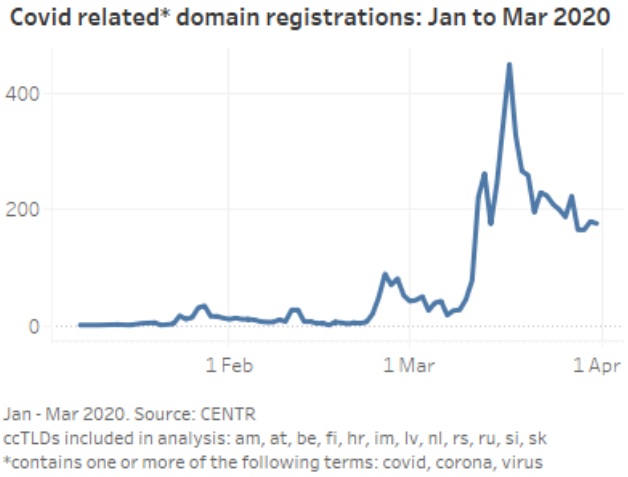
Повлияла ли “корона” на DNS?

Исследование, изложение которого мы приводим ниже, стало ответом на публикации в СМИ и соцсетях, авторы которых были возмущены снижением пропускной способности сети. Среди главных причин они называли неустойчивую работу системы доменных имен (DNS) и рост количества схем, указывающих на то, что приливная волна мошенничества и злоупотреблений поражает мир.

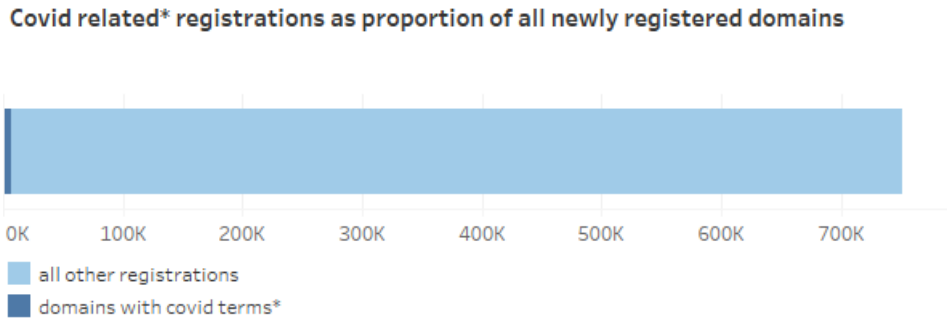
В CENTR изучили ситуацию и... "обнаружили, что пандемия COVID-19 не оказала существенного влияния на DNS ни с точки зрения регистрации, ни с точки зрения выявленных злоупотреблений".

COVID-19 и доменные регистрации

Чтобы оценить степень воздействия пандемии на систему DNS, CENTR изучил большую выборку доменных имен из 12 ccTLD – национальных доменных системы верхнего уровня – за три месяца – с января по март 2020 года. Выборка была ограничена доменами, которые включали слова: cow (корова), crown (корона) или вирус. В общей сложности 6 164 обращения включали эти условия, и большинство из них были зарегистрированы во второй половине марта 2020 года.

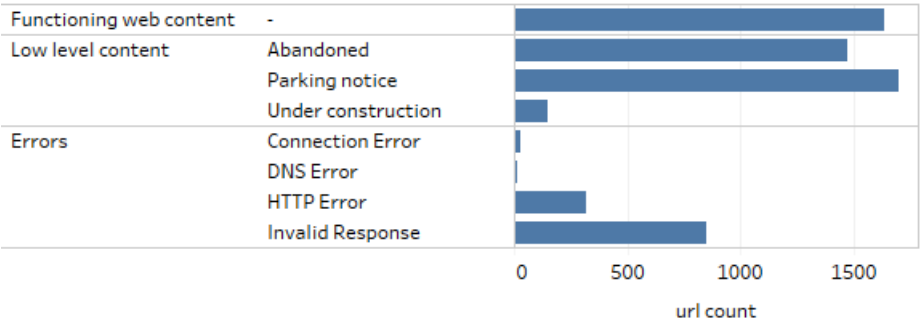


Для сравнения: в той же группе национальных доменов за первый квартал 2020 года зарегистрировано в общей сложности 751 000 новых доменов. То есть, домены связанные с со словом covid (с использованием одного из трех терминов), составляют 0,8 процента всех новых регистраций в этот период.



В рамках исследования, эксперты CENTR просканировали все домены, связанные по названию с коронавирусом, чтобы оценить их технический статус и понять, как они использовались, если использовались вообще. Результаты сканирования показывают, что только 26 процентов (или 1637 доменов) имеют работающий веб-контент. Остальные либо просто забронированы, либо владельцы выложили табличку "в процессе строительства", либо отображают другие формы технических ошибок.

Classification of domains with covid related terms*



*contains one or more of the following terms: covid, corona, virus

Часть доменов оказались общими для нескольких национальных доменов. В списке приведены десять лучших изо всех зарегистрированных:

Top 10 most common domain names registered using a covid related term*

covid19	15
covid-19	13
coronavirus	13
koronavirus	11
covid	9
corona-virus	8
anticorona	8
coronamask	6
coronainfo	6
corona	6

*contains one or more of the following terms: covid, corona, virus

Как DNS выдерживает давление?

