Network Hygiene, Incentives, and Regulation:

Deployment of Source Address Validation in the Internet

Matthew Luckie - University of Waikato
Robert Beverly - Naval Postgraduate School
Ryan Koga - CAIDA / UC San Diego
Ken Keys - CAIDA / UC San Diego
Joshua A. Kroll - Naval Postgraduate School
k claffy - CAIDA / UC San Diego

ACM CCS 2019

November 12th, 2019

Motivation

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By John Leyden 27 Mar 2013 at 17:03 124 SHARE ▼

Gits club GitHub code tub with record-breaking 1.35Tbps DDoS drub

Memcache attacks are going to be this year's thing

By Iain Thomson in San Francisco 1 Mar 2018 at 21:10 21 SHARE ▼

400Gbps: Winter of Whopping Weekend DDoS Attacks

Share Like 27 Tweet

Marek Majkowski

3/3/2016, 3:32:00 AM GMT+1

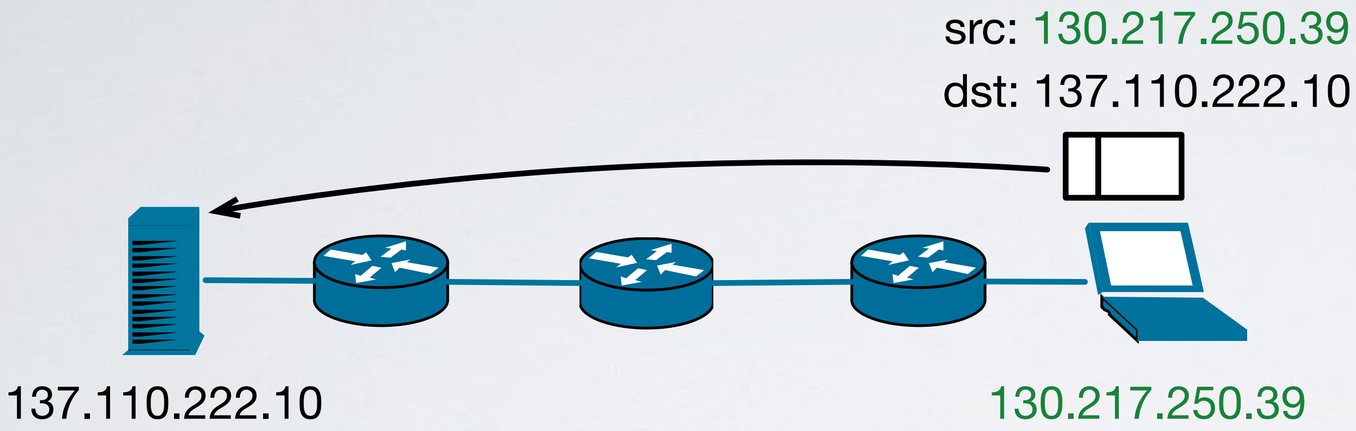
How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics

DAVID BISSON Follow @DMBisson

SEP 5, 2016 | FEATURED ARTICLES

Root cause: architectural limitation that provides an attacker with the ability to send packets using **spoofed source IP addresses**

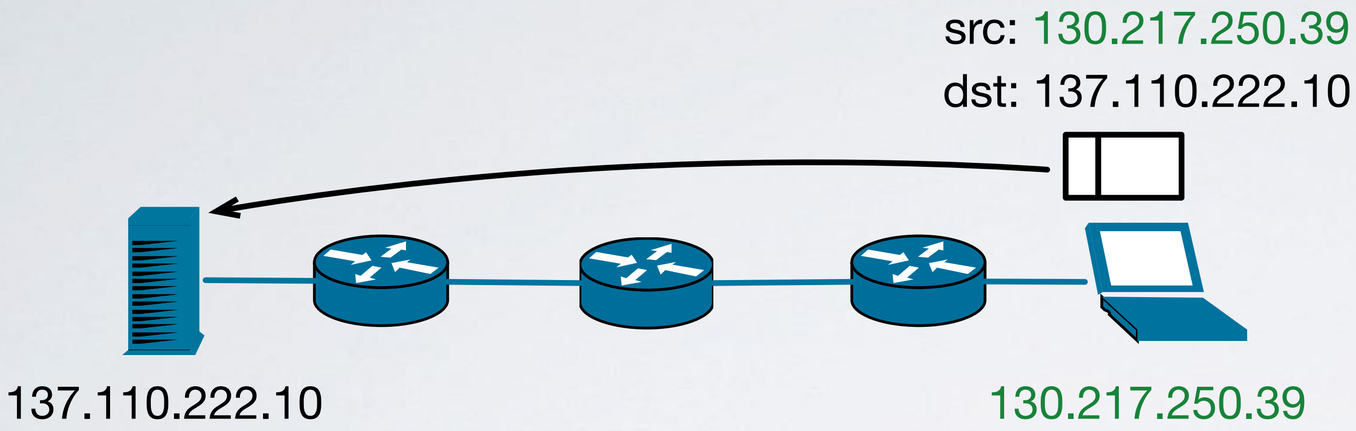
What is Spoofing?



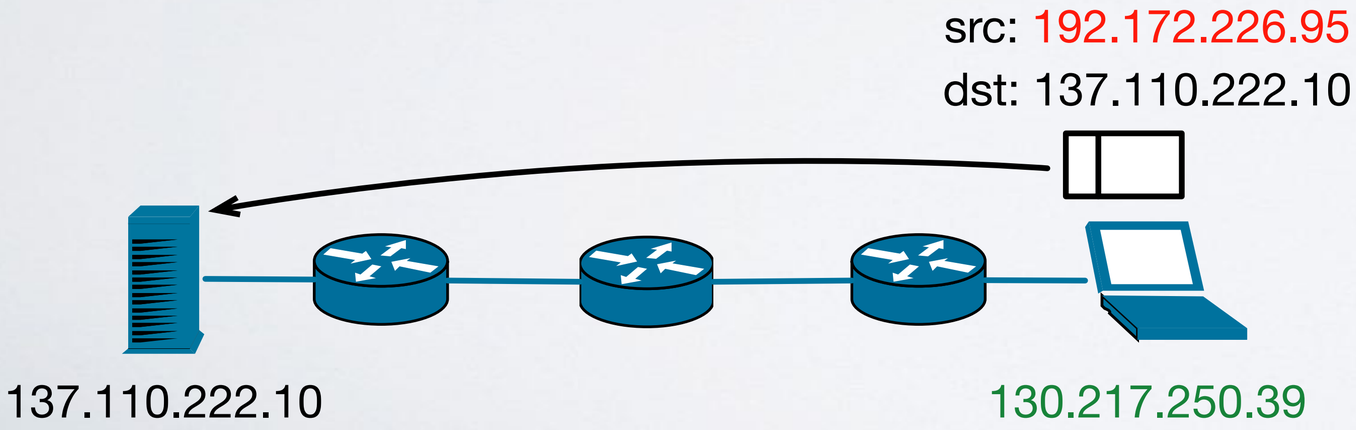
Non-spoofed packets use the address assigned to the sender as the source address.

What is Spoofing?

Using a Fake Source address in an IP packet.

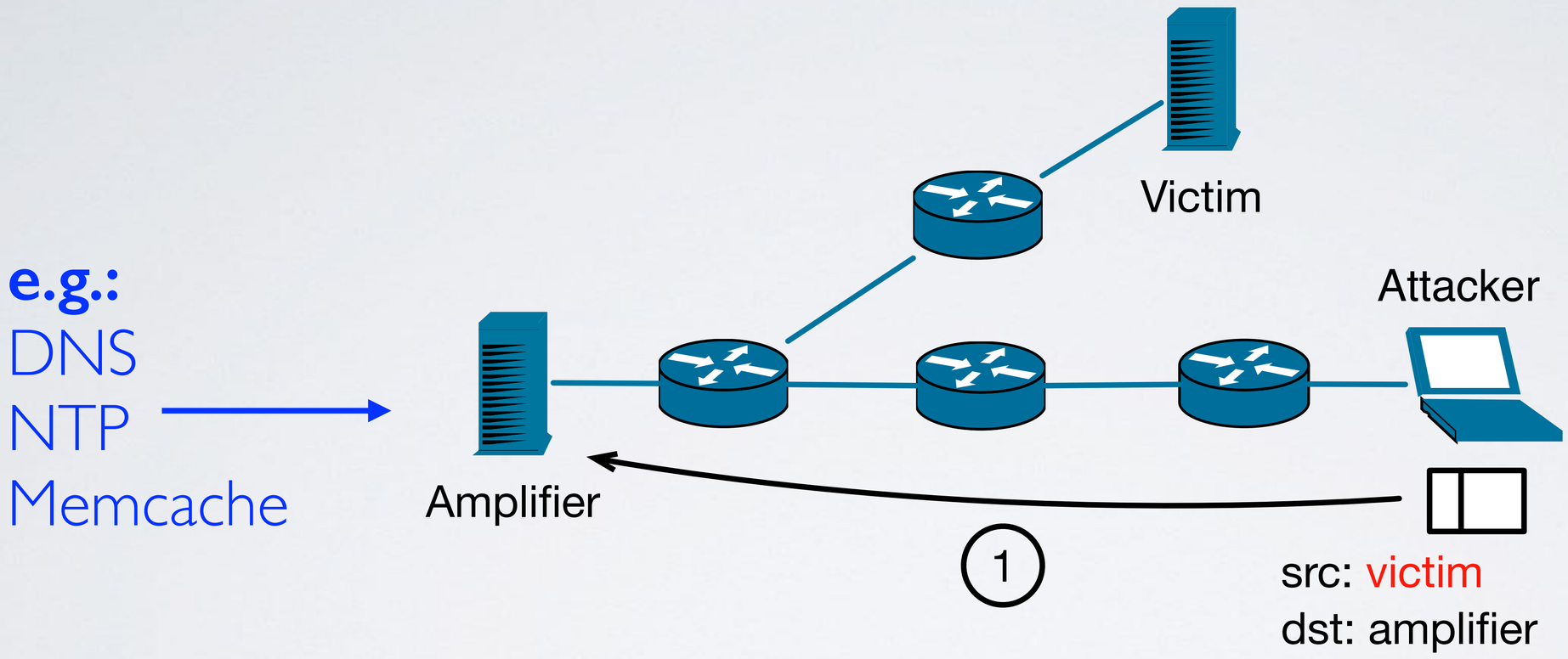


Non-spoofed packets use the address assigned to the sender as the source address.



Spoofed packets use a different address than the address assigned to the sender as the source address.

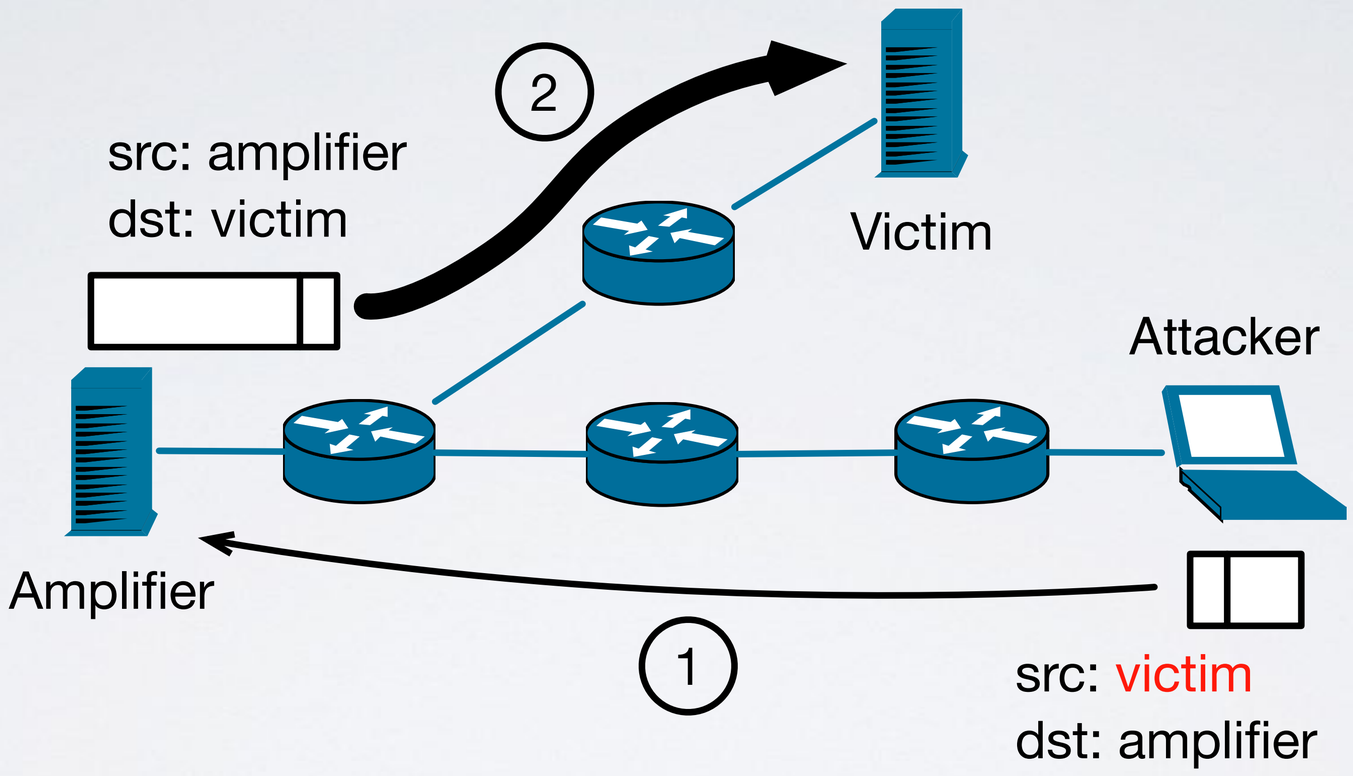
Spoofed-source Amplification DDoS Attack



Attacker sends small request packet to amplifier, with victim's address as the source address.

Spoofed-source Amplification DDoS Attack

e.g.:
DNS
NTP
Memcache



Attacker sends small request packet to amplifier, with victim's address as the source address. Amplifier sends the larger response to the victim

Motivation

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By John Leyden 27 Mar 2013 at 17:03 124 SHARE ▼

Gits club GitHub code tub with record-breaking 1.35Tbps DDoS drub

Memcache attacks are going to be this year's thing

By Iain Thomson in San Francisco 1 Mar 2018 at 21:10 21 SHARE ▼

400Gbps: Winter of Whopping Weekend DDoS Attacks

Share Like 27 Tweet

Marek Majkowski

3/3/2016, 3:32:00 AM GMT+1

How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics

DAVID BISSON Follow @DMBisson

SEP 5, 2016 | FEATURED ARTICLES

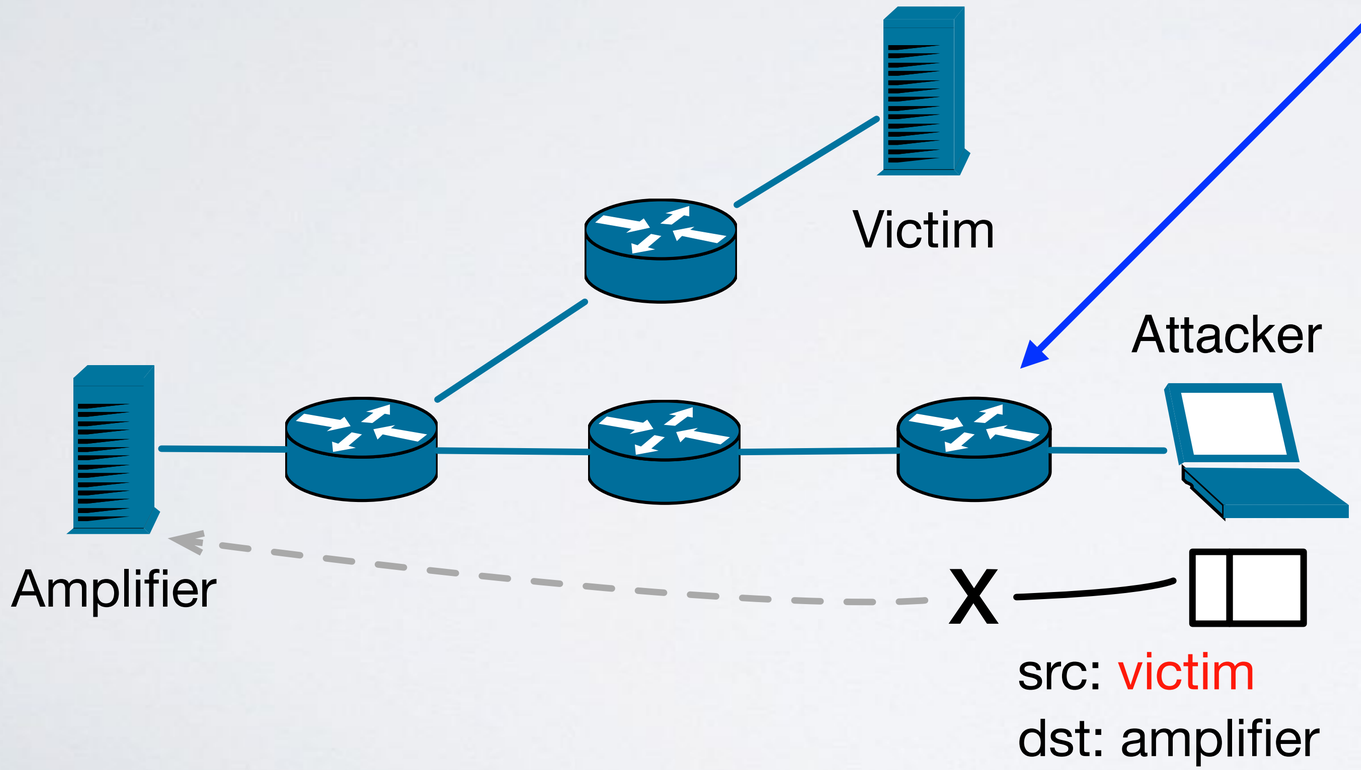
Attack sophistication increasing: e.g: blacklisting bank IP addresses

Someone is spoofing big bank IP addresses – possibly to embarrass security vendors

Written by Sean Lyngaas

APR 23, 2019 | CYBERSCOOP

Source Address Validation (SAV)



An **edge router** examines the source address of a packet.
It forwards packets with a reasonable source address given the network attachment point.

