Анализ влияния режима самоизоляции в связи с COVID-19 на трафик IMRS

Офис технического директора ICANN

Рой Арендс (Roy Arends)
OCTO-008
15 апреля 2020 г.

ICANN

СОДЕРЖАНИЕ

Этот документ входит в состав серии документов OCTO. Список документов серии см. здесь: https://www.icann.org/resources/pages/octo-publications-2019-05-24-en. Вопросы или предложения по любому из этих документов отправляйте на адрес octo@icann.org.

Основные положения

Ожидается, что режим самоизоляции и закрытие школ в связи с COVID-19 окажут ограниченное, но заметное влияние на трафик системы доменных имен (DNS) на корневых серверах под управлением ICANN (IMRS). Офис технического директора ICANN (OCTO) изучил влияние общенационального режима самоизоляции во Франции на изменение как объема, так и состава трафика для четырех зеркал IMRS во Франции.

Согласно данным зондов Atlas Европейского сетевого координационного центра IP-сетей (RIPE NCC) источники трафика французских зеркал IMRS находятся преимущественно во Франции. Режим самоизоляции был введен во Франции 17 марта 2020 года (12-я неделя 2020 года). Статистика трафика за эту неделю показала прирост на 28% по сравнению со средним показателем за предыдущие 6 недель. Был выполнен сравнительный анализ данных за 6-ю и 12-ю недели, при этом сравнивались следующие категории:

- Запросы адресов существующих доменов верхнего уровня (TLD)
- Запросы от браузеров на основе Chromium
- Запросы адресов крупных TLD
- Запросы адресов популярных TLD (.home, .lan, .corp и .local)
- Все остальные запросы

Для большинства категорий наблюдался рост трафика, способствующий общему увеличению. Самая большая категория — запросы от браузеров Chromium, на которые приходилось около трети всех полученных запросов. Некоторые категории росли быстрее других. Наибольший процентный прирост наблюдался для четырех категорий популярных несуществующих TLD (.corp, .home, .lan и .local). Вероятно, это связано с тем, что люди больше работают на дому, поскольку офисные работники обычно используют резолверы, которые понимают, как реагировать на домены .corp, .lan и .local. Теперь они теперь больше рассредоточены и работают дома, используя резолверы, которые могут неправильно реагировать на эти домены. Этим также объясняется рост числа запросов .home: больше людей чаще выходят в интернет из дома.

Общенациональная самоизоляция оказала ограниченное, но заметное влияние на трафик DNS на зеркалах IMRS на уровне страны. Такое увеличение трафика DNS наблюдается повсеместно, и отсутствие проблем говорит о том, что архитектура DNS хорошо подходит для масштабирования во время удаленной работы и более широкого использования дома.

1 Введение

Общенациональная самоизоляция, ограничение деятельности и закрытие школ оказали ограниченное, но заметное влияние на трафик DNS на зеркалах IMRS. По большому счету, источником подавляющей части трафика DNS, наблюдаемого на IMRS, являются резолверы, которые отправляют запросы DNS от имени клиентских устройств, таких как мобильные телефоны, планшеты, персональные компьютеры (ноутбуки и настольные компьютеры), игровые приставки и т. д. Эти резолверы имеют возможность временного кэширования информации, что снижает нагрузку на корневые серверы. Например, после того как резолвер кэшировал информацию о DNS-серверах пространства имен .com, ему не нужно обращаться к корневым серверам для получения информации о example.com, а нужно только запросить DNS-серверы .com.

На момент написания этой статьи (31 марта 2020 года) у IMRS 167 зеркал, расположенных в 83 странах. Это исследование посвящено четырем зеркалам IMRS во Франции. Причина, побудившая сосредоточить внимание на этих зеркалах, заключается в том, что правительство Франции очень оперативно публиковало объявления о закрытии школ, ограничении деятельности и общенациональной самоизоляции. 12 марта правительство объявило о закрытии школ и университетов с 16 марта. 13 марта были запрещены собрания численностью более 100 человек. 14 марта было приказано закрыть все второстепенные общественные места, включая рестораны, кафе, кинотеатры и дискотеки. 16 марта была объявлена общенациональная самоизоляция, начиная со следующего дня.

Трафик поступает на серверы IMRS из широкого спектра источников, которые не всегда находятся в той же стране, что и запрашиваемые зеркала. Используя зонды Atlas RIPE[1] в качестве прокси-резолверов клиентских устройств, можно определить, какие именно зонды используют четыре зеркала IMRS, находящиеся сейчас во Франции.

