Presented at **IETF 118** MAPRG

Unresolved Issues: Characterizing Open DNS Resolver (Mis)behavior for DNSSEC Queries

Sudheesh Singanamalla[◇], Ben Weintraub[■], Christian Elmerot[ɸ], Kurtis Heimerl[◇], Cristina Nita-Rotaru[■], Marwan Fayed[ɸ], Thibault Meunier[ɸ]

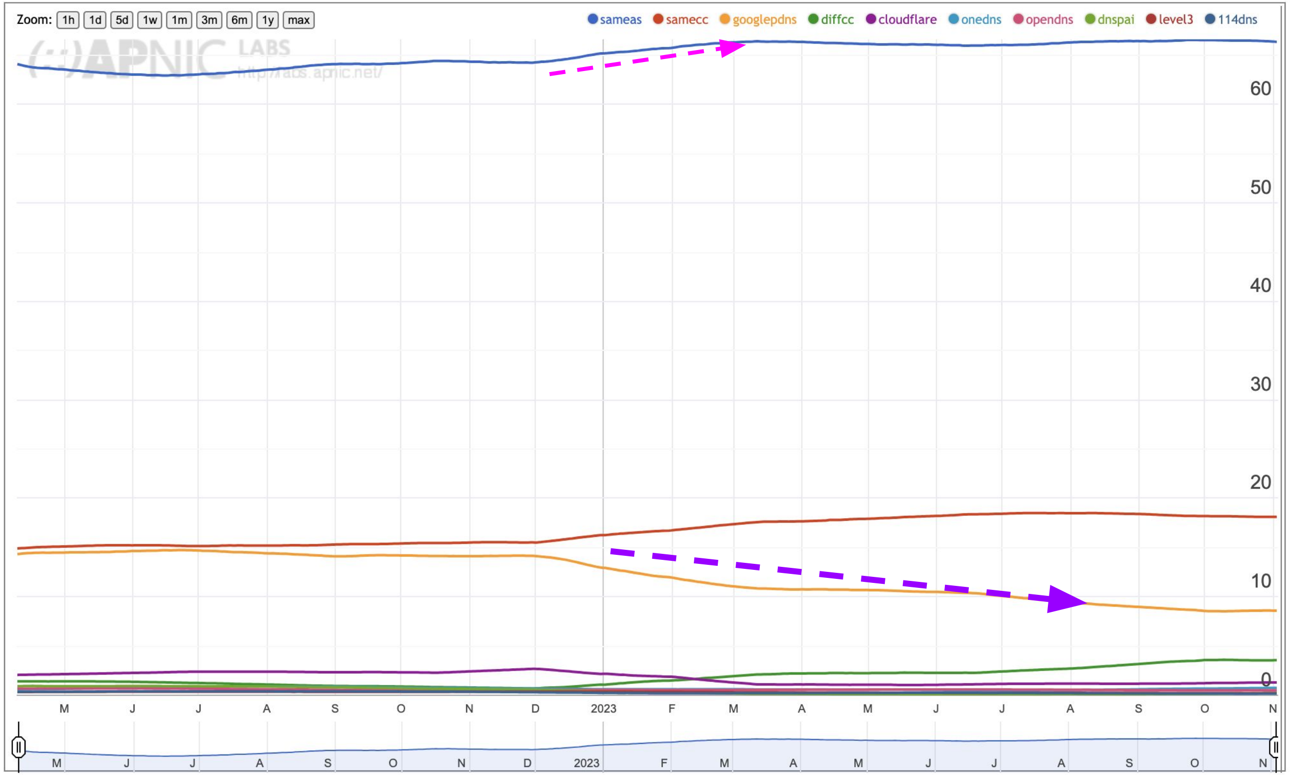
[◇] University of Washington, [■] Northeastern University, [ɸ] Cloudflare Research

