Coronavirus and DNS: view from the .nl ccTLD

SIDN Labs Technical Report TR-2020-01

March 26th, 2020

Giovane C. M. Moura (1) Thymen Wabeke (1) Cristian Hesselman (1,2)
Marc Groeneweg (3) Chiel van Spaandonk (3)
1: SIDN Labs 2: University of Twente 3: SIDN
firstname.lastname@sidn.nl

1 INTRODUCTION

The recent Coronavirus disease (COVID-19) outbreak has led to a pandemic of unseen proportions in modern times [33]. After its start in November/December 2019 in Wuhan, China, it has now (2020-03-20) spread and infected more than 487,000 patients worldwide, with more than 22,000 confirmed deaths [7].

On March 13th, the World Health Organization (WHO) has declared Europe to be the new epicenter of the Coronavirus pandemic [32]. To curb this pandemic, European countries have taken bold measures with the aim to reduce the number of infections. At the moment of this writing, five European countries are in complete lockdown: Italy, Spain, Belgium, France, and Czech Republic. Many other countries have recommended its citizens to work and stay at home as much as possible.

Altogether, these measures imposed by these European countries led to a significant reduction in the number of people outdoors and daily commuters. In the Netherlands only, the number of people making use of public transportation was reduced by 85% [29].

As such, as more people stay home, we can expect that has also consequences of such measures on Internet traffic and infrastructure well. For example, a surge in the use of social network – WhatsApp calls have doubled [25] – has been reported, and Netflix, a major video streaming platform, has decided to *reduce* the video quality in Europe for 30 days, in order to avoid congestion an impair the operation of networks in Europe [4]. Also, the Amsterdam Internet Exchange (AMS-IX) has reported an increase of 12% on Internet traffic on March 16th, 2020, in Amsterdam [1], while Cloudflare reported 20-40% traffic increase from Italy since Italy went into lockdown [20].

In this report, we focus on the Netherlands. To the writing of this report, two sets of measures were enacted by the Government of the Netherlands, as can be seen in Table 1. The first one, on March 12th, recommended employees to work from home as much as possible – even though that was done by Friday afternoon. On March 15th, more strict measures were imposed, in which all restaurants and cafes were to be closed for three weeks, in addition to gyms and schools. Even though not mandatory, most universities followed suit, and moved most lectures to online platforms.

We focus specifically on the impact of the Coronavirus pandemic indirect impact on the Netherlands' `.nl` country-code top-level domain (ccTLD), operated by SIDN [27]. In specific, we raise the follow research questions:

(1) Has there been a major impact on `.nl` DNS traffic since the Government of the Netherlands enacted measures to curb the Coronavirus spread (§3) ?

Date	Main measures
2020-03-12	Employees work from home
2020-03-15	Schools, cafe, bars, restaurants, and gyms closed
2020–03-24	Public gatherings and meetings prohibited

Table 1: Measures adopted by the Government of The Netherlands against the Coronavirus pandemic [22–24].

(2) Has there been registration of malicious domain name related to the Coronavirus pandemic (§4)?

2 BACKGROUND ON DNS

The Domain Name System (DNS) [10] is a core component of the Internet. Every web page and e-mail message requires DNS information, and a complex web page can easily require information from a dozen or more DNS lookups. With this central position, often serving as the initial transaction for every network connection, it is not surprising that DNS performance, security and stability are critical.

DNS *must* always work, and failures of major DNS resolution systems frequently makes public newspaper headlines. In 2016, when a Distributed Denial-of-Service (DDoS) attack led to problems at a DNS provider, it resulted in disruptions to multiple popular public services (including Github, Twitter and Netflix) [19].

2.1 Domain name registration and resolution

Registering a domain name is the process of creating a unique name that is added to a DNS zone file. Next, we describe this process under `.nl`. It usually involves a *registrant*, *registrar* (or reseller), and *registry*. The registrant (a user) requests an accredited registrar to register an available domain name at the registry. The registrar only executes this request once certain requirements are met, such as registrant information and payment being cleared, as shown in the left part of Figure 1.

