APNIC

Insights on DNS Security in the APAC region

Sheryl (Shane) Hermoso

January 2023

Overview

- DNS Security Landscape
- DNS Security Stats & Trends in the region
- DNS Best Practices & Guidelines

DNS Security Landscape

DNS Threat Landscape

88% of organisations experienced DNS attack [1]

DNS Phishing **51%**
DNS-based malware **43%**
DNS-based DDoS attacks **30%**

DNS hijacking / credentials attack **28%**
Zero-day vulnerabilities **26%**
Cloud instance misconfiguration abuse **27%**

40% increase in use of DoT traffic [2]

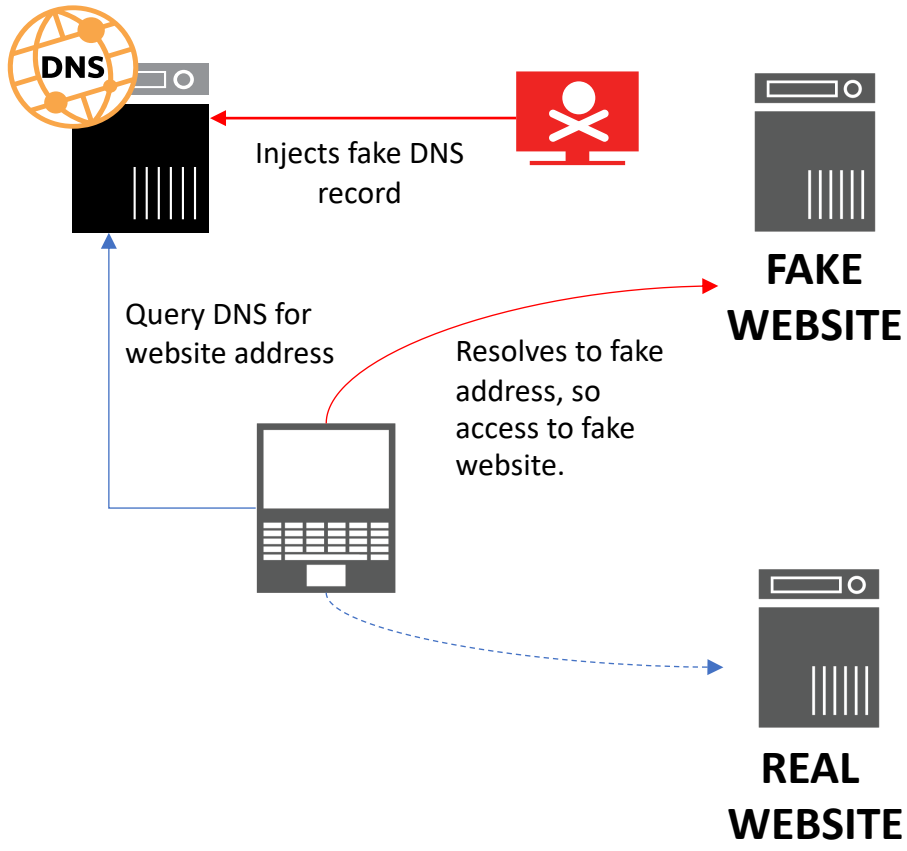
[1] 2022 Global DNS Threat Report

[2] Akamai DNS Threat Report Q3 2022

DNS Spoofing

Injects incorrect DNS data into DNS to redirect clients to fake or malicious site

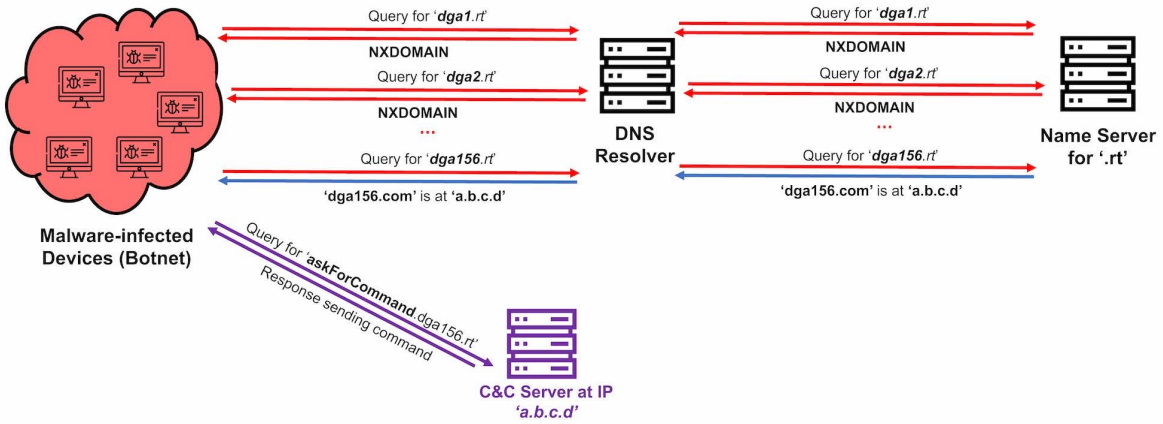
- Methods:
  - DNS cache poisoning
- Mitigation:
  - DNSSEC

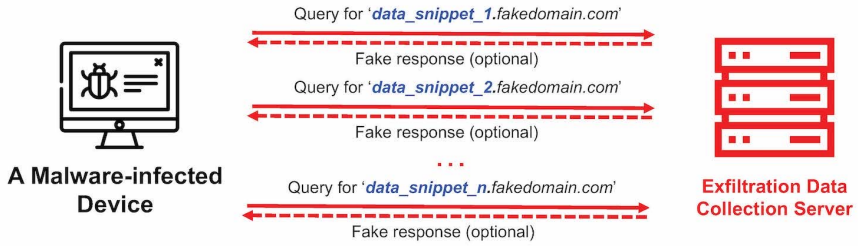


DNS-based Malware

Using DNS for malware activities

- Methods:
  - Command & control over DNS
  - Data exfiltration
- Mitigation:
  - DNS packet inspection



