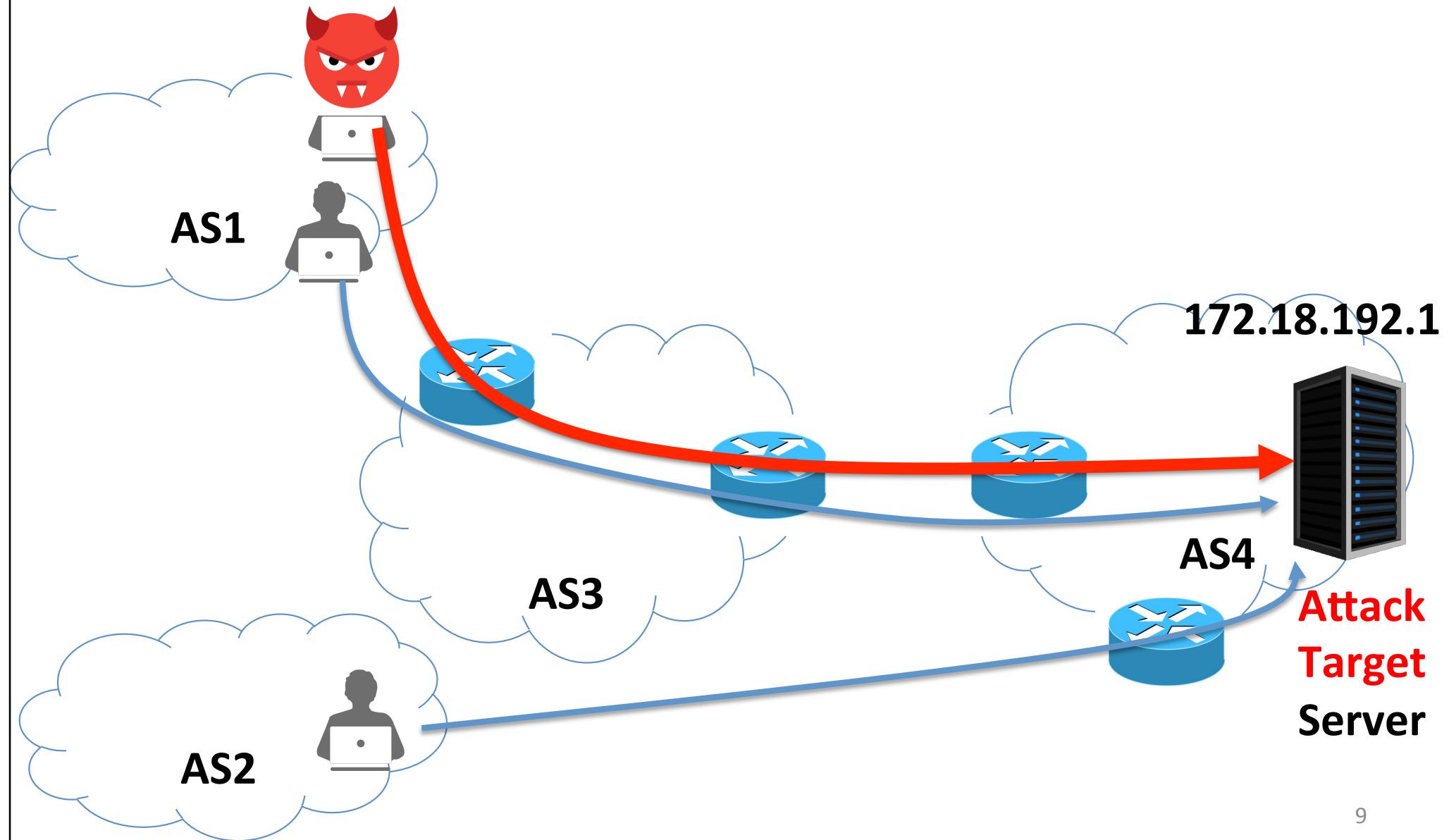
Agenda

- BGP Blackholing in Detail
- Inference Methodology for BGP Blackholing
- Trends in BGP Blackholing Activity
- Visibility of BGP Blackholing
- BGP Blackholing Network Efficacy
- Profile of BGP Blackholing Adopters

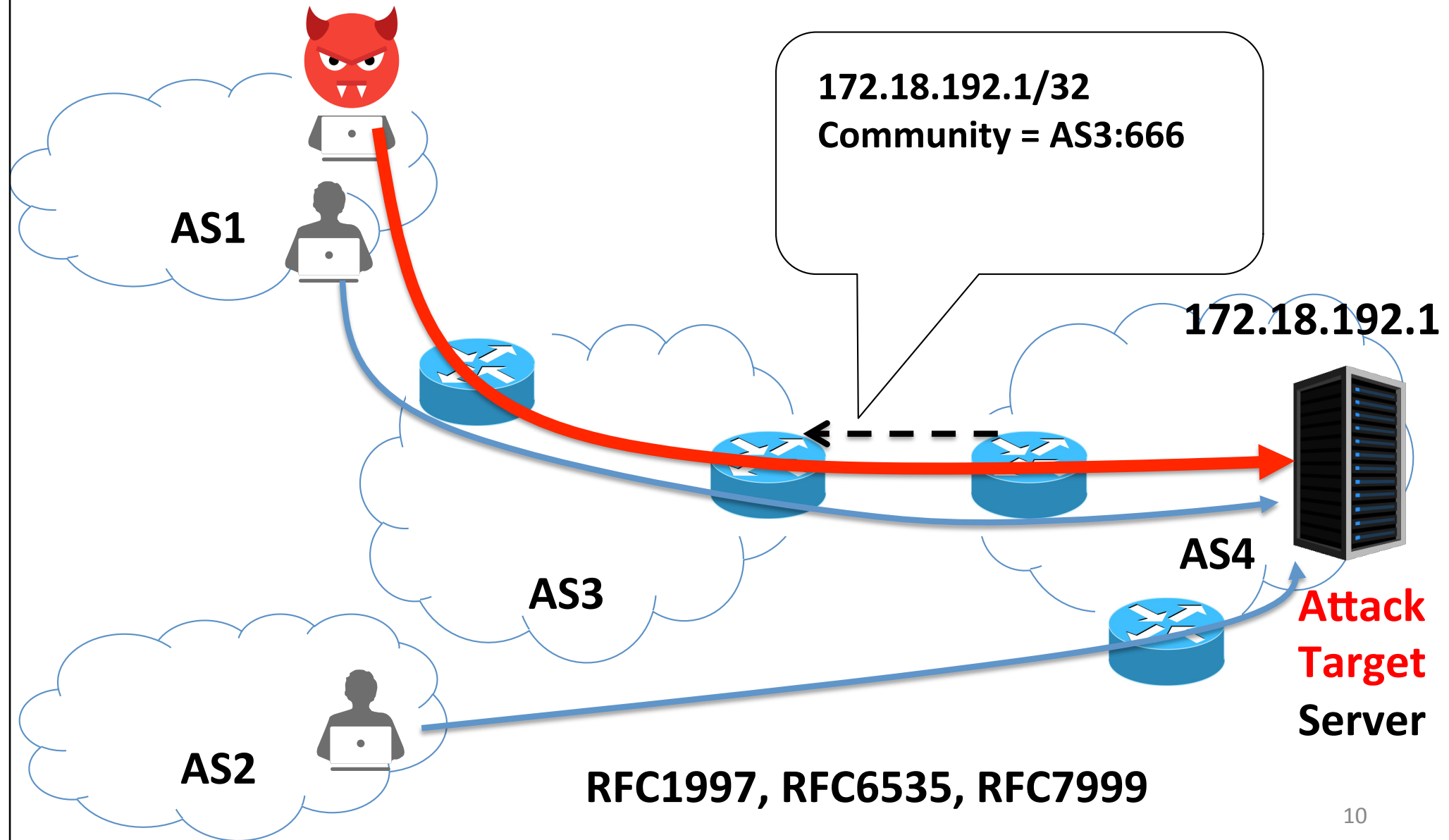
Agenda

- **BGP Blackholing in Detail**
- Inference Methodology for BGP Blackholing
- Trends in BGP Blackholing Activity
- Visibility of BGP Blackholing
- BGP Blackholing Network Efficacy
- Profile of BGP Blackholing Adopters