Approaches:
Reverse Path Forwarding (RPF)
Access Control Lists (ACLs)

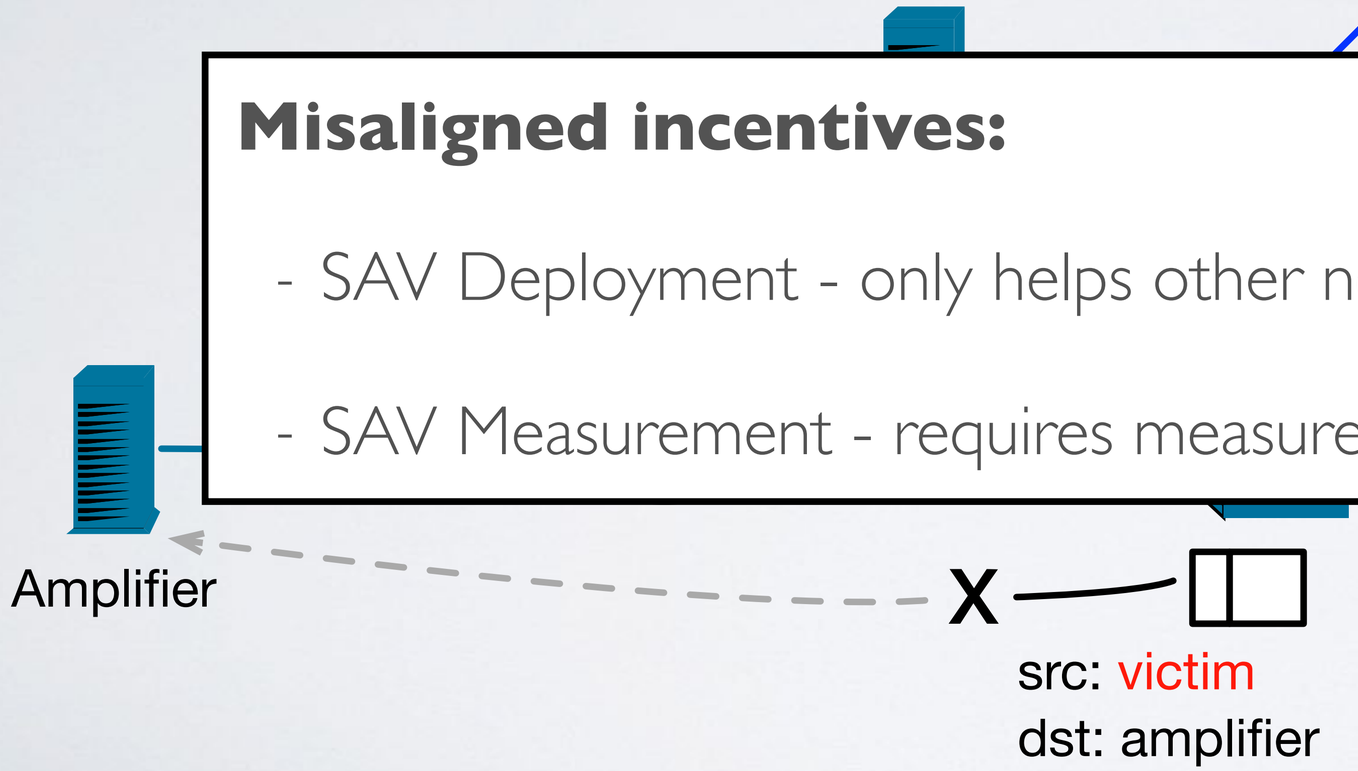
SAV: Packets outbound from the network

Source Address Validation (SAV)

An **edge router** examines the source address of a packet.
It forwards packets with a reasonable source address given

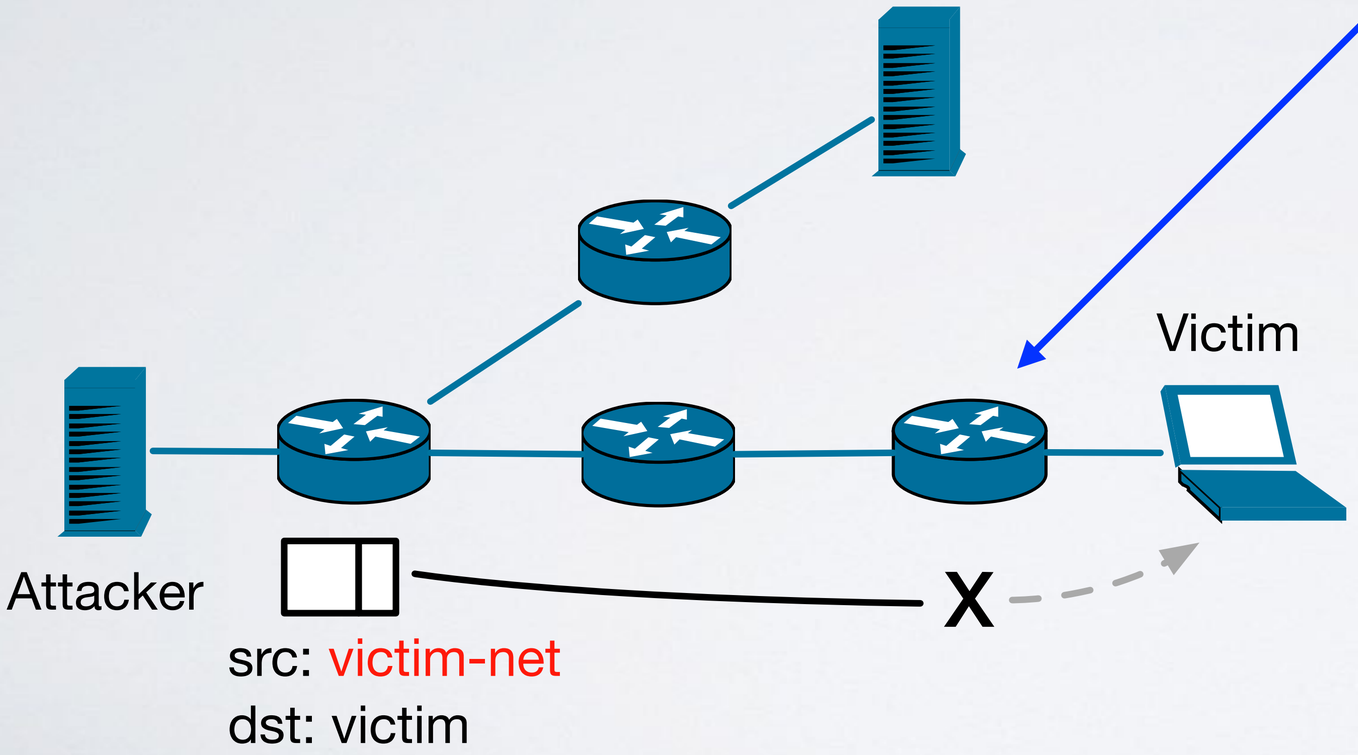
Misaligned incentives:

- SAV Deployment - only helps other networks
- SAV Measurement - requires measurement from ***within the network***



SAV: Packets outbound from the network

Source Address Validation (SAV)



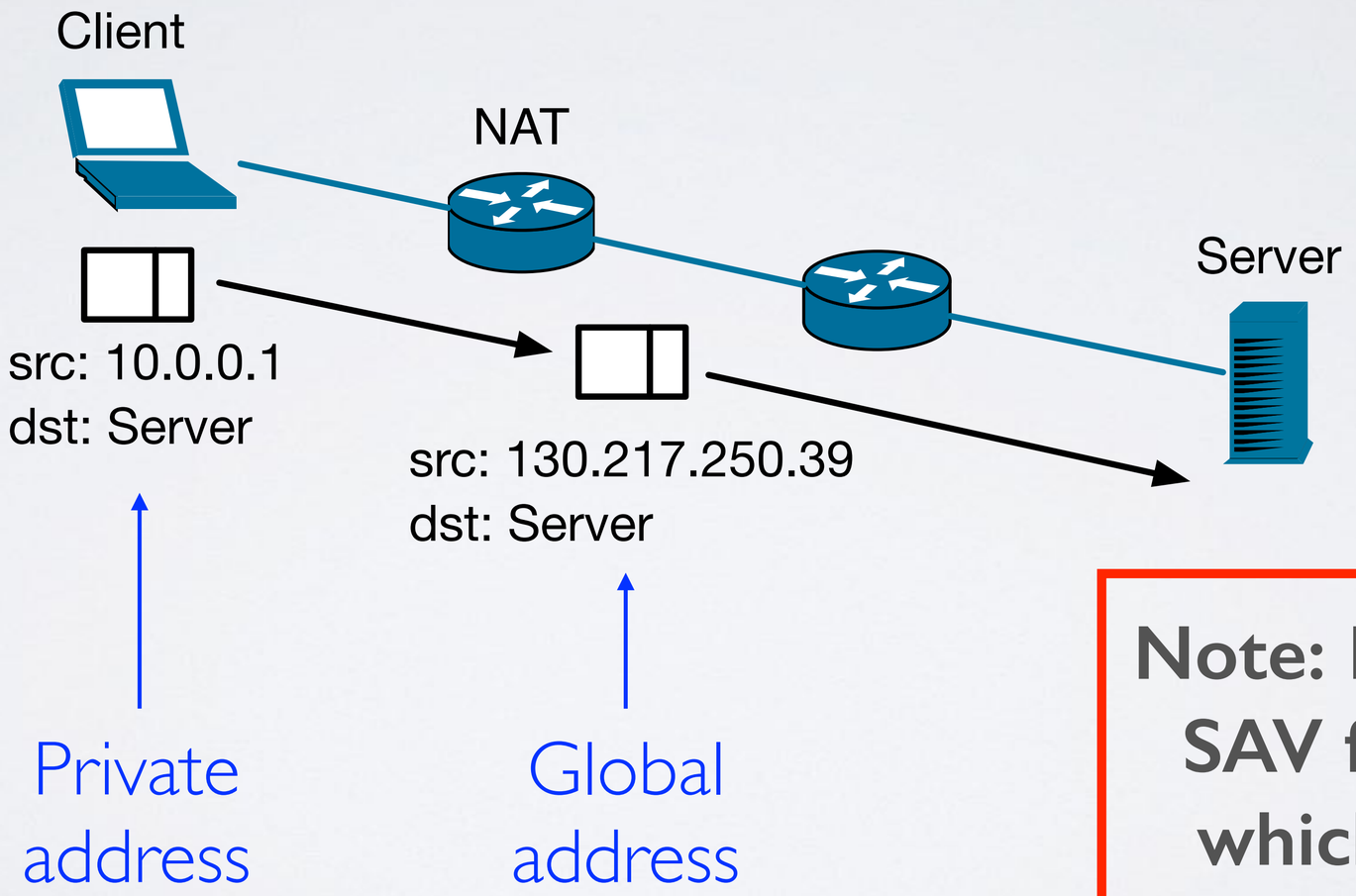
An **edge router** examines the source address of a packet.
It forwards packets with a reasonable source address given the network attachment point.

Approaches:
Reverse Path Forwarding (RPF)
Access Control Lists (ACLs)

SAV: Packets inbound to the network

SAV is different from NAT

A Network Address Translation (NAT) router modifies the source IP address of forwarded packets

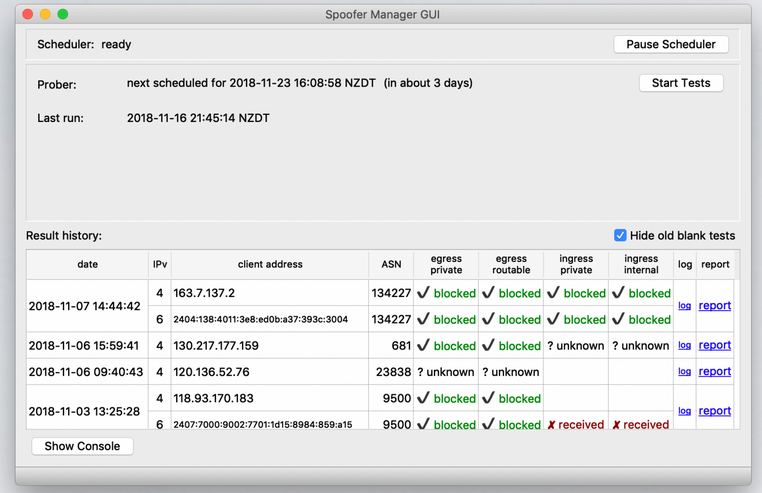


Note: NATs have two SAV failure modes, which we analyze.

Contributions

Contributions

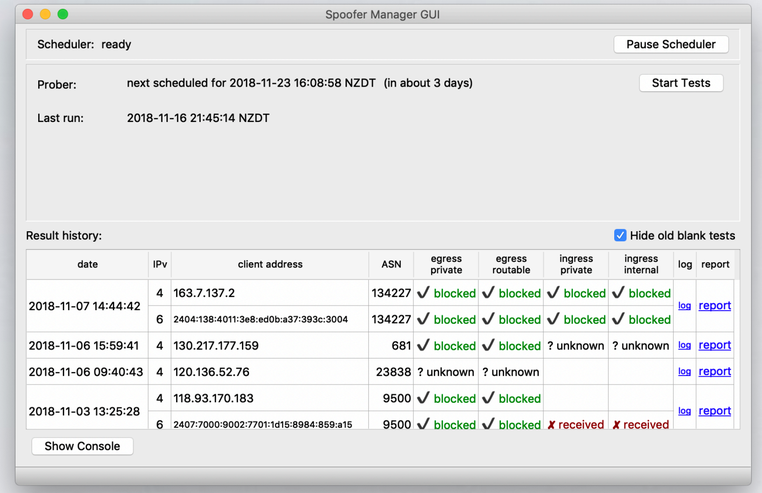
Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

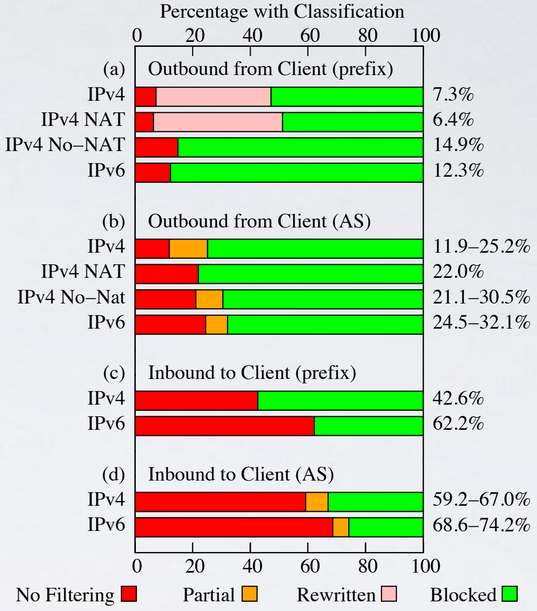
Contributions

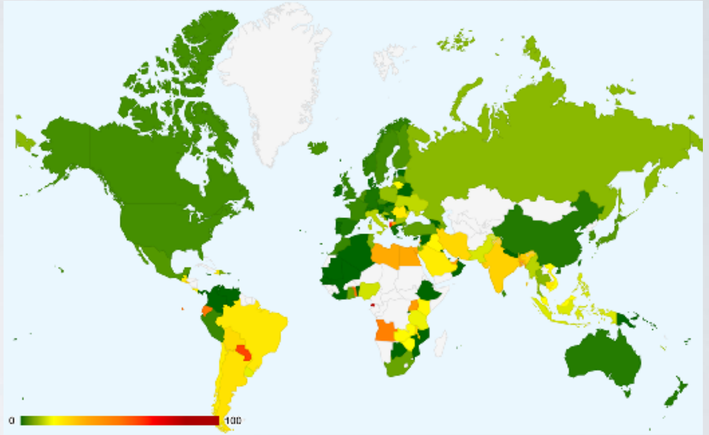
Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

