RIPE 85

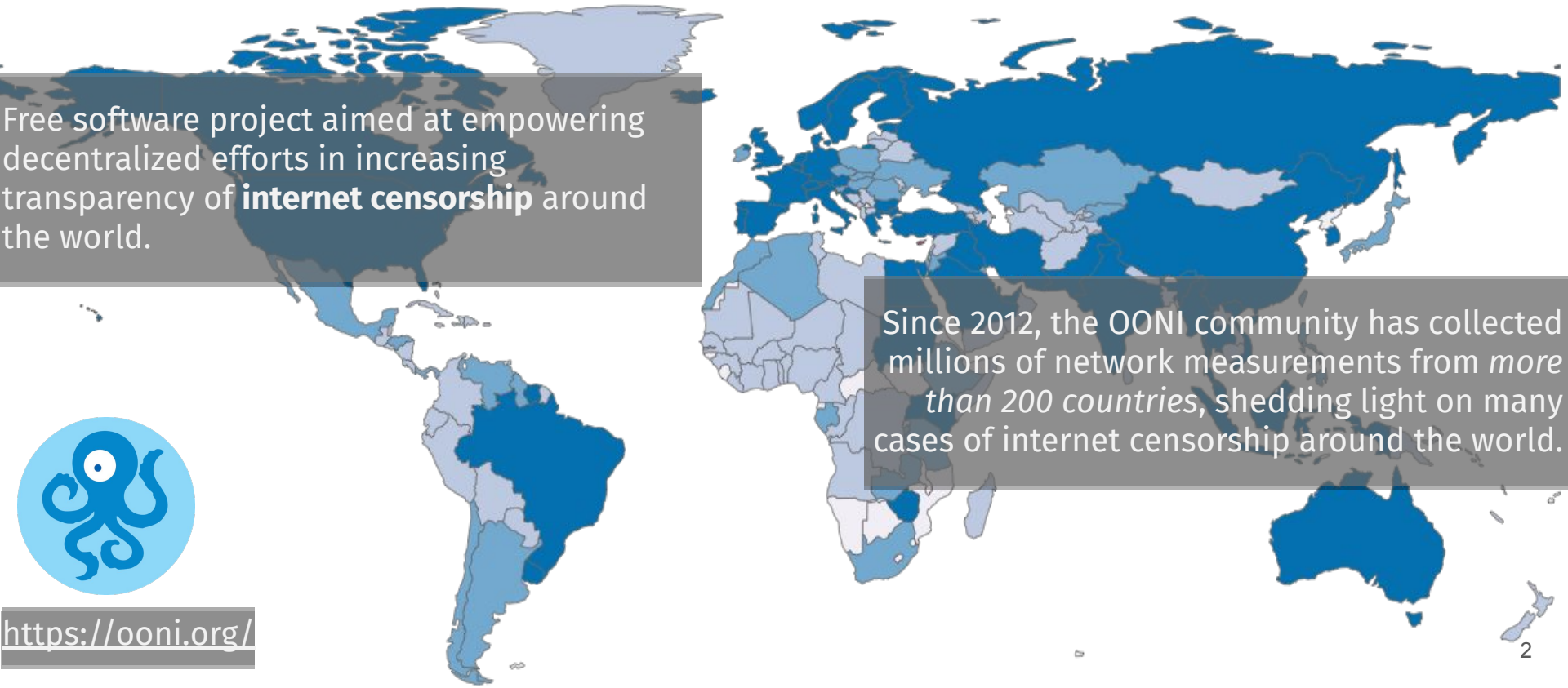
Measuring Encrypted-DNS Censorship Using OONI Probe

Arturo Filastò (OONI)