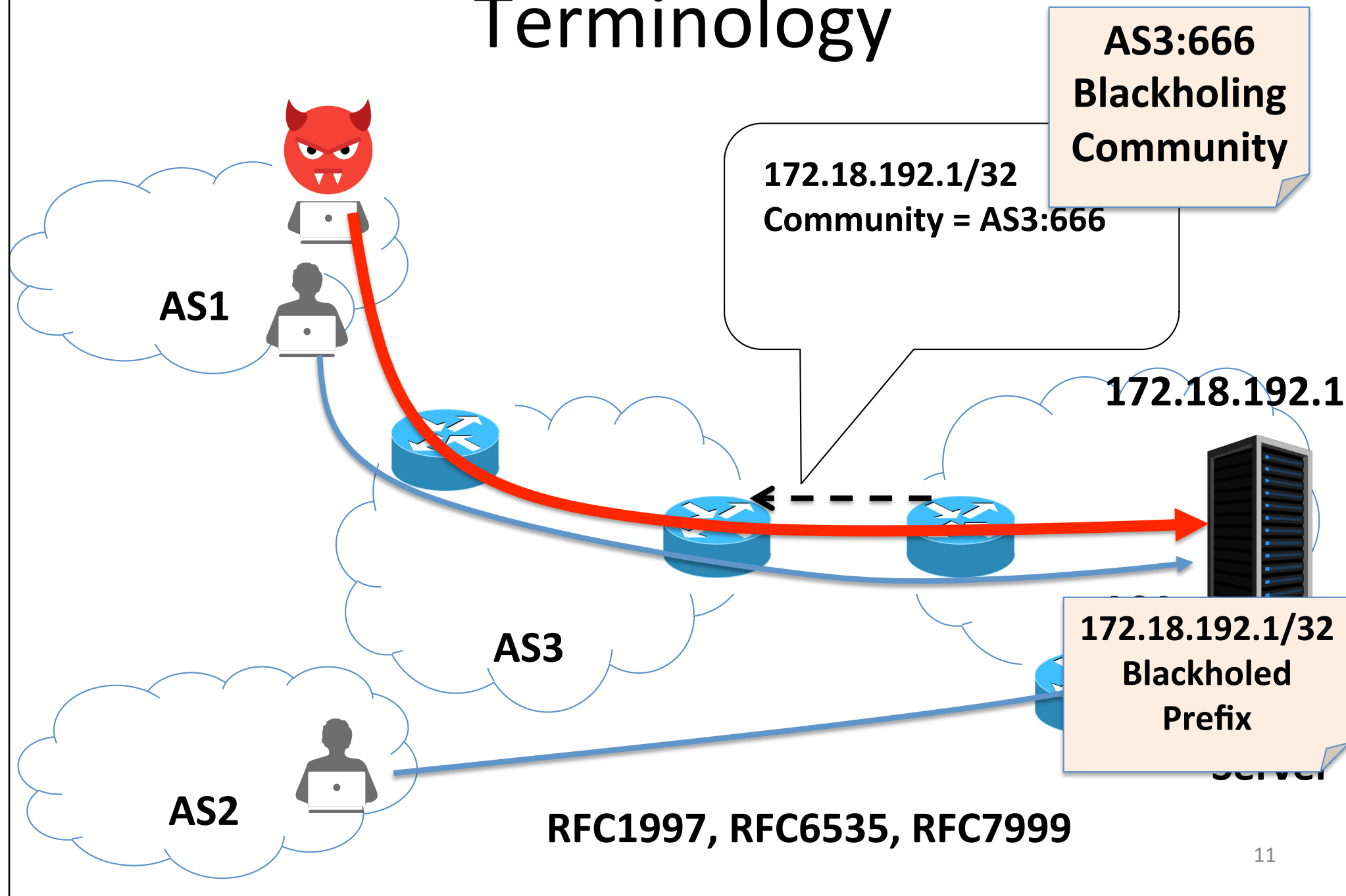
BGP Blackholing in the Internet



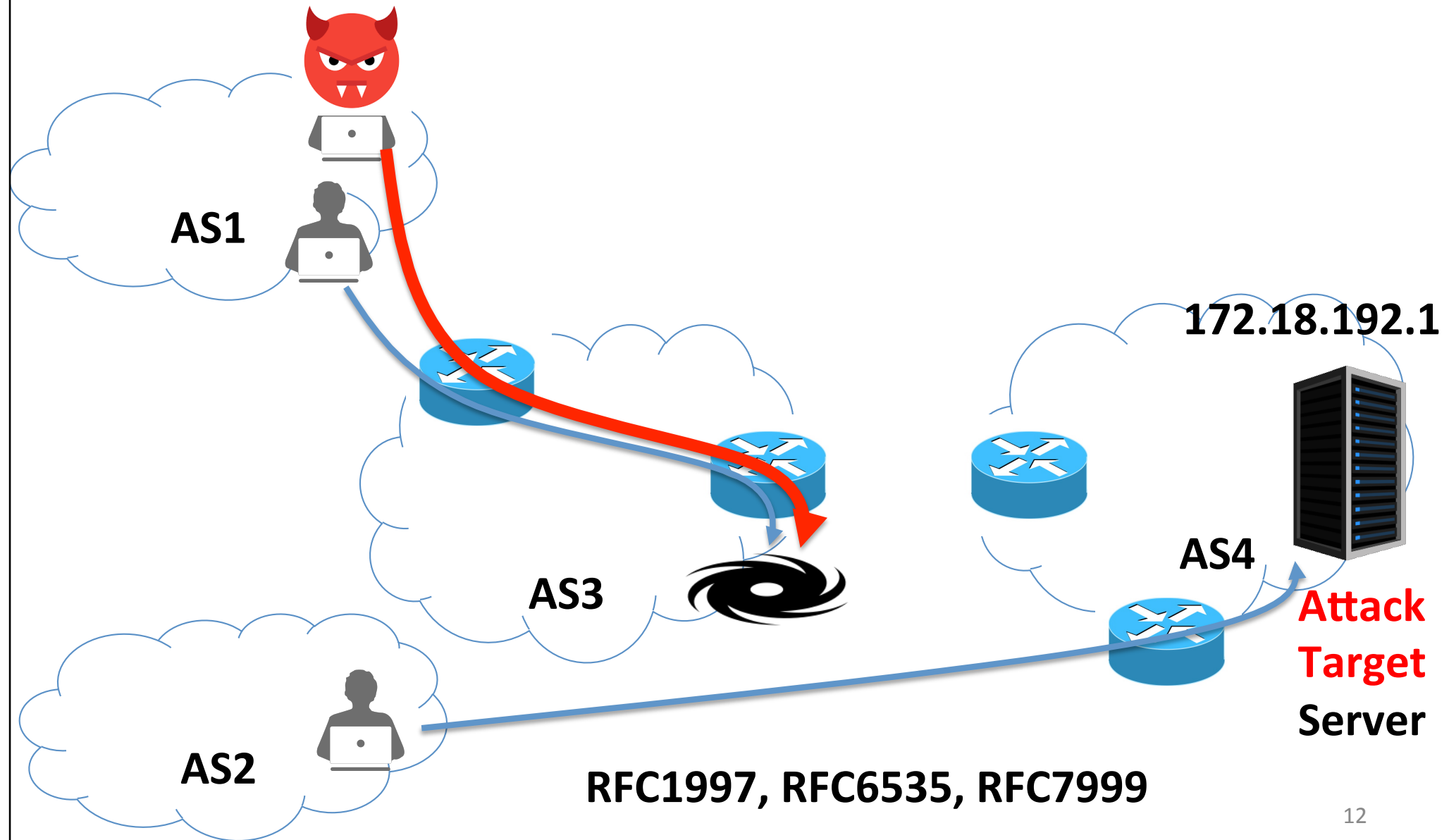
BGP Blackholing in the Internet



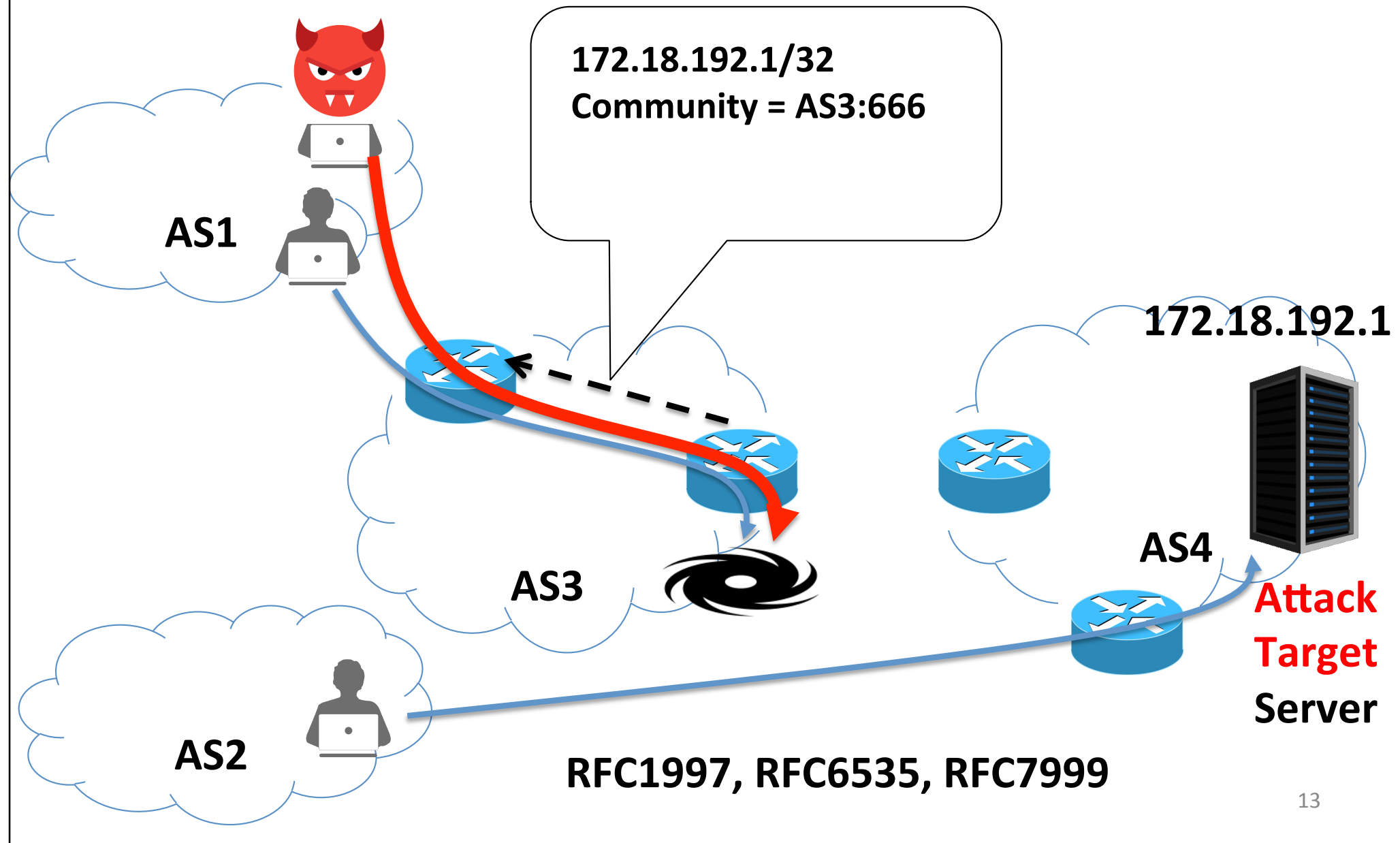
Terminology



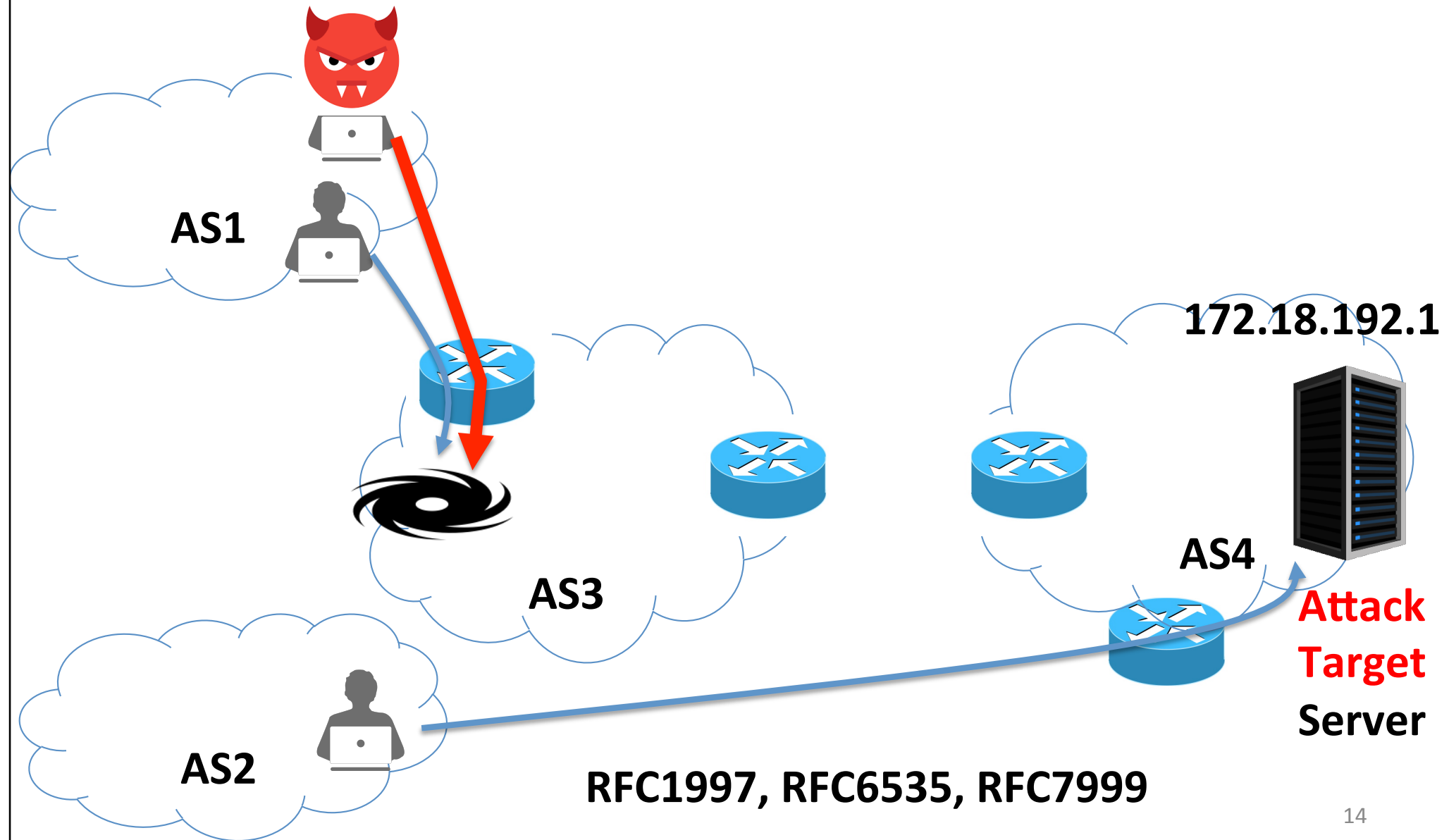
BGP Blackholing in the Internet



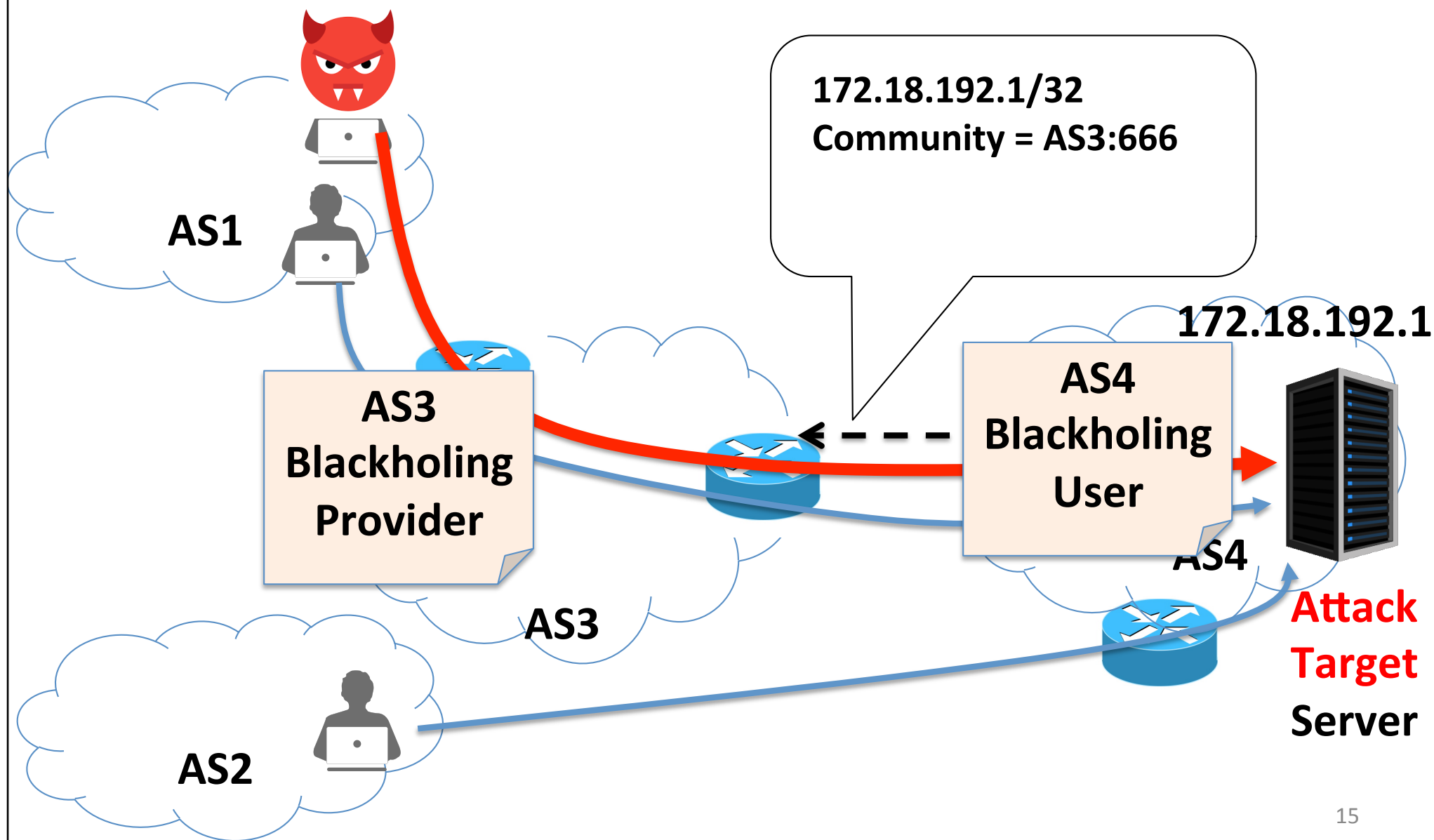
BGP Blackholing in the Internet



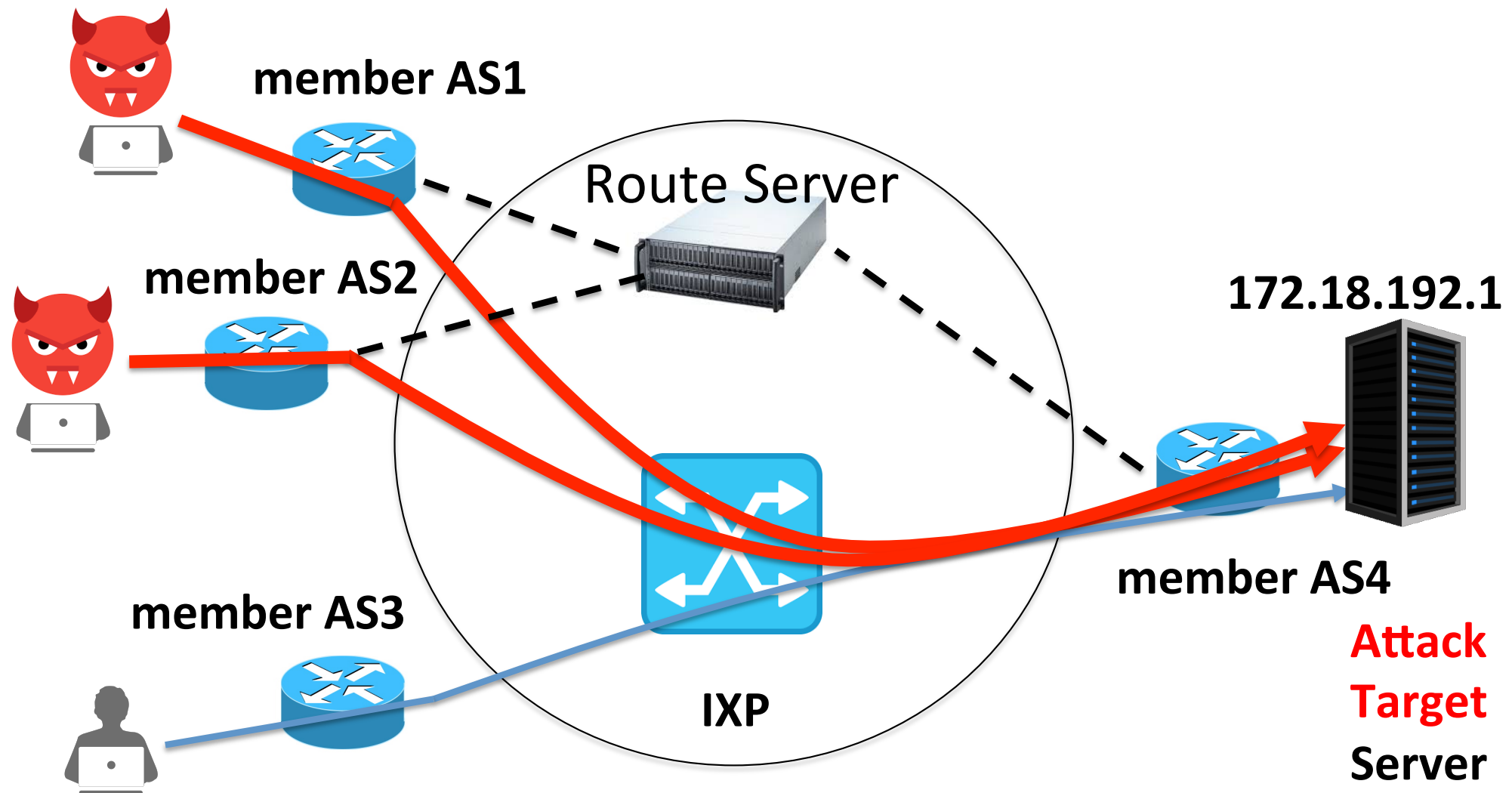
BGP Blackholing in the Internet



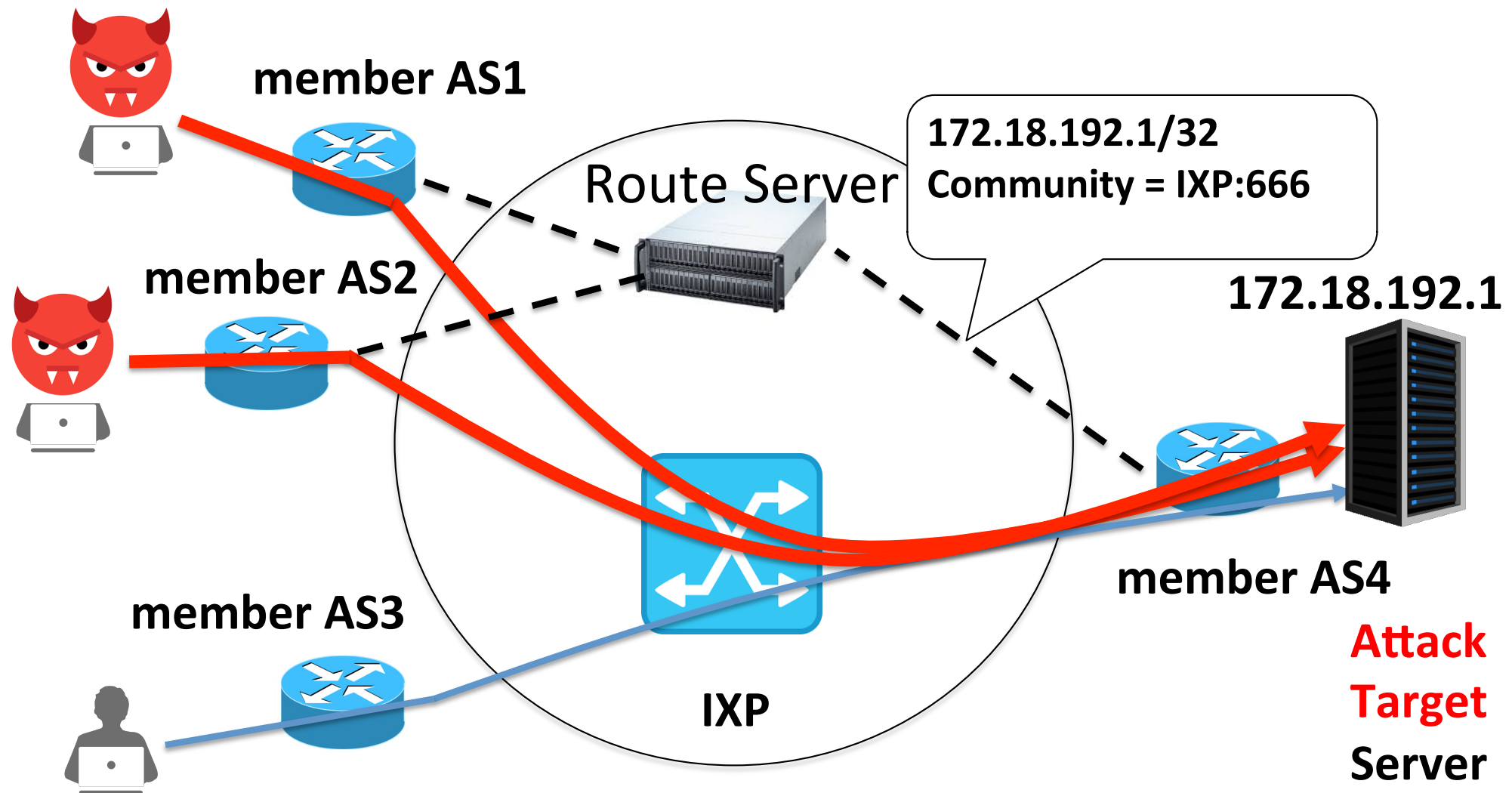
Terminology



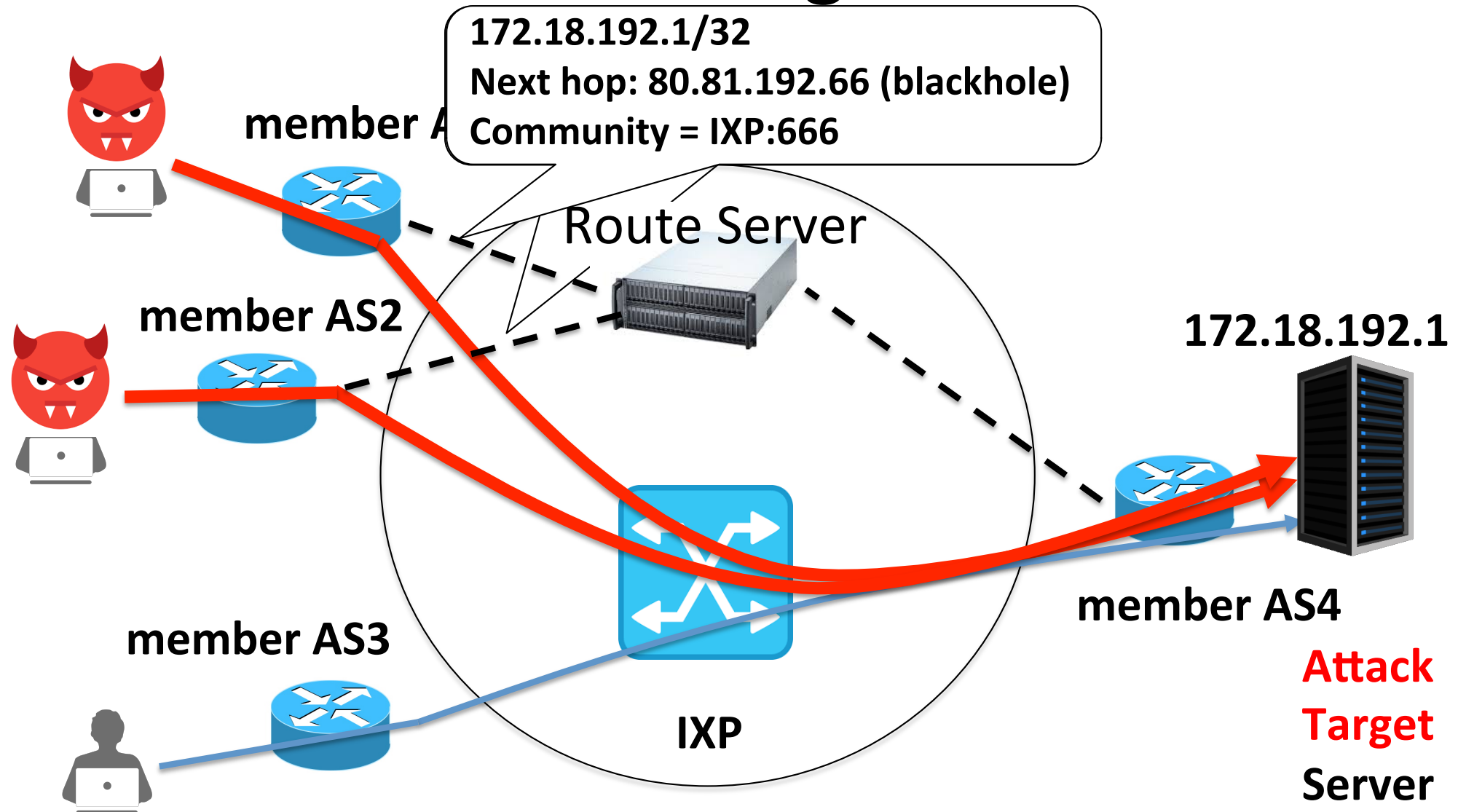
BGP Blackholing in an IXP



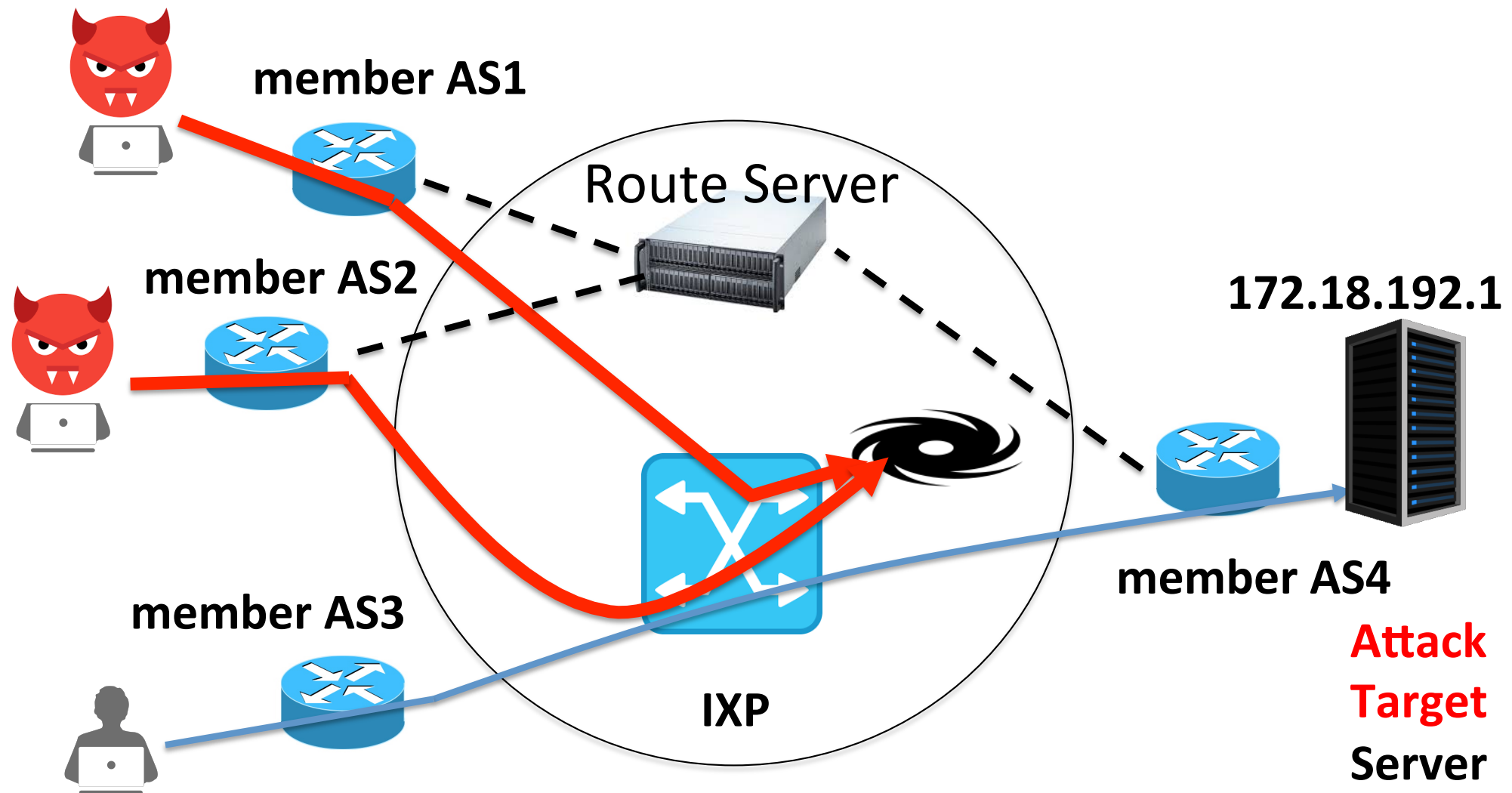
BGP Blackholing in an IXP



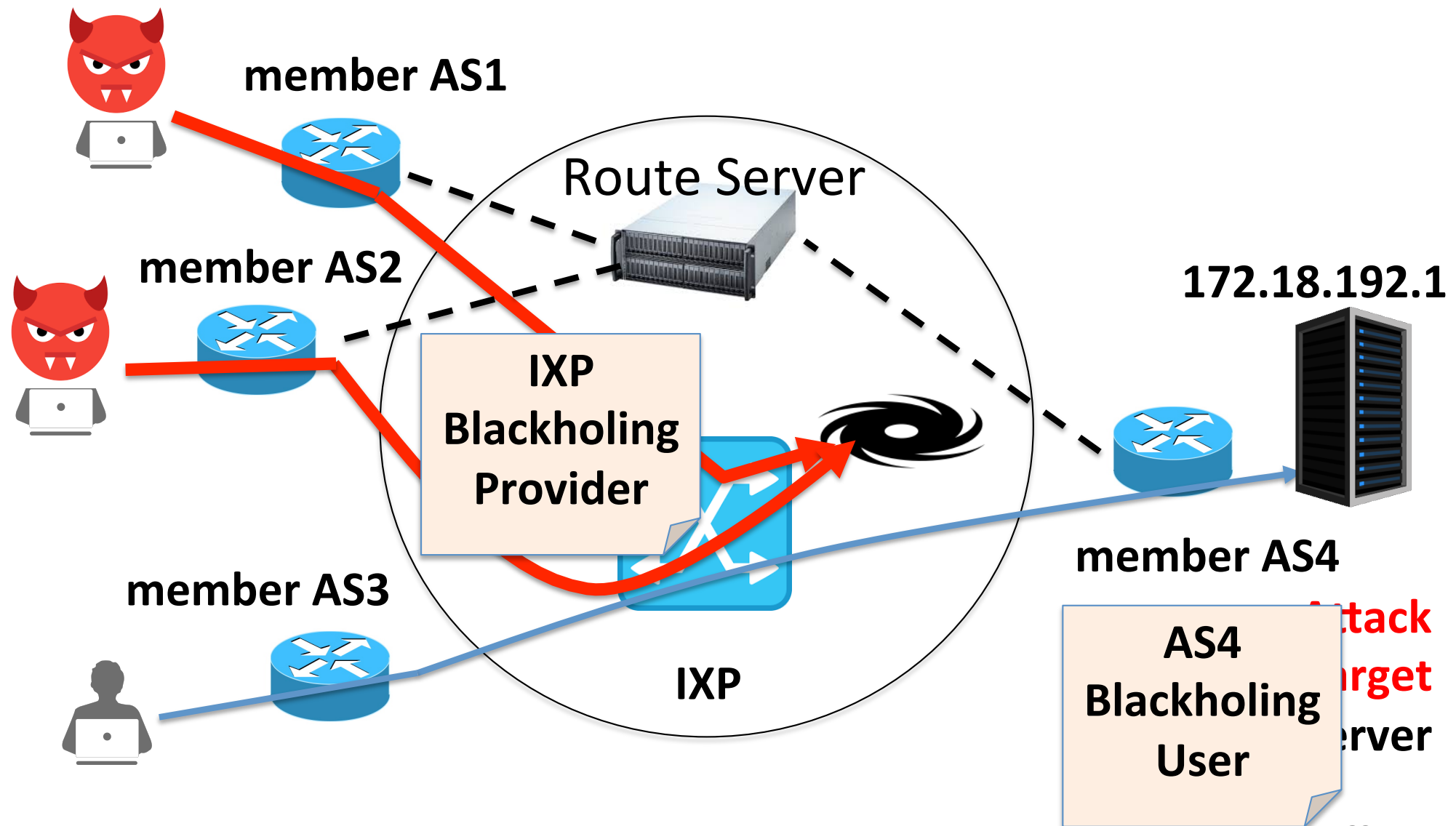
BGP Blackholing in an IXP



BGP Blackholing in an IXP



BGP Blackholing in an IXP



Agenda

- BGP Blackholing in Detail
- **Inference Methodology for BGP Blackholing**
- Trends in BGP Blackholing Activity
- Visibility of BGP Blackholing
- BGP Blackholing Network Efficacy
- Profile of BGP Blackholing Adopters

BGP Blackhole Community Dictionary

- BGP Communities are **not standardized**