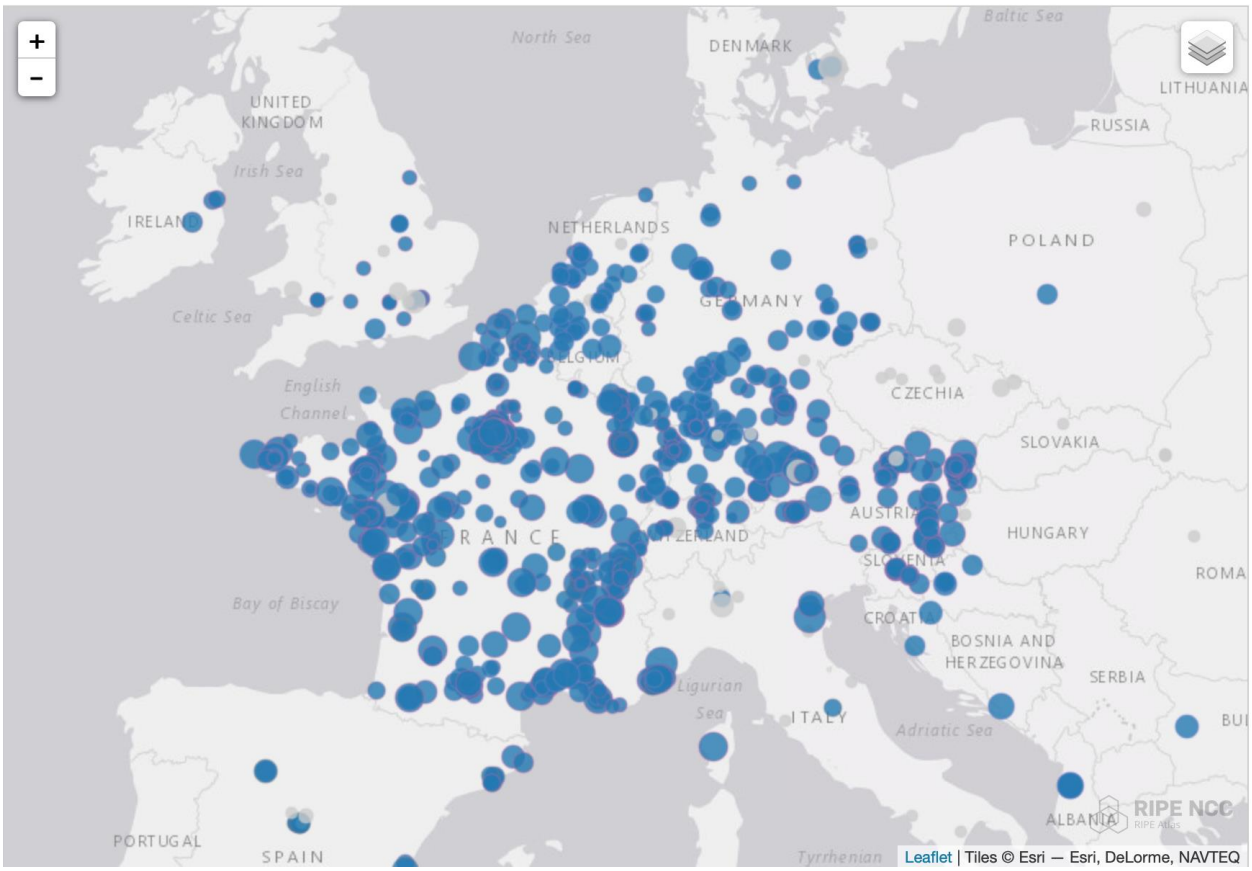

Рис. 1. Распределение зондов Atlas в перехватывающих модулях зеркал IMRS, находящихся во Франции

Как видно из рисунка 1, хотя за пределами Франции достаточно много зондов, получивших ответы от вышеупомянутых зеркал IMRS, источники значительного объема трафика на французских зеркалах IMRS находятся во Франции.

[1] Atlas RIPE — это глобальная, открытая и распределенная платформа для оценки параметров интернета, состоящая из тысяч измерительных устройств, оценивающих подключение к интернету в режиме реального времени.