UNIVERSITY *of* WASHINGTON

Northeastern University

Cloudflare Research

ISP Managed DNS Resolvers and Usage on the Rise

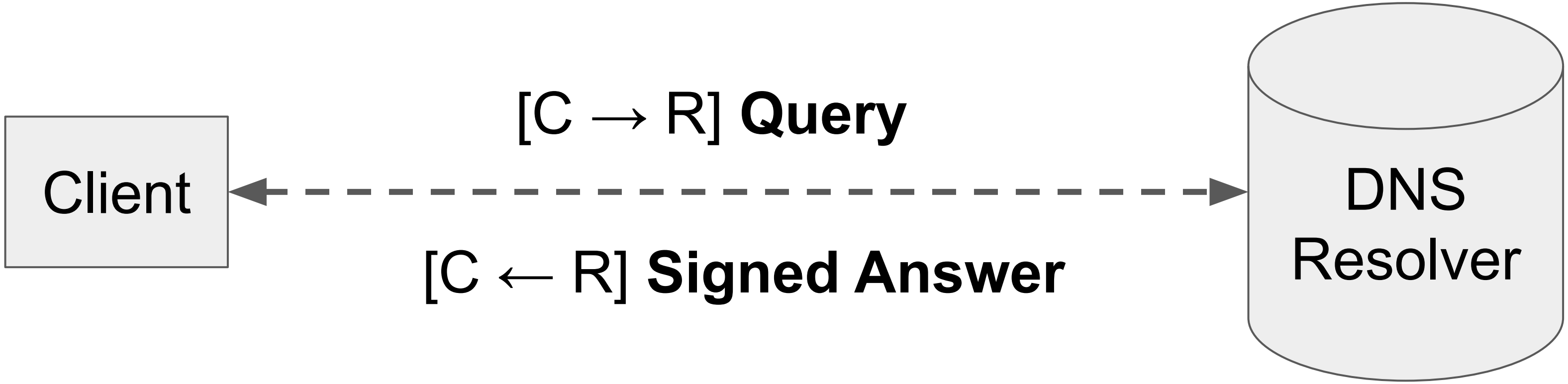


https://stats.labs.apnic.net/rvrs

Over 65% of all Internet clients use default ISP configured DNS resolvers.

Increasing trend in deploying and managing local DNS resolver instructure due to regulatory mandates eg. filtering.