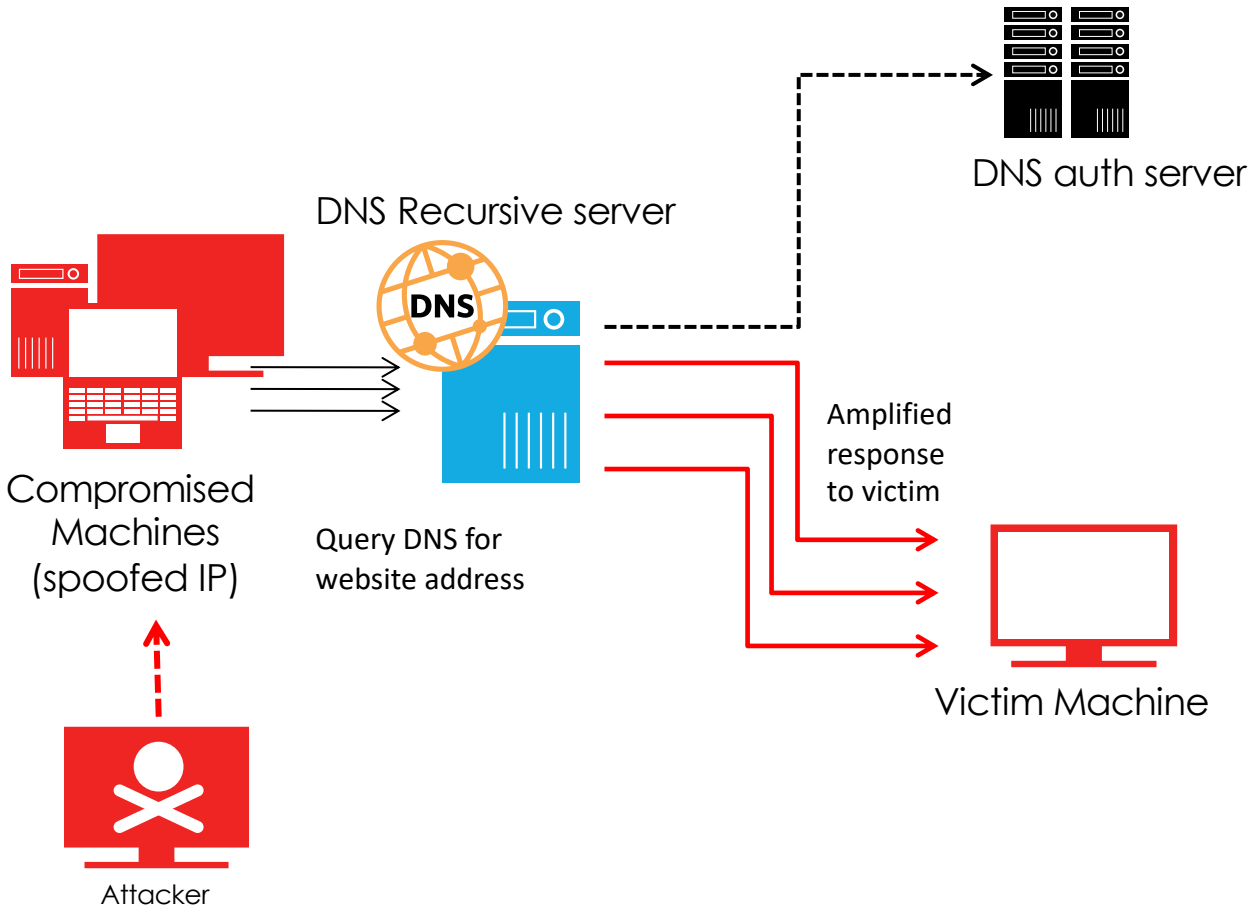


Ref: APNIC Blog: DNS malware misuse and current countermeasures

DNS-based DDoS Attacks

Using DNS to overwhelm a [dns] server to disrupt its function

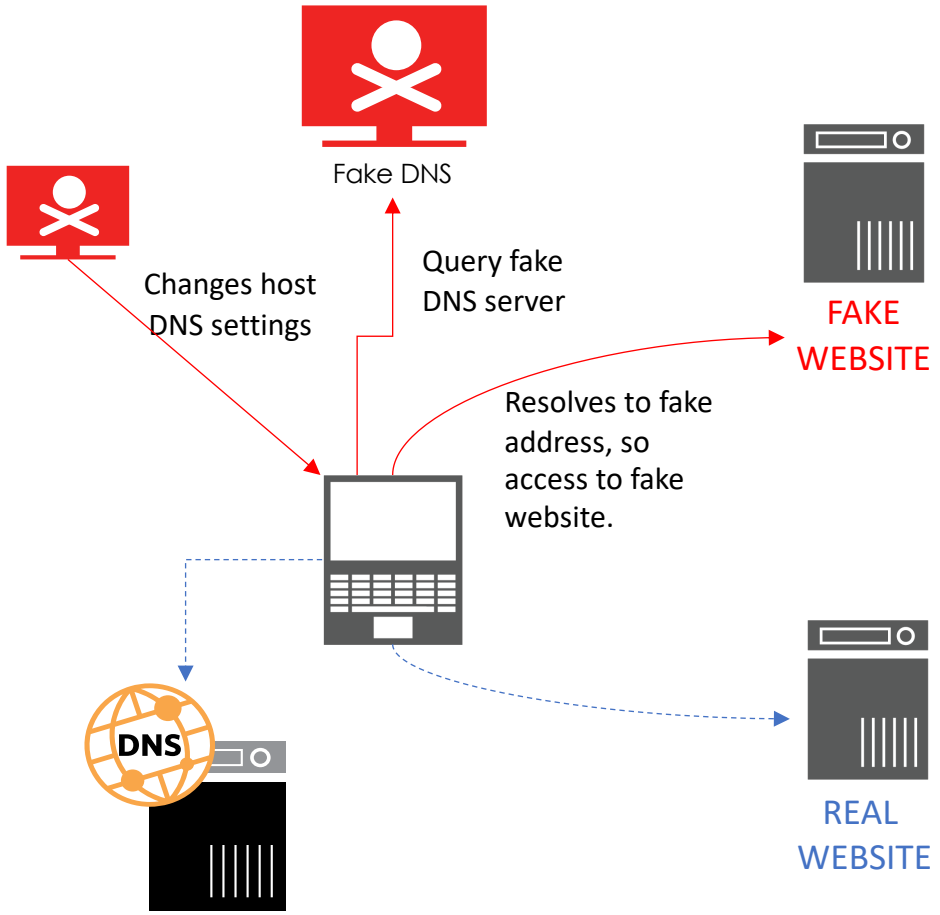
- Methods:
  - DNS Amplification
  - DNS Flooding
  - DNS Water Torture
- Mitigation:
  - Distributed DNS system
  - Rate limiting
  - Third-party DDoS protection



DNS Hijacking

Hijack a client or server to change DNS settings or records

- Methods:
  - Change the host or router DNS settings through malware
  - Hack DNS server to change DNS records
- Mitigation:
  - Improve DNS server security (authentication & data integrity)

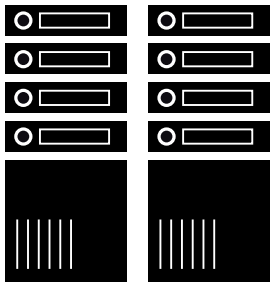


DNS Security

- Data exchange or transactions => (**TSIG**, **SIG0**)
- Data accuracy from the right source => (**DNSSEC**)
- DNS transport security or privacy => (**DoH**, **DoT**)
- Access to legitimate sites/content => (**DNS Filtering**)
- Availability of DNS service => (**DNS Resiliency**)

DNSSEC Signing

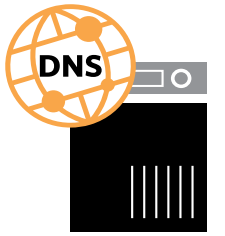
- Applied on authoritative server
- Signs the zones
- Answers queries with the record requested
- Also sends the digital signature corresponding to the record



DNS Auth Server

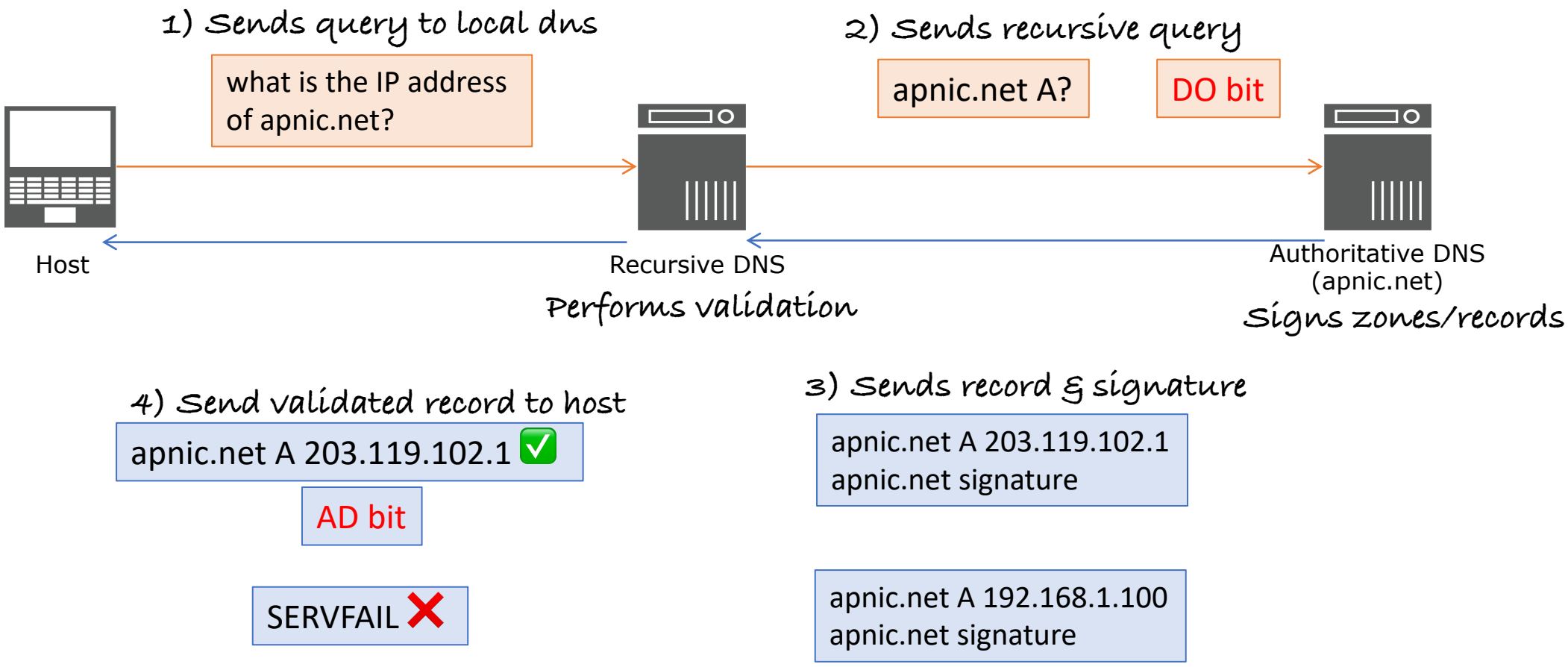
DNSSEC Validation

- implemented in resolvers
- Authenticates the responses from the server
- Data that is not validated results to a “SERVFAIL” error



DNS Resolver

DNSSEC Validation (Diagram)



Encrypted DNS

DNS over TLS

- DNS queries are sent over TLS-encrypted TCP connections
- Avoids spoofing, eavesdropping and DNS-based filters

DNS over HTTPS

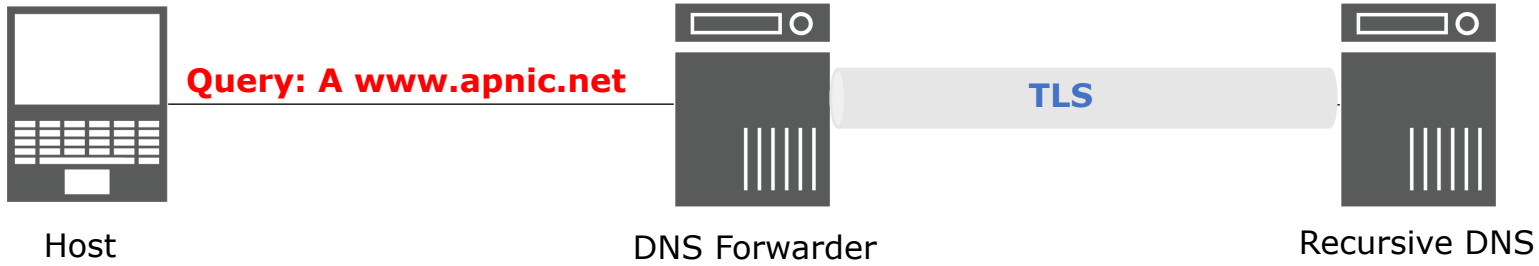
- DNS queries done securely over HTTPS
- prevents on-path devices from interfering with DNS operations
- allows web applications to access DNS information via existing browser APIs