Domains are registered for a period of one year, which will be automatically renewed at `.nl`. If the domain is cancelled, it will expire and is put on hold for 40 days and right after that made available for a new registration by any registrant. The list of valid domain names is then used to generate a DNS *Zone File* (Figure 1) that contains the list of all domains under `.nl`, and their respective DNS records. These Zone Files are used as input on the *authoritative name servers*, which are used to answer queries on `.nl` domain names.

Domain name resolution: Domain name resolution consists of resolving a domain name into, ultimately, its IP address or other specific types of DNS records [10]. To do that, a user's application

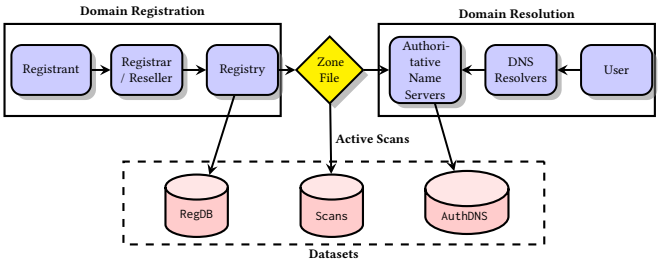

Figure 1: TLD operations: registration (left), domain resolution (right), and datasets.

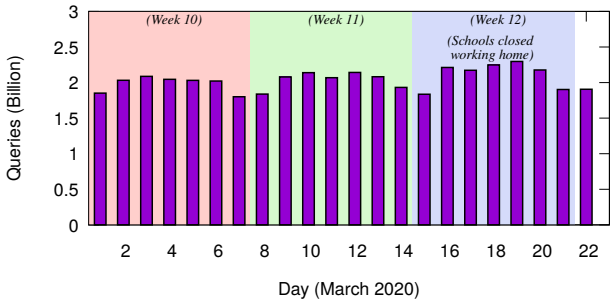

Figure 2: Daily DNS queries on .nl authoritative servers in March, 2020.

Week	Days (March)	∑ queries
10	1–6	13.86 billion
11	7–13	14.28 billion
12	14–21	14.84 billion

Table 2: Total queries per week – March 2020

contacts the stub DNS resolver (Figure 1) on his/her computer, which, in turn, sends a DNS request to its DNS *resolver* [6]. The DNS resolver will, on behalf of the user, recursively resolve the requested domain name, and ultimately contact the appropriate authoritative name server. Caching on DNS resolvers [12, 13] is used to eliminate frequently issued queries, improving response times.

This report focuses on the analysis of *authoritative* DNS servers, from the .nl zone, and on the registration of malicious domain names. SIDN [27], which is the registry and operator for .nl, handles the registration of .nl domain names, and publish zone updates on the authoritative servers.

SIDN Labs, the research arm of SIDN, collects data from two of the authoritative name servers with the goal of improving the security and stability of DNS. To this end, it has developed an open-source data streaming warehouse called ENTRADA [28, 35], which we use in this report, which we have been using since 2014 to support our research on security and stability of the .nl zone.

Privacy considerations. SIDN has developed a publicly available data privacy framework [2] that conforms to both EU and Dutch legislation [2, 5]. This framework has been implemented, including a privacy board that oversees SIDN Labs' research. While not part of this report, we refer the interested reader to the original documents [2, 5].

3 PRELIMINARY DNS TRAFFIC ANALYSIS

Figure 2 shows the number of daily queries (in billion) arriving at two of the three authoritative .nl DNS servers. Each server has IPv4 and IPv6 addresses, and employs IP anycast [9], in which the same addresses are announced from multiple locations (sites), in the attempt to server clients from closer servers, reducing latency. Overall, these three authoritative servers are distributed over one hundred global locations.

From Figure 2, we can see that the measures adopted against the Coronavirus spread has not incurred a large increase in the total number of .nl authoritative DNS queries. Overall, each day has 1.85–2.20 billion daily queries.