DNSSEC Usage and Responses



Client

[C → R] **Query**

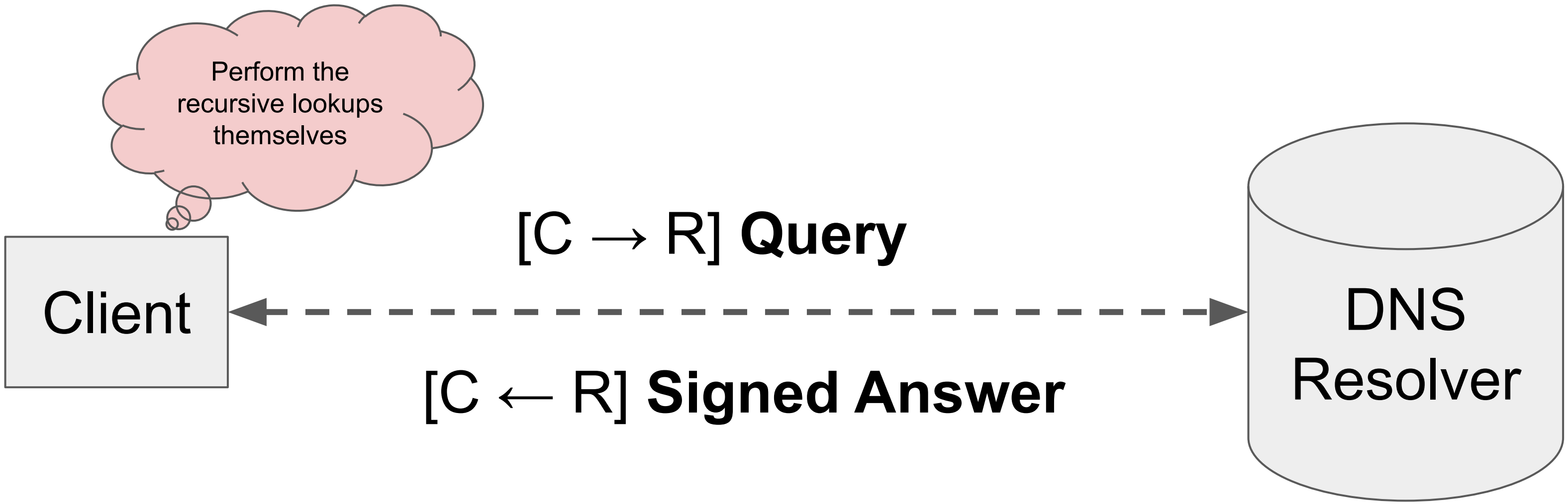
[C ← R] **Signed Answer**

DNS Resolver

Authenticity of the Answer

Integrity of the Answer

DNSSEC Usage and Responses



Perform the recursive lookups themselves

Client

[C → R] **Query**

[C ← R] **Signed Answer**

DNS Resolver

Authenticity of the Answer

Integrity of the Answer

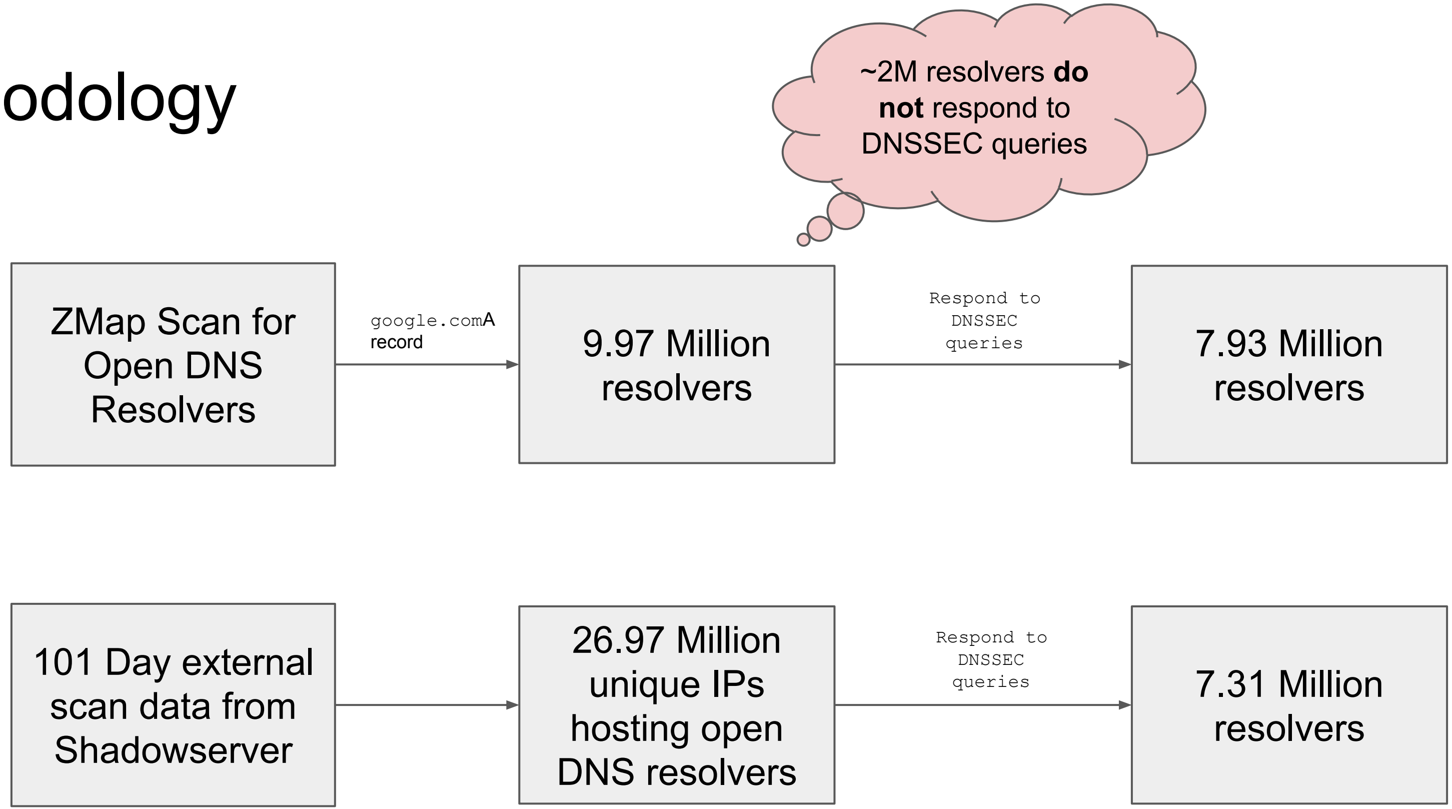
Resolver can **drop signatures**

Research Questions

1. To what extent do the recursive DNS resolvers provide “valid” and “correct” responses to DNSSEC enabled user queries?

2. To what extent are the recursive DNS resolvers validating the DNSSEC responses obtained from the name servers?

Methodology



~2M resolvers **do not** respond to DNSSEC queries

ZMap Scan for Open DNS Resolvers

`google.com`A record

9.97 Million resolvers

Respond to DNSSEC queries

7.93 Million resolvers

101 Day external scan data from Shadowserver

26.97 Million unique IPs hosting open DNS resolvers

Respond to DNSSEC queries

7.31 Million resolvers

Shadowserver identifies ~2.5M open resolvers daily, the difference could be due to filtering opt-out requests

