Handling DNS Abuse and Securing DNS

SANOG36

Champika Wijayatunga

January 2021

DNS Security: Understanding Threats and Abuses

- Large attack surface due to the complexity of the DNS ecosystem
- Query/Response data integrity
  - As originally defined in the protocol, no protection against data corruption
- Query/Response confidentiality
  - As originally defined in the protocol, all data is in clear text (Attacker can see connection meta data)
- Namespace risks
  - Homoglyphs e.g. **example.com** vs **examplé.com** (xn--exampl-gva.com)
  - Typosquatting e.g. **example.com** vs **exmaple.com**

DNS Security: Understanding Threats and Abuses

- Redirection
  - Change domain's name servers to point to attacker-controlled authoritative servers
- Resolver Hijacking
  - Cause DNS queries to be answered by attacker-controlled resolver
- Denial of Service
  - Overload victim traffic and services
- Impact of Hierarchical name space
  - Compromise of higher layers means potential compromise of that layer and all lower layers

DNS Security: Understanding Threats and Abuses

- Registrant Compromise
  - Allow attacker to pose as registrant and change domain data
- Registrar Compromise
  - Attacker breaks into registrar system and change customer data
- Registry Compromise
  - Attacker can modify any domain data administered by the registry
- DNS Software vulnerabilities

ICANN DNS Abuse Handling Initiatives

The Domain Abuse Activity Reporting System

What is it?

- A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of reputation feeds (e.g., blocklists)
- Accommodates historical studies
- Studies multiple threats: phishing, botnet, malware, spam
- Takes a scientific approach: transparent, reproducible

https://www.icann.org/octo-ssr/daar

DAAR Sample Report (Oct. 2020)

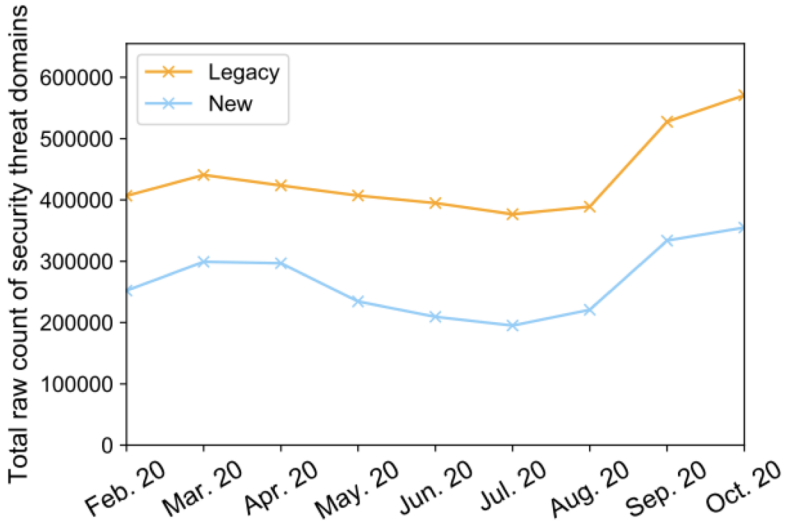


Figure 6: Total number of domains identified as security threats over time

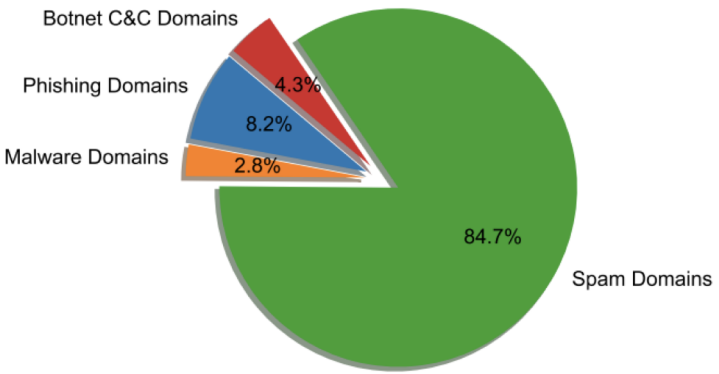


Figure 7: Breakdown of domains identified as security threats across all DAAR threat types