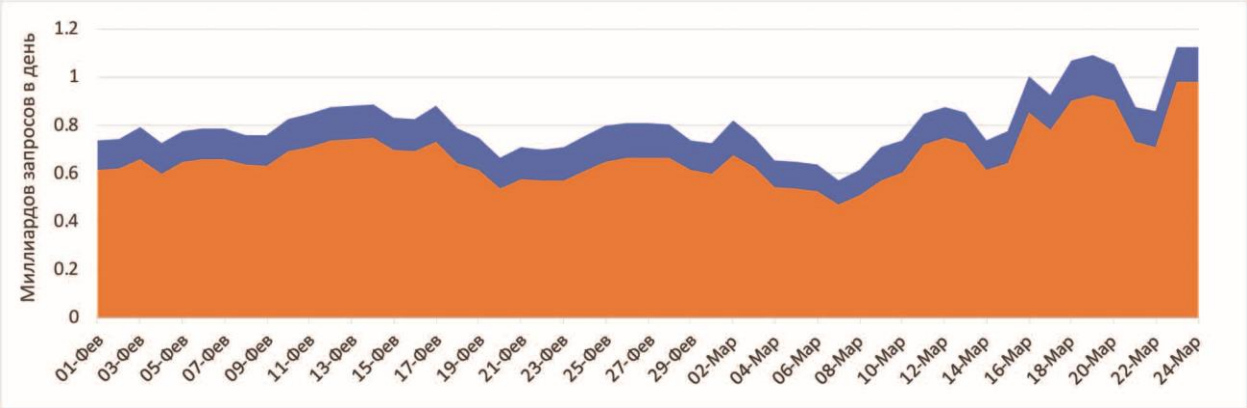

Рис. 2. Ежедневный объем запросов (синий) и дневной объем ответов NXDOMAIN (оранжевый), наблюдаемый на 4 зеркалах IMRS во Франции. Черная вертикальная линия указывает на начало 17 марта.

Как видно из рисунка 2, после 16 марта объем трафика увеличился. Чтобы понять причины этого роста, мы изучили состав трафика. Сравним состав до и после 16 марта, чтобы понять, связаны ли изменения состава с самоизоляцией.

2 Методология

Мы сравним две недели трафика. Первую неделю в феврале (6-я неделя, начиная с 3 февраля) с неделей, начавшейся 16 марта (12-я неделя), которая стала первой неделей самоизоляции. Затем мы затем разделим этот трафик по категориям и покажем, в какой из них произошли наиболее значительные изменения.

2.1 Классификация

Трафик сгруппирован по нескольким категориям в зависимости от запрашиваемого TLD:

- **Существующие**: запросы данных о TLD, делегированных в настоящее время в корневой зоне
- **Chrome** : запросы данных о несуществующих TLD длиной от 7 до 15 символов
- **Огромные**: запросы данных о несуществующих TLD длиннее 15 символов
- **.home**: запросы данных о доменах, которые заканчиваются на .home
- **.lan**: запросы данных о доменах, которые заканчиваются на .lan
- **.local**: запросы данных о доменах, которые заканчиваются на .local
- **.corp**: запросы данных о доменах, которые заканчиваются на .corp
- **Другие**: запросы данных о всех остальных доменах

2.1.1 Запросы Chrome

Браузер Chromium и его производные (такие как Google Chrome, последние версии Microsoft Edge, Amazon Silk и Opera) отправляют три DNS-запроса со случайной меткой, чтобы определить, переадресует ли используемый в локальной сети резолвер несуществующие домены, например, возвращается ли в ответ на запрос адрес поискового «вспомогательного» сайта для несуществующих доменов. Метка состоит

из случайного набора букв длиной от 7 до 15 символов.[2] Поскольку запрашивается случайный домен, у получающего резолвера нет кэшированных данных и он отправит запрос корневому серверу. В сетях без переадресации ожидаемым ответом на этот случайный запрос будет код ошибки NXDOMAIN.