We focus on Week 12 – the first week in which people were requested to work from home and schools/day care were closed, from the measures imposed on March 15th, 2020. (We compare weeks since the Internet traffic is known to exhibit weekly diurnal traffic patterns [21]). On Week 12, we see more queries on each business days (16–20), in comparison to Weeks 10 and 11. Table 2 shows the total number of queries per each week. We see an increase of 560 million queries in Week 12 — a 3.9% increase in comparison with Week 11.

Reasons from growth. At this stage, it is hard to establish a direct connection between the growth of queries with the measures imposed by the Government of the Netherlands. We could only speculate. For example, one of the reasons for this growth observed on Week 12 could be due to people possibly spending more time online – given that other forms of leisure (sport clubs, gyms, bars, cafes, restaurants) remain closed. More time online may reflect on the total number of queries. Another reason may be that the overall effectiveness of caching in DNS is reduced, given people are more distributed. Both, however, are hard to validate with the data we have. We will further monitor this growth to determine its causes, as we do continuously with our traffic data.

What the data does not say. The data does not reflect *Internet traffic volume* – for example, how much data is transmitted in the Netherlands, or that passes by a Internet Exchange point (such as AMS-IX [1] and Cloudflare [20]). DNS queries are rather small, and can be used to indicate trends. For example, to stream a movie, it may take a dozen of DNS messages to resolve the domain names used by the streaming platform, which amount to a few kilobytes. The movie size itself, in turn, will take gigabytes of data – two orders of magnitude larger than DNS packets. As such, DNS traffic volumes cannot be directly correlated with other traffic volumes.

Also, authoritative DNS data is *intrinsically sampled*: DNS resolvers have *local caches*, which are used to store responses from queries they sent on behalf of users. If a user of a resolver queries for a domain at time x, any other subsequent users that query for the same domain will be directly answered from cache (so the resolver does not have to ask the authoritative server over and over the same question) [12]. As such, our data does not show individual' user behavior, rather, show aggregated behavior for records they do not have in cache.

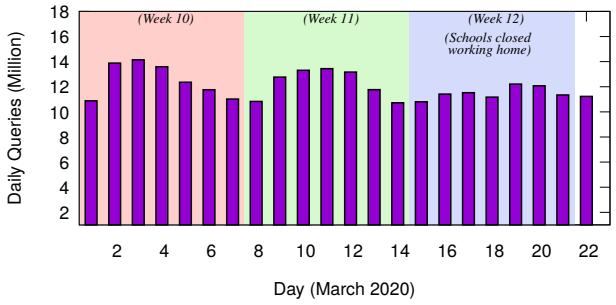

Figure 3: Queries from Educational Network

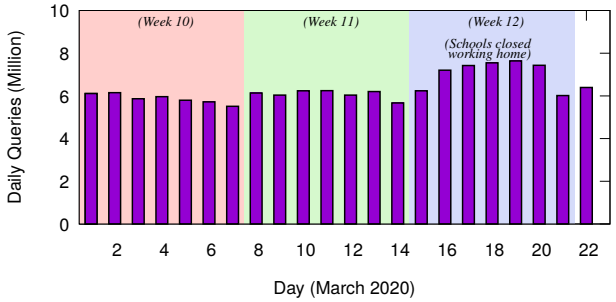

Figure 4: Queries from Consumer ISP

Week	∑ Educational	∑ ISP
10	87.6 million	41.1 million
11	86.0 million	42.5 million
12	80.5 million	49.6 million

Table 3: Sum of queries per week for Education network and an Anonymous Consumer ISP – March 2020

.

However, the authoritative server's side provides a *centralized* but *sampled* view of the zone: we observed resolver's cache misses traffic, for the two of three anycast authoritative servers we capture traffic.

3.1 DNS: queries move from school to homes

Given that more people are staying at home, and schools are closed, could this trend also be seen on DNS queries? We find evidence of *shifting* of traffic sources.

For example, Figure 3 shows the number of daily queries (in millions) from an Educational network in the Netherlands, which provide DNS services for schools and universities. We see a decrease of 6 million queries on Week 12 in comparison to Week 11 (6.4%, Table 3), which is expected given schools stayed closed throughout Week 12.