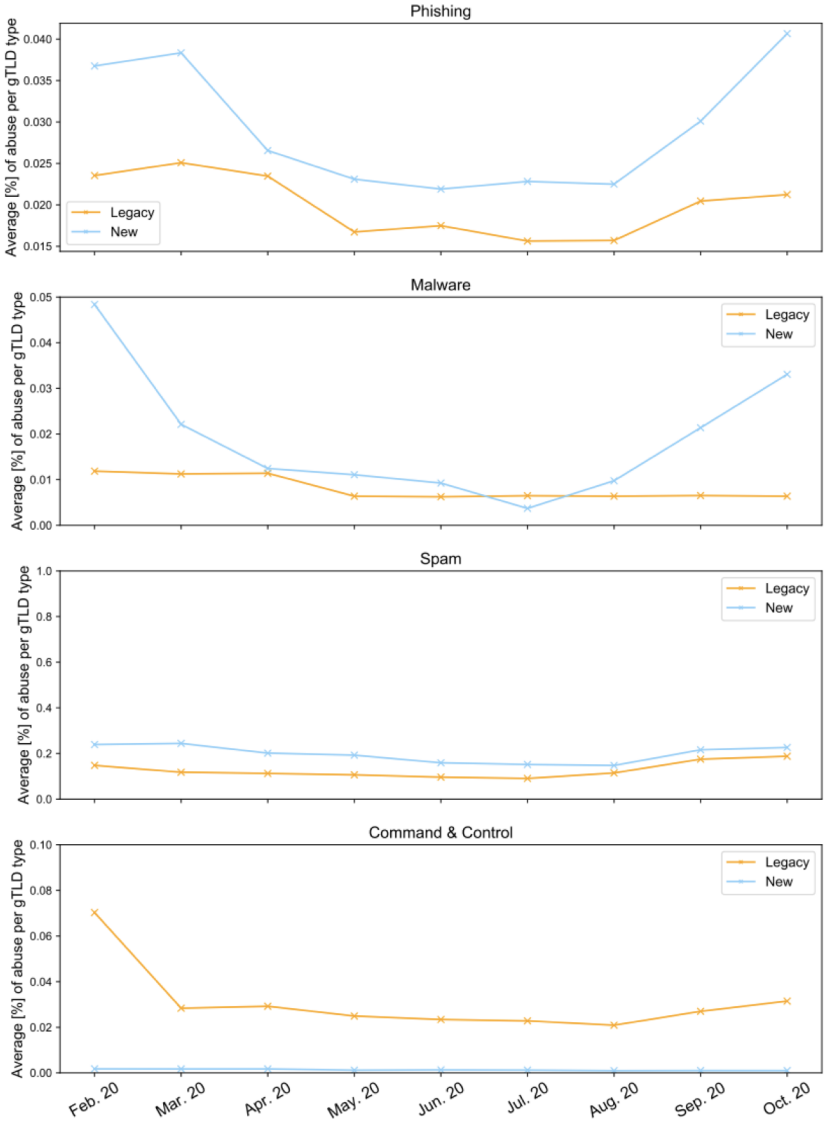
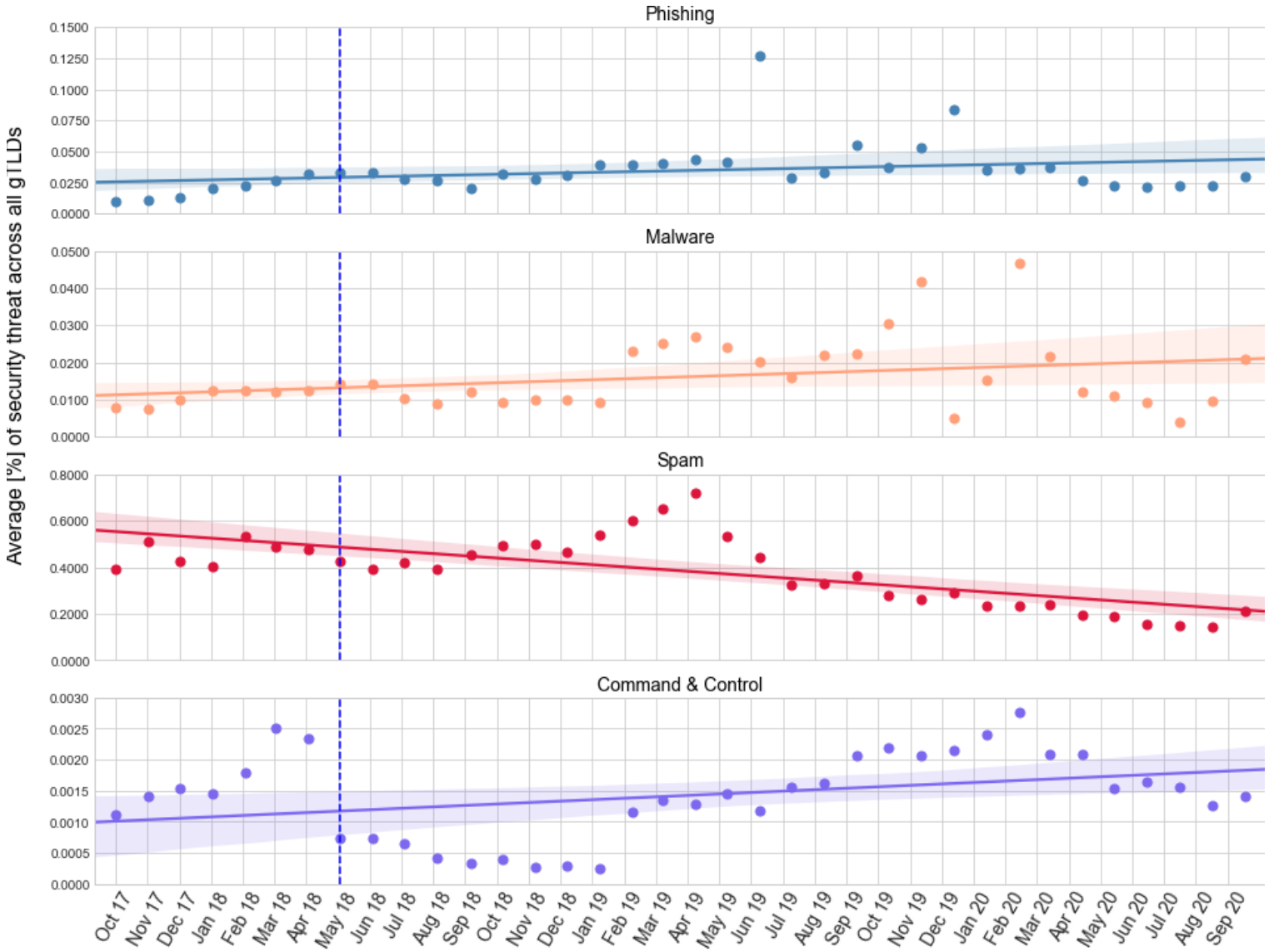