OONI

27 October 2022

OONI: Open Observatory of Network Interference

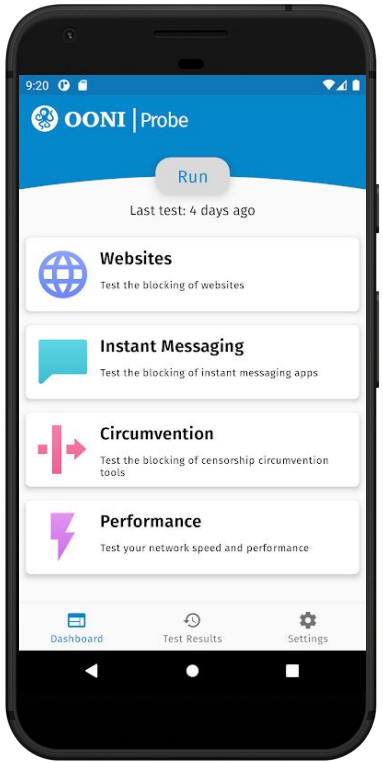


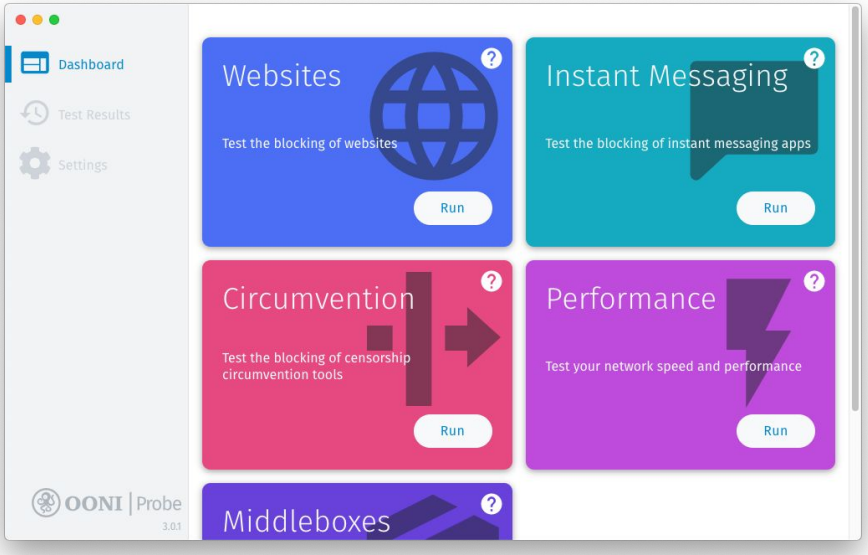
Free software project aimed at empowering decentralized efforts in increasing transparency of **internet censorship** around the world.

Since 2012, the OONI community has collected millions of network measurements from *more than 200 countries*, shedding light on many cases of internet censorship around the world.