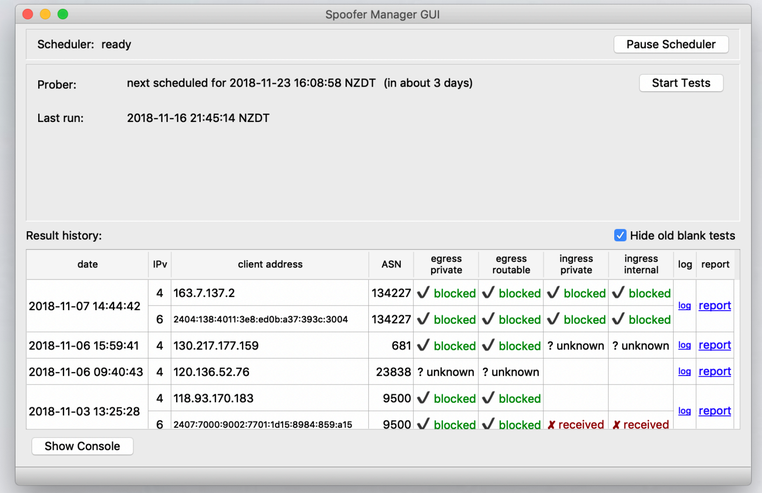
Data + Analysis





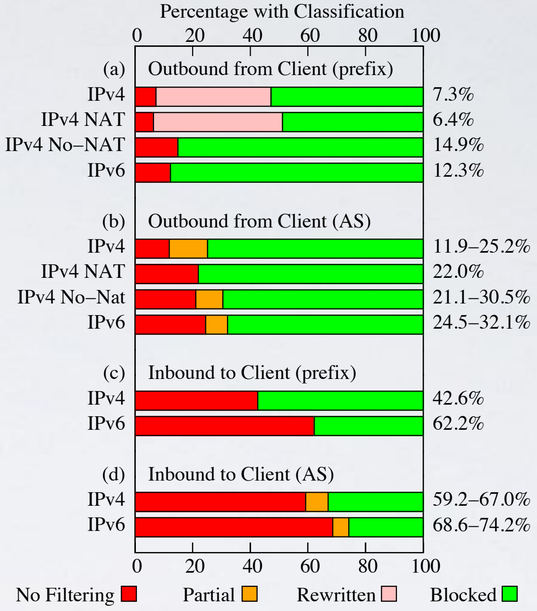
Contributions

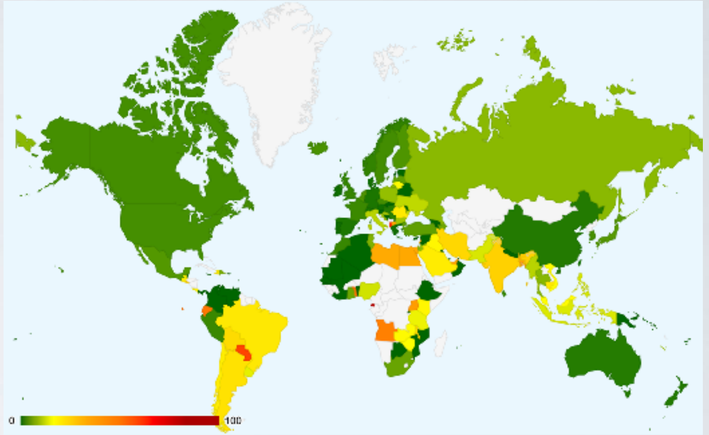
Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

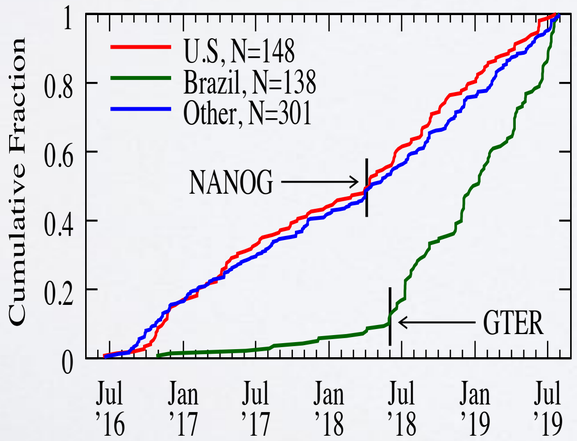
Data + Analysis





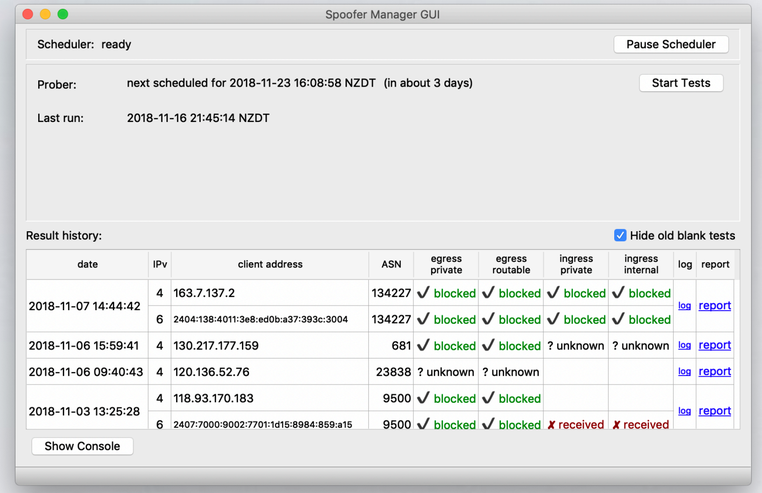
Remediation

```
From: Matthew Luckie <mjl@caida.org>
To: <abuse contact>
Subject: source IP address spoofing from <name of network>

While reviewing recent public tests from the CAIDA spoofer client

https://www.caida.org/projects/spoofer/

I came across one involving <name of network>. It seems that
based on the testing history for AS<num>, there is inadequate
filtering of IPv6 packets with invalid source addresses, so
packets with spoofed IPv6 source addresses can leave your
network. These systems can participate in volumetric denial of
service attacks. However, it seems that packets with spoofed
source IPv4 addresses are correctly being filtered. Further,
packets with spoofed source addresses claiming to be from inside
your network are not filtered when they arrive from outside your
network.

https://spoofer.caida.org/recent_tests.php?as_include=<num>

https://www.ietf.org/rfc/rfc2827.txt

Matthew
```



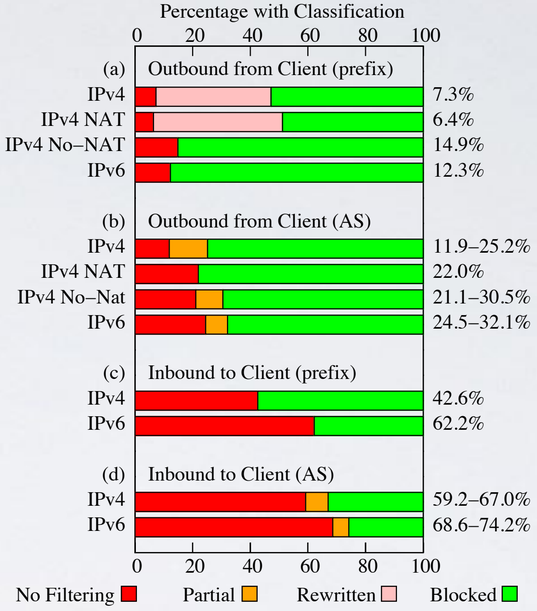
Contributions

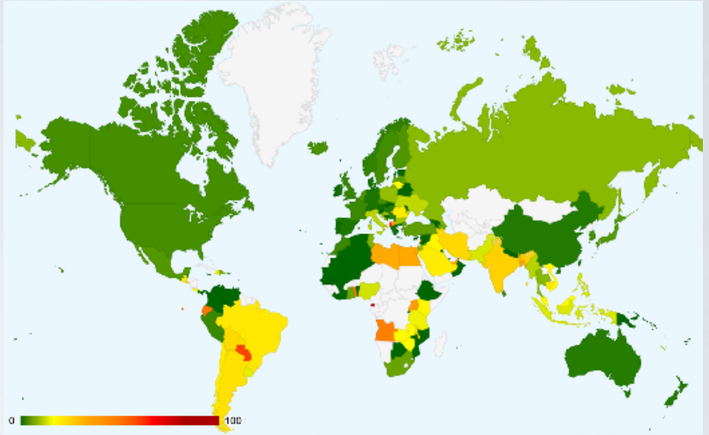
Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

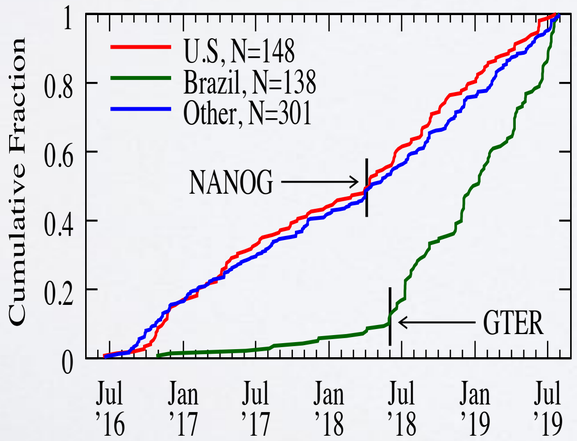
Data + Analysis





Remediation

```
From: Matthew Luckie <mjl@caida.org>
To: <abuse contact>
Subject: source IP address spoofing from <name of network>

While reviewing recent public tests from the CAIDA spoofer client

https://www.caida.org/projects/spoofer/

I came across one involving <name of network>. It seems that
based on the testing history for AS<num>, there is inadequate
filtering of IPv6 packets with invalid source addresses, so
packets with spoofed IPv6 source addresses can leave your
network. These systems can participate in volumetric denial of
service attacks. However, it seems that packets with spoofed
source IPv4 addresses are correctly being filtered. Further,
packets with spoofed source addresses claiming to be from inside
your network are not filtered when they arrive from outside your
network.

https://spoofer.caida.org/recent_tests.php?as_include=<num>

https://www.ietf.org/rfc/rfc2827.txt

Matthew
```



Incentives + Regulation

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Case 3:17-cv-00039-JD Document 90 Filed 09/19/17 Page 1 of 10

FEDERAL TRADE COMMISSION,
Plaintiff,
v.
D-LINK SYSTEMS, INC.,
Defendant.

Case No. 3:17-cv-00039-JD

ORDER RE MOTION TO DISMISS

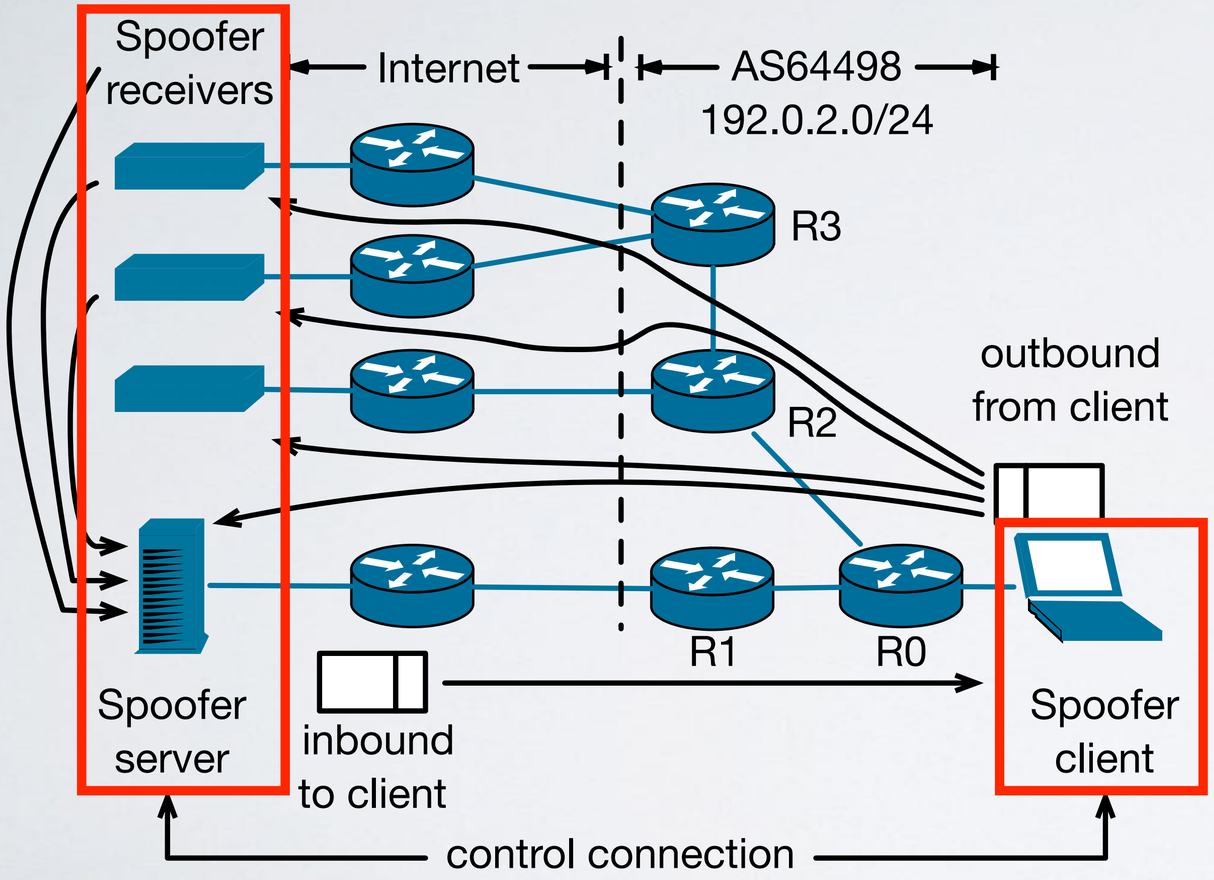
Re: Dkt. No. 25

Spoofer Report for NANOG for Sep 2019

CAIDA Spoofer Project spoofer-info at caida.org
Tue Oct 8 17:00:06 UTC 2019

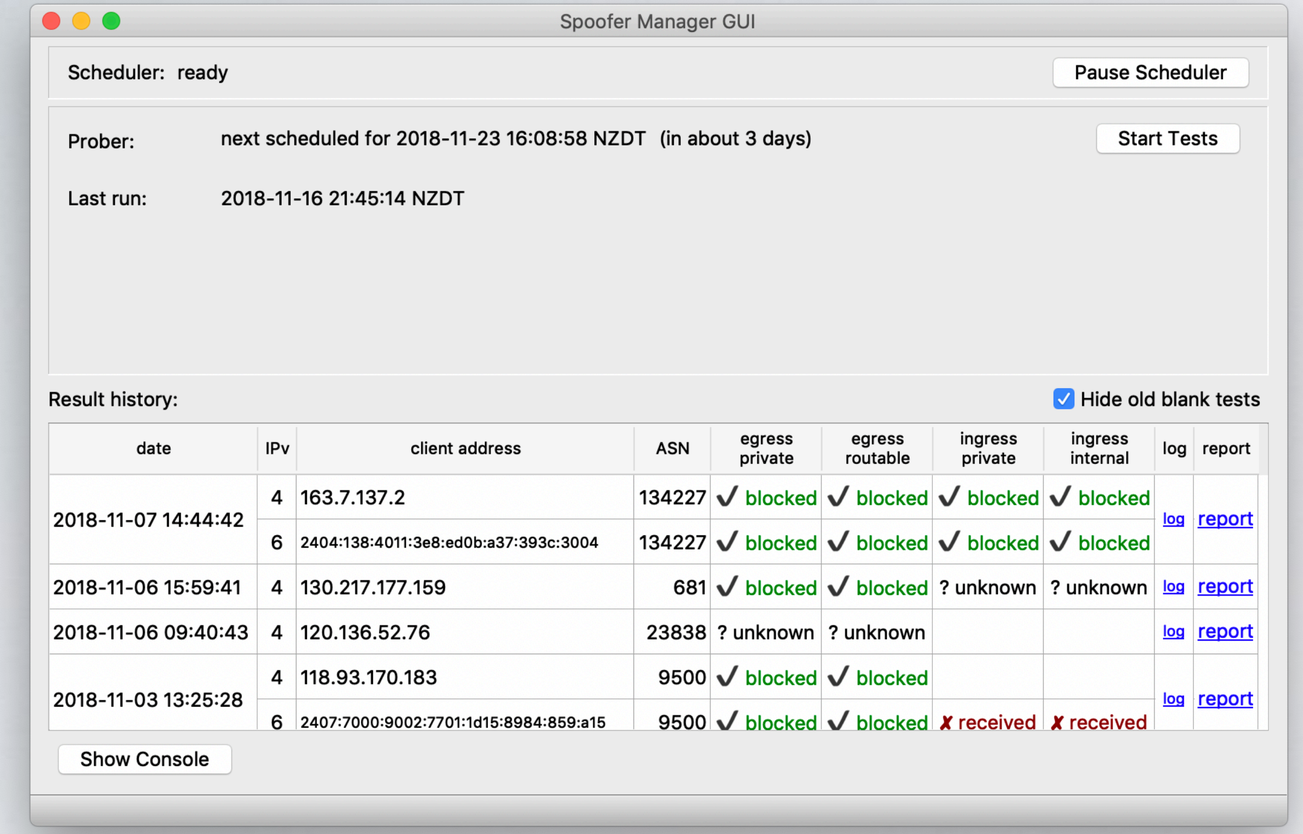
Contribution: Infrastructure

https://spoofer.caida.org/



- We built a measurement infrastructure to support data collection and analysis
  - **Crowdsourced collection by volunteers**
  - Operators also use our client to check their SAV compliance
- We continue to operate the platform to study and motivate remediation

