Aliens **Among Us**

Observing Bogon IPs on the Public Internet

Quantifying the prevalence of reserved and non-routable IP addresses on the public Internet

Radu Anghel (TU Delft) **Carlos Gañán** (ICANN)
Qasim Lone (RIPE NCC) Matthew Luckie (CAIDA)
Yury Zhauniarovich (TU Delft)

The Source Address Validation ~~feature~~

- Cloudflare DDoS threat report 2024q4 summary:
    - Attacks are increasing in frequency, volume
    - Almost half (49%) are L3/4 attacks (can be **spoofed**!)

- Akamai SOTI 2024:
    - >1/3 of global DDoS are in EMEA region
    - Trending attack vector: **spoofed** DNS requests

- In short, DDoS attacks are increasing, **spoofed** packets play an important part in this

- **Lots of networks still don’t properly implement SAV**

How Can We Measure SAV Deployment?

Active probing (CAIDA Spoofer) has limited coverage

Key idea: Look for packets that shouldn't exist on the public Internet

If private IPs (Bogons) cross AS borders → Border filtering is broken

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.”

- Per [RFC1208] : **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

Key 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?

Places where Martians and Bogons could

- 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?
  - Yes, we can! So, we’re looking for a selection:

RFC	Description	CIDR
1112	Former Class E	240.0.0.0/4
1122	Loopback	127.0.0.0/8
1918	Private-Use	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	100.64.0.0/10
6890	Protocol Assignments	192.0.0.0/24
7526	6to4 Relay Anycast	192.88.99.0/24

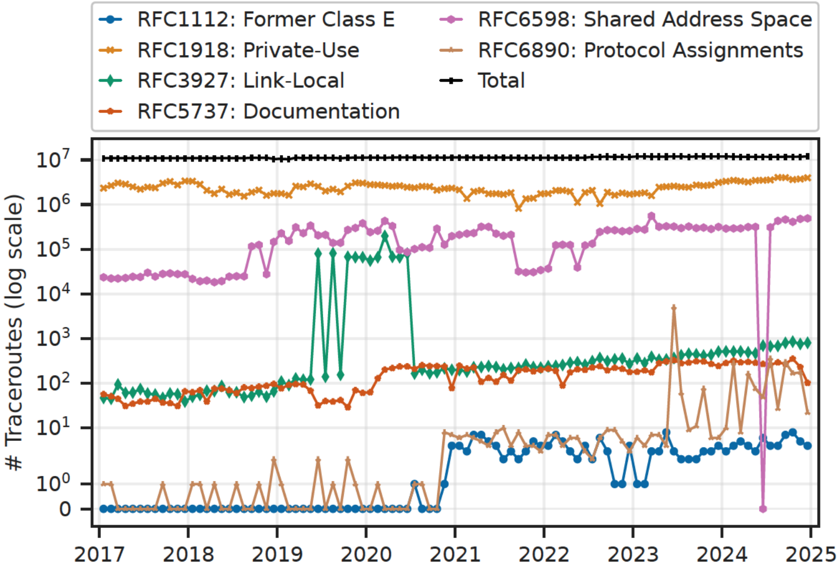
CAIDA: The Ark IPv4 Routed /24 Topology

- 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

OK Spoofer!

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

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

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	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%**

Summary of findings

- We found **Bogon** packets are transited by 15k 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