Three Years in the Life of the Spoofer Project

Matthew Luckie, Ken Keys, Ryan Koga,
Robert Beverly, kc claffy

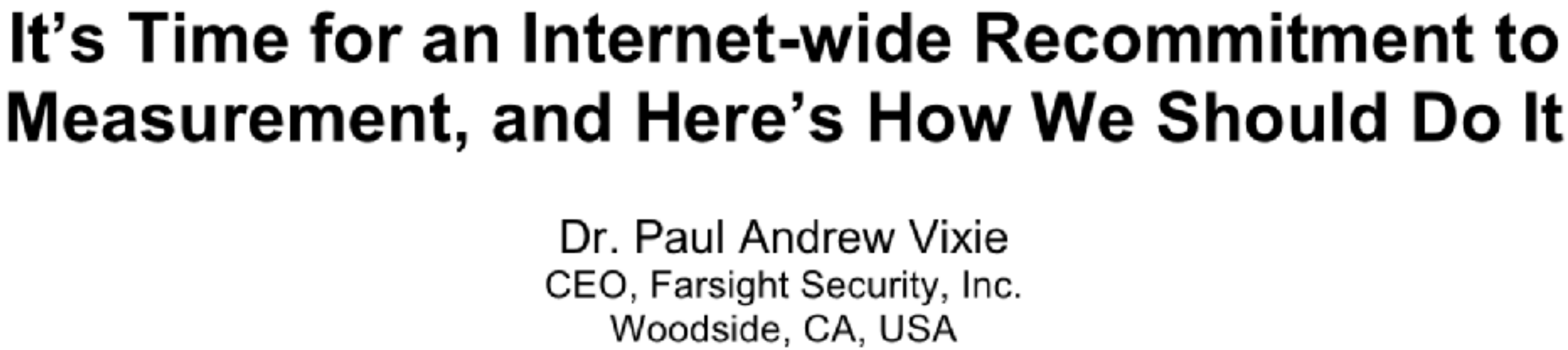
https://spoofer.caida.org/

WTMC, August 20th 2018

Pitch

- Measurement enables solutions to fundamentally non-technical security problems
  - Peer pressure
  - Industry standards (common practices)
  - Regulation
- Whatever the solution is, it cannot be effective without rigorous, publicly observable measurement

Flashback: WTMC 2016 keynote



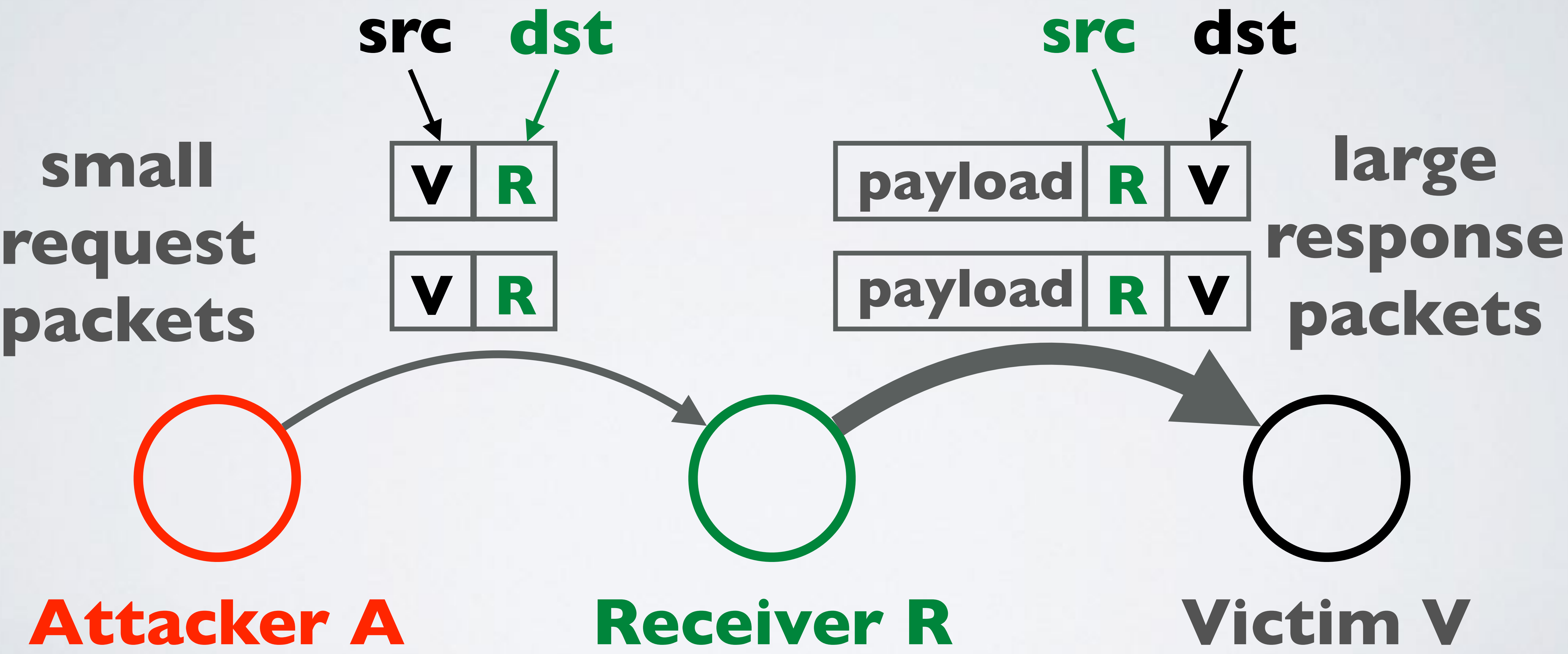
It’s Time for an Internet-wide Recommitment to Measurement, and Here’s How We Should Do It

Dr. Paul Andrew Vixie
CEO, Farsight Security, Inc.
Woodside, CA, USA

> “ *There has never been a greater need for comprehensive Internet metrics than now. Even basic security-critical facts about the Internet, such as “How many systems are botted?” or “**What networks still don’t do Source Address Validation?**” remain murky and poorly quantified.* ”

Why does SAV matter?

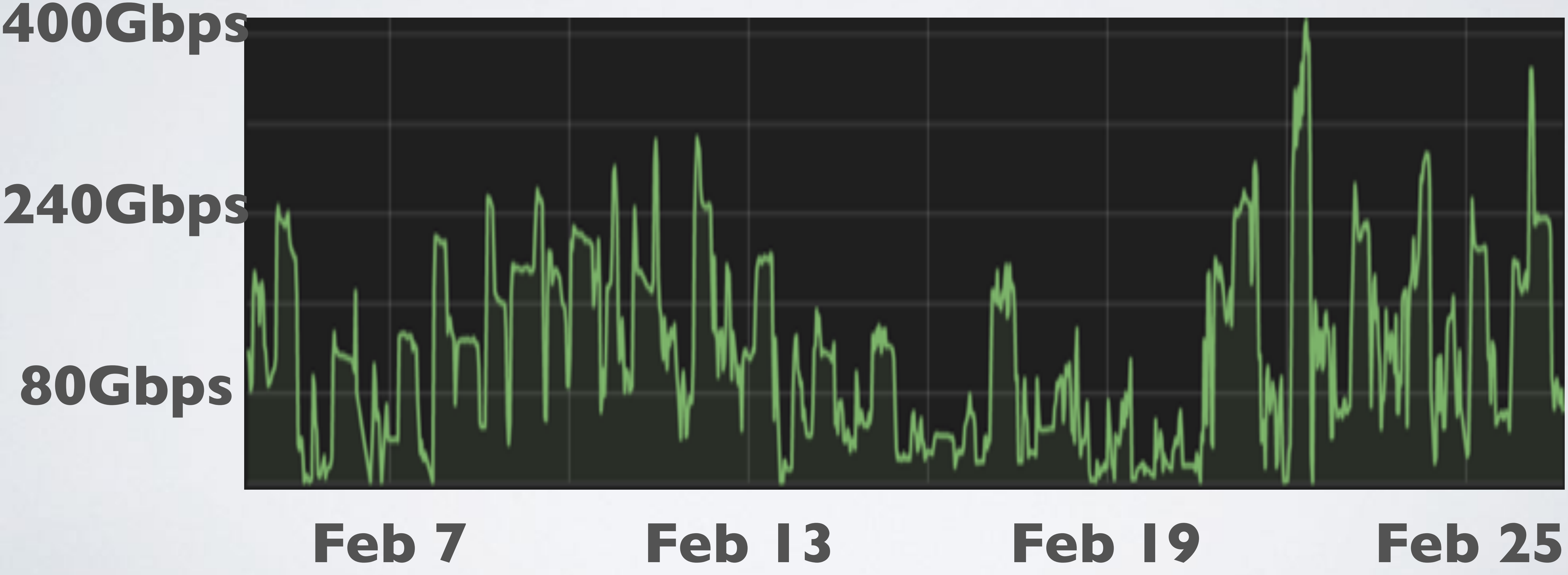
- Attacker sends packet with spoofed source IP address
- Receiver cannot always know if packet's source is authentic



Volumetric Reflection-Amplification Attack

Why does SAV matter?

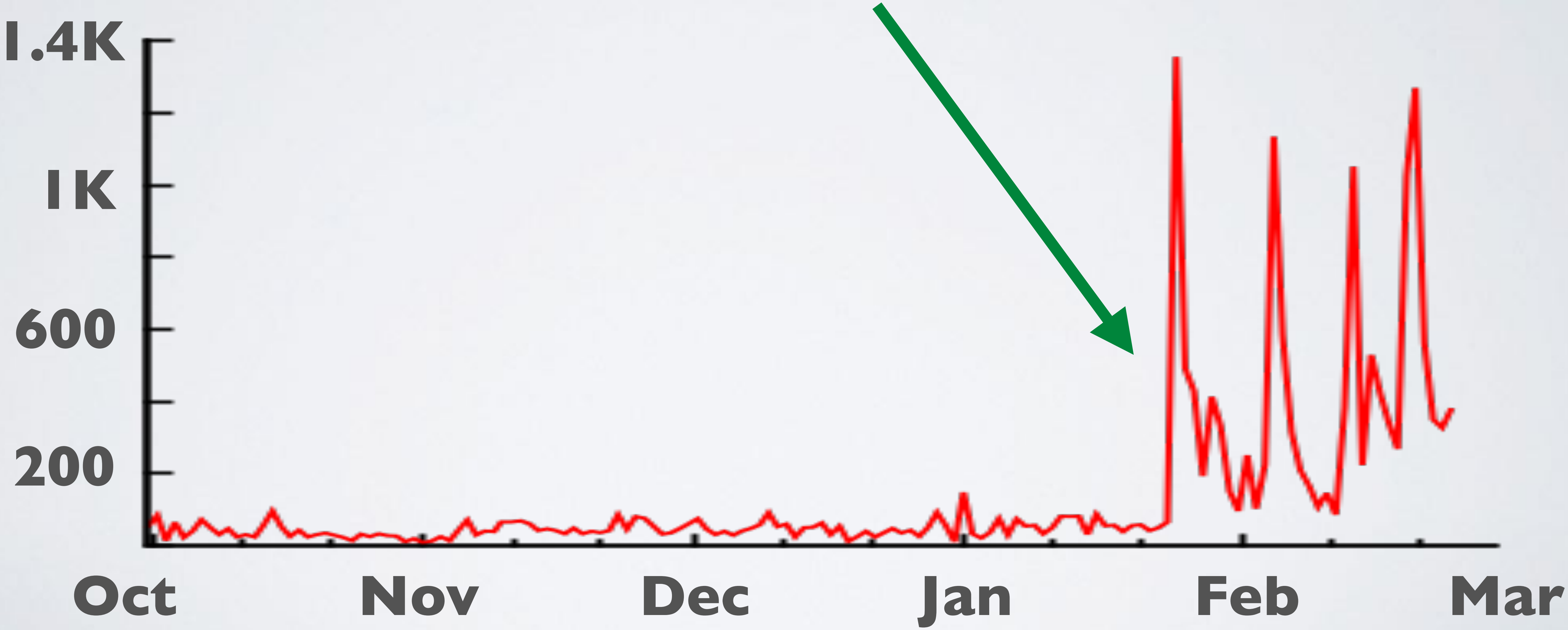
- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **400Gbps** attacks on their systems through 2016; GitHub a **1.7Tbps** attack in 2018



https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

Why does SAV matter?

- Lack of filtering allows anonymous denial of service attacks.
- Example: CloudFlare reports **>1K DoS attack events** on their systems, per day, starting **Feb 2016**



https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

Why does SAV matter?