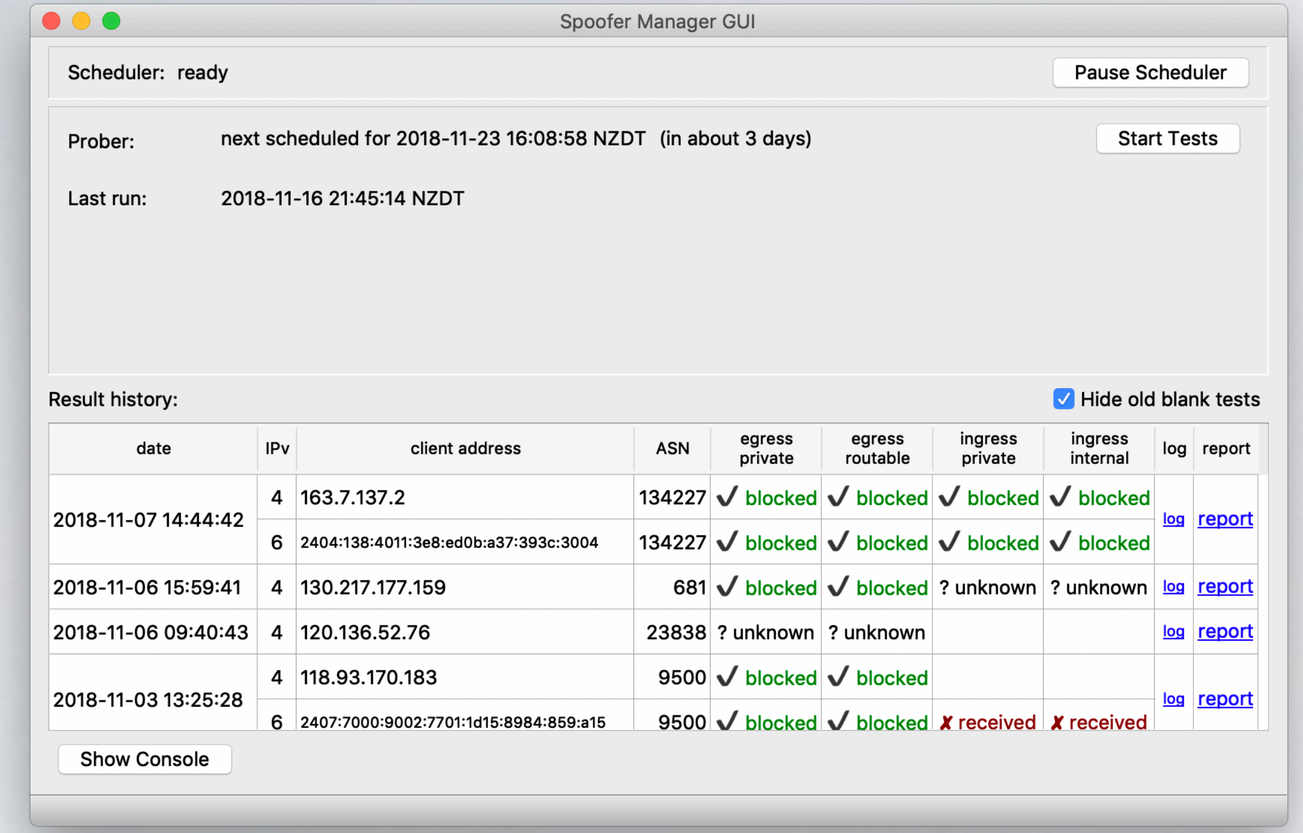
Contribution: Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

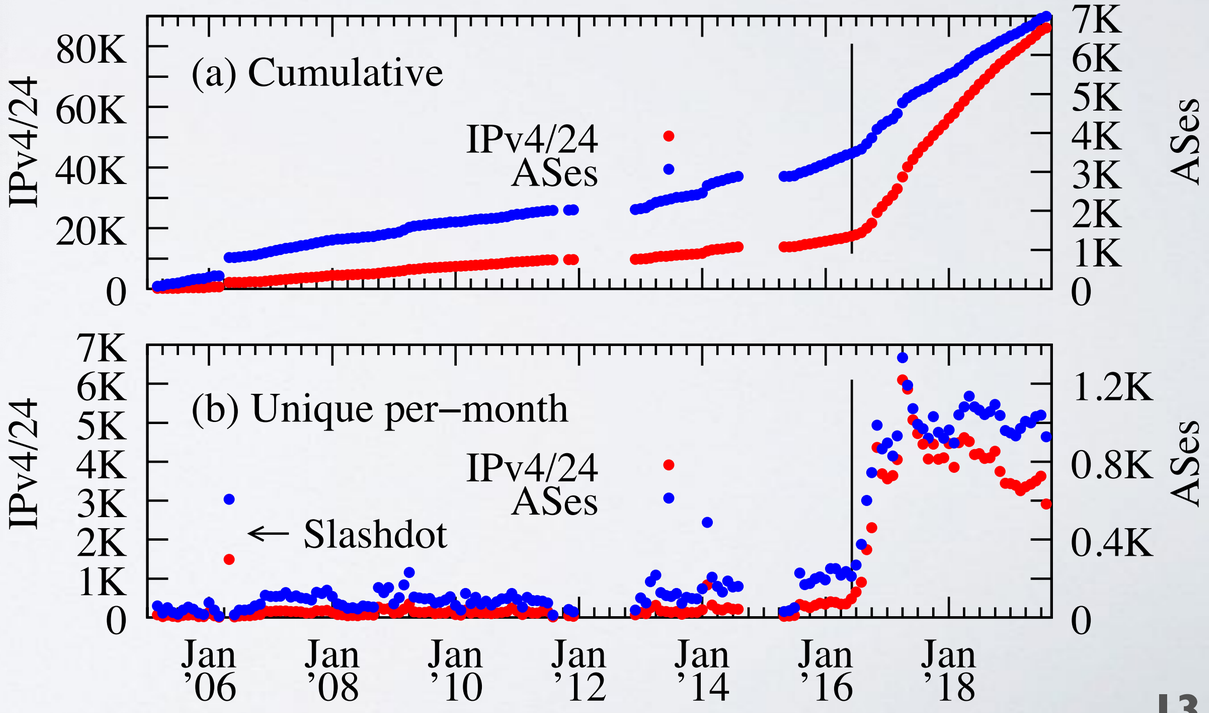
Client with GUI for Windows, MacOS, and Linux automatically tests networks once per week

Contribution: Infrastructure



date	IPv	client address	ASN	egress private	egress routable	ingress private	ingress internal	log	report
2018-11-07 14:44:42	4	163.7.137.2	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked	log	report
	6	2404:138:4011:3e8:ed0b:a37:393c:3004	134227	✓ blocked	✓ blocked	✓ blocked	✓ blocked		
2018-11-06 15:59:41	4	130.217.177.159	681	✓ blocked	✓ blocked	? unknown	? unknown	log	report
2018-11-06 09:40:43	4	120.136.52.76	23838	? unknown	? unknown			log	report
2018-11-03 13:25:28	4	118.93.170.183	9500	✓ blocked	✓ blocked			log	report
	6	2407:7000:9002:7701:1d15:8984:859:a15	9500	✓ blocked	✓ blocked	✗ received	✗ received		

Client with GUI for Windows, MacOS, and Linux automatically tests networks once per week



From **3410** IPv4 ASes in May 2016 to **6938** in August 2019 — **10.6%** of routed ASes.
Tests from ~1K ASes per month

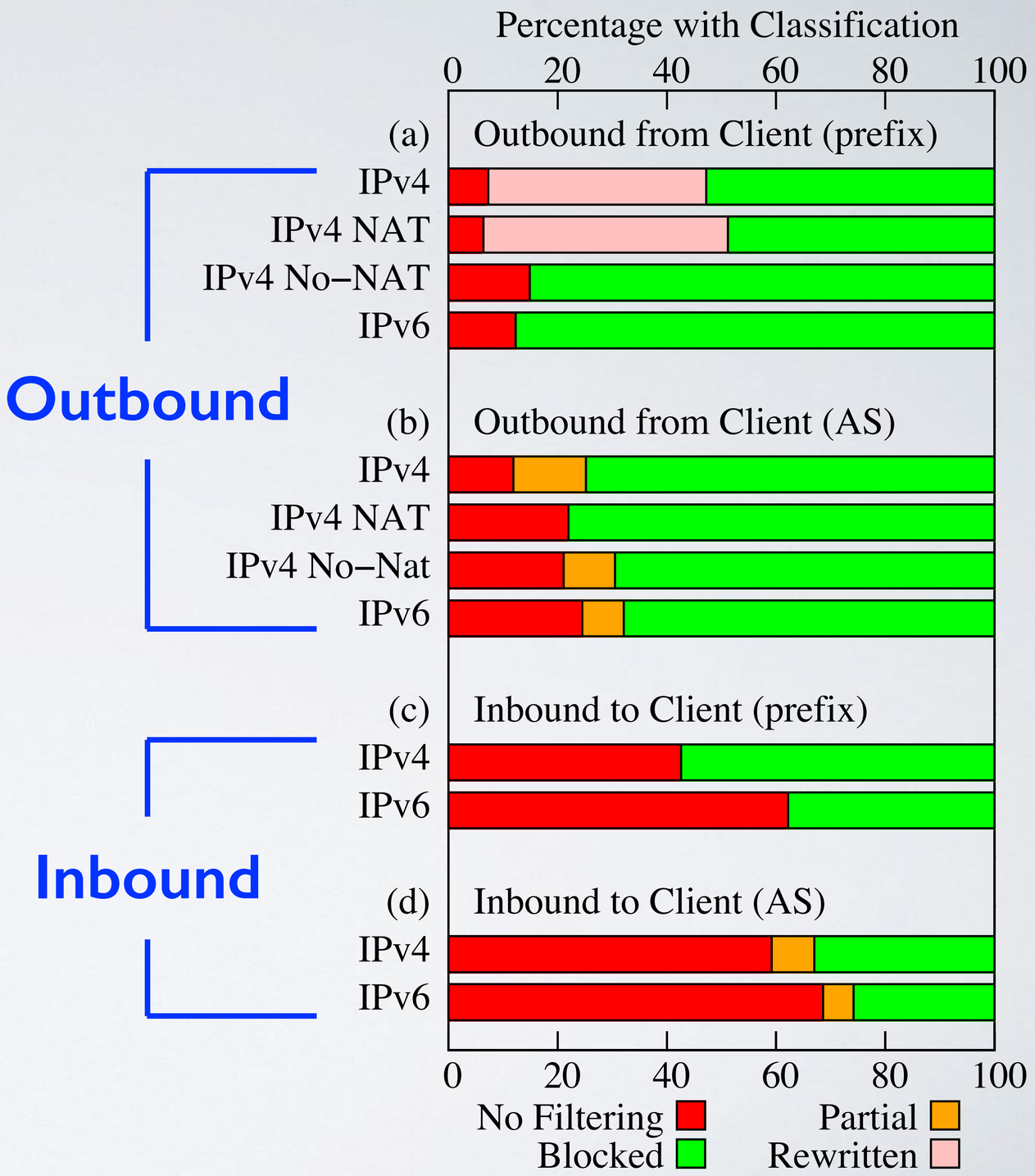
Legend:

No Filtering: Spoofed packets are not blocked.

Partial: An AS blocks spoofed packets for some prefixes.

Rewritten: Spoofed source address translated by a NAT

Blocked: Spoofed packets are blocked.

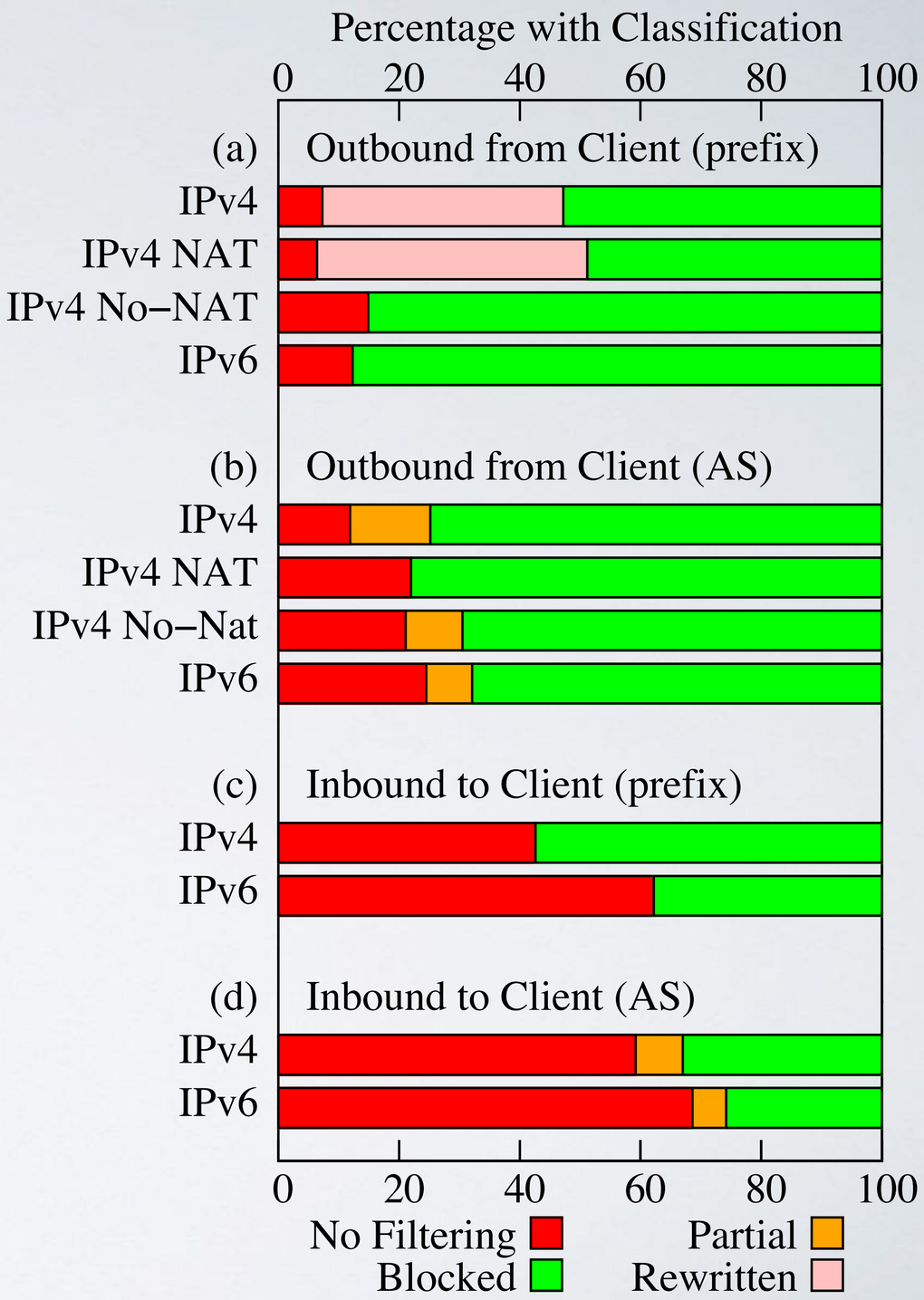


August 2018 - August 2019

NAT does not block ability to spoof in IPv4

Could spoof from **6.4%** of **21K** IPv4/24 prefixes where NAT was present.