- We mine Internet Registries, NOC webpages etc. for keywords like “blackhole”, “null route” using Natural Language Processing

Level3

customer traffic engineering communities - LocalPref

3356:70 - set local preference to 70

3356:80 - set local preference to 80

3356:90 - set local preference to 90

customer traffic engineering communities - Blackhole

3356:9999 - blackhole (discard) traffic

Traffic destined for any prefixes tagged with this community will be discarded at ingress to the Level 3 network. The prefix must be one permitted by the customer's existing ingress BGP filter.

Support@Level3.com may need to be contacted to allow in some cases. For some router vendors the peering

DE-CIX

There are additional communities for controlling announcements:

65535:666 set community BLACKHOLE

6695:65281 set community NO-EXPORT

6695:65282 set community NO-ADVERTISE

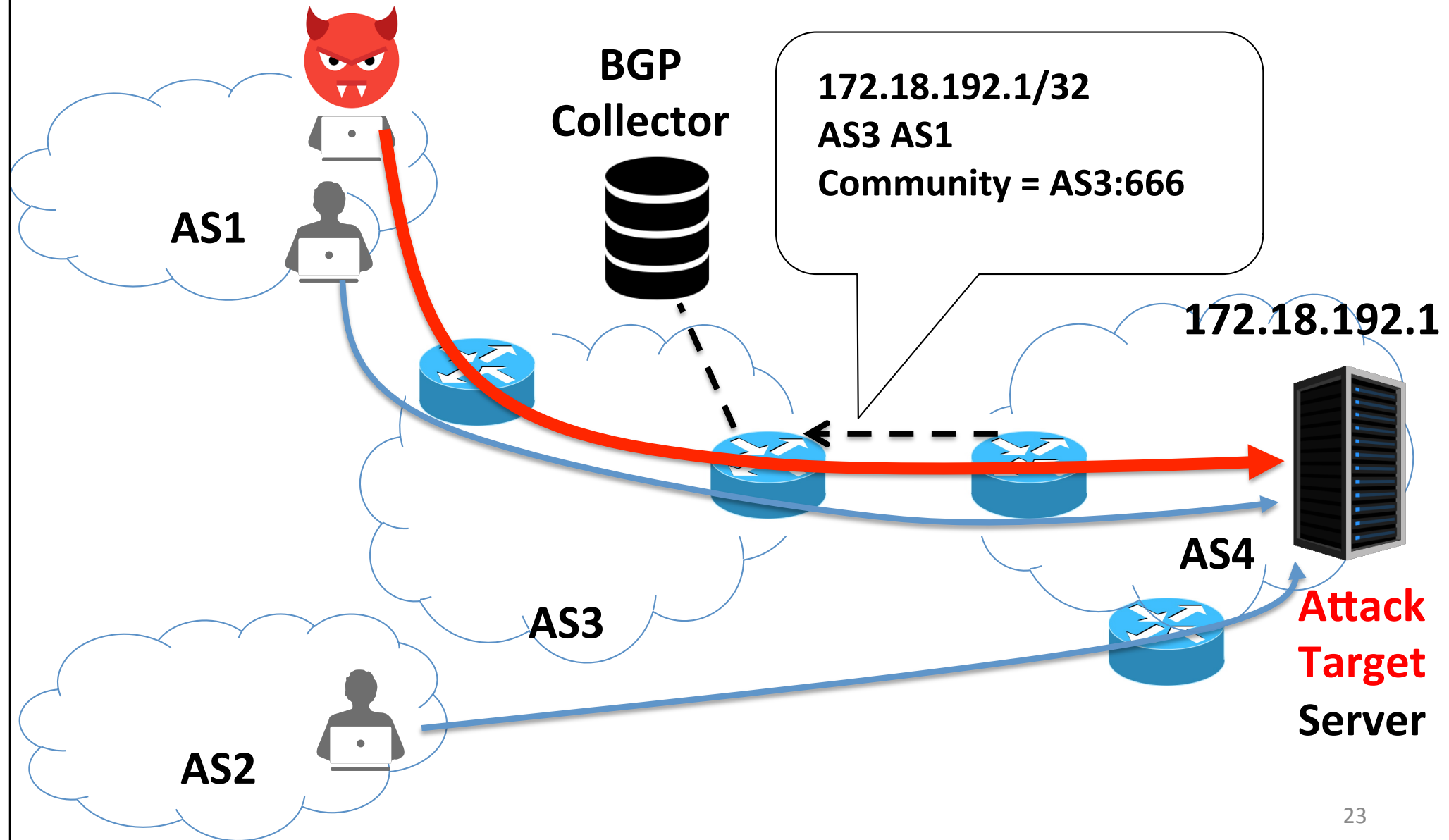
For more information on Route Server control and Blackholing, please see:

<https://portal.de-cix.net/home/documentation/routeserver-guides/>

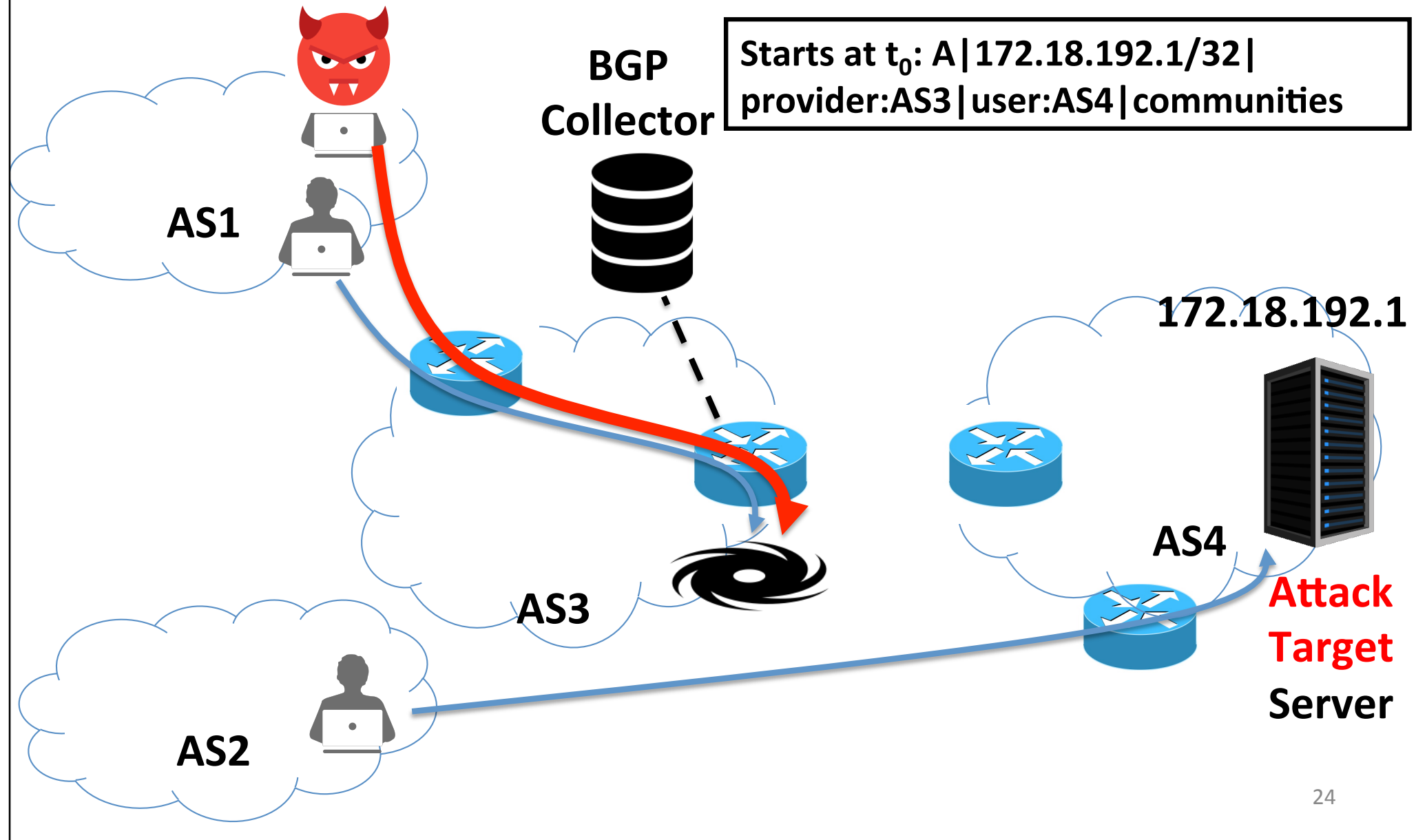
<https://portal.de-cix.net/home/documentation/blackholing-guide/>