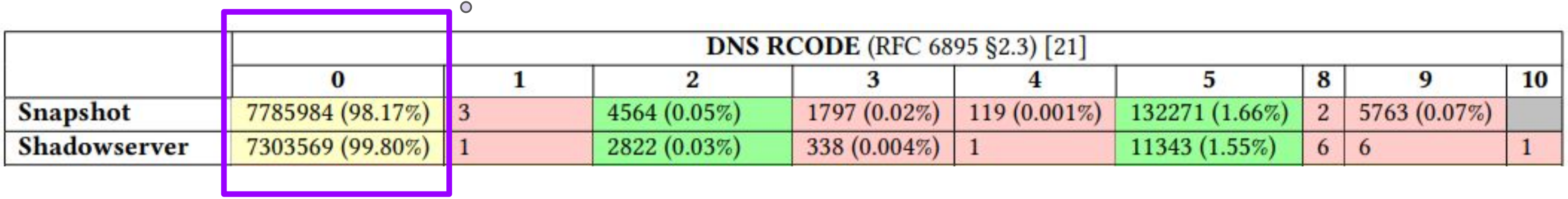
Types of Responses from DNS Resolvers

Query: google.com

Record Type: A

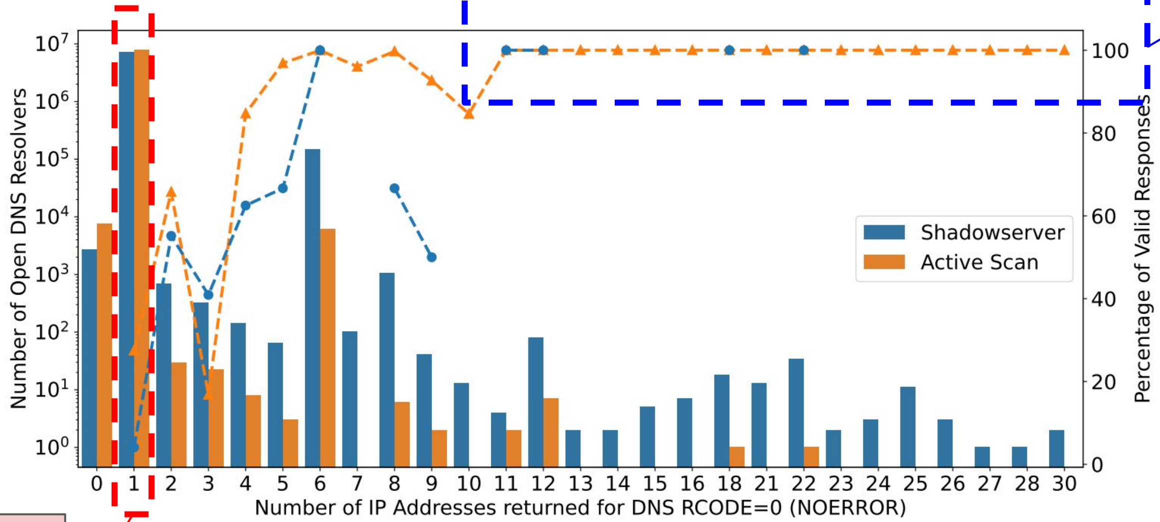
DNSSEC (DO) bit set

Over 98% respond successfully



	DNS RCODE (RFC 6895 §2.3) [21]								
	0	1	2	3	4	5	8	9	10
Snapshot	7785984 (98.17%)	3	4564 (0.05%)	1797 (0.02%)	119 (0.001%)	132271 (1.66%)	2	5763 (0.07%)	
Shadowserver	7303569 (99.80%)	1	2822 (0.03%)	338 (0.004%)	1	11343 (1.55%)	6	6	1

