



European ccTLDs and COVID-19

European response

Peter Van Roste

peter@centr.org

Everywhere

4th June 2020





COVID-19 impact on DNS

- Overall readiness of ccTLDs to deal with the lockdown
- The resilience of DNS infrastructure
- Registrations facilitating abuse/crime
- Upward trend in registrations

Information in this presentation is based on a CENTR survey from April 2020 with 20 respondents unless otherwise indicated.



Overall readiness of ccTLDs



The DNS is a decentralised system that is built to withstand heavy workloads, and its underlying technical components have been refined and optimised for almost half a century.



Traffic increase is not outside the current capacity of the ccTLD infrastructure.



ccTLDs have deployed anycast networks networks that offer an additional level of protection against attacks or high levels of DNS queries. (see also LACTLD stats!)



The resilience of infrastructure

Due to increased teleworking, streaming, and general reliance on digital infrastructure during COVID-19 pandemic the overall internet usage increased but impact on ccTLDs is softened and infrastructure handled this well.

Caching

- DNS relies on a caching system and this means that the load on the ccTLD servers does not increase proportionally to the increased traffic from end-user side

DDoS

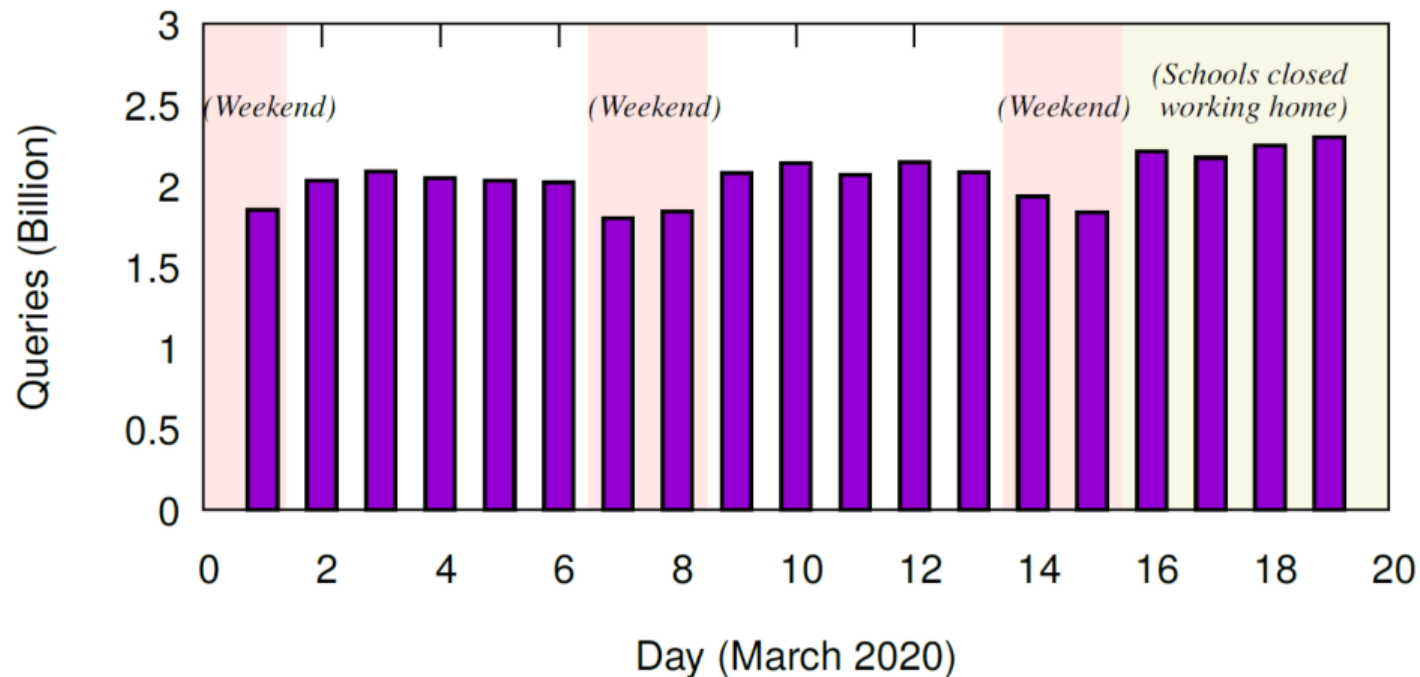
- DNS has more than 20 years of experience in dealing with DDoS attacks. These attacks typically generate demand levels that are many times higher than the number of queries during lockdown

Query stats

- ccTLDs publish query statistics which illustrate increase of traffic to DNS servers no higher than 25% percent