On the opposite direction, we see the number of queries from an anonymous Internet service provider (ISP) dedicated to home users to *increase* on Week 12 – possibly due to the fact of people working from home. We see an increase by 6.9 million queries (16% with relation to Week 11), as can be seen on both Table 3 and Figure 4.

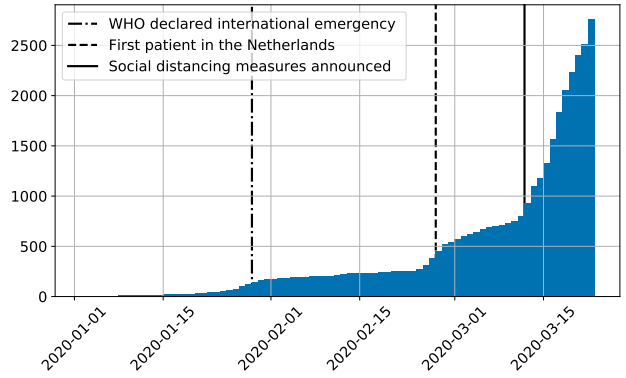

Figure 5: Daily registered domain names on the `.nl` zone with Coronavirus related terms in their names.

These two cases illustrate of what has been observed in practice: more people working from homes, more Internet traffic and DNS queries from consumer ISPs, and fewer from educational networks.

4 PRELIMINARY CORONAVIRUS DOMAIN REGISTRATION ANALYSIS

As a DNS registry, SIDN is responsible for maintaining a list of all `.nl` domain names, and to include, remove, and update domain name on behalf of registrars (*e.g.,* GoDaddy), which are, in turn, used by users to registry domains.

Our position as a registry gives a complete view of the .nl zone, which we leverage to monitor registration of malicious domains names. For example, we have published on detection and take down of phishing domains [3] and more recently on the so-called counterfeit luxury goods webshops [31] designed to scam users — who end up inadvertently buying fake products and have to deal with financial losses [16, 17].

In fact, on March 23rd, it has been reported a fraudulent website in The Netherlands that was involved in a 28,000 Euro face mask scam involving a client in Hong Kong [18] (the Public Prosecution Office of the Netherlands, in charge of this case, has not publicly disclosed which domain name was used in this scam operation, so we do not know if it was a `.nl` domain or not. The website, however, was hosted in the United States).

4.1 Suspicious domain name registration

We can also expect fraudsters to attempt to profit from Coronavirus pandemic, given it is a topic guaranteed to have user attention. To investigate that, we scrutinize the domain names registered under `.nl` to see if they have in their names one or few words associated with the pandemic, such as `corona, covid, n95, mondmasker, mondkap, virus, WHO` and `lockdown`, among others.

Figure 5 shows total number of newly registered domain names with the predefined keywords in their names. In total, 2766 domain names were registered between 2020-01-01 and 2020-03-23. We saw a daily increase of over 100 domains per day over the last weeks.

Domains classification: Registering domain names with Coronavirus terms is not a problem per se: many domains names are expected to be legitimate and informative domain names. Another

Coronavirus domains	2766
Without website	653
With website	2113
Undeveloped /default page	1109
E-commerce	120
Others	989

Table 4: Classification of Coronavirus related domains.

type of legitimate (but questionable) use of Coronavirus related domains are the "domainers" – a branch of the DNS industry dedicated with registering domain names with the purpose of *legally* profiting from ads hosted on their webpages [8, 30]. We can expect domainers to register such domains in order to profit from online advertisement.

We proceed them to classify the 2766-corona related domains based on their content. To do that, we used Dmap [34] to crawl and classify automatically the content of their webpages into three categories (we crawl in fact the entire `.nl` zone as well). Out of the 2766 domains, 2113 had an active web page on it, as can be seen in Table 4.