DoT – Architecture

SETUP 1:

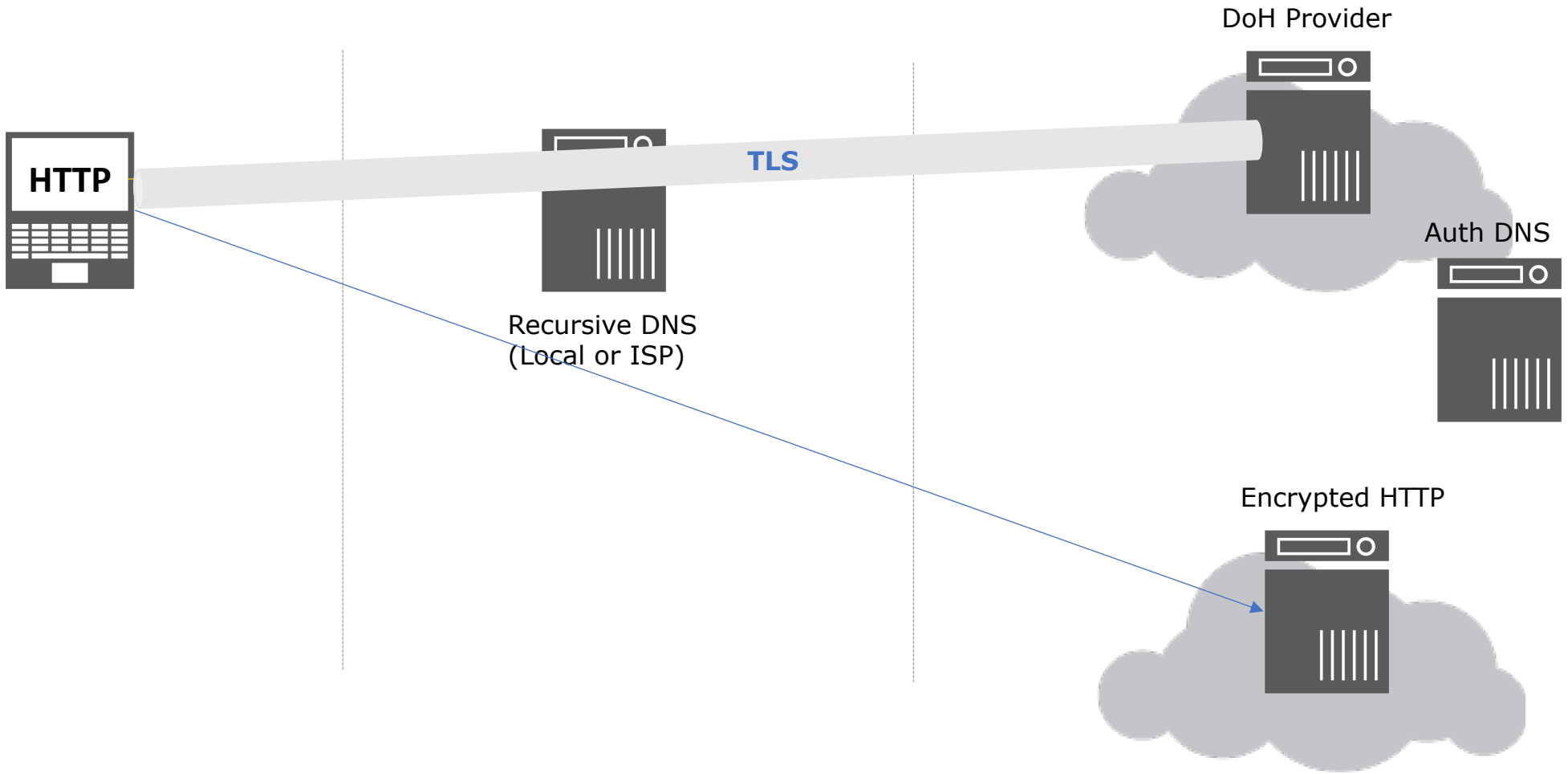
Host must run a DoT-capable resolver
No DNS Traffic will show to eavesdropper

SETUP 2:



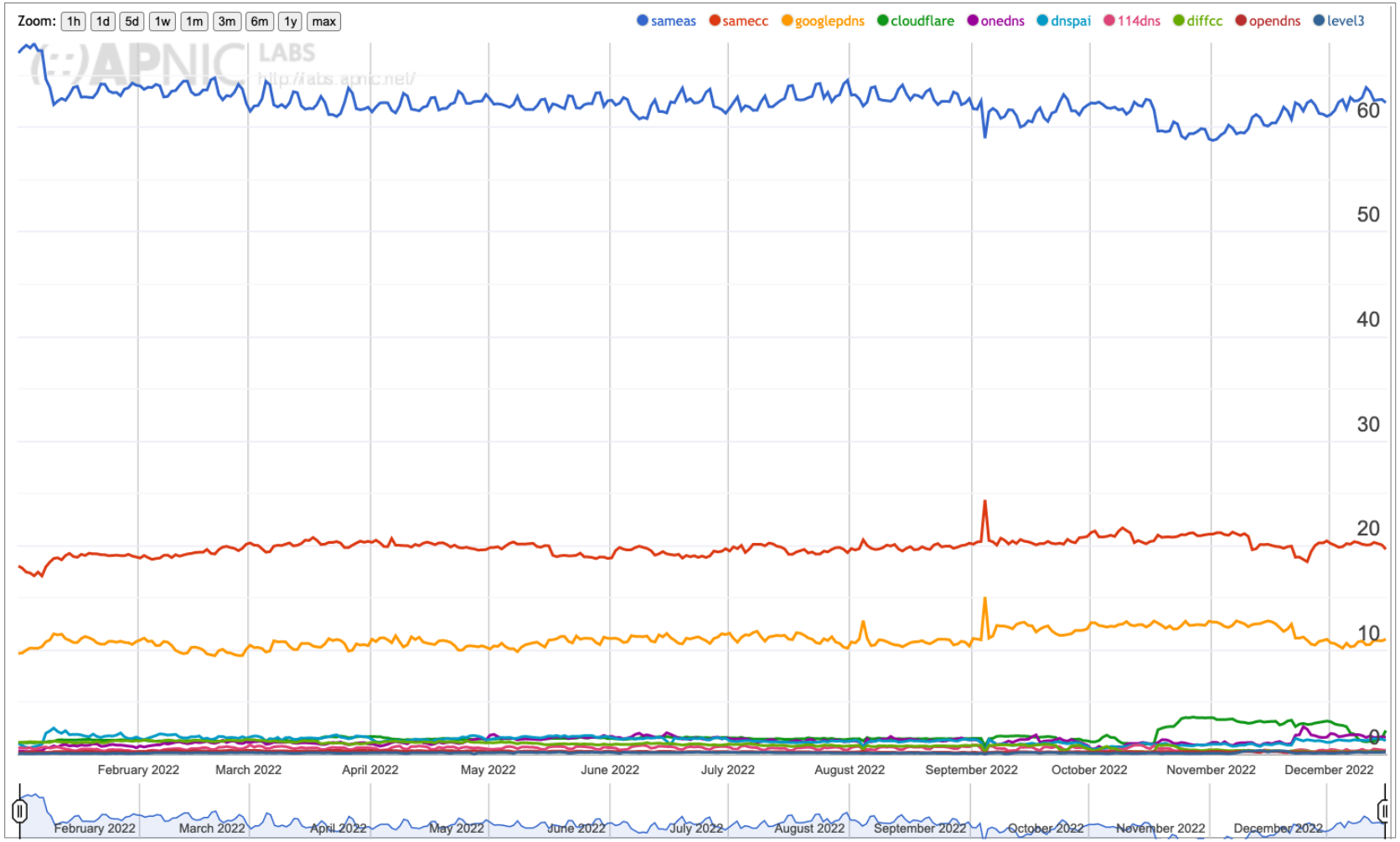
Local recursive server forwards queries via TLS
Typically sent to chosen/trusted local or cloud DNS

DoH – Architecture



DNS Security Stats & Trends

DNS Resolvers – Asia (1)



https://stats.labs.apnic.net/rvrs/XD?o=cXAw1l1s0t10x

DNS Resolvers – Asia (2)

Majority of DNS servers are deployed in the same network and/or within the same economy.