- Impossible to prevent people from accidentally opening up new amplification vectors, or attackers using them
- We must instead make the infrastructure resilient to these natural human tendencies
    - 2013 DNS: 300 Gbps against Spamhaus
    - 2014 NTP: 400 Gbps against Cloudflare
    - 2018 memcached: 1.7 Tbps attack against GitHub
- Not enough to just measure SAV deployment;
  need to encourage remediation and change in behavior

Defenses

- **BCP38**: Network ingress filtering: defeating denial of service attacks which employ IP Source Address Spoofing
  - https://tools.ietf.org/html/bcp38
  - May 2000
- **BCP84**: Ingress filtering for multi-homed networks
  - https://tools.ietf.org/html/bcp84
  - March 2004
  - Not always straightforward to deploy "source address validation" (SAV): BCP84 provides advice how to deploy

The Spoofer Project

- A DHS-funded crowd-sourced effort (2015-present) to measure SAV deployment in the Internet
    - Project started by Robert Beverly while MIT student (2005)
    - Measures ISP filtering practices for packets with spoofed source IP addresses
- Important security issue in the Internet to measure, but a project that faces incentive issues everywhere

https://spoofer.caida.org/

Incentive Issues everywhere

- Incentive incompatible problem for
  - Research Community
  - Crowd-sourcing Volunteers
  - Network Operators
  - Funding Agencies

Incentive Issues: Research Community

- SAV measurement has a high cost of entry compared measuring DNSSEC deployment, or TLS properties
  - SAV requires a Vantage Point in a network of interest
- Hard to get an Internet-wide sample to publish on SAV
  - Inevitable questions about sample bias

Incentive Issues: Volunteers

- To obtain an Internet-wide view, we rely on volunteers installing measurement software on their computer
- Few volunteers are likely to have been the victim of an attack relying on ability to spoof, or could individually contribute in a significant way

> “*If we want the public to embrace Internet measurement activities, they will need to be made aware of its importance, and the potential role that the public can play in collecting and reporting data using standardized tools.*”
>
> — Paul Vixie, WTMC 2016

Incentive Issues: Network Operators

- Deploying source address validation is **primarily for the benefit of other networks**
- **Incentive not clear for some networks**
  - majority of networks do seem to deploy filtering
  - filtering gives an operator moral high-ground to pressure other networks to deploy, which does benefit the operator
  - "Cyber Insurance" takes into account security practice of the network
- ISOC RoutingManifesto.org: Mutually Agreed Norms for Routing Security (MANRS)

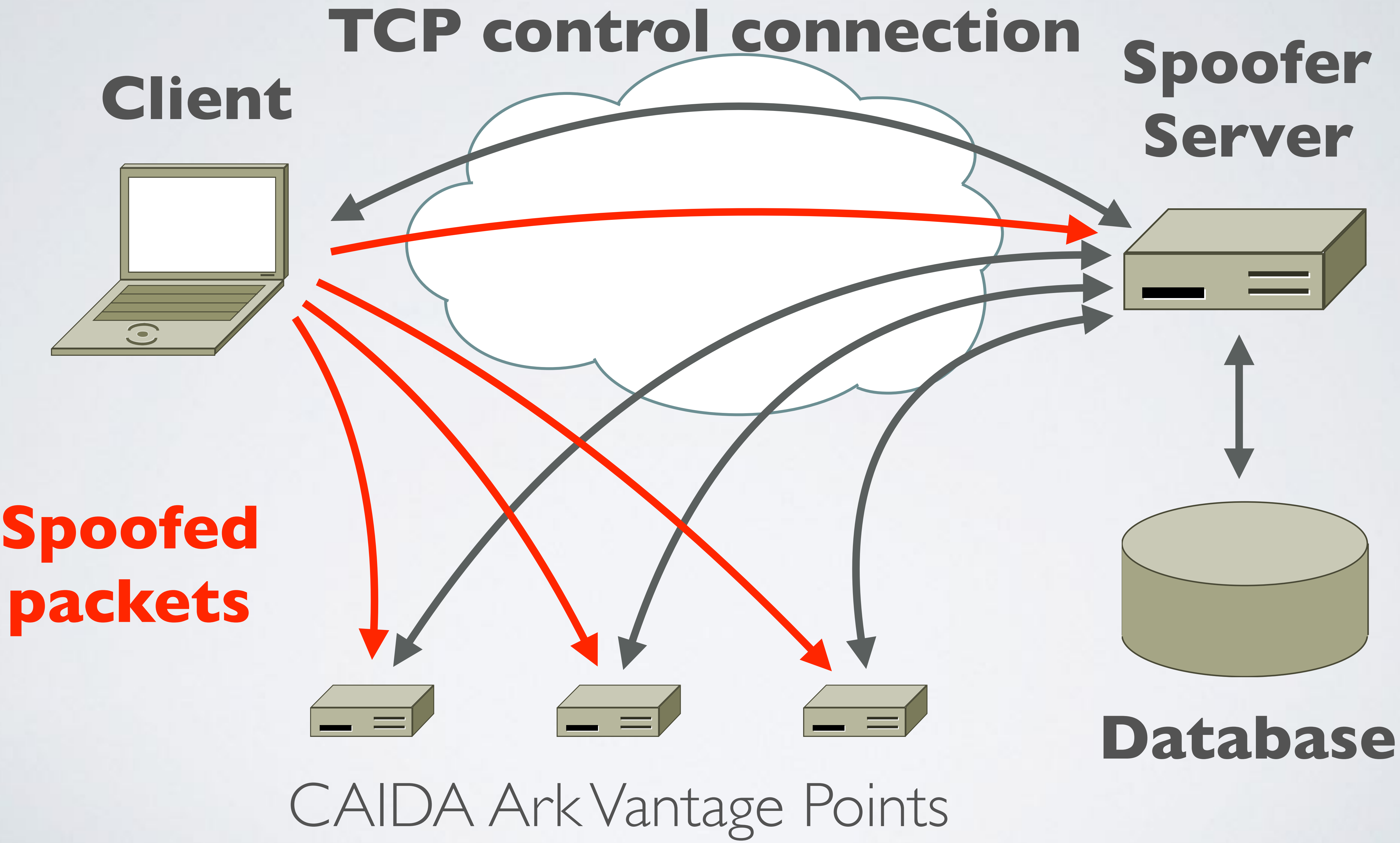
Incentive Issues: Funding Agencies

- SAV is a global problem; typically individual governments provide funding obtained from their nation's taxpayers
  - Need to have impact for a project to continue to receive funding
  - Limited commercialization opportunities for SAV measurement
- Class of public health task, but computer security doesn't have that

Three Years in the Life of Spoofer

- **Data Collection:** we built a new software system for collecting crowd-sourced SAV measurements
- **Data Reporting:** we built a public-facing website for reporting test outcomes
- **Remediation**: we privately contact network operators, and send geographically-scoped emails to network operator mailing lists

Spoofer: Client/Server Overview



Spoofer Client Overview

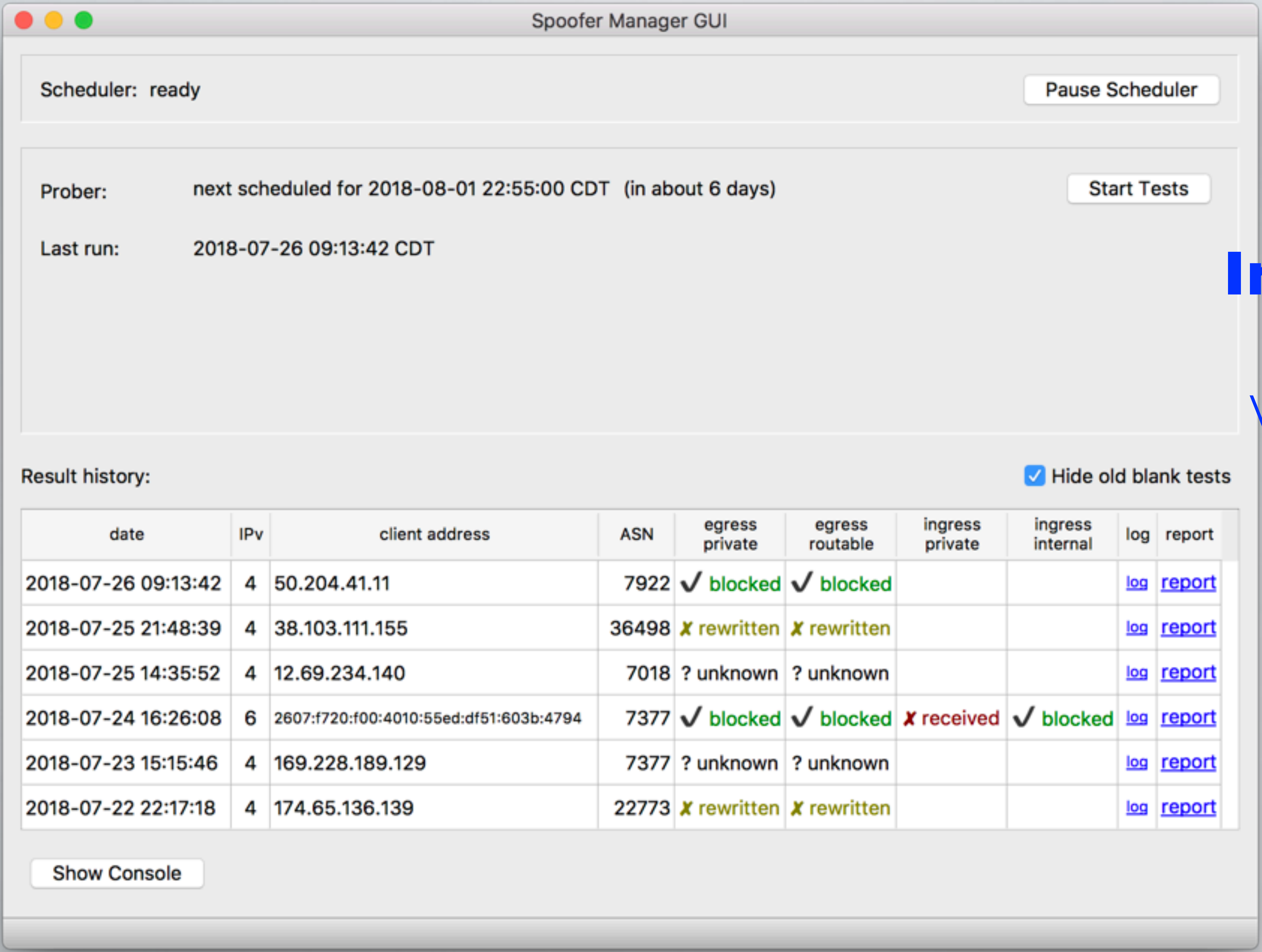
- Client tests ability to spoof packets of different types
  - Routed and Private addresses
  - IPv4 and IPv6
  - Leaving and Entering the network hosting the client
- **`traceroute`** to infer forward path to destinations
- **`tracefilter`** to infer first location of filtering in a path
  - traceroute but with spoofed packets
- Filtering prefix granularity: how many addresses in the same network prefix can be spoofed?

Spoofer Client Overview

- **opt-in** to publicly share anonymized results, and **opt-in** to share unanonymized results for remediation
- **Automatically tests networks** the host is attached to, once per week, by running in the background
- **GUI** to browse test results from your host, and schedule tests
- **Speed improvements** through parallelized probing

https://spoofer.caida.org/

Spoofer Client GUI



Scheduler: ready

Prober: next scheduled for 2018-08-01 22:55:00 CDT (in about 6 days)

Last run: 2018-07-26 09:13:42 CDT

Result history:

☑ Hide old blank tests

date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-07-26 09:13:42	4	50.204.41.11	7922	✓ blocked	✓ blocked			log	report
2018-07-25 21:48:39	4	38.103.111.155	36498	✗ rewritten	✗ rewritten			log	report
2018-07-25 14:35:52	4	12.69.234.140	7018	? unknown	? unknown			log	report
2018-07-24 16:26:08	6	2607:f720:f00:4010:55ed:df51:603b:4794	7377	✓ blocked	✓ blocked	✗ received	✓ blocked	log	report
2018-07-23 15:15:46	4	169.228.189.129	7377	? unknown	? unknown			log	report
2018-07-22 22:17:18	4	174.65.136.139	22773	✗ rewritten	✗ rewritten			log	report