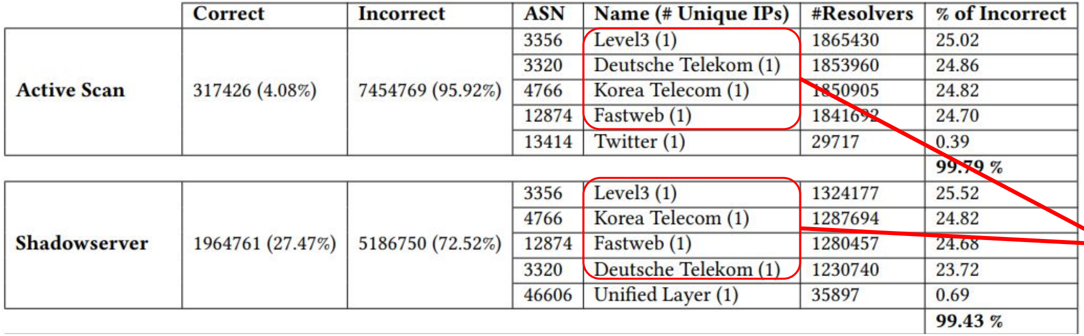
Not all successful responses have correct IP addresses



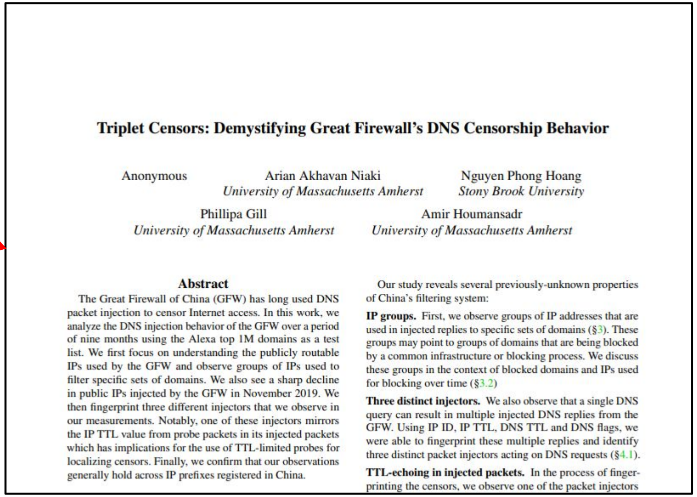
Resolvers returning high number of IP addresses in the Answer tend to be **100% valid**.

Majority of the open resolvers return incorrect IP addresses that **do not belong to google IP ranges**

99% Invalid Answers point users to 4 Unique IP addresses



	Correct	Incorrect	ASN	Name (# Unique IPs)	#Resolvers	% of Incorrect
Active Scan	317426 (4.08%)	7454769 (95.92%)	3356	Level3 (1)	1865430	25.02
			3320	Deutsche Telekom (1)	1853960	24.86
			4766	Korea Telecom (1)	1850905	24.82
			12874	Fastweb (1)	1841692	24.70
			13414	Twitter (1)	29717	0.39
						99.79 %
Shadowserver	1964761 (27.47%)	5186750 (72.52%)	3356	Level3 (1)	1324177	25.52
			4766	Korea Telecom (1)	1287694	24.82
			12874	Fastweb (1)	1280457	24.68
			3320	Deutsche Telekom (1)	1230740	23.72
			46606	Unified Layer (1)	35897	0.69
						99.43 %



Triplet Censors: Demystifying Great Firewall's DNS Censorship Behavior

Anonymous

Arian Akhavan Niaki
University of Massachusetts Amherst

Nguyen Phong Hoang
Stony Brook University

Phillipa Gill
University of Massachusetts Amherst

Amir Houmansadr
University of Massachusetts Amherst

Abstract

The Great Firewall of China (GFW) has long used DNS packet injection to censor Internet access. In this work, we analyze the DNS injection behavior of the GFW over a period of nine months using the Alexa top 1M domains as a test list. We first focus on understanding the publicly routable IPs used by the GFW and observe groups of IPs used to filter specific sets of domains. We also see a sharp decline in public IPs injected by the GFW in November 2019. We then fingerprint three different injectors that we observe in our measurements. Notably, one of these injectors mirrors the IP TTL value from probe packets in its injected packets which has implications for the use of TTL-limited probes for localizing censors. Finally, we confirm that our observations generally hold across IP prefixes registered in China.