Figure 14: Average percentage of abuse in gTLDs across different threat types over time

Individual Security Threats Oct 2017 to Sep 2020



ITHI: Identifier Technologies Health Indicators

- **ITHI**, or **I**dentifier **T**echnologies **H**ealth **I**ndicators is an ICANN initiative to "**measure**" the "**health**" of the "**identifier system**" that "**ICANN helps coordinate**".
- The goal is to produce a set of **indicators** that will be **measured and tracked over time** that will help determine if the system of identifiers is overall doing better or worse.
- ISPs; universities and other operators running DNS recursive resolvers can participate)
- https://ithi.research.icann.org

Some ITHI Results

	Indicator		July 2020	Past 3 months	Historic Low	Historic High
Root Server DGA	% of DGA queries seen by root servers		**44%**	40%	35%	49%
DNSSEC	% of resolvers that perform DNSSEC validation		**32%**	32%	23%	34%
Resolver Concentration	Number of resolvers seeing 50% of first queries		**212**	217	206	240
	Number of resolvers seeing 90% of first queries		**2149**	2133	2036	2231
Name collision	%requests to top 3 names at the root	**.LOCAL**	**4.4%**	4.6%	2.4%	5.1%
		.HOME	**3.0%**	3.1%	2.5%	3.7%
		.LAN	**1.0%**	1.2%	0.5%	1.3%
	%requests to top 3 names at resolvers	.LOCALDOMAIN	**0.2%**	0.0%	0.00%	0.1%
		.LOCAL	**0.0%**	0.0%	0.0%	0.1%
		.WORKGROUP	**0.0%**	0.0%	0.0%	0.1%