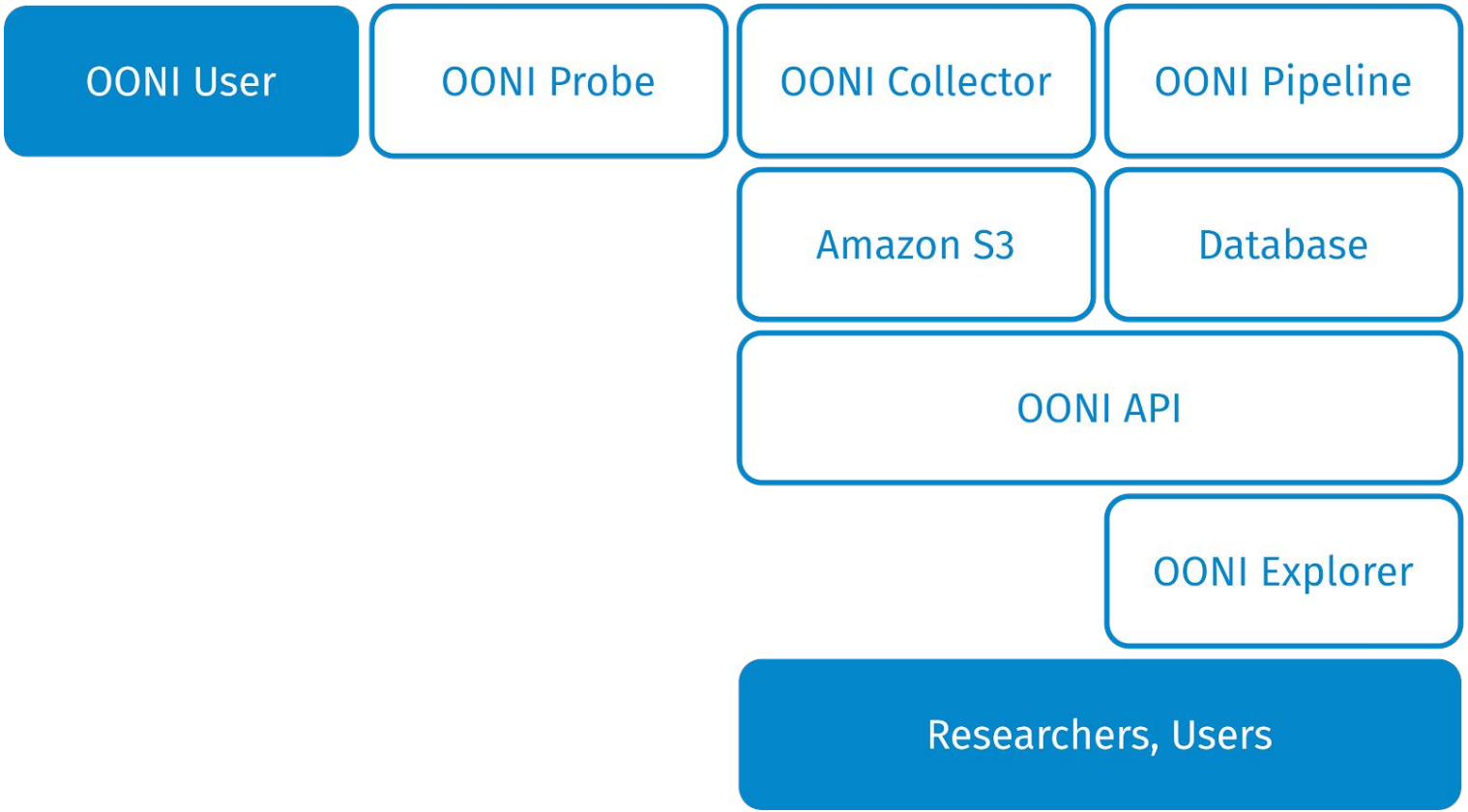
https://ooni.org/

OONI Probe (https://ooni.org/install)

