

# Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic

**Matt Larson**

Vice President of Research, Office of the CTO

eco webinar

30 April 2020



# ICANN Managed Root Server (IMRS) traffic analysis

---

- ⦿ The ICANN org operates the ICANN Managed Root Server (IMRS)
  - Also known as *l.root-servers.net*
  - IPv4 address is 199.7.83.42, IPv6 address is 2001:500:9f::42
  - One of 13 root server identities
  - IMRS comprises 167 instances in 83 countries as of April 2020
- ⦿ The Research group in ICANN's Office of the CTO (OCTO) routinely analyzes IMRS traffic
- ⦿ Recent research question: *Have traffic patterns to the IMRS changed in light of recent events?*
- ⦿ Investigation is ongoing
- ⦿ Today's presentation describes initial findings

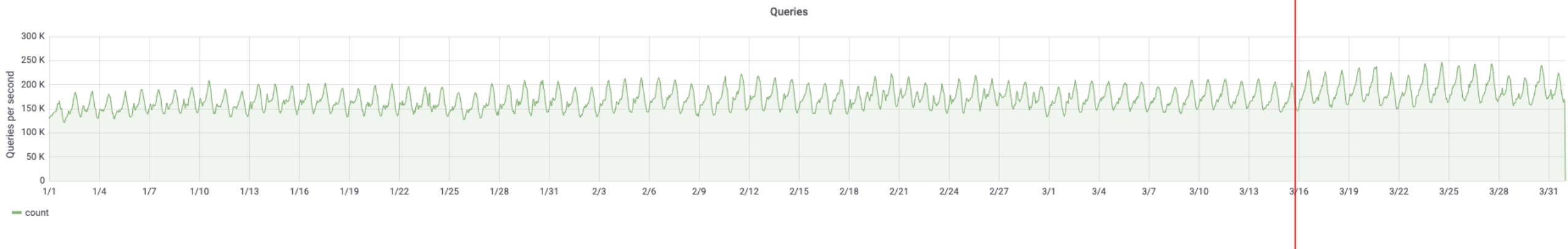
# Root servers in context

---

- ⦿ A user enters a domain name into an application running on an device such as a phone or laptop
- ⦿ The device needs to resolve the domain name into an IP address
- ⦿ The application constructs a DNS query and sends it to a recursive resolver
  - The recursive resolver could be run by the user's ISP, the user's employer, or someone else (e.g., a public recursive resolver)
- ⦿ The recursive resolver might already have the answer in its cache because it recently looked up the same domain name
- ⦿ If not, the recursive resolver finds the answer by sending DNS queries to different authoritative name servers
- ⦿ If the recursive resolver has no relevant information in its cache, it will start this resolution process by sending a DNS query to one of the root servers

# ICANN Managed Root Server (IMRS) traffic analysis

- ⦿ **Peak traffic to all IMRS instances combined has increased 20-25% starting in mid-March 2020**
- ⦿ The graph shows DNS queries per second to all IMRS instances worldwide from 1 January 2020 through 31 March 2020:

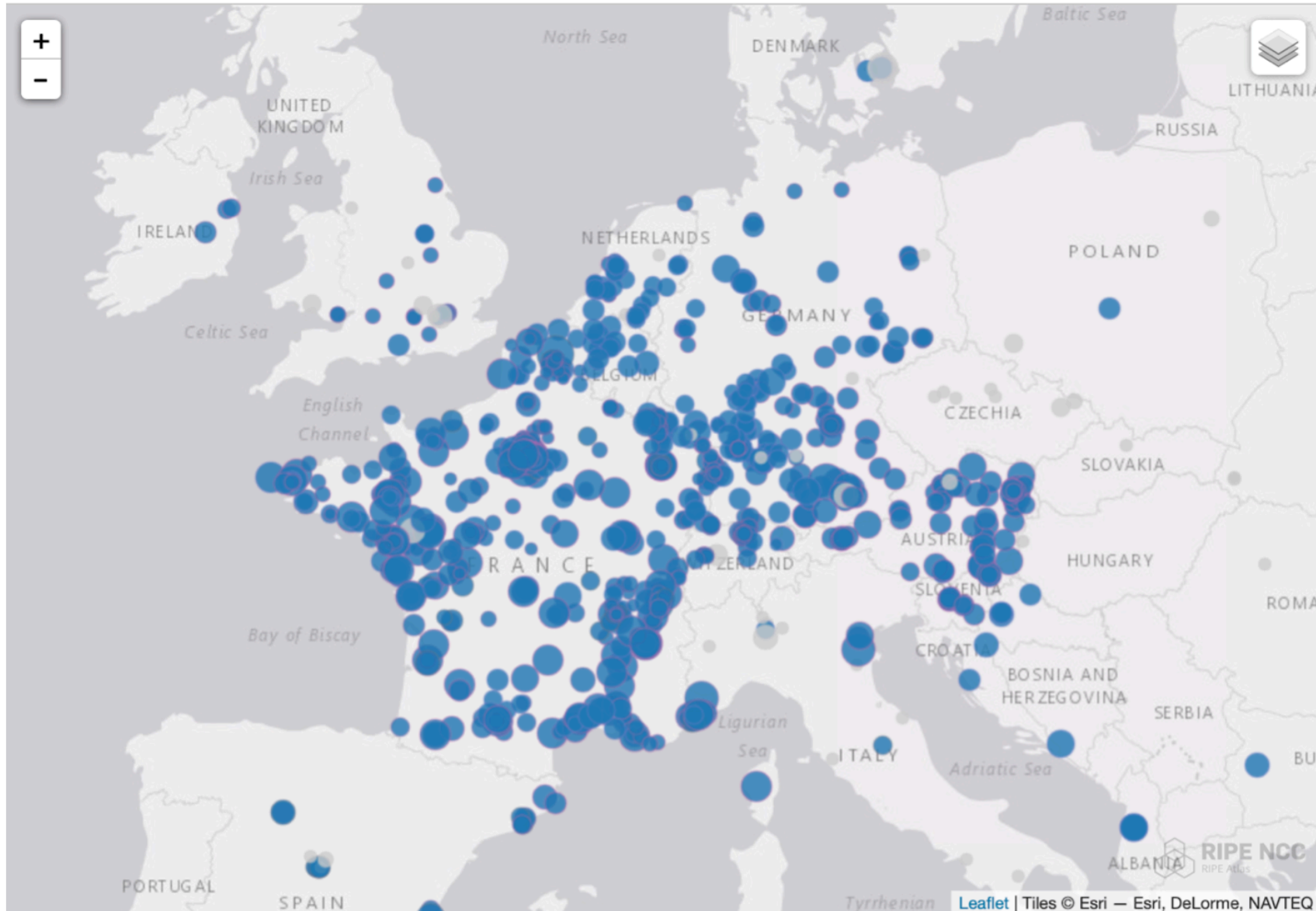


# ICANN Managed Root Server (IMRS) traffic analysis

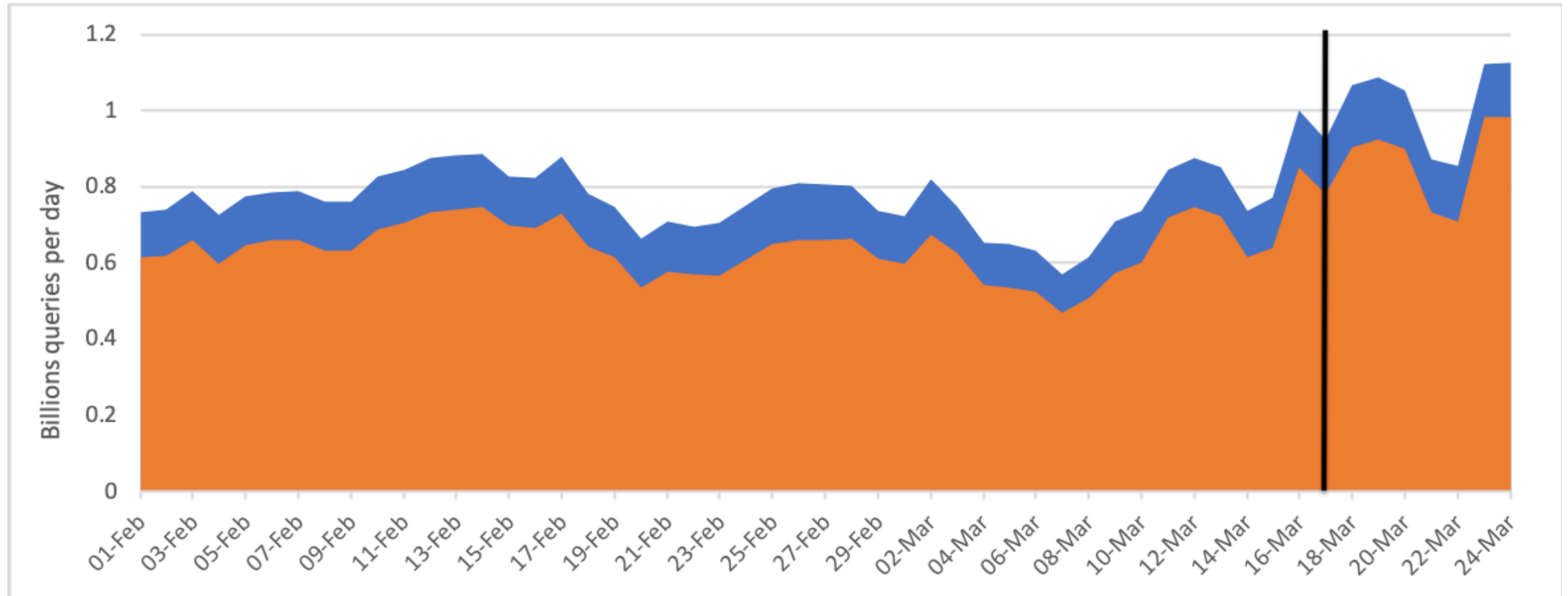
---

- ⦿ We looked into the cause of this traffic increase
- ⦿ We decided to focus on the four IMRS instances in France
  - Paris (2 sites), Lyon, Marseille
- ⦿ The lock down in France happened relatively quickly:
  - March 12: government announces school and university closures by March 16
  - March 13: gatherings with more than 100 people prohibited
  - March 14: non-essential public places closed