There is also a significant percentage using cloud DNS providers

CC	Country	sameas	samecc	onedns	dnspai	googlepdns	114dns	cloudflare	diffcc	diffccneu	opendns	Samples	Weight	Weighted Samples
MN	Mongolia, Eastern Asia, Asia	93.256%	0.249%	0.000%	0.000%	6.215%	0.000%	0.178%	0.036%	0.031%	0.066%	19,646	0.2	3,886
MO	Macao Special Administrative Region of China, Eastern Asia, Asia	91.719%	0.063%	0.009%	0.000%	4.895%	0.045%	2.718%	0.415%	0.415%	0.108%	11,073	0.2	2,653
JP	Japan, Eastern Asia, Asia	89.722%	5.196%	0.037%	0.043%	3.070%	0.021%	0.938%	0.577%	0.575%	0.335%	264,749	2	527,044
KR	Republic of Korea, Eastern Asia, Asia	75.708%	20.648%	0.005%	0.021%	2.072%	0.009%	1.071%	0.329%	0.326%	0.096%	131,492	1.8	238,383
CN	China, Eastern Asia, Asia	71.607%	16.575%	4.805%	3.505%	1.730%	1.549%	0.056%	0.088%	0.083%	0.056%	418,039	9.2	3,854,928
HK	Hong Kong Special Administrative Region of China, Eastern Asia, Asia	59.770%	10.990%	0.478%	0.574%	15.418%	0.298%	4.183%	7.287%	7.256%	0.564%	99,013	0.3	32,629
TW	Taiwan, Eastern Asia, Asia	56.660%	34.050%	0.033%	0.029%	7.274%	0.012%	0.904%	0.816%	0.812%	0.121%	180,371	0.7	122,113

CC	Country	sameas	samecc	googlepdns	cloudflare	opendns	diffcc	diffccneu	quad9	level3	neustar	Samples	Weight	Weighted Samples
MY	Malaysia, South-Eastern Asia, Asia	86.977%	1.711%	9.441%	1.133%	0.348%	0.344%	0.309%	0.025%	0.017%	0.003%	234,437	0.6	130,449
TL	Timor-Leste, South-Eastern Asia, Asia	77.893%	0.345%	20.380%	0.173%	0.000%	0.000%	0.000%	0.000%	1.209%	0.000%	579	3.4	1,947
VN	Vietnam, South-Eastern Asia, Asia	72.039%	0.704%	23.221%	1.997%	1.752%	0.151%	0.147%	0.044%	0.019%	0.067%	209,514	1.2	250,808
ID	Indonesia, South-Eastern Asia, Asia	66.168%	16.059%	14.637%	2.014%	0.725%	0.089%	0.084%	0.293%	0.006%	0.007%	1,381,922	0.4	546,062
KH	Cambodia, South-Eastern Asia, Asia	63.202%	2.142%	32.837%	1.498%	0.086%	0.191%	0.191%	0.024%	0.004%	0.000%	24,561	1.3	32,881
MM	Myanmar, South-Eastern Asia, Asia	59.485%	0.706%	30.093%	9.435%	0.042%	0.110%	0.109%	0.129%	0.000%	0.000%	143,527	0.7	100,664
LA	Lao People's Democratic Republic, South-Eastern Asia, Asia	55.869%	0.015%	29.572%	14.162%	0.059%	0.147%	0.132%	0.162%	0.000%	0.000%	6,807	1.6	10,924
PH	Philippines, South-Eastern Asia, Asia	43.192%	34.839%	17.787%	3.493%	0.315%	0.199%	0.193%	0.092%	0.048%	0.015%	565,815	0.6	341,660
SG	Singapore, South-Eastern Asia, Asia	37.153%	23.506%	29.167%	4.931%	0.826%	3.599%	3.503%	0.395%	0.075%	0.010%	70,851	0.3	23,914
TH	Thailand, South-Eastern Asia, Asia	22.861%	65.291%	9.810%	1.340%	0.339%	0.321%	0.307%	0.026%	0.004%	0.008%	211,808	1	210,200
BN	Brunei Darussalam, South-Eastern Asia, Asia	2.248%	0.000%	96.685%	0.738%	0.082%	0.246%	0.246%	0.000%	0.000%	0.000%	6,094	0.4	2,294

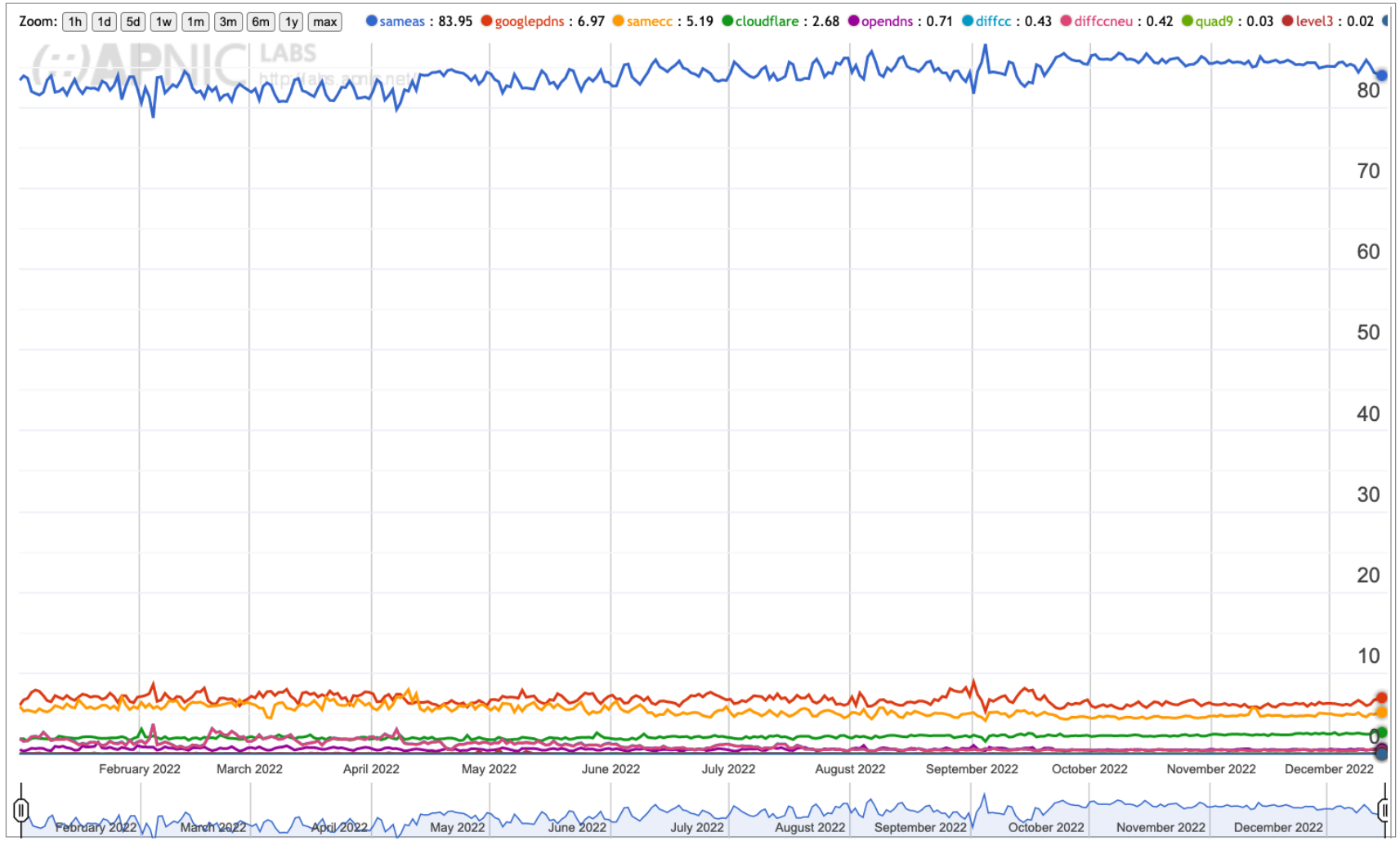
Good read: Looking at centrality in the DNS

DNS Resolvers – Asia (3)

Due to large user population, 17% of all Google DNS users are from India.

CC	Country	sameas	samecc	googlepdns	cloudflare	diffcc	diffccneu	opendns	level3	diffcceu	quad9	Samples	Weight	Weighted Samples
LK	Sri Lanka, Southern Asia, Asia	93.391%	0.021%	6.175%	0.264%	0.055%	0.039%	0.090%	0.003%	0.015%	0.002%	65,913	0.6	37,794
NP	Nepal, Southern Asia, Asia	81.432%	3.331%	14.058%	0.874%	0.153%	0.147%	0.089%	0.004%	0.005%	0.055%	56,382	0.6	33,670
BT	Bhutan, Southern Asia, Asia	80.802%	9.893%	7.861%	0.428%	0.107%	0.107%	0.267%	0.000%	0.000%	0.642%	1,870	1.1	2,053
IN	India, Southern Asia, Asia	57.287%	27.690%	14.159%	0.354%	0.230%	0.224%	0.166%	0.097%	0.006%	0.016%	4,420,702	0.6	2,754,187
PK	Pakistan, Southern Asia, Asia	54.587%	17.730%	25.844%	1.394%	0.263%	0.245%	0.118%	0.013%	0.018%	0.029%	431,196	0.4	169,156
BD	Bangladesh, Southern Asia, Asia	53.218%	3.460%	36.432%	5.890%	0.554%	0.553%	0.159%	0.266%	0.001%	0.006%	421,828	0.4	155,230
AF	Afghanistan, Southern Asia, Asia	21.373%	3.216%	39.693%	5.547%	21.481%	8.799%	4.770%	1.066%	12.683%	0.145%	5,535	4.5	25,046
IR	Iran (Islamic Republic of), Southern Asia, Asia	16.311%	0.231%	18.478%	64.489%	0.177%	0.139%	0.068%	0.192%	0.038%	0.047%	46,828	6.2	290,264
MV	Maldives, Southern Asia, Asia	1.802%	0.065%	74.924%	22.340%	0.109%	0.109%	0.651%	0.087%	0.000%	0.000%	4,606	0.4	1,791