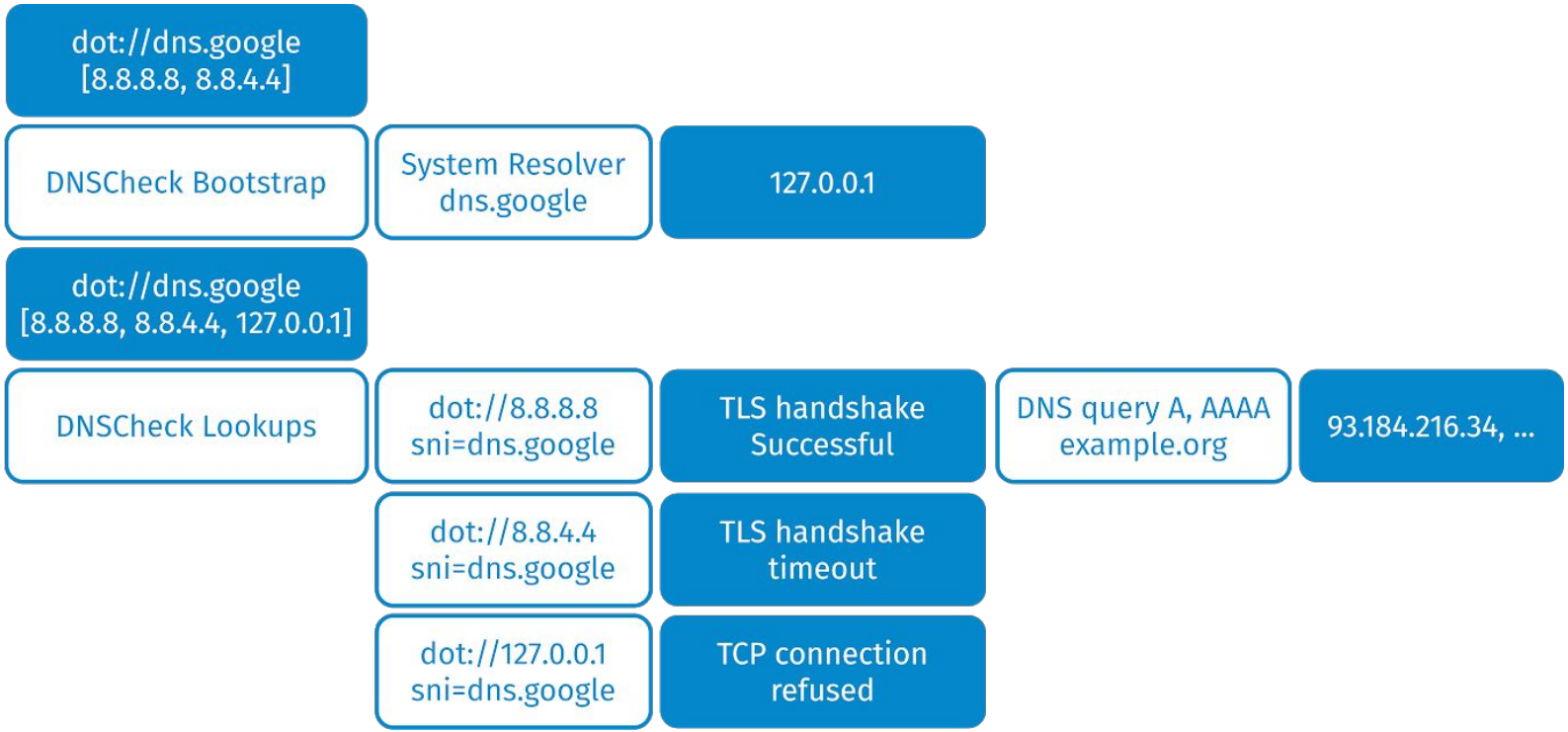




Value Chain of a OONI Measurement



The DNSCheck Experiment



Measurements campaign

- From 15th December 2020 to 10th January 2021
- 123 DoT/DoH services (=> 461 TCP/QUIC endpoints)
- The paper and this presentation focus on DoH over TCP only
- We used an experimental CLI client (miniooni)

Country	ASN	Type
Kazakhstan	AS48716	VPS
Iran	AS197207	Mobile
China	AS45090	VPS

Main Findings

- bootstrap: dns.adguard.com resolved to 10.10.34.36 in the IR ISP
- lookups: most endpoints fail or succeed consistently
- 1.1.1.1:853 and 1.0.0.1:853 were blocked and unblocked frequently in KZ
- Same for 1.1.1.1:853 in IR
- dot://dot-jp.blahdns.com was unblocked in CN around 1st January 2021

	Kazakhstan	**Iran**	**China**
Successful DoT lookups	8157 (95%)	1156 (50%)	4332 (93%)
Successful DoH lookups	16466 (82%)	4824 (92%)	9414 (89%)

Distribution of Lookups Failures (DoT vs DoH)

Failure	Kazakhstan		Iran		China	
	DoT	DoH	DoT	DoH	DoT	DoH
Timeout after the TLS handshake	323 (72%)	2701 (77%)	79 (7%)	160 (41%)	2 (~0%)	3 (~0%)
TLS handshake timeout	88 (20%)	331 (9%)	906 (80%)	1 (~0%)	63 (20%)	61 (5%)
Connect timeout	1 (~0%)	397 (11%)	72 (6%)	72 (19%)	233 (75%)	813 (72%)
RST during TLS handshake	1 (~0%)	1 (~0%)	74 (7%)	77 (20%)	0 (0%)	152 (14%)
Other	33 (8%)	92 (3%)	3 (~0%)	79 (20%)	13 (~5%)	93 (9%)

