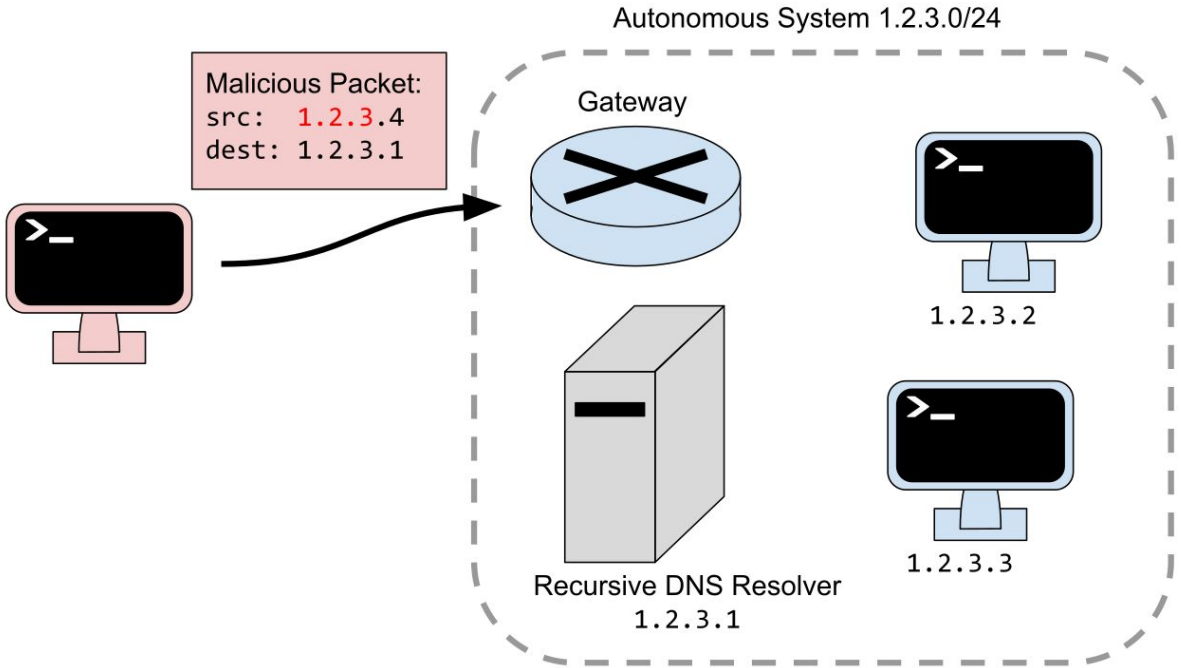
A Replication of DSAV Measurement

Deccio et al.
Chris Kitras and Bryson Schiel

Background

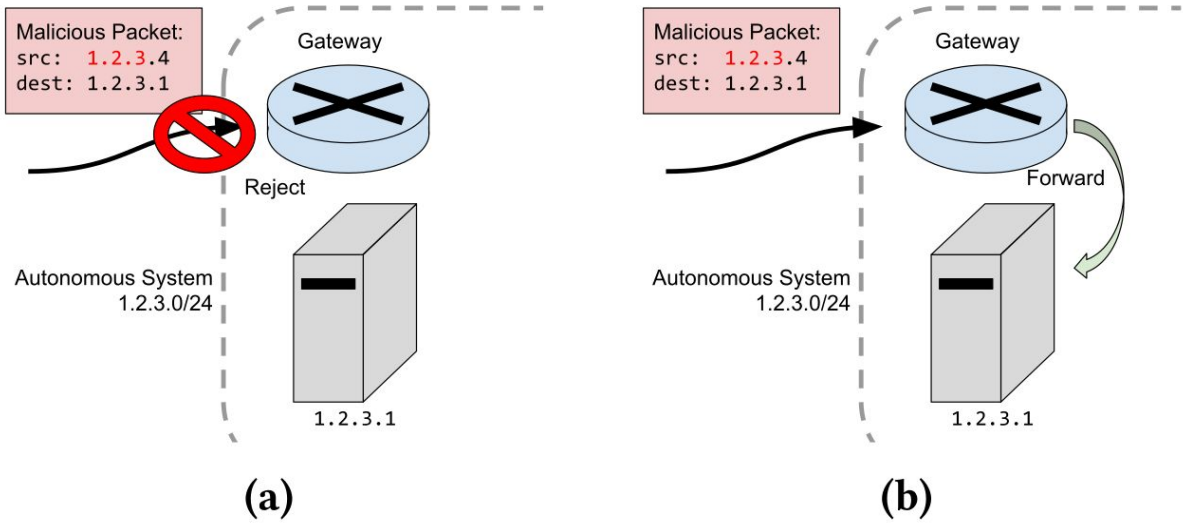
DSAV

- Destination-side source address validation (DSAV)
- A malicious attacker may try and **spoof their packet source** to be within an AS
- This could give that packet **certain privileges** within a network



DSAV through the gateway

- A **gateway node** is **responsible for performing DSAV** - making sure that the source address is correct
- There are many factors that go into DSAV
    - Detecting an internal packet coming from outside the network is a major part of that



Behind Closed Doors

In 2020, a paper was published where researchers attempted to measure DSAV usage

Deccio *et al*.