Could spoof from **14.9%** of **2.7K** IPv4/24 prefixes where NAT was not present.



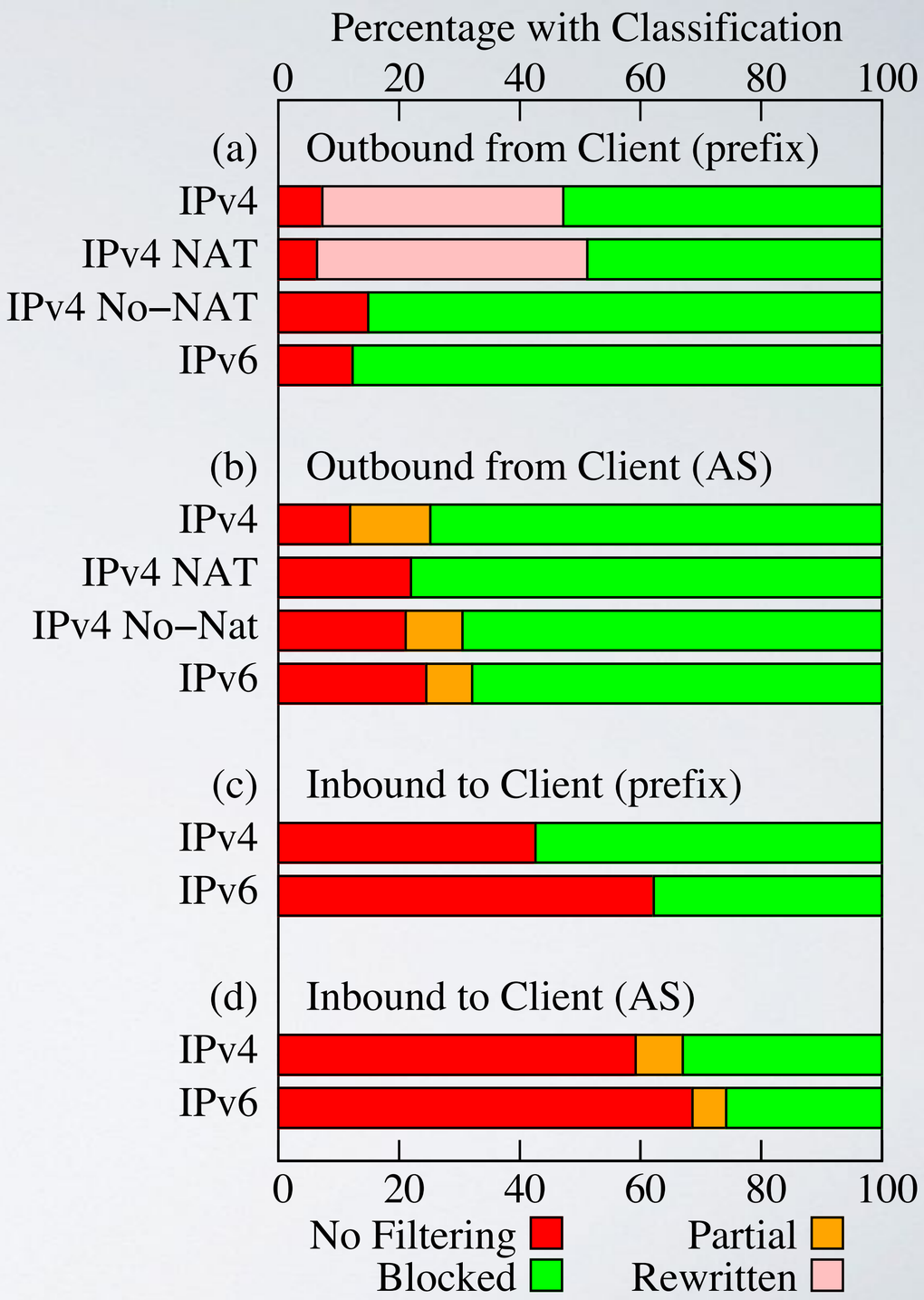
August 2018 - August 2019

NAT does not block ability to spoof in IPv4

Could spoof from **6.4%** of **21K** IPv4/24 prefixes where NAT was present.

Could spoof from **14.9%** of **2.7K** IPv4/24 prefixes where NAT was not present.

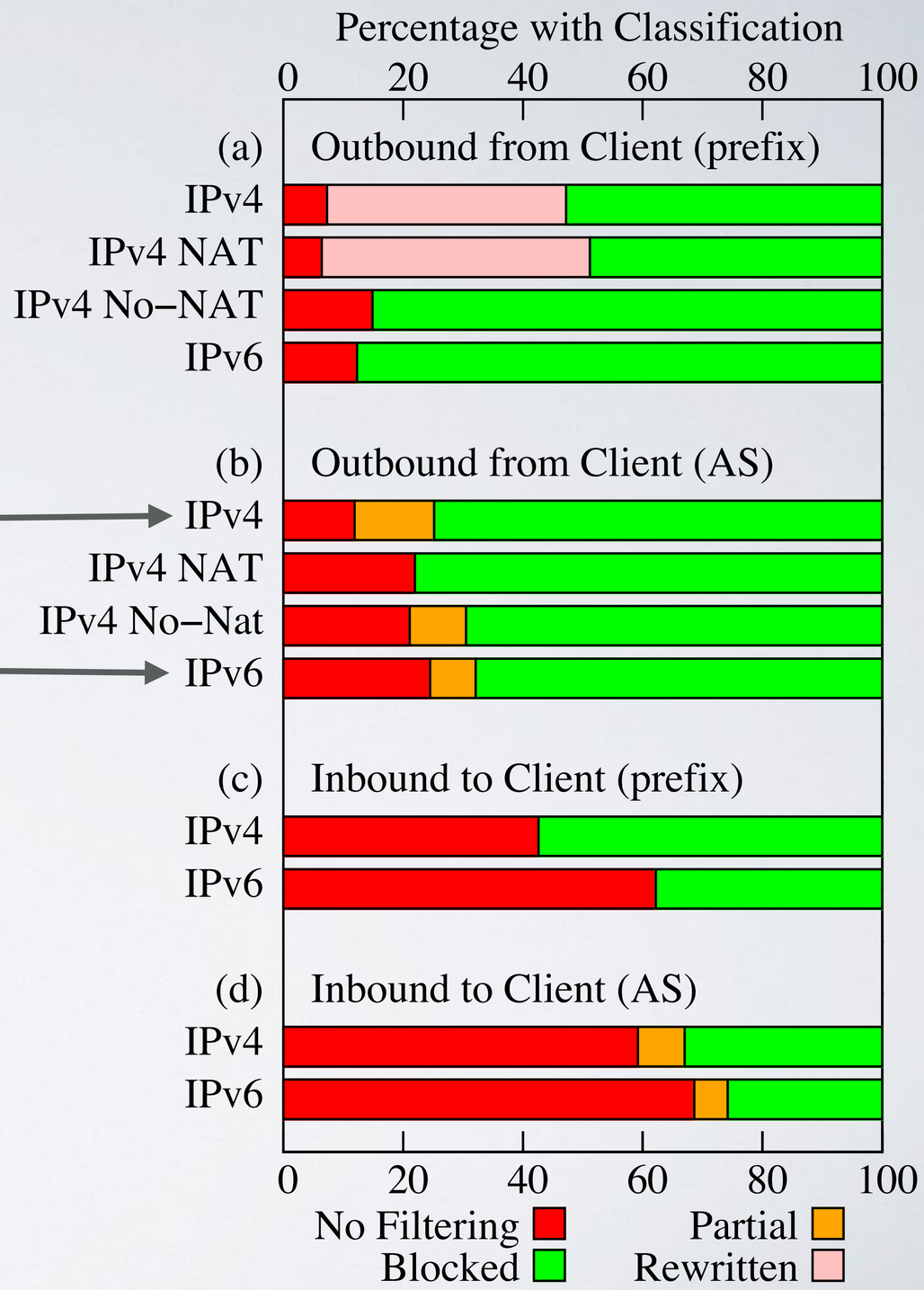
Could spoof from **12.3%** of **2.2K** IPv6/40 prefixes.



August 2018 - August 2019

SAV deployment is inconsistent at the AS-level

25.2% of **2.8K** IPv4 ASes and **32.1%** of **593** IPv6 ASes had at least one prefix where operators allowed spoofing.



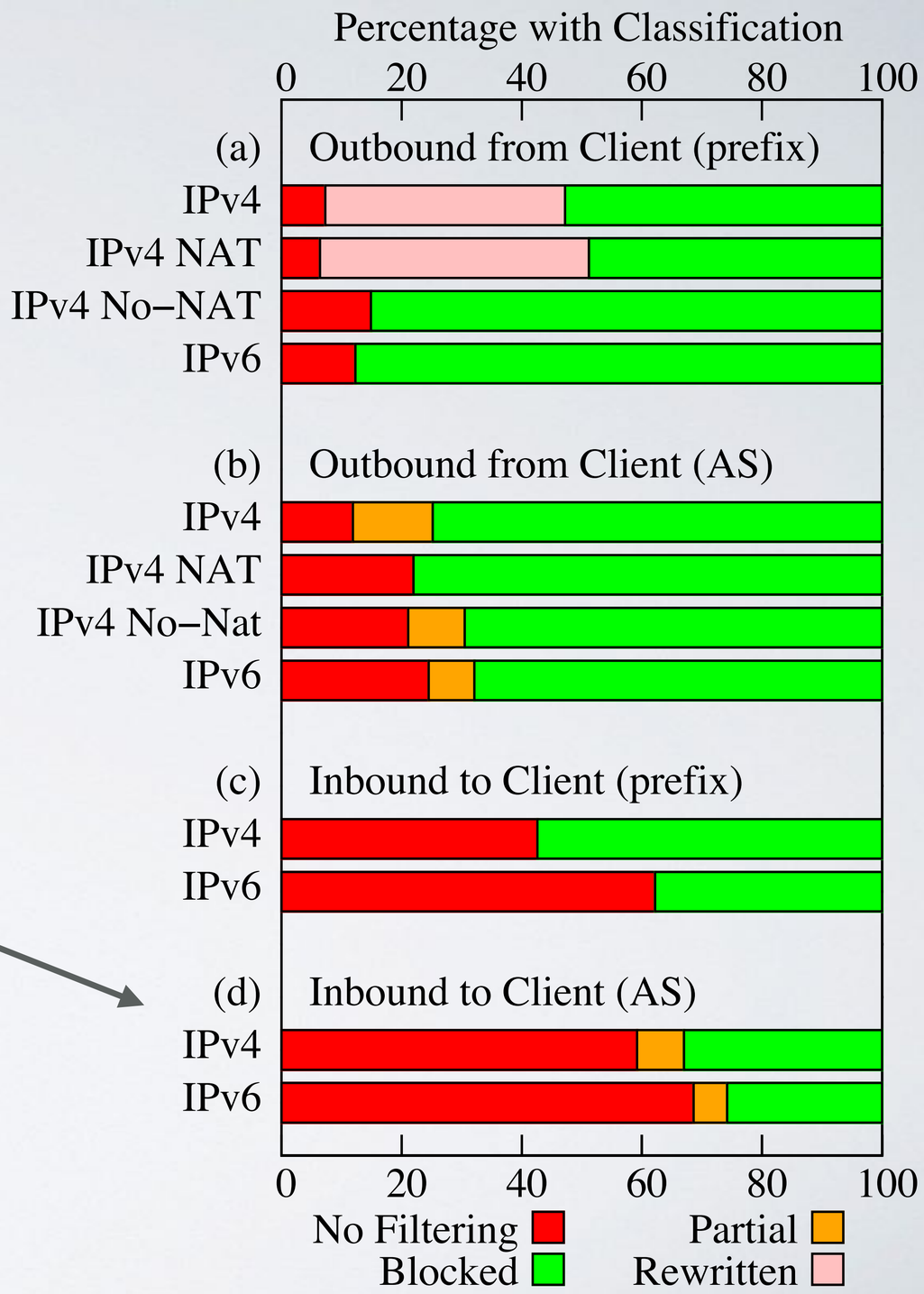
August 2018 - August 2019

Inbound filtering is less deployed than outbound filtering

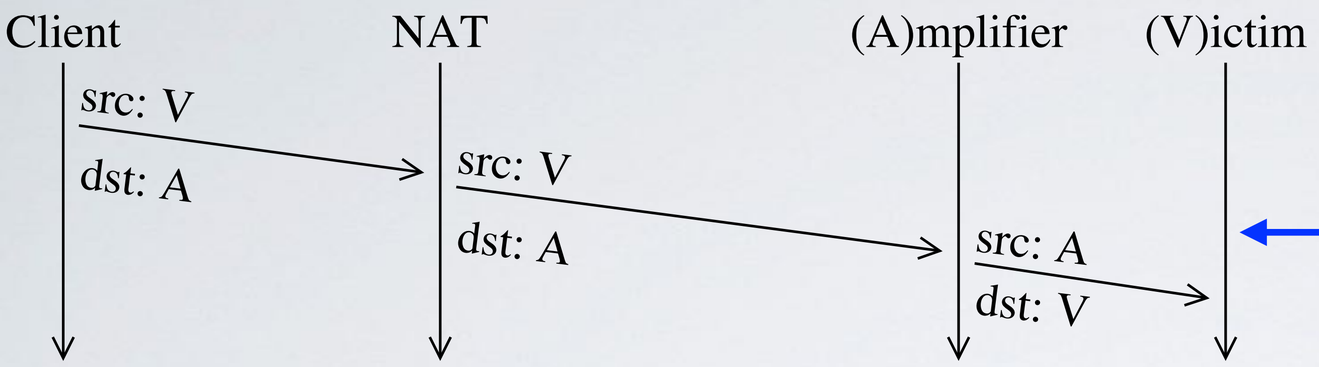
(despite being incentive compatible!)

67.0% of **552** IPv4 ASes, and **74.2%** of **376** IPv6 ASes do not block packets claiming to be from within their network that arrive from outside their network.

August 2018 - August 2019



Two NAT Failure Modes



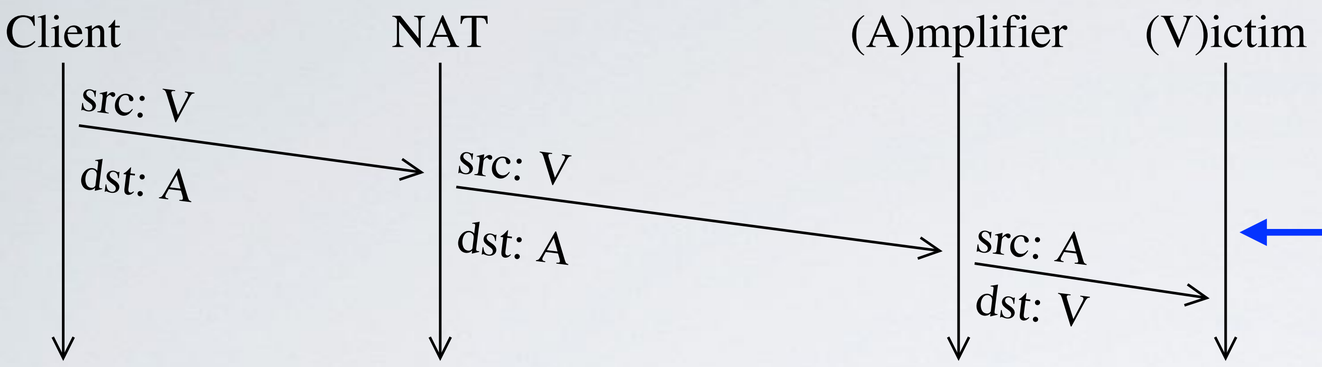
(11 months: Sep 2018 to Aug 2019)

NAT forwards packet intact without rewriting spoofed source address.