Our study reveals several previously-unknown properties of China's filtering system:

IP groups. First, we observe groups of IP addresses that are used in injected replies to specific sets of domains (§3). These groups may point to groups of domains that are being blocked by a common infrastructure or blocking process. We discuss these groups in the context of blocked domains and IPs used for blocking over time (§3.2)

Three distinct injectors. We also observe that a single DNS query can result in multiple injected DNS replies from the GFW. Using IP ID, IP TTL, DNS TTL and DNS flags, we were able to fingerprint these multiple replies and identify three distinct packet injectors acting on DNS requests (§4.1).

TTL-echoing in injected packets. In the process of fingerprinting the censors, we observe one of the packet injectors

RANCHER
BY SUSE

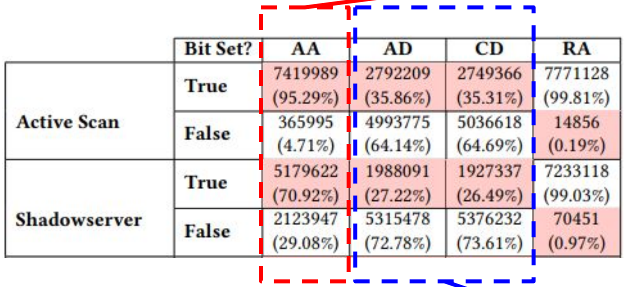
Included in the `Cattle-CA` module certificate of `rancher`

8.7.198.46
46.82.174.69
59.24.3.174
93.46.8.90

IPs returned from DNS resolvers matching GFW DNS injection fingerprint

99% of all invalid responses contain one of the same 4 IP addresses.

Resolvers Claim Authoritativeness of Answers …

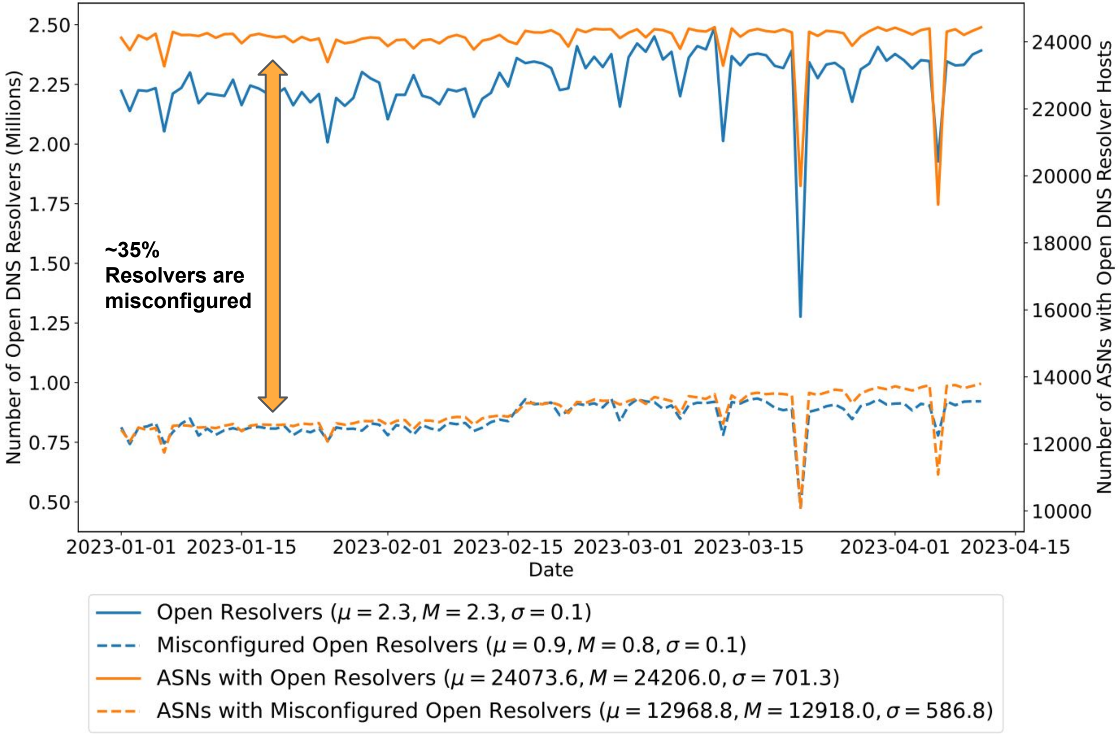


	Bit Set?	AA	AD	CD	RA
Active Scan	True	7419989 (95.29%)	2792209 (35.86%)	2749366 (35.31%)	7771128 (99.81%)
	False	365995 (4.71%)	4993775 (64.14%)	5036618 (64.69%)	14856 (0.19%)
Shadowserver	True	5179622 (70.92%)	1988091 (27.22%)	1927337 (26.49%)	7233118 (99.03%)
	False	2123947 (29.08%)	5315478 (72.78%)	5376232 (73.61%)	70451 (0.97%)