  - March 16: national lockdown beginning 17 March announced
- ⦿ A significant portion of DNS queries to IMRS instances in France originates from within the country
  - We used RIPE ATLAS probes in France as a proxy for recursive resolvers
  - Each ATLAS probe sends a periodic diagnostic query to each root server address and the response indicates which instance the sent the reply

# Location of ATLAS probes routing to IMRS instances in France



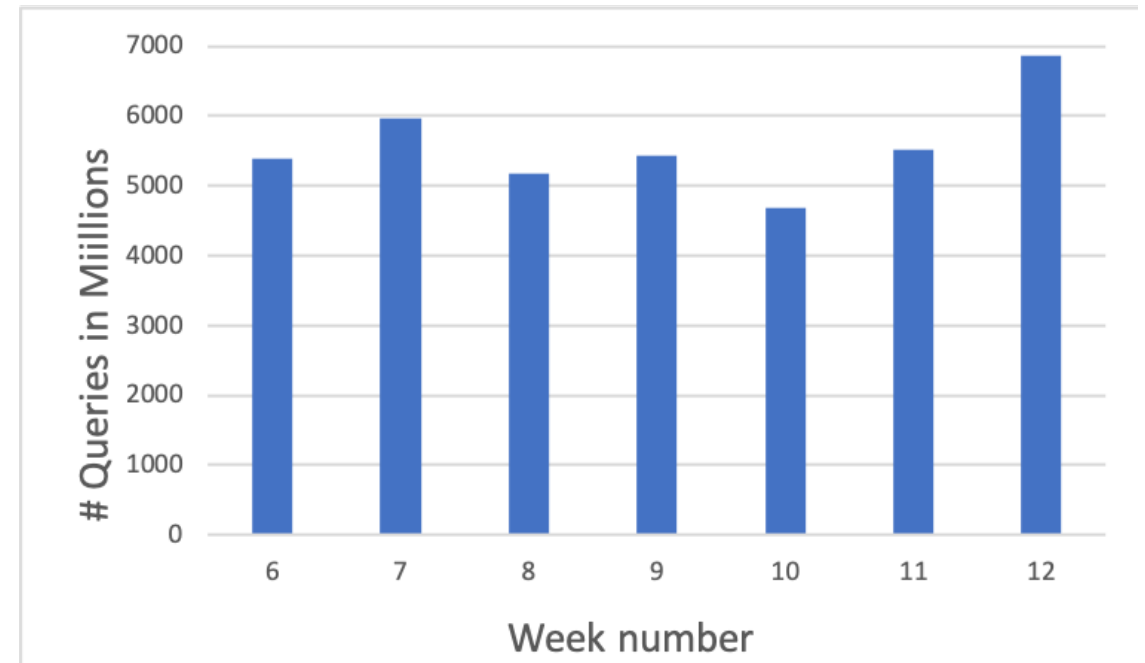
# Traffic increase to IMRS instances in France