Signed Installers

MacOS

Windows

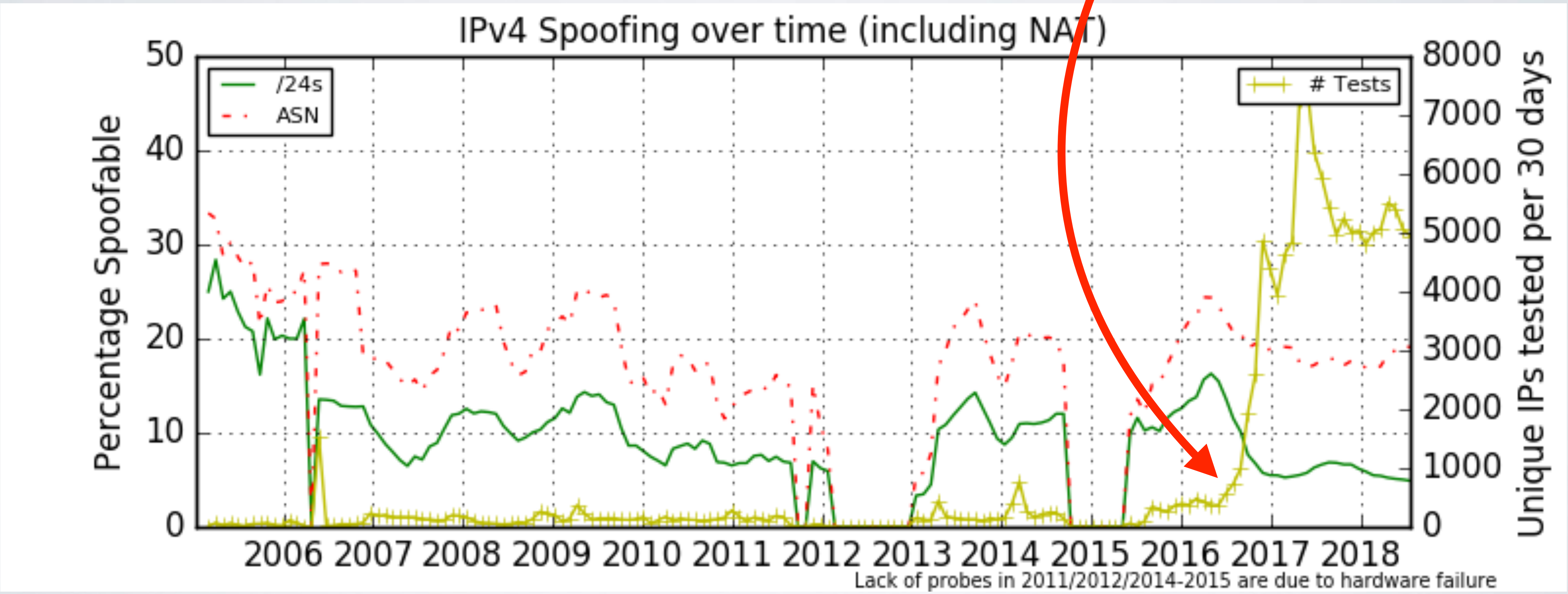
Linux

Open Source

C++

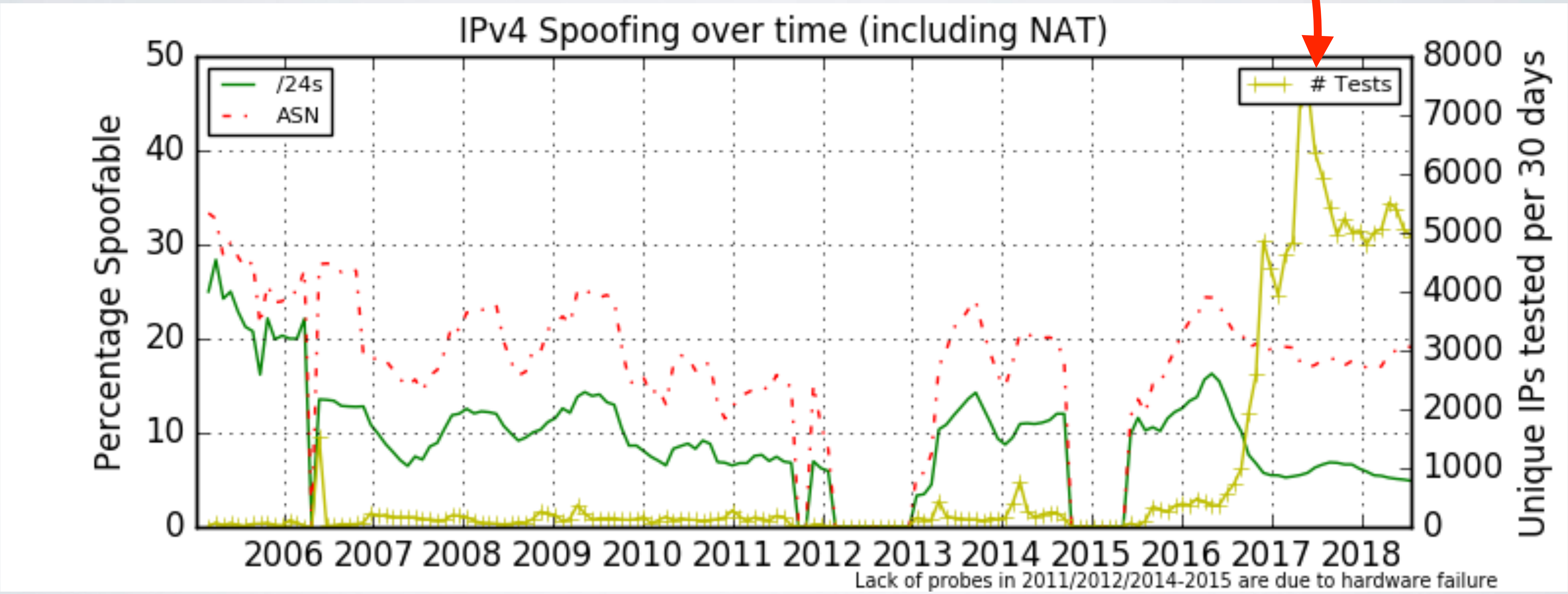
Client/Server Deployment

- Since releasing new client in May 2016, increasing trend of more tests (yellow line)
  - Benefit of system running in background



Client/Server Deployment

- Peak coincided with experiments by Qasim Lone et al. when they solicited work through Amazon Turk and similar platforms
  - TMA 2018 paper

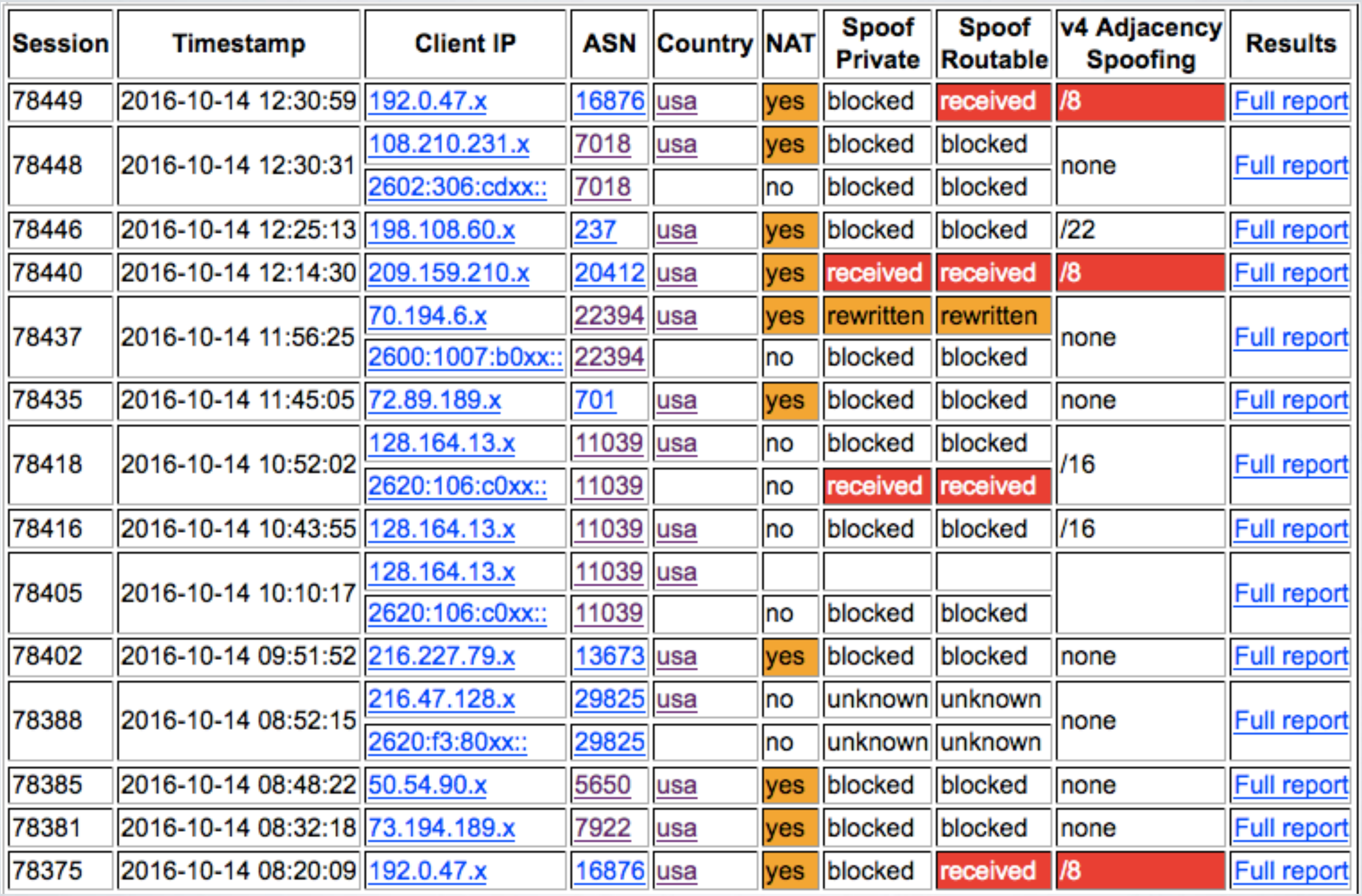


Spoofer Reporting Engine

- Publicly shows outcomes of sharable tests
- Allows users to select outcomes
  - per country: which networks in a country need attention?
  - per ASN: which subnets need attention?
  - per provider: which of my BGP customers can spoof?
- What address space does an AS announce, or could act as transit for? Is that address space stable?
  - Useful for deploying ACLs

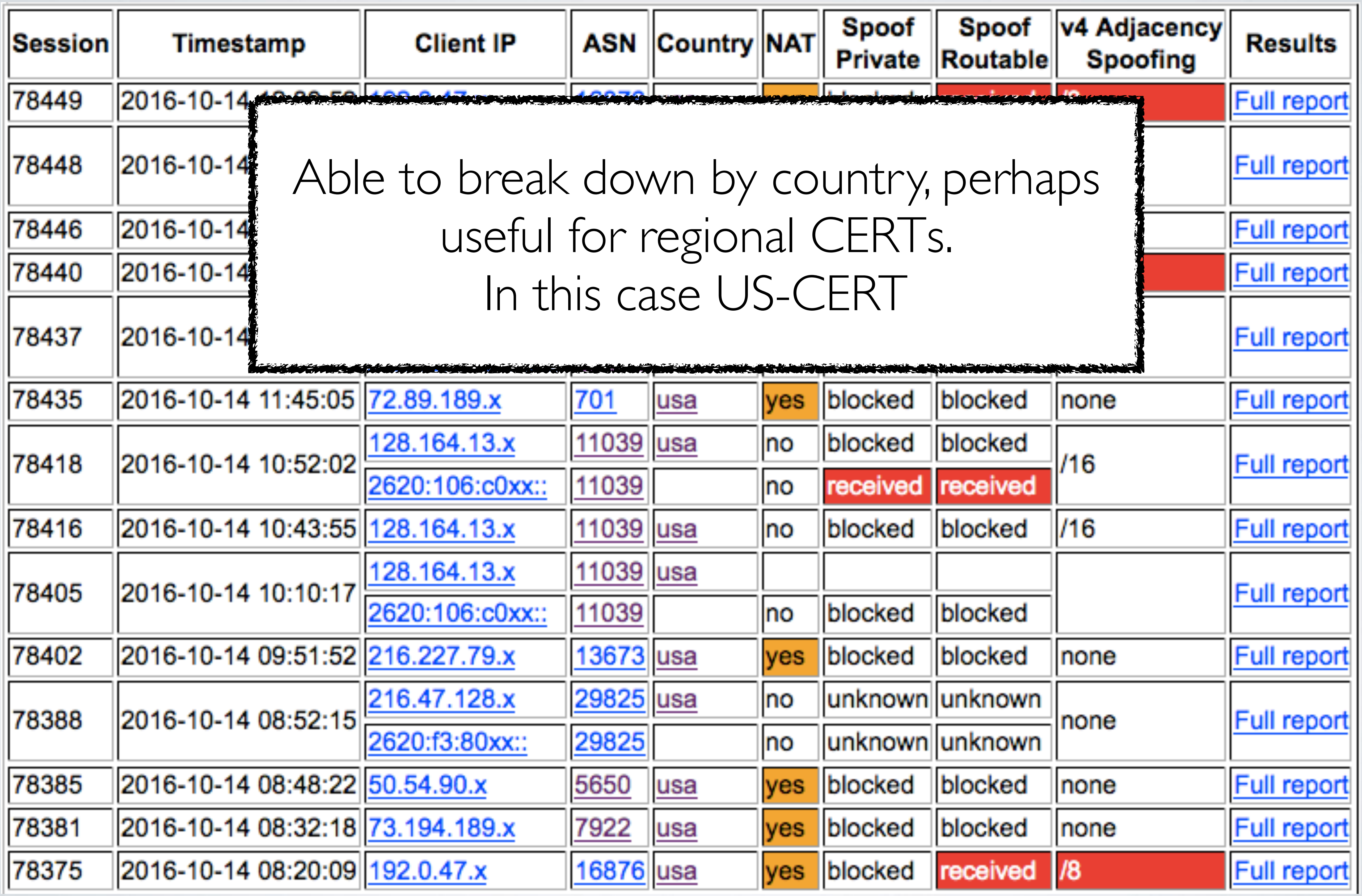
https://spoofer.caida.org/

Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306:cdxx::	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007:b0xx::	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					Full report
		2620:106:c0xx::	11039		no	blocked	blocked		
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa	yes	blocked	blocked	none	Full report
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa	no	unknown	unknown	none	Full report
		2620:f3:80xx::	29825		no	unknown	unknown		
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa	yes	blocked	blocked	none	Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

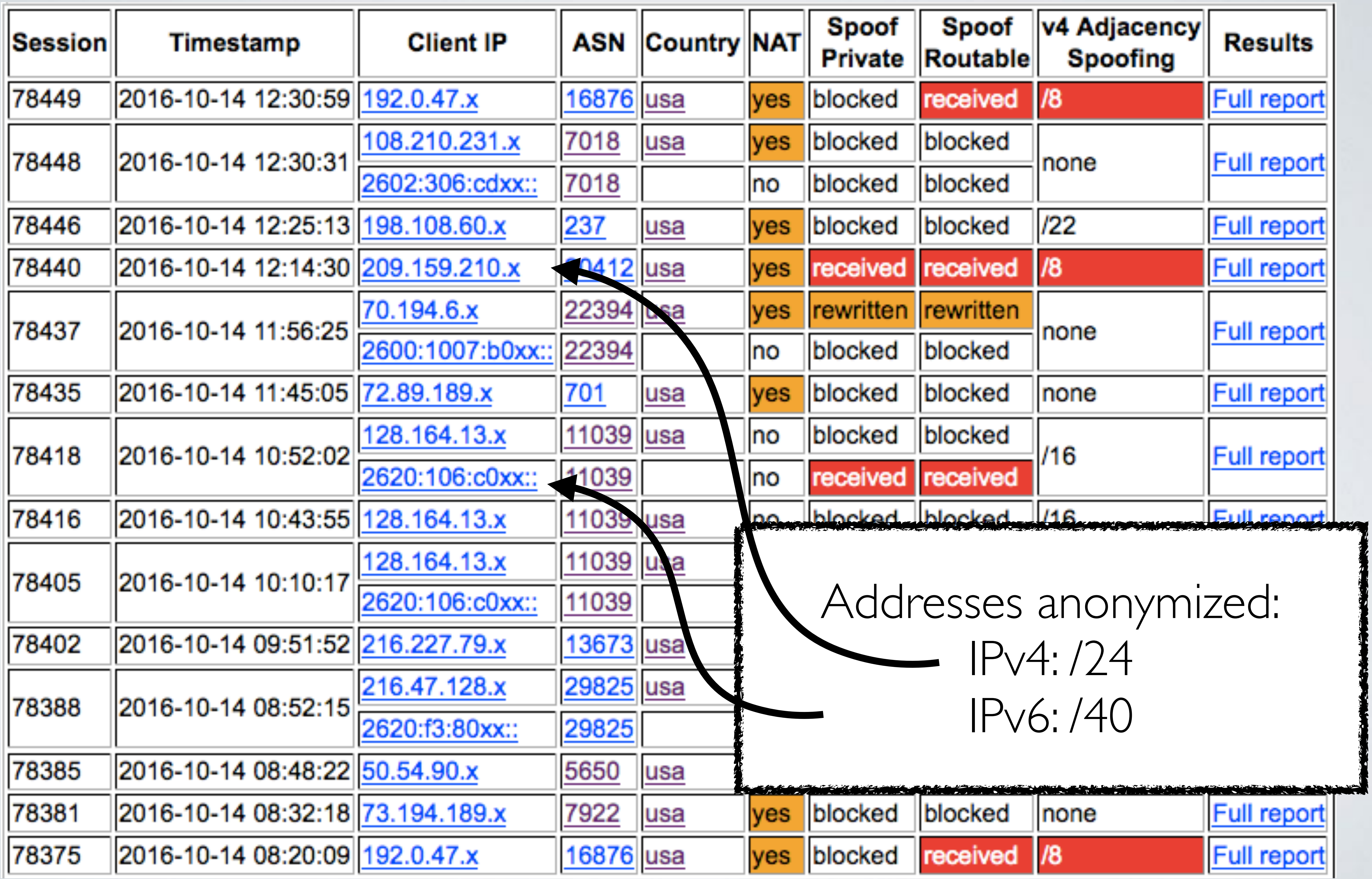
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14								Full report
78448	2016-10-14								Full report
78446	2016-10-14								Full report
78440	2016-10-14								Full report
78437	2016-10-14								Full report
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					Full report
		2620:106:c0xx::	11039		no	blocked	blocked		
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa	yes	blocked	blocked	none	Full report
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa	no	unknown	unknown	none	Full report
		2620:f3:80xx::	29825		no	unknown	unknown		
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa	yes	blocked	blocked	none	Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Able to break down by country, perhaps useful for regional CERTs.
In this case US-CERT