We further classify these domains with webpages into three categories. From the 2113, 1109 are classified as "Undeveloped/default page", which means that they show the hosting provider default landing page, and, as such, these domains have not been developed yet and, as such, they pose no risk.

The second category is e-commerce, in which the webpage has at least one e-commerce related technology, such as shopping carts used in payment systems (e.g., Zen Cart or WooCommerce). This category is the most worrying, given such websites can in principle carry out financial transactions, and if they are malicious, winding up scamming users (similarly to counterfeit luxury goods [31]). The "Others" category refers to the rest of the domains that did not fit in the other two categories. This category includes, among others, legitimate websites providing advice on handling the Coronavirus pandemy.

Manual Inspection. To determine whether these e-commerce were malicious or not, anti-abuse experts at SIDN's Support team analyzed individually 73 randomly chosen e-commerce domains from the 120 ones (Table 4). They found that most of the domains were dedicated to the sales of products related to preventing Coronavirus infections, such as alcohol-based gel and face masks — often at very high prices (not malicious per se).

Based on their insights, they singled out 24 suspicious domains out of the 73. These 24 domains are current under evaluation, and their registrants are being requested to conform their identities. The `.nl` regulations [26] determines that registrant data must be legitimate. Failure to conform to the regulation may result in domain name removal from the zone — a legal instrument that has been used in some take down procedures.

4.2 Detection Automation

We have automated this detection process and generate feeds with new domains to our Support colleagues, which evaluate these domains on a daily basis.

We also crawl on a daily basis all Coronavirus related domain names – do determine if they have changed their content or have been developed. Our goal is to prevent users from being scammed, and we will keep on continuously evaluate this process, similar to what we have done with the counterfeit goods detection.

5 SUMMARY AND NEXT STEPS

The DNS is one of the core parts of the Internet. The `.nl` ccTLD is the top-level domain used by most Dutch media, government, and companies. As such, its security and stability are always a major concern, but in these turbulent times caused by Coronavirus even more. As the `.nl` operator, SIDN strives for maximum security and stability of the `.nl` zone, as well as for improved performance [11–15, 31].

In this report, we asked two questions. The first one was whether there has been the impact of the Coronavirus measures taken by Government of the Netherlands on DNS traffic. We show that for the first week after the closure of schools and people working from home, that did not indirectly lead to a massive increase in DNS traffic to `.nl` authoritative servers. In fact, this growth has been so far of less than 4% – which can and has been easily handled by our infrastructure, which has anycast servers located in 5 continents over 100 global locations. By design, large DNS operators employ various layers of redundancy (namely multiple NS records, IP anycast, multiple servers per location) in order to cope with failure and very large DDoS attacks [11]. On the client's side, there is caching to cope with transient failures [12, 13].

We also asked if there have been malicious domains registrations related to the Coronavirus pandemic. We found more than 2000 domain names that keywords in their names related to the pandemic, and currently 24 are being further assessed to determine if they are malicious our not. To help our Support Department colleagues, we have also automated this process. The ultimate goal is to prevent `.nl` users to be scammed by malicious websites.

Last, the results here presented cover the very first week after the measures determined by the Government of The Netherlands. We will keep on monitoring closely both traffic patterns and registration of domain names for the coming months, in order to make sure that `.nl` keeps stable and secure.

REFERENCES

[1] AMS-IX. 2020. 12% more internet traffic last Monday (16 March) at 12:00 over the @AMS_IX #Amsterdam interconnection platform, due to the #Corona quarantine. https://twitter.com/AMS_IX/status/1239933280046272515.

[2] C. Hesselman, J. Jansen, M. Wullink, K. Vink, and M. Simon. 2014. *A privacy framework for DNS big data applications.* Technical Report. https://www.sidnlabs.nl/downloads/yBW6hBoaSZe4m6GJc_0b7w/2211058ab6330c7f3788141ea19d3db7/SIDN_Labs_Privacyraamwerk_Position_Paper_V1.4_ENG.pdf

[3] Giovane C. M. Moura, Moritz Muller, Maarten Wullink, and Cristian Hesselman. 2016. nDEWS: a New Domains Early Warning System for TLDs. In *IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2016), co-located with IEEE/IFIP Network Operations and Management Symposium (NOMS 2016).*

[4] Hadas Gold. 2020. Netflix is slowing down in Europe to keep the internet from breaking. https://edition.cnn.com/2020/03/19/tech/netflix-internet-overload-eu/index.html.