Behind Closed Doors: A Network Tale of Spoofing, Intrusion, and False DNS Security

Casey Deccio
Brigham Young University
Provo, UT
casey@byu.edu

Alden Hilton
Brigham Young University
Provo, UT
aldenhilton@byu.edu

Michael Briggs
Brigham Young University
Provo, UT
briggs25@byu.edu

Trevin Avery
Brigham Young University
Provo, UT
trevinavery@byu.edu

Robert Richardson
Brigham Young University
Provo, UT
richardson@stat.byu.edu

ABSTRACT

Networks not employing destination-side source address validation (DSAV) expose themselves to a class of pernicious attacks which could be easily prevented by filtering inbound traffic purporting to originate from within the network. In this work, we survey the pervasiveness of networks vulnerable to infiltration using spoofed addresses internal to the network. We issue recursive Domain Name System (DNS) queries to a large set of known DNS servers worldwide, using various spoofed-source addresses. We classify roughly half of the 62,000 networks (autonomous systems) we tested as vulnerable to infiltration due to lack of DSAV. As an illustration of the dangers these networks expose themselves to, we demonstrate the ability to fingerprint the operating systems of internal DNS servers. Additionally, we identify nearly 4,000 DNS server instances vulnerable to cache poisoning attacks due to insufficient—and often non-existent—source port randomization, a vulnerability widely publicized 12 years ago.

CCS CONCEPTS

• **Networks** → **Firewalls**; **Security protocols**; **Naming and addressing**; *Network layer protocols*; **Network measurement**.

ACM Reference Format:
Casey Deccio, Alden Hilton, Michael Briggs, Trevin Avery, and Robert Richardson. 2020. Behind Closed Doors: A Network Tale of Spoofing, Intrusion, and False DNS Security. In *ACM Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3419394.3423649

1 INTRODUCTION

Network administrators often use network protections such as firewalls and access control lists (ACLs) to disallow traffic from untrusted third parties from reaching internal hosts. However, source address *spoofing* creates a scenario in which inbound traffic might *appear* to be from a trusted party—even from another internal system. If traffic arriving at a given system has a source address that originates *from* that system, the legitimacy of the traffic should be questioned. This is loosely analogous to a postal service delivering a letter to an address, with the letter claiming to be *from* that address. Yet the source address of packets is often *not* checked—allowing a spoofed-source packet to penetrate a network border and reach systems not intended for public access. While the effects of this penetration can be mitigated in some cases with protocols that include some form of identity check (e.g., TCP), in other cases, this infiltration creates a vulnerability that can be exploited for surveillance or compromise.

There are two significant locations in the path of a spoofed-source packet: 1) the border of the network from which it *originates*; and 2) the border of the network for which it is *destined*. Network Ingress Filtering [20] [1]—also known as Source Address Validation (SAV) [2]—is the de facto solution for combating source address spoofing at packet *origin*, codified as Best Current Practice (BCP) 38 [20]. When spoofed-source packets are dropped as they attempt to leave their Internet Service Provider (ISP), they never become a presence in the Internet at large. However, once a spoofed-source packet reaches its *destination*, determining its validity is much more difficult—that is, unless the packet has a source IP address claiming to have originated from *within* the target network. Just as an ISP can block outbound packets that claim to have originated from outside, it can block inbound packets that claim to have originated from inside. We refer to these actions, more specifically, as *origin-side SAV (OSAV)* and *destination-side SAV (DSAV)*, respectively.

When DSAV is absent, a network is vulnerable to *infiltration*—masquerading as a network insider to penetrate a network border and access internal resources. The first major contribution of this paper is a **large-scale study of the lack of DSAV**. In late 2019, we surveyed 62,000 networks for DSAV, using methodology that was effective in its detection, yet harmless. We sent spoofed-source packets to these networks, each packet having a source appearing to originate from the network for which it was destined. We observed

IMC '20, October 27–29, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-8138-3/20/10…$15.00
https://doi.org/10.1145/3419394.3423649

[1] Note that the term "ingress" is used not because the filtering happens as a packet enters a *network* but because the filtering happens at the ingress (input) link of the participating *router*.

Spoofing and Measuring

- Send **DNS queries** with **spoofed sources** to seem internal
- If a DNS **recursive resolver sends the query** to an authoritative server we control, **we got 'em**