DNS Resolvers – Oceania (1)



https://stats.labs.apnic.net/rvrs/XF?o=cXAw1l1s0t10x

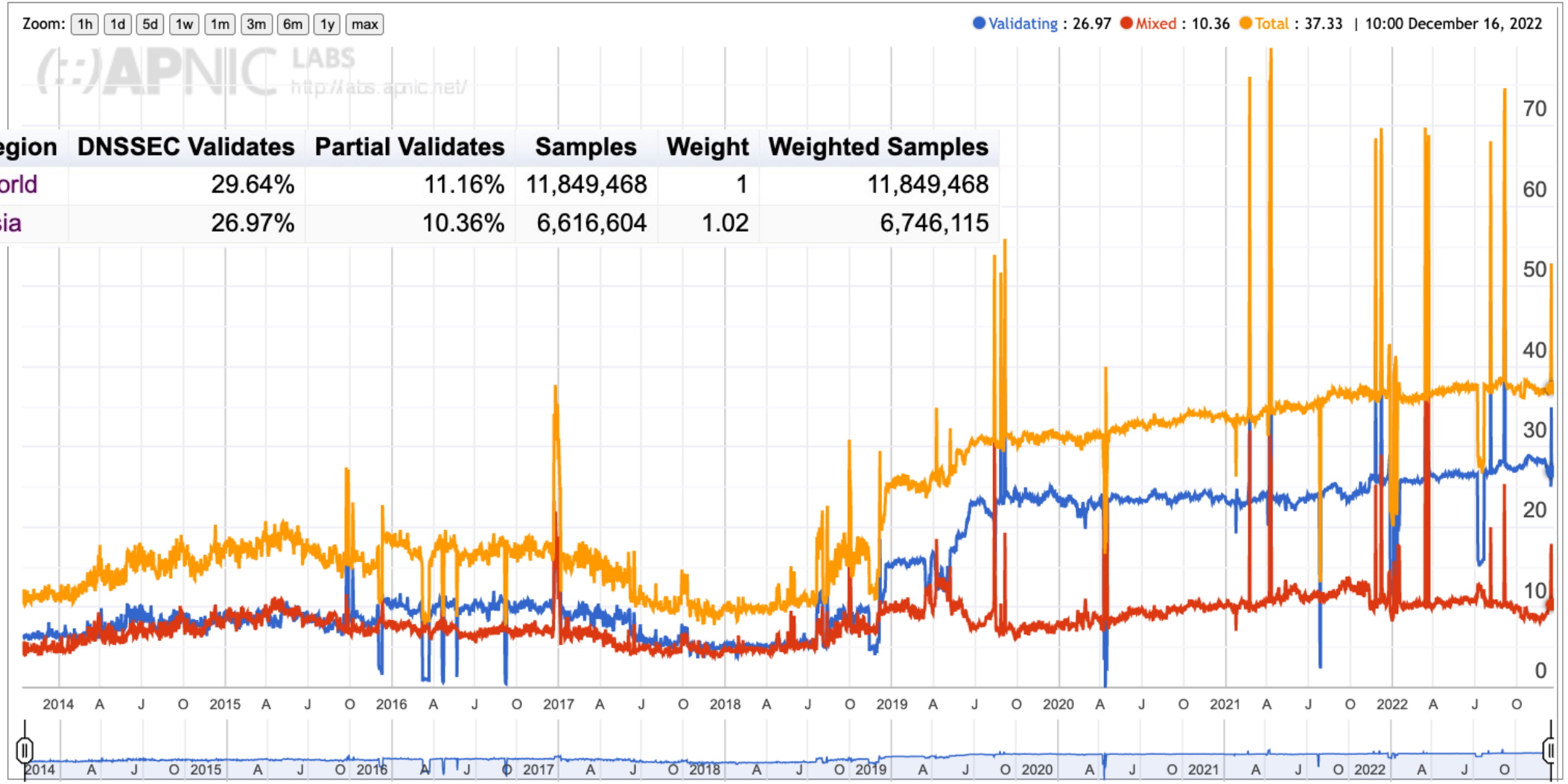
DNS Resolvers – Oceania (2)

Majority of DNS servers are deployed in the same network.

CC	Country	sameas	googlepdns	samecc	cloudflare	opendns	diffcc	diffccneu	quad9	level3	cleanbrowsing	Samples	Weight	Weighted Samples
WS	Samoa, Polynesia, Oceania	98.152%	1.087%	0.000%	0.000%	0.000%	0.761%	0.761%	0.000%	0.000%	0.000%	920	0.4	370
TO	Tonga, Polynesia, Oceania	92.100%	2.287%	0.000%	4.366%	0.000%	1.247%	1.247%	0.000%	0.000%	0.000%	481	0.4	208
NR	Nauru, Micronesia, Oceania	92.000%	2.667%	0.000%	1.333%	0.000%	4.000%	4.000%	0.000%	0.000%	0.000%	75	0.4	26
VU	Vanuatu, Melanesia, Oceania	91.775%	5.628%	0.000%	1.299%	0.433%	0.866%	0.866%	0.000%	0.000%	0.000%	231	1.7	400
SB	Solomon Islands, Melanesia, Oceania	87.908%	9.981%	0.000%	0.000%	0.768%	0.576%	0.576%	0.000%	0.000%	0.768%	521	0.8	423
AU	Australia, Australia and New Zealand, Oceania	85.953%	4.966%	5.591%	2.464%	0.593%	0.375%	0.356%	0.024%	0.017%	0.003%	126,162	0.8	101,198
FJ	Fiji, Melanesia, Oceania	85.780%	2.794%	2.476%	8.560%	0.230%	0.053%	0.053%	0.018%	0.000%	0.088%	5,654	0.4	2,303
CK	Cook Islands, Polynesia, Oceania	85.463%	10.132%	0.000%	0.000%	0.000%	3.524%	3.524%	0.000%	0.000%	0.000%	227	0.2	44
KI	Kiribati, Micronesia, Oceania	84.390%	12.683%	0.000%	1.463%	0.000%	0.976%	0.976%	0.000%	0.488%	0.000%	205	0.4	87
NZ	New Zealand, Australia and New Zealand, Oceania	83.064%	5.414%	6.418%	3.524%	0.852%	0.594%	0.591%	0.106%	0.000%	0.027%	32,972	0.6	20,478
NC	New Caledonia, Melanesia, Oceania	80.387%	13.131%	0.168%	4.882%	0.168%	0.084%	0.084%	0.589%	0.337%	0.000%	1,188	1	1,186
PW	Palau, Micronesia, Oceania	78.605%	13.953%	0.000%	5.116%	0.000%	0.930%	0.930%	0.000%	0.000%	0.000%	215	0.2	45
PG	Papua New Guinea, Melanesia, Oceania	70.508%	28.051%	0.466%	0.297%	0.127%	0.466%	0.466%	0.000%	0.000%	0.085%	2,360	2.4	5,756
FM	Micronesia (Federated States of), Micronesia, Oceania	66.767%	29.305%	0.906%	0.000%	0.000%	0.604%	0.604%	0.000%	0.000%	0.000%	331	2.9	964
PF	French Polynesia, Polynesia, Oceania	57.047%	17.195%	8.631%	5.664%	0.607%	10.856%	10.856%	0.000%	0.000%	0.000%	1,483	0.7	1,021
AS	American Samoa, Polynesia, Oceania	54.844%	43.906%	0.000%	0.938%	0.156%	0.156%	0.156%	0.000%	0.000%	0.000%	640	0.2	137
GU	Guam, Micronesia, Oceania	42.560%	38.400%	14.320%	1.760%	1.960%	0.640%	0.640%	0.000%	0.000%	0.000%	2,500	0.3	666
NF	Norfolk Island, Australia and New Zealand, Oceania	35.714%	64.286%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	14	0.4	5
MH	Marshall Islands, Micronesia, Oceania	24.766%	57.477%	0.000%	12.150%	0.000%	5.607%	5.607%	0.000%	0.000%	0.000%	214	0.7	150
MP	Northern Mariana Islands, Micronesia, Oceania	23.762%	69.901%	0.000%	1.188%	5.149%	0.000%	0.000%	0.000%	0.000%	0.000%	505	0.3	143
TV	Tuvalu, Polynesia, Oceania	0.000%	25.000%	0.000%	0.000%	62.500%	12.500%	12.500%	0.000%	0.000%	0.000%	16	1.8	29
WF	Wallis and Futuna Islands, Polynesia, Oceania	0.000%	100.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	42	0.7	27