[5] C. Hesselman, G. C. M. Moura, R. d. O. Schmidt, and C. Toet. 2017. Increasing DNS Security and Stability through a Control Plane for Top-Level Domain Operators. *IEEE Communications Magazine* 55, 1 (January 2017), 197–203. https://doi.org/10.1109/MCOM.2017.1600521CM

[6] P. Hoffman, A. Sullivan, and K. Fujiwara. 2018. *DNS Terminology.* RFC 8499. IETF. http://tools.ietf.org/rfc/rfc8499.txt

[7] Johns Hopkins University & Medicine. 2020. Johns Hopkins Coronavirus Resource Center. https://coronavirus.jhu.edu/map.html, accessed on 2020-03-26.

[8] C. Lever, R. Walls, Y. Nadji, D. Dagon, P. McDaniel, and M. Antonakakis. 2016. Domain-Z: 28 Registrations Later Measuring the Exploitation of Residual Trust in Domains. In *2016 IEEE Symposium on Security and Privacy (SP)*. 691–706. https://doi.org/10.1109/SP.2016.47

[9] D. McPherson, D. Oran, D. Thaler, and E. Osterweil. 2014. *Architectural Considerations of IP Anycast.* RFC 7094. IETF. http://tools.ietf.org/rfc/rfc7094.txt

[10] P.V. Mockapetris. 1987. *Domain names - concepts and facilities.* RFC 1034. IETF. http://tools.ietf.org/rfc/rfc1034.txt

[11] Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei, and Christian Hesselman. 2016. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Santa Monica, California, USA, 255–270. https://doi.org/10.1145/2987443.2987446

[12] Giovane C. M. Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker. 2019. Cache Me If You Can: Effects of DNS Time-to-Live (extended). In *Proceedings of the ACM Internet Measurement Conference*. ACM, Amsterdam, the Netherlands, to appear. https://doi.org/10.1145/3355369.3355568

[13] Giovane C. M. Moura, John Heidemann, Moritz Müller, Ricardo de O. Schmidt, and Marco Davids. 2018. When the Dike Breaks: Dissecting DNS Defenses During DDoS. In *Proceedings of the ACM Internet Measurement Conference*. Boston, MA, USA, 8–21. https://doi.org/10.1145/3278532.3278534

[14] Moritz Müller, Giovane C. M. Moura, Ricardo de O. Schmidt, and John Heidemann. 2017. Recursives in the Wild: Engineering Authoritative DNS Servers. In *Proceedings of the ACM Internet Measurement Conference*. ACM, London, UK, 489–495. https://doi.org/10.1145/3131365.3131366

[15] Moritz Müller, Matthew Thomas, Duane Wessels, Wes Hardaker, Taejoong Chung, Willem Toorop, and Roland van Rijswijk-Deij. 2019. Roll, Roll, Roll Your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover. In *Proceedings of the Internet Measurement Conference (IMC '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3355369.3355570

[16] NOS. 2018. Consumenten voor 5 miljoen euro opgelicht via nepwinkels op sociale media *(in Dutch)*. (Dec. 12 2018). https://nos.nl/artikel/2258095-consumenten-voor-5-miljoen-euro-opgelicht-via-nepwinkels-op-sociale-media.html

[17] NOS. 2018. Waar komen al die nep-webshops toch vandaan? *(in Dutch)*. (May 5 2018). https://nos.nl/artikel/2230087-waar-komen-al-die-nep-webshops-toch-vandaan.html

[18] Openbaar Ministerie . 2020. Onderzoek naar oplichtingswebsite die mondkapjes aanbood (in Dutch). https://www.om.nl/actueel/nieuws/2020/03/23/onderzoek-oplichtingswebsite-die-mondkapjes-aanbood.