3.0% of NAT IPs

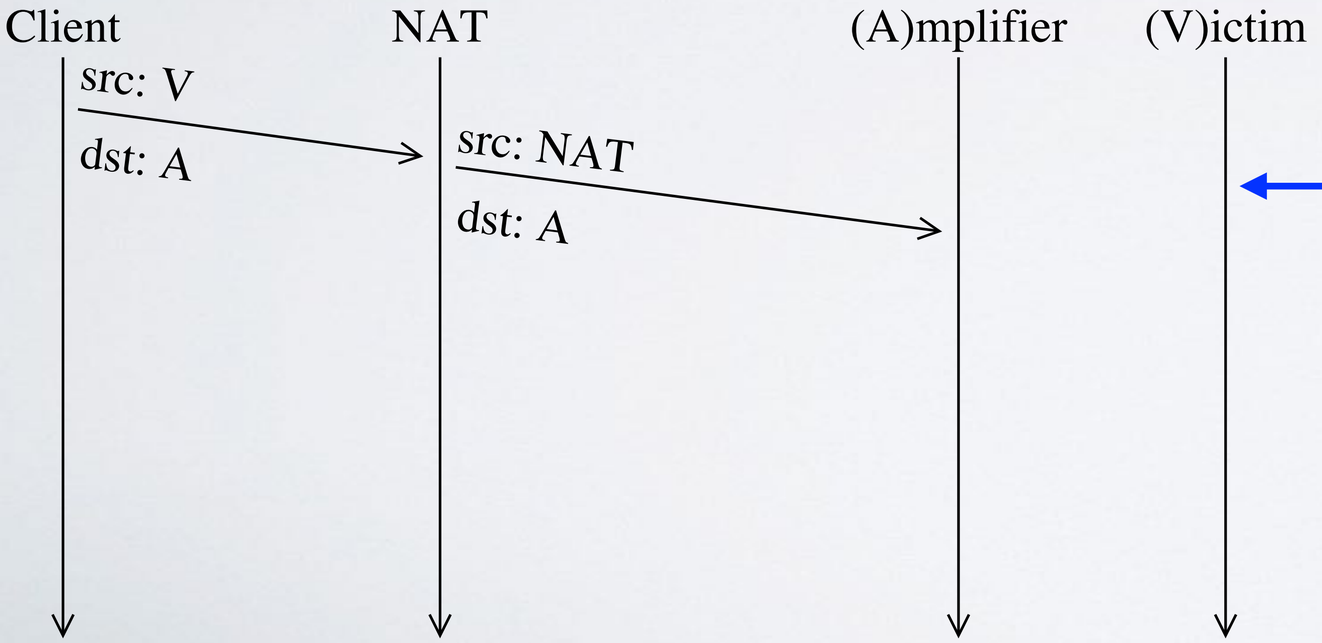
Two NAT Failure Modes

(11 months: Sep 2018 to Aug 2019)



NAT forwards packet intact without rewriting spoofed source address.

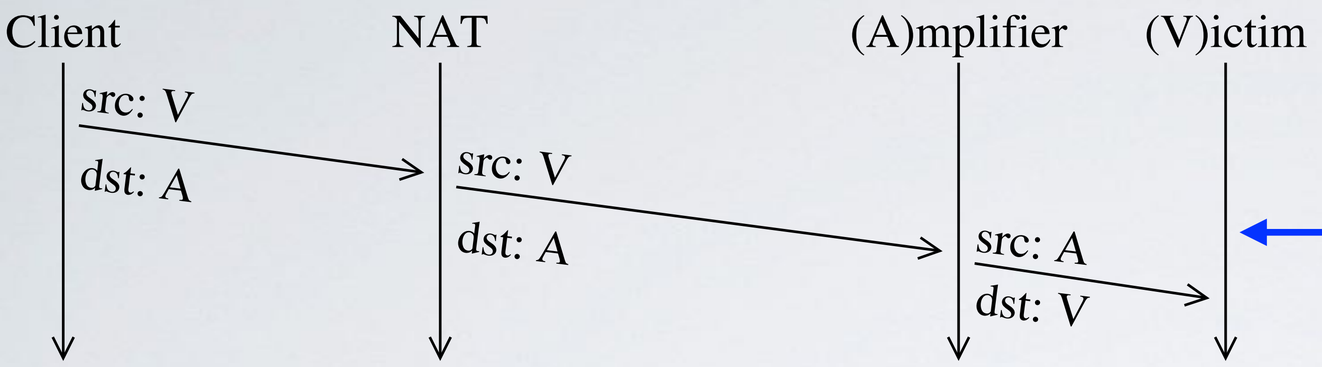
3.0% of NAT IPs



NAT rewrites spoofed source address and forwards the packet.

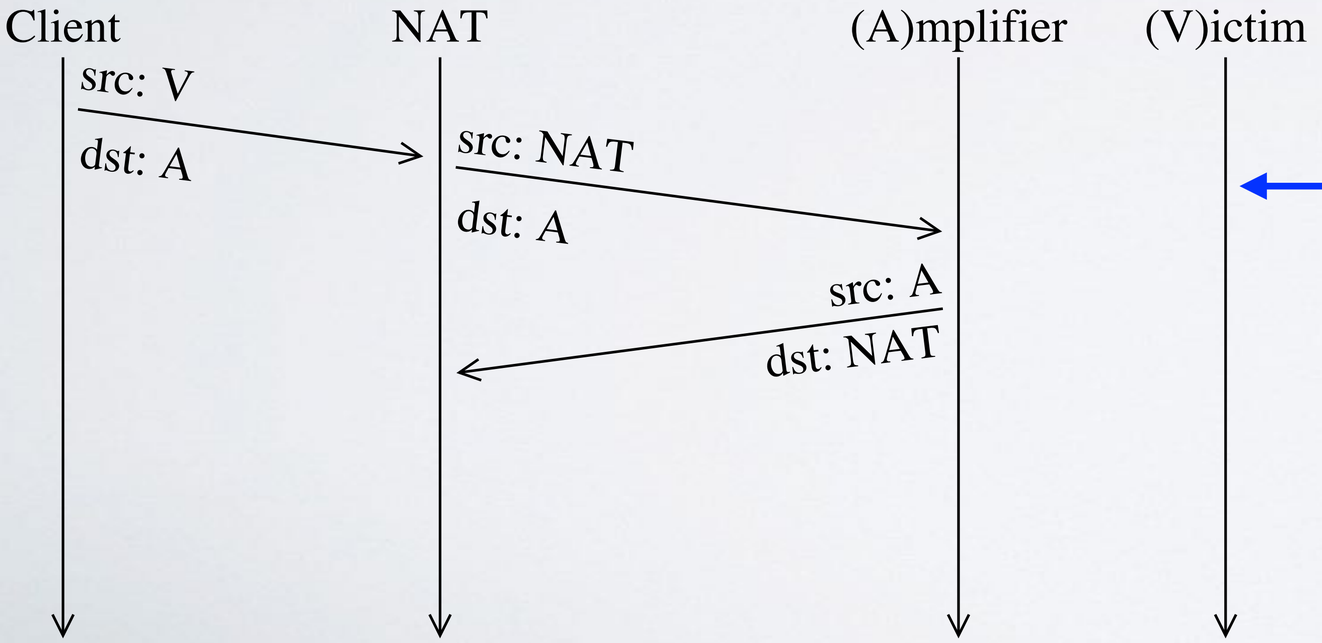
Two NAT Failure Modes

(11 months: Sep 2018 to Aug 2019)



NAT forwards packet intact without rewriting spoofed source address.

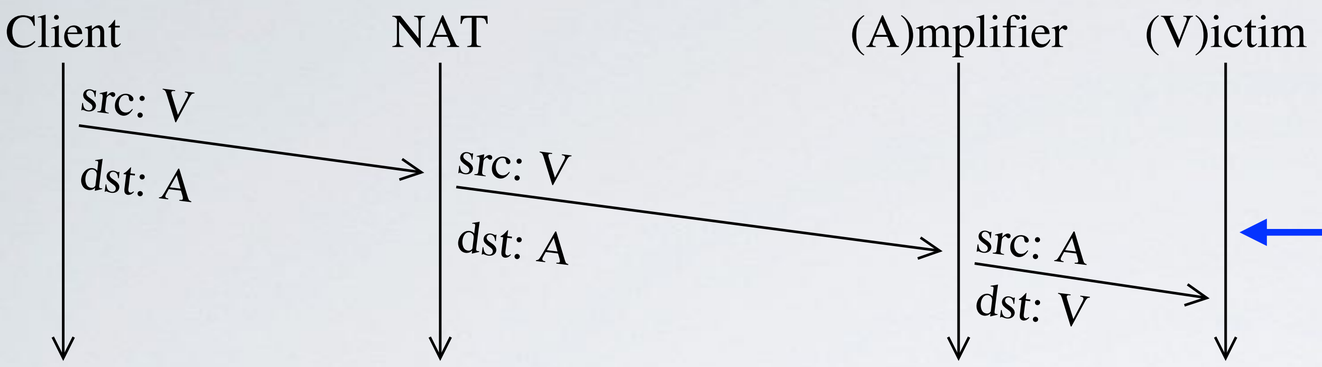
3.0% of NAT IPs



NAT rewrites spoofed source address and forwards the packet.

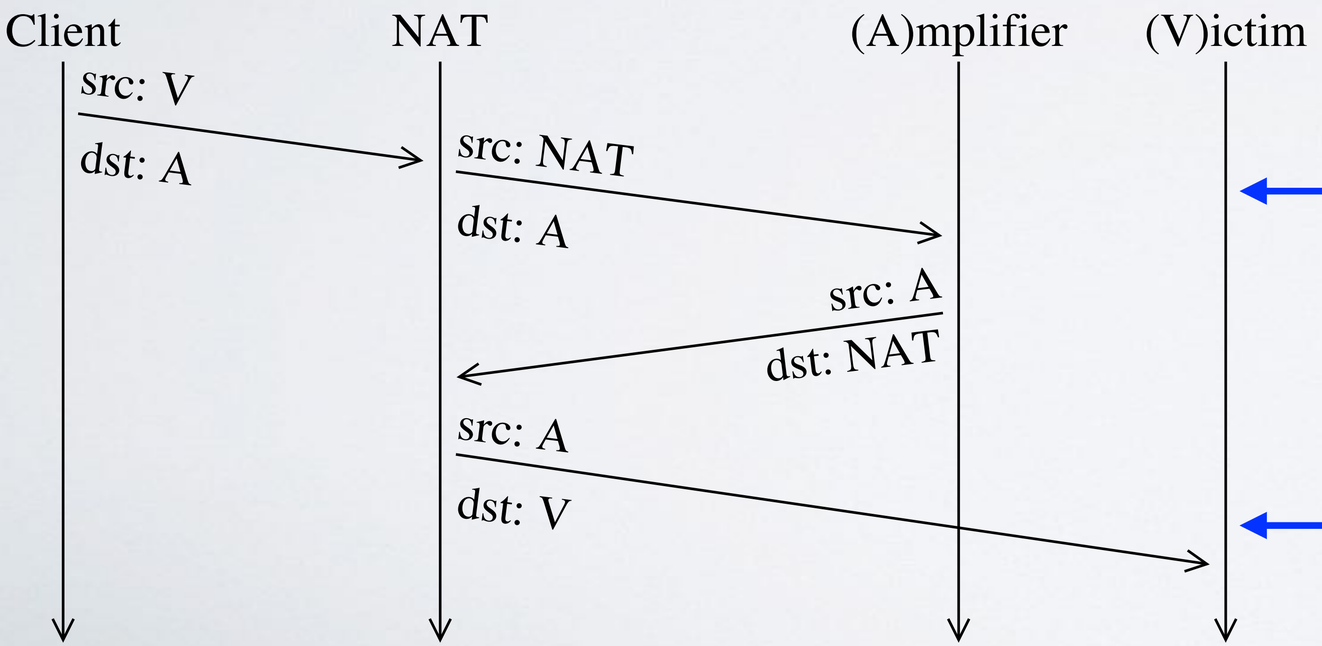
Two NAT Failure Modes

(11 months: Sep 2018 to Aug 2019)



NAT forwards packet intact without rewriting spoofed source address.

3.0% of NAT IPs



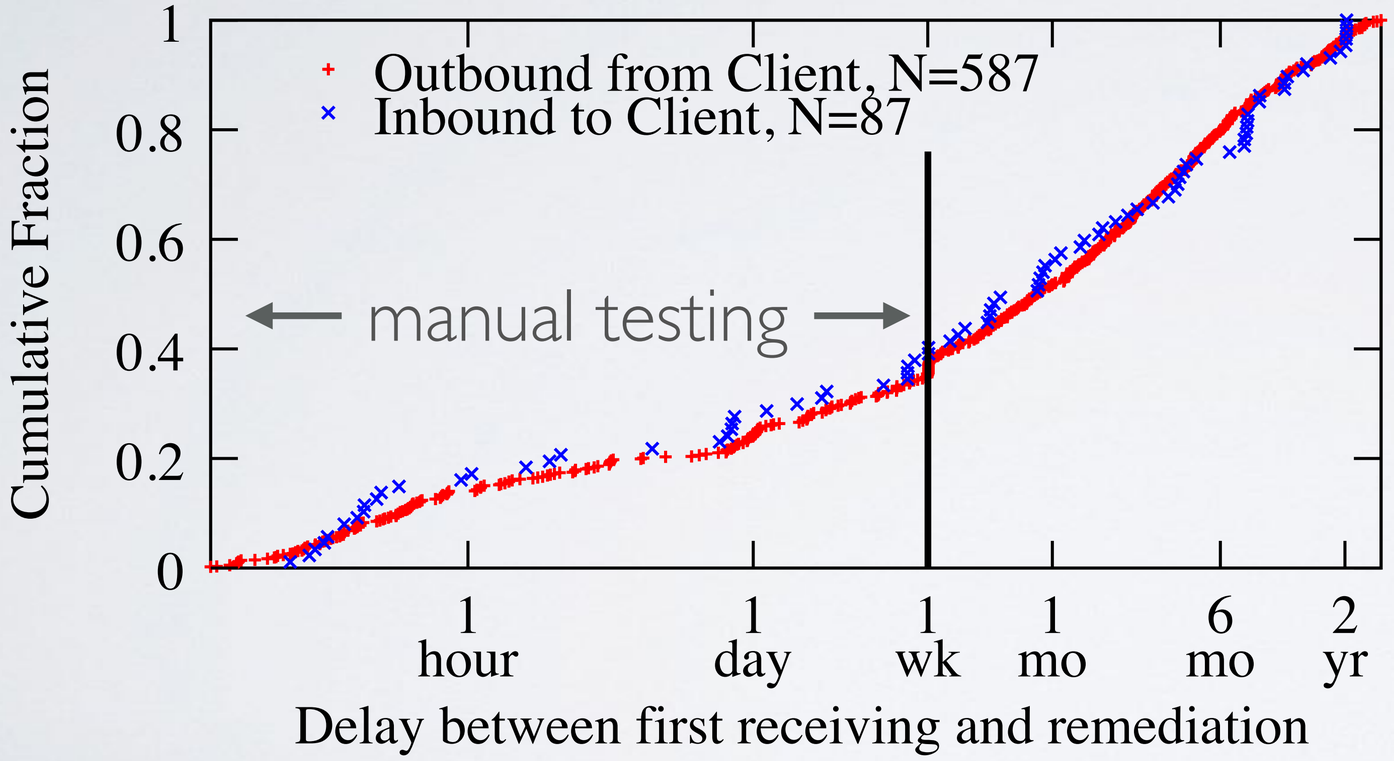
NAT rewrites spoofed source address and forwards the packet.

3.2% of NAT IPs

NAT translates the destination address and forwards the response.

Contribution: Remediation

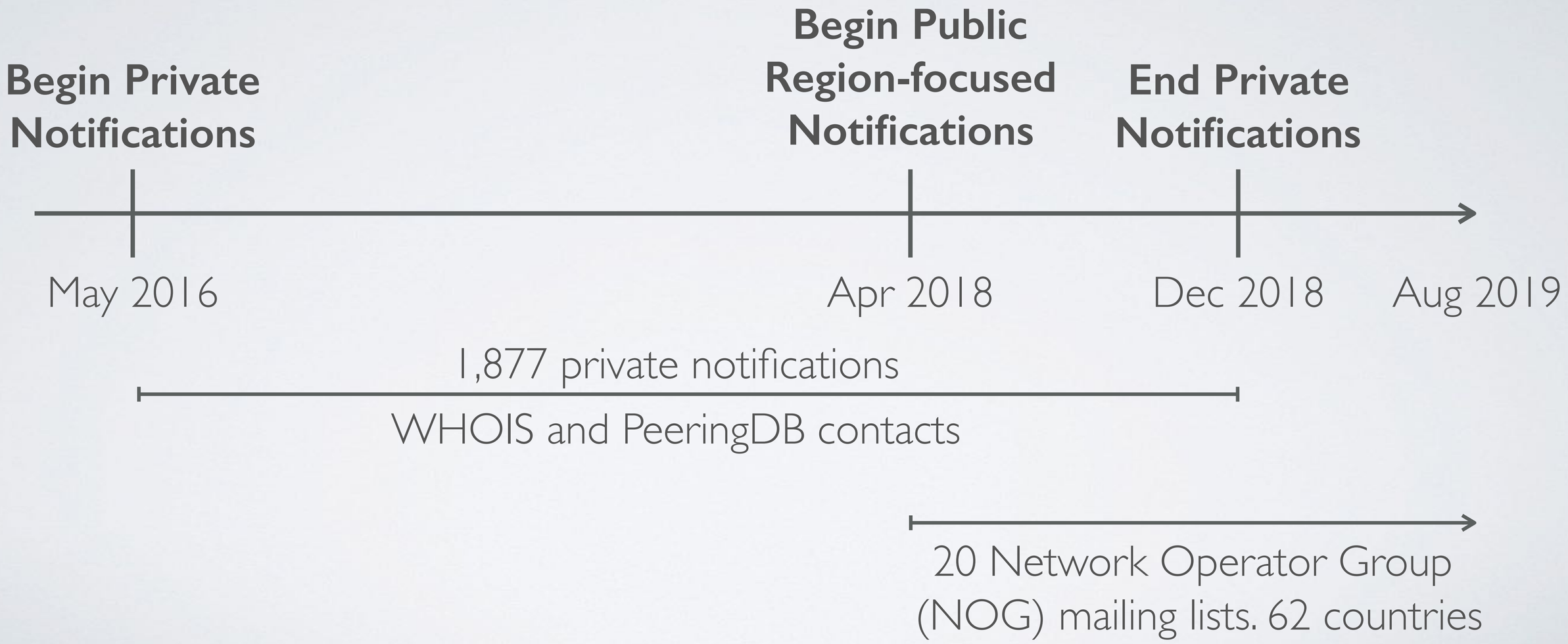
Remediation: tests within a prefix go from allowing spoofing to blocking spoofing.