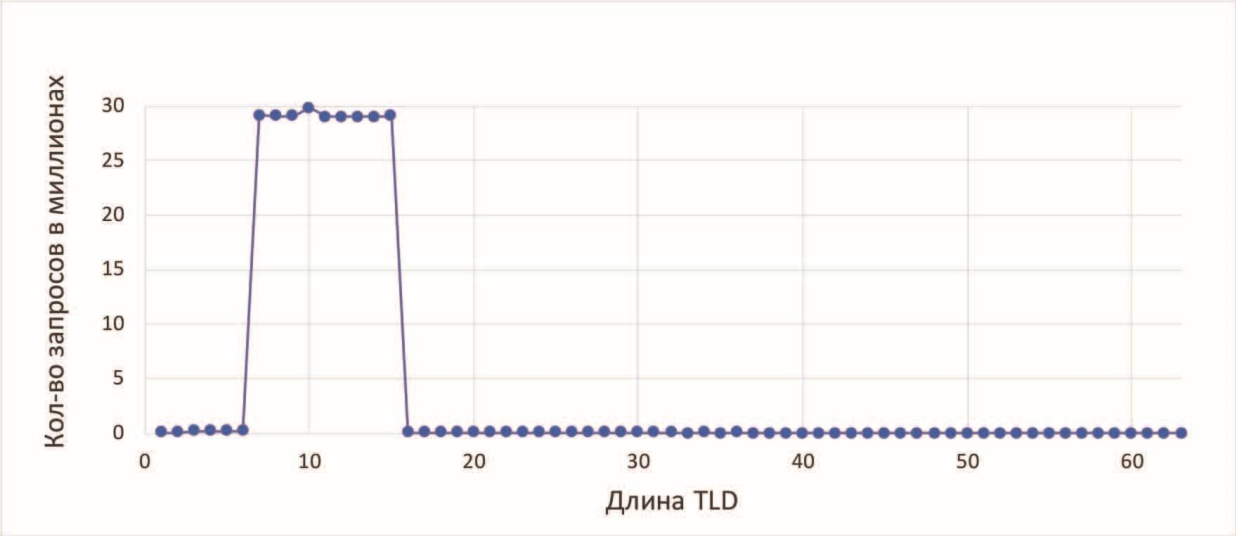

Рис. 3. Гистограмма количества запросов несуществующих TLD в разрезе длины TLD.

Гистограмма на рисунке 3, отображающая данные от 19 марта, показывает частотное распределение запросов по длине TLD. Подавляющая часть этих запросов относится к доменным именам в диапазоне от 7 до 15 символов. На рисунке 5 показано, что эти запросы Chrome составляют 28% всех запросов данных о несуществующих доменах.

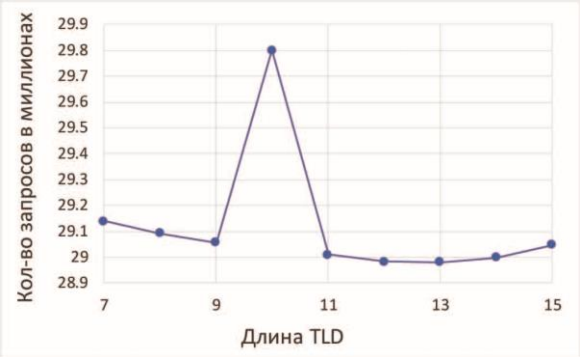

Рис. 4. Сведения о гистограмме количества запросов несуществующих TLD в разрезе длины TLD.

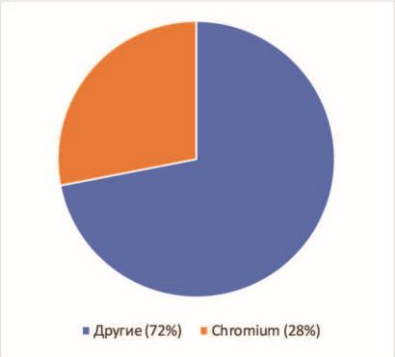

Рис. 5. Количество запросов Chromium по всем запросам несуществующих доменов.

За исключением 10-символьных TLD распределение среди TLD длиной от 7 до 15 символов довольно равномерное. Аномалию для 10-символьных меток можно объяснить тем, что более старые версии Chrome выдавали случайные домены длиной 10 символов.[3]

[2] «Мы генерируем случайное имя хоста длиной от 7 до 15 символов». https://chromium.googlesource.com/chromium/src/+/master/chrome/browser/intranet_redirect_detector.cc#150

[3] «Изменение длины имен для обнаружения взлома DNS». https://src.chromium.org/viewvc/chrome?view=revision&revision=249013

2.1.2 Огромные запросы

Это запросы данных о несуществующих TLD длиннее 15 символов. Нам неизвестны источники или причины таких запросов.

2.1.3 Популярные несуществующие TLD

Существует ряд популярных меток, которые не были делегированы в корневой зоне и отсутствуют в общедоступном пространстве имен DNS интернета. В число наиболее популярных несуществующих TLD входят .home, .lan, .corp и .local. Эти TLD классифицируются индивидуально, поскольку за исследуемый период для всех наблюдался прирост объема.