The above information was collected from whois.ripe.net, using object "AS6695" on October 15, 2017

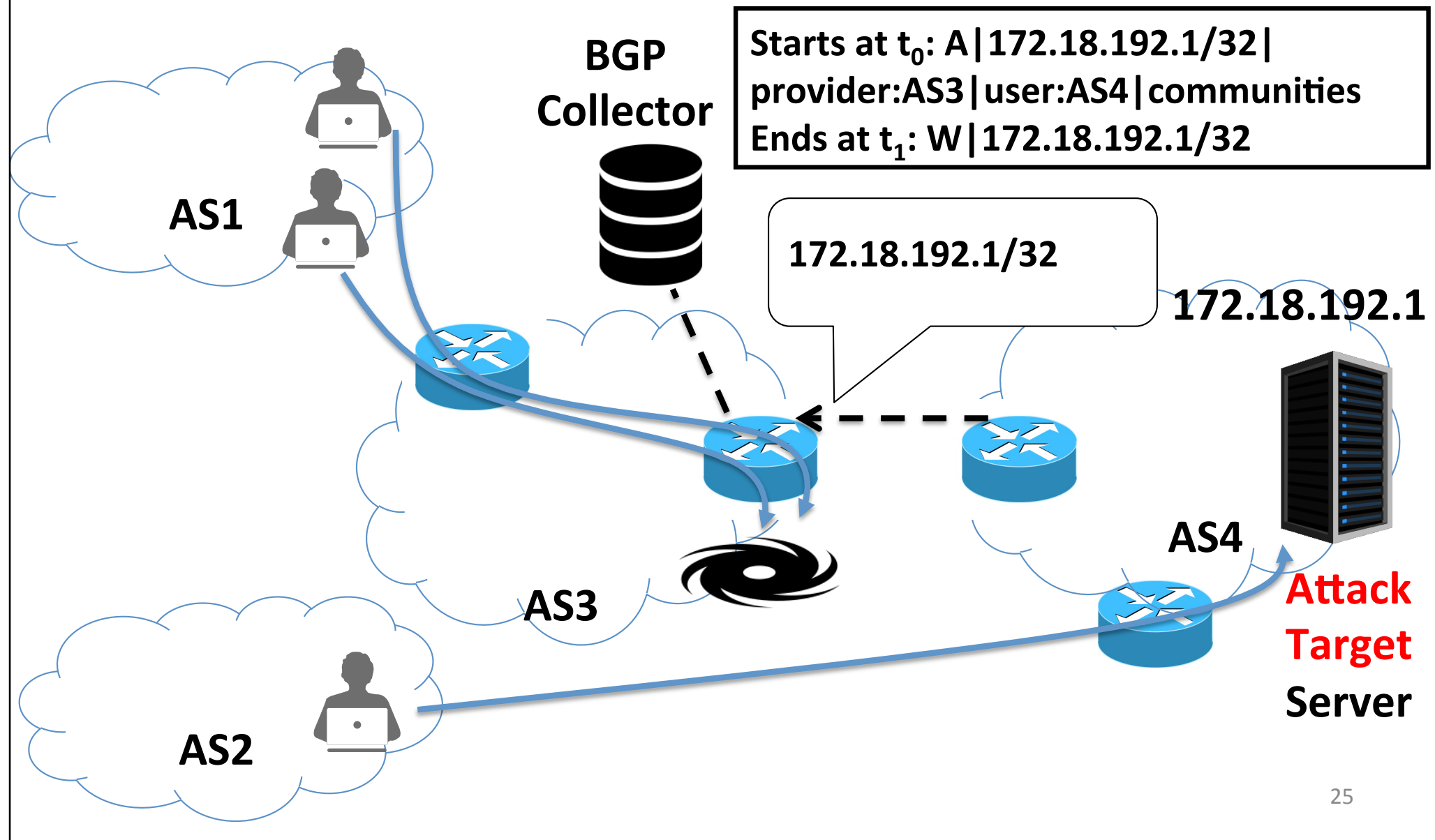
Methodology



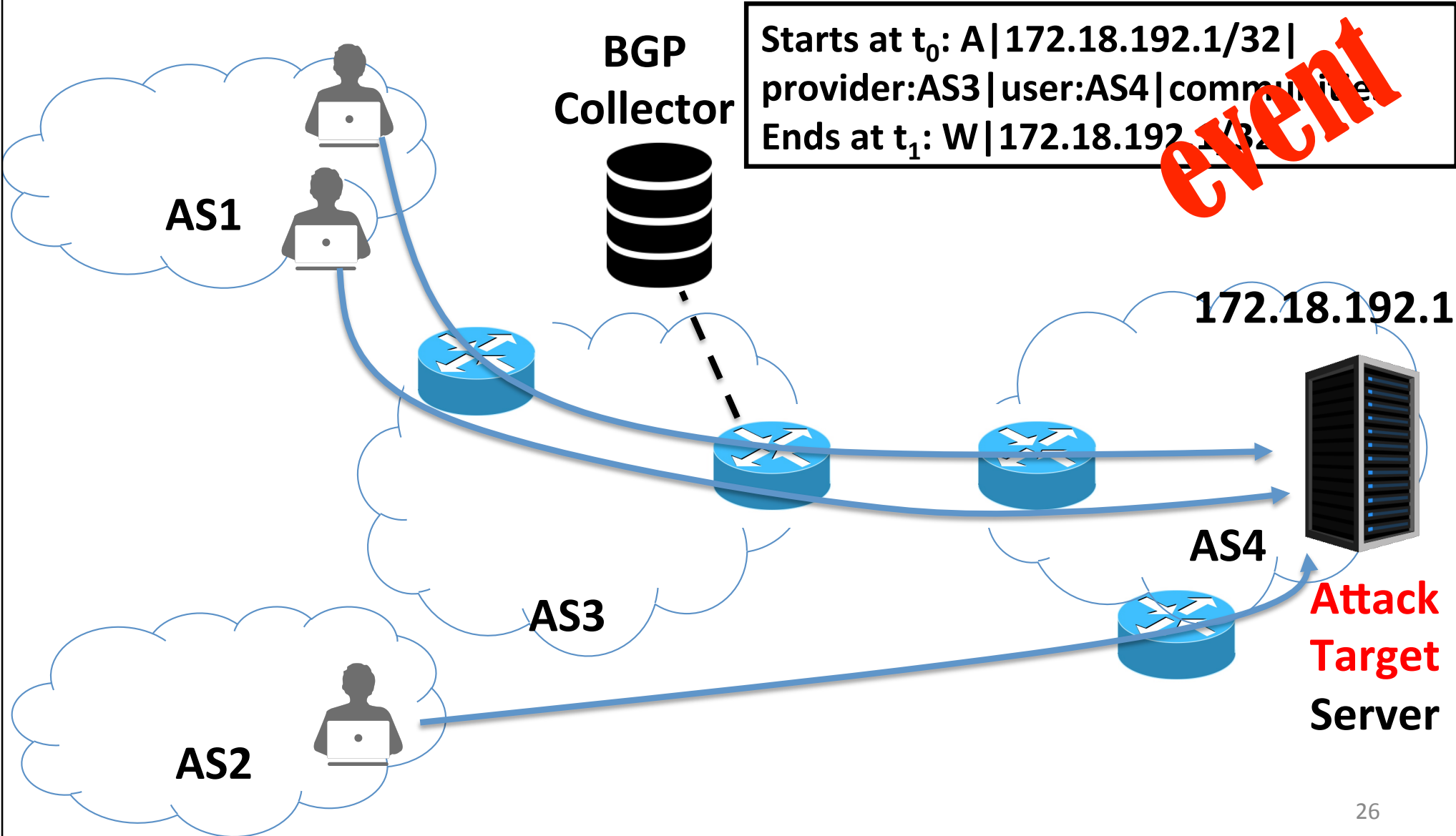
Methodology



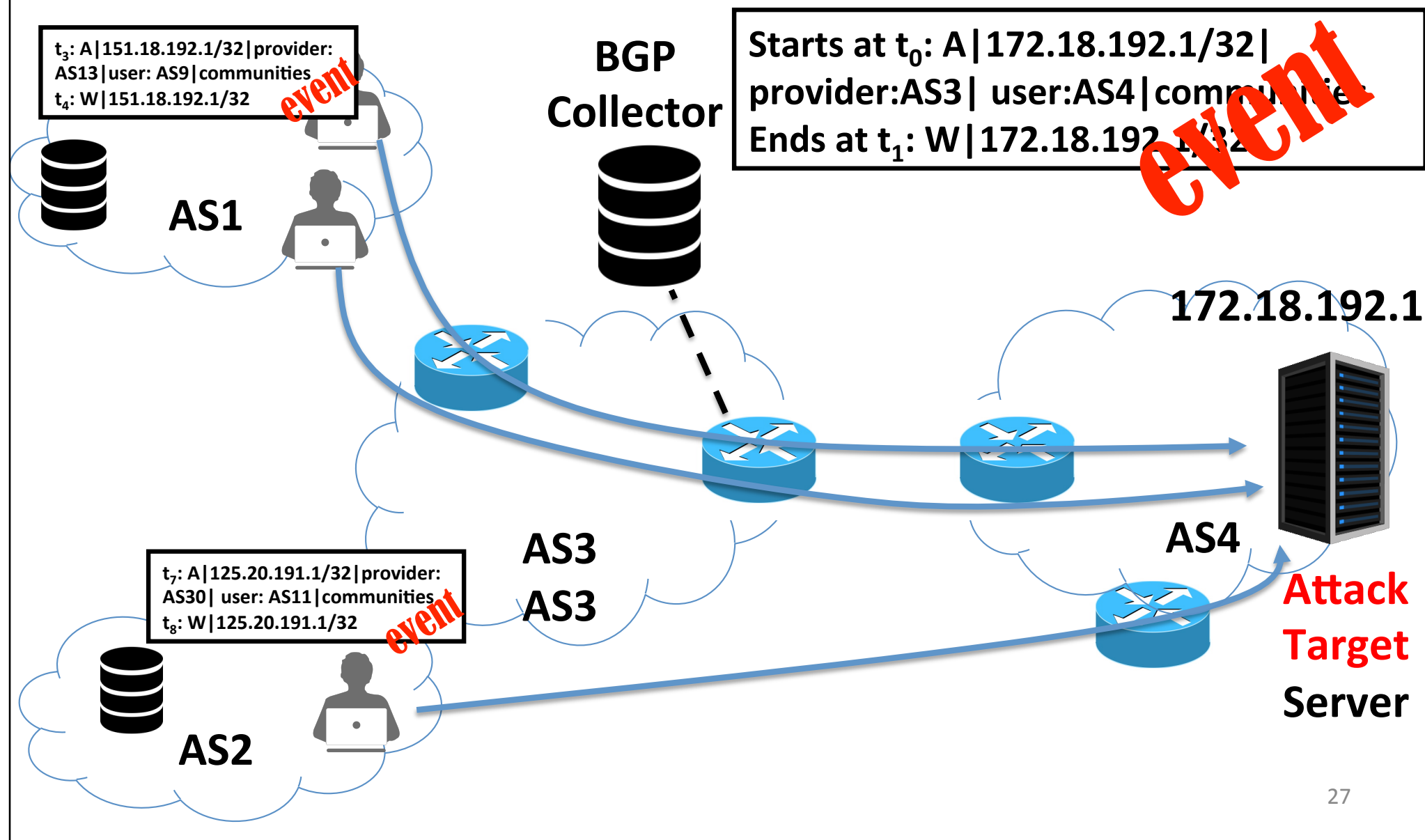
Methodology



Methodology



Methodology



Agenda

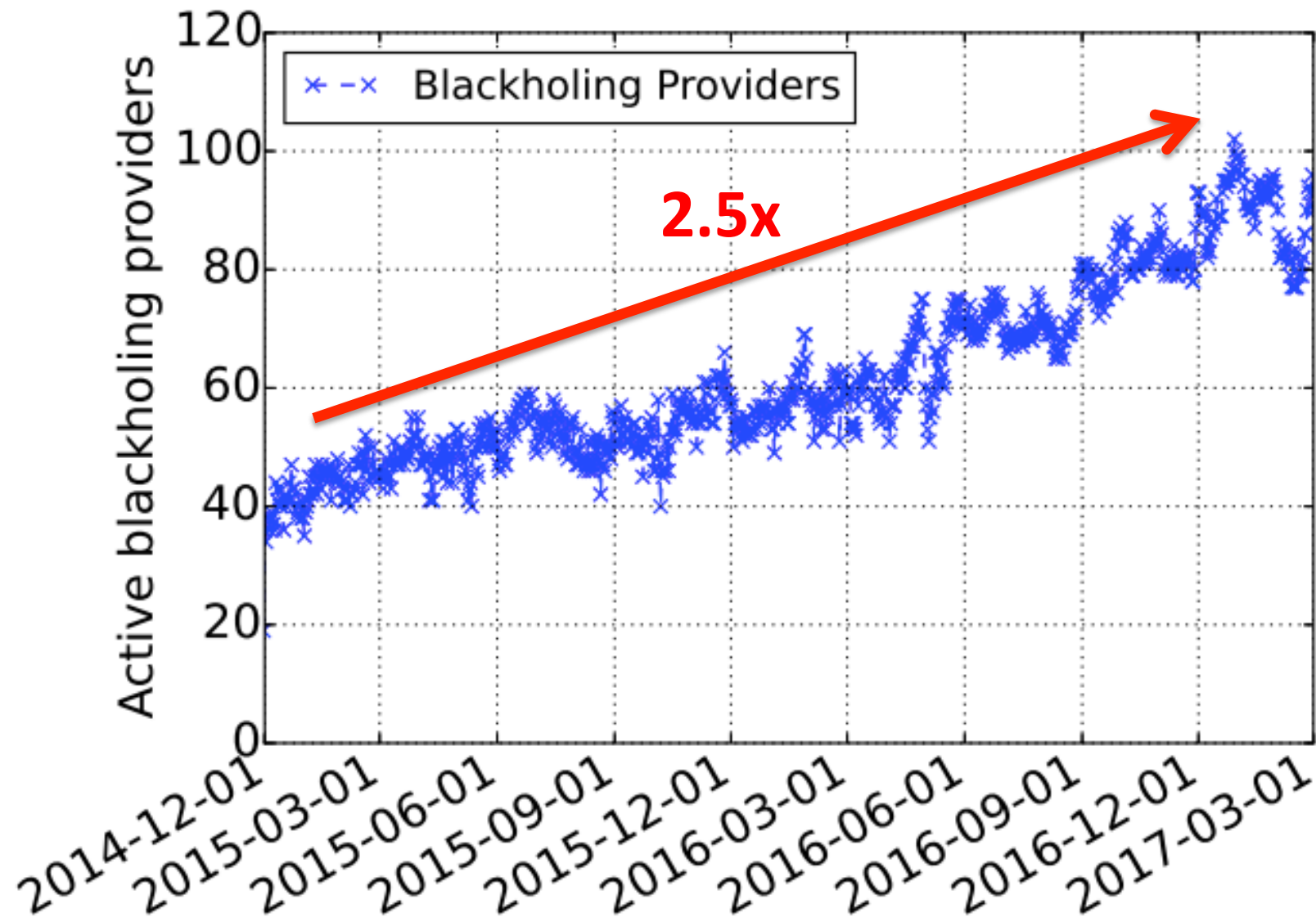
- BGP Blackholing in Detail
- Inference Methodology for BGP Blackholing
- **Trends in BGP Blackholing Activity**
- Visibility of BGP Blackholing
- BGP Blackholing Network Efficacy
- Profile of BGP Blackholing Adopters