(Orange represents queries for names for non-existent TLDs, blue for existing TLDs)

# Methodology

- ⦿ Compared two weeks of traffic to the four IMRS instances in France
  - Week 6: week starting 3 February 2020
  - Week 12: week starting 17 March 2020
- ⦿ **28% increase in overall traffic**
  - Average 5.4B queries/week in weeks 6-11
  - 6.9B queries/week in week 12





# Methodology (*continued*)

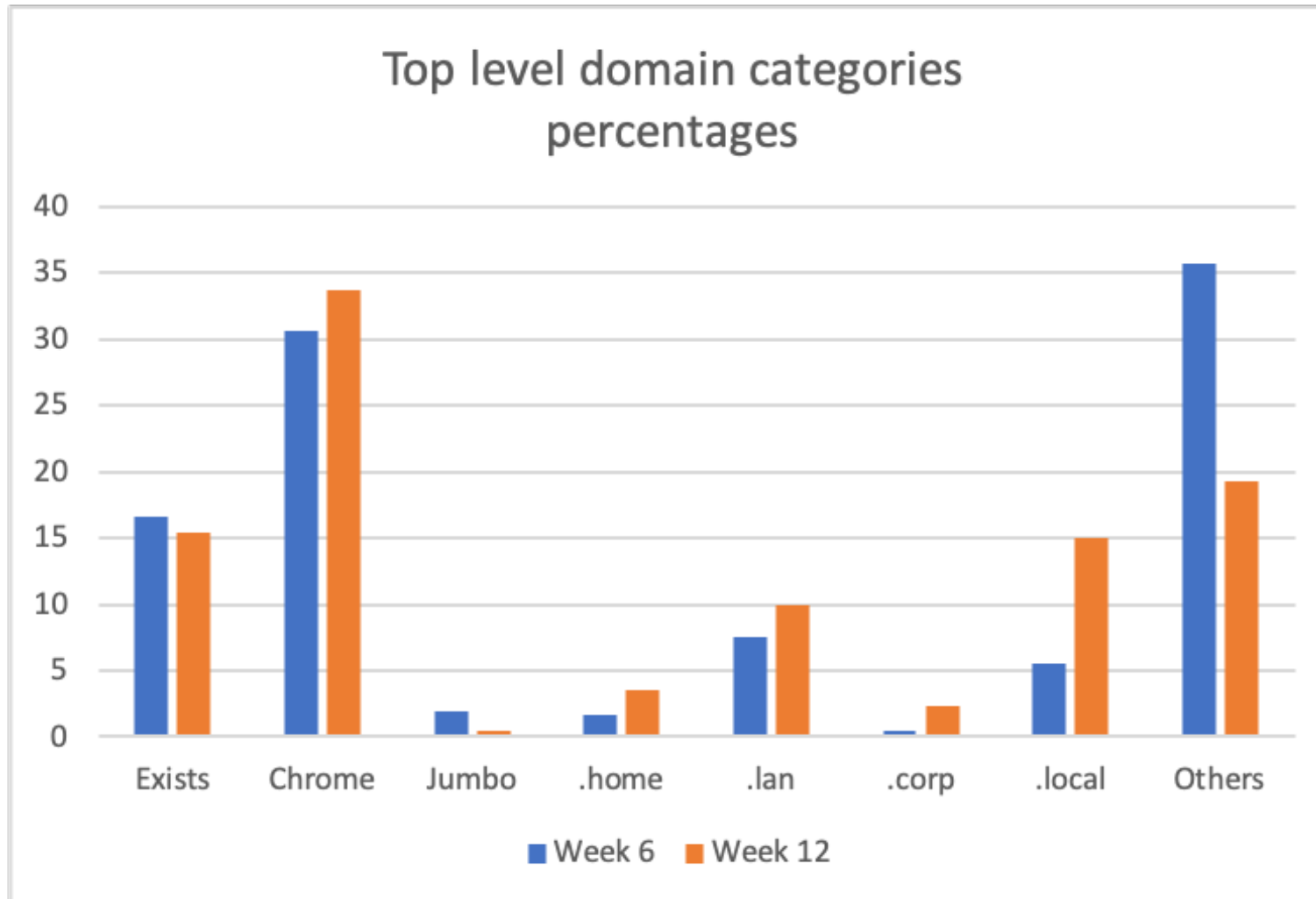
- ◉ We grouped each query into one of eight categories:

| Category        | Represents queries for...  |
|-----------------|--|
| <b>Exists</b>   | Domain names in TLDs that are currently delegated in the root zone |
| <b>Chromium</b> | Domain names in non-existent TLDs between 7 and 15 characters long |
| <b>Jumbo</b>    | Domain names in non-existent TLDs longer than 15 characters        |
| <b>.home</b>    | Domain names in the non-existent TLD “.home”                       |
| <b>.lan</b>     | Domain names in the non-existent TLD “.lan”                        |
| <b>.local</b>   | Domain names in the non-existent TLD “.local”                      |
| <b>.corp</b>    | Domain names in the non-existent TLD “.corp”                       |
| <b>Others</b>   | All other non-existent domain names                                |

# Queries per category compared Week 6 to Week 12

|                 | Week 6<br>(3 February 2020) |        | Week 12<br>(17 March 2020) |        | Increase/<br>Decrease |
|-----------------|-----------------------------|--------|----------------------------|--------|-----------------------|
| <b>Exists</b>   | 892,368,008                 | 16.6%  | 1,058,216,729              | 15.4%  | <b>19%</b>            |
| <b>Chromium</b> | 1,648,137,196               | 30.6%  | 2,317,414,531              | 33.8%  | <b>41%</b>            |
| <b>Jumbo</b>    | 102,962,057                 | 1.9%   | 36,596,751                 | 0.5%   | <b>-64%</b>           |
| <b>.home</b>    | 87,155,981                  | 1.6%   | 244,878,703                | 3.6%   | <b>181%</b>           |
| <b>.lan</b>     | 408,542,223                 | 7.6%   | 679,890,040                | 9.9%   | <b>66%</b>            |
| <b>.corp</b>    | 25,291,920                  | 0.5%   | 163,473,699                | 2.4%   | <b>546%</b>           |
| <b>.local</b>   | 296,288,423                 | 5.5%   | 1,035,726,205              | 15.1%  | <b>250%</b>           |
| <b>Others</b>   | 1,922,600,465               | 35.7%  | 1,327,598,837              | 19.3%  | <b>-31%</b>           |
| <b>Total</b>    | 5,383,346,273               | 100.0% | 6,863,795,495              | 100.0% | <b>28%</b>            |

# Changes in category of queried domain names



(All categories other than “Exists” represent non-existent domain responses)

# Queries for popular non-existent TLDs

|                 | Week 6<br>(3 February 2020) |        | Week 12<br>(17 March 2020) |        | Increase/<br>Decrease |
|-----------------|-----------------------------|--------|----------------------------|--------|-----------------------|
| <b>Exists</b>   | 892,368,008                 | 16.6%  | 1,058,216,729              | 15.4%  | <b>19%</b>            |
| <b>Chromium</b> | 1,648,137,196               | 30.6%  | 2,317,414,531              | 33.8%  | <b>41%</b>            |
| <b>Jumbo</b>    | 102,962,057                 | 1.9%   | 36,596,751                 | 0.5%   | <b>-64%</b>           |
| <b>.home</b>    | 87,155,981                  | 1.6%   | 244,878,703                | 3.6%   | <b>181%</b>           |
| <b>.lan</b>     | 408,542,223                 | 7.6%   | 679,890,040                | 9.9%   | <b>66%</b>            |
| <b>.corp</b>    | 25,291,920                  | 0.5%   | 163,473,699                | 2.4%   | <b>546%</b>           |
| <b>.local</b>   | 296,288,423                 | 5.5%   | 1,035,726,205              | 15.1%  | <b>250%</b>           |
| <b>Others</b>   | 1,922,600,465               | 35.7%  | 1,327,598,837              | 19.3%  | <b>-31%</b>           |
| <b>Total</b>    | 5,383,346,273               | 100.0% | 6,863,795,495              | 100.0% | <b>28%</b>            |