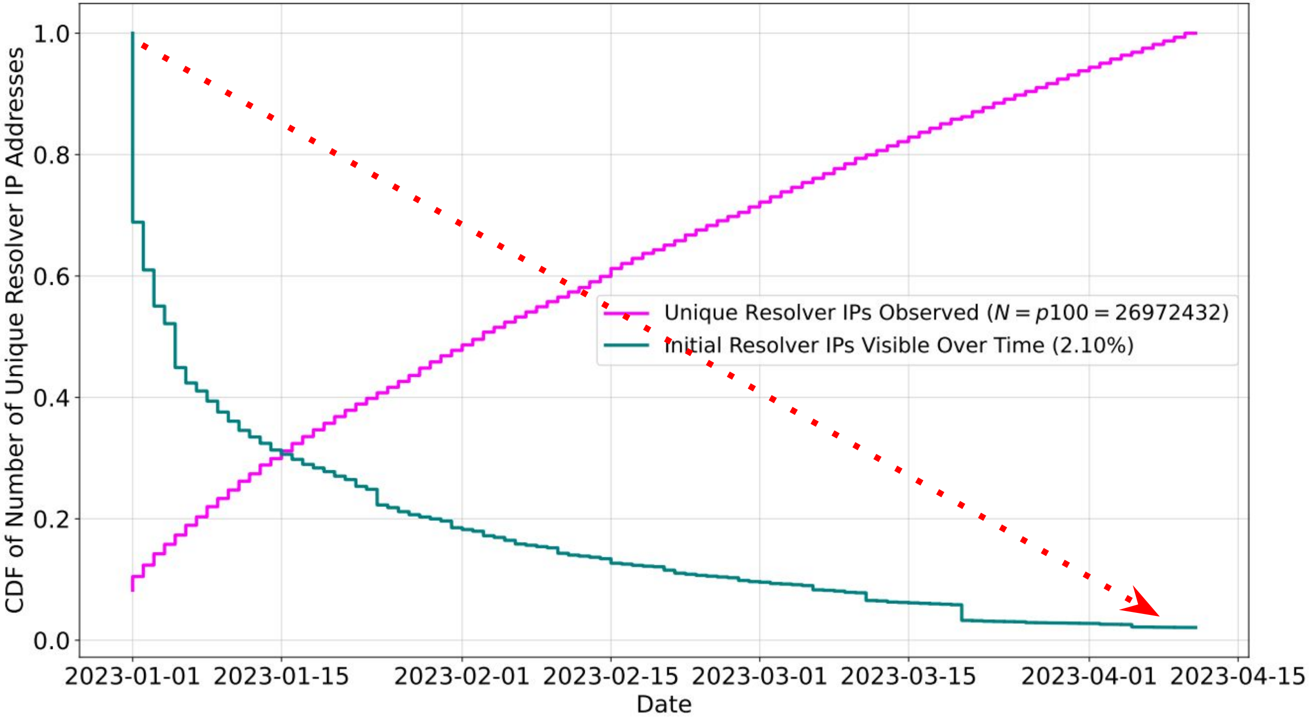
Majority resolvers **claim to be authoritative** when resolving the query for google.com

> ¼ of the resolvers **claim to have validated DNSSEC** responses … when none exist.