2.1.4 Другие

В эту категорию попадают все запросы, которые нельзя отнести ни к одной из ранее описанных категорий.

3 Наблюдения

Четыре зеркала IMRS во Франции получали в среднем по 5,4 миллиарда DNS-запросов в неделю между 6 и 11 неделями (см. рис. 6). Те же самые зеркала получили 6,9 миллиардов DNS-запросов за 12-ю неделю. Это означает прирост входящего трафика этих четырех узлов IMRS на 28%.

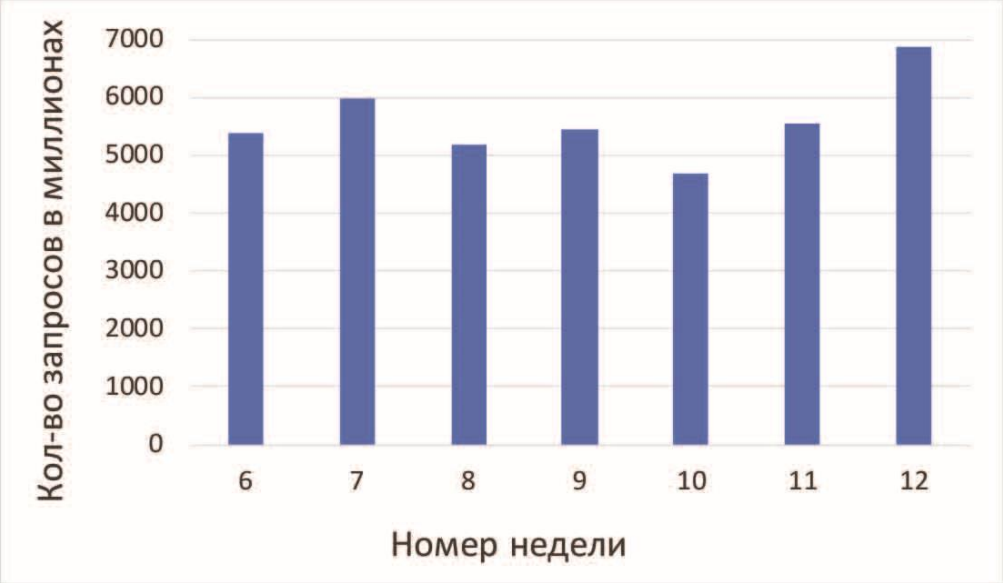

Рис. 6. Еженедельный объем запросов для 4 зеркал во Франции с 6-ю по 12-ю неделю.

В этот период мы зафиксировали некоторые аномалии, такие как короткие всплески трафика или отключение на техобслуживание, но они, как правило, были кратковременными, и мы не считаем, что они существенно влияют на общий трафик. Другие типовые изменения трафика, такие как суточная картина или выходные дни,

также были поглощены, поскольку объем трафика накапливался за неделю. Нам неизвестно о каких-либо других изменениях или событиях за этот период времени, которые могли бы столь существенно повлиять на объем DNS-запросов.

Рис. 7. Объем трафика для существующих и несуществующих TLD в 6-ю и 12-ю недели

Рис 8. Объем трафика для существующих и несуществующих TLD в 6-ю и 12-ю недели в процентах от общего объема за эти недели

На рисунке 7 показана разница абсолютных значений объема запросов для существующих и несуществующих доменов. Объем в обеих группах вырос. Рисунок 8 показывает, что также наблюдается небольшое изменение структуры трафика, поскольку процент запросов для существующих доменов верхнего уровня снизился по сравнению с запросами для несуществующих доменов. Увеличение трафика в основном определяется запросами данных о несуществующих доменах.

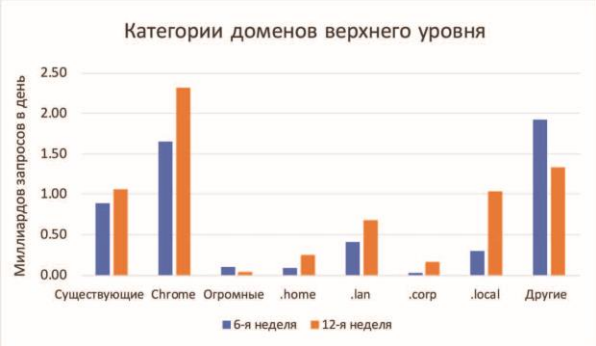

Рис. 9. Распределение трафика по различным категориям при сравнении 6-й и 12-й недель в абсолютных значениях.