Example: SNI-based Blocking (Kazakhstan; DoH)

Address	SNI	Result	Frequency
2606:4700::6810:f8f9	cloudflare-dns.com	Timeout after the TLS handshake	85 (99%)
2606:4700::6810:f8f9	cloudflare-dns.com	Connect timeout	1 (1%)
2606:4700::6810:f8f9	mozilla.cloudflare-dns.com	Success	88 (100%)

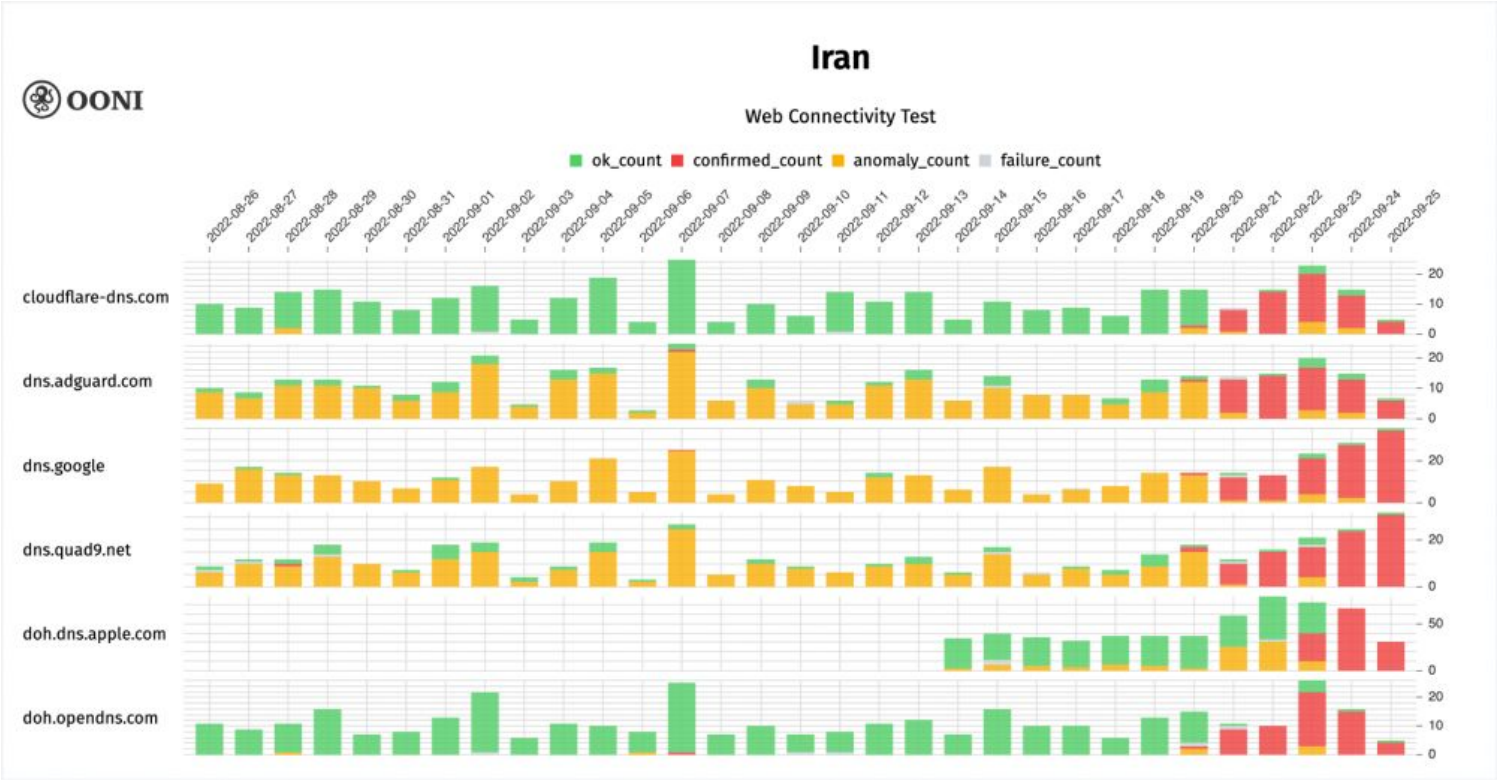
Example: Endpoint-based Blocking (Iran; DoT)