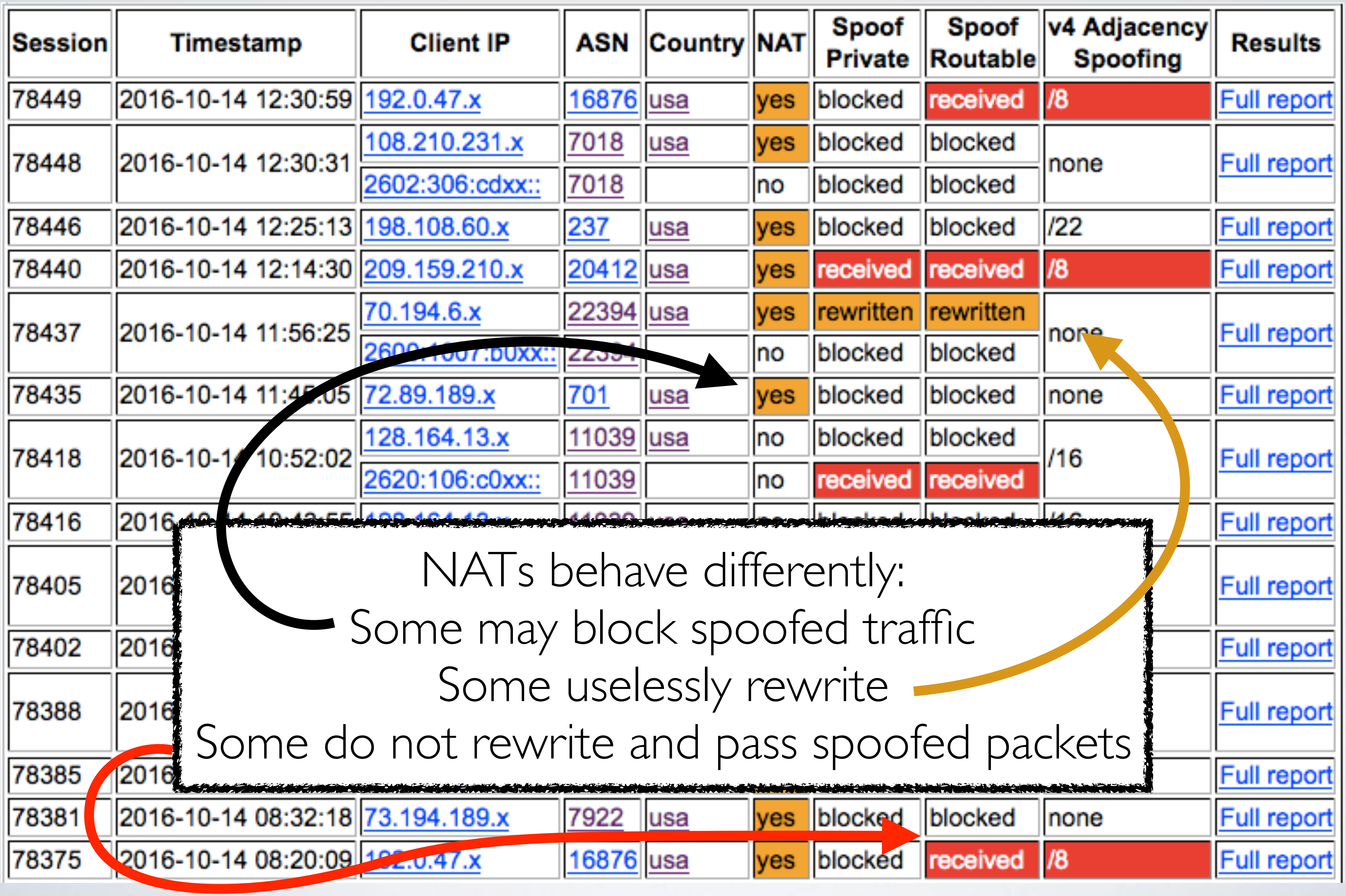
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306:cdxx::	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007:b0xx::	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016-10-14 10:10:17	128.164.13.x	11039	usa					
		2620:106:c0xx::	11039						
78402	2016-10-14 09:51:52	216.227.79.x	13673	usa					
78388	2016-10-14 08:52:15	216.47.128.x	29825	usa					
		2620:f3:80xx::	29825						
78385	2016-10-14 08:48:22	50.54.90.x	5650	usa					
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Addresses anonymized:
IPv4: /24
IPv6: /40

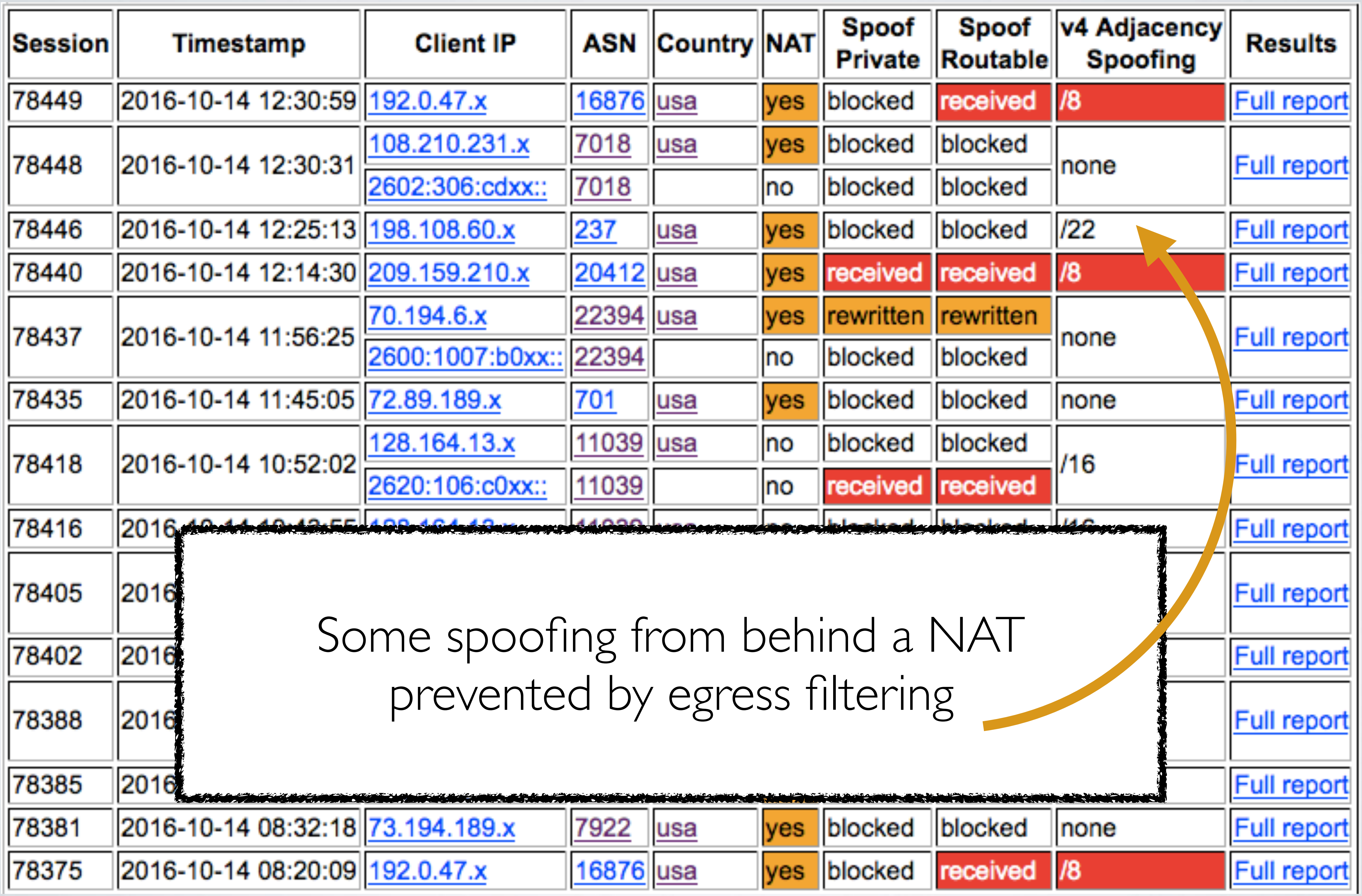
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306:cdxx::	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007:b0xx::	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106:c0xx::	11039		no	received	received		
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
78405	2016								Full report
78402	2016								Full report
78388	2016								Full report
78385	2016								Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

NATs behave differently:
Some may block spoofed traffic
Some uselessly rewrite
Some do not rewrite and pass spoofed packets

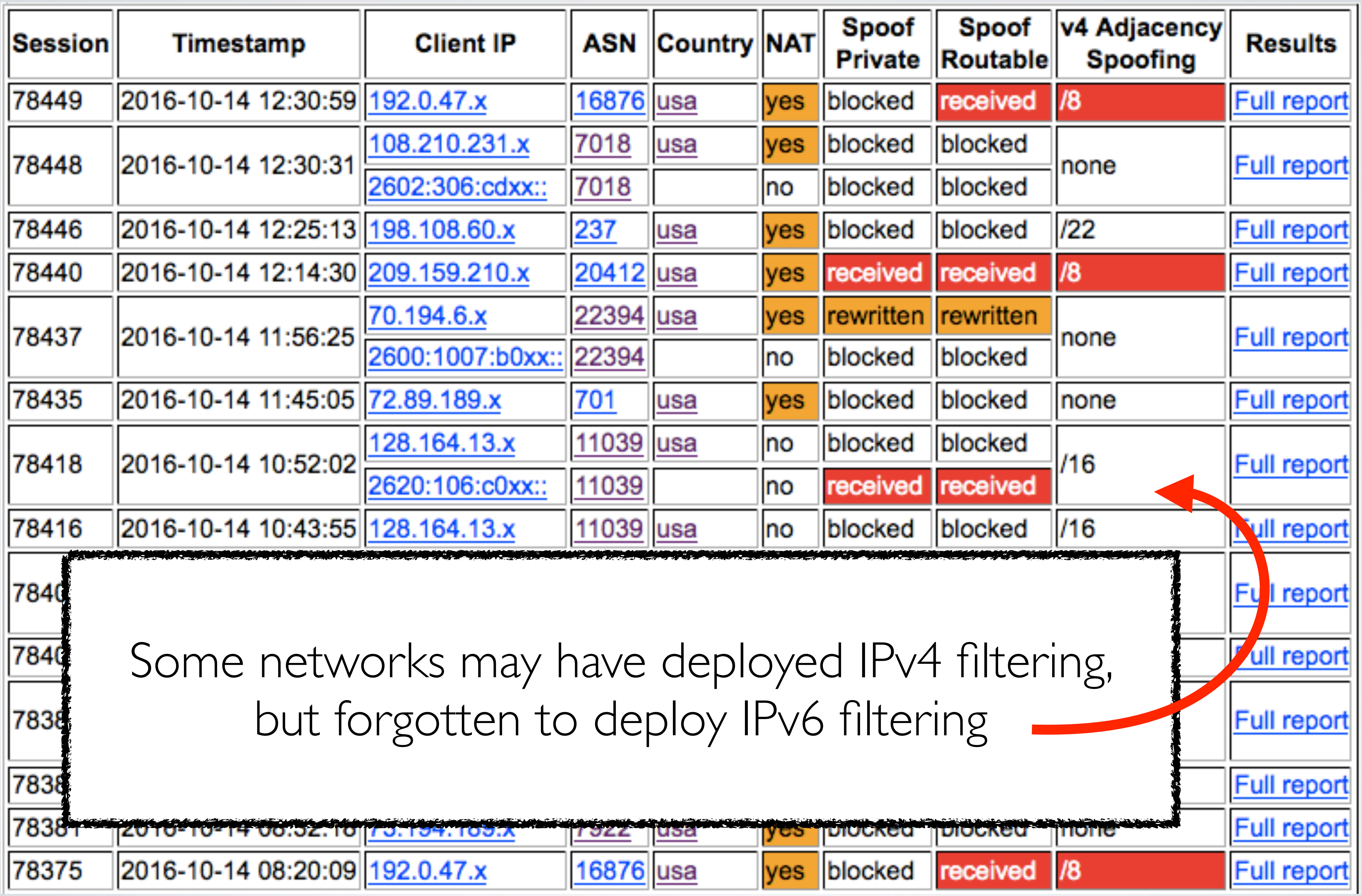
Reporting Engine: Recent Tests



Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x	7018	usa	yes	blocked	blocked	none	Full report
		2602:306:cdxx::	7018		no	blocked	blocked		
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x	22394	usa	yes	rewritten	rewritten	none	Full report
		2600:1007:b0xx::	22394		no	blocked	blocked		
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
		2620:106:c0xx::	11039		no	received	received		
78416	2016								Full report
78405	2016								Full report
78402	2016								Full report
78388	2016								Full report
78385	2016								Full report
78381	2016-10-14 08:32:18	73.194.189.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Some spoofing from behind a NAT prevented by egress filtering