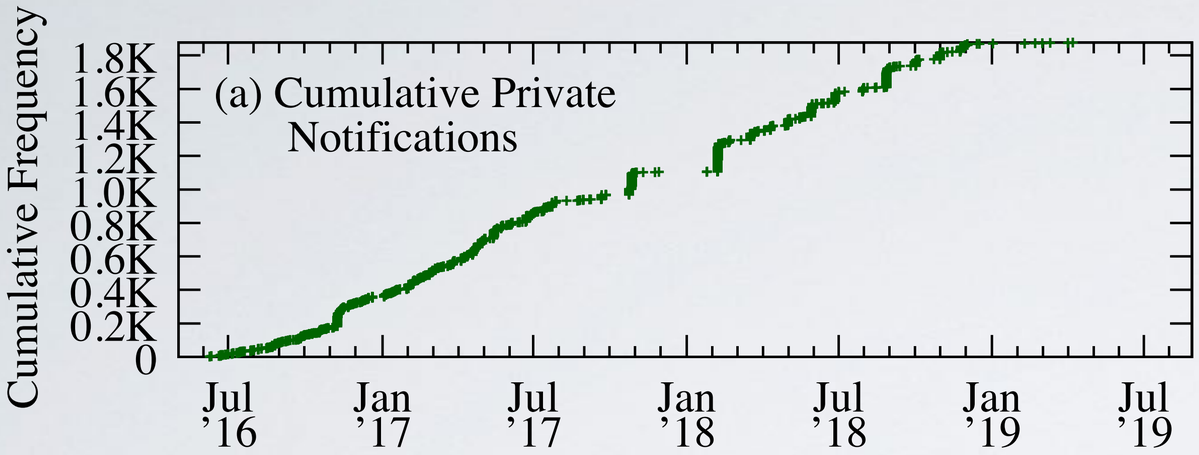
- **587 outbound, 87 inbound,** across IPv4 and IPv6
- **35.4% occurred within a week,** i.e., client was used by an operator in the network to deploy SAV

Analyzing Impact of Remediation Efforts

Cannot easily conduct A/B testing to measure effect of interventions on remediation because we do not control testing

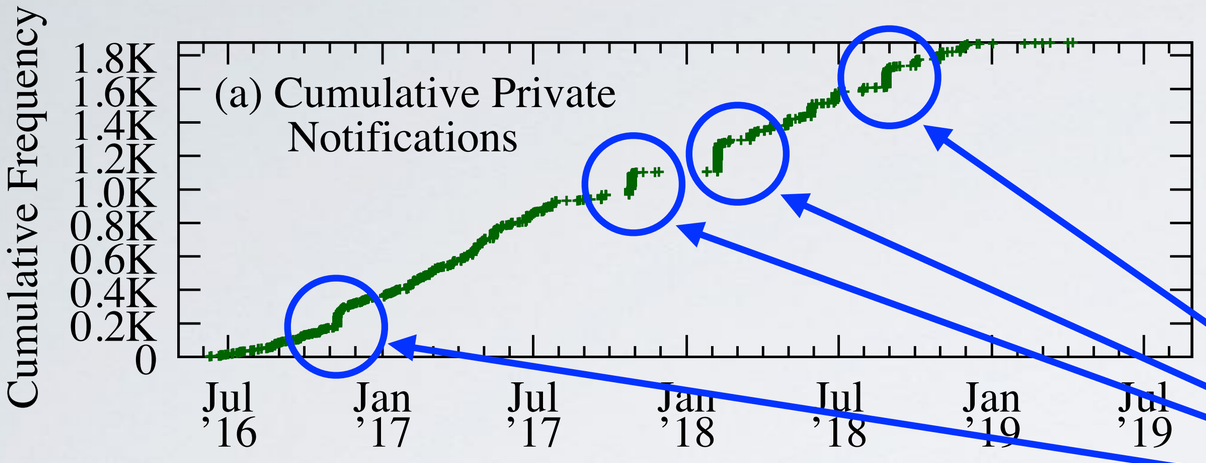


Remediation Impact Across Time



1,877 Private Notifications, ending Jan 2019

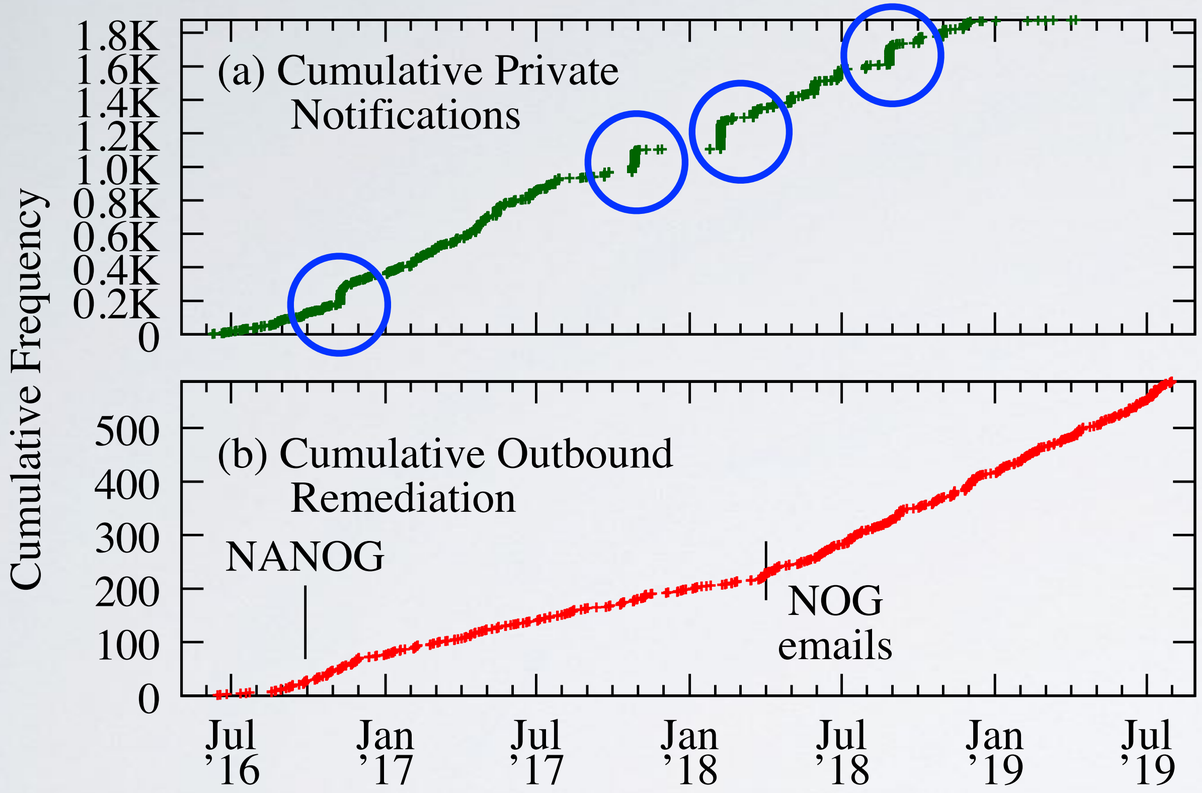
Remediation Impact Across Time



1,877 Private Notifications, ending Jan 2019

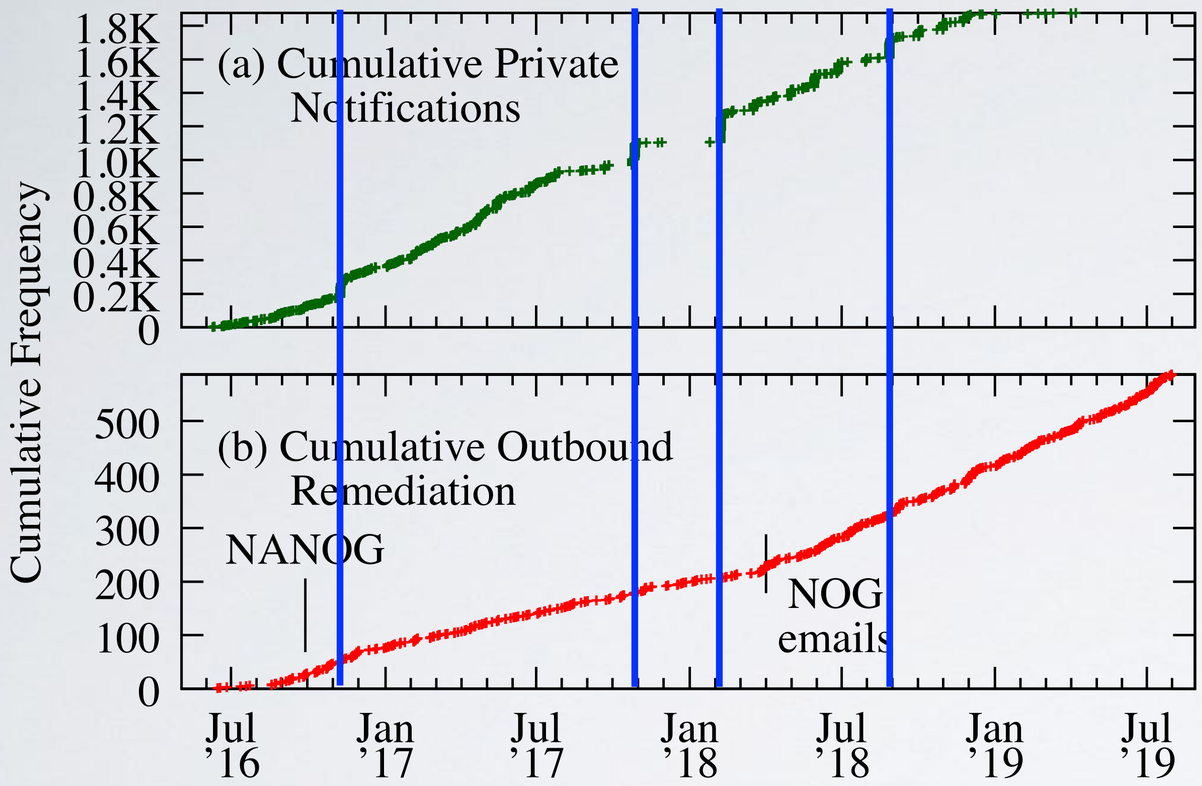
Private Notification Bursts

Remediation Impact Across Time



587 outbound remediation inferences between May 2016 and August 2019.

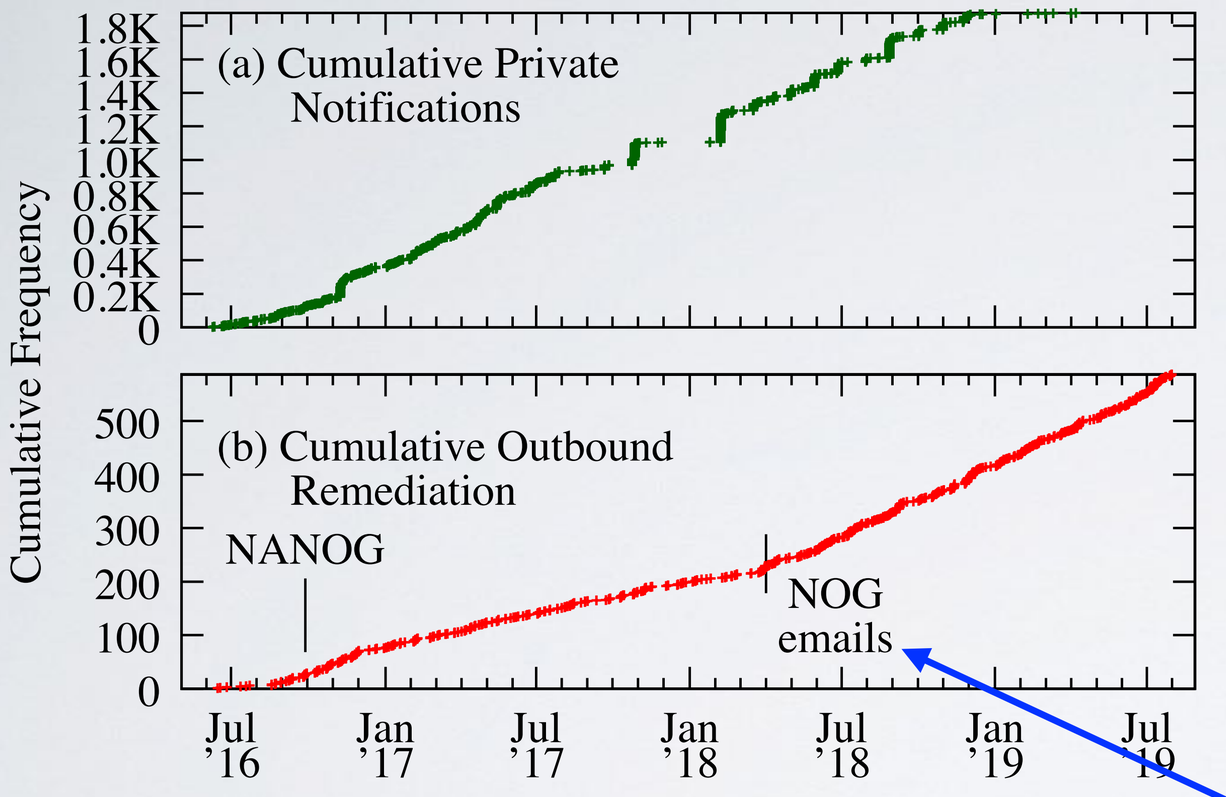
Remediation Impact Across Time



587 outbound remediation inferences between May 2016 and August 2019.

Private Notification Bursts had limited impact on remediation.