# Queries for popular non-existent TLDs (*continued*)

---

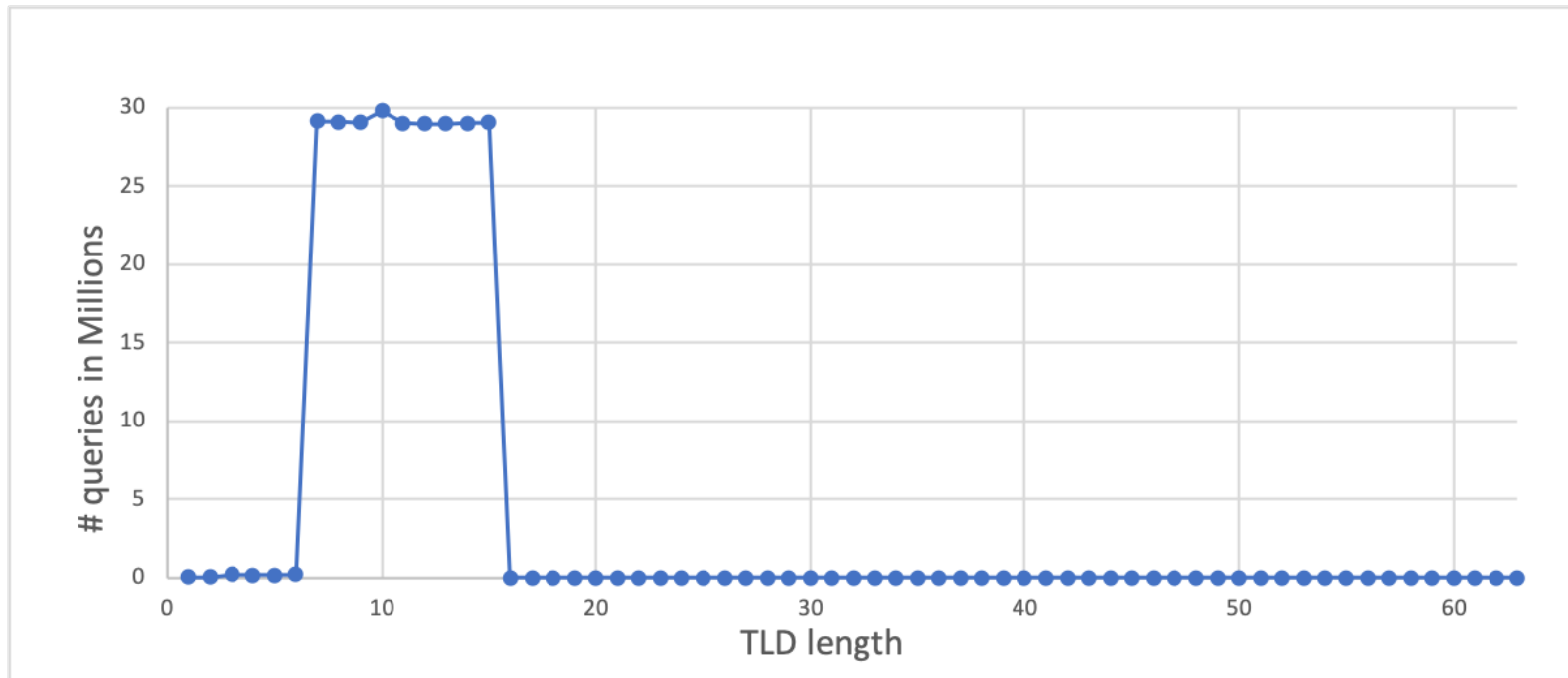
- ⦿ The most popular non-existent TLDs queried were *.corp*, *.home*, *.lan*, and *.local*
- ⦿ Significant increase in non-existent domain responses for *.corp* (546%), *.local* (250%), and *.home* (181%)
- ⦿ Hypothesis: The increase in queries for these TLDs is due to more users working from home
  - The *.corp* TLD is potentially used by employers to name internal devices
    - Older Microsoft documentation for Active Directory used *.corp* as an example TLD
  - The *.local* TLD is used by mDNS (Multicast DNS)
  - The *.home* TLD is used by default on many home routers issued by ISPs
  - Devices previously using employers' resolvers are now sending queries to the users' configured resolvers on home networks
  - Queries for domain names in these TLDs get spread out through more resolvers
  - More resolvers means more caches, which means more cache misses, which means more queries to the root servers

# Chromium queries

|                 | Week 6<br>(3 February 2020) |        | Week 12<br>(17 March 2020) |        | Increase/<br>Decrease |
|-----------------|-----------------------------|--------|----------------------------|--------|-----------------------|
| <b>Exists</b>   | 892,368,008                 | 16.6%  | 1,058,216,729              | 15.4%  | <b>19%</b>            |
| <b>Chromium</b> | 1,648,137,196               | 30.6%  | 2,317,414,531              | 33.8%  | <b>41%</b>            |
| <b>Jumbo</b>    | 102,962,057                 | 1.9%   | 36,596,751                 | 0.5%   | <b>-64%</b>           |
| <b>.home</b>    | 87,155,981                  | 1.6%   | 244,878,703                | 3.6%   | <b>181%</b>           |
| <b>.lan</b>     | 408,542,223                 | 7.6%   | 679,890,040                | 9.9%   | <b>66%</b>            |
| <b>.corp</b>    | 25,291,920                  | 0.5%   | 163,473,699                | 2.4%   | <b>546%</b>           |
| <b>.local</b>   | 296,288,423                 | 5.5%   | 1,035,726,205              | 15.1%  | <b>250%</b>           |
| <b>Others</b>   | 1,922,600,465               | 35.7%  | 1,327,598,837              | 19.3%  | <b>-31%</b>           |
| <b>Total</b>    | 5,383,346,273               | 100.0% | 6,863,795,495              | 100.0% | <b>28%</b>            |

# Chromium queries (*continued*)

- ⦿ Browsers based on Google Chromium send queries for random single label names between 7-15 characters long to check the local resolver's behavior (e.g., behind a captive portal)
- ⦿ Histogram of TLD length in all queries for non-existent domain names on 19 March 2020:



# Chromium queries (*continued*)

---

- ⦿ Queries for non-existent TLDs from browsers derived from Google Chromium account for around **one third of all queries to the IMRS**
- ⦿ The relative percentage of Chromium queries grew
  - 30.6% of all queries in Week 6, 33.8% in Week 12
- ⦿ The absolute number of Chromium queries grew more than non-Chromium queries
  - Chromium queries increased 41%
    - 1.6B in Week 6, 2.3B in Week 12
  - Non-Chromium queries increased 22%
    - 3.7B in Week 6, 4.5B in Week 12
- ⦿ Hypothesis: More devices running Chromium-derived browsers are now being used



# Summary of findings

---

- ⦿ Traffic to the IMRS has increased from levels before mid March 2020
  - Peak traffic to all IMRS instances combined has increased 20-25%
  - Total queries per week to the four IMRS instances in France is up 28%
- ⦿ There has been a significant increase in queries for non-existent domains in the TLDs *.corp* (546%), *.local* (250%), and *.home* (181%) to the four IMRS instances in France
  - Likely because user devices are dispersed more widely in homes rather than concentrated in offices and these devices are therefore using more recursive resolvers
- ⦿ Google Chromium-based browsers continue to send a lot of queries to the IMRS for non-existent TLDs: about one third of all queries
  - This Chromium-based traffic to the IMRS has increased along with all other traffic, suggesting more devices with Chromium-based browsers are now in use

# Acknowledgements

---

- ⦿ Roy Arends (OCTO Research team) is the primary author of the paper that this presentation is based on
  - “Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic”
    - <https://www.icann.org/en/system/files/files/octo-008-en.pdf>
- ⦿ Adiel Akplogan, David Conrad, Alain Durand, Paul Hoffman, David Huberman, Matt Larson, Sion Lloyd, Terry Manderson, David Soltero, Samaneh Tajalizadehkhoob, and Mauricio Vergara Ereche also contributed to this work