Reporting Engine: Recent Tests

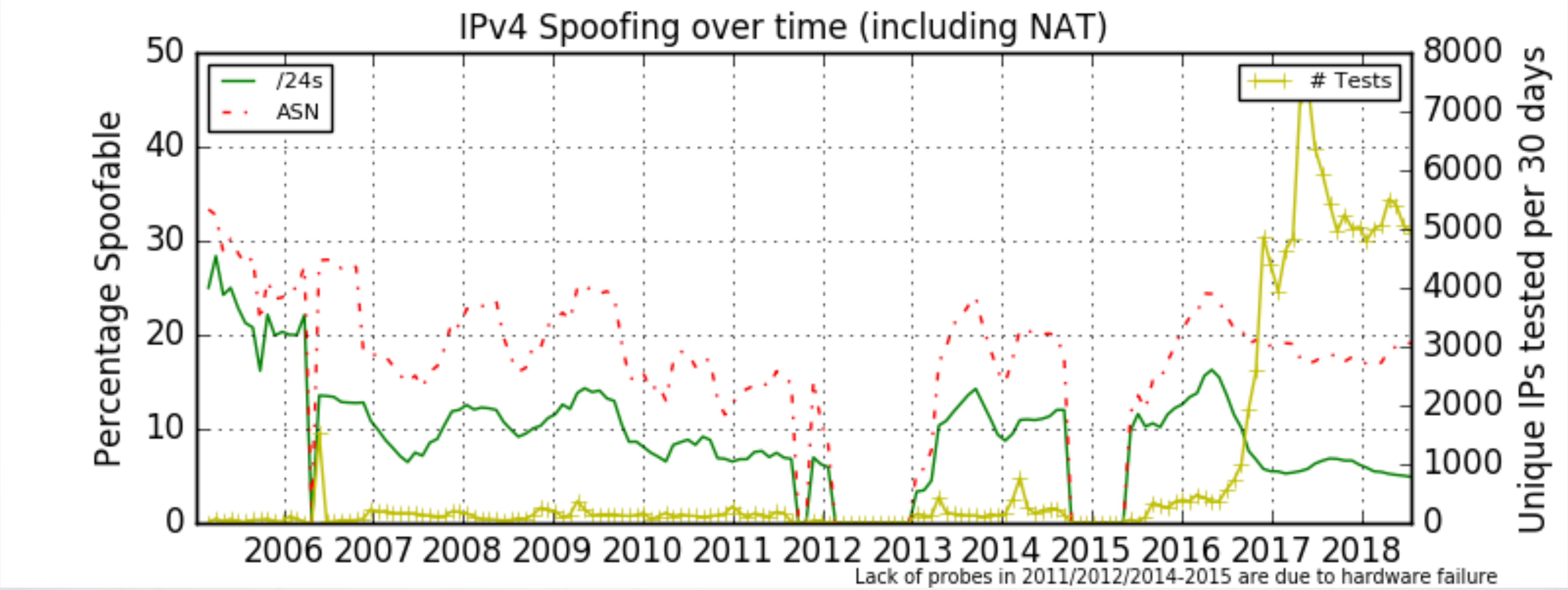


Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
78449	2016-10-14 12:30:59	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report
78448	2016-10-14 12:30:31	108.210.231.x 2602:306:cdxx::	7018 7018	usa	yes no	blocked blocked	blocked blocked	none	Full report
78446	2016-10-14 12:25:13	198.108.60.x	237	usa	yes	blocked	blocked	/22	Full report
78440	2016-10-14 12:14:30	209.159.210.x	20412	usa	yes	received	received	/8	Full report
78437	2016-10-14 11:56:25	70.194.6.x 2600:1007:b0xx::	22394 22394	usa	yes no	rewritten blocked	rewritten blocked	none	Full report
78435	2016-10-14 11:45:05	72.89.189.x	701	usa	yes	blocked	blocked	none	Full report
78418	2016-10-14 10:52:02	128.164.13.x 2620:106:c0xx::	11039 11039	usa	no no	blocked received	blocked received	/16	Full report
78416	2016-10-14 10:43:55	128.164.13.x	11039	usa	no	blocked	blocked	/16	Full report
7840									Full report
7840									Full report
7838									Full report
7838									Full report
78381	2016-10-14 08:32:16	73.194.183.x	7922	usa	yes	blocked	blocked	none	Full report
78375	2016-10-14 08:20:09	192.0.47.x	16876	usa	yes	blocked	received	/8	Full report

Some networks may have deployed IPv4 filtering, but forgotten to deploy IPv6 filtering

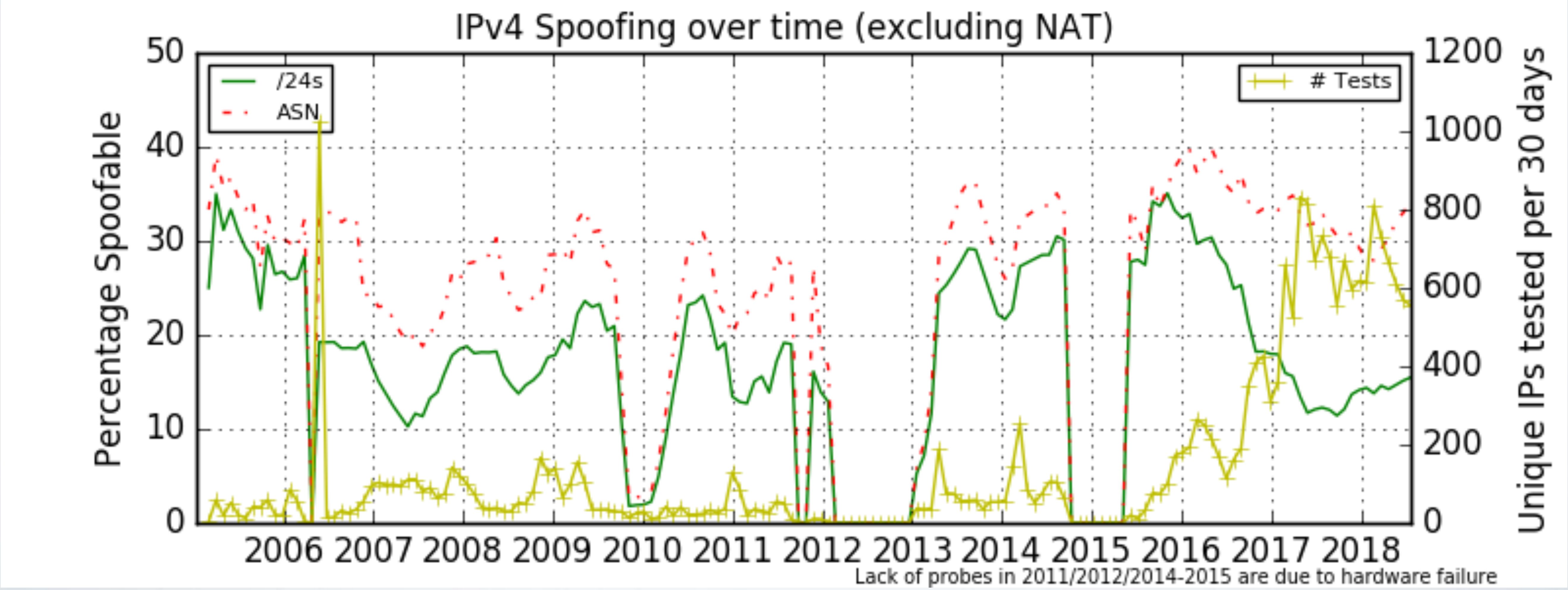
IPv4 Spoofing: All Tests

- 5K IPs tested per 30 days starting 2017
- 19% of tested ASes did not block spoofed packets
- 5% of tested IPv4 blocks did not block spoofed packets



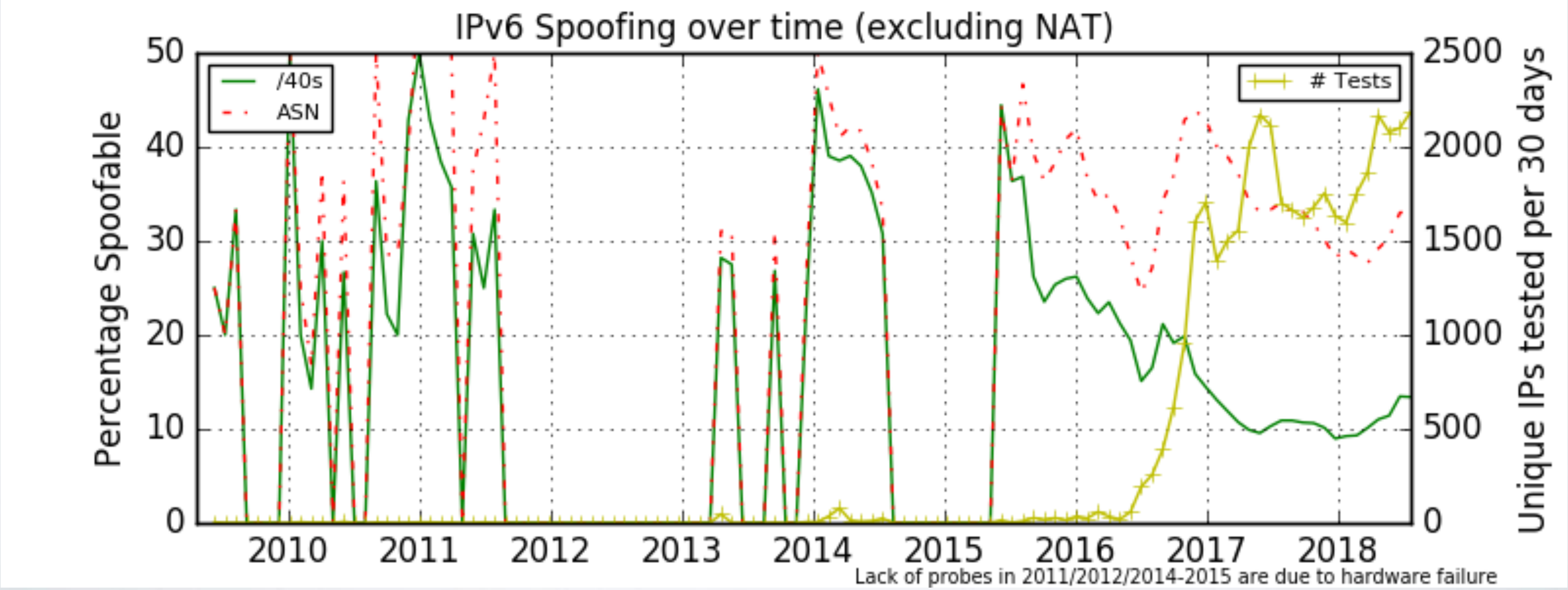
IPv4 Spoofing: No NAT Tests

- 600 to 700 IPs tested per 30 days starting 2017
- ~35% of tested ASes did not block spoofed packets
- 15% of tested IPv4 blocks did not block spoofed packets

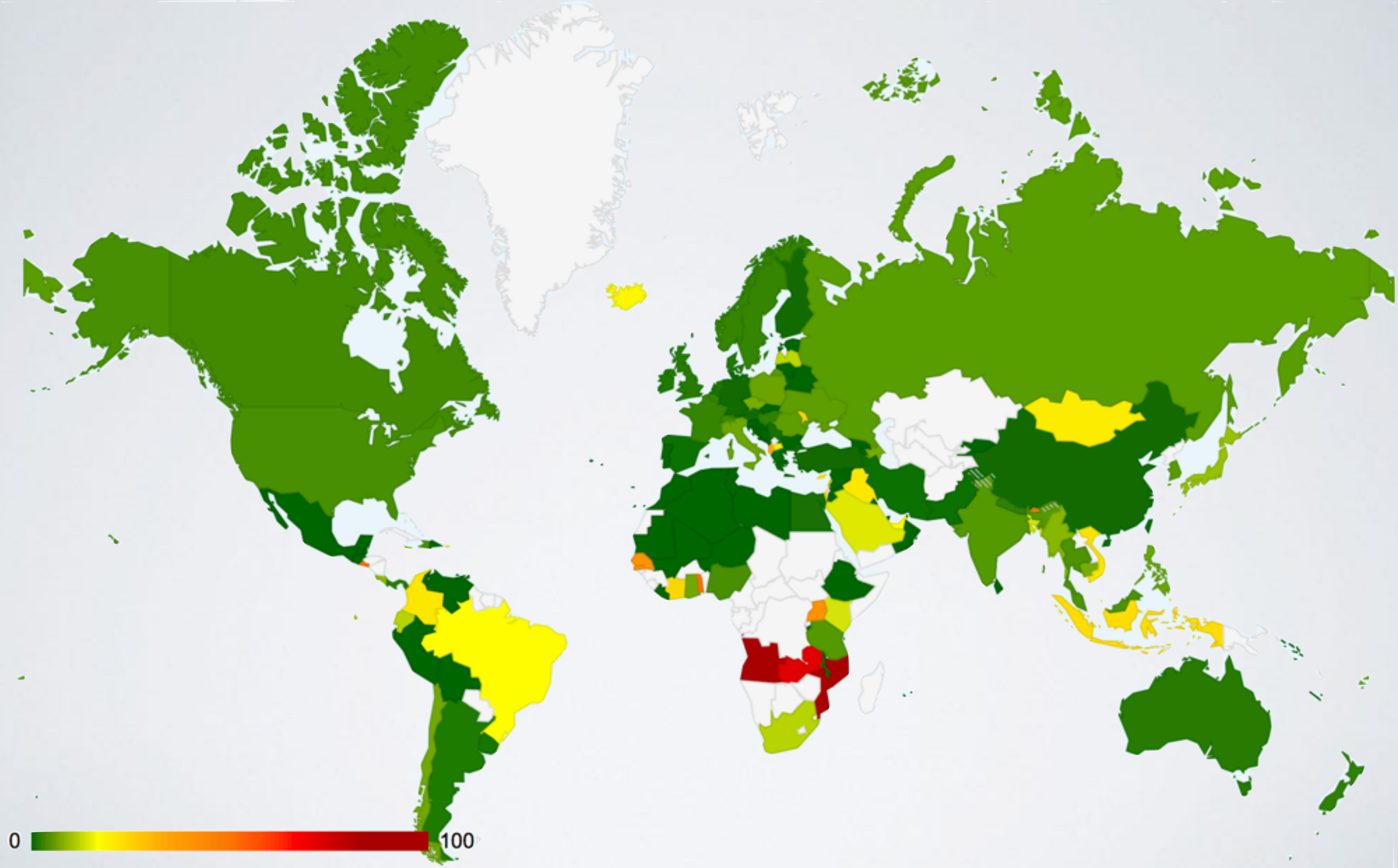


IPv6 Spoofing

- 1.5K to 2K IPs tested per 30 days starting 2017
- ~35% of tested ASes did not block spoofed packets
- 15% of tested IPv6 blocks did not block spoofed packets