We sought to replicate this pattern and see if any changes have occured

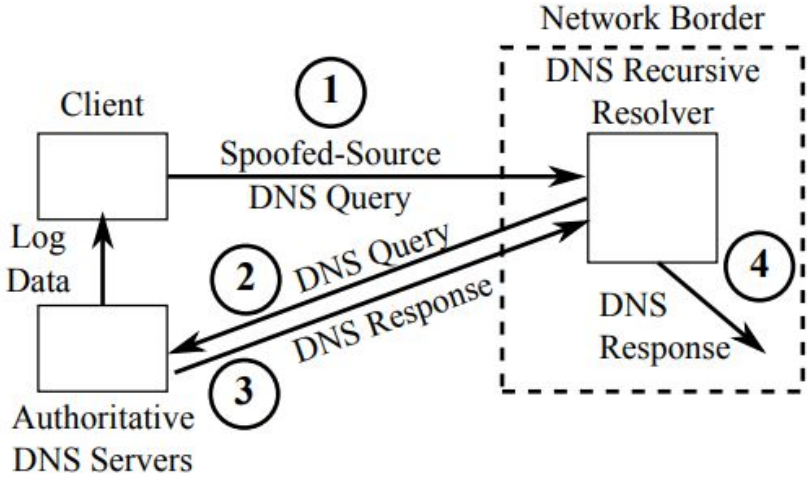


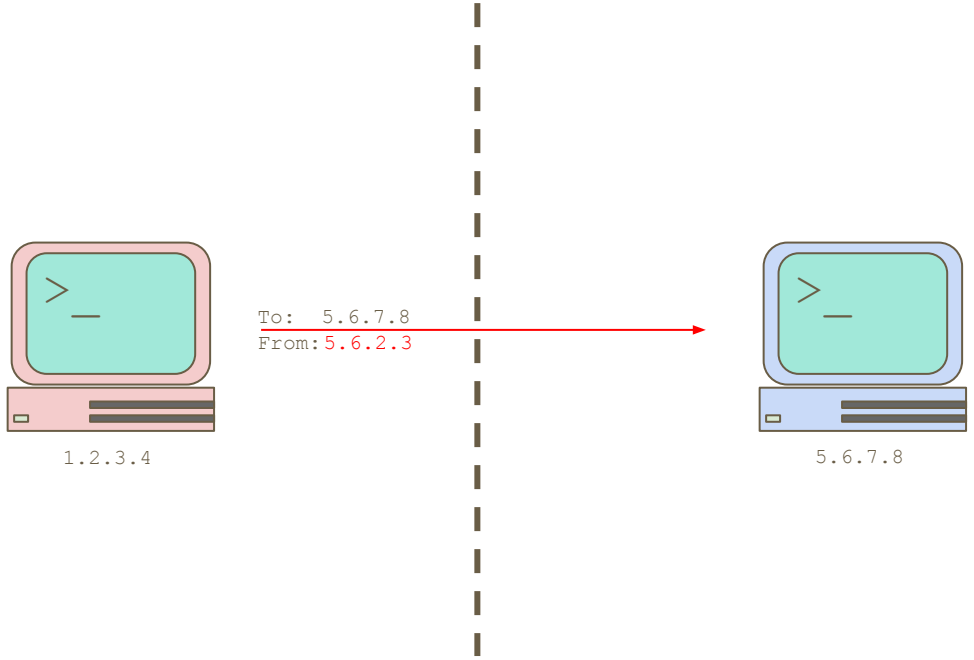
Figure 1: Experiment setup, in which (1) a client sends a DNS query with spoofed source to an internal DNS recursive resolver, (2) the recursive resolver issues a query to our DNS authoritative servers, (3) the authoritative server responds, and (4) a DNS response is issued by the DNS recursive server.

From Deccio *et al*.

Methodology

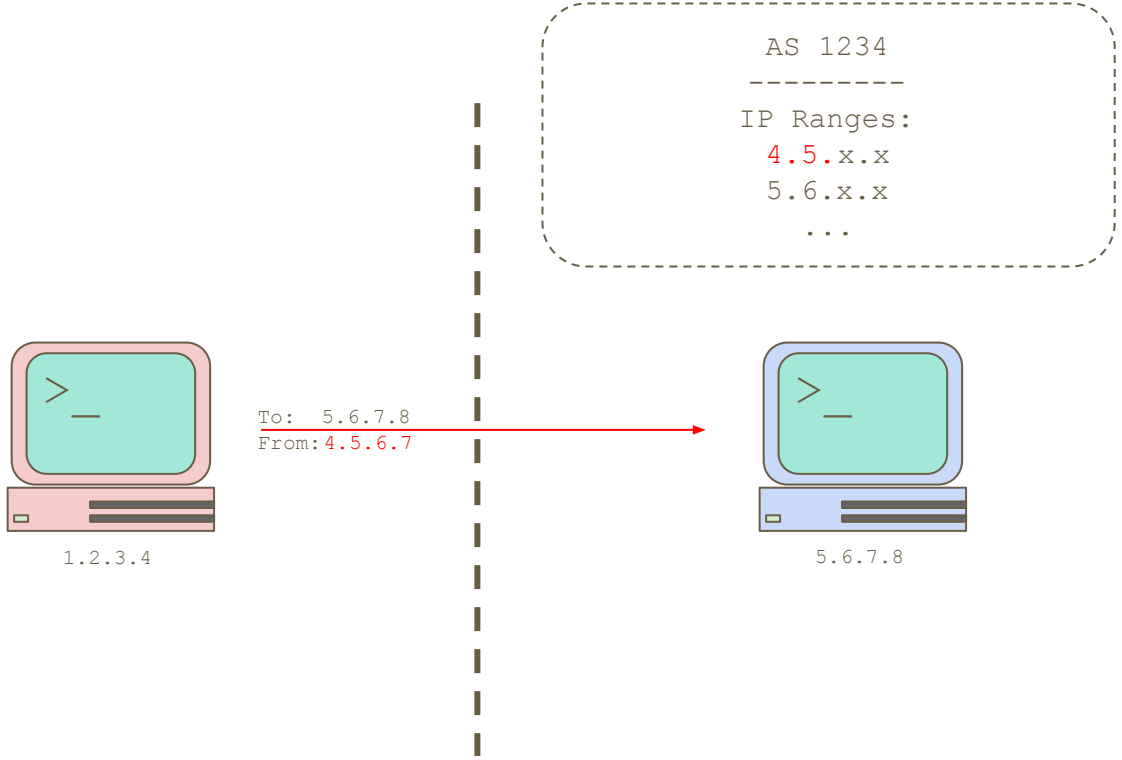
Deriving Spoofed Sources

- Same Prefix (1)
- Other Prefix (21)
- Private (1)
- Dst-as-Src (1)
- Loopback (1)