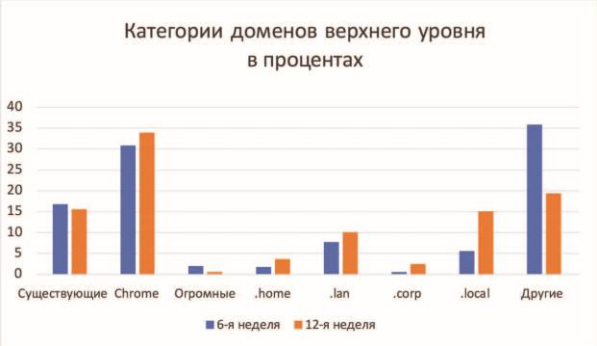

Рис. 10. Распределение трафика по различным категориям при сравнении 6-й и 12-й недель в процентах от общего объема.

3.1 Запросы Chromium

Мы заметили, что 31% запросов, полученных на 6-й неделе, и 34% запросов, полученных на 12-й неделе, относятся к категории DNS-запросов Chromium. Это остается значительной частью общего трафика. После самоизоляции общее количество запросов увеличилось на 28%, а доля Chromium увеличилась на 41%. Вероятно, такое увеличение связано с тем, что больше устройств чаще подключаются к сети для выполнения обязанностей, связанных с работой на дому.

Из-за DNS-запросов Chromium, связанных с обнаружением переадресации, частота DNS-запросов для произвольных строк длиной от 7 до 15 символов, видимых в трафике, будет выше, когда к сети подключено больше устройств с браузерами на основе Chromium. Обратите внимание, что количество DNS-запросов Chromium не выросло на тот же процент, что и общий трафик. Это указывает на незначительное изменение структуры общего трафика. В других категориях наблюдался более высокий прирост, по сравнению с запросами Chromium.

Запросы Chromium — самой большая группа запросов к корневым серверам. Другие зеркала IMRS часто получают более 50% всех входящих запросов от Chromium. Целью этих запросов является проверка того, находится ли Chromium за порталом авторизации. Резервирование корневых серверов часто зависит от общей нагрузки на корневые серверы для удовлетворения потребностей в масштабировании. Хотя эти запросы бесплатны для Chromium, затраты на резервирование зеркал корневых серверов нет. Google получила уведомление об этой проблеме, но она остается нерешенной.[4]

3.2 Огромные запросы

Мы заметили, что объем запросов с большими доменами TLD (длиннее 15 символов) сократился. Мы не изучили причину этого падения трафика.

3.3 Популярные несуществующие TLD

Четырьмя наиболее популярными несуществующими TLD, для которых наблюдалось увеличение объема, были .corp, .home, .lan и .local. Из них наиболее значительное увеличение наблюдалось для .corp, .lan и .local. Вероятно, это связано с тем, что люди больше работают на дому. Как правило, офисные работники обычно используют группу резолверов, которые понимают, как реагировать на домены .corp, .lan и .local. Теперь они теперь больше рассредоточены и работают дома, используя резолверы, которые могут неправильно реагировать на эти домены. Этим также объясняется рост числа запросов .home: больше людей чаще выходят в интернет из дома.

4 Заключение

Общенациональная самоизоляция для сдерживания пандемии оказала ограниченное, но заметное влияние на трафик DNS на зеркалах IMRS на уровне страны. Такое увеличение трафика DNS наблюдается повсеместно. Отсутствие проблем говорит о том, что архитектура DNS хорошо подходит для масштабирования в сценариях удаленной работы и более широкого использования дома.

Авторы: Адиэль Акплоган (Adiel Akplogan), Рой Арендс (Roy Arends), Дэвид Конрад (David Conrad), Ален Дюран (Alain Durand), Пол Хоффман (Paul Hoffman), Дэвид Хуберман (David Huberman), Мэтт Ларсон (Matt Larson), Сион Ллойд (Sion Lloyd), Терри Мандерсон (Terry Manderson), Дэвид Сольтеро (David Soltero), Саманэ Таджализадехкуб (Samaneh Tajalizadehkhoob), Маурисио Вергара Эреш (Mauricio Vergara Ereche).

[4] У трех случайных зондов детектора переадресации в интрасети нет TLD и поэтому они запрашивают корневые серверы. https://bugs.chromium.org/p/chromium/issues/detail?id=946450&q=intranet%20redirect&can=2