DNSSEC Validation – Asia

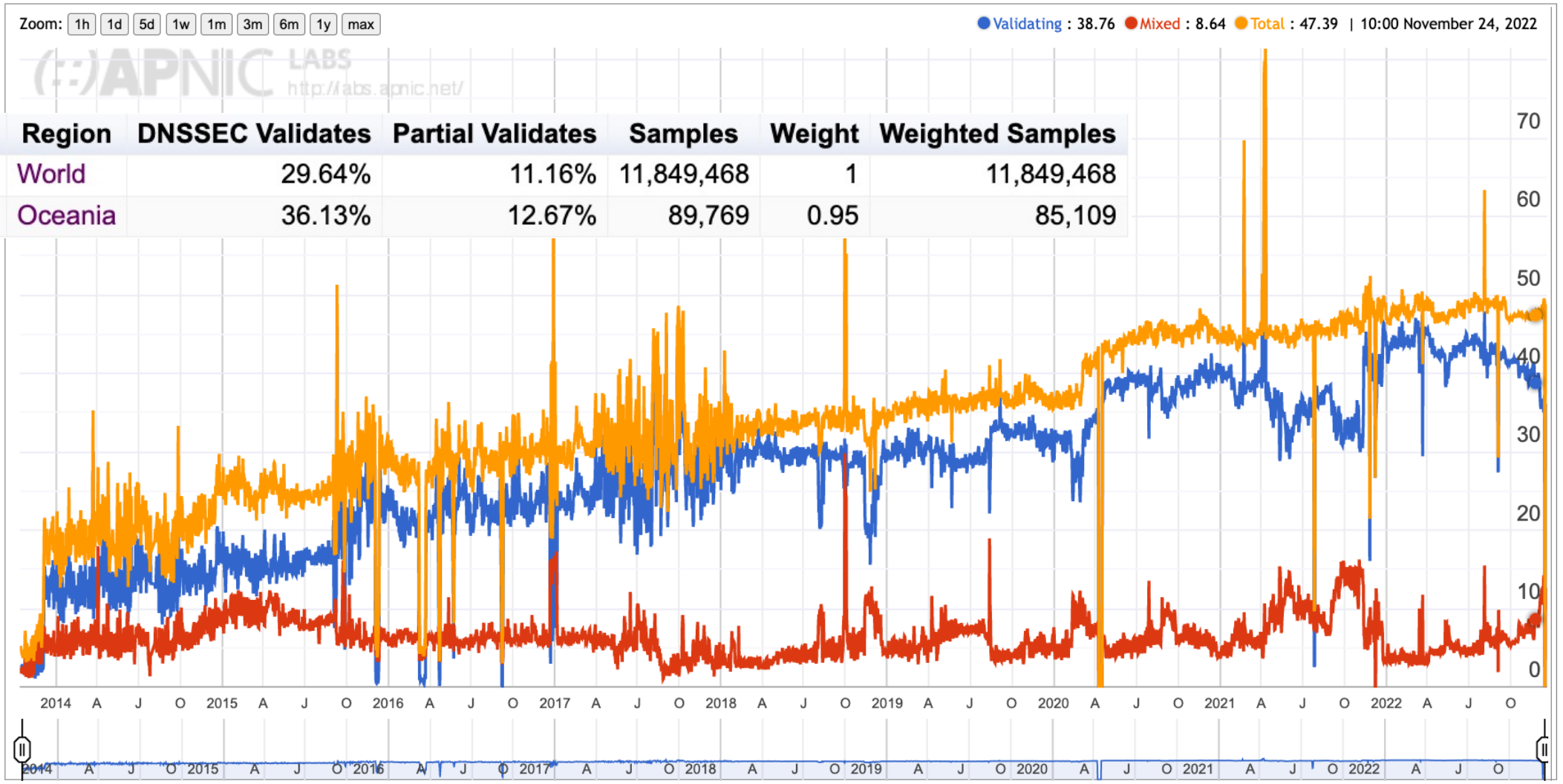
Code	Region	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
XA	World	29.64%	11.16%	11,849,468	1	11,849,468
XD	Asia	26.97%	10.36%	6,616,604	1.02	6,746,115



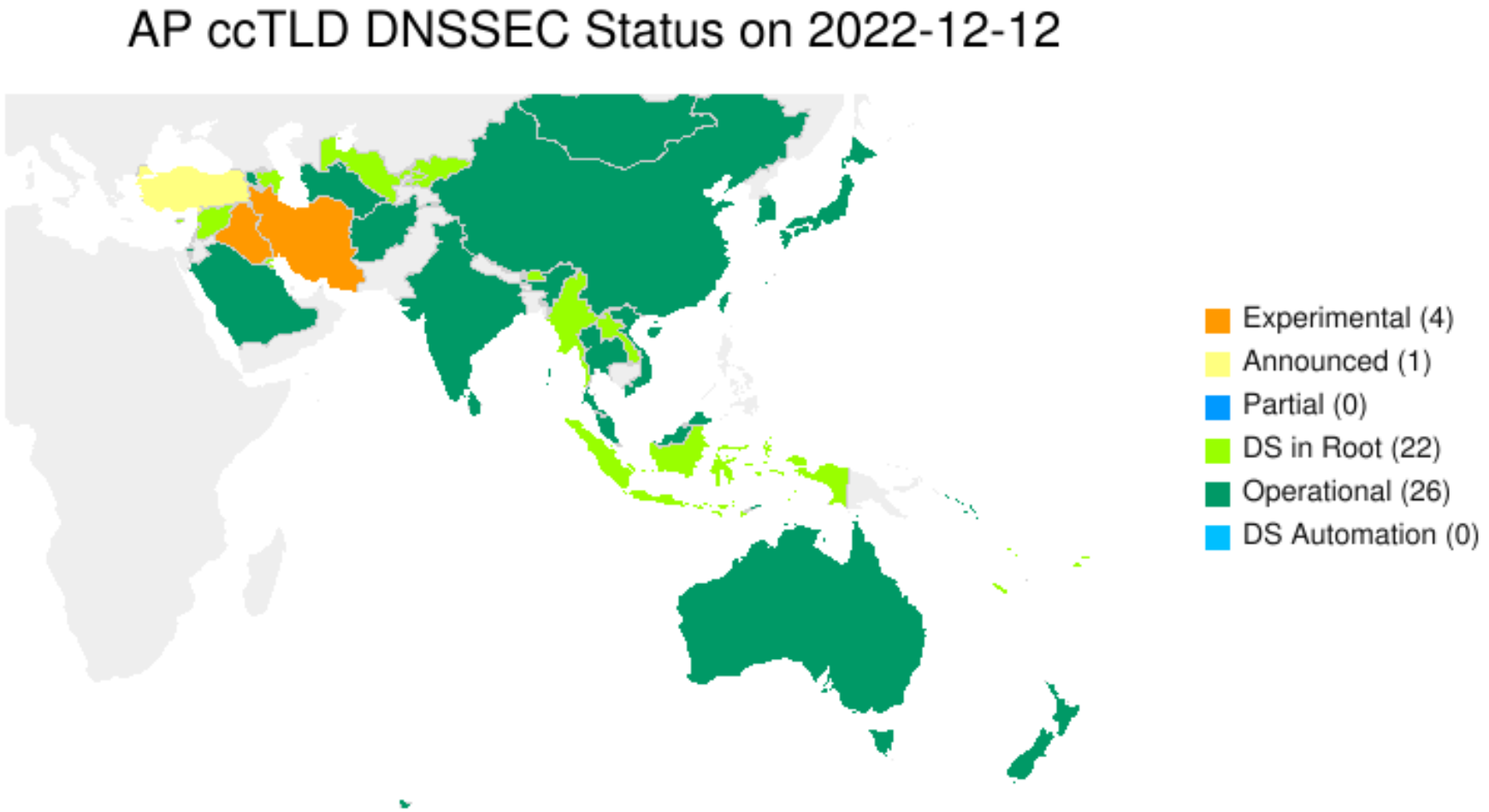
https://stats.labs.apnic.net/dnssec

DNSSEC Validation – Oceania

Code	Region	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
XA	World	29.64%	11.16%	11,849,468	1	11,849,468
XF	Oceania	36.13%	12.67%	89,769	0.95	85,109