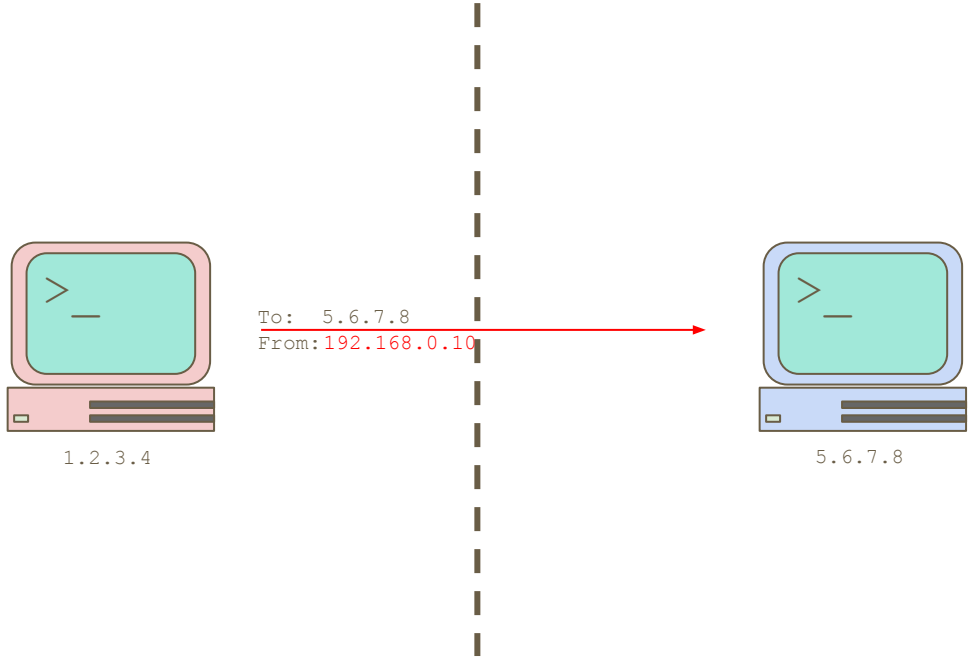
Deriving Spoofed Sources

- Same Prefix (1)
- Other Prefix (21)
- Private (1)
- Dst-as-Src (1)
- Loopback (1)



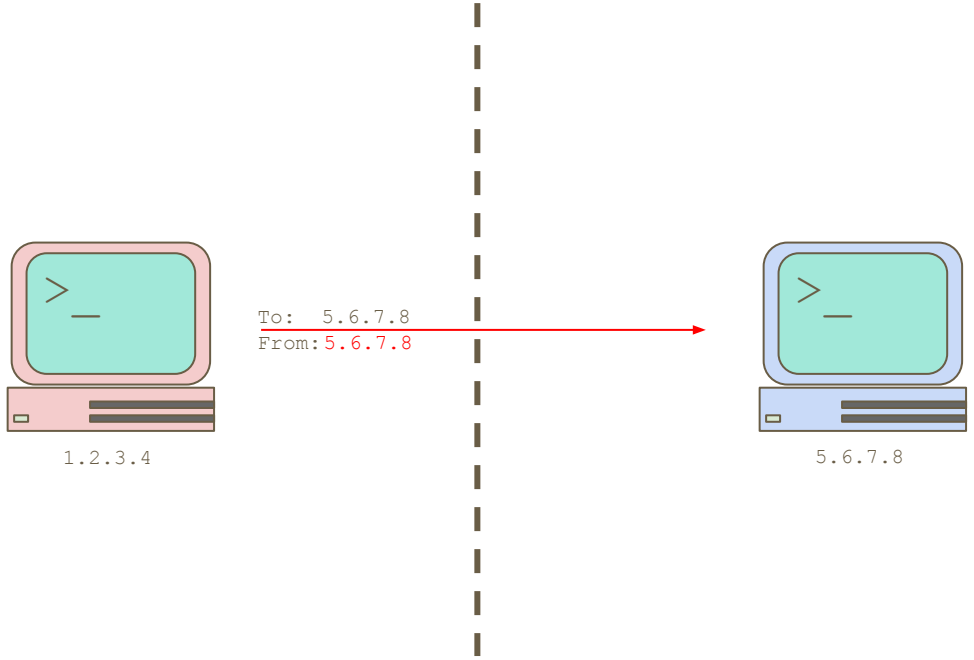
Deriving Spoofed Sources

- Same Prefix (1)
- Other Prefix (21)
- Private (1)
- Dst-as-Src (1)
- Loopback (1)



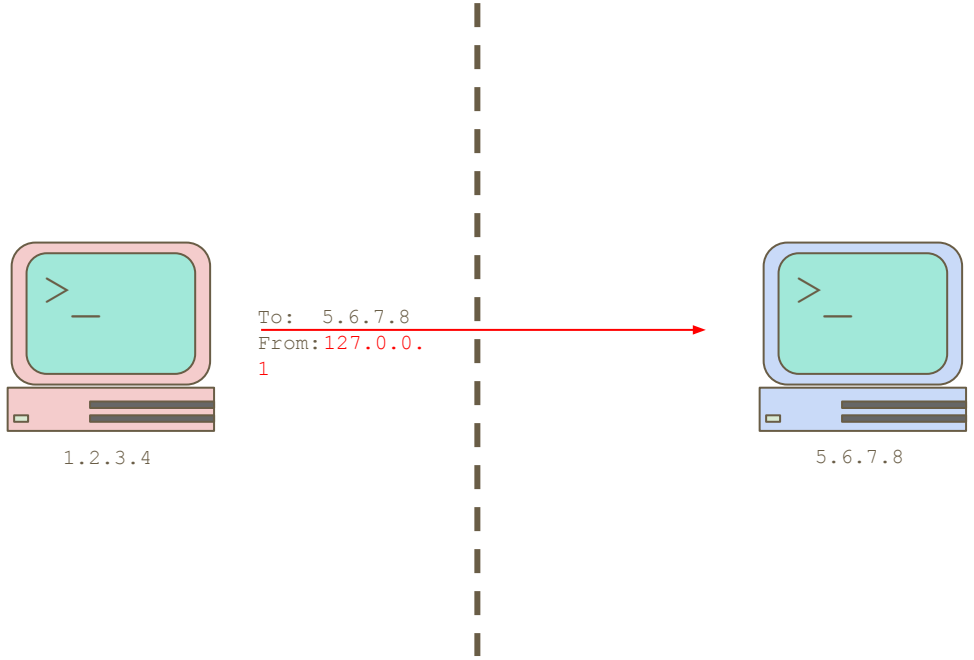
Deriving Spoofed Sources

- Same Prefix (1)
- Other Prefix (21)
- Private (1)
- Dst-as-Src (1)
- Loopback (1)



Deriving Spoofed Sources

- Same Prefix (1)
- Other Prefix (21)
- Private (1)
- Dst-as-Src (1)
- Loopback (1)



Resources Used

- tcpdump
  - Like **Wireshark**
  - **Sniff** incoming/outgoing tcp **packets**
- scapy
  - Create and send **custom packets**
  - Insanely **easy** to use
- RIPE.net
  - ASN **IP ranges**
- MaxMind GeoLite
  - ASN to **Country**

RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Resources Used (cont.)