BGP Datasets

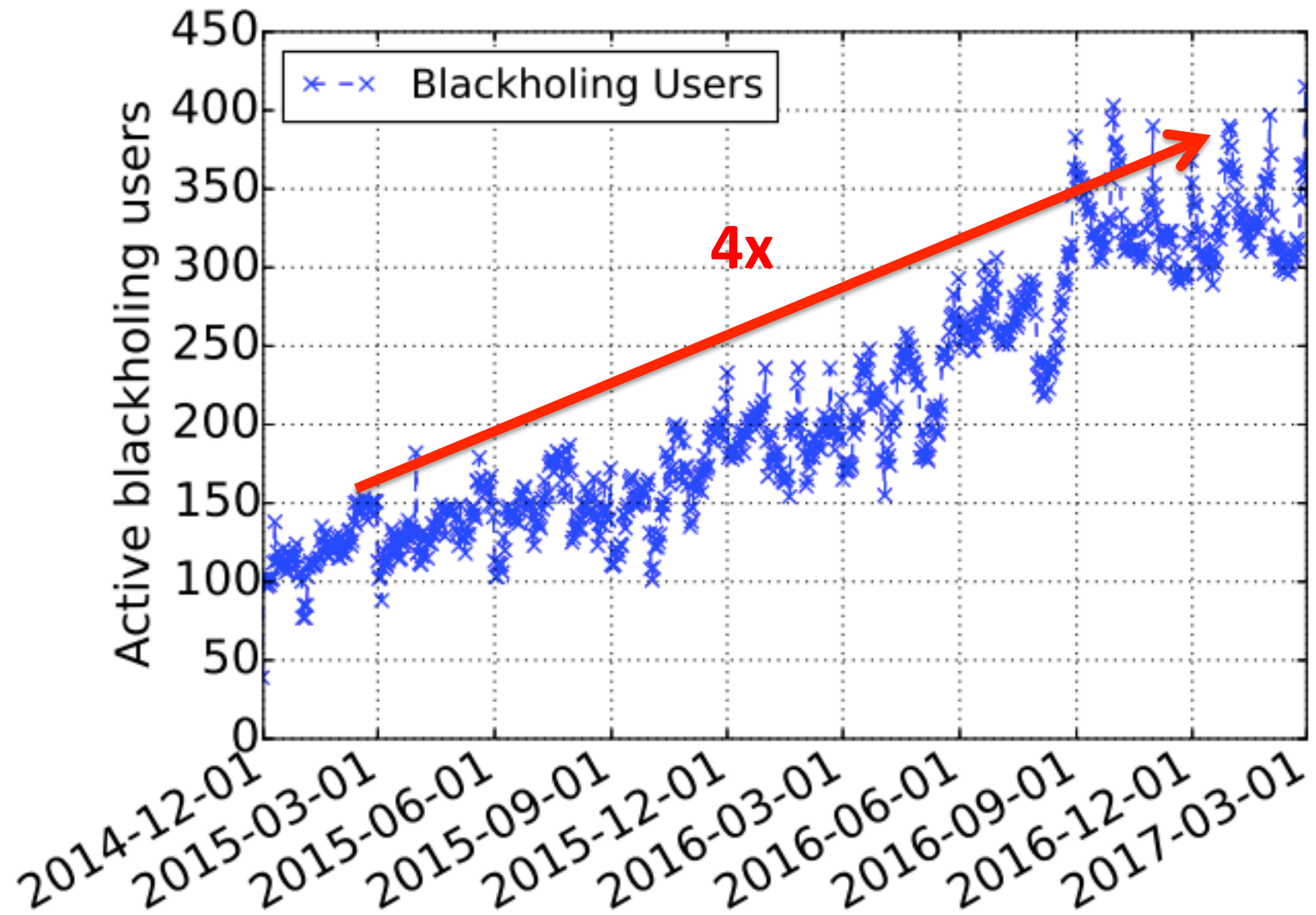
Source	#IP peers	#AS peers
RIPE	425	313
Route Views	269	197
PCH	8,897	1,721
CDN	3,349	1,282
Total	12,940	2,798

CDN and PCH infer **3x** more blackholed prefixes than RIPE and Route Views

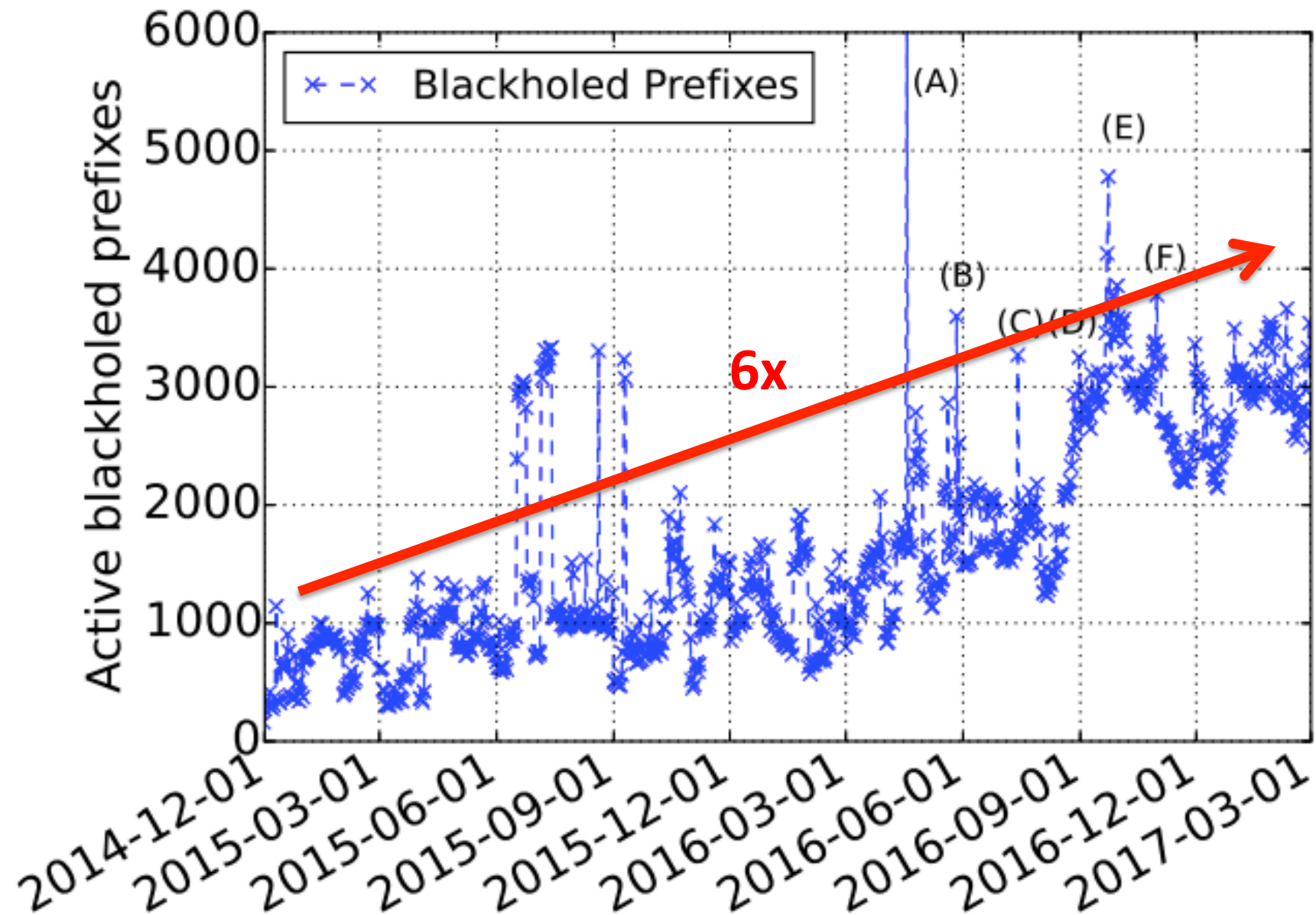
The Rise of BGP Blackholing



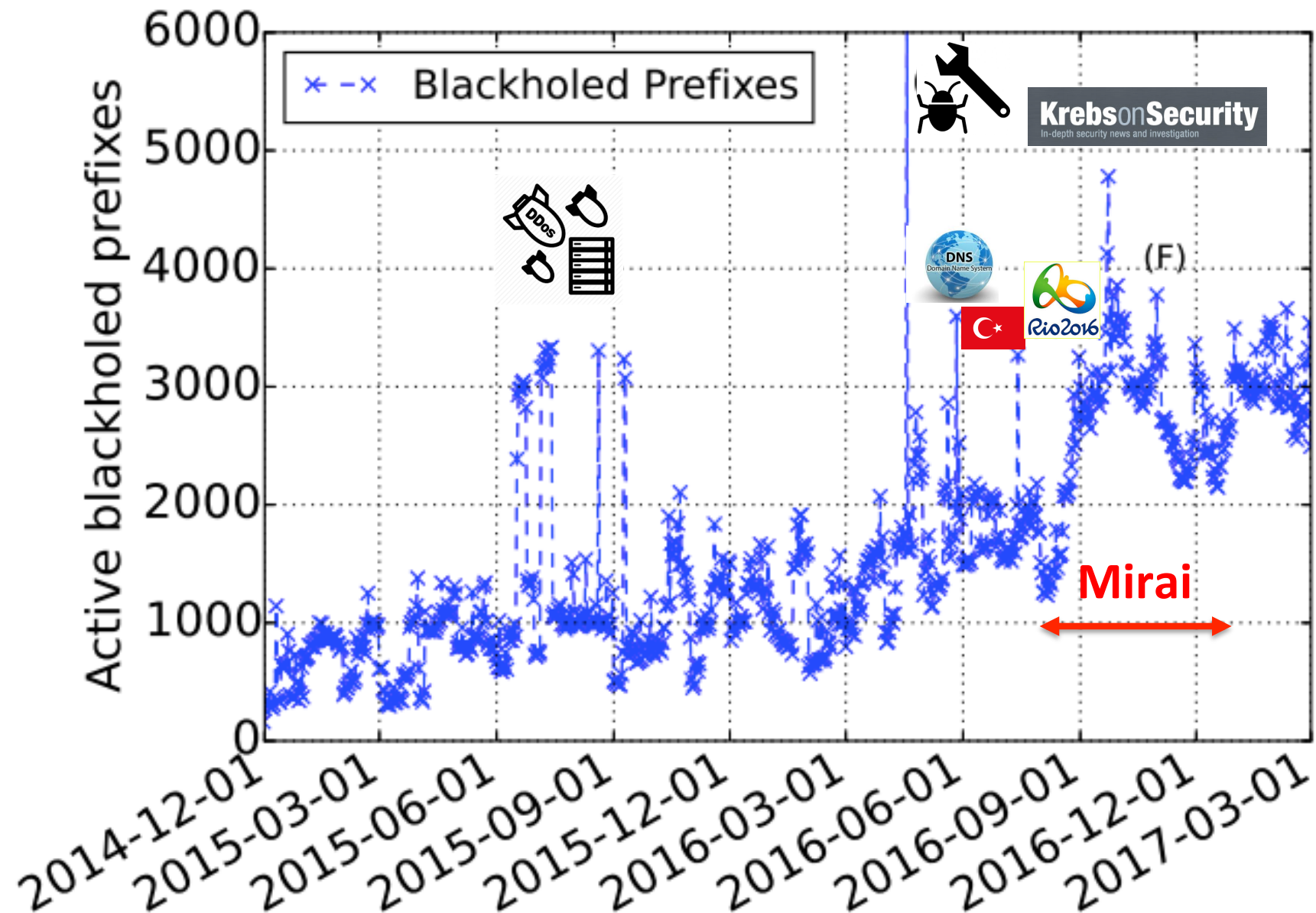
The Rise of BGP Blackholing



The Rise of BGP Blackholing



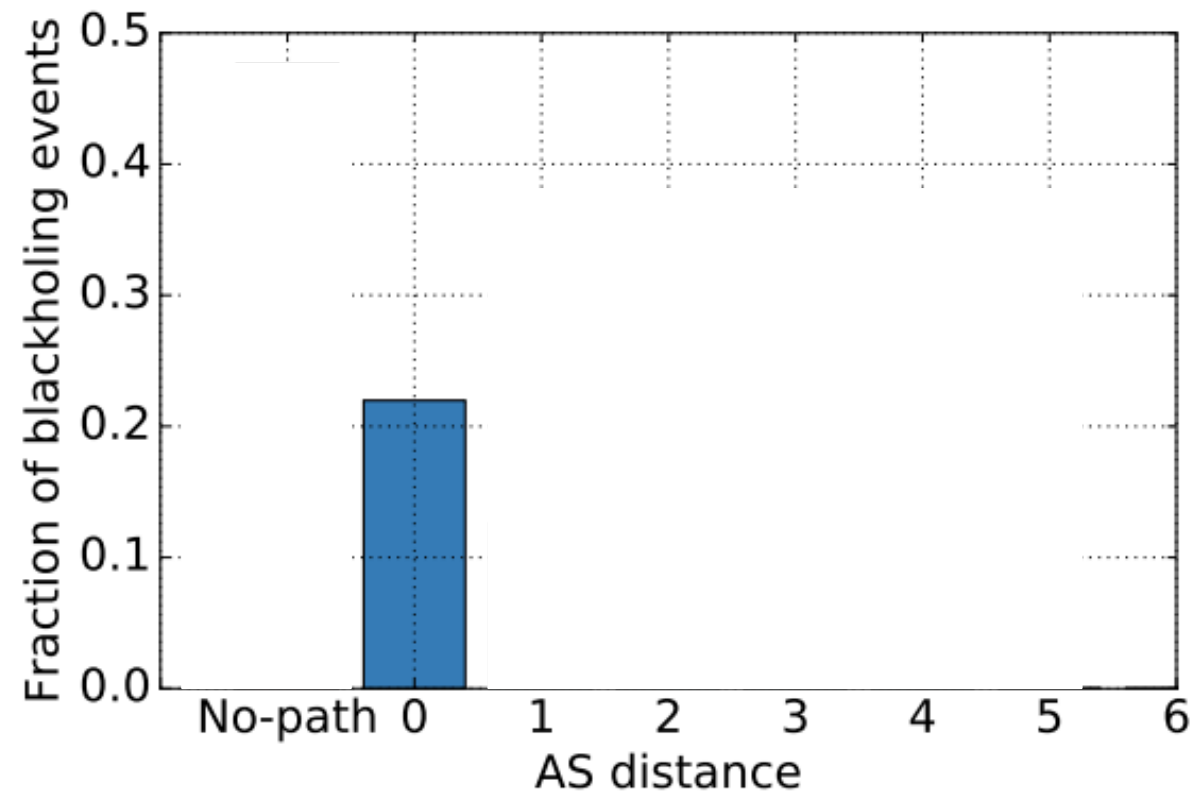
The Rise of BGP Blackholing



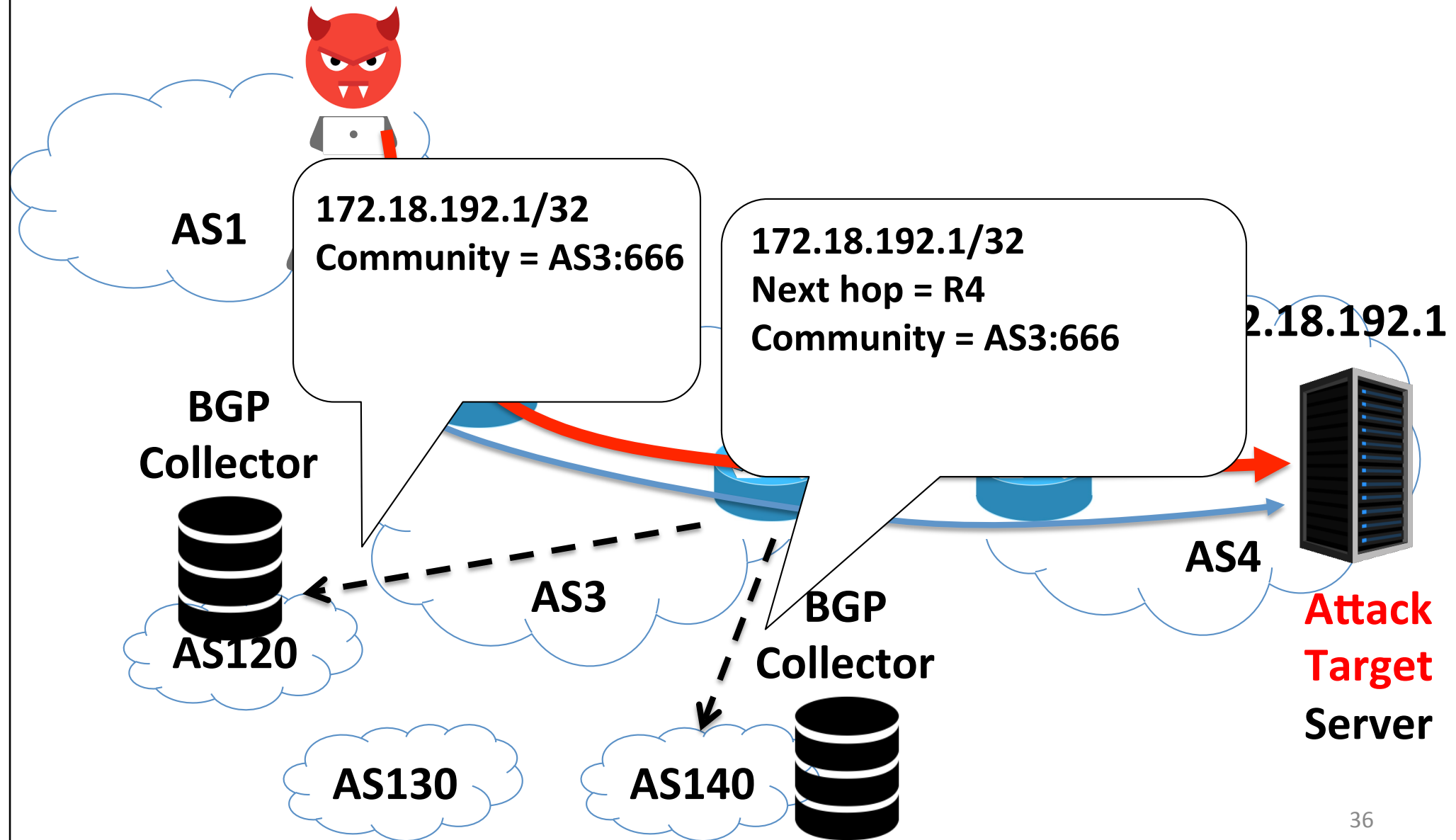
Agenda

- BGP Blackholing in Detail
- Inference Methodology for BGP Blackholing
- Trends in BGP Blackholing Activity
- **Visibility of BGP Blackholing**
- BGP Blackholing Network Efficacy
- Profile of BGP Blackholing Adopters