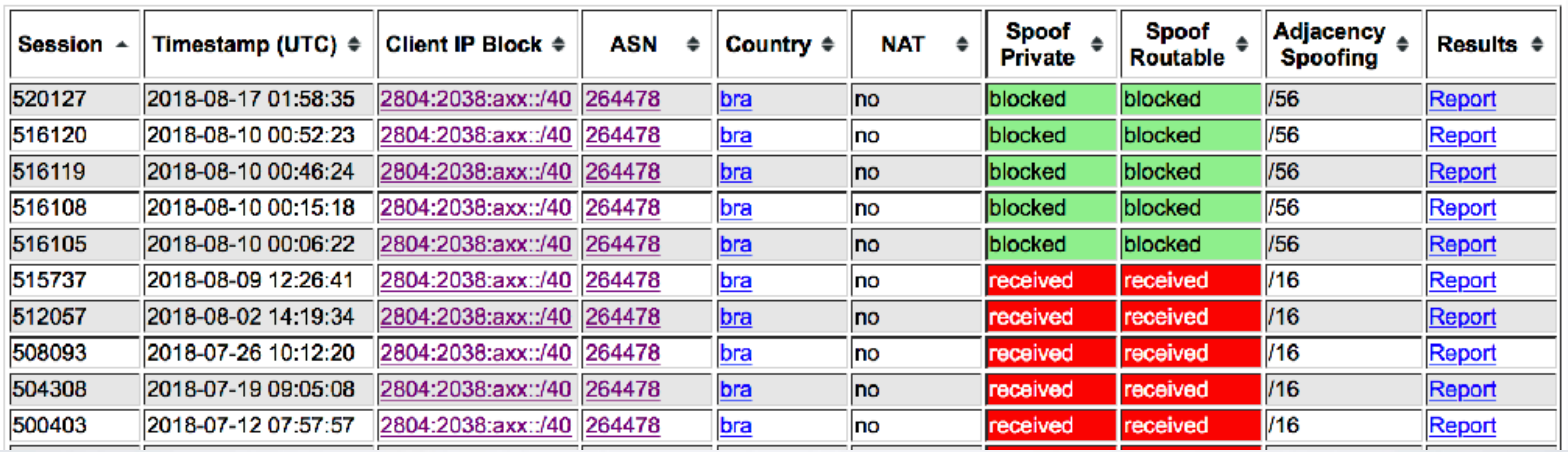
Fraction of prefixes not filtering by country



Notifications and Remediation

- Currently, we send notifications to abuse contacts of prefixes from which we received spoofed packet

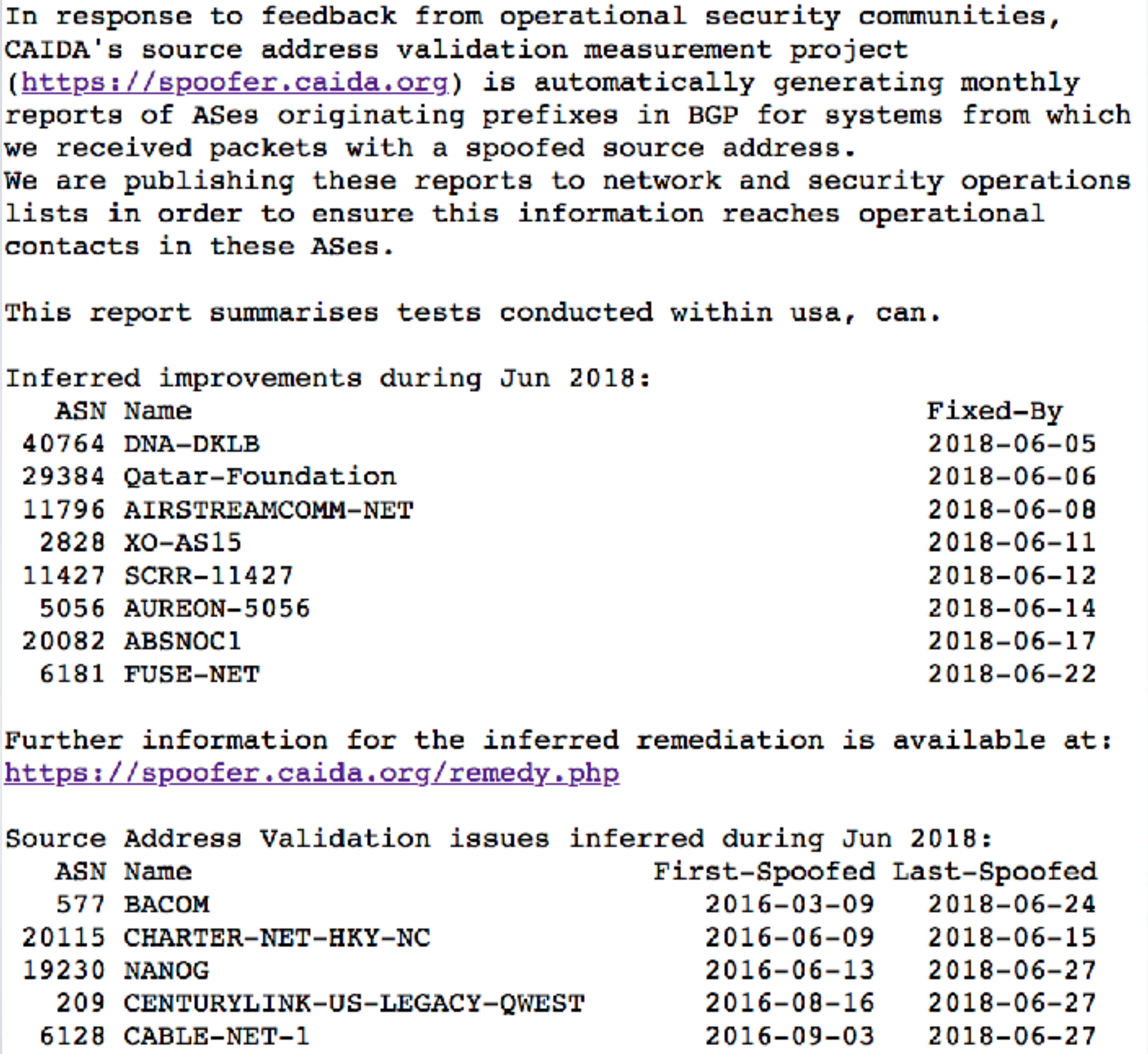
- We have also started to send geo-scoped emails to NOG lists



Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Spoof Private	Spoof Routable	Adjacency Spoofing	Results
520127	2018-08-17 01:58:35	2804:2038:axx::/40	264478	bra	no	blocked	blocked	/56	Report
516120	2018-08-10 00:52:23	2804:2038:axx::/40	264478	bra	no	blocked	blocked	/56	Report
516119	2018-08-10 00:46:24	2804:2038:axx::/40	264478	bra	no	blocked	blocked	/56	Report
516108	2018-08-10 00:15:18	2804:2038:axx::/40	264478	bra	no	blocked	blocked	/56	Report
516105	2018-08-10 00:06:22	2804:2038:axx::/40	264478	bra	no	blocked	blocked	/56	Report
515737	2018-08-09 12:26:41	2804:2038:axx::/40	264478	bra	no	received	received	/16	Report
512057	2018-08-02 14:19:34	2804:2038:axx::/40	264478	bra	no	received	received	/16	Report
508093	2018-07-26 10:12:20	2804:2038:axx::/40	264478	bra	no	received	received	/16	Report
504308	2018-07-19 09:05:08	2804:2038:axx::/40	264478	bra	no	received	received	/16	Report
500403	2018-07-12 07:57:57	2804:2038:axx::/40	264478	bra	no	received	received	/16	Report

https://spoofer.caida.org/remedy.php

Notifications and Remediation



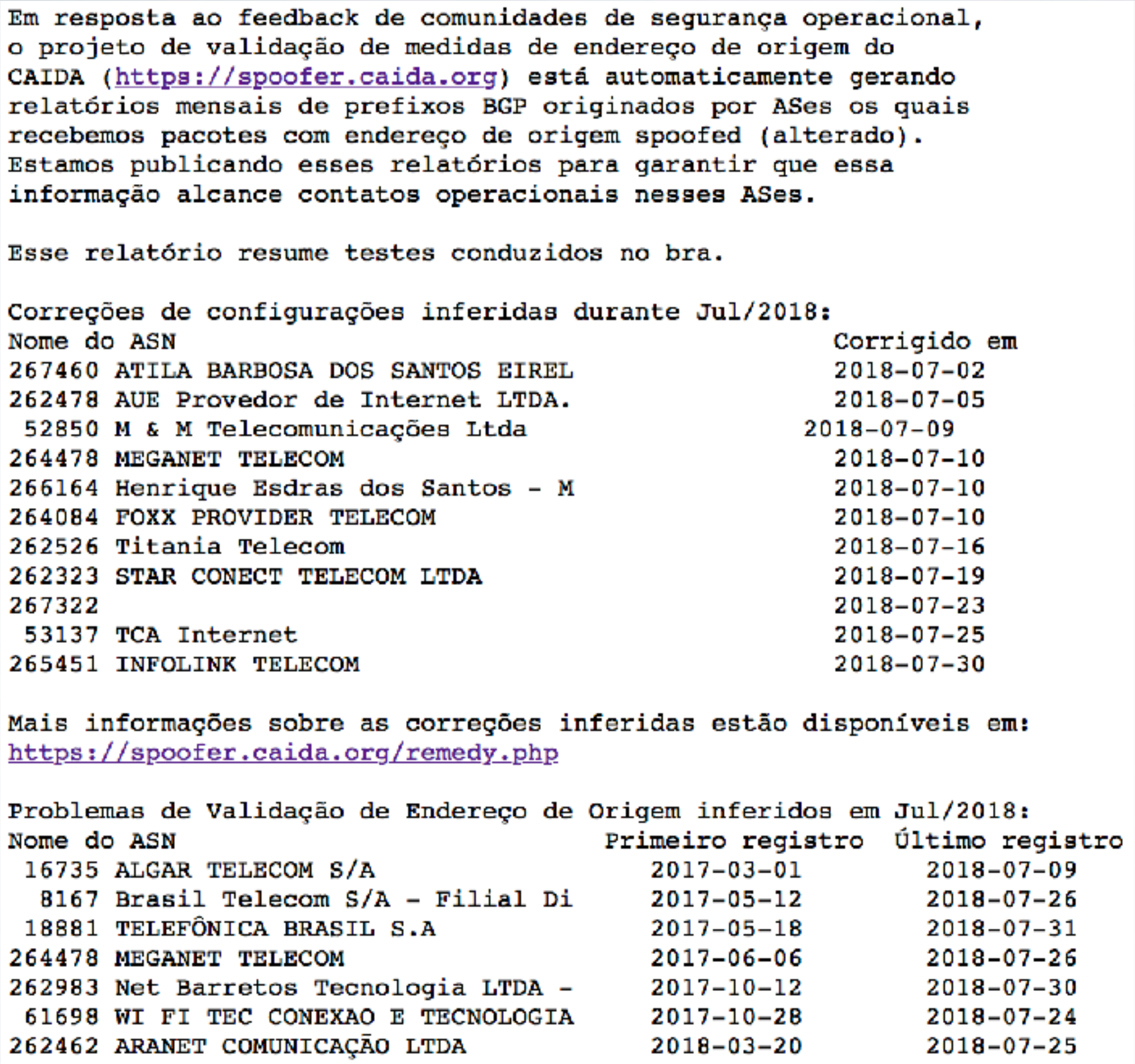
```
In response to feedback from operational security communities,
CAIDA's source address validation measurement project
(https://spoofer.caida.org) is automatically generating monthly
reports of ASes originating prefixes in BGP for systems from which
we received packets with a spoofed source address.
We are publishing these reports to network and security operations
lists in order to ensure this information reaches operational
contacts in these ASes.

This report summarises tests conducted within usa, can.

Inferred improvements during Jun 2018:
   ASN Name                                          Fixed-By
 40764 DNA-DKLB                                      2018-06-05
 29384 Qatar-Foundation                              2018-06-06
 11796 AIRSTREAMCOMM-NET                             2018-06-08
  2828 XO-AS15                                       2018-06-11
 11427 SCRR-11427                                    2018-06-12
  5056 AUREON-5056                                   2018-06-14
 20082 ABSNOC1                                       2018-06-17
  6181 FUSE-NET                                      2018-06-22

Further information for the inferred remediation is available at:
https://spoofer.caida.org/remedy.php

Source Address Validation issues inferred during Jun 2018:
   ASN Name                        First-Spoofed Last-Spoofed
   577 BACOM                          2016-03-09   2018-06-24
 20115 CHARTER-NET-HKY-NC             2016-06-09   2018-06-15
 19230 NANOG                          2016-06-13   2018-06-27
   209 CENTURYLINK-US-LEGACY-QWEST    2016-08-16   2018-06-27
  6128 CABLE-NET-1                    2016-09-03   2018-06-27
```

Monthly email to NANOG

Inferred Remediation

Problems Inferred

Notifications and Remediation



Em resposta ao feedback de comunidades de segurança operacional, o projeto de validação de medidas de endereço de origem do CAIDA (https://spoofer.caida.org) está automaticamente gerando relatórios mensais de prefixos BGP originados por ASes os quais recebemos pacotes com endereço de origem spoofed (alterado). Estamos publicando esses relatórios para garantir que essa informação alcance contatos operacionais nesses ASes.