- DNS dataset given in Project 1
  - **444,781** different IP addresses
  - IPv4 only
- Old dataset
  - DITL from root servers
  - **11,204,889** different IP addresses
  - Used IPv4 and IPv6

Analysis

Top 10 Countries with Most Represented ASes

Country	ASes Total	ASes Reachable	ASes Old Rate	IP Targets Total	IP Targets Reachable	IP Targets Old Rate
United States	4,340	1,746 (40.23%)	↓ 28%	248,300	7,155 (2.88%)	↑ 3.2%
Brazil	2,613	1,741 (66.62%)	↓ 59%	8,316	2,888 (34.72%)	↓ 4.8%
Russia	1,161	80 (6.89%)	↑ 59%	4,713	119 (2.52%)	↑ 11.6%
Germany	606	236 (38.94%)	↓ 36%	19,846	1100 (5.54%)	↓ 3.8%
India	584	403 (69.00%)	↓ 41%	11,651	1258 (10.79%)	↑ 11.6%
Indonesia	507	382 (75.34%)	–	6,006	834 (13.88%)	–
Great Britain	489	218 (44.58%)	↓ 33%	22,831	814 (3.56%)	↑ 4.5%
Poland	472	312 (66.10%)	↓ 52%	2,068	612 (29.59%)	↓ 6.0%
Canada	445	205 (46.06%)	↓ 36%	12,110	615 (5.07%)	↓ 2.8%
Ukraine	386	256 (66.32%)	↓ 63%	1,033	460 (44.53%)	↓ 15.4%

Top 10 Countries with Most Represented ASes

Country	ASes Total	ASes Reachable	ASes Old Rate	IP Targets Total	IP Targets Reachable	IP Targets Old Rate
United States	4,340	1,746 (40.23%)	↓ 28%	248,300	7,155 (2.88%)	↑ 3.2%
Brazil	2,613	1,741 (66.62%)	↓ 59%	8,316	2,888 (34.72%)	↓ 4.8%
Russia	1,161	80 (6.89%)	↑ 59%	4,713	119 (2.52%)	↑ 11.6%
Germany	606	236 (38.94%)	↓ 36%	19,846	1100 (5.54%)	↓ 3.8%
India	584	403 (69.00%)	↓ 41%	11,651	1258 (10.79%)	↑ 11.6%
Indonesia	507	382 (75.34%)	–	6,006	834 (13.88%)	–
Great Britain	489	218 (44.58%)	↓ 33%	22,831	814 (3.56%)	↑ 4.5%
Poland	472	312 (66.10%)	↓ 52%	2,068	612 (29.59%)	↓ 6.0%
Canada	445	205 (46.06%)	↓ 36%	12,110	615 (5.07%)	↓ 2.8%
Ukraine	386	256 (66.32%)	↓ 63%	1,033	460 (44.53%)	↓ 15.4%

Top 10 Countries with Most Represented ASes

Country	ASes Total	ASes Reachable	ASes Old Rate	IP Targets Total	IP Targets Reachable	IP Targets Old Rate
United States	4,340	1,746 (40.23%)	↓ 28%	248,300	7,155 (2.88%)	↑ 3.2%
Brazil	2,613	1,741 (66.62%)	↓ 59%	8,316	2,888 (34.72%)	↓ 4.8%
Russia	1,161	80 (6.89%)	↑ 59%	4,713	119 (2.52%)	↑ 11.6%
Germany	606	236 (38.94%)	↓ 36%	19,846	1100 (5.54%)	↓ 3.8%
India	584	403 (69.00%)	↓ 41%	11,651	1258 (10.79%)	↑ 11.6%
Indonesia	507	382 (75.34%)	–	6,006	834 (13.88%)	–
Great Britain	489	218 (44.58%)	↓ 33%	22,831	814 (3.56%)	↑ 4.5%
Poland	472	312 (66.10%)	↓ 52%	2,068	612 (29.59%)	↓ 6.0%
Canada	445	205 (46.06%)	↓ 36%	12,110	615 (5.07%)	↓ 2.8%
Ukraine	386	256 (66.32%)	↓ 63%	1,033	460 (44.53%)	↓ 15.4%

Top Countries with Vulnerable IP Target Ratio

	ASes		IP Targets	
Country	**Total**	**Reachable**	**Total**	**Reachable**
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Top Countries with Vulnerable IP Target Ratio

	ASes		IP Targets	
Country	**Total**	**Reachable**	**Total**	**Reachable**
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
French Guiana	4	3 (75.00%)	19	18 (94.74%)
Virgin Islands	3	2 (66.67%)	6	5 (83.33%)
Tajikistan	13	11 (84.62%)	35	29 (82.86%)
Mali	3	3 (100.00%)	10	8 (80.00%)
Niger	5	4 (80.00%)	10	8 (80.00%)
Solomon Islands	3	3 (100.00%)	5	4 (80.00%)
Anguilla	4	3 (75.00%)	5	4 (80.00%)
Antigua and Barbuda	2	2 (100.00%)	5	4 (80.00%)
Guinea	7	6 (85.71%)	12	9 (75.00%)
Eswatini	4	3 (75.00%)	8	6 (75.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
French Guiana	4	3 (75.00%)	19	18 (94.74%)
Virgin Islands	3	2 (66.67%)	6	5 (83.33%)
Tajikistan	13	11 (84.62%)	35	29 (82.86%)
Mali	3	3 (100.00%)	10	8 (80.00%)
Niger	5	4 (80.00%)	10	8 (80.00%)
Solomon Islands	3	3 (100.00%)	5	4 (80.00%)
Anguilla	4	3 (75.00%)	5	4 (80.00%)
Antigua and Barbuda	2	2 (100.00%)	5	4 (80.00%)
Guinea	7	6 (85.71%)	12	9 (75.00%)
Eswatini	4	3 (75.00%)	8	6 (75.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
French Guiana	4	3 (75.00%)	19	18 (94.74%)
Virgin Islands	3	2 (66.67%)	6	5 (83.33%)
Tajikistan	13	11 (84.62%)	35	29 (82.86%)
Mali	3	3 (100.00%)	10	8 (80.00%)
Niger	5	4 (80.00%)	10	8 (80.00%)
Solomon Islands	3	3 (100.00%)	5	4 (80.00%)
Anguilla	4	3 (75.00%)	5	4 (80.00%)
Antigua and Barbuda	2	2 (100.00%)	5	4 (80.00%)
Guinea	7	6 (85.71%)	12	9 (75.00%)
Eswatini	4	3 (75.00%)	8	6 (75.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
French Guiana	4	3 (75.00%)	19	18 (94.74%)
Virgin Islands	3	2 (66.67%)	6	5 (83.33%)
Tajikistan	13	11 (84.62%)	35	29 (82.86%)
Mali	3	3 (100.00%)	10	8 (80.00%)
Niger	5	4 (80.00%)	10	8 (80.00%)
Solomon Islands	3	3 (100.00%)	5	4 (80.00%)
Anguilla	4	3 (75.00%)	5	4 (80.00%)
Antigua and Barbuda	2	2 (100.00%)	5	4 (80.00%)
Guinea	7	6 (85.71%)	12	9 (75.00%)
Eswatini	4	3 (75.00%)	8	6 (75.00%)

Top Countries with Vulnerable IP Target Ratio

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
Sudan	3	3 (100.00%)	5	5 (100.00%)
American Samoa	2	2 (100.00%)	5	5 (100.00%)
Vanuatu	2	2 (100.00%)	4	4 (100.00%)
Palau	2	2 (100.00%)	4	4 (100.00%)
Caribbean Netherlands	2	2 (100.00%)	3	3 (100.00%)
Guadeloupe	2	2 (100.00%)	4	4 (100.00%)
Sint Maarten	2	2 (100.00%)	4	4 (100.00%)
Cook Islands	1	1 (100.00%)	3	3 (100.00%)
Saint Martin	1	1 (100.00%)	2	2 (100.00%)
Saint Lucia	1	1 (100.00%)	3	3 (100.00%)
Turkmenistan	2	2 (100.00%)	2	2 (100.00%)
Guernsey	1	1 (100.00%)	1	1 (100.00%)

Country	ASes		IP Targets	
	Total	Reachable	Total	Reachable
French Guiana	4	3 (75.00%)	19	18 (94.74%)
Virgin Islands	3	2 (66.67%)	6	5 (83.33%)
Tajikistan	13	11 (84.62%)	35	29 (82.86%)
Mali	3	3 (100.00%)	10	8 (80.00%)
Niger	5	4 (80.00%)	10	8 (80.00%)
Solomon Islands	3	3 (100.00%)	5	4 (80.00%)
Anguilla	4	3 (75.00%)	5	4 (80.00%)
Antigua and Barbuda	2	2 (100.00%)	5	4 (80.00%)
Guinea	7	6 (85.71%)	12	9 (75.00%)
Eswatini	4	3 (75.00%)	8	6 (75.00%)

Spoofed Source Test Success Rate

	Category-Inclusive (one-or-more)				Category-Exclusive (only)			
Source Category	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**
All Queried	444,781	11,204,889	17,487	53,922	444,781	11,204,889	17,487	53,922
All Reachable	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%
Other Prefix	26,324 (90.9%)	↓ 78%	8,238 (91.5%)	↑ 97%	7,444 (25.7%)	↑ 33%	1,381 (15.3%)	↓ 6.9%
Same Prefix	21,439 (74.1%)	↓ 63%	8,288 (92.0%)	↓ 91%	2,565 (8.8%)	↑ 17%	1,258 (13.9%)	↓ 1.4%
Private	214 (.74%)	↑ 3.4%	90 (0.9%)	↑ 12%	20 (.06%)	↑ 0.5%	13 (.14%)	↑ 0.4%
Dst-as-Src	0 (0.0%)	↑ 17%	0 (0.0%)	↑ 47%	0 (0.0%)	↑ 2.6%	0 (0.0%)	↑ 0.8%
Loopback	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%

Spoofed Source Test Success Rate

	Category-Inclusive (one-or-more)				Category-Exclusive (only)			
Source Category	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**
All Queried	444,781	11,204,889	17,487	53,922	444,781	11,204,889	17,487	53,922
All Reachable	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%
Other Prefix	26,324 (90.9%)	↓ 78%	8,238 (91.5%)	↑ 97%	7,444 (25.7%)	↑ 33%	1,381 (15.3%)	↓ 6.9%
Same Prefix	21,439 (74.1%)	↓ 63%	8,288 (92.0%)	↓ 91%	2,565 (8.8%)	↑ 17%	1,258 (13.9%)	↓ 1.4%
Private	214 (.74%)	↑ 3.4%	90 (0.9%)	↑ 12%	20 (.06%)	↑ 0.5%	13 (.14%)	↑ 0.4%
Dst-as-Src	0 (0.0%)	↑ 17%	0 (0.0%)	↑ 47%	0 (0.0%)	↑ 2.6%	0 (0.0%)	↑ 0.8%
Loopback	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%

Spoofed Source Test Success Rate

	Category-Inclusive (one-or-more)				Category-Exclusive (only)			
Source Category	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**
All Queried	444,781	11,204,889	17,487	53,922	444,781	11,204,889	17,487	53,922
All Reachable	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%
Other Prefix	26,324 (90.9%)	↓ 78%	8,238 (91.5%)	↑ 97%	7,444 (25.7%)	↑ 33%	1,381 (15.3%)	↓ 6.9%
Same Prefix	21,439 (74.1%)	↓ 63%	8,288 (92.0%)	↓ 91%	2,565 (8.8%)	↑ 17%	1,258 (13.9%)	↓ 1.4%
Private	214 (.74%)	↑ 3.4%	90 (0.9%)	↑ 12%	20 (.06%)	↑ 0.5%	13 (.14%)	↑ 0.4%
Dst-as-Src	0 (0.0%)	↑ 17%	0 (0.0%)	↑ 47%	0 (0.0%)	↑ 2.6%	0 (0.0%)	↑ 0.8%
Loopback	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%

Spoofed Source Test Success Rate

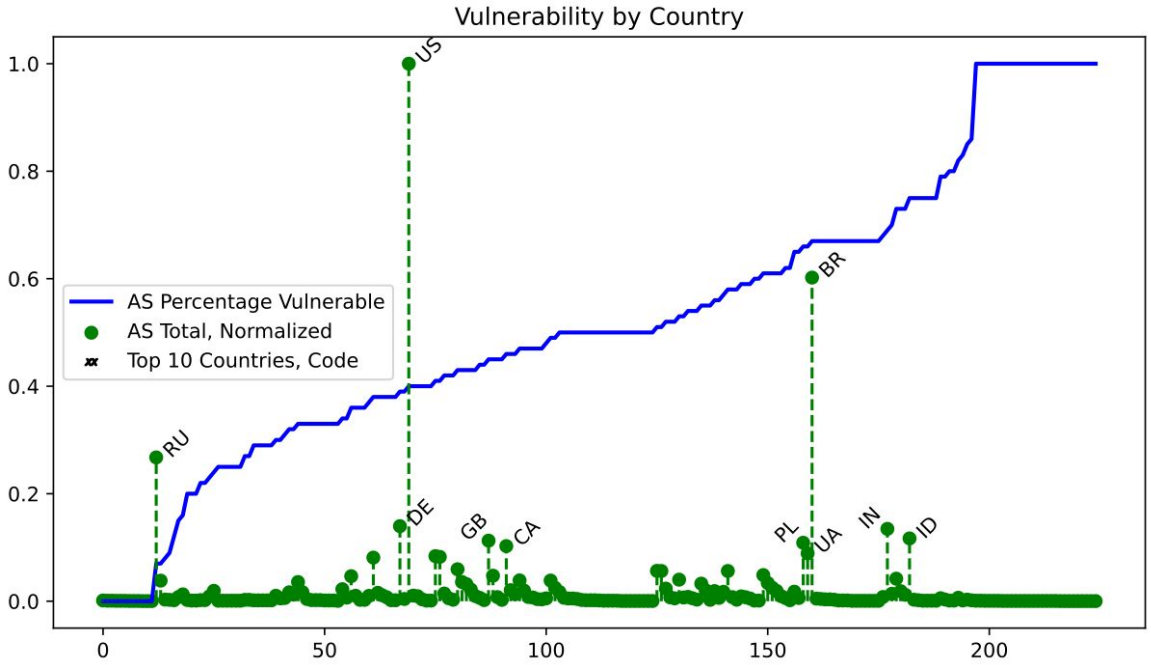
	Category-Inclusive (one-or-more)				Category-Exclusive (only)			
Source Category	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**	**Addresses**	**Old Addresses**	**ASNs**	**Old ASNs**
All Queried	444,781	11,204,889	17,487	53,922	444,781	11,204,889	17,487	53,922
All Reachable	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%	28,931 (6.5%)	↓ 4.6%	9,007 (51.5%)	↓ 49%
Other Prefix	26,324 (90.9%)	↓ 78%	8,238 (91.5%)	↑ 97%	7,444 (25.7%)	↑ 33%	1,381 (15.3%)	↓ 6.9%
Same Prefix	21,439 (74.1%)	↓ 63%	8,288 (92.0%)	↓ 91%	2,565 (8.8%)	↑ 17%	1,258 (13.9%)	↓ 1.4%
Private	214 (.74%)	↑ 3.4%	90 (0.9%)	↑ 12%	20 (.06%)	↑ 0.5%	13 (.14%)	↑ 0.4%
Dst-as-Src	0 (0.0%)	↑ 17%	0 (0.0%)	↑ 47%	0 (0.0%)	↑ 2.6%	0 (0.0%)	↑ 0.8%
Loopback	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%	0 (0.0%)	↑ 0%

Size vs. Vulnerability

- Graph of all countries, **sorted by vulnerability %**
- Endpoints (0%, 100%) have **very little data** (1-5 ASes)
- Top 10 countries fall within the **middle**

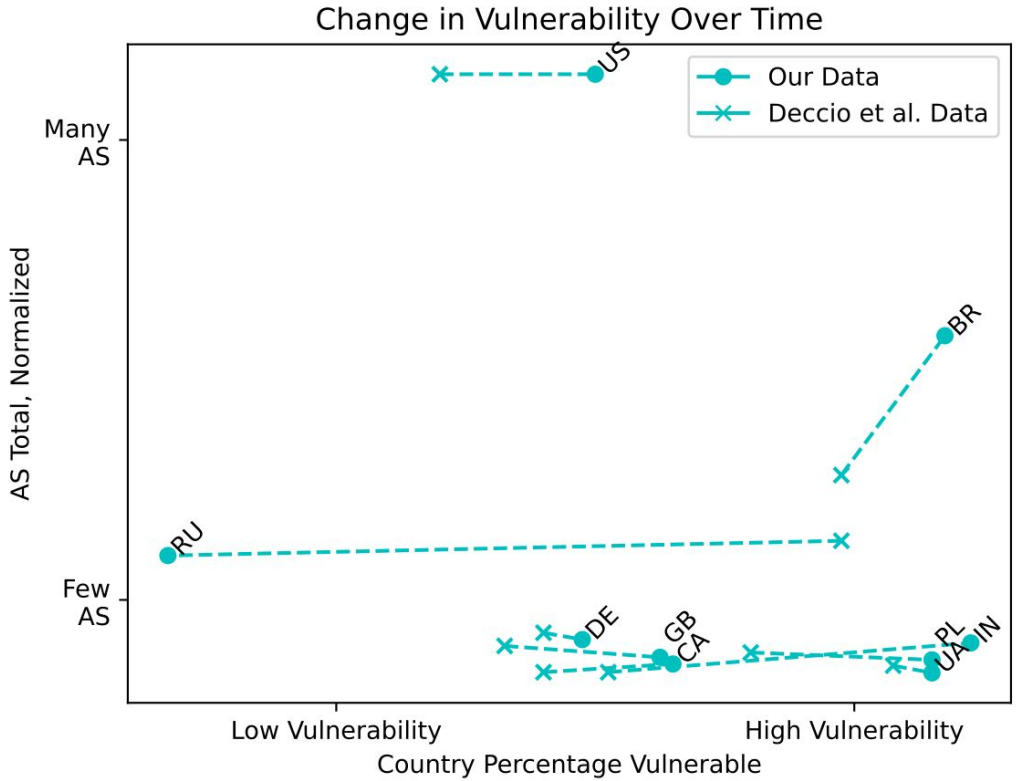
Two outliers in this group: **Russia** and **Brazil**

- Russia high usage and **low vulnerability**
- Brazil high usage and **high vulnerability**



Progression of Vulnerability

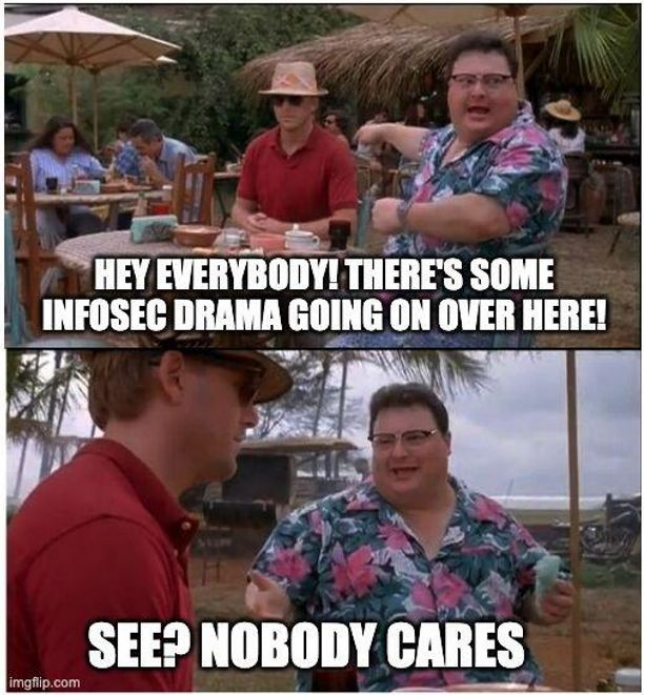
- Most of the Top 10 Most Vulnerable Countries had the **same proportion of ASes** across datasets
  - Exception of Brazil
- Shift **left** indicates **improvement in DSAV**
- Shift **right** indicates **increase** in ratio of **exposed ASes**
- Most of the **Top 10 increased** in vulnerable ASes



Conclusion

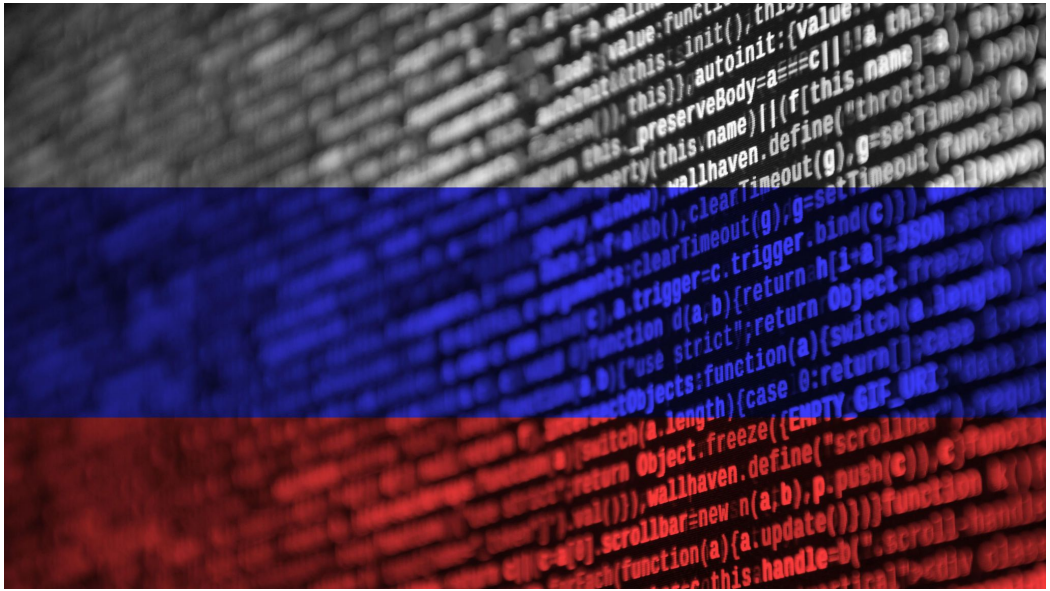
Changes?

- Many locations have **not seen major changes in utilization** percentage
- Most places are **more vulnerable** than in Deccio *et al*.



Changes?

- Many locations have **not seen major changes in utilization** percentage
- Most places are **more vulnerable** than in Deccio *et al*.
- **Russia** has made major **security improvements** for some reason



Thank you!

Any questions?