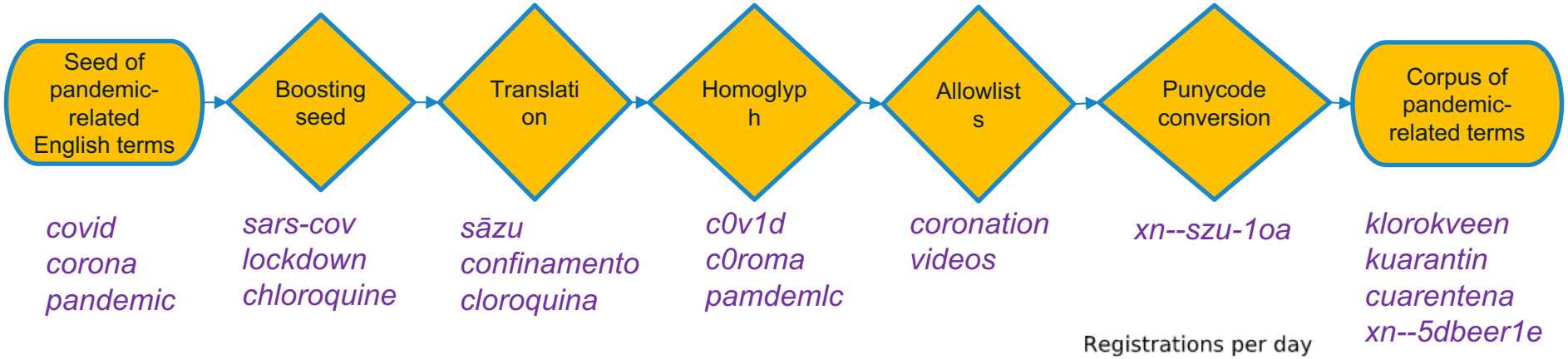
ICANN Community Work

- Domain Name Security Facilitation Initiative (DSFI) technical study group
- Outside ICANN the contracted parties (Registries & Registrars) have their project on the DNS Abuse Framework:
  - http://dnsabuseframework.org/

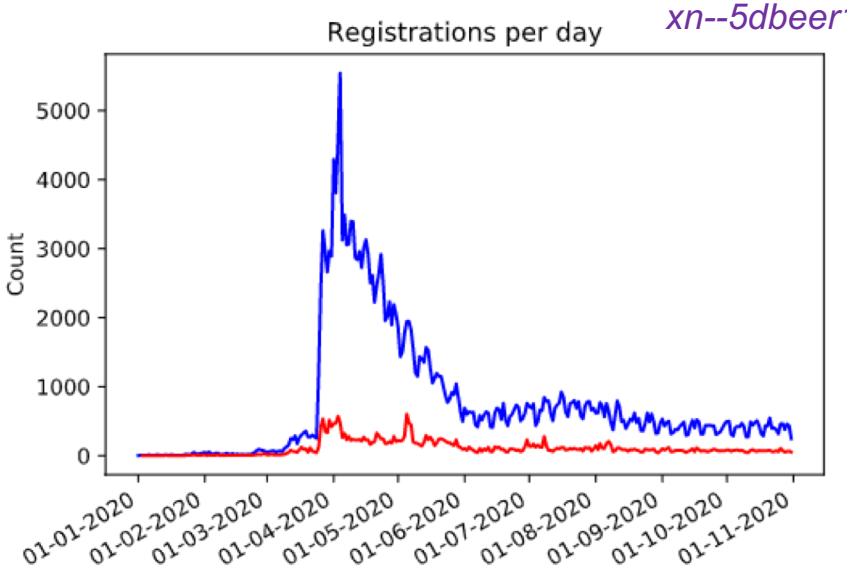
DNS Abuse during Covid-19

Methodology to Identifying Suspect Domains

- Searching for zone files (gTLD and some ccTLD) of keywords related to the Covid-19 pandemic.