Address	SNI	Result	Frequency
8.8.4.4	8888.google	TLS handshake timeout	40 (100%)
8.8.4.4	null	TLS handshake timeout	40 (100%)
8.8.8.8	8888.google	Success (TLSv1.3)	40 (100%)

TCP-based Blocking (China; DoT)

Address	SNI	Result	Frequency
1.1.1.1	1dot1dot1dot1.cloud...	Connect timeout	77 (100%)
1.1.1.1	one.one.one.one	Connect timeout	77 (100%)
1.1.1.1	null	Connect timeout	76 (100%)

Blocking of DoH in Iran



Blocking of DoH in Iran

- DoH endpoints that were previously accessible started being blocked
- DoH endpoints that previously were just “anomalies”, now began to be “confirmed” as a result of DNS based blocking
- tl;dr there is a noticeable change in how blocking of encrypted DNS is implemented in Iran starting from the 20th of September onwards

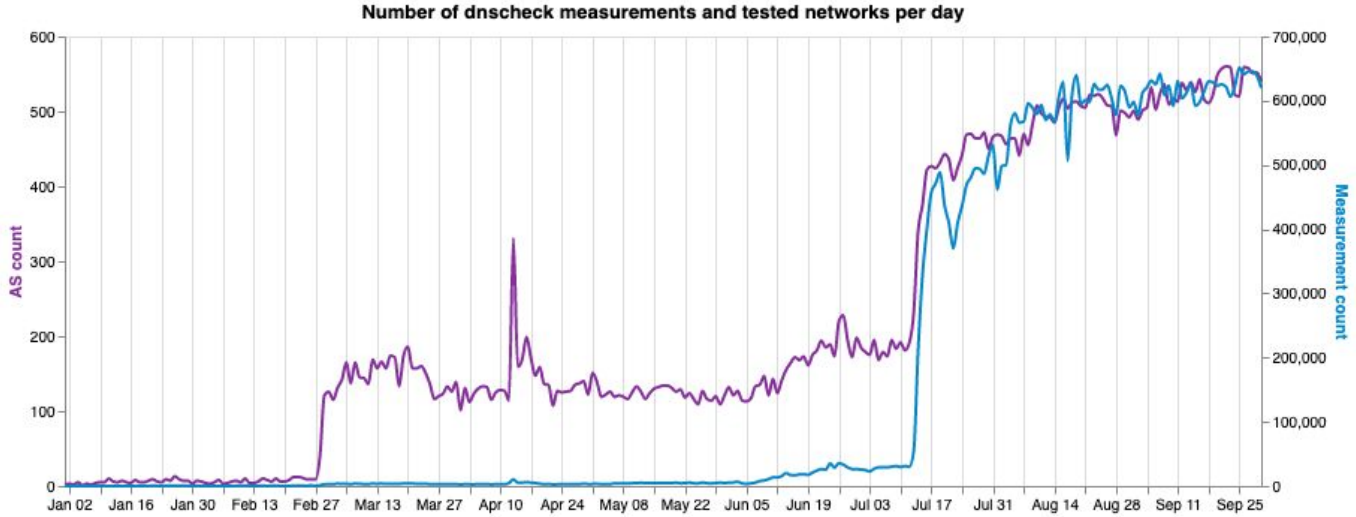
ASN	AS name	#dns	#tcpip	#tls	#success	count
197207	MCI	yes		yes		1
197207	MCI	yes		yes	yes	1
206065	Zi-Tel	yes	yes	yes		12
206065	Zi-Tel	yes		yes		18
44244	Irancell	yes	yes	yes		4
58224	TCI	yes			yes	1
58224	TCI	yes	yes		yes	1
58224	TCI	yes	yes	yes		1
58224	TCI	yes	yes	yes	yes	5
58224	TCI	yes		yes		1
58224	TCI	yes		yes	yes	21

Table: Failures and successes for `doh.dns.apple.com` using experimental Web Connectivity.