Misconfigured/Incorrect DNS Resolvers are increasing

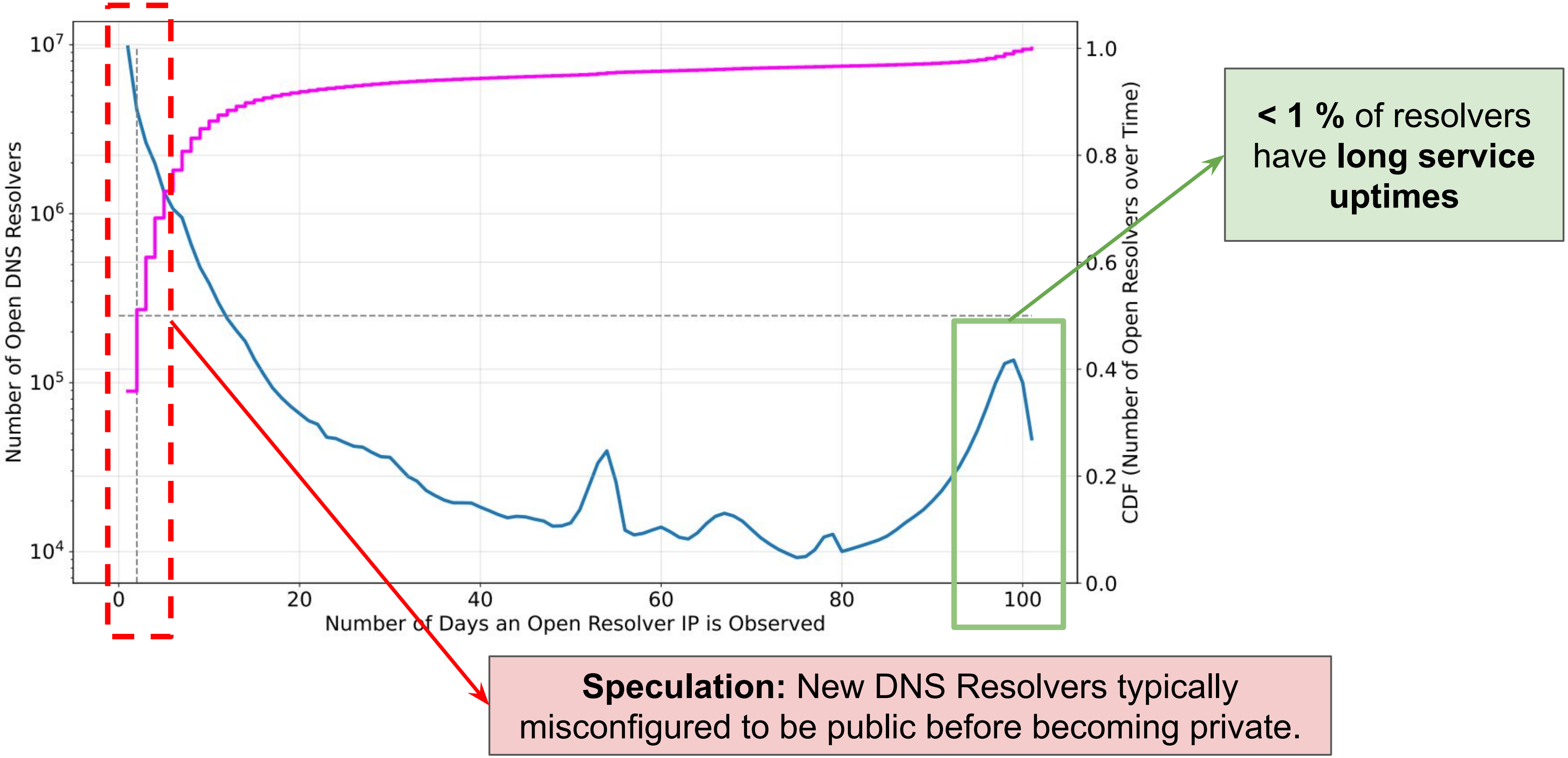


Open DNS Resolvers are Extremely Transient



Only 2.1% of resolver IP addresses **seen on the first day** are **available on the 100th day**.

50% Resolvers are available for 2 days or lesser.



< 1 % of resolvers have **long service uptimes**

Speculation: New DNS Resolvers typically misconfigured to be public before becoming private.

In the presence of *broken DNSSEC* zones

~ **17%** of the DNS resolvers responding to google.com queries **respond successfully to brokendnssec.net**

92% of resolvers answer with IP addresses of the zone and therefore do not respect client set DNSSEC bit or validate the responses.

Lesser IP answer invalidity, **is google.com query a special case?**
How do we study response behavior for different queries?

Conclusion and Gearing up for Future Challenges.

1. Increasing number of deployments of DNS resolvers
    a. Discoverability is a challenge for IPv6 deployments
    b. Transient nature of DNS resolvers makes it hard to study if IP rotations are performed. [Why?]
    c. Harder to measure and study with increasing private in-network deployments.
2. Hard to report resolvers with incorrect behavior to operators.
    a. There’s no disclosure process in place, risk amplification and reflection attacks.
3. Possibility for On-Path middleboxes tampering responses
4. Clients do not use DNSSEC DO bit by default, is it time they should?

Thank You!