Esse relatório resume testes conduzidos no bra.

Correções de configurações inferidas durante Jul/2018:

Nome do ASN	Corrigido em
267460 ATILA BARBOSA DOS SANTOS EIREL	2018-07-02
262478 AUE Provedor de Internet LTDA.	2018-07-05
52850 M & M Telecomunicações Ltda	2018-07-09
264478 MEGANET TELECOM	2018-07-10
266164 Henrique Esdras dos Santos - M	2018-07-10
264084 FOXX PROVIDER TELECOM	2018-07-10
262526 Titania Telecom	2018-07-16
262323 STAR CONECT TELECOM LTDA	2018-07-19
267322	2018-07-23
53137 TCA Internet	2018-07-25
265451 INFOLINK TELECOM	2018-07-30

Mais informações sobre as correções inferidas estão disponíveis em: https://spoofer.caida.org/remedy.php

Problemas de Validação de Endereço de Origem inferidos em Jul/2018:

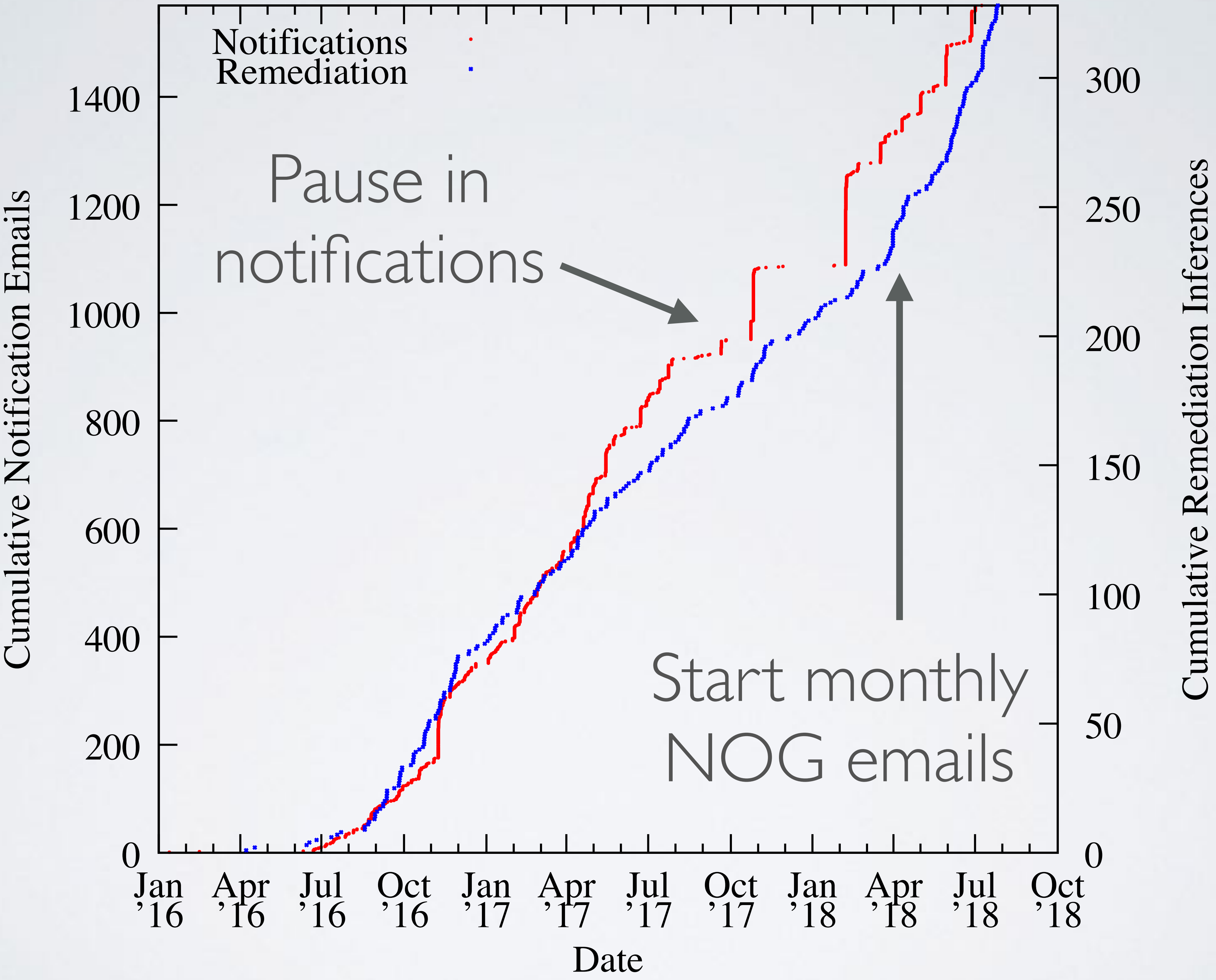
Nome do ASN	Primeiro registro	Último registro
16735 ALGAR TELECOM S/A	2017-03-01	2018-07-09
8167 Brasil Telecom S/A - Filial Di	2017-05-12	2018-07-26
18881 TELEFÔNICA BRASIL S.A	2017-05-18	2018-07-31
264478 MEGANET TELECOM	2017-06-06	2018-07-26
262983 Net Barretos Tecnologia LTDA -	2017-10-12	2018-07-30
61698 WI FI TEC CONEXAO E TECNOLOGIA	2017-10-28	2018-07-24
262462 ARANET COMUNICAÇÃO LTDA	2018-03-20	2018-07-25

Monthly email to GTER (br)

Inferred Remediation

Problems Inferred

Notifications and Remediation



Pause in notifications

Start monthly NOG emails

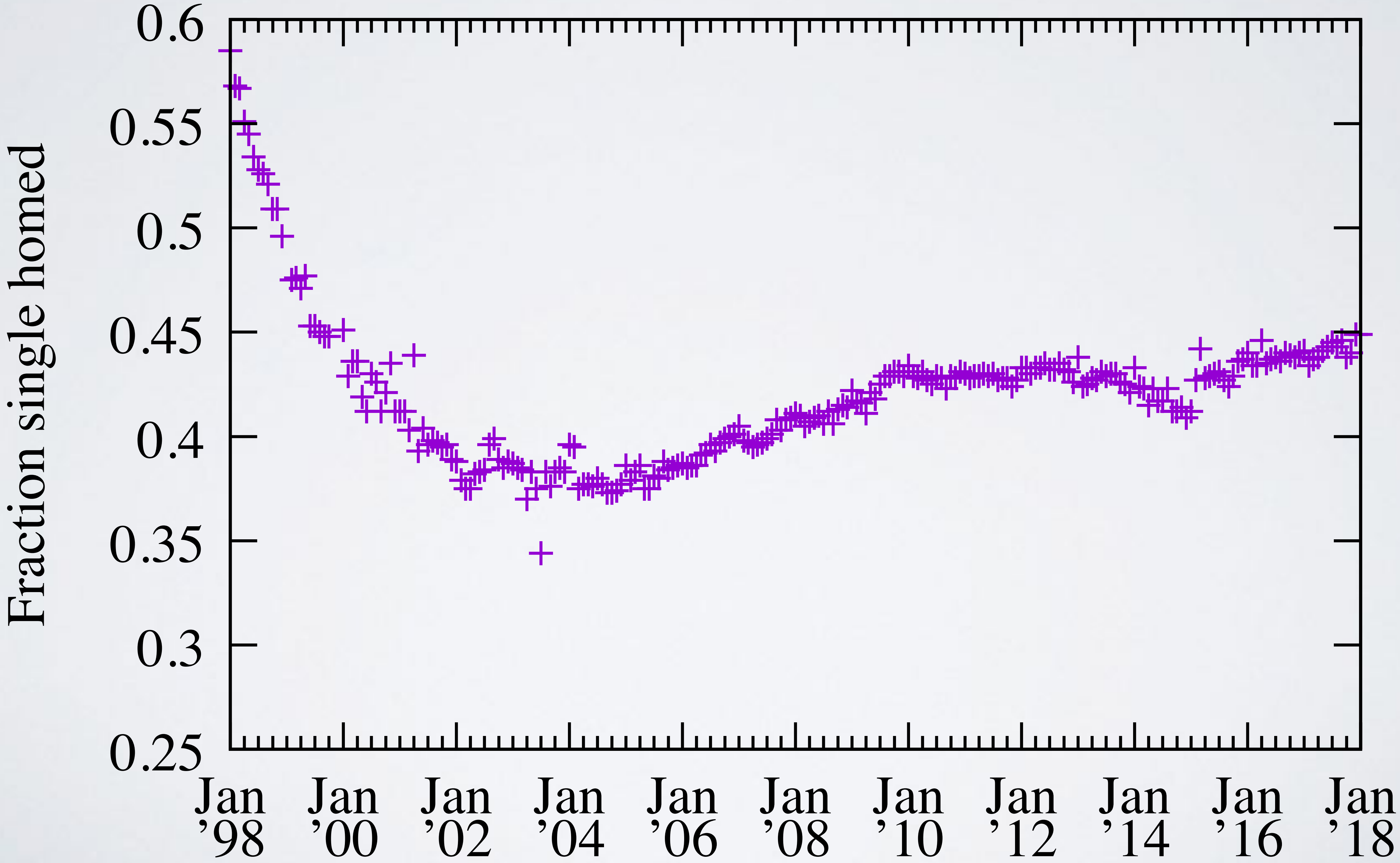
Sent 1543 private notifications, 328 remediation inferences

Is SAV hard to deploy?

- Two distinct approaches:
- Unicast Reverse Path Forwarding (uRPF)
  - Strict and Feasible: consider if source address is reachable using the interface the router received the packet
  - Loose Mode: consider if source address is reachable at all
- Statically Configured Access Control Lists (ACLs)
- Both only apply at the edge of Internet

Feasibility of Strict uRPF over time

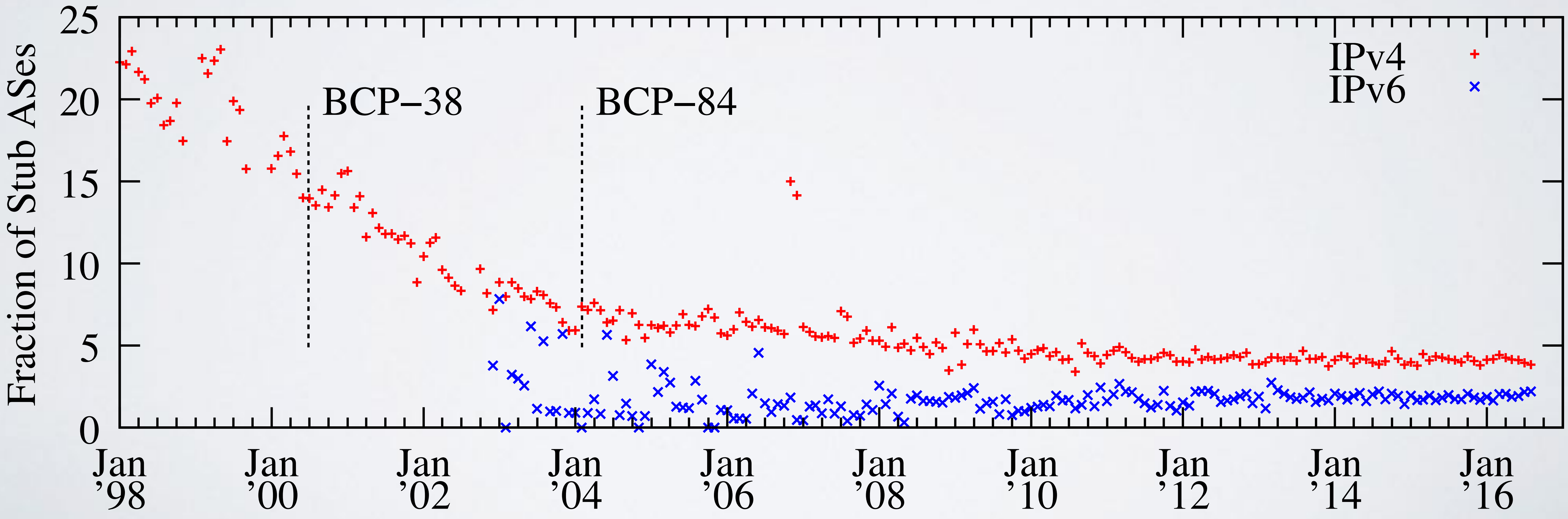
45% of stub ASes are single homed.
Their transit providers should deploy strict uRPF.



Feasibility of ACLs

ACLs are "the most bulletproof solution when done properly", and the "best fit ... when the configuration is not too dynamic, .. if the number of used prefixes is low". - BCP84

During 2015, ~5% and ~3% of ASes announced different IPv4 and IPv6 address space month-to-month, respectively.