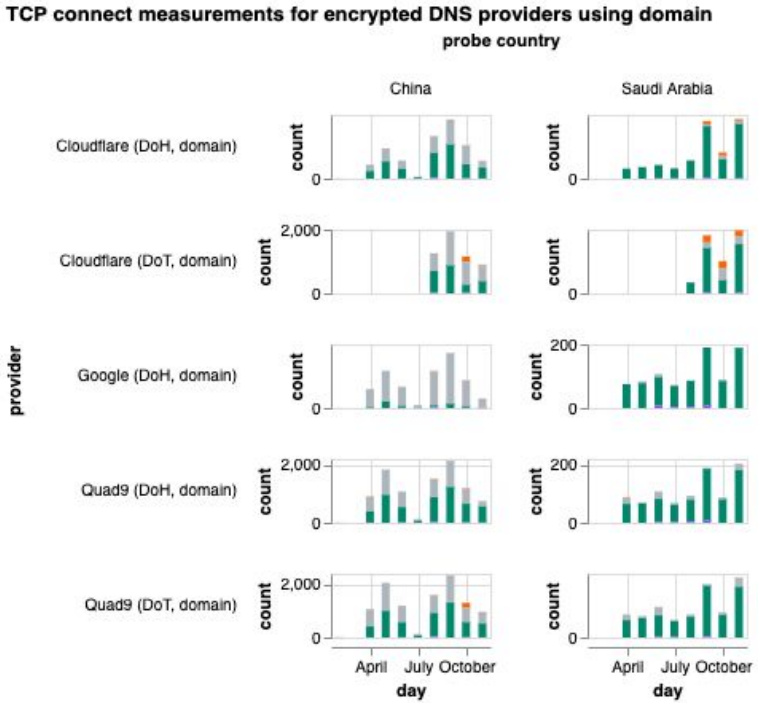
DNS Check is now in OONI Probe!