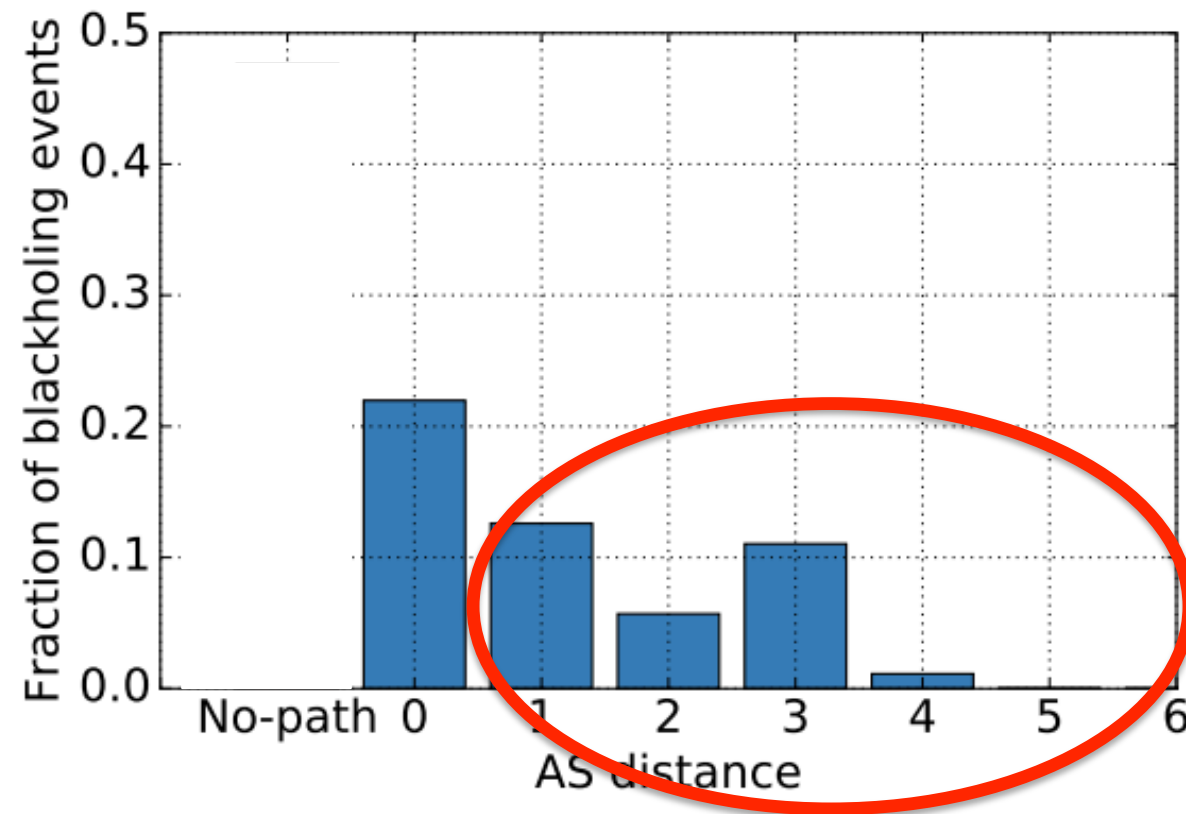
BGP Blackholing Inference Statistics



BGP Blackholing Propagation

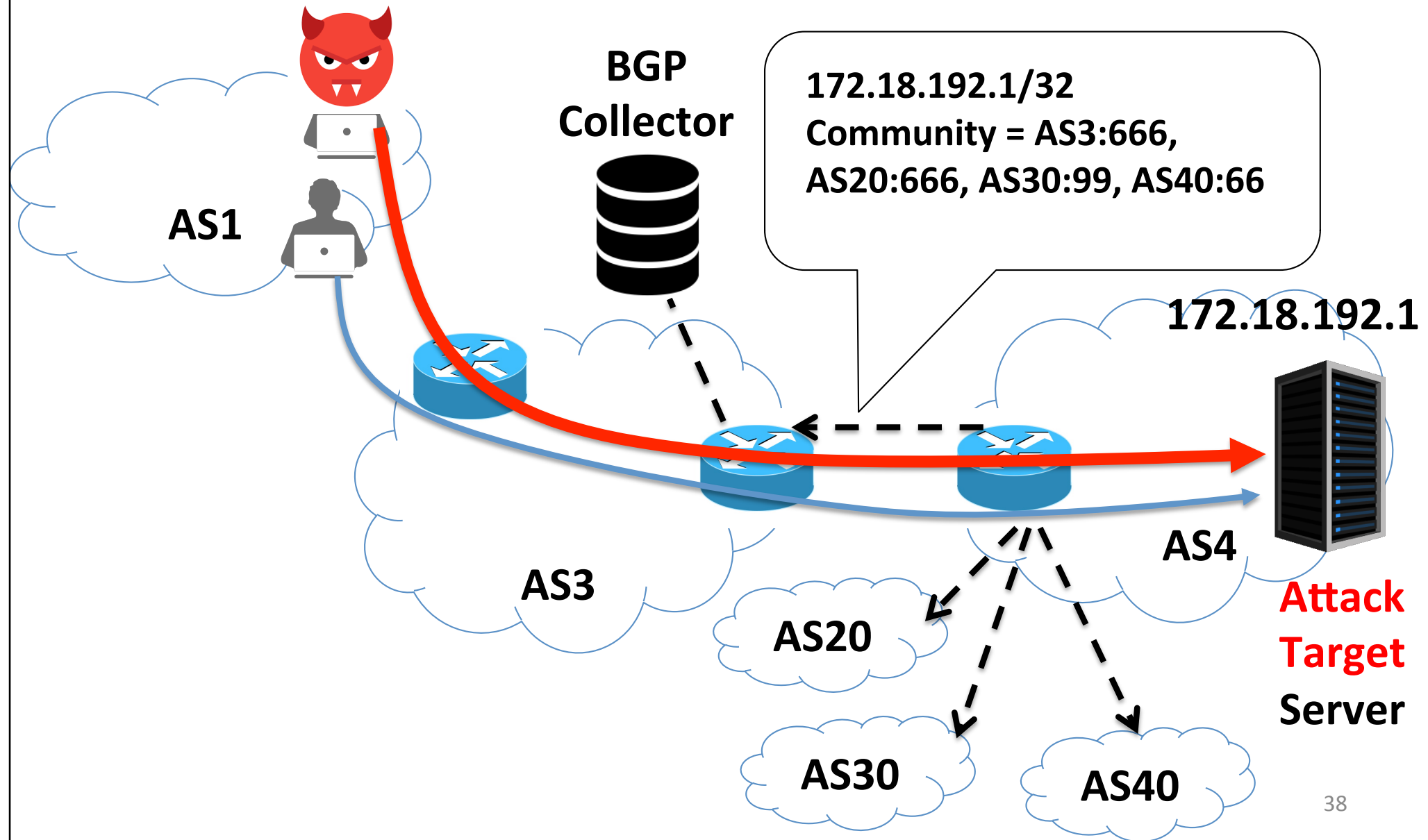


BGP Blackholing Inference Statistics

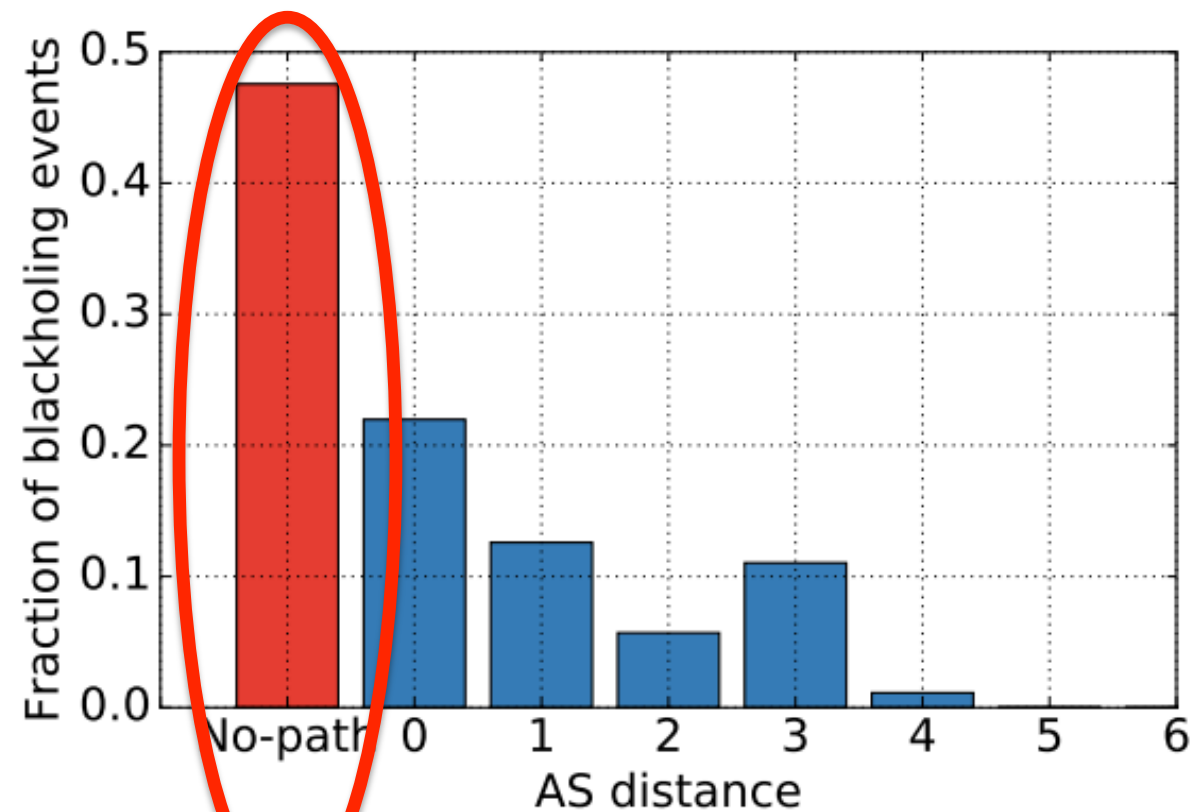


**Due to Blackholing
Propagation**

BGP Blackhole Bundling



BGP Blackholing Inference Statistics

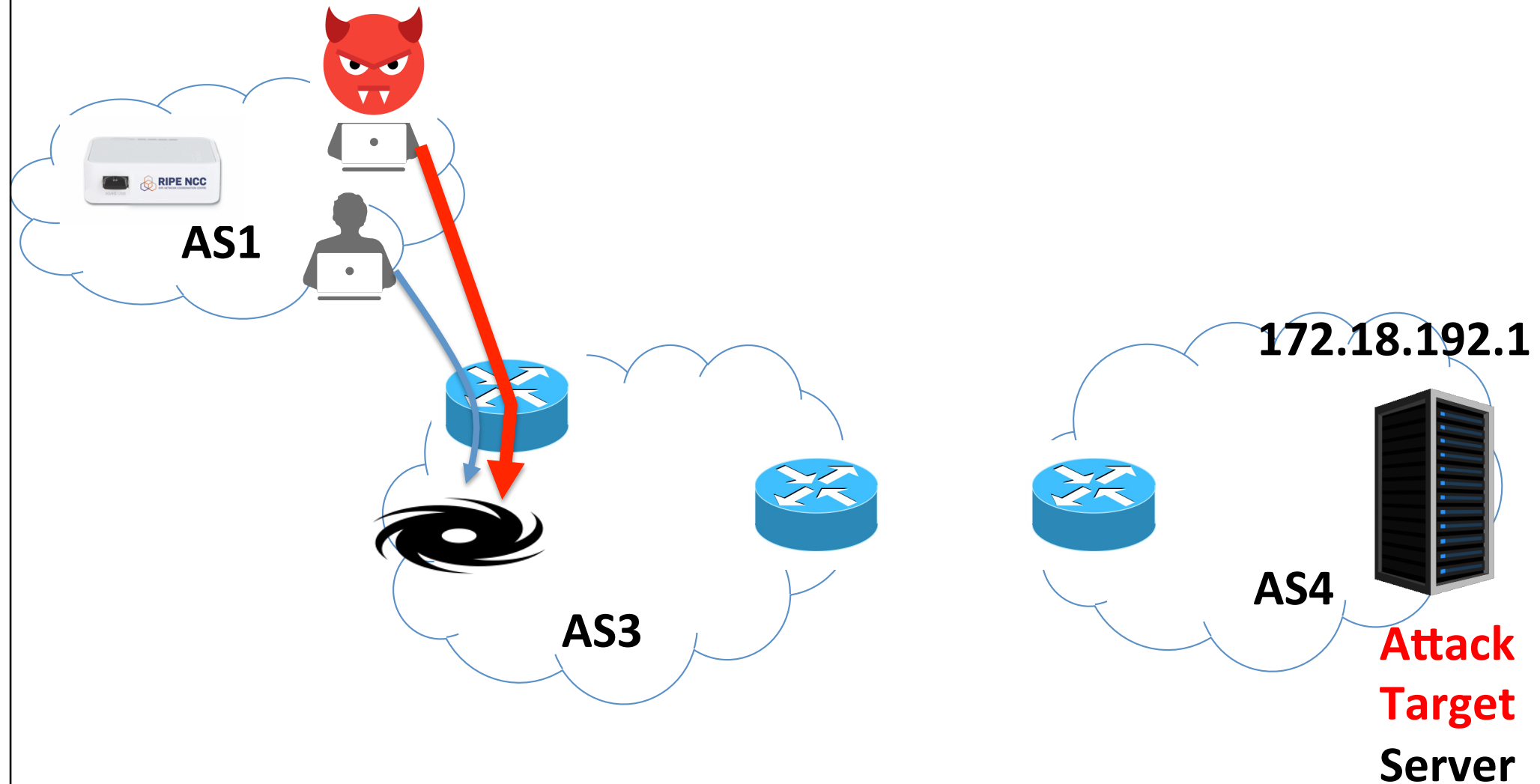


**Due to Blackholing
Bundling**

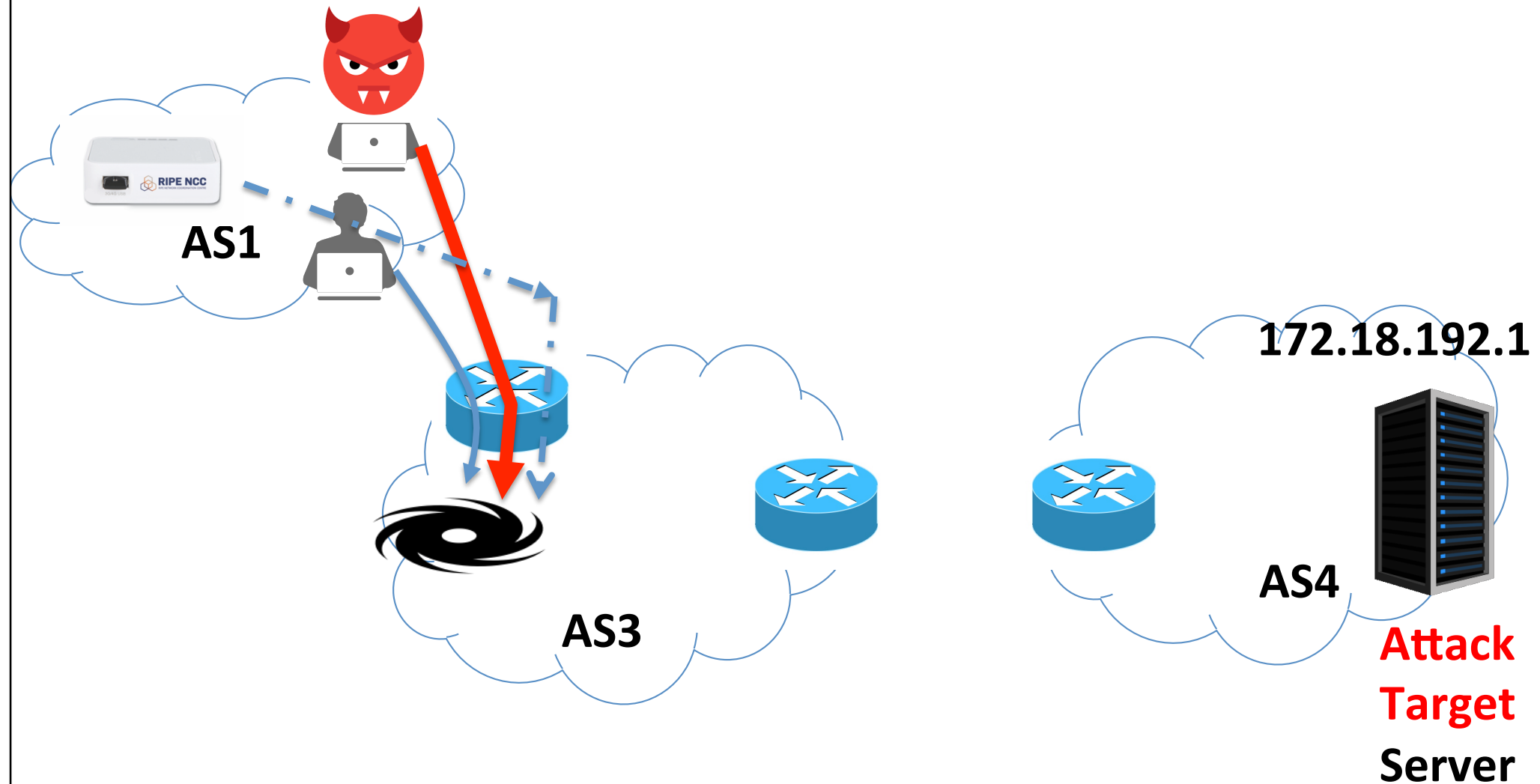
Agenda

- BGP Blackholing in Detail
- Inference Methodology for BGP Blackholing
- Trends in BGP Blackholing Activity
- Visibility of BGP Blackholing
- **BGP Blackholing Network Efficacy**
- Profile of BGP Blackholing Adopters