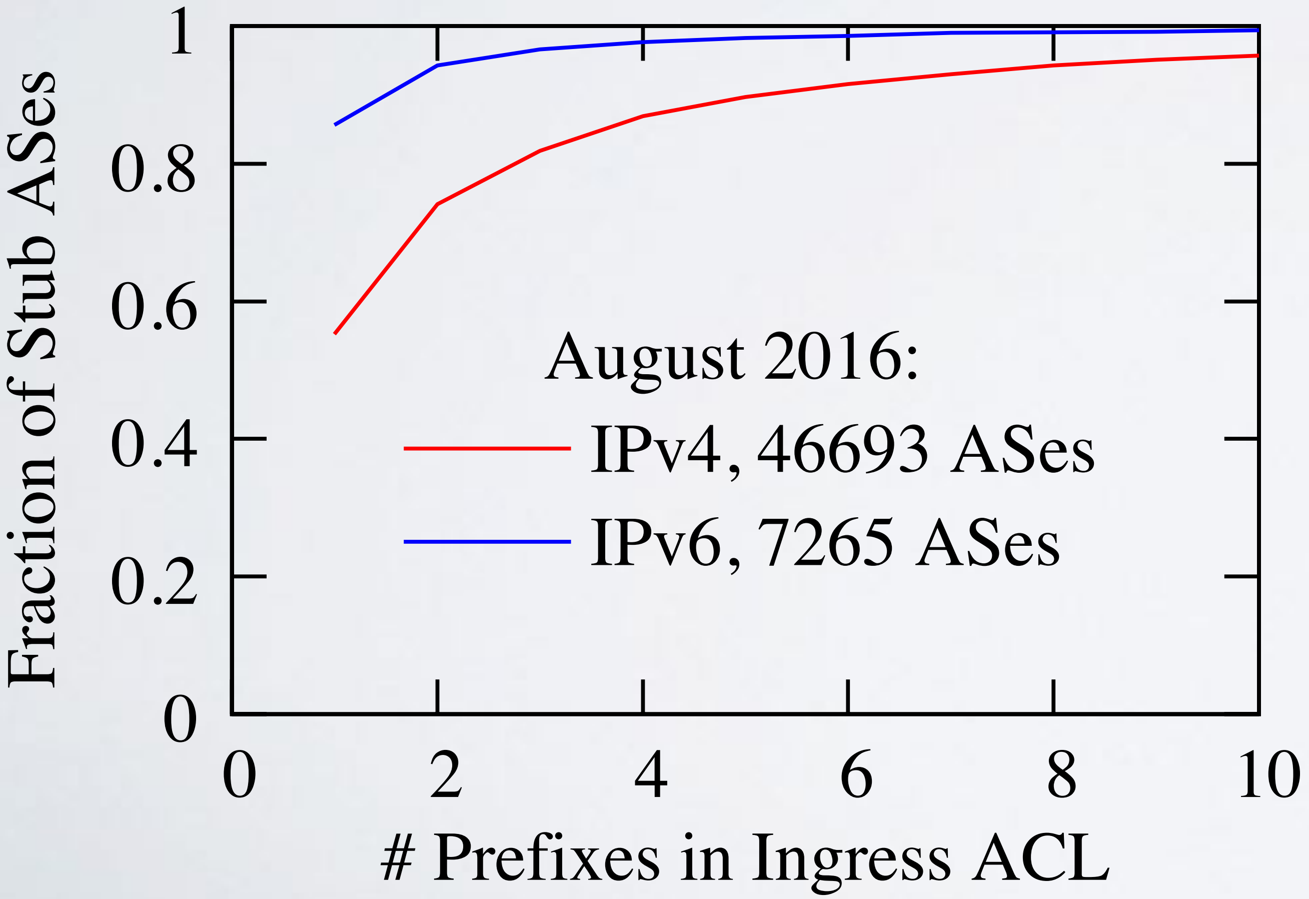


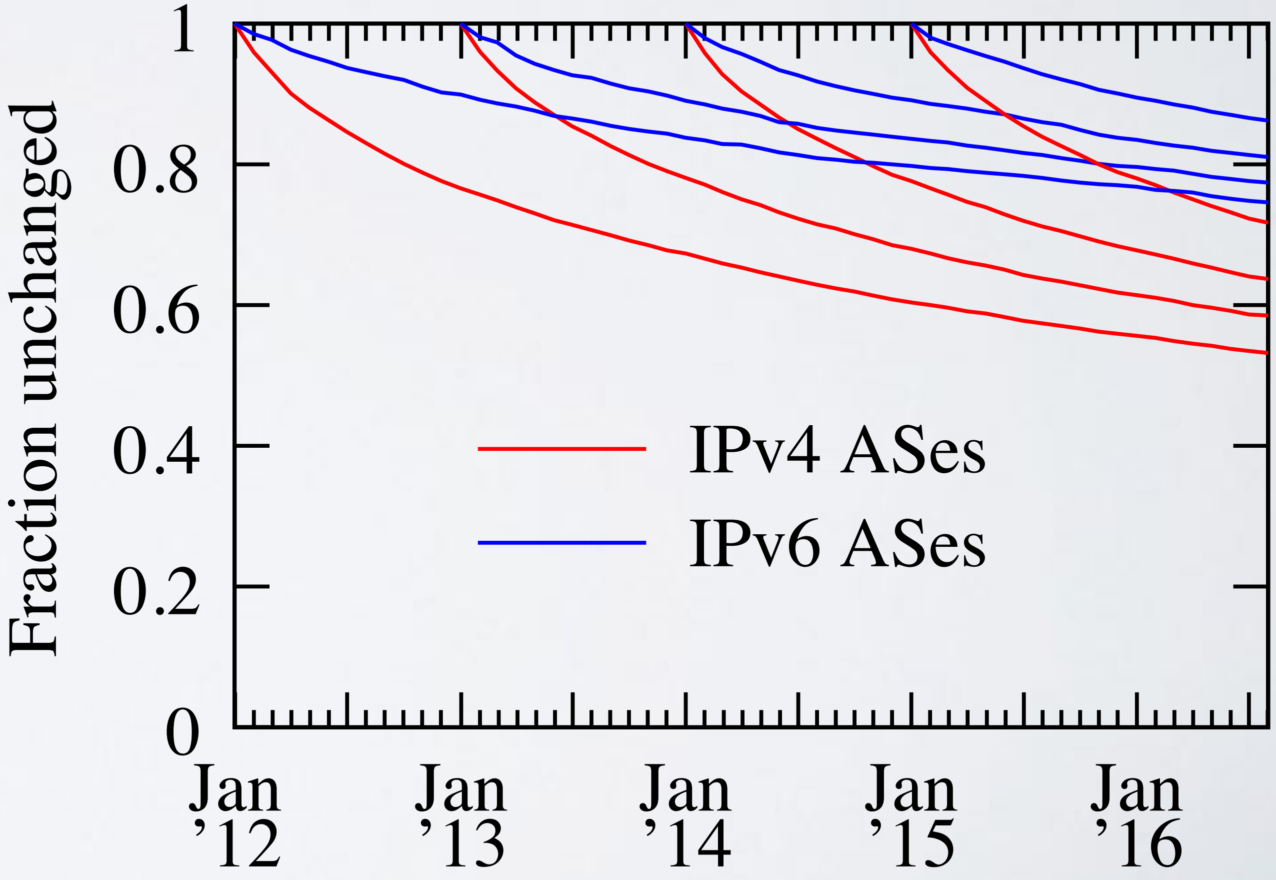
Source Routeviews and RIPE RIS data

Feasibility of ACLs

ACLs are the "best fit ... when the configuration is not too dynamic, .. if the number of used prefixes is low". - BCP84

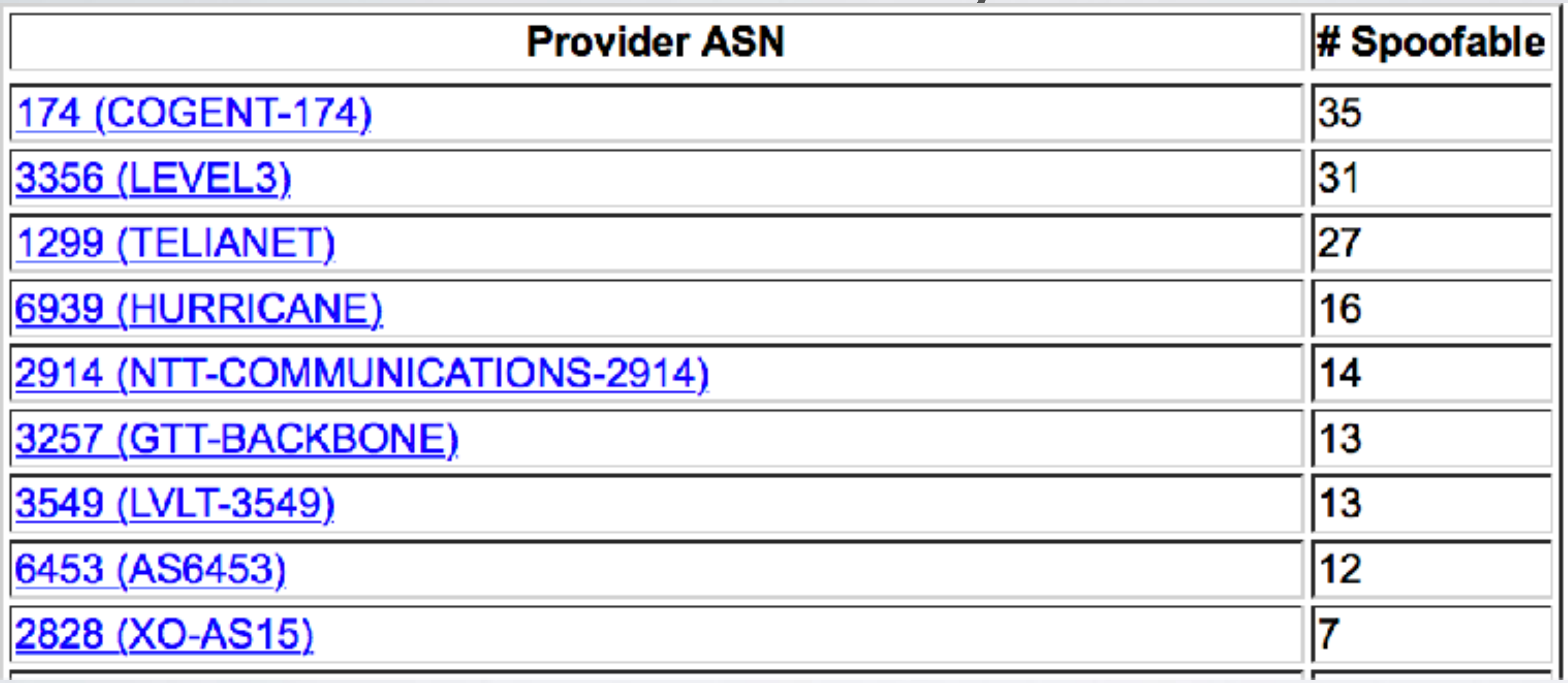
In August 2016, 86.9% of stub ASes would require an IPv4 ACL of no more than 4 prefixes. More than half of IPv4 ACLs defined in January 2012 would be unchanged 4.5 years later.



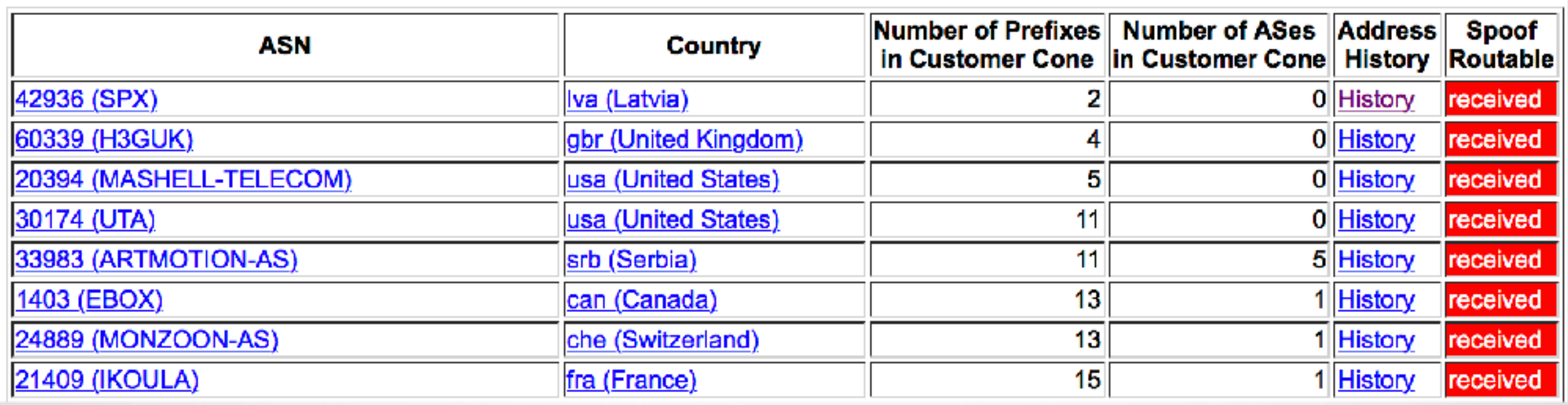


Source Routeviews and RIPE RIS data

Feasibility of ACLs



Provider ASN	# Spoofable
174 (COGENT-174)	35
3356 (LEVEL3)	31
1299 (TELIANET)	27
6939 (HURRICANE)	16
2914 (NTT-COMMUNICATIONS-2914)	14
3257 (GTT-BACKBONE)	13
3549 (LVLT-3549)	13
6453 (AS6453)	12
2828 (XO-AS15)	7



ASN	Country	Number of Prefixes in Customer Cone	Number of ASes in Customer Cone	Address History	Spoof Routable
42936 (SPX)	lva (Latvia)	2	0	History	received
60339 (H3GUK)	gbr (United Kingdom)	4	0	History	received
20394 (MASHELL-TELECOM)	usa (United States)	5	0	History	received
30174 (UTA)	usa (United States)	11	0	History	received
33983 (ARTMOTION-AS)	srb (Serbia)	11	5	History	received
1403 (EBOX)	can (Canada)	13	1	History	received
24889 (MONZOON-AS)	che (Switzerland)	13	1	History	received
21409 (IKOULA)	fra (France)	15	1	History	received

https://spoofer.caida.org/provider.php

Summary

- Measurement can enable solutions to fundamentally non-technical security problems
    - Peer pressure
    - Industry standards
    - Regulation
- Whatever the solution is, cannot be effective without rigorous, publicly observable measurement

Acknowledgements

- Project funded by U.S. Department of Homeland Security (DHS) Science and Technology (S&T) directorate

- Contacts:
  - spoofer-info@caida.org