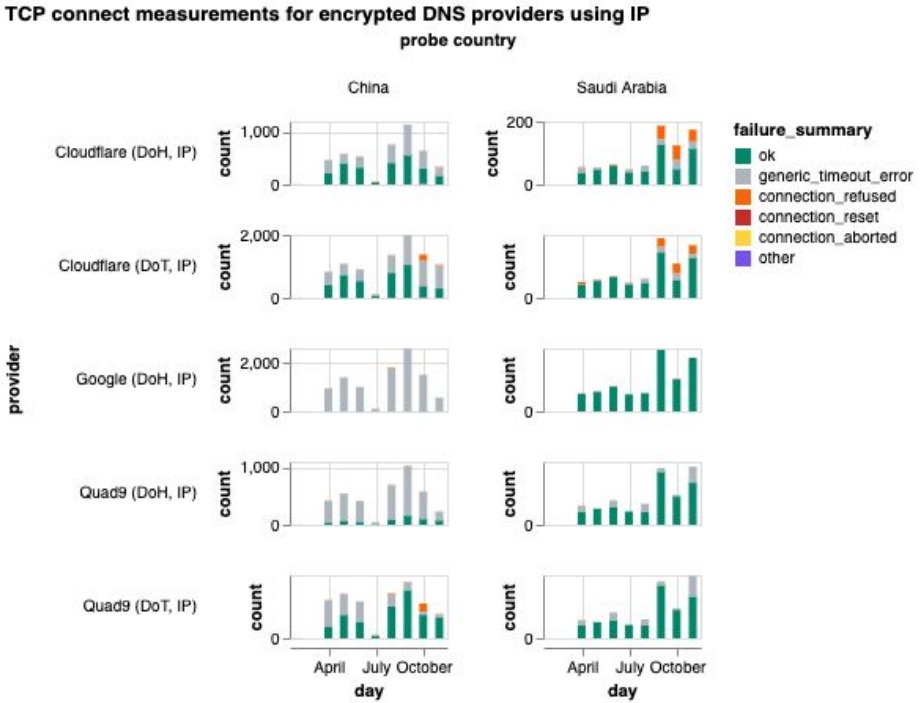
As of October 2022

- 189 countries
- 4593 ASs
- 45M measurements

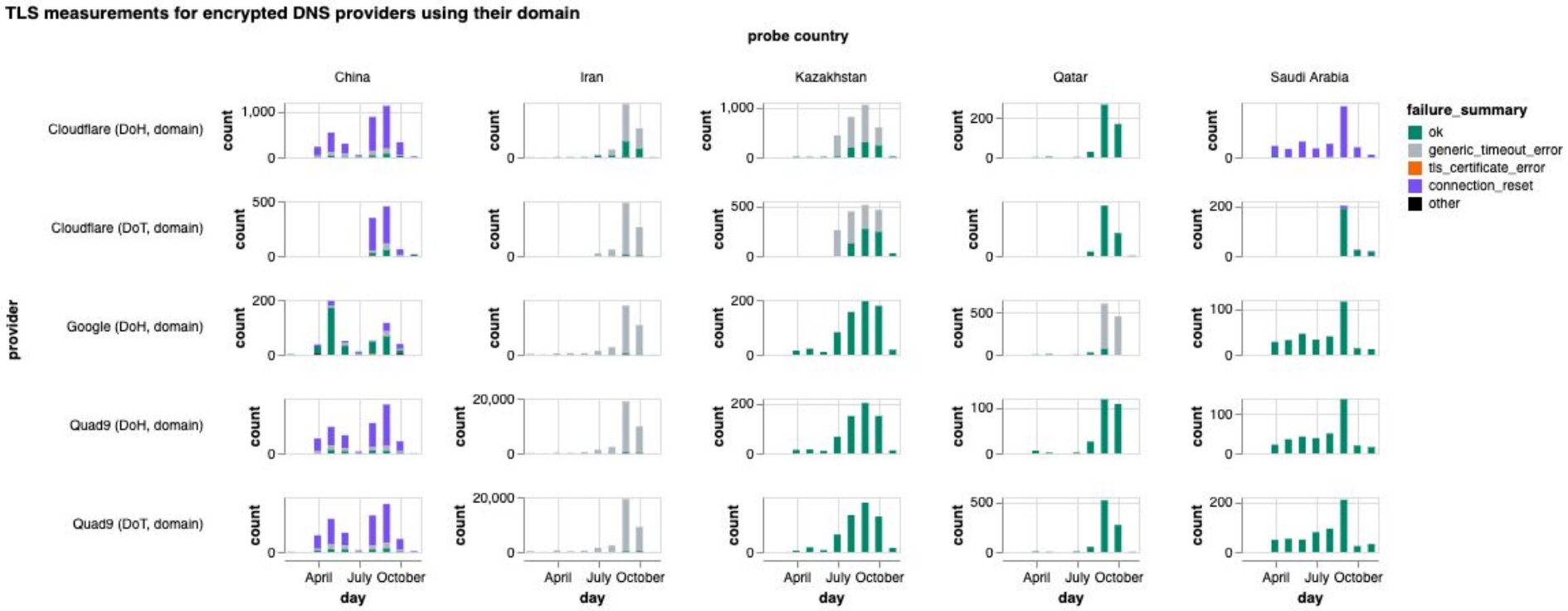


TCP Connect measurements





TLS measurements



Ongoing and Future Work

- “Parrot” the fingerprint of popular TLS implementations
- Study DoH over QUIC and DNS over QUIC blocking
- Make dnscheck more resilient to bootstrap failures
- More in-depth analysis of global OONI data
- Experiment with cloudflare/go to use Encrypted Client Hello

Thank you!

contact@openobservatory.org

https://slack.ooni.org/

@OpenObservatory

https://github.com/ooni