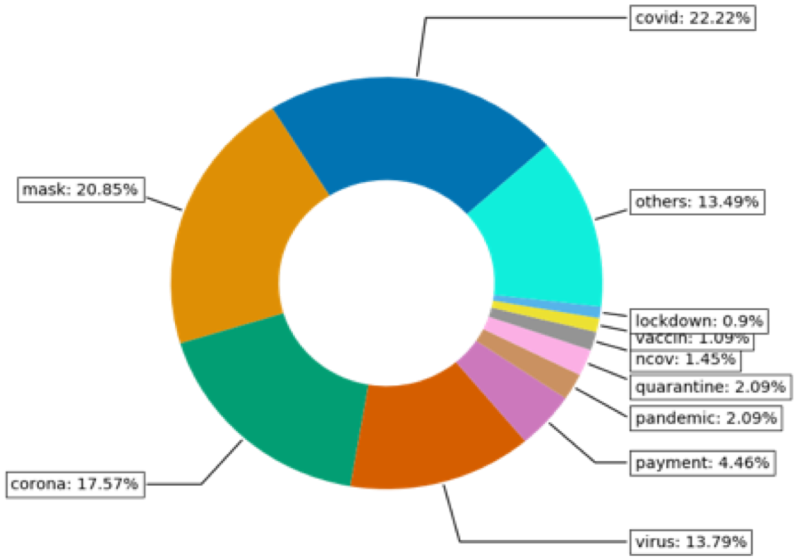


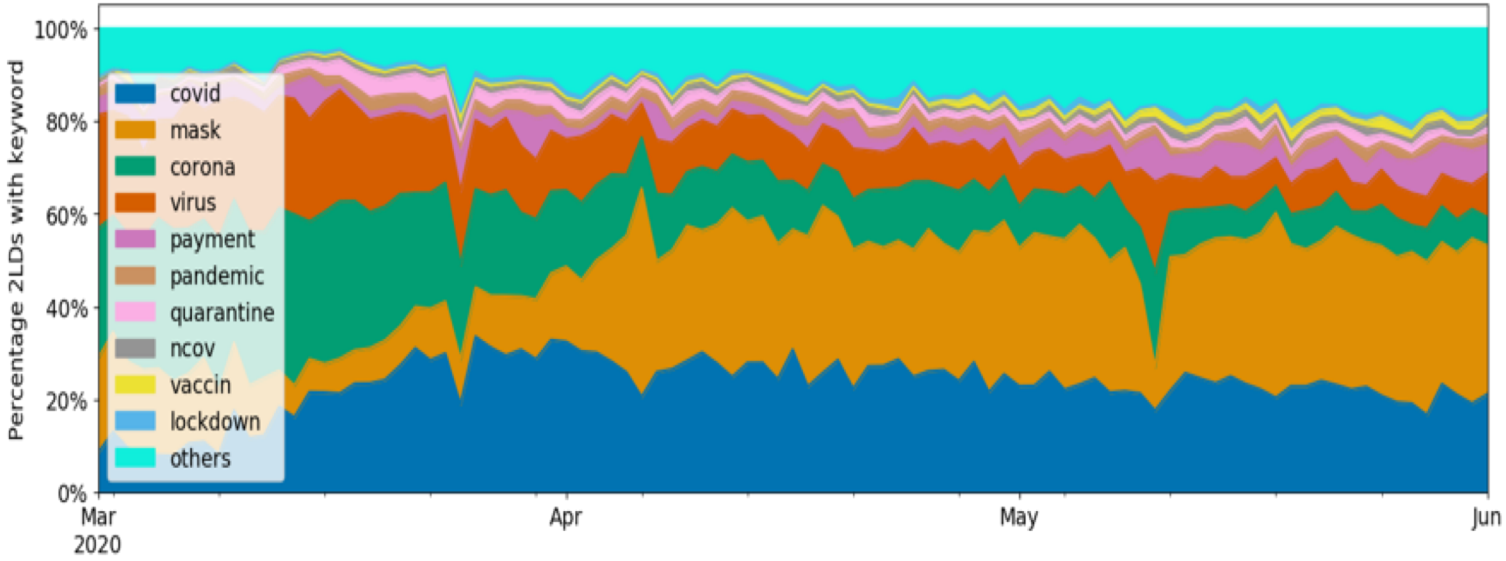
- Jan-Nov 2020: 248,718 domains Identified (blue line)
- May-Nov 2020: 9,194 of 147,529 found to have some evidence of misuse (red line)
- Of those, 2,573 had “high confidence” reports