DNSSEC in the AP Region



Ref: https://www.internetsociety.org/deploy360/dnssec/statistics/

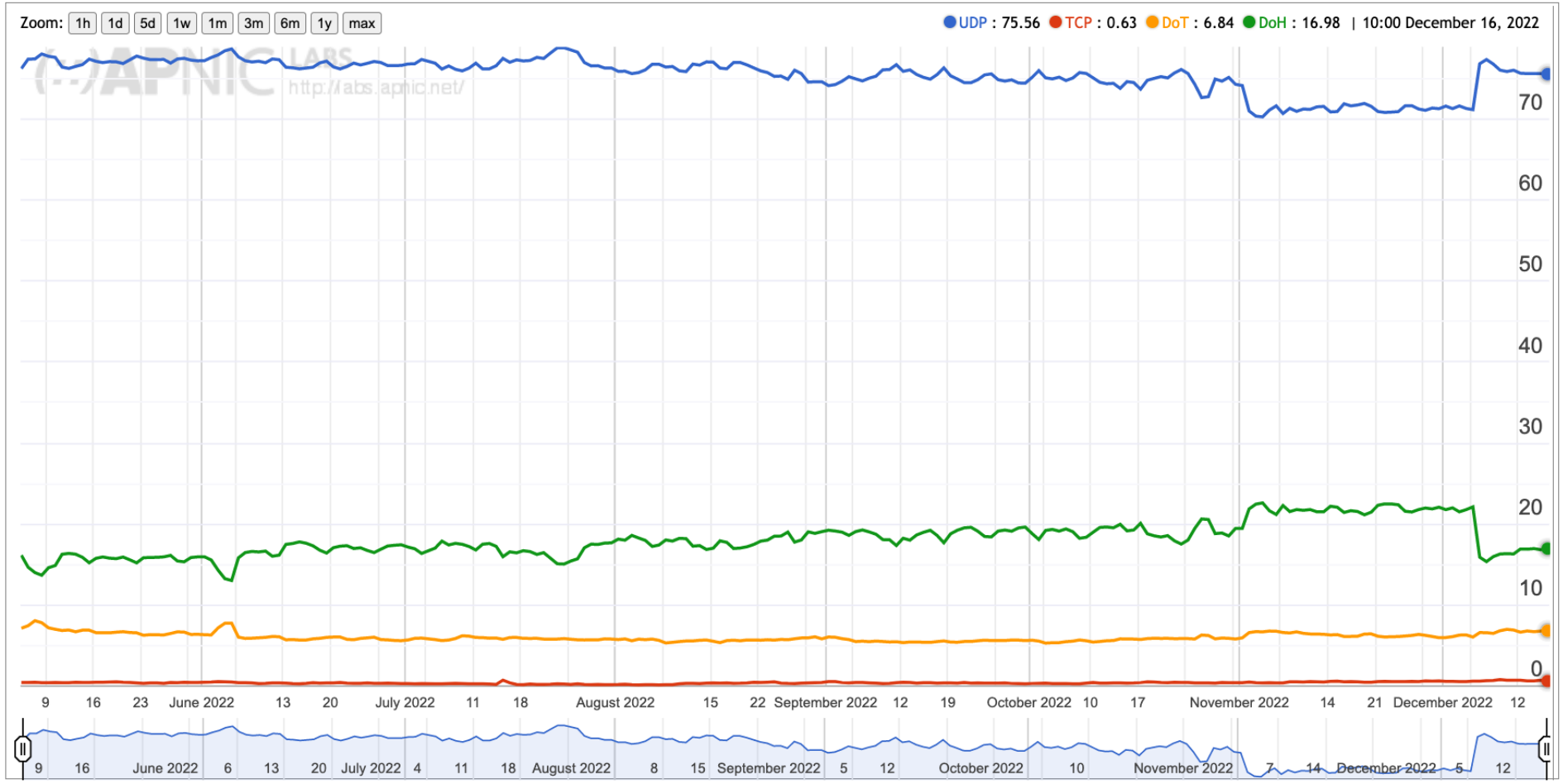
DNSSEC in the AP Region – Unsigned ccTLDs

South-East Asia	East Asia	South Asia	Oceania
.**bn** (Brunei) .**kh** (Cambodia) .**mm** (Myanmar) .**ph** (Philippines)	.**kp** (North Korea) .**mo** (Macau)	.**bd** (Bangladesh) .**mv** (Maldives) .**np** (Nepal) .**pk** (Pakistan)	.**as** (American Samoa) .**ck** (Cook Islands) .**fj** (Fiji) .**gu** (Guam) .**mh** (Marshall Islands) .**nr** (Nauru) .**pg** (PNG) .**tk** (Tokelau) .**to** (Tonga) .**ws** (Samoa)

Also check out for other gTLDs https://rick.eng.br/dnssecstat/ccmap.html

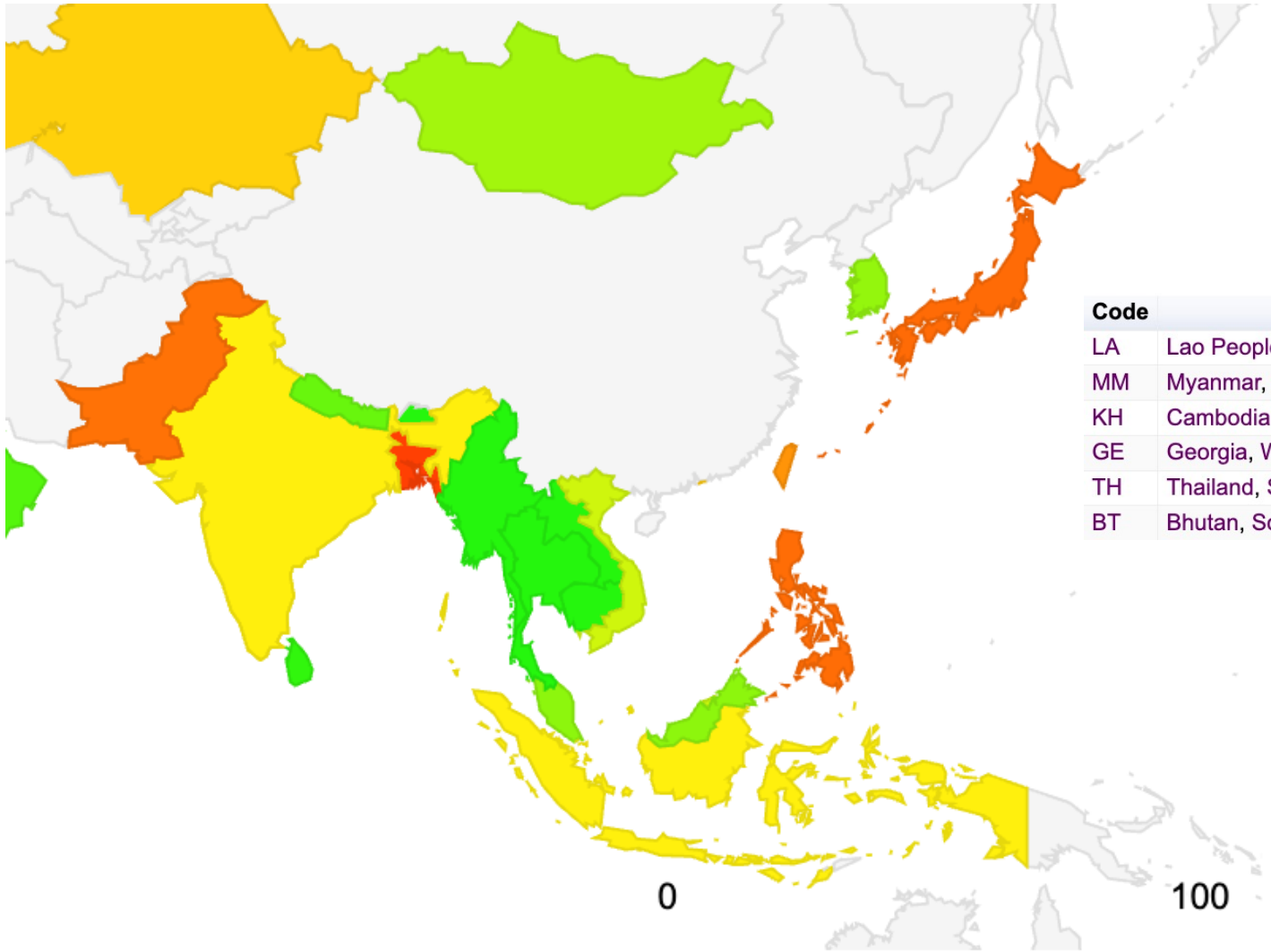
Encrypted DNS – Asia (1)

Cloudflare Open Recursive Resolver DNS Query Profile for Asia (XD)



https://stats.labs.apnic.net/edns/XF

Encrypted DNS – Asia (2)