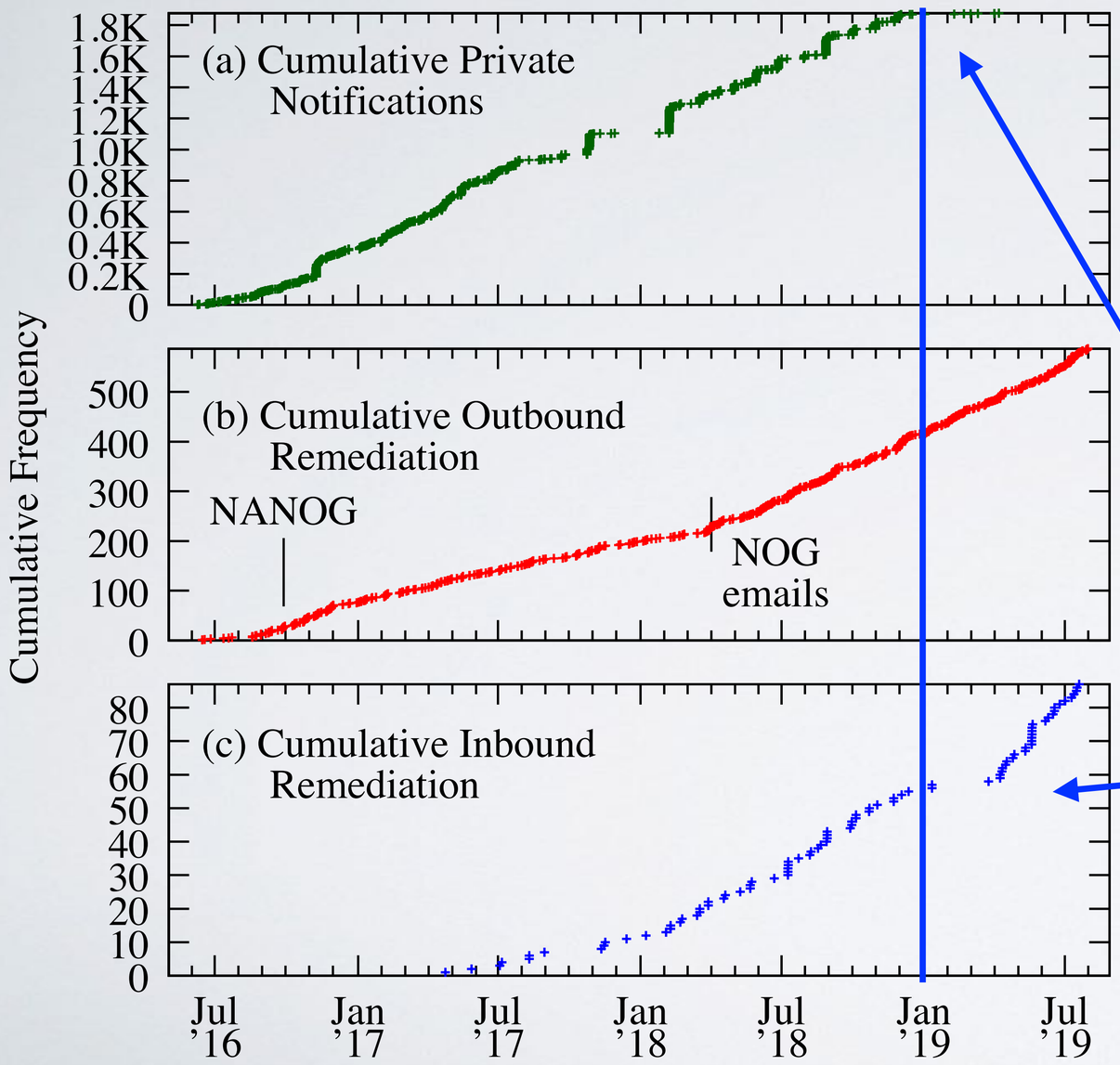
Remediation Impact Across Time



587 outbound remediation inferences between May 2016 and August 2019.

Increase in outbound remediation after Network Operator Group (NOG) emails commence is a combination of more tests and increase in remediation rate.

Remediation Impact Across Time

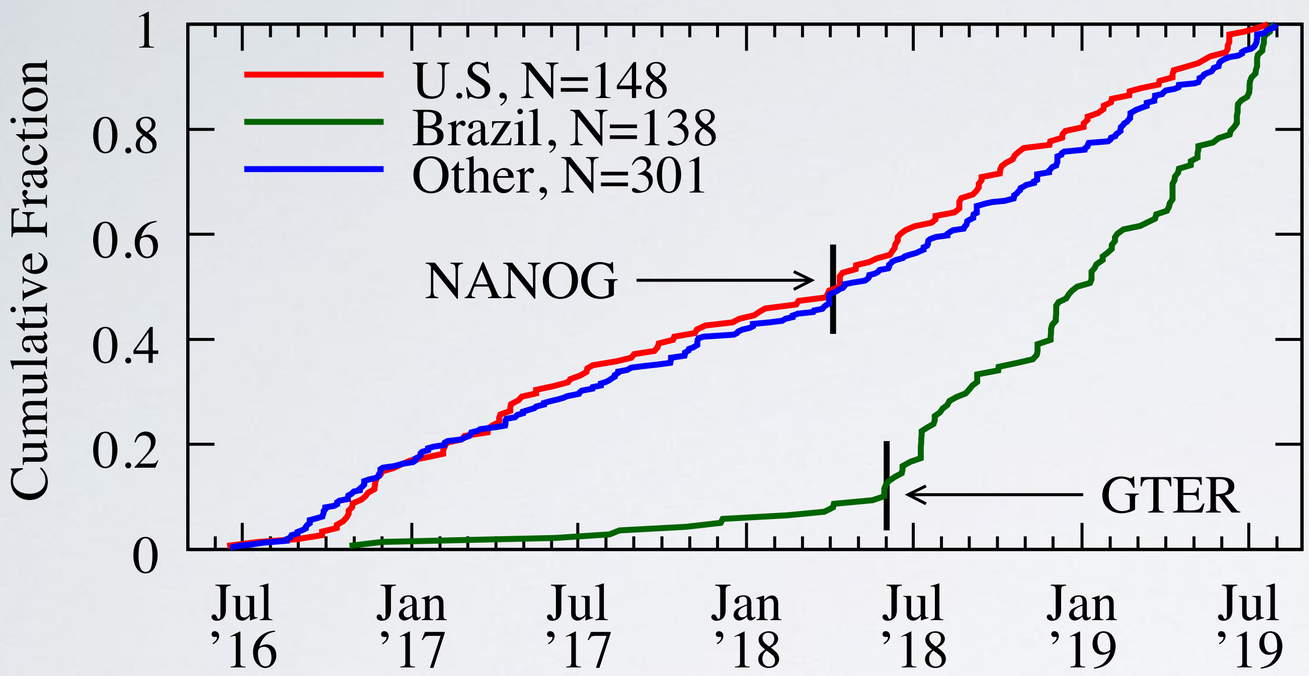


87 inbound remediation inferences between May 2016 and August 2019.

Halting notifications appeared to halt inbound remediation.

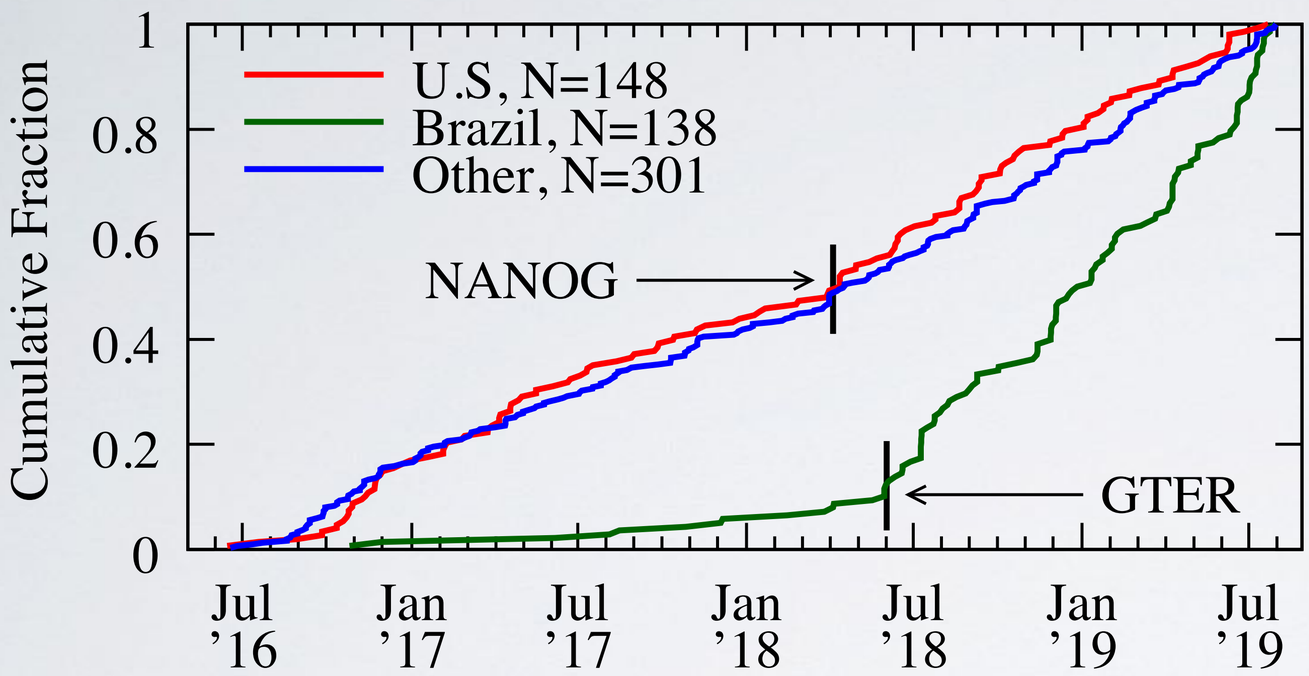
However, inbound remediation resumed in March 2019.

Impact of Public Notifications



- Of the 587 remediation events
  - 25.2% in U.S., 23.5% in Brazil
  - ~90% of observed remediations in Brazil occurred after our NOG emails
- Coincided with the beginning of NIC.br's "Program for a Safer Internet" which provides SAV training and lectures

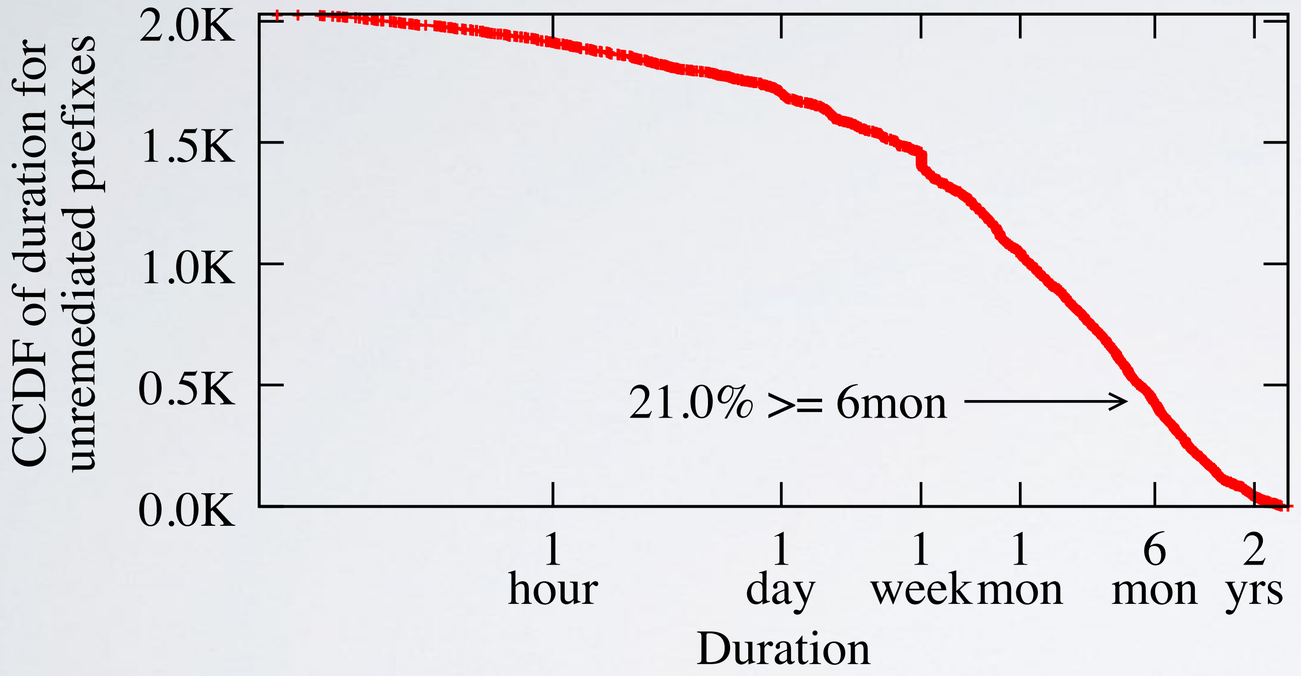
Impact of Public Notifications



- Of the 587 remediation events
  - 25.2% in U.S., 23.5% in Brazil
  - ~90% of observed remediations in Brazil occurred after our NOG emails
- Coincided with the beginning of NIC.br's "Program for a Safer Internet" which provides SAV training and lectures

	Year Before	Year After
US + CA (NANOG)	21 of 132 (16%)	35 of 147 (24%)
Brazil (GTER)	14 of 67 (21%)	52 of 168 (31%)

Long tail of unremediated networks



- Remediation inferred for 352 IPv4/24s between May 2016 and August 2019
- 2,030 spoofable IPv4/24s with multiple tests and no evidence of remediation
  - i.e., ~6x more unremediated IPv4/24s than remediated.
- 21.0% have been unremediated for at least six months

Moving the Needle: Internalizing Negative Externality

Moving the Needle: Internalizing Negative Externality

Moving the Needle: Internalizing Negative Externality

Assume Altruism in Network Operations

Idea: network operators want to do the right thing

Details in the paper

- **Private notification emails**
  - Limited impact on remediation, substantially more unremediated prefixes than remediated

Assume Altruism in Network Operations

Idea: network operators want to do the right thing

Details in the paper

DONE

- **Private notification emails**
  - Limited impact on remediation, substantially more unremediated prefixes than remediated
- **Grassroots efforts**
  - Mutually Assured Norms for Routing Security (MANRS)

Assume Altruism in Network Operations

Idea: network operators want to do the right thing

Details in the paper

- **Private notification emails**
  - Limited impact on remediation, substantially more unremediated prefixes than remediated

DONE

- **Grassroots efforts**
  - Mutually Assured Norms for Routing Security (MANRS)

DONE

- **Carrots**
  - National Science Foundation (NSF) Campus Cyberinfrastructure (CC*) funding 2014-2016 encouraged applicants to comment on their SAV policy and to run spoofer

Assume Altruism in Network Operations

Idea: network operators want to do the right thing

Details in the paper

- **Private notification emails**
  - Limited impact on remediation, substantially more unremediated prefixes than remediated

DONE

- **Grassroots efforts**
  - Mutually Assured Norms for Routing Security (MANRS)

DONE

- **Carrots**
  - National Science Foundation (NSF) Campus Cyberinfrastructure (CC*) funding 2014-2016 encouraged applicants to comment on their SAV policy and to run spoofer

DONE

Ineffective as economic theory would predict.
We empirically established this ineffectiveness.

Liability - Challenges

Idea: devices and networks that allow spoofing pay for damages

- **Attribution**
  - Hard to identify where spoofed packets come from

`Details in the paper`

Liability - Challenges

Idea: devices and networks that allow spoofing pay for damages

`Details in the paper`

- **Attribution**
  - Hard to identify where spoofed packets come from
- **Theory of Common Carriage**
  - Networks not responsible for content

Liability - Challenges

Idea: devices and networks that allow spoofing pay for damages

Details in the paper

- **Attribution**
  - Hard to identify where spoofed packets come from
- **Theory of Common Carriage**
  - Networks not responsible for content
- **Assessing Damages**
  - Difficult to establish damages caused by individual devices or networks (e.g. U.S. FTC vs. D-Link after MIRAI)

FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras

Insurance and Industry Standards - Challenges

Idea: Networks that do not deploy SAV pay higher insurance premiums

Details in the paper

- **Industry Standards**
  - Inbound SAV is a requirement in Payment Card Industry Data Security Standard (PCI DSS, requirement 1.3.3)
  - Our results indicate Inbound SAV is generally not well deployed

Insurance and Industry Standards - Challenges

Idea: Networks that do not deploy SAV pay higher insurance premiums

`Details in the paper`

- **Industry Standards**
  - Inbound SAV is a requirement in Payment Card Industry Data Security Standard (PCI DSS, requirement 1.3.3)
  - Our results indicate Inbound SAV is generally not well deployed
- **Insurance**
  - How would insurance companies enforce?
  - Networks may not know if they have correctly implemented SAV
  - Now we have a system — https://spoofer.caida.org

Regulating Government Procurement

Idea: government procurement standards can spur wider deployment

- Office of Management and Budget (OMB) policy
  - DNSSEC - 2008
  - IPv6 - 2010
  - HTTPS - 2015
- SAV in National Institute of Standards and Technology (NIST) guidelines
- SAV nearly in Federal Risk and Authorization Management Program (FEDRAMP) technology acquisition guidelines for federal agencies:
  - cloud providers assert "too hard to implement"
  - Similar to FCC's Anti-Bot Code (ABC) of conduct for ISPs 2012
    - Multi-stakeholder group, voluntary guidelines
    - ISPs asked by FCC to publicly acknowledge compliance, ISPs refused

Details in the paper

Require Vendor Default

Idea: devices must filter packets by default

`Details in the paper`

- Equivalent to a default of no empty password on CPE devices.
- Interface design for security under explored:
  - **What if operators had to select which packets to *forward*, rather than those to *filter out?***
  - Unlikely to choose to allow spoofed packets.
- Default settings have impact on human behavior
  - Johnson & Goldstein. 2013. *Do defaults save lives?* Science 302
  - **What if operators had to choose to disable SAV?**

Network Hygiene, Incentives, and Regulation:

Deployment of Source Address Validation in the Internet

- **Lack of SAV deployment is an example of market failure**
- We developed third-party measurement capability, and used it to show ineffectiveness of weak forms of internalization of this network externality
- Any stronger forms of internalization will require this same measurement capability

https://spoofer.caida.org/
spoofer-info@caida.org

BCP 38