4% Rise in .nl domain name lookups when schools closed

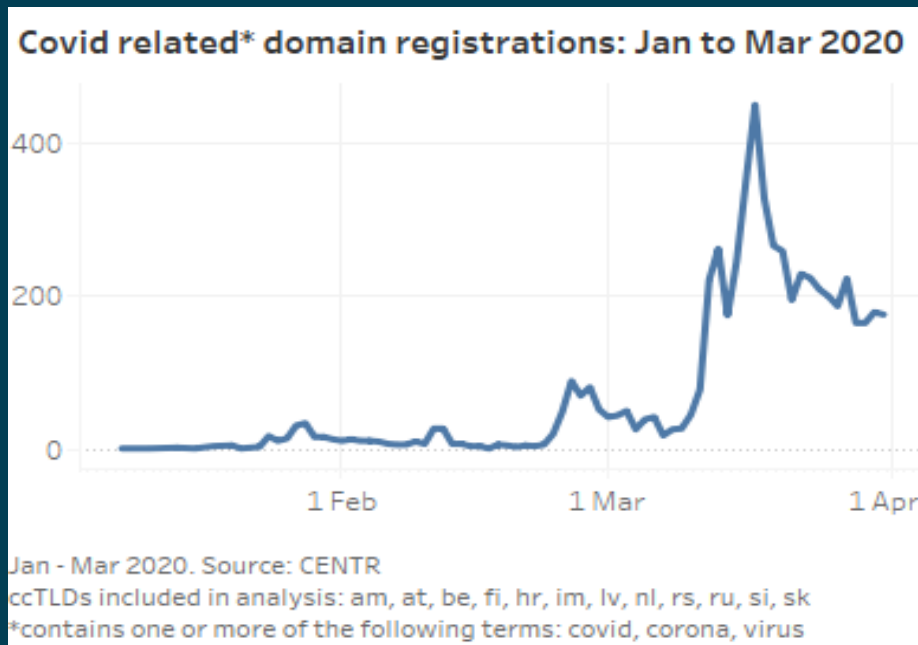


Source: [Coronavirus and the DNS: view from the .nl ccTLD](#)



Abusive registrations


CENTR survey shows that 80% of the respondents are scanning the newly-registered domains for terms such as covid, corona or virus. Roughly half of this 80% verifies the registration data of COVID-19 related domains more closely than with other newly-registered domains as a response to the pandemic, and filters out the ones with bad registrant data. The reported number of **actual criminal activity** associated with these domain names **is low**.



The chart shows the **overall increase** in COVID-19 related domain name registrations from Jan to Mar 2020. In the same period 750,000 names were registered by these ccTLDs.

The **actual abuse cases are marginally low**, as reported by our Members.





Measures to keep abuse numbers low

Closely monitoring new registrations

Manual or automated checks for COVID-19 related terms (daily)

Data verification checks

'bad whois procedure'; additional time for RANT to verify their identity and provide further documentation

Cooperation with authorities

e.g. Lists of registered domain names are shared with CERTs, law enforcement authorities for further investigation.



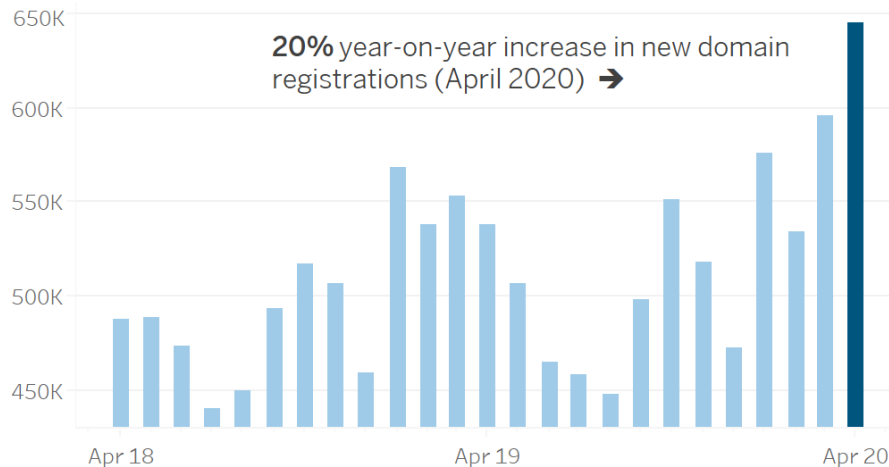
ccTLDs post-corona?

Figures from CENTR show a spike in new registrations in the month of April 2020



New domain creations

Sample: 25 ccTLDs (CENTR full members)



Source: CENTR.

- Based on a sample of 25 ccTLDs, the number of new domains registered in April 2020 is up 20% from the same time a year earlier.
- Figures show that this increase is not covid-19 related
- The boost in new domains links to the changing business and employment landscape




If you want us to keep you posted:

Subscribe to all **CENTR newsletters**: visit centr.org

Subscribe to our newsletter

<input type="text" value="First name"/>	<input type="text" value="Last name"/>
<input type="text" value="Organisation"/>	<input type="text" value="Email"/>

I'm not a robot  [reCAPTCHA](#)
[Privacy](#) • [Terms](#)

SUBMIT →





Thank You

peter@centr.org