https://stats.labs.apnic.net/edns/XD

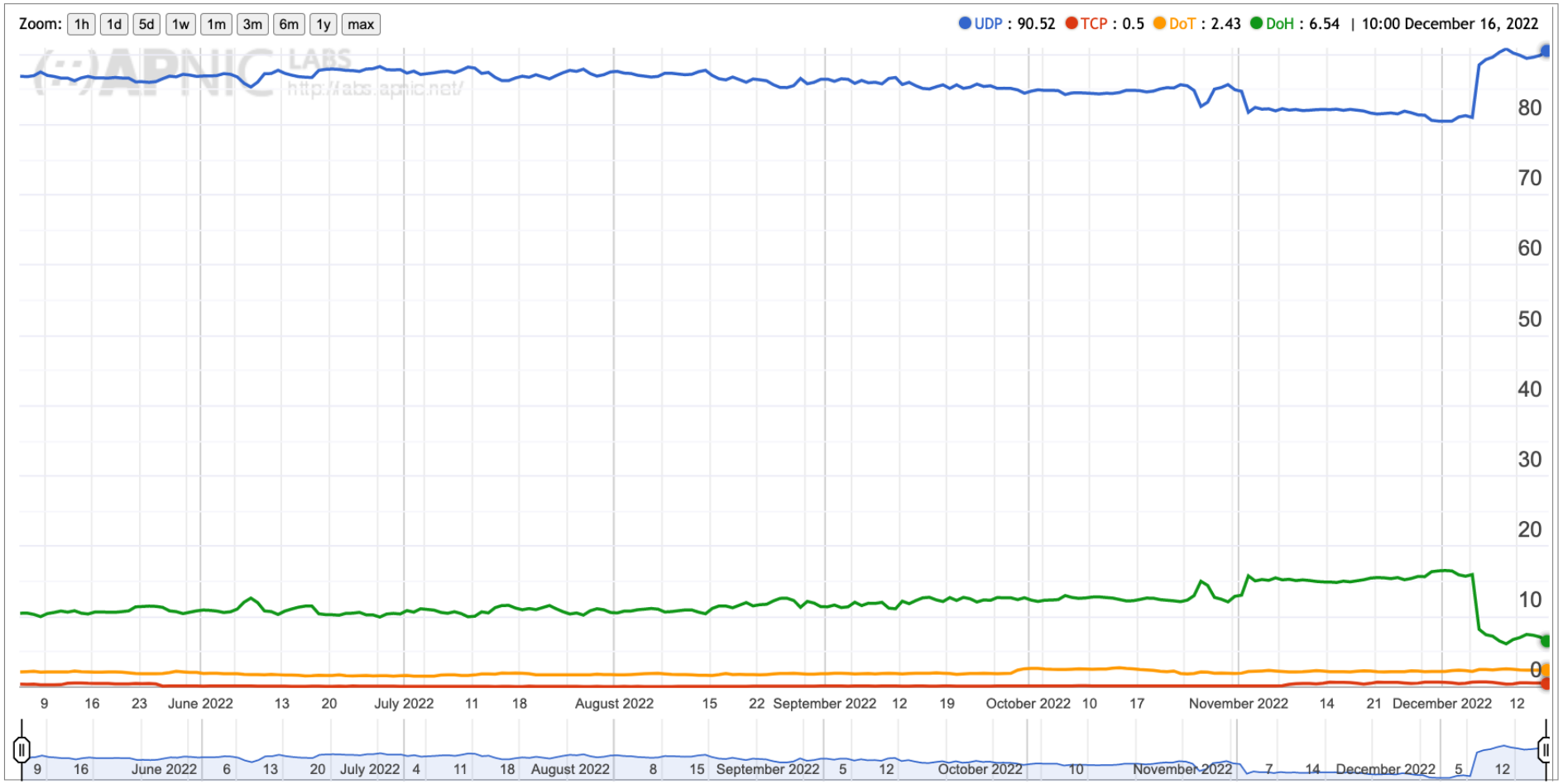
Notice LA, TH, MM are high

Code	Region	DoH Queries	DoT Queries
LA	Lao People's Democratic Republic, South-Eastern Asia, Asia	99.74%	0.02%
MM	Myanmar, South-Eastern Asia, Asia	92.71%	0.19%
KH	Cambodia, South-Eastern Asia, Asia	54.28%	3.24%
GE	Georgia, Western Asia, Asia	53.15%	0.89%
TH	Thailand, South-Eastern Asia, Asia	48.76%	3.63%
BT	Bhutan, Southern Asia, Asia	44.47%	10.17%

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

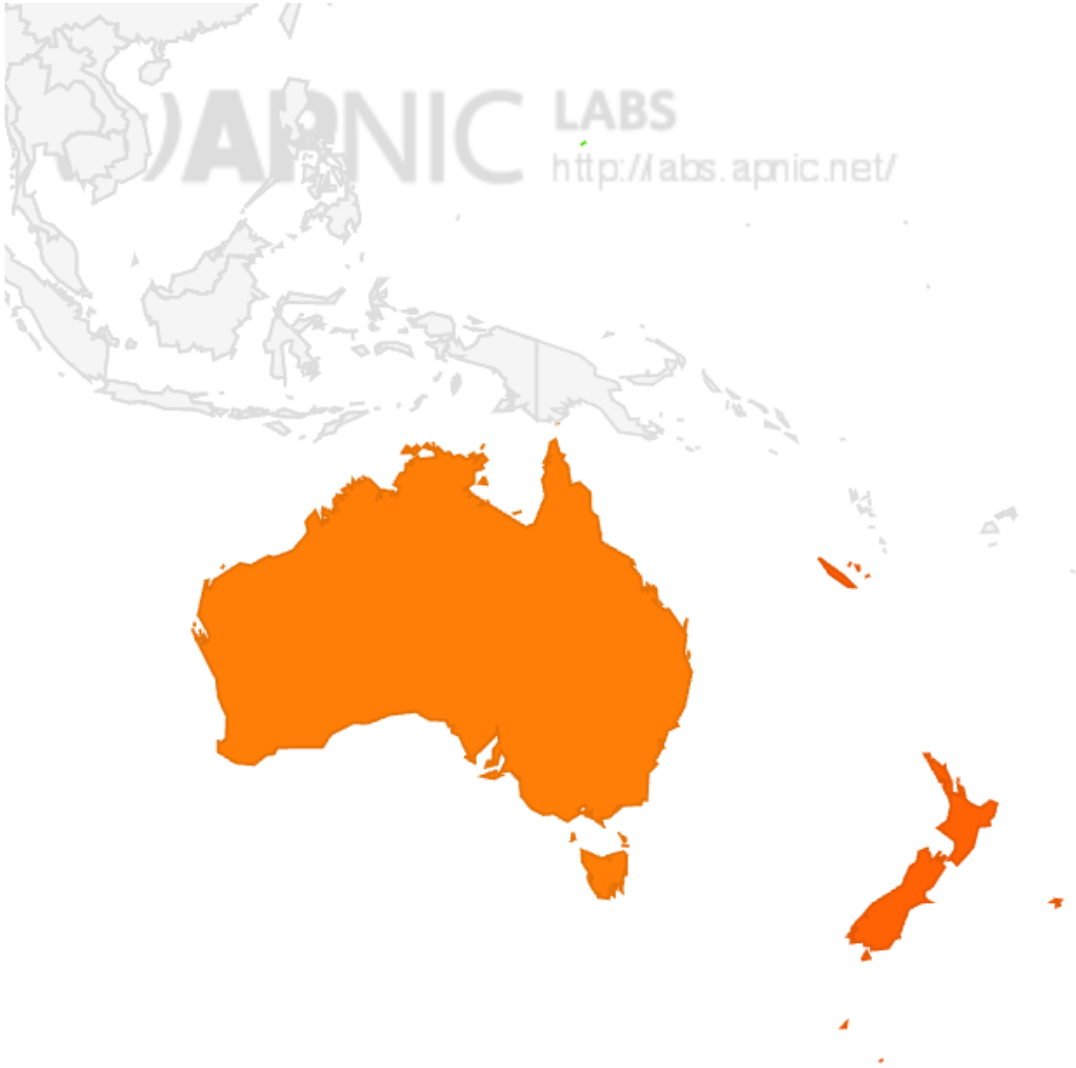
Encrypted DNS – Oceania (1)

Cloudflare Open Recursive Resolver DNS Query Profile for Oceania (XF)



https://stats.labs.apnic.net/edns/XF

Encrypted DNS – Oceania (2)



Code	Region	DoH Queries	DoT Queries
PF	French Polynesia, Polynesia, Oceania	29.27%	6.62%
GU	Guam, Micronesia, Oceania	25.80%	5.74%
AU	Australia, Australia and New Zealand, Oceania	6.87%	2.33%
NC	New Caledonia, Melanesia, Oceania	4.45%	2.39%
NZ	New Zealand, Australia and New Zealand, Oceania	4.35%	2.80%

DNS Best Practices & Guidelines

DNS Best Practices

- Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS)

- Implementation guidelines https://kindns.org/guidelines/

Good read: KINDNS initiative to improve mutual understanding and security of DNS among operators

KINDNS – Best Practices (1)

Top-Level Domain (TLD) and Critical Zones

- Sign authoritative zones with DNSSEC
- Restrict/limit access to zone transfers
- Maintain zone file integrity
- Separate recursive and authoritative DNS servers
- Setup redundant DNS servers (with diverse operational & geographical practices)
- Maintain diversity in the authoritative operations to promote resilience
- Setup monitoring for the DNS service, server and network

Ref: https://kindns.org/critical-zones/

KINDNS – Best Practices (2)

Second-Level Domain (SLD) Zones

- Sign authoritative zones with DNSSEC
- Restrict/limit access to zone transfers
- Maintain zone file integrity
- Separate recursive and authoritative DNS servers
- Setup redundant DNS servers (with diverse operational & geographical practices)
- Setup monitoring for the DNS service, server and network

Ref: https://kindns.org/other-sld-zones/

KINDNS – Best Practices (3)

[Public|Private] Resolvers

- (Restrict access to resolvers whenever possible)
- Enable DNSSEC validation
- Enable QNAME minimization
- Enable and offer DoH and DoT on top of Do53 to clients
- Separate recursive and authoritative DNS servers
- Passive logging must be retained only as necessary
- Setup redundant DNS servers (with diverse operational & geographical practices)
- Setup monitoring for the DNS service, server and network

Ref: https://kindns.org/public-resolvers/

KINDNS – Best Practices (4)

Hardening the server

- Apply ACLs to restrict network traffic to your DNS
- Implement BCP38/MANRS egress filtering
- Configuration of each DNS
- Limit user permissions and application access to system
- Use configuration management and versioning
- Restrict access to management services
- Use crypto to secure access to system

Ref: https://kindns.org/platform-hardening/

DNSSEC Best Practices

- ICANN DNSSEC Guidebook for ccTLDs
  - https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

- APNIC DNSSEC Policy and Practice Statement (DPS)
  - https://www.apnic.net/wp-content/uploads/2016/11/DNSSEC_DPS_210616v1.pdf

Thank You!

- Any questions?