[19] Nicole Perlroth. 2016. Hackers Used New Weapons to Disrupt Major Websites Across U.S. *New York Times* (Oct. 22 2016), A1. http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

[20] Louis Poinsignon. 2020. On the shoulders of giants: recent changes in Internet traffic. https://blog.cloudflare.com/on-the-shoulders-of-giants-recent-changes-in-internet-traffic/.

[21] Lin Quan, John Heidemann, and Yuri Pradkin. 2014. When the Internet Sleeps: Correlating Diurnal Networks with External Factors. In *Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14)*. ACM, New York, NY, USA, 87–100. https://doi.org/10.1145/2663716.2663721

[22] Rijksoverheid (The Government of The Kingdom of The Netherlands). 2020. Aanvullende maatregelen 23 maart (in Dutch). https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/nieuws/2020/03/24/aanvullende-maatregelen-23-maart.

[23] Rijksoverheid (The Government of The Kingdom of The Netherlands). 2020. Aanvullende maatregelen onderwijs, horeca, sport (in Dutch). https://www.rijksoverheid.nl/actueel/nieuws/2020/03/12/nieuwe-maatregelen-tegen-verspreiding-coronavirus-in-nederland.

[24] Rijksoverheid (The Government of The Kingdom of The Netherlands). 2020. Aanvullende maatregelen onderwijs, horeca, sport (in Dutch). https://www.rijksoverheid.nl/actueel/nieuws/2020/03/15/aanvullende-maatregelen-onderwijs-horeca-sport.

[25] Rishi Iyengar. 2020. The coronavirus is stretching Facebook to its limits. https://edition.cnn.com/2020/03/18/tech/zuckerberg-facebook-coronavirus-response/index.html.

[26] SIDN. 2019. General Terms and Conditions for .nl Registrants. (May 19 2019). https://www.sidn.nl/downloads/d_7zdiiDQvOGbSo1FGCcqw/6d8b113b06e293bd9af55fb11a66c499/General_Terms_and_Conditions_for_nl_Registrants.pdf

[27] SIDN. 2020. Stichting Internet Domeinregistratie Nederland. http://sidn.nl.

[28] SIDN Labs. 2020. ENTRADA - DNS Big Data Analytics. https://entrada.sidnlabs.nl/.

[29] Treinreiziger.nl. 2020. 8560 miljoen per maand mis. https://www.treinreiziger.nl/extreem-rustig-in-de-trein-door-uitbraak-coronas.

[30] Thomas Vissers, Wouter Joosen, and Nick Nikiforakis. 2015. Parking sensors: Analyzing and detecting parked domains. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS 2015)*. Internet Society, 53–53.

[31] Thymen Wabeke, Giovane C. M. Moura, Nanneke Franken, and Cristian Hesselman. 2020. Counterfighting Counterfeit: detecting and taking down fraudulent webshops at a ccTLD.. In *Proceedings of the Passive and Active Measurement Workshop*. Eugene, OR, USA.

[32] William Feuer. 2020. Europe is now the 'epicenter' of the coronavirus pandemic, WHO says. https://www.cnbc.com/2020/03/13/europe-is-now-the-epicenter-of-the-coronavirus-pandemic-who-says.html.

[33] World Health Organization . 2020. Coronavirus disease (COVID-19) outbreak. https://www.who.int/emergencies/diseases/novel-coronavirus-2019.

[34] Maarten Wullink, Giovane CM Moura, and Cristian Hesselman. 2018. Dmap: Automating Domain Name Ecosystem Measurements and Applications. In *Proceedings of the IEEE Network Traffic Monitoring and Analysis Conference*. IEEE, Vienna, Austria, 1–8. https://doi.org/10.23919/TMA.2018.8506521

[35] Maarten Wullink, Giovane CM Moura, Moritz Müller, and Cristian Hesselman. 2016. ENTRADA: A high-performance network traffic data streaming warehouse. In *Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP*. IEEE, 913–918.