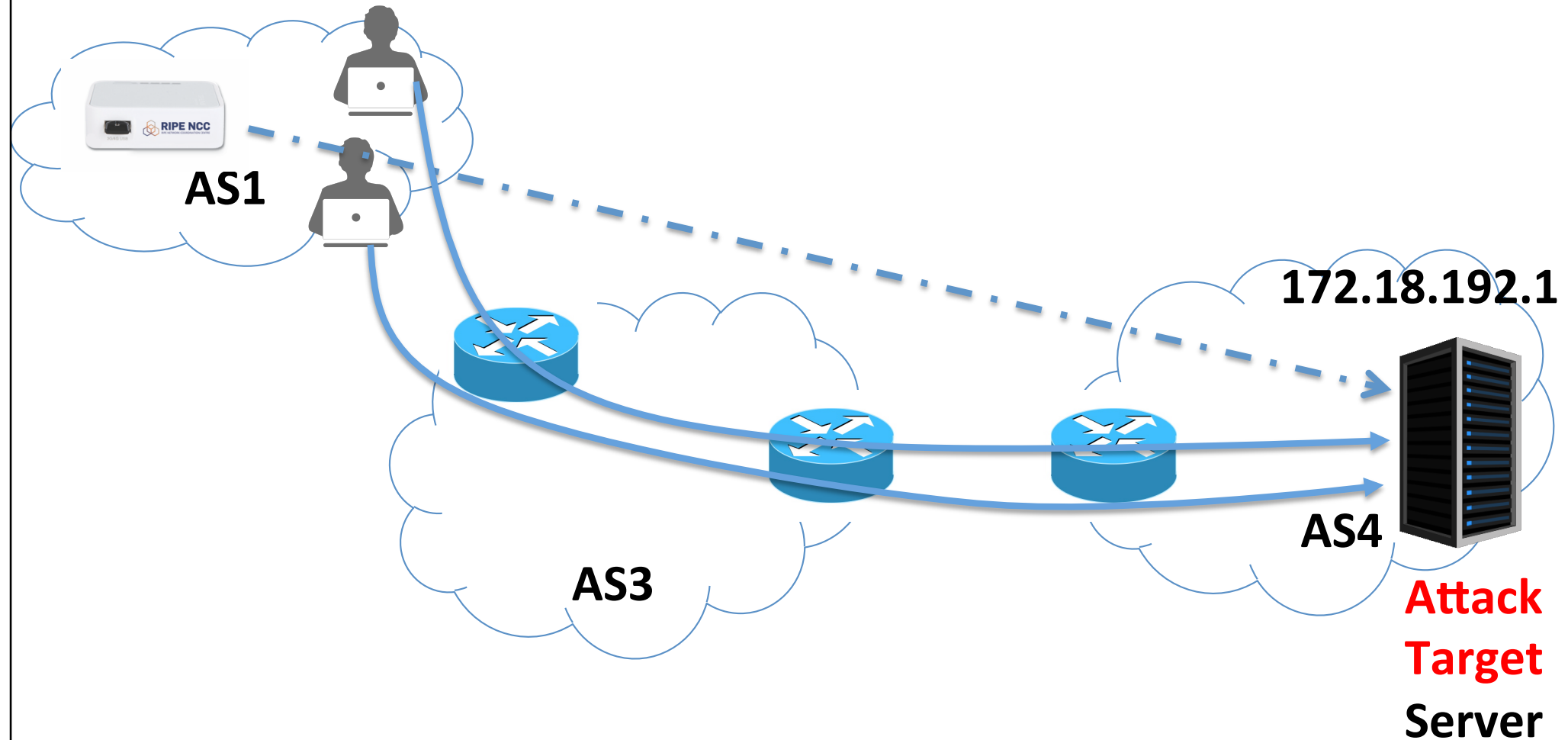
BGP Blackholing Efficacy: Active Measurements



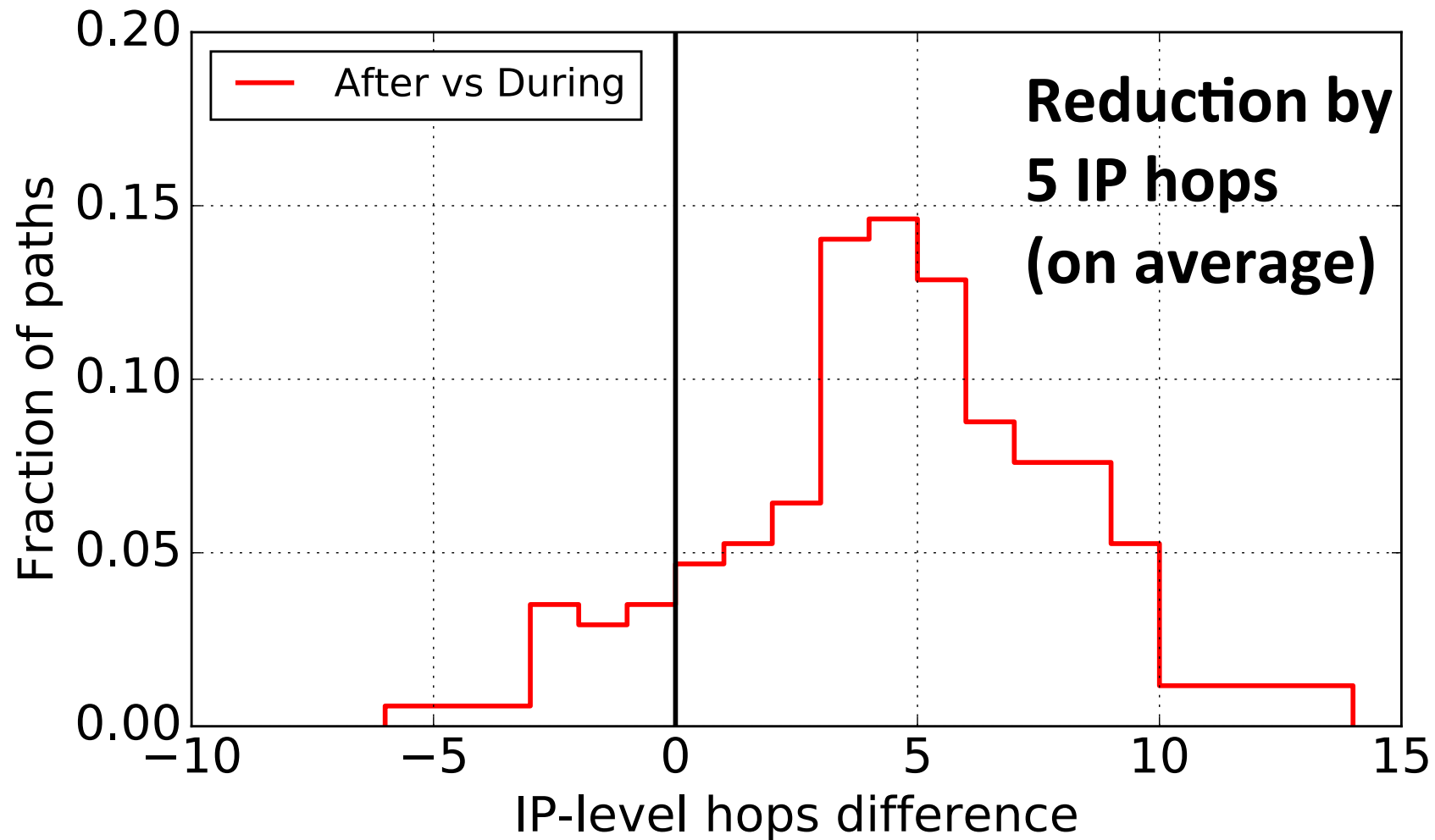
BGP Blackholing Efficacy: Active Measurements



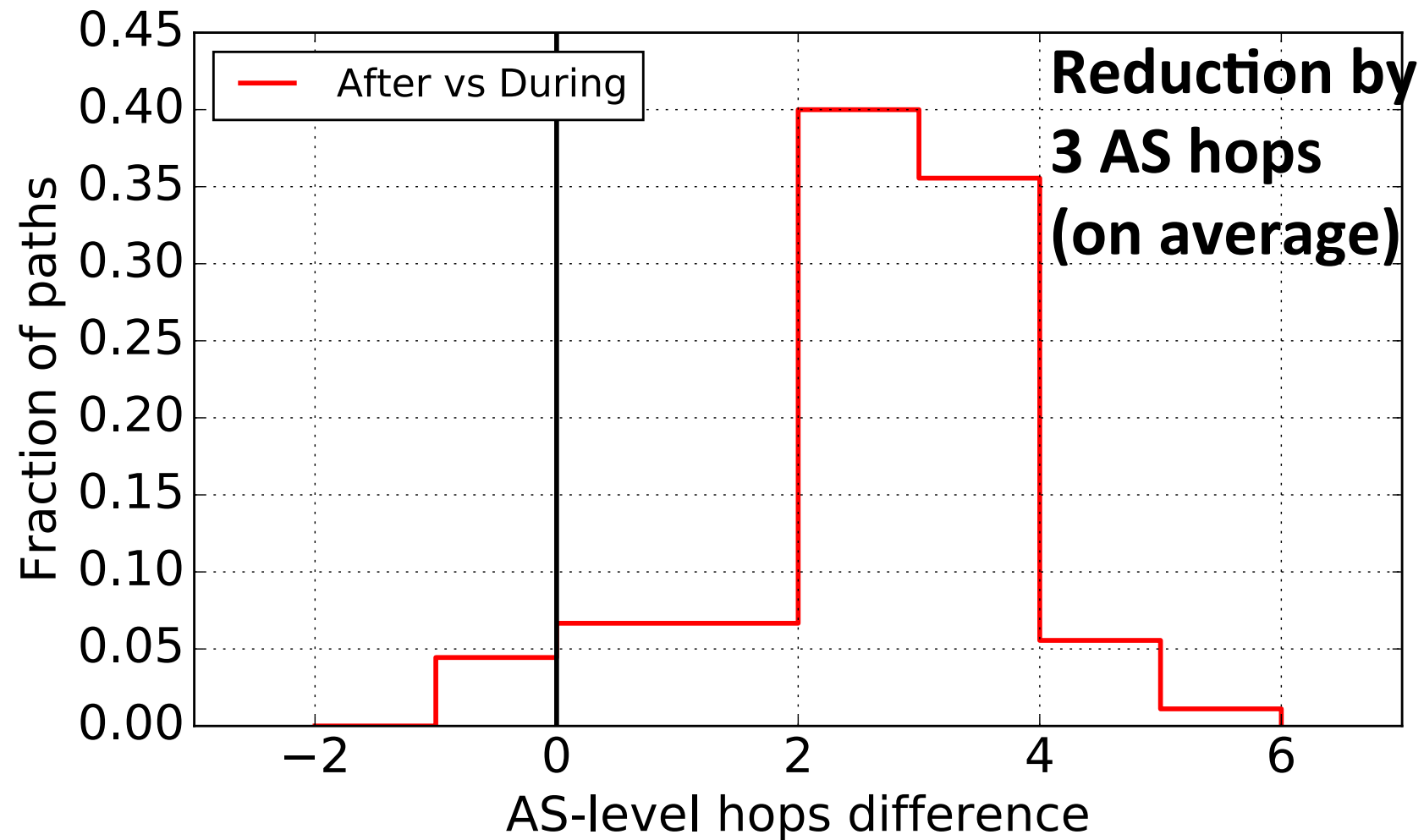
BGP Blackholing Efficacy: Active Measurements



BGP Blackholing Efficacy: Active Measurements



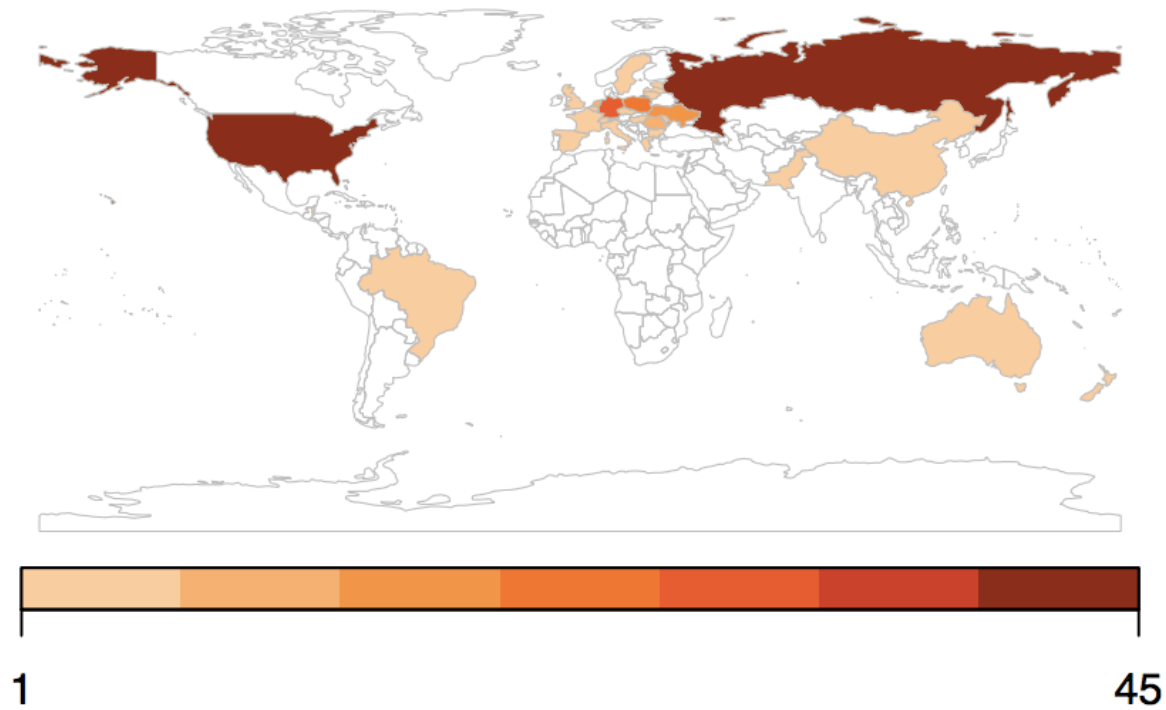
BGP Blackholing Efficacy: Active Measurements



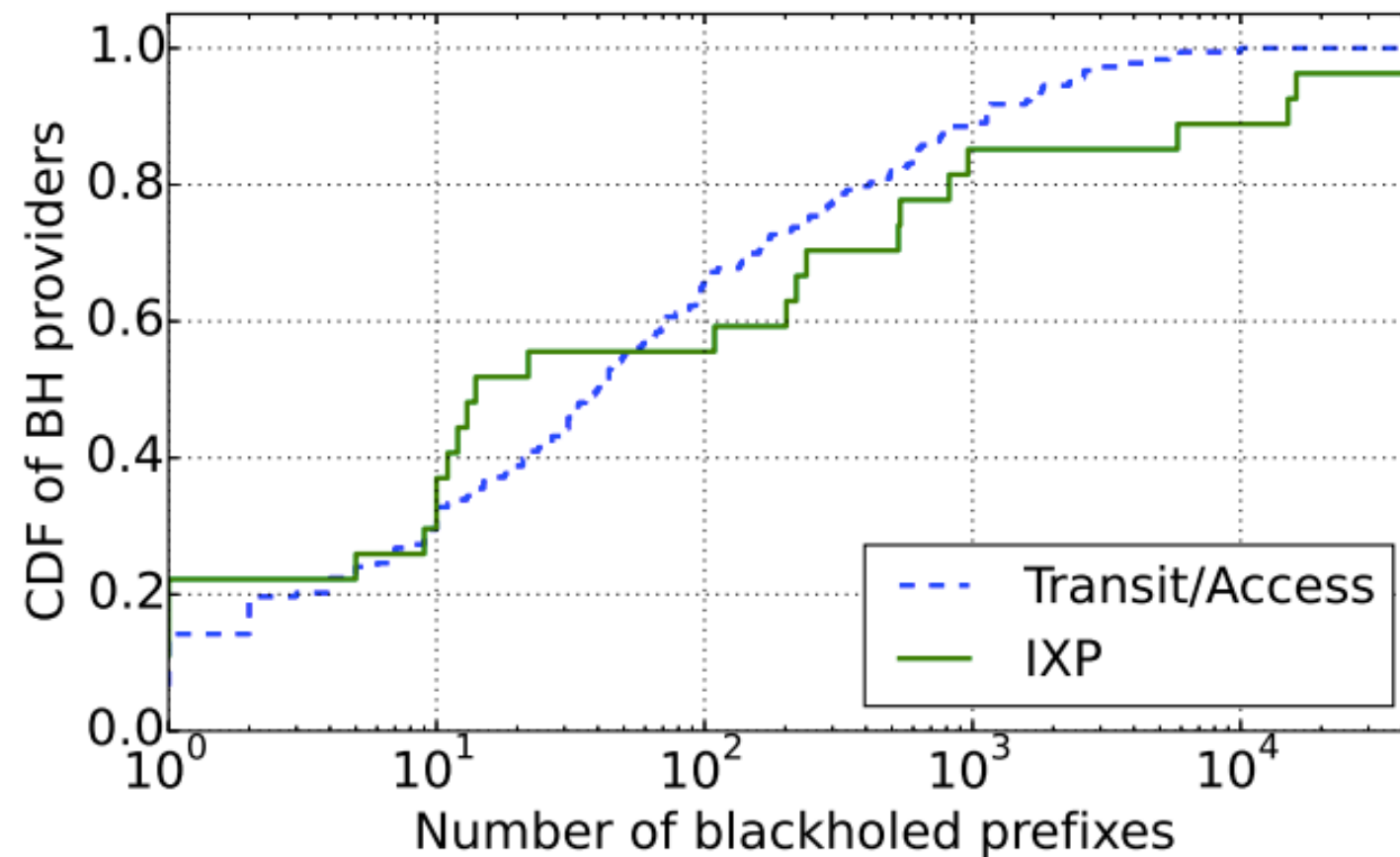
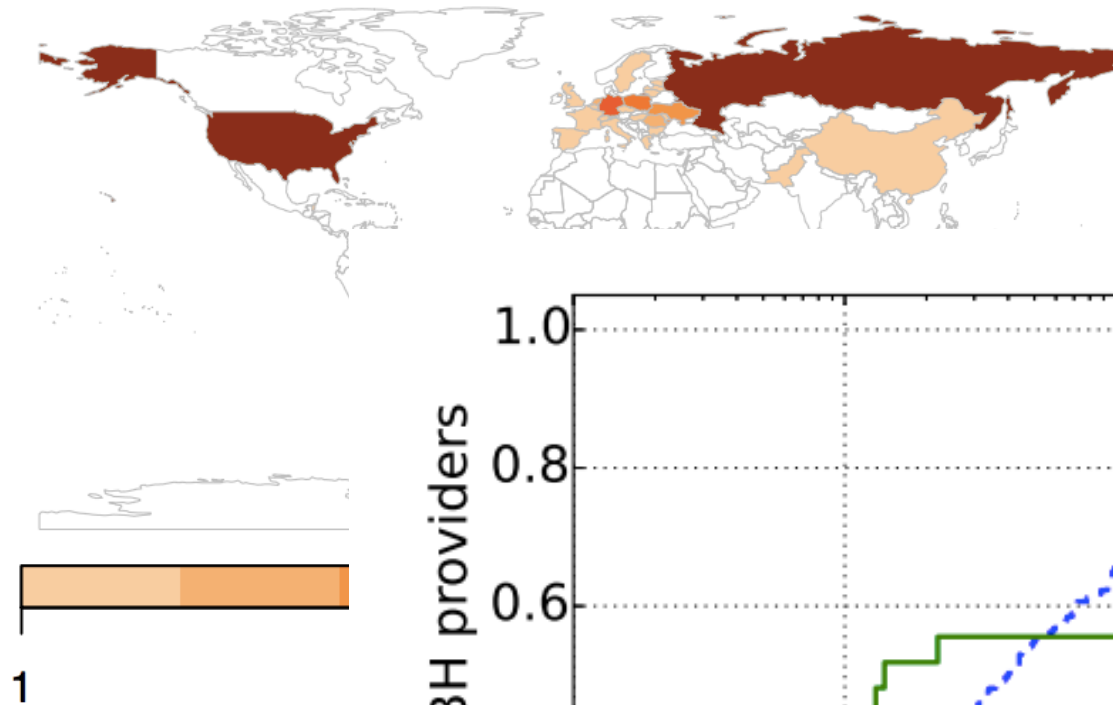
Agenda