DNS - это децентрализованная система, созданная с расчётом на высокие рабочие нагрузки, её базовые технические компоненты совершенствуются и оптимизируются уже почти полвека. В то время, как многие члены CENTR сообщали о более высоком, чем обычно, трафике и его перераспределении (пользователи начали потреблять больше трафика дома, и меньше – на предприятиях или в учебных заведениях), увеличение трафика не выходит за пределы текущей емкости европейской инфраструктуры ccTLD.

Каждый раз, когда пользователь вводит доменное имя или отправляет электронное письмо, системе DNS необходимо преобразовать это имя в IP-адрес. Поэтому любое значительное увеличение активности в Интернете означает увеличение трафика для DNS.

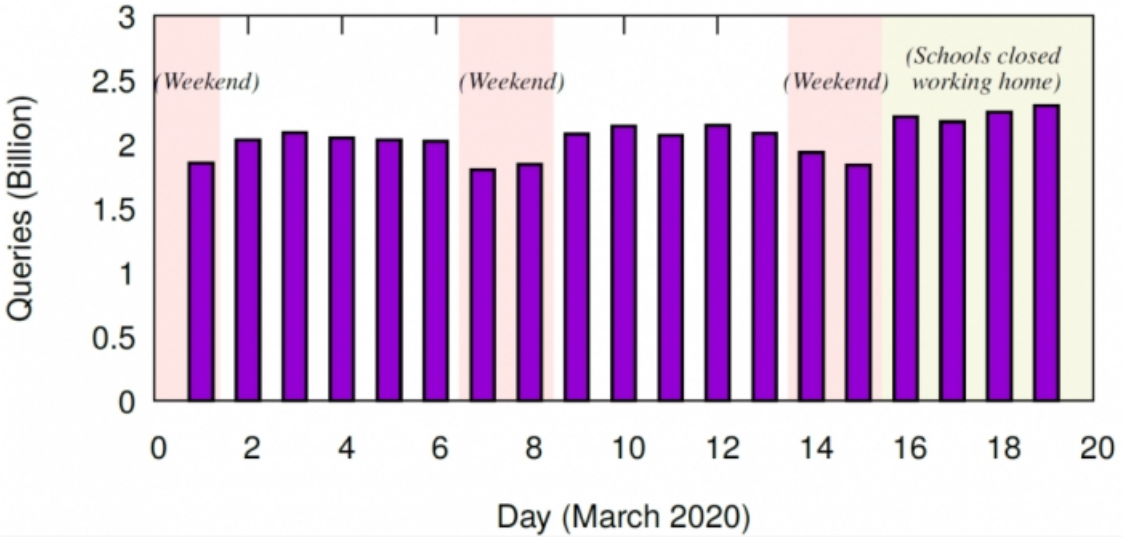
Для того чтобы справиться с нагрузкой, DNS использует систему кеширования (данные хранятся на разных уровнях сети для сокращения времени отклика), поэтому нагрузка на DNS-серверы верхнего уровня увеличивается не пропорционально росту потребления трафика.

Кроме того, у DNS более чем 20-летний опыт борьбы с DDoS-атаками. Эти атаки обычно генерируют уровни спроса, которые во много раз превышают количество запросов, которые генерируют сегодня пользователи.

Наконец, операторы национальных доменов верхнего уровня (реестры ccTLD) развернули сети anycast, которые предполагают дополнительный уровень защиты от атак или высокого уровня запросов DNS.

С учетом объема серверной ёмкости, которую реестры ccTLD развернули для обработки трафика, резервная мощность останется у них даже при десятикратном росте обращений.

Устойчивость сетей подтверждает и статистика. Вот как справляется с 25-процентным ростом нагрузки голландский оператор:



Как реагируют реестры?

Операторы доменов верхнего уровня – технические операторы, они не контролируют контент веб-сайтов, но если речь идёт о злоупотреблениях или нарушении закона, тесно сотрудничают с государственными надзорными органами. Такой же политики операторы придерживаются и в ситуации со злоупотреблениями, связанными с COVID-19.

Ситуация осложняется тем, что сегодня правительства и государственные органы регистрируют доменные имена, связанные с COVID-19, для информирования общественности о пандемии, и в то же время частные лица и компании используют доменные имена для взаимодействия с друзьями и партнёрами.

Между тем, фактических злоупотреблений с недавно зарегистрированными доменными именами, связанными с COVID-19 в Европе зафиксировано пока сравнительно немного.

В феврале 2020 года в CENTR создана группа, которая координирует обмен информацией в отношении доменов, зарегистрированных для неправомерных целей. Задача этой группы - выяснить, регистрируются ли в разных реестрах одновременно одинаковые или похожие доменные имена для мошенничества или фишинга. Пока злоупотреблений, связанных с доменами, связанными с COVID-19, немного, а большинство зарегистрированных доменов до сих пор не активны.

Эксперты CENTR изучили ситуацию, и, основываясь на широком спектре наборов данных и метрик пришли к выводу: пандемия COVID-19 не оказала существенного влияния на работу системы DNS. Пользователи продолжают регистрировать домены, причём, темпы роста – порядка двух процентов в месяц – пока не изменились. Инфраструктура справляется с нагрузкой, которая увеличилась примерно на 10 процентов, а уровень злоупотреблений с начала пандемии не повысился.Так что претензии к работе DNS, которые и стали поводом для расследования, совершенно безосновательны.