Breakdown of Keyword Identified Domains

- 60% of domains related to 4 keywords
  Top 4 keywords: **covid, mask, corona and virus**

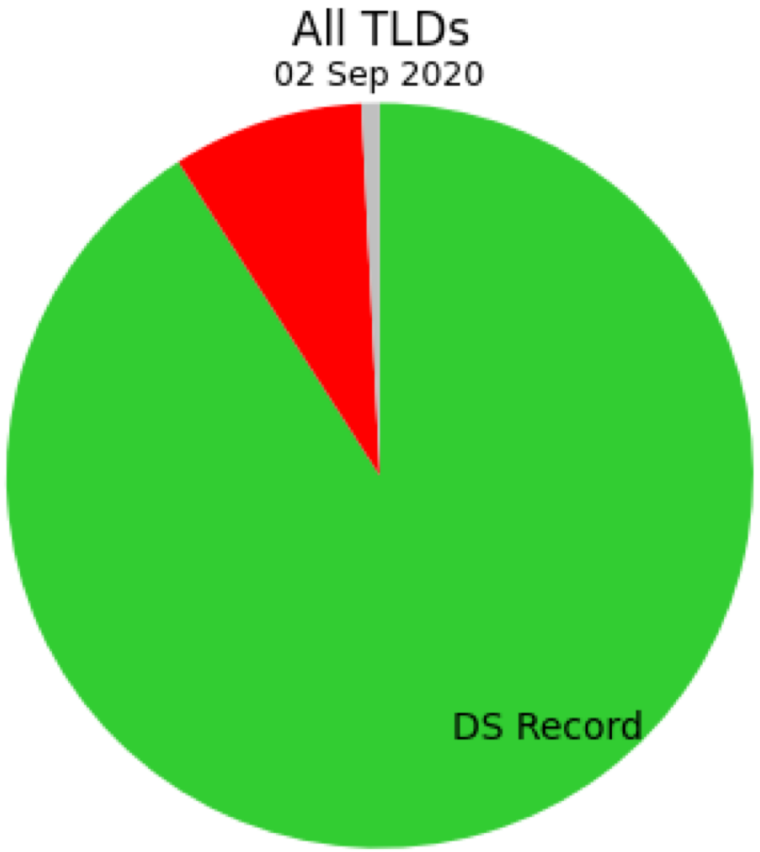




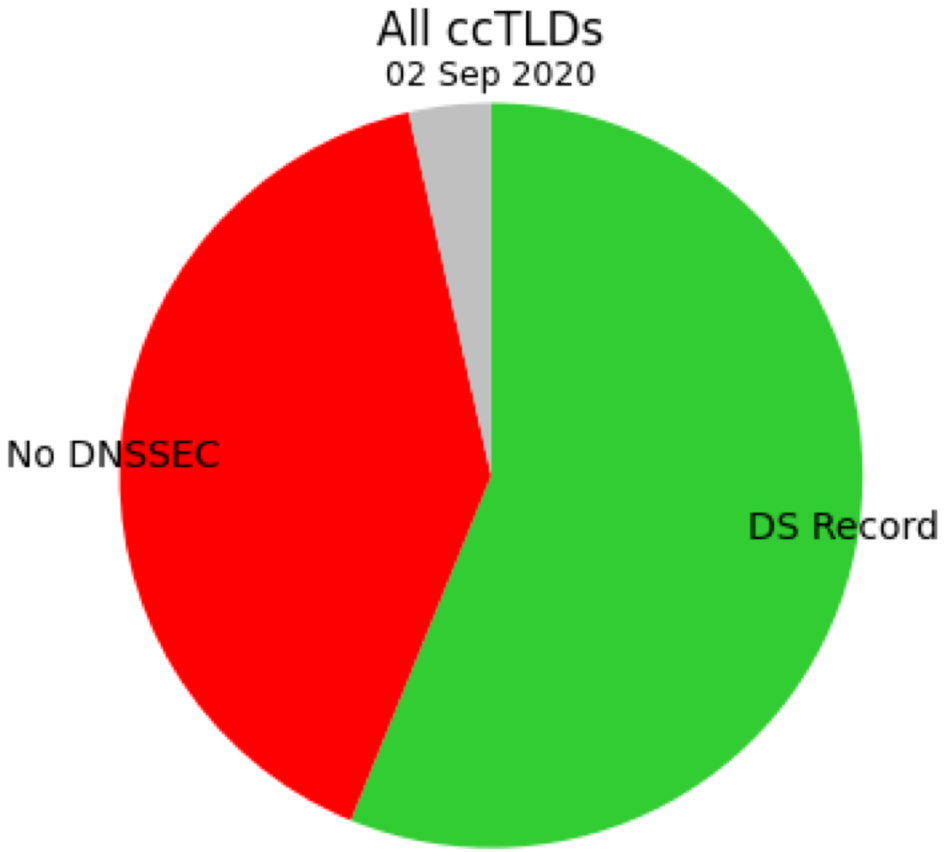
Language	%Domains
English	94,21%
German	2,13%
French	1,26%
Spanish	0,71%
Dutch	0,68%
Turkish	0,59%
Italian	0,14%
Hindi	0,11%
Malay	0,08%
Japanese	0,04%
Portuguese	0,02%
Chinese	0,02%

