Aliens Among Us:

Observing Bogon IPs on the Public Internet

Radu, Carlos, Qasim, Matthew, Yury

(TU Delft, ICANN, RIPE NCC, CAIDA**)**

IMD Bucharest 30-09-2026

TU Delft



The Source Address Validation ~~feature~~ problem

- Cloudflare DDoS threat report 2024q4 summary:
  - Attacks are increasing in frequency, volume
  - Almost half (49%) are L3/4 attacks (can be **spoofed**!)
  - **Their H1 2026 report is similar**
- Akamai SOTI 2024:
  - >1/3 of global DDoS are in EMEA region
  - Trending attack vector: **spoofed** DNS requests

- In short, DDoS attacks are, as always, increasing, **spoofed** packets play an important part in this
- **Lots of networks still don't properly implement SAV**

TU Delft

The Martians and their Bogon friends

- **Martians**: "packets having a source address that, by application of the current forwarding tables, would not have its return traffic routed back to the sender.“
- **Bogon**: “a packet with an IP source address in an address block not yet allocated by IANA or the RIRs as well as all addresses reserved for private or special use by RFCs.”
- Previously: **Martians ~ Bogons**: “Humorous term applied to packets that turn up unexpectedly on the wrong network because of bogus routing entries. Also used as a name for a packet which has an altogether bogus (non-registered or ill-formed) Internet address.”
- “**Spoofed** packets” are a common source of **Martians** and **Bogons**
  - RFC3871 & RFC1208

- Packets are serious business though!

TU Delft

Research Questions

- **Bogons** are **Bogons** and shouldn't cross AS borders
  - If **Bogons** from one AS can visit another AS can **spoofed** packets do the same?
  - Is there a correlation between ASes (not) implementing SAV and those not filtering **Bogons**?

- Can we find **Martians** / **Bogons** in the wild, on the Internet?
  - Where should we look for them?

- In research, **Bogons** are often ignored or considered errors of the measurement, are they?

TU Delft

AS8708 DIGI Romania <-> AS3213 Bogons Ltd

Probe ID: 30983
Source IP: 10.2.2.20
AS8708

Min RTT: 48.67ms
Responded: yes

Complete Traceroute:

Hop	IP Address	Hostname	ASN	RTT (ms)
1	10.2.2.1			0.46/0.25/0.21
2	10.0.45.122			1.3/1.43/1.42
3	10.30.3.1			1.76/1.81/1.75
4	10.220.178.146			3.75/3.6/3.71
5	10.221.100.112			3.82/3.77/4.04
6	10.221.96.54			34.44/34.43/34.58
7	195.66.224.228	linx-224-gw.rbsov.bogons.net		32.57/32.51/32.49
8	185.102.248.45		3213	41.33/41.26/41.26
9	185.102.249.41		3213	32.65/32.35/32.53
10	93.186.42.243	93-186-42-243.thdo.bogons.net	3213	47.26/47.28/47.56
11	93.186.39.228	93-186-39-228.thdo.bogons.net	3213	46.97/46.88/46.88
12	93.186.38.205		3213	55.22/55.75/54.5
13	93.186.40.233	93-186-40-233.thdo.bogons.net	3213	53.34/48.67/49

Probe ID: 1013475
Source IP: 93.186.40.234
93-186-40-234.thdo.bogons.net
AS3213

Min RTT: 53.48ms
Responded: yes

Complete Traceroute:

Hop	IP Address	Hostname	ASN	RTT (ms)
1	93.186.40.233	93-186-40-233.thdo.bogons.net	3213	2.26/2.31/2.31
2	93.186.38.214	sw-upperbt.culty.bogons.net	3213	2.46/0.69/1.01
3	93.186.38.204		3213	0.62/0.49/0.56
4	93.186.39.229	93-186-39-229.thdo.bogons.net	3213	1.03/0.64/0.82
5	93.186.42.242	93-186-42-242.thdo.bogons.net	3213	12.39/12.42/12.37
6	185.102.249.40		3213	13.03/12.66/12.65
7	185.102.248.44		3213	12.5/12.47/12.4
8	195.66.224.46	xr01.london.rdsnet.ro		19.66/27.81/13.21
9	10.221.100.85			53.2/53.21/53.27
10	10.220.156.151			53.23/59.63/53.58
11	82.76.255.222	rcsrds01.ring.nlnog.net	8708	53.48/54.43/53.49

TU Delft

But why?

- My 10.0.0.1 is not your 10.0.0.1.
  - Unless we're playing some weird anycast. We're not.
  - Not useful for debug purposes. Seeing * * * is just as helpful.
  - Can be spoofed. But we only allow ICMP, rate-limit. Does not scale.
  - Should we filter? **Yes**.

Pros (for not filtering)	Cons
Pretty traceroute without * * *	Spoofable
Can show IP to $provider when debugging	Makes DDoS origin hard to trace
	Not globally unique (address collisions)
	Can't reply to the origin of the packet
	You can do fun UDP-based stuff
	Not compliant with BCP38 / BCP84
	Not compliant with MANRS
Bypass firewalls (because those IPs can't possibly come from somewhere unsafe)	Not compliant with most IXP policies



TU Delft

BCP38 – Network Ingress Filtering
BCP84 – Ingress Filtering for Multihomed Nets

Places where Martians and Bogons could hang out

- CAIDA Ark runs traceroutes to “all routed /24 networks in the IPv4 address space”
  - Can we find Bogons in The Ark IPv4 Routed /24 Topology Dataset?
  - So, we’re looking for a selection from IANA’s special purpose address space registry:
  - (fwd/globally reachable)

RFC	Description	CIDR
1112	Former Class E	240.0.0.0/4
1122	Loopback	127.0.0.0/8
1918	Private-Use	**(F)**10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
3927	Link-Local	169.254.0.0/16
5737	Documentation	192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24
6598	Shared Address Space	**(F)**100.64.0.0/10
6890	Protocol Assignments	192.0.0.0/24
7526	6to4 Relay Anycast	192.88.99.0/24

TU Delft

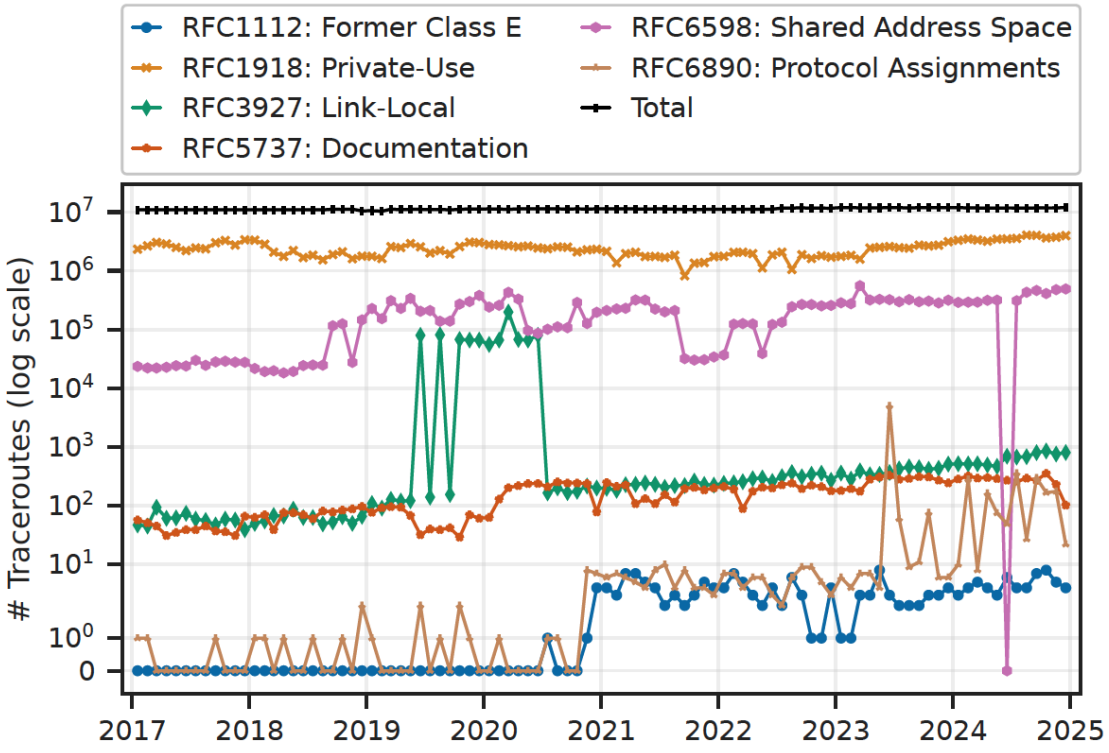
CAIDA: The Ark IPv4 Routed /24 Topology Dataset

- We looked at one day per month for 8 years (2017.01 – 2024.12)
  - ~11M traceroutes / measurement cycle

- The dataset is **not perfect** ™
  - The traceroute measurements are run daily
  - Except on days when the measurements are missing
  - But other days contain multiple measurement cycles (not related to missing days)
  - => lucky number 18 (day 18 of each month between 2017-2024 has at least one measurement cycle)

Where is Area 51?

- ~20% of visible ASes (15.5k of 77k) were seen in the company of Bogons



CC	#ASes	# Unique ASNs per RFCs					
		1112	1918	3927	5737	6598	6890
US	1207	14	1122	120	83	335	53
BR	938	0	869	11	8	197	3
RU	437	3	421	27	10	65	5
ID	288	1	279	8	1	32	0
GB	181	1	160	18	9	55	7
PL	175	0	171	5	3	20	0
CA	173	0	167	3	2	34	2
DE	171	1	158	13	3	40	7
BD	170	2	170	2	2	12	2
IT	155	0	150	3	2	25	2

TU Delft

OK Spoofer!

- What does the CAIDA Spoofer project think about the ASes we detected? (- 6mo)

Bogon Type	# ASNs	# in Spoofer	Only Spoofable	Only non-Spoofable	Both Spoofable & non-Spoofable
RFC1112	74	30	15 (33.33%)	20 (66.67%)	8 (26.67%)
RFC1918	14,896	2,529	358 (14.16%)	1,333 (52.71%)	725 (28.67%)
RFC3927	875	309	25 (8.09%)	159 (51.46%)	116 (37.54%)
RFC5737	502	226	13 (5.75%)	125 (55.31%)	85 (37.61%)
RFC6598	3,241	811	97 (11.96%)	408 (50.31%)	283 (34.90%)
RFC6890	241	88	5 (5.68%)	56 (63.64%)	26 (29.55%)

How are their MANneRS though?

- MANRS uses CAIDA Spoofer to check for anti-spoofing compliance (should overlap with prev.)

Members	Conf.	# ASNs	# Unique ASNs per RFC					
			1112	1918	3927	5737	6598	6890
All	Conf.	258	12	244	64	58	128	28
	Not Conf.	154	5	142	23	14	64	10
Before 2024	Conf	231	11	217	60	55	117	27
	Not Conf.	129	5	118	20	12	53	9

TU Delft

But 8 years is a lot in Internet time!

- Networks change a lot in 8 years, focus on 1 year (2024)
- What region (RIR) has most ASes not filtering Bogons?
- To what industries most of these ASes belong? (ASdb 2024-01)

RIR	#ASes	%
RIPE NCC	2,414	34.73%
APNIC	1,431	20.59%
ARIN	1,392	20.03%
LACNIC	1,334	19.19%
AFRINIC	364	5.24%
Not found	16	0.23%
Total ASNs	**6,951**	**100.00%**

Category	#ASes	%
Computer and Information Technology - Internet Service Provider (ISP)	4,552	65.49%
Computer and Information Technology - (no second category found)	488	7.02%
Computer and Information Technology - Hosting and Cloud Provider	308	4.43%
Education and Research - Colleges, Universities, and Professional Schools	175	2.52%
Other	1,232	17.72%
Not found	196	2.82%
Total ASNs 2024	**6,951**	**100%**

TU Delft

Summary

- We found **Bogon** packets are transited by 15.5k ASes in a period of 8 years (**not routes**!)
- The number of ASes not filtering **Bogon** packets is increasing
  - IPv4 runout makes networks use more private space
- Available datasets do not have enough coverage to link **Bogon** packets to SAV in general
  - Future research: improved datasets, methodology, availability of data

- **Since RIPE*NCC* registered a large part of these ASes, raising awareness about network hygiene in the region is important**

- **Don't like traceroutes showing * * *? Use IPv6!**

(not the only alternative)



TU Delft

Thank you!

TU Delft