- BGP Blackholing in Detail
- Inference Methodology for BGP Blackholing
- Trends in BGP Blackholing Activity
- Visibility of BGP Blackholing
- BGP Blackholing Network Efficacy
- **Profile of BGP Blackholing Adopters**

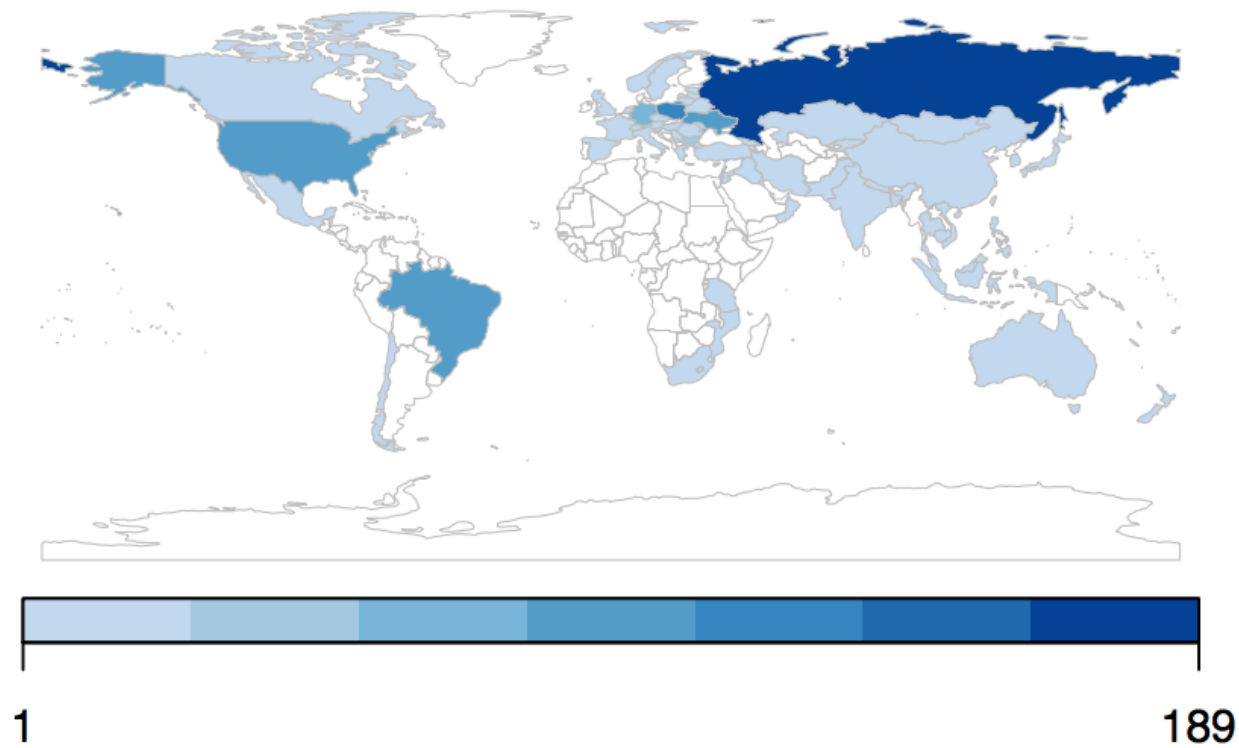
Popularity of Blackholing Providers



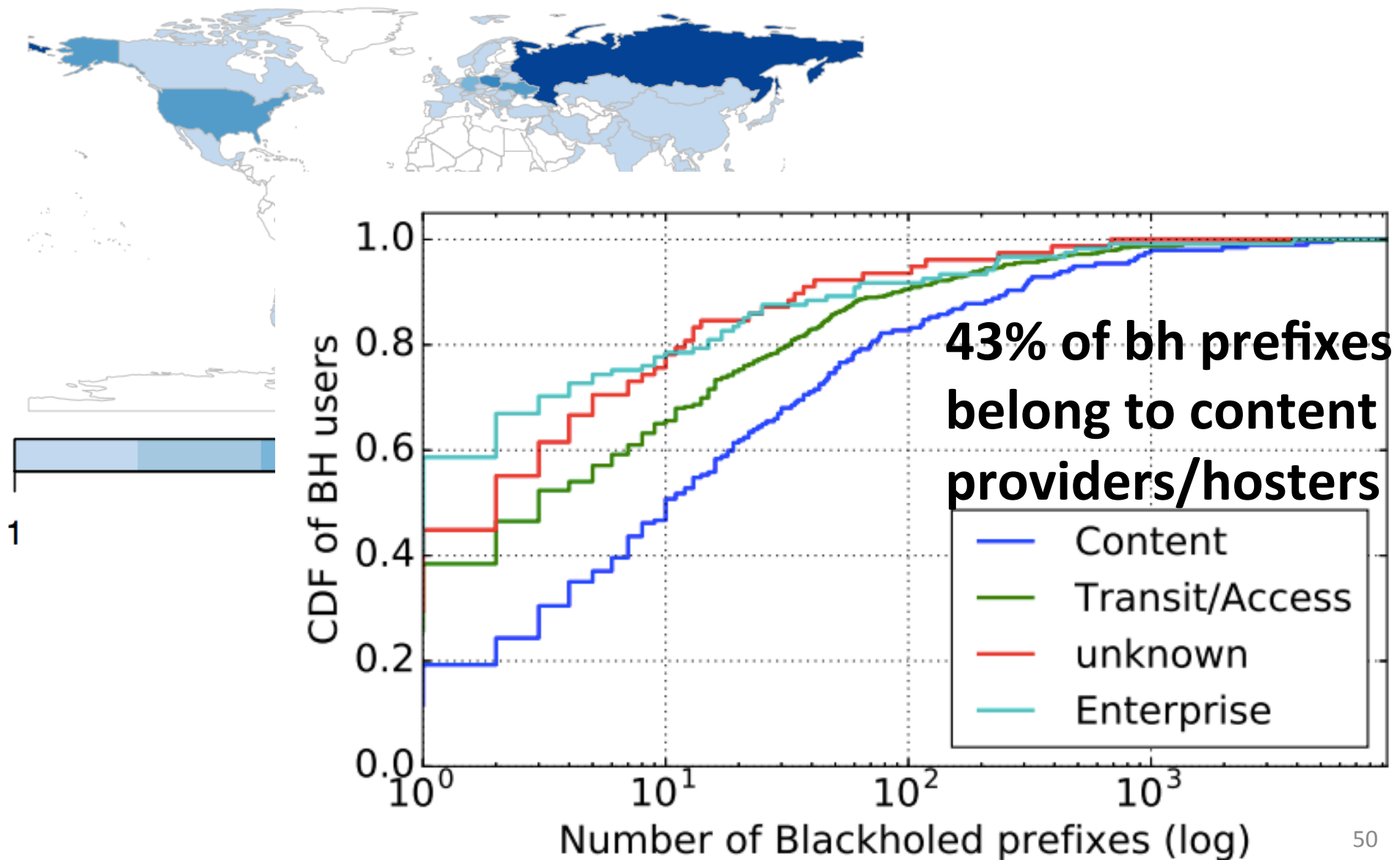
Popularity of Blackholing Providers



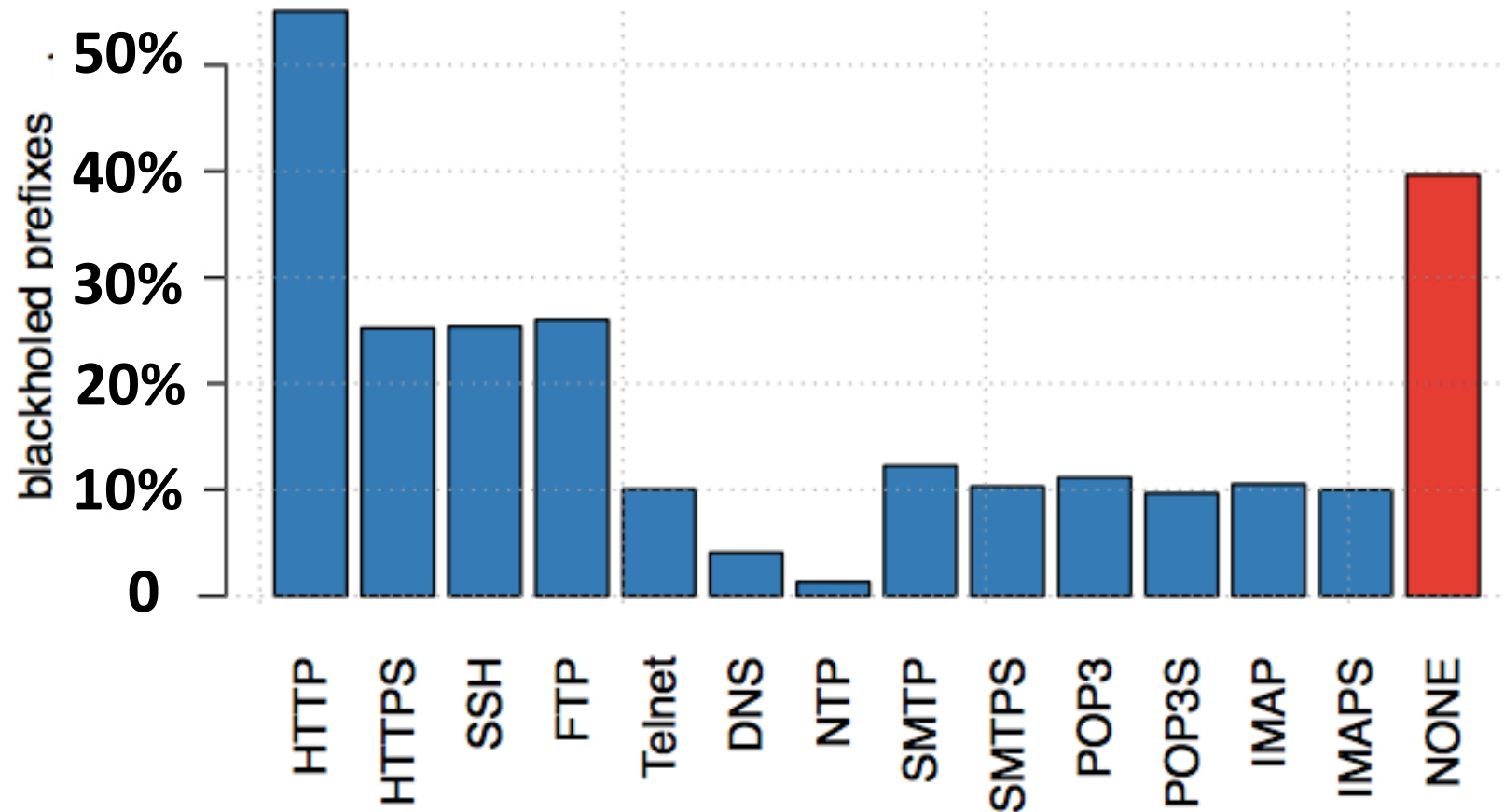
Popularity of Blackholing Users



Popularity of Blackholing Users

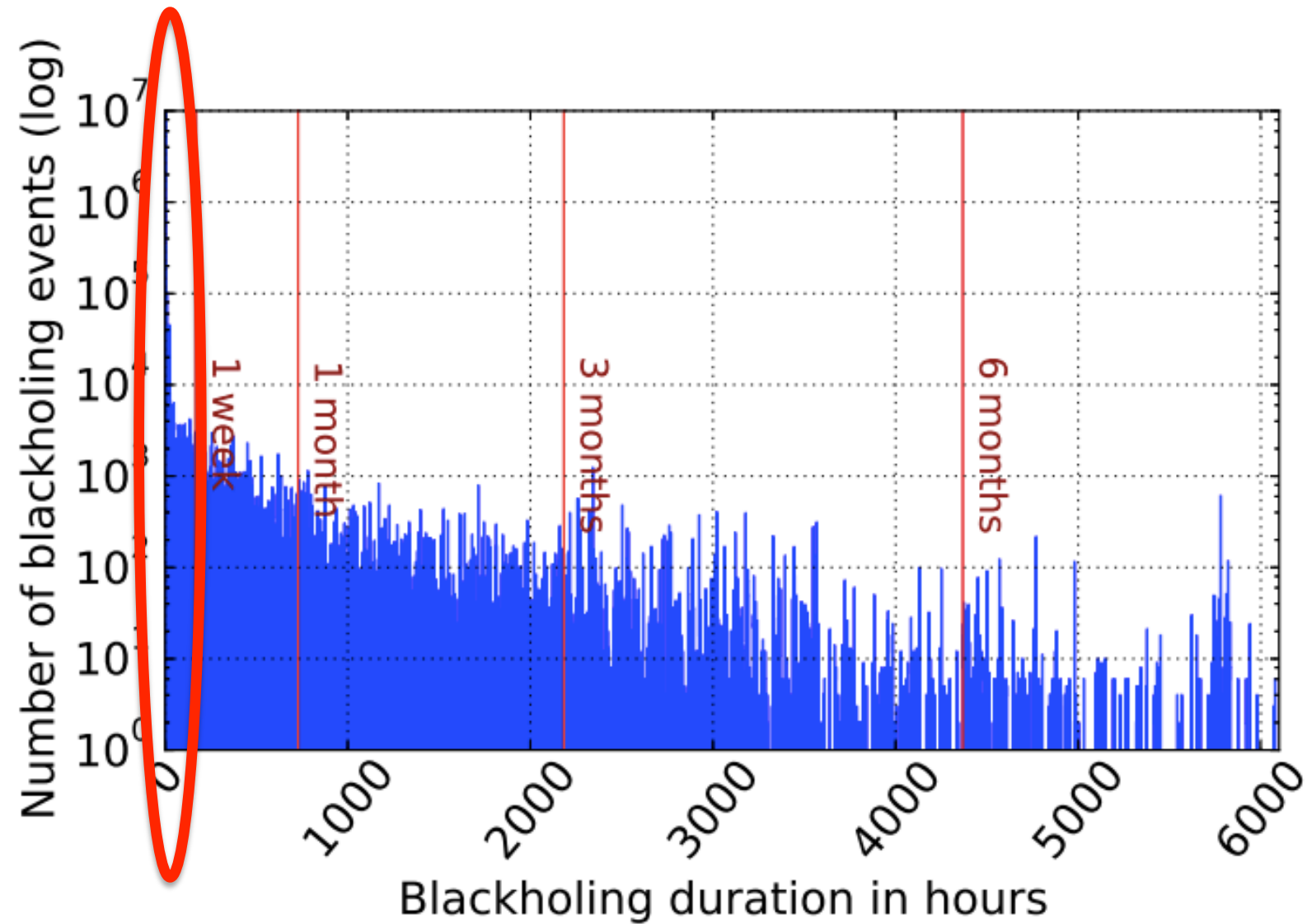


Profile of Blackholed Prefixes



- Open ports in hosts in 60% of the blackholed prefixes
- In many cases default hosting software configurations
- Serve ephemeral or low-ranked domains

BGP Blackholing Duration



Conclusion

- The first Internet-wide study on the adoption and state of BGP Blackholing
- Methodology to infer Blackholing activity from BGP data
- BGP Blackholing is on the rise in all three metrics (Providers, Users, Prefixes)
- BGP Blackholing is effective in dropping traffic early
- Profile of Blackholed adopters and Insights on Usage

Thank you!