Consider deploying DNSSEC!

All TLDs vs. ccTLDs

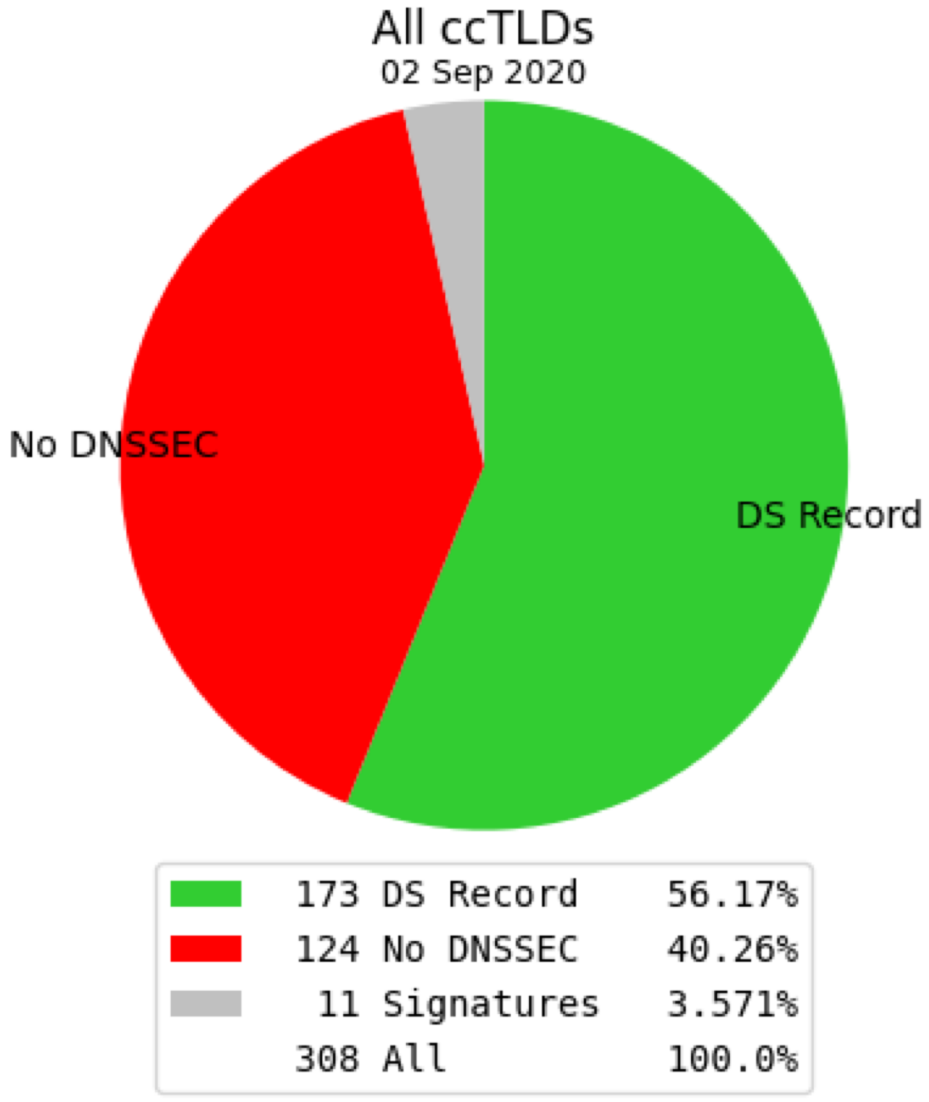


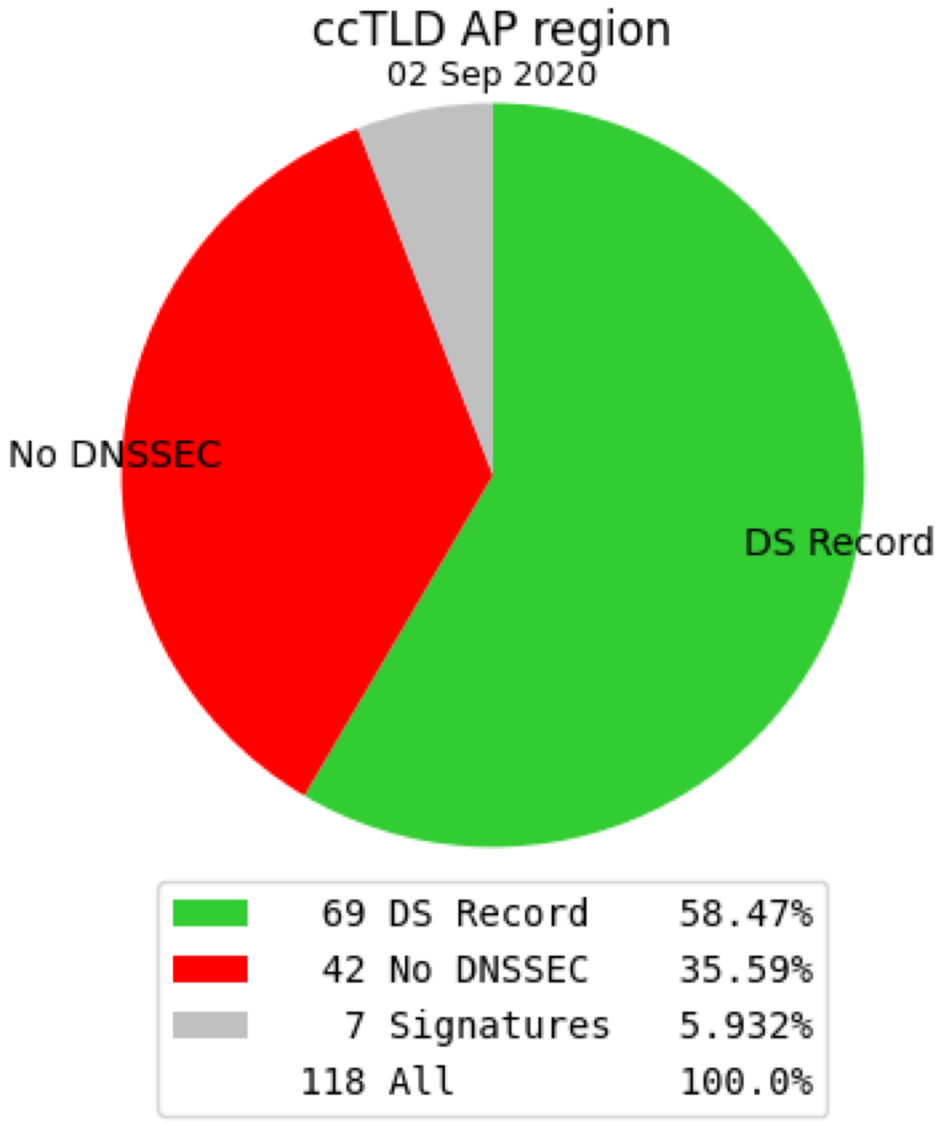
1373	DS Record	90.93%
125	No DNSSEC	8.278%
12	Signatures	0.7947%
1510	All	100.0%



173	DS Record	56.17%
124	No DNSSEC	40.26%
11	Signatures	3.571%
308	All	100.0%

All ccTLDs vs. Asia Pacific ccTLDs





Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann