№12
Ноябрь 2019

MSK IX

Интернет изнутри

ИЗМЕРЕНИЯ

Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №12, дата выхода: ноябрь 2019 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Ильина Наталья

Корректор:
Рябова Наталья

Всякое дело мера красит

главный редактор,
Андрей Робачевский

Дорогой читатель!

Интернет - чрезвычайно сложная коммуникационная система, в основе которой лежит очень простая концептуальная модель. Органическая эволюция Интернета и секреты этого потрясающего развития заслуживают отдельной дискуссии, и мы уже затрагивали эту тему в одном из прошлых выпусков журнала.

Сегодня же мы посвятили отдельный раздел вопросу измерений и, в частности, тому, как измерения с помощью глобальной системы трансляции имен DNS помогают нам лучше узнать об использовании различных технологий и приложений, и использованию Интернета в целом. Джефф Хьюстон совместно с сотрудниками лаборатории APNIC использовали средства онлайн-рекламы для анализа возможности снижения нагрузки на систему DNS и предотвращения целого класса атак. Об этом Джефф рассказывает в статье («В поиске несуществующего». Александр Венедюхин в своей статье «DNS как источник глобальной информации о Сети» развивает эту тему, исследуя, что может рассказать DNS о различных аспектах Интернета.

Следуя новой концепции журнала, мы разместили также статьи, которые выходят за рамки темы измерений, но обсуждают актуальные проблемы сегодняшнего Интернета. От новых разновидностей вредоносов («Бесфайловое вредоносное программное обеспечение») до новой мутации DNS, известной под именем DoH («DoH, или DNS, похожий на веб»), от цифровой повестки ЕС («Цифровая повестка ЕС: реформирование регулирования телекоммуникаций и контента в правовой системе Европейского союза») до обсуждения возможности построения Интернета в отдельно взятой стране («Локален ли глобальный Интернет?») - все это вы найдете в этом выпуске.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках?

Пишите нам по адресу info@internetinside.ru.

В поиске несуществующего

Джефф Хьюстон (Geoff Huston)

DNSSEC часто считают решением, которое никак не найдет себе проблему. С одной стороны, возможность явно проверить достоверность и актуальность ответов на запросы DNS вроде бы должна зачем-то да пригодиться, но вот с практическими примерами беда. Подписание зон DNS по DNSSEC распространяется довольно медленно, как бы показывая, что польза от DNSSEC весьма сомнительна. А такие распространенные примеры, как неподписанное имя www.google.com, тоже вроде бы свидетельствуют, что даже Google не видит особого смысла подписывать такой крупный сайт. Так в чем же может быть польза от DNSSEC?

DNSSEC часто считают решением, которое никак не найдет себе проблему. С одной стороны, возможность явно проверить достоверность и актуальность ответов на запросы DNS вроде бы должна зачем-то да пригодиться, но вот с практическими примерами беда. Подписание зон DNS по DNSSEC распространяется довольно медленно, как бы показывая, что польза от DNSSEC весьма сомнительна. А такие распространенные примеры, как неподписанное имя www.google.com, тоже вроде бы свидетельствуют, что даже Google не видит особого смысла подписывать такой крупный сайт. Так в чем же может быть польза от DNSSEC?

Некоторые надежды возлагаются на DANE, т.е. доменные ключи в составе DNS. Данные, которые используются для проверки достоверности сертификата доменного имени по TLS, тоже можно публиковать в составе DNS, чтобы клиент мог с помощью DNS проверить данные TLS для удаленного конца соединения, а ответ DNS можно проверить по DNSSEC. Для браузеров эта идея не «взлетела» по ряду причин, связанных с уязвимостью для разнообразных атак посредника (man-in-the-middle attack), а также из-за озабоченности повсеместным применением ключей RSA малого размера в DNSSEC... не говоря уже о том, что все пространство DANE уязвимо для атак ределегирования регистратора. DANE получил кое-какое признание в почтовом сегменте в качестве метода борьбы со спамом, но более масштабные планы внедрения DANE и DNSSEC в дополнение к структуре CA WebPKI или даже на замену ей с треском провалились.

Есть ли у DNSSEC другая прямая польза? Зачем-то еще нам может сейчас потребоваться подписывать доменные имена?

Довольно неожиданный сценарий применения связан с тем, как именно DNS объявляет, что такого-то доменного имени не существует. Если авторитетный сервер имен DNS обслуживает заранее подписанные зоны, то он не может подписать то,

Поскольку большая часть запросов DNS возникает от потребности сопоставить доменное имя IP-адресу перед тем, как установить то или иное сетевое соединение, подписанный ответ DNS означал бы, что хакеру труднее заменить адрес в ответе DNS и обмануть конечного пользователя. Но хотя в прошлом это было серьезной проблемой, ныне ее эффективно решают безопасные транспортные сервисы в виде TLS (Transport Layer Security).

TLS-соединение получает набор учетных данных, с помощью которых можно проверить, обладает ли удаленная сторона соединения закрытым ключом, связанным с ее доменным именем. Это делается путем выдачи сертификата X.509 от доверенного сертификационного органа. При использовании TLS хакеру становится мало заставить DNS выдавать ложные ответы – ему потребуется заставить кучу элементов инфраструктуры Интернета сгенерировать правдоподобный, но фальшивый сертификат доменного имени.

По опыту атак с подменой имен можно сказать, что гораздо проще ввести в заблуждение регистратора доменных имен и вынудить его ределегировать целую зону серверам имен, находящимся под контролем злоумышленника. Если эта зона подписана по DNSSEC, то в рамках той же самой атаки можно подменить записи DS – и все защитные свойства DNSSEC пойдут прахом. После этого сертификационный орган может выдать сертификаты на ределегированное имя, и атака увенчается успехом. По крайней мере, временным.

чего нет в статическом файле зоны, а потому не может заранее подписать набор ответов NXDOMAIN на запросы обо всех возможных именах, которые не определены в данной зоне DNS. Вместо этого в DNSSEC определен альтернативный метод: DNSSEC подписывает «пробелы» между именами в зоне, в которой имена упорядочены лексикографически. Такой метод эффективен даже в сочетании с NSEC3, так как NSEC3 просто переопределяет порядок меток в зоне, чтобы незначительно усложнить ее нумерацию. Ответ NXDOMAIN, подписанный DNSSEC, несет в себе гораздо больше информации, чем «такого-то конкретного имени не существует». Он подтверждает, что не существует целого диапазона имен, поэтому тот же самый ответ можно использовать для запросов о наличии любых имен из диапазона. Рекурсивный резолвер с поддержкой DNSSEC мог бы кэшировать эти «ответы о пустых диапазонах» и повторно использовать их для любых имен, которые попадают в подобный диапазон, не отправляя запросы авторитетному серверу имен зоны.

Такой процесс кэширования отрицательных ответов пока что довольно непривычен. Но в нем есть большой смысл: он защищает от атак на DNS с использованием случайных имен. Если хакер запрограммирует несколько slave-ботов так, чтобы каждый из них потихоньку кормил DNS-сервер запросами о случайно сгенерированных именах в зоне, которая является мишенью для атаки, то рекурсивные резолверы, не найдя это имя в кэше, будут пересылать запросы авторитетному серверу зоны. При достаточно большом числе ботов авторитетный сервер зоны «ляжет», как показала атака на DNS-инфраструктуру DYN в октябре 2016 года.

Как защищаться от таких DNS-атак со случайной генерацией имен? Создание армии ботов не предотвратить никак. Запретить им выполнять скрипты для автогенерации имен и запросов DNS тоже не получится. А вот поставить барьер на уровне рекурсивного резолвера мы можем, если поручим ему генерацию ответов NXDOMAIN на такие случайные имена, чтобы запросы не передавались на авторитетные серверы. Если зона подписана по DNSSEC, а рекурсивный резолвер выполняет проверку DNSSEC и кэширование NSEC, как описано в RFC 8198, то резолвер будет выдавать ответы на запросы о случайных именах прямо из кэша. В результате большая часть запросов так и не попадет на сервер имен.

Кэширование NSEC на рекурсивных резолверах было проанализировано в лабораторной конфигурации Петром Шпашеком (Petr Špaček) из CZNIC. Петр подавал запросы на рекурсивные резолверы с помощью инструмента повтора запросов и сравнивал конфигурацию с кэшированием NSEC и обычный кэш NXDOMAIN. [https://indico.dns-oarc.net/event/28/contributions/509/attachments/479/786/DNS-OARC-28-presentation-RFC8198.pdf] По его данным, кэширование NSEC оказалось особенно эффективным для борьбы с атаками, основанными на генерации случайных имен.

Кэширование NSEC поддерживает целый ряд изготовителей инструментов рекурсивных резолверов DNS, включая BIND, Unbound и KNOT: либо по умолчанию, либо в качестве опции при настройке.

Измерение кэширования NSEC

Мы в APNIC Labs давно изучаем различные аспекты инфраструктуры DNS и подумали, что было бы неплохо проверить, имеет ли в наши дни смысл реализовывать DNSSEC с кэшированием NSEC. Мы хотели получить ответ на вопрос: насколько сейчас эффективно кэширование NSEC?

Вопрос непростой, поскольку мы пытались измерить то, что не видно с поверхности. Нам нужно было отслеживать те запросы на преобразование несуществующих имен, которые НЕ передаются на авторитетный сервер имен зоны. Иными словами, мы искали отсутствующие ответы на запросы об отсутствующих именах!

И снова мы для этой цели использовали платформу для измерений интернет-рекламы. Платформа рассылает примерно 5-10 миллионов реклам в день по всему «видимому» Интернету, а реклама содержит встроенный Javascript, который указывает «подопытному» выбрать небольшой набор URL. Используя имена DNS, выдаваемые авторитетным сервером имен под нашим управлением, мы можем наблюдать DNS-взаимодействие между рекурсивными резолверами конечного клиента и экспериментальными серверами DNS. Непосредственные действия клиента нам не видны, равно как и то, что происходит в DNS между клиентом и его рекурсивными резолверами: нам видны только наши серверы на нашем конце соединения.

В этом случае тест кэширования NSEC довольно просто описать. Скрипт предписывает клиенту получить объект по URL-адресу, чье доменное имя подписано, но само это имя не существует. Спустя две секунды скрипт предписывает клиенту получить второй объект по URL-адресу, чье доменное имя также не существует, но попадает в диапазон несуществующих имен, охваченный записью NSEC от первого запроса. Нас интересуют клиенты, у которых рекурсивный резолвер опрашивает первое имя, но не второе.

Искать запрос, которого не должно быть, непросто, так как в скриптах измерения есть и элемент частичного выполнения, поэтому несуществующие запросы легко спутать с экспериментальным шумом. Для лучшей интерпретации результатов мы использовали двухэтапный процесс DNS, где уникальное имя преобразовывается в ответ CNAME (подписанный по DNSSEC), который сопоставлен с несуществующим именем, и эксперимент использует два прохода: первый для загрузки кэша, а второй для использования кэша. На рис. 1 изображена последовательность прохождения запроса DNS.

Тупиковый резолвер в оконечной клиентской системе получает задачу – выполнить преобразование двух доменных имен, оба со случайными метками. Первое имя взято из зоны, подписанной DNSSEC, второе – из неподписанной зоны.

Когда авторитетный сервер имен получает запрос о первом имени, он отвечает записью CNAME, указывающей на имя в другой подписанной зоне. При запросе этого нового имени авторитетный сервер отправляет в

ответ код NXDOMAIN. Если в состав запроса входит флаг OK EDNS(0) DNSSEC (бит DO), то авторитетный сервер также возвращает запись NSEC, охватывающую пространство имен зоны нового имени.

Второе имя не подписано и всегда приводит к появлению ответа NXDOMAIN.

Затем скрипт делает паузу в 2 секунды и повторяет те же самые два запроса, но с чуть-чуть измененным именем. Для подписанной зоны ответ CNAME будет использовать имя, которое попадает в диапазон, обозначенный предыдущей записью NSEC. Если рекурсивный резолвер выполняет кэширование NSEC, то он выдаст ответ на основе этой же записи NSEC, не опрашивая авторитетный сервер. В примере на рис. 1 на запрос имени name3.signed2.example можно отправить ответ из локального кэша NSEC.

Мы получили тест, который (в теории) способен показать, где рекурсивные резолверы используют NSEC и где нет. Рекурсивный резолвер с кэшированием NSEC сгенерирует только пять запросов к авторитетному серверу имен, в то время как рекурсивные резолверы без средств безопасности или без кэширования NSEC выдадут запросы на все шесть уникальных имен.

Ожидания

Рекурсивные резолверы с проверкой DNSSEC использует целых 29% пользователей Интернета – на удивление много. Примерно 8% пользователей находятся в смешанной среде резолверов с проверкой DNSSEC и без, так что когда резолвер с проверкой DNSSEC возвращает SERVFAIL, что означает неудачную проверку, тупиковый резолвер повторно отправляет запрос, уже к серверу без проверки. Остальные 21% используют только рекурсивные резолверы с проверкой DNSSEC. (Рис. 2)

Нас в этом контексте интересует более высокая цифра – 29% пользователей, т.к. ответ NXDOMAIN должен приниматься без вопросов, а запись NSEC отправляться на рекурсивный резолвер. Иными словами, даже в частичном сценарии резолвер с проверкой DNSSEC, если запрос к нему отправлен первым, генерирует ответ NXDOMAIN, получив который, тупиковый резолвер пользователя не будет опрашивать другие резолверы.

Рекурсивные резолверы – весьма скособоченная структура: небольшое число резолверов используется непропорционально большим числом пользователей. Где-то 12% пользователей первым делом направляют свои запросы на общедоступные серверы DNS Google, и всего 10 крупнейших резолверов обслуживают треть всех пользователей Интернета.

Верхней границей кэширования NSEC по идее должны быть те же самые 29%, что и у проверки DNSSEC. Исходя из понимания, что общедоступные DNS-резолверы Google выполняют кэширование NSEC, нижняя граница должна быть где-то на 10%. В грубом предположении, что кэширование NSEC на резолверах с проверкой DNSSEC составит где-то 50%, мы получим разумное ожидание того, что примерно 15-20% всех пользователей покажут результаты, коррелирующие с кэшированием NSEC.

Результаты

Результаты эксперимента проиллюстрированы на рис. 3.

За 98 дней мы провели наш эксперимент примерно 266 миллионов раз. Паттерны запросов, коррелирующие с кэшированием NSEC, обнаружились в 6-9% случаев, остальные не выказывали признаков кэширования NSEC. Цифры были ниже в рабочие дни и выше в выходные. Когда в конце мая объем показов эксперимента снизился, вместе с ним упала и доля кэширования NSEC.

На основе этих данных было бы разумно заключить, что кэширование NSEC слабо распространено и не развивается, а наши ожидания в чем-то оказались ошибочными.

Рис. 1. Измерение кэша NSEC: модель запроса DNS.

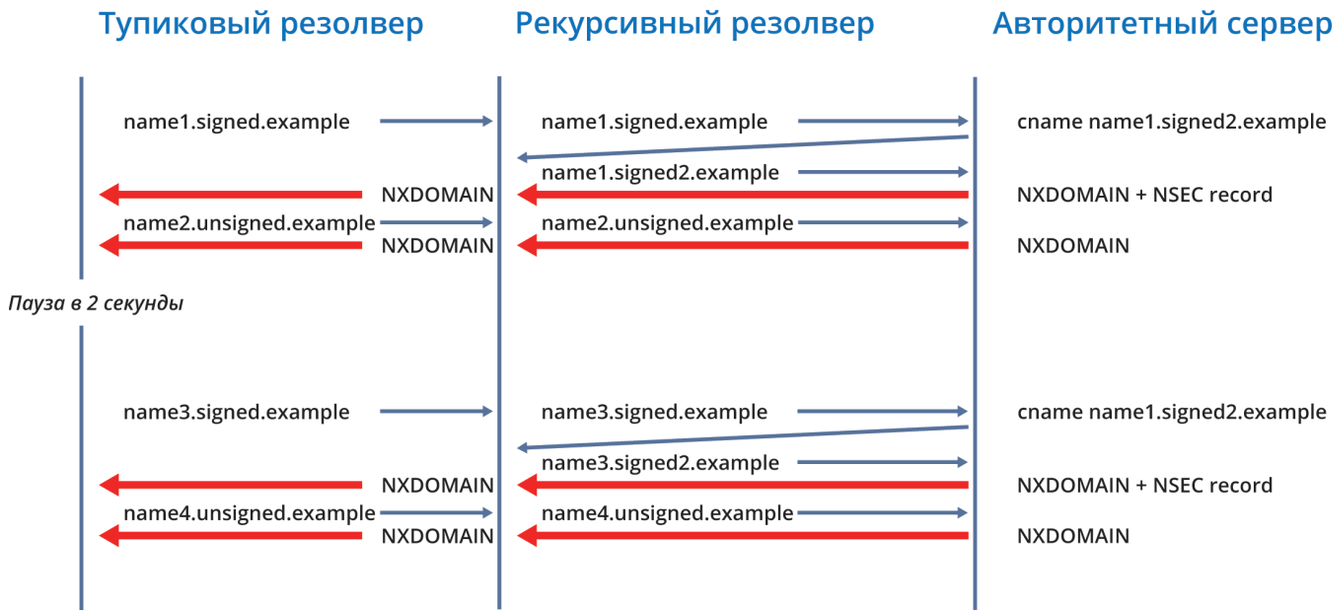


Рис. 2. Использование валидации DNSSEC в мире.

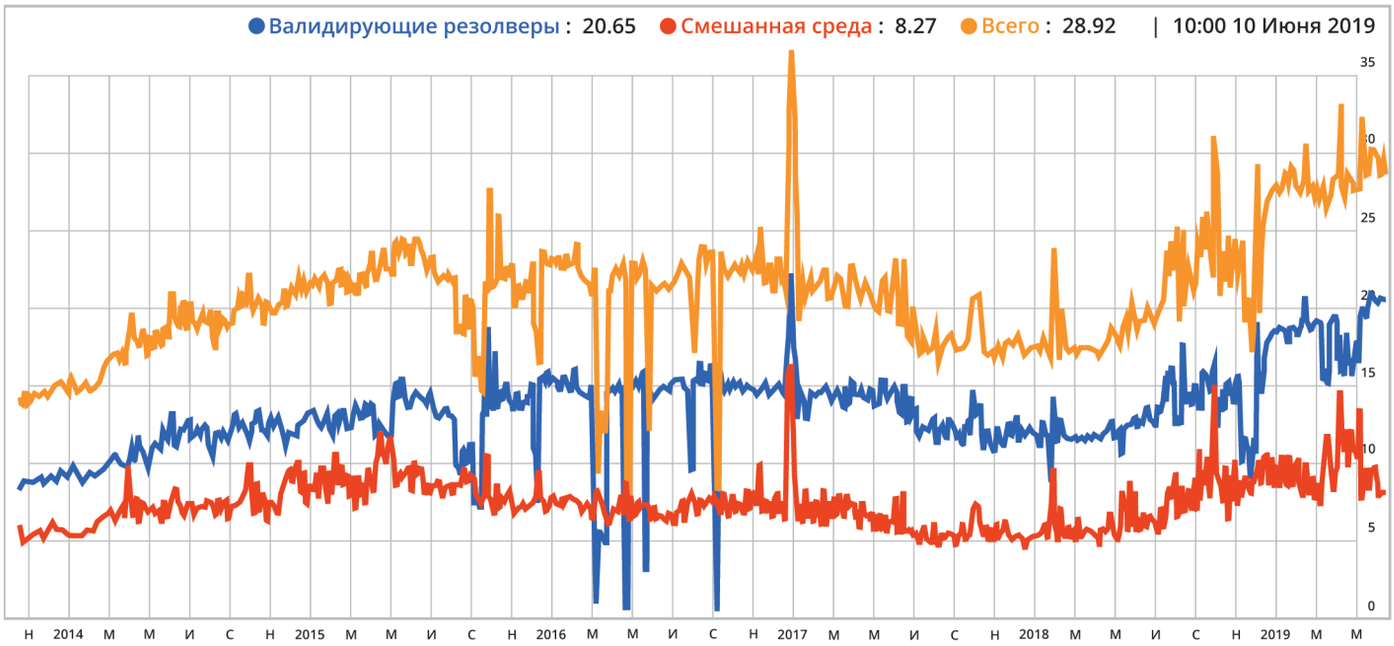
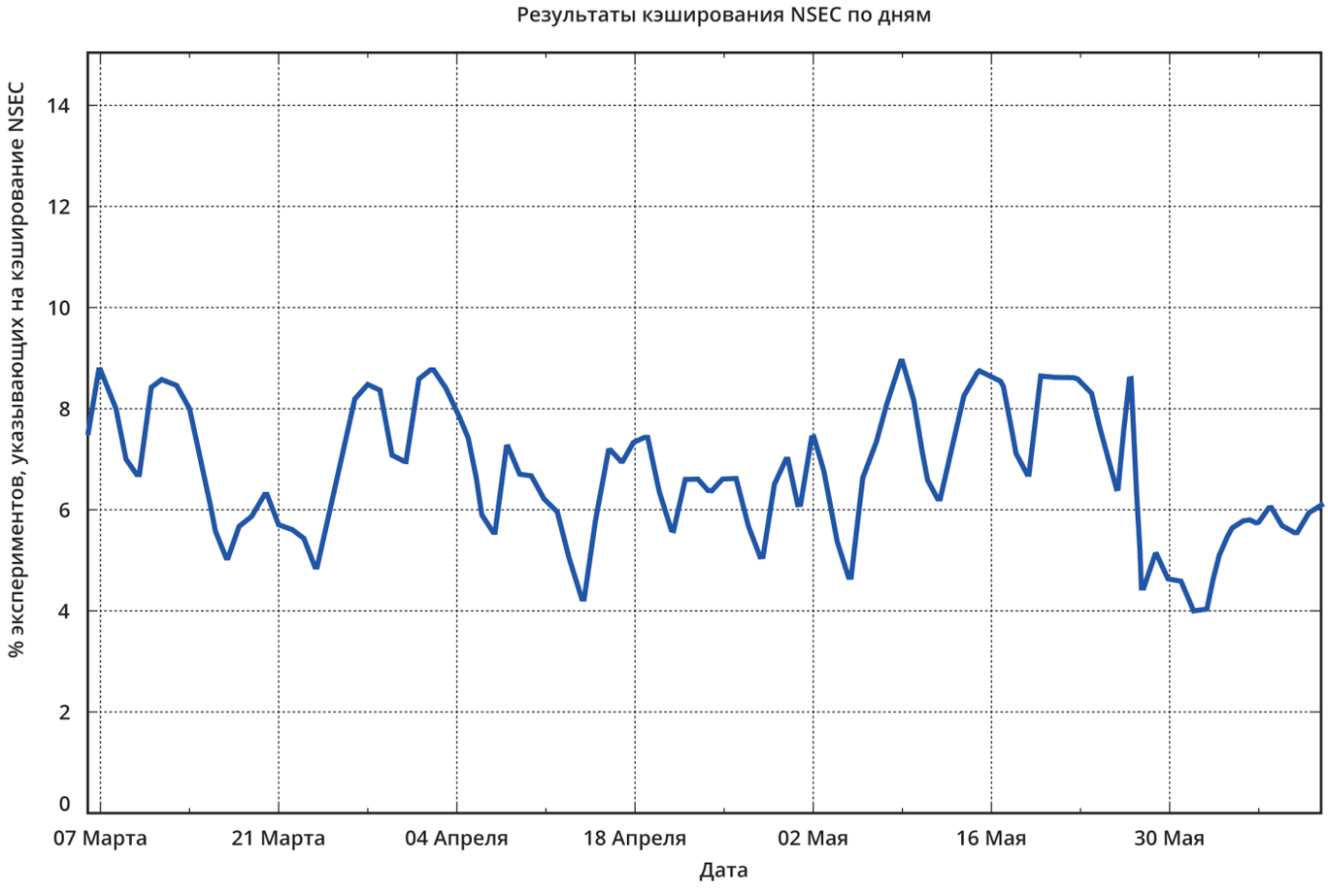


Рис. 3. Процент экспериментов, указывающих на кэширование NSEC, по дням.



А может быть, наши выводы тоже ошибочны, поскольку в DNS все всегда не так и не то, чем кажется.

Балансировщики нагрузки резолверов и кэширование NSEC

Недостатком использованной нами модели DNS было предположение, что резолвер DNS является одиночной машиной DNS. В наши дни это скорее редкость, поскольку структура рекурсивного резолвера обычно построена как «ферма» машин-резолверов DNS.

Каждый день эти три миллиона измерений передавали запросы DNS где-то к 100 тысячам рекурсивных резолверов, которые, как мы видели, опрашивали авторитетные серверы. За 98 дней мы наблюдали 559 357 различных IP-адресов рекурсивных резолверов: этого и следовало ожидать от длинного конца распределения рекурсивных резолверов в Интернете.

Если сгруппировать эти резолверы по подсетям IPv4 или IPv6 (соответственно /24 или /48), мы насчитаем только 295 546 различных подсетей резолверов. Больше половины резолверов, а точнее, 347 302, если считать по IP-адресам, находятся в общей подсети с другим резолвером или несколькими. Весьма вероятно, что это компоненты фермы. Во многих фермах рекурсивных резолверов применяется техника распределенной балансировки нагрузки, при которой несколько машин-резолверов скрываются за одним сервисным адресом, обращенным к клиенту. Так можно построить масштабируемую систему рекурсивных резолверов DNS, добавляя новые машины для того, чтобы справляться с пиками нагрузки на сервис рекурсивного преобразования.

Как в этих фермах распределяется нагрузка? Цикл и иные простые формы распределения запросов могут привести к плохой производительности системы, особенно в части управления кэшем, но в то же время дают лучшую балансировку нагрузки для определенных паттернов запросов. Говоря более общо, каждая машина для рекурсивного преобразования вынуждена поддерживать и заполнять собственный кэш имен, а последовательность запросов на одно и то же имя может попасть к разным машинам, что сведет к нулю эффективность любого кэша на отдельной машине, если распределение основано на относительной загрузке текущей машины по всем компонентам фермы.

Общепринятый подход к распределению потока запросов – хешировать имя запроса и адресовать запросы на одно и то же имя одной и той же машине. При таком подходе у каждой машины формируется систематический кэш запрашиваемых имен, а вся конструкция может быть очень эффективно настроена. Хеширование имен работает и для имен, «определенных» в DNS (т.е. ответы DNS кэшируются каждый раз на той же самой машине), и для «неопределенных» имен (статус «имя не существует» тоже каждый раз кэшируется на той же самой машине).

А что с кэшированием NSEC и нашим экспериментом NSEC?

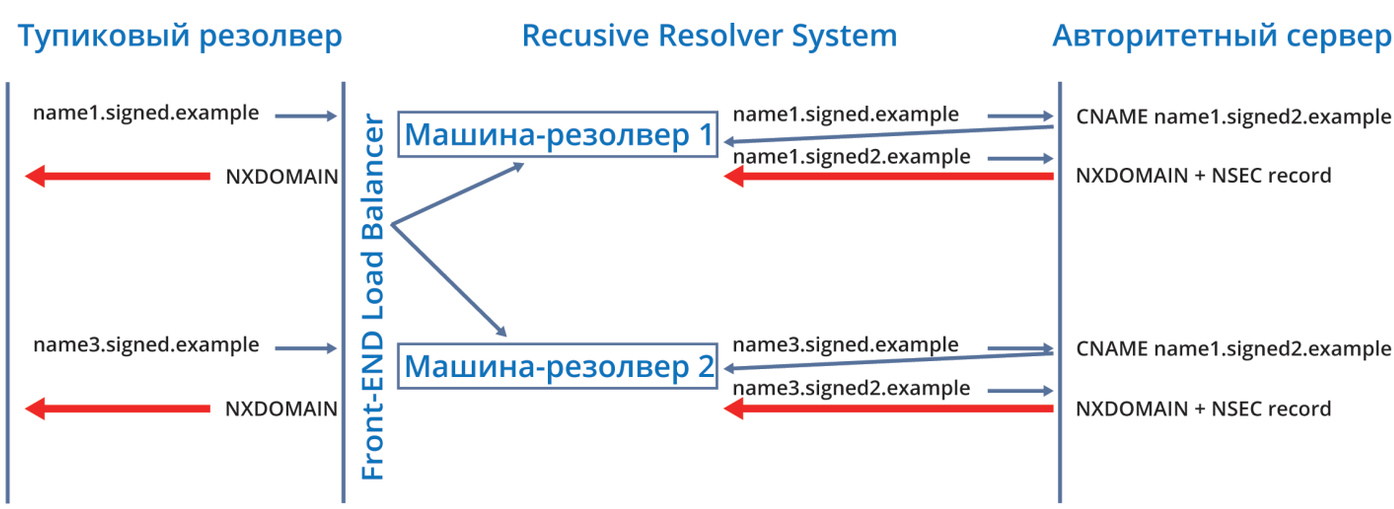
В эксперименте мы используем два различных имени для запросов: первый запрос служит для того, чтобы загрузить в рекурсивный резолвер ответ NSEC, а второй – чтобы попытаться попасть в диапазон имен, определенный кэшированной записью NSEC из первого запроса и увидеть смысл кэширования NSEC.

Что случится, если два этих имени попадут на две разных машины, входящих в кластер резолверов? Оба запроса станут попаданиями мимо кэша и дойдут до авторитетного сервера, пусть и с разных резолверов. А мы, увидев запросы к авторитетному серверу, сделаем вывод, что кэширование NSEC не используется – и, возможно, ошибемся (см. рис. 4).

Как в более общем виде взаимодействуют балансировщики нагрузки резолверов и кэширование NSEC?

У вопросов о DNS, заданных в таком виде, обычно не бывает четкого «черно-белого» ответа, и наш случай – не исключение: тут тоже однозначного ответа не дашь. Для корневой зоны каждая машина-резолвер быстро набирает полный набор записей из ответов NSEC. Но если зона используется не так часто, запросы «на наполнение кэша» с ответами NSEC могут оказаться распределены по всей ферме, а потому не дать крупного выигрыша от кэширования NSEC. Возможно, неожиданно низкий результат

Рис. 4. Балансировщики нагрузки по хешам имен запросов и кэширование NSEC на «фермах» резолверов.



нашего эксперимента по наблюдению за кэшированием NSEC в какой-то степени объясняется несоответствием между хешированием запрашиваемых имен для балансировки нагрузки на ферму и тем, что запросы NSEC охватывали довольно редко опрашиваемый диапазон имен.

В обычной ситуации при опросе имен, невысоко стоящих в иерархии DNS, кэширование NSEC может не дать ощутимого эффекта в плане нагрузки на авторитетные серверы. Кроме того, чем ниже количество запросов, тем ниже эффективность кэширования NSEC. Этим объясняется и снижение процента кэширования NSEC, которое мы наблюдали, когда самих экспериментов стало меньше.

Однако наш сценарий – редкие спорадические запросы – не та ситуация, в которой кэширование NSEC призвано дать значительную выгоду. Если на серверы зоны идет масштабная атака случайными именами, то сочетание большого числа запросов и хеширующего балансировщика нагрузки приведет к тому, что все машины в составе фермы быстро «выучат» все содержимое зоны, после чего рекурсивные резолверы смогут гасить атаки с помощью кэширования NSEC.

Проверка сценария атаки звучит как увлекательное продолжение нашего эксперимента: можно проанализировать уровни интенсивности запросов и их воздействие на эффективность кэширования на фермах резолверов. Но в наши задачи не входит развертывание DNS-атаки с использованием случайных имен на базе нашей измерительной платформы, даже если объектами атаки станут наши собственные серверы – поэтому мы не сможем измерить эффективность кэширования NSEC в более жестких условиях на реальном Интернете. Возможно, такие вещи лучше изучать методом моделирования.

Источник: «Looking for What's Not There», https://www.potaroo.net/isp-col/2019-06/nsec-cache.html

Выводы

Кэшировать NSEC на рекурсивных резолверах, пожалуй, имеет смысл. Если рекурсивный резолвер уже выполняет проверку DNSSEC, то для него не будет большой разницы в том, чтобы кэшировать диапазоны записей NSEC вместо имен запросов. Нагрузка на рекурсивный резолвер вроде бы не должна вырасти, а с другой стороны, появится возможность повысить эффективность кэширования.

Однако если в этом и заключается весь эффект, то можно вспомнить аргумент о «верблюде DNS». Да, возможно, мы сумеем чуть-чуть повысить общую эффективность работы DNS, но ценой добавления еще одной программной функции, которой нужно управлять, а стоимость пожизненной возни с дополнительным функционалом в коде преобразования DNS все-таки ненулевая для каждой такой дополнительной функции. Так стоит ли овчинка выделки?

С другой стороны, мы вообще мало что можем противопоставить DNS-атакам с использованием случайных имен. Такие атаки могут быть чрезвычайно просты в развертывании, и, как мы видели по предыдущим атакам такого типа, достаточно большая армия ботов позволяет очень просто и легко обрушить DNS-инфраструктуру Интернета. В нынешней среде DNS стала очень концентрированной службой, где считанное количество авторитетных серверов имен обслуживает большой набор имен DNS, связанных с популярными сервисами. Эффективная атака всего лишь на одного оператора подобной службы, как мы видели в октябре 2016 года на примере DYN, может оказаться исключительно действенной. В таком сценарии кэширование NSEC может пригодиться. Возможно, перекрытие значительной уязвимости в инфраструктуре DNS стоит всевозрастающих затрат на очередное дополнение к функции преобразования DNS.

DNS как источник глобальной информации о Сети

Александр Венедюхин, ФРСТ «ИнДата»

Система доменных имён DNS и соответствующий ей сервис, обеспечивающий поиск, является частью фундаментальной инфраструктуры Интернета. Практически любое обращение к сервисам Интернета, будь то посещение веб-сайта, отправка электронной почты, сообщение мессенджера или открытие приложения на смартфоне, начинается с запроса к этой системе. А раз так – DNS представляет собой богатый источник данных для самых разных измерений в глобальной Сети.

Введение

Предполагая, что читатель уже знаком с DNS, вспомним только некоторые технические аспекты, которые лежат в основе измерений Сети, проводимых при помощи DNS.

Так, упомянутые выше роли DNS (система и сервис) позволяют рассматривать Сеть под разными углами: как с точки зрения инфраструктуры адресации, так и с точки зрения доступа конечного пользователя к узлам и ресурсам, адресуемым доменными именами.

Инфраструктура адресации, применительно к DNS, это иерархия имён, заданная на множестве авторитативных серверов. Авторитативным (иногда также используют русскоязычный термин «авторитетный») называется сервер имён, который уполномочен отвечать на запросы об адресации внутри той или иной доменной зоны, то есть пространства имён. Такие «полномочия» у сервера возникают из его отношений с другими авторитативными серверами DNS, в рамках операции делегирования, позволяющей одним авторитативным серверам делегировать другим авторитативным серверам управление подмножеством имён в своей зоне ответственности. Например, сервер A, отвечающий за доменную зону второго уровня test.ru, может делегировать зону третьего уровня name.test.ru серверу C. В таком случае для поиска DNS-записи с именем внутри name.test.ru, например, для long.name.test.ru, резолверу потребуется обратиться к серверу C.

Как **сервис поиска**, DNS решает задачу обнаружения в иерархии записей по известному ключу некоторого значения. Этот процесс принято называть рекурсивным резолвингом (англ. resolve, resolving). Чаще всего в пример приводят один из самых распространённых сценариев использования DNS: определение IP-адреса, соответствующего имени узла, или, в технических терминах, поиск адресной записи (A-записи или AAAA-записи) для имени хоста. Здесь ключом является символьное имя, например, google.com, а значением - IP-адрес, извлечённый из адресной записи. Для DNS важна возможность установить, что искомой DNS-записи в системе не задано. Это состояние в DNS отличается от состояния, когда запись по каким-то причинам *не удалось найти*. Подтверждённое отсутствие записи для заданного имени является одним из эффективных инструментов измерения, который позволяет, например, изучать те или иные сервисы, работающие в Сети.

Фундаментальным свойством DNS, со всех точек зрения, является кеширование значений DNS-записей. Именно кеширование делает данную систему распределённой и очень устойчивой. Само по себе кеширование не оказывает влияния на содержание DNS-записей, однако метод управления временем кеширования, использующий поля со значением TTL (Time To Live), может являться источником содержательной статистики. В частности, анализ значений TTL, передаваемых авторитативными серверами для разных DNS-записей и разных DNS-имён, позволяет исследовать настройки CDN и механизмов балансировки нагрузки.

Информация об инфраструктуре

Процессу делегирования в DNS соответствуют NS-записи. NS-запись содержит перечень имён серверов (авторитативных), которые должны отвечать на запросы о записях в данной зоне. Другими словами, NS-записи содержат

списки «главных» серверов и позволяют сопоставить перечень NS каждой делегированной зоне. Делегирование начинается от корневого домена (он обозначается «пустым именем» или просто точкой, часто обозначение корневого домена просто опускают). На первом уровне делегирования находятся домены верхнего уровня: com., net., org., ru., su. и др. Второй уровень, соответственно, это всем привычные домены вида google.com., ididb.ru. и т. д. При рекурсивном поиске записей резолвер получает перечень серверов имён, которые могут предоставить ответ на искомый запрос. Если какая-то доменная зона опубликована в DNS, то ей должны соответствовать те или иные NS-записи (точнее, для этой зоны должно быть возможно обнаружить авторитативные серверы). При этом процесс регистрации доменного имени не обязательно связан с делегированием этого имени. Имя может быть зарегистрировано, но при этом быть недоступно в DNS. В таком случае говорят, что домен не делегирован. Итак, данные о делегировании доступны в глобальной DNS, а для корректно делегированных доменов всегда возможно получить некоторый набор имён авторитативных серверов: он возвращается серверами, находящимися уровнем выше, в ответ на DNS-запрос. Например, перечень авторитативных серверов для домена test.ru можно получить в ответ на запрос к авторитативным серверам домена ru. Это и есть базовый шаг алгоритма сбора сведений из DNS.

Система доменных имён (DNS — Domain Name System) и соответствующий ей сервис, обеспечивающий поиск записей (его тоже обозначают DNS, но только последняя буква обозначает Service), являются богатым источником исходных сведений для самых разных измерений в глобальной Сети.

Сбор сведений выполняется силами рекурсивного DNS-резолвера. Иногда это специально настроенный для решения конкретных задач сбора данных резолвер, на входе у которого обычно список делегированных имён. Для зон верхнего уровня этот список можно получить различными способами, в зависимости от действующих политик. Например, для «новых доменов» верхнего уровня (New gTLD) ICANN поддерживает центральный сервис Centralized Zone Data Service (https://czds.icann.org/), предоставляющий единый интерфейс для доступа к спискам имён.

Сведения о делегировании являются источником важной информации о распределении имён, об административном делении доменного адресного пространства. Во многих случаях доменные имена делегируются на авторитативные серверы, принадлежащие провайдеру хостинга или доменному регистратору.

Как эти данные используются? Возьмём список делегированных имён второго уровня в домене ru. Для каждого имени получим список авторитативных DNS-серверов (это ответ на запрос NS-записей). Агрегируем полученные ответы по уникальным именам DNS-серверов и посчитаем количество имён, делегированных на каждый из авторитативных серверов - результат отражает распределение имён по различным провайдерам DNS-сервисов. Уже такая элементарная статистика позволяет получить следующие сведения:

- общее количество различных (по именам) авторитативных серверов. Этот показатель часто удивляет неспециалистов: например, в зоне ru делегировано около 4,7 миллиона зон (август 2019), при этом различных имён авторитативных серверов — лишь около 130 тысяч;
- рейтинг провайдеров: у каких провайдеров большое количество доменных зон на обслуживании (по именам DNS-серверов, которые можно сопоставить с провайдерами). Обычно лидерами такого рейтинга оказываются провайдеры бесплатного DNS-хостинга, регистраторы доменов и хостеры, а также крупные доменные парковки. Если дополнительно отобразить имена авторитативных серверов в IP-адреса и распределить их по автономным системам (AS), то получим рейтинг AS по числу размещённых доменных зон, таким способом, например, можно увидеть услуги DNS-хостинга типа White-label, когда имена серверов соответствуют одному провайдеру, но физически сервис предоставляется другим.
- «степень разнообразия» серверов имён: какая доля от всех делегированных зон размещена на наиболее популярных авторитативных серверах (по именам). Например, в зоне ru около 30% имен второго уровня сосредоточены на серверах трёх-пяти крупных провайдеров, каждый из которых поддерживает сотни тысяч зон.

Интересно, что наличие имён авторитативных серверов в делегирующей зоне вовсе не означает, что указанные серверы действительно обслуживают делегированное имя. Более того, в некоторых случаях под указанным именем вовсе нет доступного DNS-сервера. «Дефектное имя» в делегирующей зоне может появиться из-за ошибки (простой опечатки), а также и по другим причинам.

DNS повсеместно используется для публикации адресов и другой информации, связанной с теми или иными сервисами, работающими под данным доменным именем. Самым важным и распространённым, конечно, является веб-сервис, использующий для адресации A- и AAAA-записи. Как известно, эти записи содержат IP-адреса, v4 и v6 соответственно. Раньше типовым способом публикации адреса веб-сервиса (веб-узла) являлось использование поддомена (префикса) www., например, вот так: www.example.com. Сейчас данная практика перестала быть повсеместной и веб-сервис обычно доступен по «базовому» имени: example.com. Нередко поддомен www. сохраняется в качестве синонима либо с www. выполняется HTTP-редирект на имя без этого префикса; возможна, впрочем, и обратная ситуация: так, google.com перенаправляет веб-запросы на www.google.com, аналогичным образом поступает и facebook.com. Тем не менее, общепринятый сейчас вариант — перенаправление с www. на имя без специального префикса. Это пример того, что уже алгоритм использования префикса www. администраторами доменных зон позволяет собирать сведения о том, как настроена адресация веб-сервиса для данного имени.

Нужно заметить, что A- или AAAA-записи вовсе не являются специально предназначенными для адресации веб-узлов, они несут только IP-адреса, без привязки к одному конкретному сервису. Например, эти записи могут адресовать почтовые серверы, авторитативные DNS-серверы, а также и любые другие. Тем не менее, в современном Интернете использование записей этого типа для адресации веб-узлов является очень распространённым сценарием. Анализ значений A- и AAAA-записей даёт много информации об инфраструктуре Сети:

- наличие AAAA-записей позволяет сделать предположение об IPv6-коннективности узла, адресуемого исследуемой зоной;
- IP-адреса можно сопоставить с номерами автономных систем, получив, таким образом, проекцию доменного пространства в административную структуру, то есть можно определить, у каких провайдеров хостинга размещены веб-узлы, адресуемые различными именами, или почтовые серверы;
- подсчёт «разнообразия» используемых IP-адресов позволяет определить, насколько доменные имена сконцентрированы на тех или иных узлах. Например, в случае веба один и тот же IP-адрес в A-записи нередко соответствует тысячам и десяткам тысяч имён.

Так как адресные (A-, AAAA-) записи позволяют сопоставить доменным именам IP-адреса, можно с их помощью исследовать BGP-маршруты, связанные с теми или иными доменными кластерами. Например, можно увидеть особенности маршрутизации различных CDN или обнаружить транзитные автономные системы, через которые проходит много трафика электронной почты.

Записи, размещаемые в DNS, сейчас довольно разнообразны. Практически все они служат источником интересной информации, если анализируются на достаточно большой выборке. Свежий пример: не так давно появилась технология ESNI (Encrypted Server Name Indication), позволяющая скрыть имя сервера, с которым клиент устанавливает TLS-соединение. Пока что (август 2019) эта технология имеет статус проекта (draft), но уже поддерживается браузером Mozilla Firefox на стороне клиента, а на стороне сервера - одним из крупнейших CDN-провайдеров: Cloudflare. ESNI существенным образом использует DNS — в доменной зоне публикуются криптографические ключи. Поэтому сканирование доменного пространства на предмет ESNI-записей позволяет обнаружить узлы, которые (потенциально) реализуют защищённую передачу имени сервера. При этом оказывается, что почти 100% таких узлов, адресуемых именами в домене .ru, размещены в сетях Cloudflare. Более того, они используют небольшое количество криптографических ключей, то есть многие узлы используют один и тот же ключ (это не является какой-то уязвимостью и полностью допускается спецификацией). Все эти сведения обнаруживаются при помощи анализа DNS-записей. А наличие ESNI-ключей является маркером, обнаружить который можно только при помощи сканирования DNS, несмотря на то что сама технология применима к TLS (защищённому протоколу обмена данными на базе TCP, который DNS не использует).

Отдельный интерес представляет DNSSEC — механизм защиты адресной информации, публикуемой в DNS. С данной технологией связаны специальные DNS-записи, которые позволяют опубликовать электронные подписи, удостоверяющие данные DNS, а также ключи, необходимые для проверки подписей. DNSSEC пока что используется очень редко, тем не менее, позволяет обнаружить безопасные (то есть удостоверенные) зоны, выявить зоны, настроенные с ошибками, классифицировать эти ошибки. Также полезной оказывается статистика используемых криптографических ключей и криптосистем. Например, исследование записей, относящихся к DNSSEC, позволяет обнаружить доменные зоны, которые были некорректно перенесены от одного провайдера DNS-хостинга к другому.

Отметим, что DNS также широко используется для хранения информации о соответствии IP-адресов именам хостов, то есть ключом в этом случае является IP-адрес. Выполнение этой функции обеспечивают так называемые обратные зоны. С их помощью можно определить символьное имя узла, зная только его IP-адрес (конечно, лишь в том случае, если соответствующая запись есть в обратной зоне). Этот инструмент применяется, например, в процессе доставки электронной почты - в качестве источника дополнительного признака «подлинности» узла-источника сообщения. Аналогичную роль обратные зоны играют в процессе авторизации удалённого пользователя SSH-серверами. С точки зрения исследований Интернета, обратные зоны позволяют получить информацию о том, как распределены площадки хостинга по провайдерам, в каких случаях для веб-узлов обратные зоны настроены в соответствии с прямыми, а в каких — нет (например, при размещении множества веб-узлов на общем IP-адресе).

В таблицах 1, 2 и 3 приведены некоторые данные, полученные путем измерения DNS.

Таблица 1. Top-20 автономных систем*.

N	Автономная система	as-name	Количество ресурсов	Страна
1	AS197695	AS-REGRU	382 612	RU
2	AS198610	BEGET-AS	344 636	RU
3	AS9123	TimeWeb-AS	221 940	RU
4	AS24940	HETZNER-AS	145 501	DE
5	AS8342	RTCOMM-AS	123 531	RU
6	AS48287	RU-CENTER	111 836	RU
7	AS29182	THEFIRST-AS	105 867	RU
8	AS13335	CLOUDFLARENET-AS	92 012	AU
9	AS44112	SWEB-AS	83 509	RU
10	AS203226	IHCRU	69 897	RU
11	AS50245	SERVEREL-AS	69 509	CZ
12	AS25532	MASTERHOST-AS	59 717	RU
13	AS50340	SELECTEL-MSK	57 583	RU
14	AS35278	SPRINTHOST	53 030	RU
15	AS49505	SELECTEL	50 085	RU
16	AS60357	MEGAGROUP-AS	49 278	RU
17	AS62082	HOSTLAND	48 886	RU
18	AS16276	OVH	47 467	CA
19	AS43362	MAJORDOMO	42 525	RU
20	AS64432	VARITI-AS	41 614	CH

*— В данных системах размещены веб-ресурсы, адресуемые доменами .ru, .рф, .su. Рейтинг построен путём определения принадлежности блока IP-адресов из A-записей (июль 2019, источник: ididb.ru).

Таблица 2. Версии ПО.**

Указанная версия сервера	IP-адреса, Число
Всего	42 077
BIND RedHat	13 801
<other>	12 232
BIND generic	6785
BIND Debian	3427
PowerDNS	3010
BIND Ubuntu	2380
UltraDNS	222
NSD	220

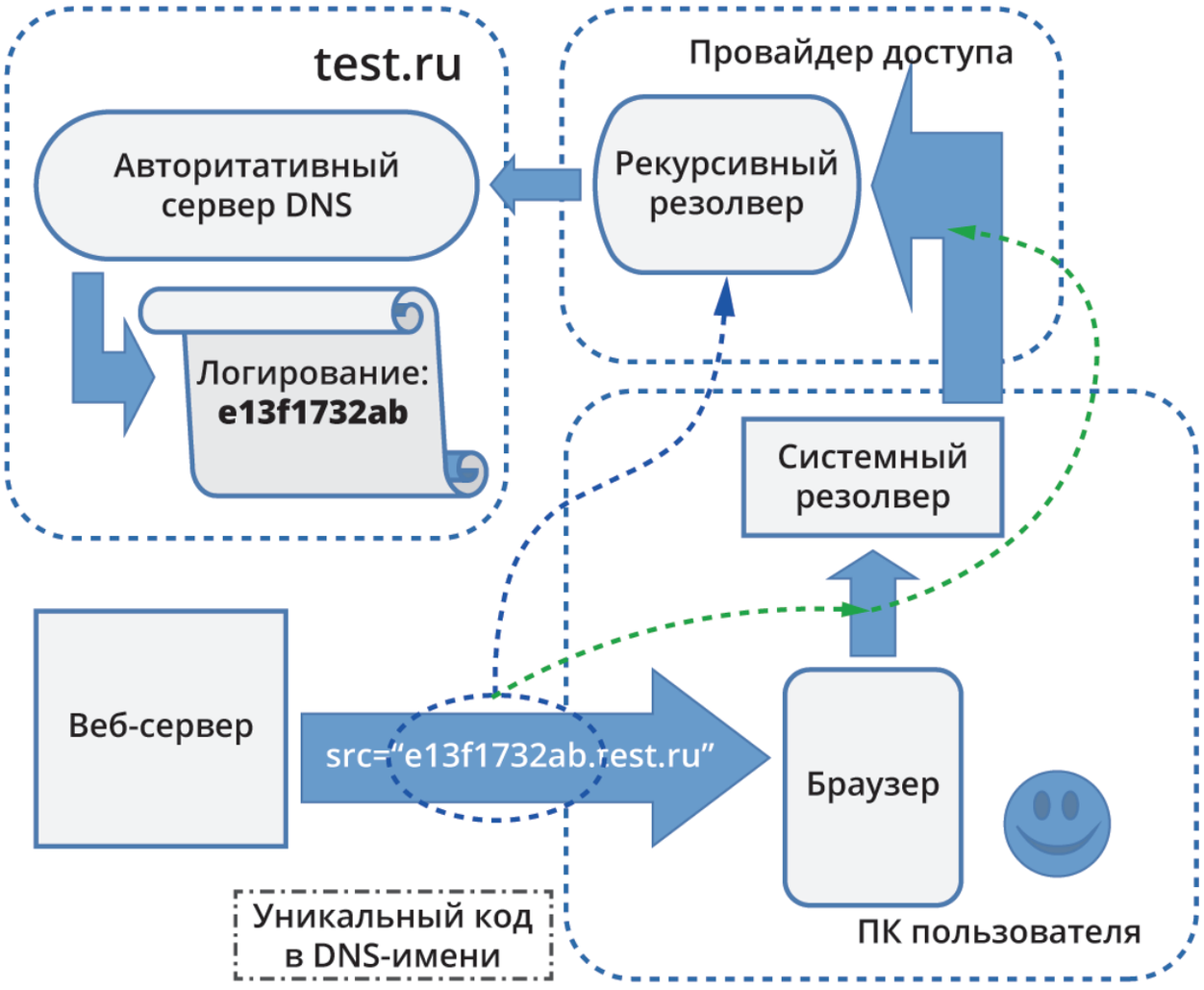
**— получены на основе анализа сигнатур в ответах авторитативных серверов имён для зоны .ru, по количеству уникальных IP-адресов (июль 2019, источник: statdom.ru)

Таблица 3. Количество уникальных IP-адресов*.**

	.ru	.su	.рф
Число уникальных IP веб-узлов	273 883	19 487	39126
Число уникальных IP TLS-узлов (HTTPS)	218 603	18 830	38721

***— полученны для веб-узлов и TLS-узлов на основе анализа DNS российских национальных TLD (июль 2019, источник: ididb.ru).

Рис. 1. Схема измерения пользовательских резолверов.



Прежде всего, создаётся специальная доменная зона, делегированная на лабораторные авторитативные серверы, которые и будут собирать данные.

Предположим, что это зона test.ru. Также настраивается веб-сервер, основная задача которого отправлять браузеру клиента код веб-страницы в составе ссылки на ресурс, специальное уникальное имя хоста, находящееся в зоне test.ru. (Сам веб-сервер может работать под адресом в любой другой зоне, это не важно.) Так как код веб-страницы ссылается на ресурс, расположенный в зоне test.ru., браузеру потребуется определить адрес (A- или AAAA-запись) для этого ресурса. Соответственно, браузер обратится к тому или иному резолверу, что, в конечном итоге, приведёт к отправке запросов к авторитативным серверам зоны test.ru. Авторитативные серверы зафиксируют источник запроса — его IP-адрес.

Отличить один запрос от другого авторитативный сервер может потому, что в составе запрашиваемого имени присутствует уникальная метка. Например, конкретное имя может выглядеть так: e13f1732ab.test.ru. Здесь крайняя слева подстрока является таким уникальным кодом. В веб-страницу соответствующий код может быть встроен в составе ссылки на изображение, например, так: . Остаётся только получить веб-трафик (это и есть «праймер»), то есть пользователи должны открыть веб-страницу браузером.

Клиентская сторона

Типичный сценарий использования DNS на стороне клиента сводится к взаимодействию прикладных программ с системным резолвером, а через него — с рекурсивным резолвером провайдера доступа (системный резолвер чрезвычайно редко является полноценным рекурсивным). Сейчас распространена ситуация, когда вместо резолвера, предоставляемого провайдером доступа, пользователи настраивают открытые рекурсивные резолверы крупных DNS-сервисов. Примерами таких сервисов являются Google Public DNS (известен как 8.8.8.8) и Cloudflare DNS (1.1.1.1). В ряде случаев использование подобных «внешних» сервисов резолвинга прямо поддерживается прикладной программой. Например, современные версии браузера Mozilla Firefox могут непосредственно обращаться к такому резолверу, минуя системный (для этого используется протокол DNS-over-HTTPS).

Рекурсивный резолвер, обслуживающий того или иного пользователя, в общем случае определить не так просто. Сканирование адресного пространства, подобное тому, которое используется при анализе доменных зон, но только в отношении IP, не даёт нужного результата по двум основным причинам: во-первых, провайдерские рекурсивные резолверы обычно закрыты для доступа из других сетей, поэтому не видны снаружи; во-вторых, даже если список резолверов удалось построить, то это не означает, что тот или иной пользователь настроил в своей системе именно этот резолвер. Таким образом, измерение клиентских резолверов и их характеристик (например, типичного времени ответа, настроек кеширования) представляет собой отдельную интересную задачу.

Обнаружить и измерить клиентские рекурсивные резолверы возможно, так как они обращаются к авторитативным DNS-серверам. Одним из эффективных способов измерения является использование в качестве «праймера» того или иного дополнительного интернет-сервиса, обычно это веб.

Как работает данный метод? Принцип работы и схема этого метода приведена на рисунке 1.

Получив тестовые запросы резолверов, используя различные алгоритмы формирования меток в исходных запросах, возможно проводить следующие измерения:

- распределение трафика DNS-запросов по провайдерам (в том числе, по провайдерам сервисов DNS-резолвинга);
- настройки времени кеширования резолверов;
- поддержка DNSSEC, в том числе, наличие валидации;
- время, затрачиваемое рекурсивным резолвером на получение ответа;
- географическое распределение резолверов, настройки внутренней балансировки для крупных провайдеров резолвинга.

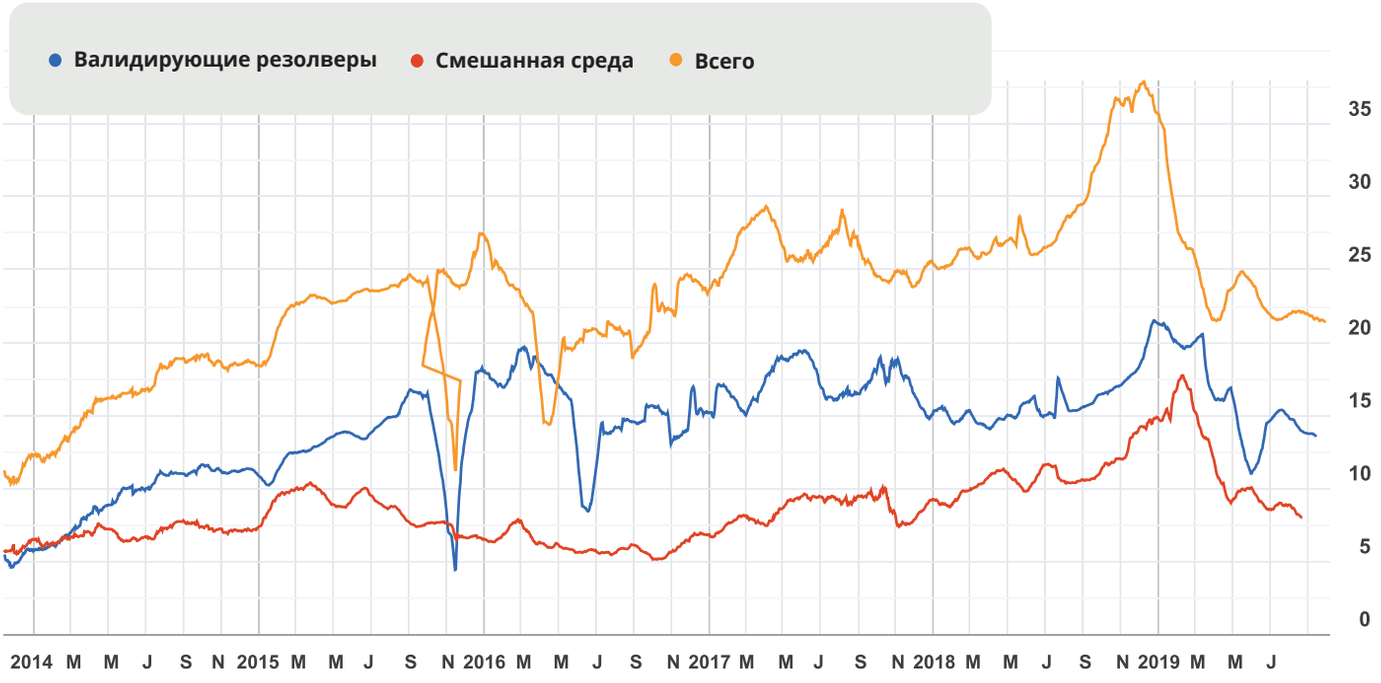
Выводы

DNS, как и тридцать лет назад, является всеобъемлющей для глобальной Сети технологией. Так как типичные сценарии работы с Сетью обычного пользователя всегда включают явное и неявное обращение к DNS, имена хостов и состав доменных зон, сам сервис доменных имён служат богатым источником информации для исследований Интернета в целом.

РОСТ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА (% НАСЕЛЕНИЯ, СРЕДНИЙ ПО РЕГИОНУ)

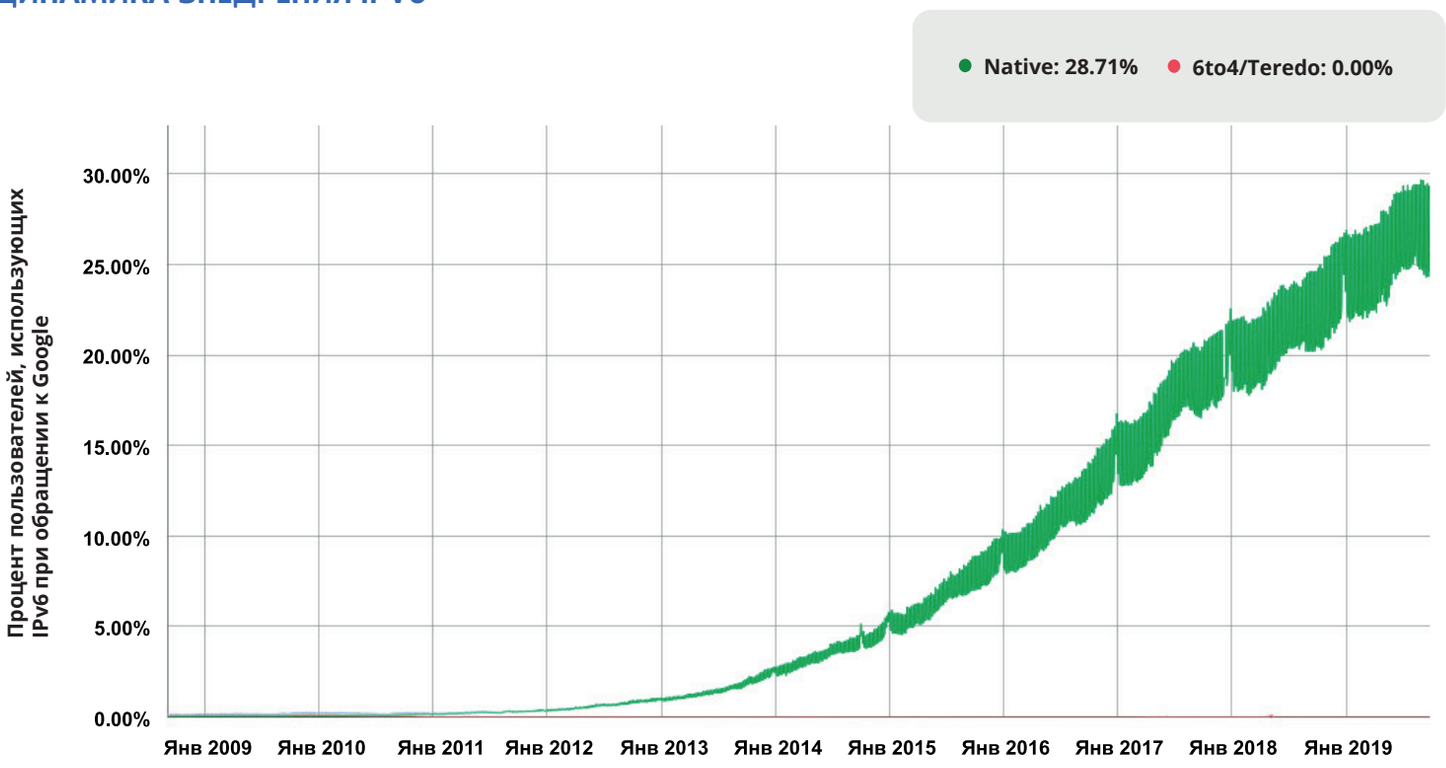
Источник: https://public.tableau.com/profile/rohit.sinha5535#!/vizhome/Internet_15664048302500/Dashboard1

ИСПОЛЬЗОВЫВАНИЕ ВАЛИДАЦИИ ОТВЕТОВ DNS В РОССИИ



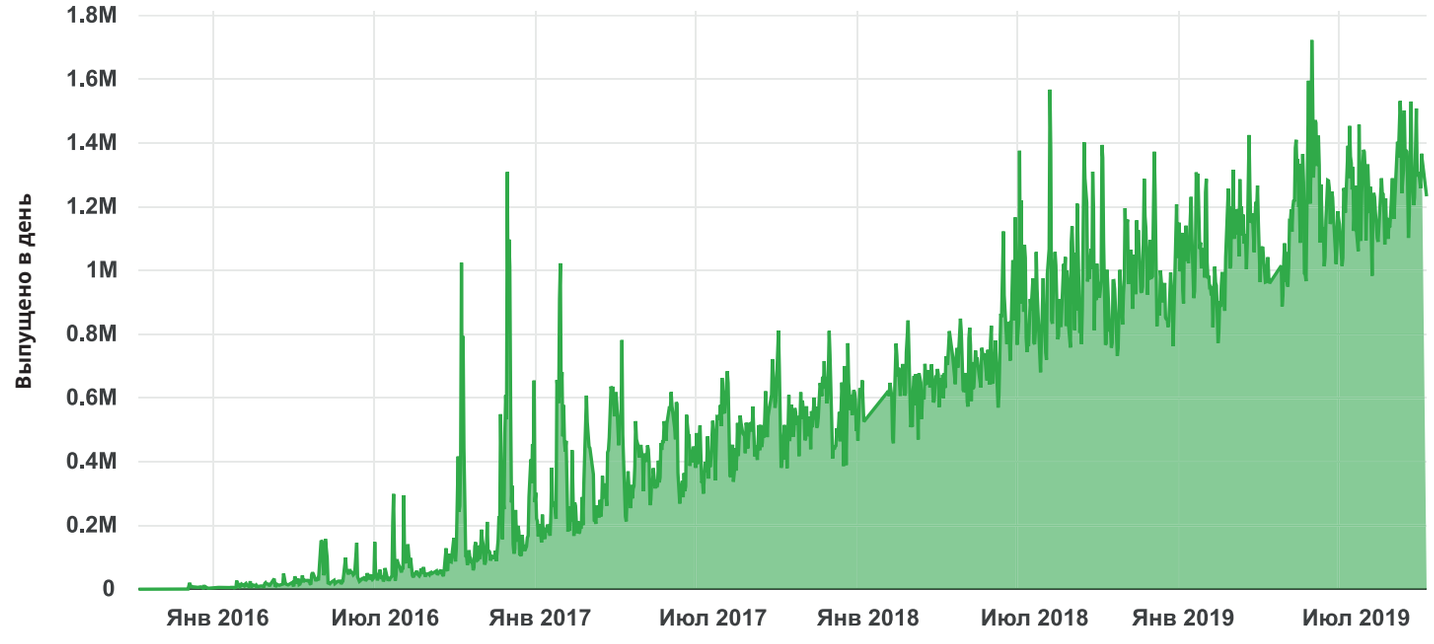
Источник: https://stats.labs.apnic.net/dnssec/RU

ДИНАМИКА ВНЕДРЕНИЯ IPV6



Источник: https://www.google.com/intl/en/ipv6/statistics.html

КОЛИЧЕСТВО СЕРТИФИКАТОВ LET'S ENCRYPT, ВЫПУЩЕННЫХ ЕЖЕДНЕВНО



Источник: https://letsencrypt.org/stats/#daily-issuance

DoH, или DNS, похожий на веб

Андрей Робачевский

Защита личных данных и конфиденциальности информации в Интернете является важной и в то же время сложной задачей. Но кто бы мог подумать, что разработчики, пользователи и операторы DNS – системы трансляции имен в Интернете – будут озабочены этой проблемой? Шифрование данных – одно из стандартных решений конфиденциальности, но как и что шифровать в DNS? В этой статье речь пойдет о новом протоколе защиты данных и особенно метаданных DNS - «DNS over HTTPS». Несмотря на то, что стандарту меньше года, он уже прошел интенсивную стадию экспериментирования и активно внедряется ведущими разработчиками браузеров. До сих пор не утихают споры, что означает внедрение централизованного DoH для безопасности и конфиденциальности данных пользователей. Но может быть DoH – это знак нового эволюционного витка развития DNS и Интернета в целом?

Все началось с разоблачений Эдварда Сноудена. IETF встал на тропу войны и объявил всеобщий мониторинг трафика в Интернете ничем иным как технической атакой[1]. А раз так, то борьба с ней должна осуществляться техническими средствами, путем усиления безопасности протоколов IETF. Основным методом для этого явилось шифрование.

Наиболее заметен прогресс в области шифрования веб-трафика. Если в начале 2014 года (когда был опубликован RFC7258) процент трафика HTTPS к сайтам Google составлял около 50%, то сегодня он равен 94%. Процент загруженных страниц с использованием HTTPS по различным оценкам сегодня составляет 80-90%[2] (см. рис.1).

Само шифрование также было усилено – TLS 1.3, являющийся основой различных протоколов приложений, как, например, тот же HTTPS, получил возможность использования эфемерных сеансовых ключей, существенно затрудняющую мониторинг трафика не только в большом Интернете, но и в корпоративных сетях. В отношении последних шифрование и, в частности, новые протоколы, такие как TLS 1.3., усложнили, а подчас сделали невозможным использование решений сетевой безопасности – экранов безопасности (firewalls) и систем обнаружения вторжений (Intrusion Detection Systems, IDS). См., например, «TLS 1.3 Impact on Network-Based Security»[3].

Несомненно, развитие в этом направлении сделало использование Интернета более защищенным, как в плане целостности передаваемых данных, так и в их конфиденциальности. Правда, остаются так называемые метаданные, например, IP-адреса отправителя и получателя, тип используемого приложения (порт), а также некоторая другая информация, например, SNI (Server Name Indication), указывающая на имя сервера, с которым устанавливается связь. В отношении SNI в IETF ведется работа по шифрованию и этого поля, т.н. Encrypted SNI[4].

Но что такое SNI по сравнению с информацией, которую можно получить, имея доступ к DNS! Каждое обращение к новому ресурсу начинается с запроса к этой глобальной «телефонной книге» и, соответственно, онлайн-поведение пользователя можно четко отследить по его обращениям к DNS. Великолепный инструмент тотальной слежки.

Проблема с конфиденциальностью в DNS заключается в том, что эта система представляет собой распределенную базу данных, отдельные компоненты которой обслуживаются различными организациями. Поэтому для получения интересующего нас ответа, например, IP-адреса сервера www.example.com, наш запрос будет обрабатываться несколькими организациями, не имеющими отношения к интересующему нас ресурсу. В наиболее часто применяемой модели одной из таких организаций будет оператор рекурсивного резолвера, чаще всего Интернет сервис-провайдер пользователя, а другими – операторы корневых серверов (в общем случае запрос начинается именно здесь) и оператор домена .com. Добавим к этому, что конфиденциальность данных до недавнего времени не считалась проблемой – в конце концов, вся эта информация является публично доступной - чтобы представить масштаб задачи.

Ну если мы не можем зашифровать данные самого DNS[5], можно ли хотя бы защитить от посторонних глаз обмен информацией между пользователем и резолвером и между резолвером и авторитетными серверами? Первая задача кажется вполне решаемой, и именно с этого IETF начал свою работу в рамках рабочей группы DPRIV.

Одним из решений, разработанных этой группой, явился DoT, или DNS over TLS. Этот протокол документирован в RFC7858[6] и как подсказывает название, использует протокол безопасности транспортного уровня (TLS) для шифрования связи между клиентом и сервером, а также для аутентификации сервера. Подобно тому, как TLS используется для защиты сеансов HTTP и обеспечения некоторой гарантии того, что сервер авторизован владельцем размещенного на нем информационного ресурса, этот протокол также можно использовать в контексте DNS между пользователем (т.н. резолвером-заглушки, stub resolver) и выбранным им рекурсивным резолвером.

Хотя DoT сегодня реализован в программном обеспечении таких известных резолверов, как Unbound и Knot, вопрос внедрения остается проблемой. Немногие операторы резолверов предлагают эту возможность, да и поддержка и настройка DoT в клиентском ПО, особенно на мобильных устройствах, оставляет желать лучшего.

Как обычно, даже если решение проблемы существует, его внедрение представляет основную задачу. Особенно, если это требует совместных действий независимых сторон – операторов резолверов и пользователей с их клиентским ПО, - что является типичным в Интернете.

Однако, говоря о клиентском ПО, задумаемся – какое наиболее используемое приложение в Интернете сегодня? Конечно же веб, и даже если некоторые приложения маскируются как самостоятельные единицы, за кулисами они используют веб-протокол HTTPS. А раз HTTPS самый распространенный протокол приложений в Интернете, почему бы не использовать именно его для шифрования трафика DNS?

Ко всему прочему, используя HTTPS, мы получаем ряд преимуществ: этот протокол очень редко подлежит блокировке и поддерживает такие функции, как «кэширование, перенаправление, проксирование, аутентификация и сжатие».

И появился DoH – DNS over HTTPS.

Как работает DoH

DoH[7] позволяет клиенту инкапсулировать обмен сообщениями DNS в протокол HTTPS. Существует два возможных способа отправки данных - через запрос POST или GET. У каждого есть свои особенности и преимущества.

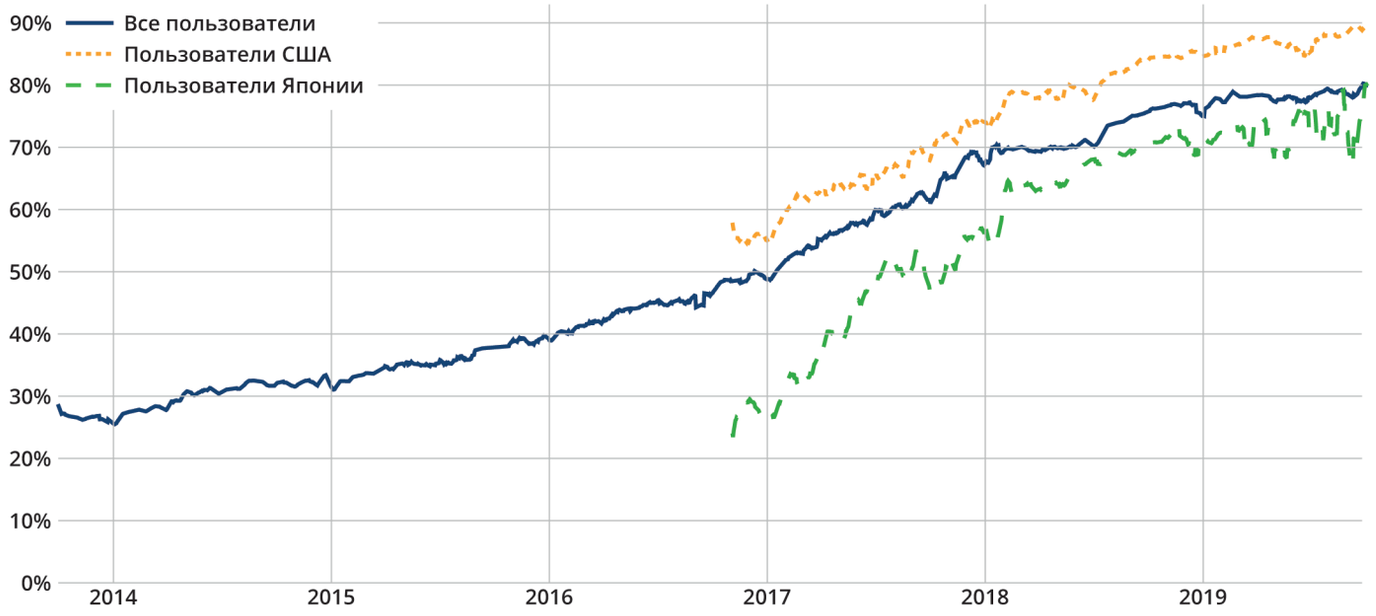
При отправлении запроса методом POST тип передаваемых данных (MIME заголовок Content-Type) определен как application/dns-message, а сам запрос передается без какого-либо кодирования – в «сыром» двоичном виде, начиная с заголовка DNS. Объем передаваемых данных в случае POST несколько меньше.

Метод GET передает запрос DNS с использованием параметра ?dns= с последующим запросом в кодировке Base64Url[8]. Этот метод лучше работает с кэшированием, поэтому можно рассчитывать на меньшую задержку получения ответа, хотя размер самого запроса больше, чем в случае POST.

Ответ всегда приходит с заголовком application/dns-message, когда данные DNS инкапсулированы в «сыром» виде.

Стоит отметить, что клиенту DoH придется иметь дело с двумя группами кодов успеха или неудачи операции – собственно DNS и HTTP. Так, например, клиент может получить

Рис. 1. Процент веб-страниц, загруженных Firefox с использованием HTTPS.



Источник: https://letsencrypt.org/stats/#percent-pageloads.

формально правильный ответ (код HTTP «200 OK»), в то время как ответ DNS будет содержать код SERVFAIL или NXDOMAIN.

Сценарии внедрения DoH

Нетрудно заметить, что как протокол DoH не многим отличается от DoT. Также, представляется разумным использовать современные методы шифрования для защиты трафика DNS. Хотя DNS в силу своей архитектуры не предусматривает сквозную защиту (никто не предполагал, что она потребуется), защита канала между клиентом (например, резолвер-заглушка пользовательского компьютера) позволяет защитить от целого класса MITM-атак, а использование транспортного протокола TCP избавит нас от зловредных отражающих атак с усилением, которые используют открытые резолверы.

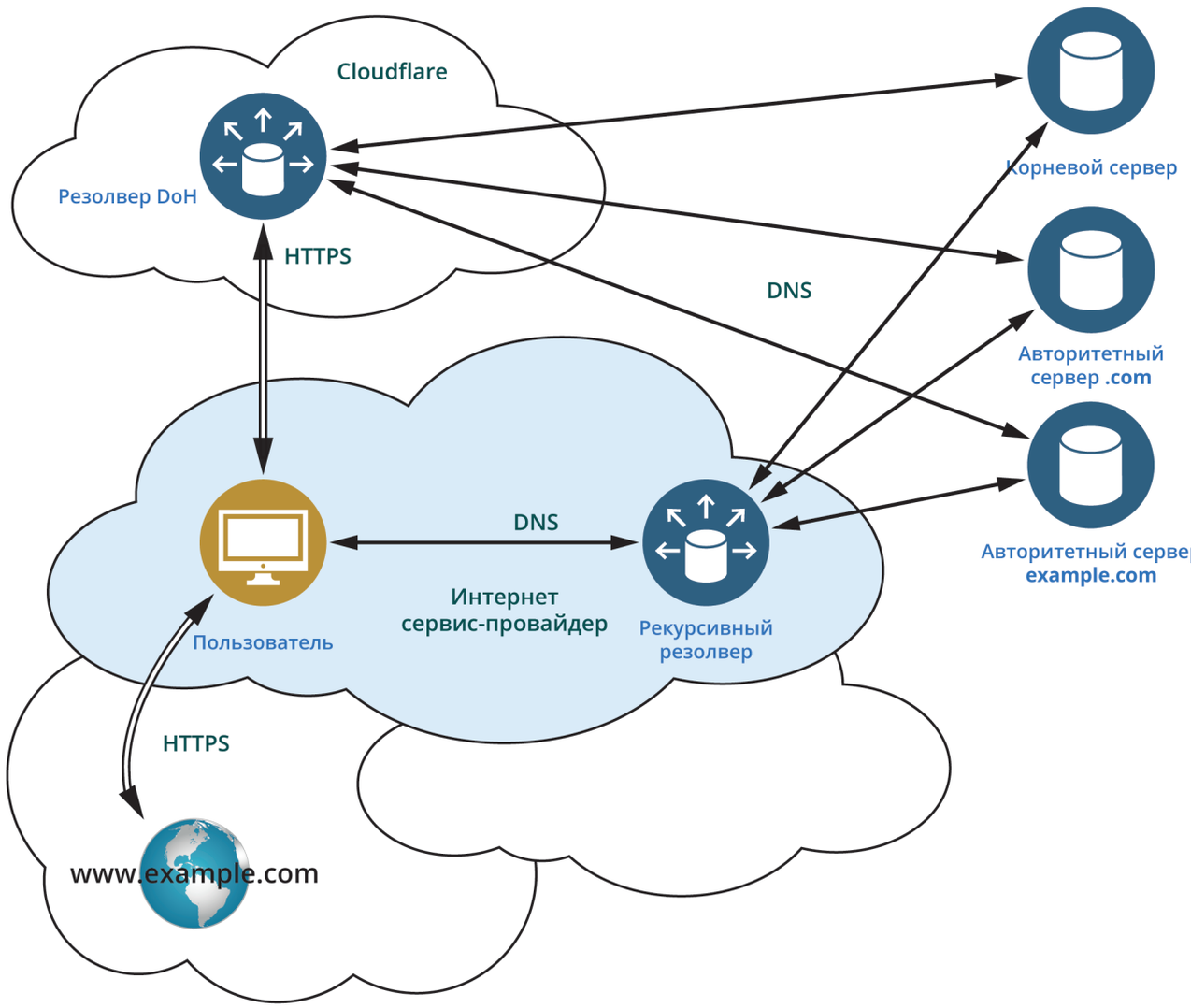
Что касается приватности, то тут есть оговорки. Начнем с того, что внедрение этого протокола для обмена данными между резолвером и авторитетными серверами проблематично как с точки зрения аутентификации, так и с точки зрения производительности. Поэтому стандарт DoH сфокусирован на «обмене данными между клиентами DNS (такими как резолверы-заглушки операционной системы) и рекурсивными резолверами». Далее, одним из основных сценариев применения DoH является «предотвращение вмешательства промежуточных устройств в обмен данными DNS». Но в большинстве случаев путь между пользователем и резолвером, включая и сам резолвер, полностью контролируется сервис-провайдером. Так что в этом варианте особых преимуществ пользователь не получает.

Совсем по-другому выглядит ситуация, когда в качестве резолвера используются «публичные» резолверы, такие как Public Google DNS (8.8.8.8) или Cloudflare (1.1.1.1). Использование такого резолвера может быть решением пользователя, но некоторые сервис-провайдеры используют их для полного аутсорсинга услуг DNS. В этом случае защита от посторонних глаз безусловно имеет смысл – DNS очень «разговорчивый» протокол и его прослушивание может рассказать много о клиенте.

Привлекательность этого сценария для разработчиков клиентских приложений, например, браузеров, заключается в том, что можно выбрать установку по умолчанию и взять трансляцию имен в свои руки. А заодно и заботу о приватности пользователей (см. рис. 2).

Однако здесь нас встречают несколько проблем.

Рис. 2. Традиционная схема работы DNS и с использованием централизованного DoH.



Технические и бизнес-риски централизованного DNS

Интернет-драфт «Проблемы и риски реализации централизованного DNS через HTTPS (DoH)»[9] обсуждает технические и бизнес-риски, связанные с централизованной схемой внедрения DoH. Перечислим некоторые из них.

Ухудшение детектирования угроз безопасности:

Некоторые пользователи могут потерять способность использовать DNS-блокировки, которые являются одним из основных способов защиты сети и ее пользователей от вредоносных программ, фишинга, спама, DDoS-атак и т.д.

Политика безопасности многих сетей, в том числе и сетей доступа, сетей предприятий, школ и других публичных заведений, включает в себя мониторинг и защиту безопасности сети и устройств в этой сети. Одним из широко распространенных методов осуществления этой политики является использование DNS для мониторинга, исправления и/или предотвращения заражения вредоносным ПО или других проблем безопасности.

Например, сетевые операторы могут применять этот метод (отдельно или совокупно с более детальным анализом трафика) для блокировки доступа к запрещенному контенту или вредоносным и фишинговым веб-сайтам. Так, многие сети проверяют, не присутствует ли запрашиваемое доменное имя в списках известных вредоносных команд и командных центров ботнетов. В случае совпадения владелец устройства или администратор локальной сети могут быть уведомлены о потенциальном заражении вредоносным ПО. В другом варианте резолвер перезаписывает ответ на запрос такого доменного имени, предоставляя адрес сервера, предупреждающего конечного пользователя о риске вредоносного ПО, или же предоставляя ответ NXDOMAIN – несуществующее имя – для прекращения поиска. Очевидно, что эта функциональность не будет работать, если DNS-запросы обходят резолверы, которые выполняют эту функцию, в случае централизованного внедрения DoH. Таким образом, централизованный DoH может создать «слепые» зоны в этой критической области противодействия угрозам безопасности.

Потеря видимости угроз может привести к использованию DoH в качестве нового и не обнаруживаемого вредоносного канала управления и контроля. Одним из примеров является DoHC2[10]. В результате, сам DoH иногда может рассматриваться как угроза безопасности, учитывая его возможное использование в качестве скрытого канала управления вредоносными программами и контроля.

Нарушение функций портала доступа в Интернет (captive portal)

Многие сети доступа используют различные порталы, основанные на DNS, например, для регистрации устройства для доступа в Интернет в публичных (например, беспроводные сети в кампусах, аэропортах и кафе) и корпоративных сетях или восстановления доступа после неуплаты. Централизованный DoH нарушает работу таких систем, поскольку браузер переопределяет специально назначенные адреса DNS-резолверов, реализующих эти функции, и вместо этого пытается использовать централизованный резолвер DoH. Хотя новые стандарты в рабочей группе IETF CAPPORT[11] могут избежать этого в будущем, стандарты CAPPORT все еще разрабатываются и широко не используются.

Потеря родительского контроля или других элементов управления контентом

Аналогично использованию DNS в локальных сетях для мониторинга и защиты от угроз безопасности, DNS часто используется для реализации элементов управления контентом, например, таких как родительский контроль. С помощью этих элементов управления родитель может настроить службу в своей домашней сети, чтобы дети не могли получить доступ к нежелательному или другому запрещенному контенту. Например, родители могут настроить политику, чтобы запретить своим детям-дошкольникам доступ к любым сайтам, связанным с социальными медиа, азартными играми, наркотиками, порнографией и так далее. Такие сервисы часто предоставляются сетями доступа или доступны по подписке и пользуются большой популярностью, особенно потому, что они могут работать с разными типами устройств (например, ПК и мобильные устройства) и экосистемами устройств (например, Android и Apple), программным обеспечением (например, Mac и Windows) и экосистемами платформ (например, Google, Apple и Amazon).

Как и в примере с вредоносным ПО, это обычно реализуется посредством сопоставления и перезаписи ответов DNS, когда конечному пользователю предоставляется либо перенаправление на страницу блокировки контента, либо получение ответа несуществующего имени NXDOMAIN. Эта функциональность не будет работать, если DNS-запросы обходят серверы, которые выполняют эту функцию, для централизованных резолверов DoH. Даже если поставщик централизованного DoH и предлагает подобные услуги, их характеристики могут не соответствовать требованиям пользователя.

Проблемы с разделенным DNS

Разделенный DNS, или DNS с «расщепленным горизонтом»[12] - это система, в которой внутренние и внешние сети обслуживаются различными DNS-серверами. Это чаще всего используется в корпоративных, образовательных и государственных сетях в качестве средства управления безопасностью и конфиденциальностью. На практике это означает, что существуют имена, которые транслируются только в адреса внутренней сети, или имена, которые транслируются в адреса внутренних серверов для пользователей внутренней сети и в адреса общедоступных серверов для пользователей за пределами сети. Например, предприятие может иметь внутреннюю службу с именем «Система учета», доступную в Интернете через https://accounting-system или https://accounting- system.example.com и подключенную через внутренний не маршрутизируемый RFC1918 IPv4-адрес, такой как 192.168.1.77. Эти доменные имена поддерживаются только в локальных резолверах и не могут быть транслированы с использова-

нием авторитетной DNS-инфраструктуры Интернета. Эти имена больше не будут транслироваться на основе внешней реализации DoH.

Утечка корпоративных данных

При использовании разделенных имен DNS, как отмечено в приведенном выше примере для пользователя в корпоративной сети, пытающегося подключиться к хосту по адресу https://accounting-system.example.com, поиск с централизованным резолвером DoH будет обычно терпеть неудачу (NXDOMAIN). Но поскольку внутреннее имя было отправлено в централизованный распознаватель DoH, это частное имя «просочилось» за пределы локальной сети или сети предприятия, делая корпоративную сеть более уязвимой с точки зрения компьютерной безопасности. Аналогично, поиск обратных DNS-имен (in-addr.arpa) также приведет к утечке частных IP-адресов. Утечка данных IP-адреса может произойти независимо от того, используется ли разделенный DNS.

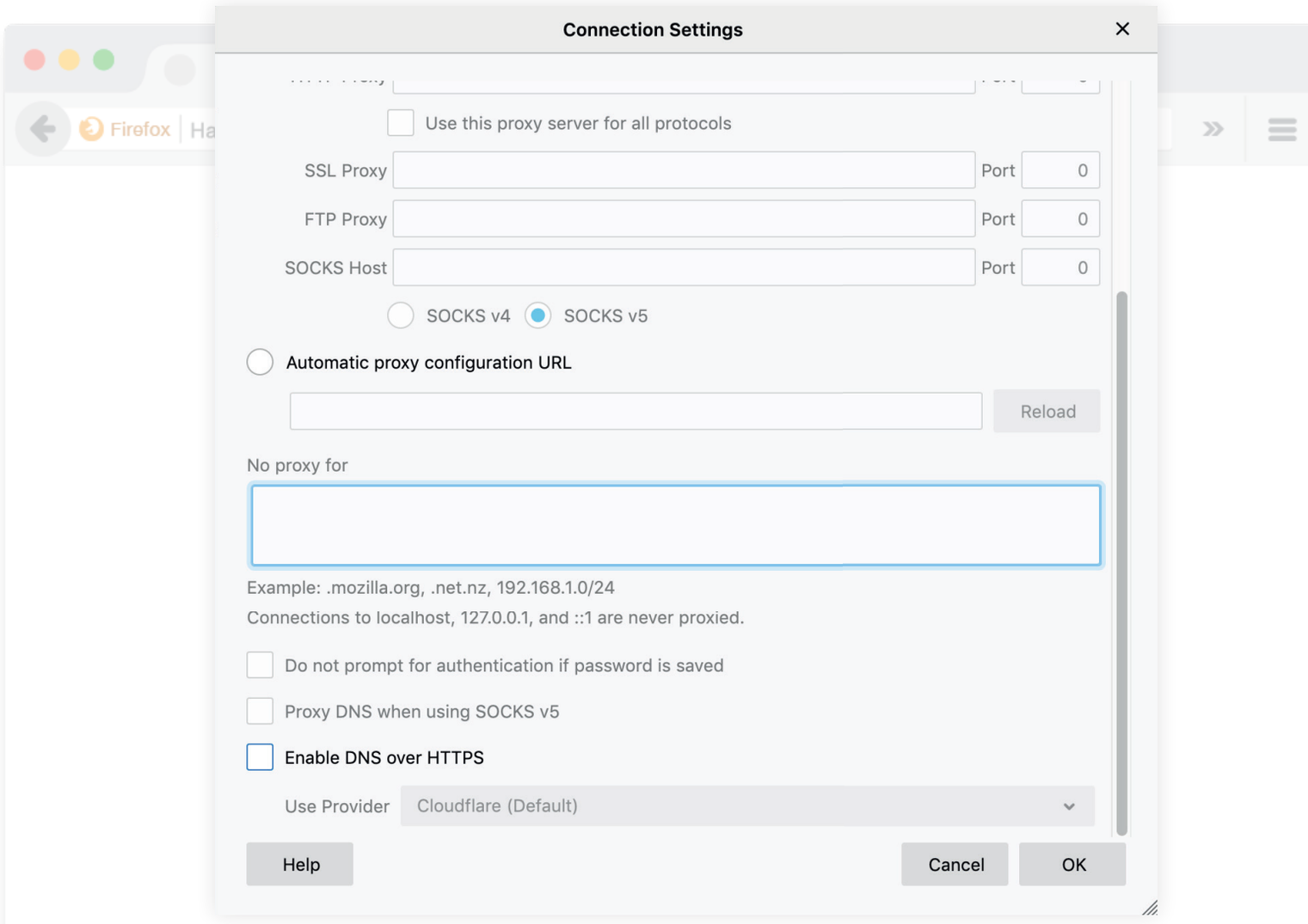
Один из основных пропонентов DoH – некоммерческая компания Mozilla, разработчик популярного браузера Firefox, работает над решениями, которые позволят уменьшить, если не свести на нет негативные последствия DoH, которые мы обсудили. Например, проверки, включен ли родительский контроль. Для этого Firefox пытается транслировать специальное доменное имя, которое занесено в «черные списки». В случае обнаружения блокировки Firefox автоматически отключит DoH и станет использовать DNS, предоставляемый операционной системой пользователя. Подобным образом определяются конфигурации «расщепленного горизонта». Более подробно с этими методами можно ознакомиться на сайте Mozilla[13].

Вопросы приватности

Централизованные решения внедрения DoH вызывают также озабоченность в области защиты личных данных и приватности. Иронично, что шифрование передачи данных DNS и, в частности, DoH, призваны усилить защиту личных данных, но иногда лекарство может быть хуже болезни.

Представьте, что все ваши перемещения в Интернете фиксируются одним провайдером DoH. Пользуетесь ли вы Интернетом дома, на работе, в кафе, на компьютере или смартфоне, все запросы DNS, а значит, и ваши действия, регистрируются в одном месте. Это, конечно, не означает, что провайдер DoH непременно станет использовать эту информацию, но кто оценивает эти риски и выбирает подходящего провайдера DoH? По всей видимости – это сами браузеры. Для минимизации рисков, например, Mozilla

Рис. 3. Пока что использование DoH в браузере Firefox нужно настраивать вручную. Надолго ли?



создала специальную программу Mozilla Trusted Recursive Resolver (TRR), содержащую минимальный набор требований политики, которым должен соответствовать оператор, чтобы считаться потенциальным партнером программы. Требования включают конкретное описание политики сбора и хранения данных, прозрачности и блокирования[14].

Вопрос относительно преимуществ и недостатков использования централизованного DoH также связан с конкретной моделью угроз. Нет никаких сомнений, что централизованный DoH может быть полезен в некоторых сетях. Например, при использовании Интернета в кафе Public DNS Google, скорее всего, лучший выбор, чем местный резолвер. Или тот факт, что многие пользователи в США рассматривают своих интернет-провайдеров как угрозу, поскольку известно, что эти интернет-провайдеры напрямую монетизируют DNS-запросы и продают их рекламодателям. Обратное верно в отношении Европейского Союза. Благодаря GDPR, интернет-провайдеры в ЕС жестко ограничены в том, что они могут делать с данными DNS, и поэтому в девяти случаях из десяти провайдер интернет-доступа, вероятно, является лучшим выбором с точки зрения конфиденциальности, чем любой облачный DNS-резолвер. Другими словами, какой резолвер использовать, зависит от конкретной ситуации.

Проблема в том, что пользователь весьма далек от настроек такого типа – многие не знают, что такое DNS, не говоря уже о конфигурации конкретного резолвера. Поэтому настройки по умолчанию в большинстве случаев вряд ли будут изменены. Сегодня для того, чтобы включить DoH в Firefox, необходимо изменить установку, но Mozilla уже сообщила о планах конфигурации DoH по умолчанию для американских пользователей уже в конце сентября 2019 (см. рис.3).

Заключение

В заключение хочется заметить, что централизованный DNS не является порождением DoH. Публичные резолверы, такие как Public DNS компании Google, OpenDNS (Cisco), 1.1.1.1 (Cloudflare), Quad9 (https://www.quad9.net/about/), существуют уже не первый год и активно используются. Согласно измерениям APNIC Labs чуть более одного из шести пользователей используют один из публичных резолверов в качестве основного[15]. DoH усиливает эту тенденцию и, учитывая его тесную интеграцию с поставщиками контента, это, может быть, обозначает новый эволюционный виток развития DNS и Интернета в целом.

Ссылки

1. RFC7258 “Pervasive Monitoring Is an Attack”, https://datatracker.ietf.org/doc/rfc7258/

2. см. https://letsencrypt.org/stats/#percent-pageloads, https://transparencyreport.google.com/https/overview

3. https://datatracker.ietf.org/doc/draft-camwinget-tls-use-cases

4. “Encrypted Server Name Indication for TLS 1.3”, https://datatracker.ietf.org/doc/draft-ietf-tls-esni

5. Хотя сами данные DNS шифровать не имеет смысла, частичную защиту приватности можно осуществить путем т.н. минимизации данных запроса. Обычно один и тот же вопрос (например, «каков IP-адрес www.example.com?») отправляется всем участникам процесса разрешения имени. Хотя лучше было бы спрашивать корневые серверы о серверах .com, а тех, в свою очередь, о серверах, обслуживающих домен example.com. И только последних – об адресе www.example.com. Этот метод описан в экспериментальном RFC 7816 “DNS Query Name Minimisation to Improve Privacy” (https://datatracker.ietf.org/doc/rfc7816/)

6. RFC7858 “Specification for DNS over Transport Layer Security (TLS)”, https://datatracker.ietf.org/doc/rfc7858/

7. RFC8484 “DNS Queries over HTTPS (DoH)”, https://datatracker.ietf.org/doc/rfc8484

8. RFC4648 “The Base16, Base32, and Base64 Data Encodings”, https://datatracker.ietf.org/doc/rfc4648/

9. “Centralized DNS over HTTPS (DoH) Implementation Issues and Risks”, https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues

10. https://github.com/SpiderLabs/DoHC2

11. https://datatracker.ietf.org/wg/capport/about/

12. см. RFC8499 “DNS Terminology”, https://datatracker.ietf.org/doc/rfc8499

13. https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

14. https://wiki.mozilla.org/Security/DOH-resolver-policy

15. “DNS resolver centrality”, https://blog.apnic.net/2019/09/23/dns-resolver-centrality/

«Цифровая повестка ЕС»:

реформирование регулирования телекоммуникаций и контента в правовой системе Европейского союза

Мадина Касенова

В нынешних условиях ориентации социально-экономического развития современных государств на «цифровую экономику» Европейский Союз демонстрирует последовательный, системный и комплексный подход правовой регламентации внутреннего цифрового рынка. При этом эволюционное развитие соответствующих «правовых инструментов ЕС» (*European legal instruments*)[1] определяет суть двух взаимосвязанных процессов: с одной стороны, установление общих нормативных рамок, закрепляемых на уровне Евросоюза в политико-правовых документах и, с другой стороны, формирование организационных структур, обеспечивающих функционирование институциональных основ регулирования. Именно такой подход унифицирует правовые и организационно-институциональные основы, создавая «общие юридические рамки» на уровне ЕС, содействуя гармонизации национального права стран-членов ЕС, позволяющей в большей степени избежать фрагментации регулирования отношений в «цифровой сфере».

Стремительное развитие и совершенствование интернет-технологий, интенсификация социальных сфер их использования и т.д. объективировали формирование «общей интернет-повестки» Евросоюза, что и определило подход, при котором самостоятельными объектами регулирования, в т.ч. правового регулирования, стали рассматриваться телекоммуникации, персональные данные, контент и т.д. Регуляторные подходы и практика Европейского Союза приобретают практическое значение для многих государств, и в этой связи представляют несомненный интерес новые нормативные акты, принятые в Евросоюзе в сфере телекоммуникаций и цифрового контента (уже вступившие в силу), а также акты, предлагаемые к принятию.

В числе новых актов Европейского парламента и Совета отметим Директиву (ЕС) 2018/1972 об учреждении Европейского кодекса электронных коммуникаций[2] и Регламент (ЕС) 2018/1971 об органе европейских регуляторов по электронным коммуникациям и агентстве по поддержке органа европейских регуляторов, изменяющий Регламент (ЕС) 2015/2120 и отменяющий Регламент (ЕС) № 1211/2009[3] (принятые 11 декабря 2018 г.); Директиву (ЕС) 2019/790 от 17 апреля 2019 об авторском праве и смежных правах на едином цифровом рынке и изменяющую Директивы 96/9/ЕС и 2001/29/ЕС[4]. Кроме названных актов следует также обратить внимание на обсуждаемую в настоящее время законодательную резолюцию Европейского парламента относительно принятия регламента по предотвращению онлайнового распространения террористического контента (версия 17.04.2019)[5].

1. Телекоммуникации.

Эволюционно сложившиеся за несколько десятилетий в Евросоюзе общие нормативные и организационно-институциональные основы правового регулирования телекоммуникационной сферы значительно обновлены и реформированы в связи с принятием 11.12. 2018 г. Европейским парламентом и Советом двух нормативных актов: Директивы (ЕС) 2018/1972 об учреждении Европейского кодекса электронных коммуникаций (далее – «Телекоммуникационный Кодекс» или «Директива о Кодексе») и Регламента (ЕС) 2018/1971 об органе европейских регуляторов по электронным коммуникациям и агентстве по поддержке органа европейских регуляторов (далее – «Регламент о BEREC/Агентстве BEREC» или «Регламент 2018/1971»). При оценке значения этих актов целесообразно принять во внимание следующие факторы.

Первым фактором является *одновременное* принятие и вступление в силу Директивы о Кодексе и Регламента о BEREC/Агентстве BEREC[6], поскольку тем самым решается «двуединая задача», отмеченная в начале статьи, свя-

занная с обеспечением корреляции общенормативных и институциональных основ регулирования телекоммуникаций на уровне ЕС.

Вторым – появление в Евросоюзе нормативного акта «в ранге» кодекса, т.к. в общеправовом плане кодекс выступает законодательным кодификационным актом, который всегда «поднимает» регулирование конкретных отношений на новый, «высокий порядок». Нельзя не отметить при этом, что правовое значение и регуляторная роль Телекоммуникационного Кодекса обусловлена тем, что он учрежден *директивой*, т.е. нормативным актом «вторичного права» правовой системы Евросоюза, предполагающего его транспонирование в национальное право стран-членов ЕС. Третий фактор связан с реформированием институциональной основы регулирования телекоммуникаций на уровне ЕС, коррелирующей соответствующим нормативным основам, что закреплено *регламентом* – Регламентом о BEREC/Агентстве BEREC. Нелишне отметить, что согласно нормам «первичного» права ЕС, регламент Европейского парламента и Совета является актом «вторичного права» ЕС, который обладает общеобязательным действием, непосредственно (прямо) применяется всеми государствами-членами ЕС, всеми органами ЕС, а также лицами (физическими/юридическими), к которым он может быть применим[7].

Совокупность отмеченных факторов диктует последующее рассмотрение содержательных характеристик Директивы о Кодексе и Регламента о BEREC/Агентстве BEREC не только в «корреляционной связи», но и в ретроспективе их принятия, т.к. это даст возможность понять логику появления этих актов и развитие подходов правового регулирования телекоммуникаций в ЕС.

Пожалуй, сложно подвергнуть сомнению то, что в Евросоюзе телекоммуникации выступают самостоятельным объектом правового регулирования, достаточно назвать, в частности, «Зеленую книгу по телекоммуникациям» 1987 г.[8], Программу единого рынка 1992 г.[9]; ряд актов «вторичного права» ЕС, в т.ч. Резолюцию Совета 88/С от 30.06.1988 г. об общем рынке телекоммуникационных услуг и оборудования до 1992 г.[10]; Директиву Совета 87/372/ЕЕС от 25.06.1987 г. о диапазоне частот, зарезервированных для согласованного внедрения на территории всего ЕС общеевропейской сотовой цифровой наземной мобильной связи в Сообществе («Директива GSM 1987»)[11]; Директиву 98/84/ЕС Европейского парламента и Совета от 20.11.1998 г. о правовой защите услуг с использованием условного доступа или основанных на условном доступе[12] и др.

Уже в начале XXI века регулирование телекоммуникаций в Евросоюзе приобрело системный и комплексный характер и это подтверждается принятием Европейским парламентом и Советом пяти директив, комплекс которых получил название «первой пакетной» реформы Евросоюза. Четыре директивы были приняты 7.03.2002 г., а именно: Директива 2002/19/ЕС о доступе к сетям электронных коммуникаций, взаимосвязанности сетей электронных коммуникаций и связанных с ними технических средств, «Директива о доступе» (*Access Directive*)[13]; Директива 2002/20/ЕС относительно разрешений общего характера для сетей электронных коммуникаций и услуг, «Директива о разрешениях общего характера» (*Authorization Directive*)[14]; Директива 2002/21/ЕС об общей нормативно-правовой основе для сетей электронных коммуникаций и услуг, «Рамочная директива» (*Framework Directive*)[15]; Директива 2002/22/ЕС об универсальных услугах и правах пользователей, связанных с сетями электронных коммуникаций и услугами, «Директива об универсальных услугах» (*Universal Service Directive*)[16]. Пятой директивой стала Директива 2002/58/ЕС 12.06.2002 г., касающаяся обработки персональных данных и обеспечения конфиденциальности в секторе электронных коммуникаций, «Директива о конфиденциальности и электронных сообщениях» (*e-Privacy Directive*)[17]. Названные директивы представляли собой систему нормативных актов, сформированных на основании «взаимодополняемости» и «взаимосогласованности», и по сути, создали на уровне ЕС формально-юридические основы общенормативного регулирования телекоммуникаций.

К тому же временному периоду относится принятие Решения Комиссии ЕС 2002/627/ЕС от 29.07.2002 г. об учреждении Европейской регуляторной группы по электронным коммуникационным сетям и услугам (*European Regulators Group, ERG*)[18]. Это Решение способствовало формированию организационно-структурных основ регулирования телекоммуникаций на уровне ЕС. Дальнейшее развитие, а затем и реформирование регулирования телекоммуникаций в ЕС происходило в парадигме реализации пяти обозначенных директив, а также деятельности созданной структуры – *Group ERG*.

В 2009 году был предпринят критический обзор реализации «первой пакетной» реформы Евросоюза, который с очевидностью выявил потребность диверсификации сложившегося инструментария регулирования телекоммуникаций в ЕС, что увязывалось с необходимостью решения «двуединой задачи». С одной стороны, необходимостью дальнейшего совершенствования общенормативных основ, и это было вызвано, в т.ч. спецификой актов «вторичного» права, принимаемых в форме директив. «Опосредованная» (двухступенчатая) применимость директив, требующая их транспонирования в национальные правопорядки стран-членов ЕС, отчасти приводила к фрагментации и возникновению противоречий в национально-правовом регулировании телекоммуникаций. С другой стороны, потребностью обеспечить организационно-структурную поддержку регулирования телекоммуникаций как на уровне ЕС, так и на уровне национальных регуляторных органов стран-членов ЕС, создавая тем самым ясные институциональные рамки регулирования.

В рамках решения этой «двуединой задачи» следует рассматривать Соглашение Европейского парламента и Совета министров о реформе телекоммуникаций 2009 года[19], а также пересмотр директив «первой пакетной» реформы. Так, комплексно были изменены: Директива 2002/19/ЕС «О доступе» (*Access Directive*), Директива 2002/20/ЕС относительно разрешений общего характера (*Authorization Directive*); Директива 2002/21/ЕС (*Framework Directive*), Директива 2002/22/ЕС об универсальных услугах (*Universal Service Directive*), Директива 2002/58/ЕС о конфиденциальности и электронных сообщениях (*e-Privacy Directive*). Приятием Директивы 2009/114/ЕС от 16 сентября

2009 г. (*Directive modernising the 1987 GSM Directive*)[20] была модернизирована и Директива GSM 1987 года.

В формате решения «двуединой задачи» происходило развитие организационного обеспечения регулирования телекоммуникаций на уровне ЕС. Создание новых структурных органов Евросоюза специальной компетенции было оформлено Регламентом (ЕС) 1211/2009 от 25.11.2009 г. об учреждении Органа европейских регуляторов по электронным коммуникациям и Бюро европейских регуляторов по электронным коммуникациям (далее – «Регламент 1211/2009»)[21]. Знаменателен сам факт учреждения новых структурных органов ЕС специальной компетенции (BEREC и Бюро BEREC) и то, что их создание закреплено законодательным актом прямого действия. Нормативные положения Регламента 1211/2009 предусматривали существенные новации, развивающие институциональные рамки регулирования телекоммуникаций.

В числе новаций Регламента 1211/2009 – замена созданной ранее Европейской регуляторной группы по электронным коммуникационным сетям и услугам (ERG) Органом европейских регуляторов по электронным коммуникациям (далее – «BEREC»). Регламент 1211/2009 закрепил, что BEREC не будучи «...ни агентством, ни юридическим лицом» (п. 6 Преамбулы Регламента 1211/2009), является «центральной» институциональной структурой ЕС, функциональная роль которой заключается в обеспечении реализации общенормативных основ ЕС регулирования телекоммуникаций в целях содействия развитию внутреннего рынка электронных коммуникаций. В этом плане на BEREC возлагались широкие консультативные функции (в т.ч. представление экспертных заключений, консультаций, информации и т.д.). Основанием деятельности BEREC стали стратегии развития, которые им разрабатывались и регулярно пересматривались[22].

С учетом статуса BEREC, Регламент 1211/2009 закрепил его внутриорганизационную структуру. В состав BEREC вошли 28 независимых национальных регуляторных органов (*National regulatory authorities, NRAs*) стран-членов ЕС; в статусе наблюдателей в его состав вошли представители Еврокомиссии, а также стран-участниц Европейского экономического пространства (*EEA countries*) и стран, ассоциированных с ЕС. Такая структура BEREC позволяла обеспечивать, с одной стороны, сотрудничество между национальными регуляторными органами (*NRAs*) и с другой стороны, между национальными регуляторными органами (*NRAs*) и Еврокомиссией. Немаловажно, что статус и структура BEREC позволяли обеспечивать сотрудничество лиц, непосредственно входящих в его состав, и также привлекать широкий круг субъектов, действующих в телекоммуникационной сфере, а также координировать их взаимодействие.

Значительной новацией Регламента 1211/2009 явилось создание органа специальной компетенции – Бюро BEREC, которое изначально было создано как юридическое лицо, предметная и функциональная компетенция которого заключалась в административной, организационной, профессиональной, вспомогательной и проч. поддержке деятельности BEREC. В принятом в последующем Решении 2010/349/ЕС представители правительств стран-членов ЕС предусмотрели, что Бюро BEREC будет размещено в г. Рига (Латвия), а соответствующее соглашение с правительством Латвийской Республики вступило в силу 5 августа 2011 года[23].

Комплекс мероприятий, связанных с совершенствованием нормативных актов Евросоюза, регулирующих сферу телекоммуникаций, а также «организационно-структурные новации», приведшие к институциональным изменениям, получил название «второй пакетной» реформы ЕС в телекоммуникационной сфере. С учетом специфики транспонирования директив и действия регламентов в ЕС, полноценное функционирование общенормативной и институциональной основ регулирования телекоммуникаций «второй пакетной» реформой *de facto* началось в 2011 году[24].

Во втором десятилетии текущего века рельефно и четко определился стратегический вектор социально-экономического развития современных государств, ориентированный на «цифровую экономику», а телекоммуникации стали рассматриваться как ее критически важный компонент, имеющий экономическую значимость и коммерческую ценность. Этот вектор развития внутреннего рынка Евросоюза нашел свое отражение в принятой 6.05.2015 г. Стратегии Единого цифрового рынка Евросоюза[25]. Широкий диапазон задач, реализуемых в рамках Единого цифрового рынка ЕС, наряду с иными факторами социально-политического плана и динамикой темпов развития телекоммуникаций, ускорили процесс реформирования регулирования телекоммуникаций на уровне ЕС.

Формат решения «двуединой задачи», обозначенной выше, не потерял своей актуальности, а поскольку с момента полноценной реализации «второй пакетной» реформы 2009 года деятельность BEREC и Бюро BEREC определяла общий контекст регулирования телекоммуникаций на уровне ЕС, дальнейшее реформирование осуществлялось параллельно: кодифицировалась общенормативная основа и совершенствовалась институциональная основа. Эти процессы инициировались и координировались Еврокомиссией, а их реализация продвигалась с разной степенью интенсивности. После 2015 года этот процесс «ускорился»[26] и *de facto* завершился *одновременным* принятием Директивы о Кодексе и Регламента 2018/1971. Рассмотрим бегло общие положения этих нормативных актов.

1.1. Директива (ЕС) 2018/1972 об учреждении европейского Кодекса электронных коммуникаций.

Телекоммуникационный Кодекс представляет собой объемный, структурированный документ (более 300 страниц текста), нормативные положения которого закреплены в 326 пунктах Преамбулы, 127 статьях, включая 13 приложений. Разумеется, в формате статьи можно осветить лишь некоторые его положения.

Доктринальный тезис о том, что кодификация выступает высшей формой систематизации и совершенствования законодательства, не является оспоримым, и имеет смысл еще раз подчеркнуть, что знаменателен сам факт принятия

единого кодификационного акта ЕС в формате кодекса. Телекоммуникационный Кодекс аккумулирует нормативный массив практически всех областей права ЕС в телекоммуникационной сфере, регулирует широкий круг вопросов, применительно к различным типам телекоммуникационных услуг в ЕС и т.д., обеспечивая тем самым целостность правового регулирования. Телекоммуникационный Кодекс (как единый кодификационный акт) в том числе устанавливает правомочия телекоммуникационных компаний по установке оборудования, находящегося как в государственной, так и в частной собственности; порядок деятельности фактически всех субъектов телекоммуникационной сферы (провайдеров телекоммуникационных сетей, поставщиков услуг, национальных регуляторных органов стран-членов ЕС и т.д.); доступ пользователей к телекоммуникационным сетям на регламентированной скорости; доступ операторов связи в жилые помещения и инфраструктурные объекты; создание государственно-частных партнерств по развертыванию телекоммуникационных сетей; тарифы и переключение между сетями и тарифы платежей с учетом технологических особенностей голосового трафика; деятельность OTT-сервисов (*OTT service*); развитие гигабитных сетей и сетей 5G; согласованный доступ и использование радиочастотного спектра; предоставление услуг широкополосного доступа в Интернет и т.д.

Исторически сложившиеся общенормативные основы регулирования телекоммуникаций в ЕС стали основой Директивы о Кодексе, и она логически сопряжена с упомянутыми ранее четырьмя директивами «второй пакетной» реформы[27], которые предметно охватывали широкий комплекс вопросов, включая регулирование деятельности поставщиков электронных коммуникационных сетей и услуг электронных коммуникаций. На это важно обратить внимание, т.к. в настоящее время Директива о Кодексе и названные четыре директивы «второй пакетной» реформы образуют действующий нормативный комплекс регулирования телекоммуникаций на уровне ЕС (п. 4 Преамбулы Директивы о Кодексе).

Согласно Директиве о Кодексе, в условиях взаимопроникновения телекоммуникаций, средств массовой информации, различных секторов информационных технологий все электронные телекоммуникационные сети и услуги, в той мере насколько это возможно, должны подпадать под действие единого кодификационного акта, создающего правовую определенность, а также «целостное единство» регулирования на уровне ЕС.

В практическом плане правовая определенность регулирования телекоммуникаций имеет несколько аспектов. Одним из важных аспектов является систематизация категориально- терминологического аппарата и содержательное определение понятий, что создает основания их адекватного использования. Категориально-терминологический аппарат, закрепленный в Директиве о Кодексе, и содержательное значение используемых в нем понятий адекватно отражает технический уровень развития новых форм сетевого управления и исходит из принципа технологической нейтральности (п. 14 и 15 Преамбулы, ст. 2 Директивы о Кодексе).

Другой немаловажный аспект правовой определенности регулирования заключается в том, что Директива о Кодексе *разграничивает* регулирование электронных телекоммуникационных сетей и регулирование контента. В этой Директиве прямо закреплено, что ее действие «не распространяется на контент услуг, предоставляемых через электронные коммуникационные сети посредством электронных коммуникационных услуг, в числе которых контент эфирного вещания (радиовещание, телевидение), финансовые услуги, а также конкретные виды услуг информационного общества»[28]. При этом разграничение между регулированием электронных коммуникаций и регулированием контента не влияет на учет существующих между ними связей, в т.ч. для гарантий сохранения плюрализма СМИ, культурного разнообразия, защиты прав потребителей и т.д. (п. 7 Преамбулы Директивы о Кодексе).

Доктринальный тезис о том, что кодификация выступает высшей формой систематизации и совершенствования законодательства, не является оспоримым, и имеет смысл еще раз подчеркнуть, что знаменателен сам факт принятия единого кодификационного акта ЕС в формате кодекса.

Помимо сказанного, правовая определенность выражается в четком закреплении в Директиве о Кодексе нормативных положений о сокращении *ex ante* регулирования – «до» возникновения того или иного события/обстоятельства. Поясним, что в общем плане регулирование *ex ante* связано со значительным (зачастую «удушающим») участием компетентных органов, устанавливающих нормы преимущественно контрольно-предписывающего характера. В этом смысле регулирование ex ante всегда противоположно *ex post* регулированию. В условиях динамичного развития рынков электронных коммуникаций важно поддерживать конкурентную среду, именно поэтому Директива о Кодексе направлена на то, чтобы *ex ante* регуляторные обязательства налагались исключительно в тех случаях, когда на конкретных рынках отсутствует эффективная и устойчивая конкуренция. Директива о Кодексе возлагает ответственность на национальные регулирующие органы за своевременность и релевантность отмены *ex ante* предварительного регулирования, с тем, чтобы по мере развития конкуренции в секторе телекоммуникаций обеспечить свободу сетей электронных коммуникаций и услуг электронных коммуникаций в масштабе ЕС (п.п. 29, 35 Преамбулы Директивы о Кодексе). Сокращение *ex ante* «контрольно-предписывающих» норм, по смыслу Директивы о Кодексе, направлено на либерализацию регулирования рынка телекоммуникаций, расширение конкуренции, поддержание высокого уровня инвестиций, инноваций, оптимизации защиты прав потребителей и т.д.

Кратко обозначим некоторые положения Директивы о Кодексе применительно к услугам широкополосного доступа в Интернет. Директива о Кодексе возлагает на государства-члены ЕС обязанность по определению услуг широкополосного доступа в Интернет и предусматривает, что такие услуги должны быть «надлежащими» и «адекватными», учитывать национальные условия их предоставления, минимальную пропускную способность, которой пользуется большинство потребителей на территории этого государства-члена (но не менее минимальной скорости в 100 Мбит/с).

Директива о Кодексе закрепляет критерии «надлежащих» и «адекватных» услуг широкополосного доступа в Интернет. К примеру, «адекватность» услуг широкополосного доступа в Интернет означает обеспечение пропускной способности, необходимой для поддержания по меньшей мере минимального набора услуг, охватывающих электронную почту; поисковые системы, позволяющие искать и находить все виды информации; базовое обучение и инструменты обучения онлайн; онлайн-газеты или новости; покупку или заказ товаров или услуг в Интернете; поиск работы и поиск доступа к профессиональной сети; интернет-банкинг; использование услуг электронного правительства; социальные сети и обмен мгновенными сообщениями; звонки и видеозвонки стандартного качества.

В завершение раздела статьи отметим, что Директива о Кодексе подлежит транспонированию в национальные правопорядки стран-членов ЕС (до 21 декабря 2020 года). Эта Директива не ограничивает права стран-членов ЕС, в частности, принимать необходимые меры для обеспечения защиты своих ключевых национальных интересов, включая решение проблем национальной безопасности.

1.2. Регламент (ЕС) 2018/1971 об учреждении Органа европейских регуляторов по электронным коммуникациям и агентства по поддержке Органа европейских регуляторов по электронным коммуникациям, изменяющий Регламент (ЕС) 2015/2120, а также отменяющий Регламент (ЕС) № 1211/2009.

В институциональном плане регулирование телекоммуникаций поддерживалось специализированными структурами на уровне ЕС – BEREC и Бюро BEREC, которые были созданы согласно Регламенту 1211/2009. В связи с принятием Регламента 2018/1971, действие Регламента 1211/2009 прекращается; функциональная роль BEREC и Бюро BEREC реформируется, прежде всего, применительно обеспечения реализации реформированных нормативных основ регулирования телекоммуникаций на уровне ЕС.

Несмотря на то, что Регламент 2018/1971 *de jure* не изменил статус BEREC как «центральной» и независимой институциональной структуры Евросоюза и, по сути, сохранил его состав (п.п. 13-15 Преамбулы Регламента 2018/1971), порядок формирования внутриорганизационных структур BEREC, их функциональная компетенция, процедурные вопросы принятия решений и т.д. – были реформированы. Так, Регламент 2018/1971 уточнил консультативную роль BEREC в плане взаимодействия с Европейским парламентом, Советом и Европейской комиссией. К примеру, инициатива проведения конкретных консультаций возлагается в равной степени как на руководящие органы Евросоюза, на Еврокомиссию, так и на BEREC. Более того, документы, принимаемые BEREC (заключения, рекомендации, руководящие принципы, директивные указания и т.д.), становятся обязательными для национальных регуляторных органов (*NRAs*) стран-членов ЕС и Европейской комиссии. Регламент 2018/1971 расширил регуляторные функции BEREC. В частности, BEREC предоставлено право устанавливать рабочие «контактные механизмы» взаимодействия практически со всеми компетентными органами Евросоюза (агентствами, консультативными группами и т.д.), а также с компетентными органами третьих стран и международными организациями. Такие «контактные механизмы» BEREC имеют важное значение, хотя они и не создают юридических обязательств, т.к. BEREC не вправе действовать как орган, представляющий позицию Евросоюза «вовне» (п. 20 Преамбулы Регламента 2018/1971).

Деятельность BEREC опирается на разрабатываемые им стратегии развития, которые упоминались ранее. В настоящее время основным документом является Стратегия BEREC на 2018-2020 гг.[29], которая закрепляет пять базовых направлений развития рынка телекоммуникаций ЕС: реагирование на проблемы подключения и новые условия доступа к сетям большой емкости; мониторинг потенциальных «узких» мест в распределении цифровых услуг; подключение 5G и продвижение инноваций в сетевые технологии; последовательный подход к принципу сетевого нейтралитета; изучение новых способов расширения прав и возможностей потребителей.

В регламентации деятельности и определении компетенции BEREC очевидным образом прослеживается «корреляционная связь» Регламента 2018/1971 и Директивы о Кодексе, о чем говорилось выше. К примеру, в статьях 3, 5.10 и др. Директивы о Кодексе непосредственно закреплены, в частности, такие правомочия BEREC, как разработка руководящих принципов и директивных положений; подготовка отчетности технологических направлений; ведение реестров баз данных; представление заключений о процедурах внутреннего рынка телекоммуникаций, в т.ч. для согласования соответствующих проектов национальных мер регулированию телекоммуникационной сферы, и т.д.

Регламентом 2018/1971 предусмотрено создание «Агентства по поддержке BEREC» (далее – «Агентство BEREC»), которое заменяет Бюро BEREC и выступает его правопреемником. Такая преемственность проявляется по целому ряду параметров: Агентство BEREC, так же, как и Бюро BEREC, обладает статусом юридического лица; его местонахождением также является г. Рига (Латвия); Агентство BEREC сохраняет обязательства Бюро BEREC относительно всех форм собственности, соглашений, включая юридические обязательства, вытекающие из трудовых, коммерческих и др. договоров (п. 41 Преамбулы Регламента 2018/1971).

Согласно Регламенту 2018/1971, цель Агентства BEREC – оказание всесторонней поддержки деятельности BEREC. Агентство BEREC является юридическим лицом, функци-

онирующим как децентрализованный орган ЕС, при этом его деятельность ограничена соответствующим мандатом, а также существующей институциональной структурой Евросоюза. По сравнению с Бюро BEREC, Агентство BEREC обладает большей самостоятельностью, в частности, оно пользуется правовой, административной, финансовой и т.д. автономией (п.п. 31, 35, 37 и др. Преамбулы Регламента 2018/1971); вправе сотрудничать с компетентными органами стран-членов ЕС по вопросам конкуренции, защиты прав потребителей, защиты данных и др. в сфере электронных коммуникаций; вправе, совместно с BEREC, сотрудничать с регулирующими органами третьих стран, а также с международными организациями. Однако Агентство BEREC, как и BEREC, не обладает правом представлять позицию Евросоюза «вовне», равно как и принимать обязательства от имени ЕС (п. 7, 12, 14 Преамбулы Регламента 2018/1971).

Даже эти, сжато изложенные положения Регламента 2018/1971, как представляется, свидетельствуют об устойчивом дискурсе консолидации нормативных и институциональных основ регулирования телекоммуникаций в Евросоюзе.

2. Контент.

2.1. Регулирование контента в аспекте авторского права и смежных прав.

В подходе Евросоюза, как уже отмечалось ранее, ясно *разграничивается* регулирование телекоммуникаций и контента (порядок доступа к контенту, его трансграничное использование и т.д.). Вместе с тем, объективная взаимосвязанность телекоммуникаций и контента, реализация задач Единого цифрового рынка Евросоюза очевидным образом диктуют общий дискурс их регулирования. В частности, контент, охраняемый авторским правом в рамках Евросоюза, стал предметом регулирования новой Директивы (ЕС) 2019/790 об авторском праве и смежных правах на едином цифровом рынке, изменяющей Директивы 96/9/ЕС и 2001/29/ЕС (далее – «Директива 2019/790» или «Директива об авторском праве»). Эта Директива, принятая 17 апреля 2019 года Европейским парламентом и Советом, 7 июня 2019 года вступила в силу.

Не углубляясь в детали, заметим, что цели Директивы 2019/790 продиктованы «цифровой повесткой» ЕС и направлены на обеспечение эффективно функционирующего цифрового рынка авторских прав, расширение доступа к нему потребителей и бизнеса в масштабах ЕС и Европы и т.д. В формате настоящей статьи важно обратить внимание на фактическое совпадение временных сроков подготовки и принятия Директивы 2019/790 и Телекоммуникационного Кодекса, рассмотренного выше, и, что существеннее, на непосредственную содержательную связь норм этих двух актов (речь об этом далее). При этом нельзя не задаться вопросом: почему обсуждение Директивы 2019/790, в отличие от Телекоммуникационного Кодекса, было столь драматичным, ее принятие прошло с мизерным перевесом голосов[30], а острые перипетии не утихают до сих пор? Однозначно ответить на этот вопрос невозможно по целому ряду причин, поэтому последующее рассмотрение Директивы 2019/790 логично ограничить выявлением тех причин, которые дают ответ на этот вопрос.

Прежде всего, Директива 2019/790, ее формальные и содержательные характеристики подлежат рассмотрению в конфигурации двух взаимосвязанных и взаимообусловленных параметров: специфики правового регулирования исключительных прав и особенностей правовой системы ЕС, которые, в частности, обусловлены рамками общенормативных основ авторского и смежных прав в ЕС, а также «форматом» транспонирования директив. Сказанное следует кратко пояснить.

Специфика правового регулирования всех исключительных прав в целом (включая авторские и смежные права) обусловлена действием принципа «территориальности», который является общим и традиционным для всех правопорядков. В практическом плане «территориальная ограниченность» регулирования исключительных прав означает признание исключительного права на результат интеллектуальной деятельности, его содержание, действие, ограничения прав, порядок защиты и т.д. определяются национальным правом[31]. Такая «территориальная ограниченность» регулирования «преодолима» либо в силу соответствующих норм национального права, либо в силу международного договора[32].

Спецификой правовой системы ЕС является обязательность для стран-членов ЕС законодательных норм, закрепляемых в актах «вторичного права» (регламенты, директивы, решения)[33]. Акты «вторичного права» ЕС, будучи обязательными законодательными актами различной юридической силы, унифицируют общенормативные основы регулирования в конкретной сфере отношений на уровне Евросоюза и гармонизируют соответствующее национальное законодательство стран-членов ЕС. Обобщенно, «территориальная ограниченность» регулирования в сфере авторских и смежных прав в Евросоюзе в той или иной мере «преодолевается» в силу соответствующих норм «вторичного права» ЕС.

Общенормативная основа регулирования в сфере авторских и смежных прав в Евросоюзе начала формироваться в 90-х годах XX века. Формирование общенормативной основы осуществлялось преимущественно посредством принятия директив, предметно регулирующих конкретную область: спутниковое вещание и кабельная ретрансляция, компьютерные программы, права проката, базы данных и т.д.[34]. Пожалуй, только Директива 2001/29/ЕС от 22.05.2001 г. об унификации некоторых аспектов авторского и смежных прав в информационном обществе[35] выступала неким комплексным нормативным актом. Директивы, безусловно, определяли рамки общенормативной основы ЕС в сфере авторских и смежных прав[36] и способствовали гармонизации национального законодательства стран-членов ЕС. Однако каждая директива принималась в разный период времени; каждая директива, в силу ее опосредованного действия, была транспонирована в разное время с учетом особенностей национального правового регулирования авторских и смежных прав в конкретном государстве-члене ЕС, а также специфики предметной сферы регулирования конкретной директивы. Такая ситуация, в итоге, не могла не привести к разрозненности (т.н. лоскутности) национального законодательства стран-членов ЕС в рассматриваемой сфере отношений.

К моменту принятия Директивы 2019/790 действующая общенормативная основа ЕС в сфере авторских и смежных прав была унифицирована двумя регламентами 2017 года[37] и объединяла более десятка директив. Директива 2019/790, несмотря на ее «широкую» предметную направленность, корреляцию реформированным положениям ряда актов ЕС в «пограничных» областях, включая сферу телекоммуникаций, становилась интеграционной частью общенормативной основы ЕС, но в целом ее принятие не меняло ни сложившуюся «предметную фрагментацию», ни разрозненность национального законодательства стран-членов ЕС в сфере авторских и смежных прав.

Изложенное дает основание для вывода о том, что «законодательный фон» регулирования авторских и смежных прав в Евросоюзе и в странах-членах ЕС явились теми причинами, которые привели к разности позиций стран-членов ЕС в отношении Директивы 2019/790.

Директива 2019/790 подлежит транспонированию (до 7 июня 2021 года) и, несмотря на право стран-членов ЕС самостоятельно устанавливать формы и методы транспонирования (принятие законодательных мер, закрепление содержания понятий, определение административных правил, процедур и проч.)[38], обязательному учету подлежат ограничения и исключения, предусмотренные Директивой 2019/790. Наиболее резкую критику вызвали ограничения и исключения, предусмотренные статьями 15 и 17, предмет которых в общем плане связан с урегулированием и обеспечением баланса интересов правообладателей, онлайн-платформ и интернет-пользователей. Положения статей 15 и 17 далее рассмотрены с акцентом на «спорные» моменты, а также с учетом содержания общих понятий, операционализация которых закреплена Директивой 2019/790.

Проект Регламента о террористическом контенте исходит из основополагающего принципа: «то, что незаконно в офлайн-формате, равным образом является незаконным в формате онлайн» - и закрепляет комплекс мероприятий, которые поставщики услуг хостинга (*hosting service providers*) и государства-члены ЕС должны предпринимать в целях борьбы с распространением террористического контента в Интернете.

Статья 15 «Защита публикаций в печатном издании, связанная с онлайн-использованием» (*Protection of press publications concerning online uses*) предусматривает право издателей печатных изданий предоставлять свои публикации для их использования в онлайн-режиме провайдерами услуг информационного общества. Понятие «публикация в печатном издании» (*press publication*)[39] содержательно означает: сборник/печатное издание, преимущественно объединяющее литературные произведения публицистического характера, а также иные произведения или объекты, среди которых находится отдельная заметка в периодическом или регулярно обновляемом издании (газеты, журналы общей или специализированной направленности и т.д.). Такое печатное издание/сборник публикуется по инициативе редакции и под ее ответственностью, а также под контролем поставщика услуг, публикация осуществляется в любых средствах массовой информации для публичного предоставления неограниченному кругу лиц информации новостей, иной тематической информации (п. (4) ст. 2 Директивы 2019/790). Директива 2019/790 исключает из сферы своего действия публикации в периодических научных/академических изданиях.

Согласно статье 15, государства-члены ЕС должны обеспечить, чтобы авторы соответствующих публикаций получали свою долю доходов, наряду с доходами, получаемыми издателями печатных изданий за использование их изданий провайдерами услуг информационного общества. В практическом плане эта норма означает, что печатные издания (включая отдельные опубликованные в них материалы) при их использовании онлайн рассматриваются как контент, охраняемый авторским правом; издатели печатных изданий и авторы публикаций при использовании их изданий/публикаций онлайн должны получать вознаграждение (включая случаи ссылок на их издания/публикации); ответственность за «соблюдение авторских прав в Интернете» переносится на провайдеров услуг информационного общества. Ряд «европейских критиков» оценивают эту норму как «введение налога на ссылки» (*link tax*)[40]. Такая оценка вполне понятна, в т.ч. с точки зрения того, что принятием этой нормы расширяется предметная сфера заключения лицензионных договоров; издатели печатных изданий получают право в договорном порядке закреплять условия о лицензионных сборах за ссылки на их цифровой контент; при использовании их публикаций онлайн без соответствующего разрешения издатели печатных изданий могут пользоваться средствами правовой защиты, включая обращение в суд.

Для положений статьи 17 «Использование охраняемого контента поставщиками услуг обмена онлайн-контентом» (*Use of protected content by online content-sharing service providers*) понятие «поставщик услуг обмена онлайн-контентом» (*online content-sharing service provider*)[41] имеет ключевое значение. Это понятие означает поставщиков услуг информационного общества, основной или одной из основных целей которых является хранение и предоставление публичного доступа к большому количеству охраняемых авторским правом произведений или иных охраняемых объектов, загружаемых пользователями, систематизируемых и распространяемых такими поставщиками в коммерческих целях (п. (6) ст. 2 Директивы 2019/790). Однако в силу упомянутого ранее разграничения регулирования в Евросоюзе телекоммуникаций

и контента, Директива 2019/790 предусматривает, что к «поставщикам услуг обмена онлайн-контентом» не относятся поставщики услуг некоммерческих онлайн-энциклопедий, некоммерческих образовательных/научных библиотек/архивов, платформы для разработки продуктов с открытым исходным кодом и обмена ими, поставщики услуг электронных коммуникаций - *в значении, установленном Директивой о Кодексе* (выделено нами – М.К.); а также торговые онлайн-площадки, облачные сервисы B2B, сервисы, позволяющие пользователям загружать контент для собственных нужд.

Нормативные положения статьи 17 предусматривают обязательства и условия ответственности «поставщиков услуг обмена онлайн-контентом», среди которых: обязанность поставщиков услуг обмена онлайн-контентом получать разрешение от правообладателей (в т.ч. посредством заключения лицензионных соглашений) на использование их произведений или иных объектов в «цифровом формате»; ответственность за неправомерное использование охраняемых произведений и объектов и предоставление доступа к ним, а также за контент, загружаемый третьими лицами, который охраняется авторским правом. Однако резонную критику вызывают «пространные» и «расплывчатые» формулировки. Так, при закреплении условий, предусматривающих освобождение «поставщиков услуг обмена онлайн-контентом» от ответственности, использованы формулировки: «*приложить все усилия* для получения разрешения, чтобы предотвратить нарушение авторских прав»; «*продемонстрировать*, что они оперативно удалили контент после получения предупреждения от владельца прав» (п. 4 (а) – (с) ст. 17 Директивы). Кроме того, закреплены положения, предусматривающие различный объем обязательств и ответственности (исходя из содержания понятия «поставщиков услуг обмена онлайн-контентом»), возлагаемый на коммерческие онлайн-платформы (*Google*, *YouTube*, *Facebook*, *DailyMotion*, *GAFA* и др.), с одной стороны, и на некоммерческие интернет-платформы (*Wikipedia*, *GitHub* и др.) – с другой. Но (!) определение собственно самого «режима ответственности» отсутствует, а это не может не увеличивать числа вопросов, подлежащих уточнению. Примечательно, что из неоднозначности норм статьи 17 в отношении «режима ответственности» исходит собственно сама Директива 2019/790. Это подтверждается статьей 30 «Критический обзор». Непосредственно ссылаясь на статью 17, а также п. (6) статьи 17, нормы статьи 30 обязывают Еврокомиссию до 7 июня 2024 года оценить «режим ответственности», применимый к поставщикам услуг обмена онлайн-контентом и принять соответствующие меры в необходимых случаях[42].

Положения статей 15 и 17 рассмотрены кратко и лапидарно, что диктуется форматом и контекстом настоящей статьи. Сказанное выше, тем не менее, свидетельствует о расширении пределов авторских прав и «приоритетности» защиты правообладателей, а это не может не нарушать баланса интересов правообладателей, онлайн-платформ и интернет-пользователей. Содержание «спорных» положений статей 15 и 17 подводит к объяснению причин «драматизма перипетий» по Директиве 2019/790.

2.2. Регулирование предотвращения распространения террористического контента в Интернете.

Наряду с целым рядом директив и регламентов, вступивших в силу, (включая те, которые рассмотрены выше), параллельно в Евросоюзе в последние годы обсуждается комплекс предложений о принятии новых актов «в русле цифровой повестки» и регулирования контента. Так, первое чтение прошла законодательная резолюция Европейского парламента о предложении относительно принятия Регламента Европейского парламента и Совета, связанного с предотвращением распространения террористического контента в Интернете, принятая 17 апреля 2019 года[43] (далее – «проект Регламента о террористическом контенте»).

Основой текста проекта Регламента о террористическом контенте послужило соответствующее предложение Еврокомиссии (сентябрь 2018 года)[44], которое широко обсуждалось заинтересованными участниками интернет-сообщества разного уровня с участием уполномоченных органов Евросоюза; более того, к обсуждению были привлечены эксперты Совета по правам человека ООН (*UN Human Rights Council*). В ходе различных публичных обсуждений выявилась разность (если не сказать противоположность) позиций: представители интернет-организаций «гражданской ориентации» выступали за сохранение открытости Интернета и свободу обмена информацией, призывая избегать «избыточности публично-правового регулирования»[45]; представители научно-академического сообщества предлагали закрепить ясно выверенную квалификацию ключевых понятий (прежде всего понятия «террористического контента в Интернете» – «*terrorist content online*»), детально разграничив виды «террористического контента»; ряд провайдеров интернет-услуг высказывались в пользу необходимости взаимодействия с правоохранительными органами и добровольного соблюдения мер их регуляторного вмешательства; правообладатели призывали усилить ответственность провайдеров интернет-услуг, включая провайдеров социальных сетей, в том числе за несвоевременное удаление террористического контента. Вариативность подходов изложена весьма обобщенно, однако о ней следует сказать, т.к. текст проекта Регламента о террористическом контенте содержит множество поправок и уточнений, аккумулирующих итоги обсуждения обозначенных позиций.

Проект Регламента о террористическом контенте исходит из основополагающего принципа: «то, что незаконно в офлайн-формате, равным образом является незаконным в формате онлайн» - и закрепляет комплекс мероприятий, которые поставщики услуг хостинга (*hosting service providers*) и государства-члены ЕС должны предпринимать в целях борьбы с распространением террористического контента в Интернете. Обозначим в порядке перечисления лишь некоторые положения проекта Регламента о террористическом контенте:

- предусматривается, что действие Регламента будет распространяться на всех поставщиков услуг хостинга (*hosting service providers*), независимо от места их основ-

ного учреждения, если они предлагают услуги в Евросоюзе широкому кругу лиц;

- закреплен ряд понятий и дано определение их содержания (в частности, «поставщик контента» (*content provider*); «террористический контент» (*terrorist content*); «распространение террористического контента» (*dissemination of terrorist content*) и др.), вместе с тем, в проекте использованы иные понятия (например, «определение террористического контента для принятия превентивных мер» (*terrorist content for preventative purposes*)[46], «наиболее вредоносный террористический контент в Интернете» (*most harmful terrorist content online*), «публичное распространение террористического контента» (*public dissemination of terrorist content online*) и др.), однако они содержательно не определены (по-видимому, это будет уточнено в дальнейшем);

- содержатся положения процедурного плана относительно порядка выдачи ордера об удалении (*removal order*) террористического контента, порядка взаимодействия между национальным уполномоченным органом и поставщиком услуг хостинга применительно исполнения ордера об удалении;

- предусмотрено т.н. правило одного часа (*the one-hour rule*), что означает установление юридически обязательного срока в один час для удаления террористического контента в соответствии с ордером об удалении (*removal order*), выданным соответствующим национальным уполномоченным органом;

- регламентирован порядок относительно выдачи дополнительных ордеров об удалении (*additional removal order*);

- предусмотрена обязанность поставщиков услуг хостинга сохранять террористический контент (удаленный, отключенный и т.д. - в соответствии с ордером об удалении) в течение шести месяцев, а также перечислены цели и порядок сохранения такого террористического контента;

- установлены обязательства поставщиков услуг хостинга по принятию мер превентивного и профилактического характера для оптимальной защиты платформ и их пользователей от террористического контента.

Проект Регламента о террористическом контенте обсуждается на регулярной основе и его принятие будет утверждаться новым составом Европейского парламента, выборы в который прошли в мае нынешнего года.

Возвращаясь к названию настоящей статьи и не повторяя те тезисы, которые были изложены выше, целесообразно отметить, что правовое регулирование телекоммуникаций в Евросоюзе прошло достаточно значительный эволюционный путь, в течение которого последовательно, системно и комплексно формировались и совершенствовались соответствующие правовые инструменты и методы. «Цифровая повестка ЕС», придав новый импульс развитию этого процесса, в настоящее время определяет общий дискурс консолидации регулирования телекоммуникаций и контента с учетом их объективной взаимосвязанности и взаимообусловленности, при одновременном реформировании нормативных и институциональных основ такого регулирования. Регуляторный опыт Евросоюза в рассмотренных сферах отношений, безусловно, существенен и полежит анализу. Такой анализ своевременен, прежде всего, как в связи с актуальностью «цифровой повестки» для многих современных государств как в контексте их внутринационального развития, так и в контексте интеграционных процессов, в которые многие из них вовлечены[47]. Общие рамки решения задач «цифровой повестки» определяет «ускоренная» динамика расширения применения информационно-коммуникационных технологий, а это едва ли оставляет государствам время на «эволюционный» путь развития соответствующего правового регулирования.

Ссылки

1. «*European legal instruments*» – URL: https://eur-lex.europa.eu/summary/glossary/community_legal_instruments.html

2. *Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. Официальный журнал ЕС, L 321/36, 17.12.2018

3. *Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009*. Официальный журнал ЕС L 321/1, 17.12.2018. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2018.321.01.0036.01.ENG

4. *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Официальный журнал ЕС, L 130/92, 17.05.2019.

5. *Legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)*. – URL: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.html

6. Директива о Телекоммуникационном Кодексе и Регламент 2018/1971, как акты «вторичного» права ЕС, были одновременно опубликованы в Официальном журнале Европейского Союза 17.12.2018 и, согласно действующей процедуре, на двадцатый день после их опубликования они вступили в силу (т.е. в 28.12.2018 г.). Официальный журнал ЕС. Право 321/1, 17.12.2018.

7. Ст. 288 Договора о функционировании Евросоюза (*Treaty on the Functioning of the European Union, TFEU*): «Регламент имеет общее действие. Он является обязательным в полном объеме и подлежит прямому применению во всех государствах-членах». Офици-

альный журнал ЕС C 326, 26.10.2012, P. 0001 – 0350. В практическом плане прямое регуляторное действие регламента не предполагает принятие имплементирующих актов; исключает действие национальных правовых актов, противоречащих регламенту; означает его непосредственное применение Судом Справедливости ЕС (*EU Court of Justice*), решения которого носят прецедентный характер. Об этом подробнее, например: Базедов Ю. Право открытых обществ – частное и государственное регулирование международных отношений: общий курс международного частного права / пер. с англ. Ю. М. Юмашева. М.: Норма, 2016. и др. // СПС КонсультантПлюс.

8. *European Commission, Towards a Dynamic European Economy – Green Paper on the Development of a Common Market for Telecommunications Services and Equipment, COM (87) 290 (1987)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0084

9. *EU Single Market Program* 1992 г. – URL: http://europa.eu/rapid/press-release_DOC-92-1_en.htm

10. *Council Resolution 88/C 257 of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992*. Официальный журнал C 257, 4.10.88 (88/C 257; OJ C257, 4.10.88).

11. *Council Directive 87/372/EEC of 25 June 1987 on the frequency bands to be reserved for the coordinated introduction of public pan-European cellular digital land-based mobile communications in the Community*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0084

12. *Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access*. Официальный журнал ЕС, L 320/5420, 20/11.1998.

13. *Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)*. Официальный журнал ЕС, Право 108 , 24/04/2002 С. 0007 – 0020.

14. *Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorization Directive)*. Официальный журнал ЕС, Право 108, 24/04/2002 С. 0021 – 0032.

15. *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)*. Официальный журнал ЕС, Право 108, 24/04/2002 С. 0033 – 0050.

16. *Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)*. Официальный журнал ЕС, Право 108, 24/04/2002 С. 0051 - 0077.

17. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Официальный журнал ЕС, Право 201 31/07/2002 С. 0037 – 0047.

18. *Commission Decision 2002/627/EC of 29 July 2002 establishing the European Regulators Group for Electronic Communications Networks and Services*. Официальный журнал ЕС L 200, 30/07/2002. С. 38).

19. *Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens*. – URL: http://europa.eu/rapid/press-release_MEMO-09-219_en.htm?locale=en

20. *Directive 2009/114/EC of 16 September 2009 amending Council Directive 87/372/EC Directive modernizing the 1987 GSM Directive*. – URL: http://europa.eu/rapid/press-release_IP-09-1545_en.htm?locale=en

21. *Regulation (EU) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office*. Официальный журнал ЕС L 337/1 ,18/12/2009.

22. *BEREC Mediumterm Strategy Outlook 2012*. – URL: https://www.berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/56-berec-mediumterm-strategy-outlook; а также *BEREC Strategy 2015-2017*. – URL: https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/4785-berec-strategy-2015-2017

23. *Decision taken by common accord between the Representatives of the Governments of the Member States of 31 May 2010 on the location of the seat of the Office of the Body of European Regulators for Electronic Communications (BEREC) (2010/349/EU)*. Официальный журнал ЕС. Право. 156, 23.6.2010, С. 12.

24. *Telecom Reform Package*. Официальный журнал ЕС L 33 ,18/12/2009. Volume 52. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2009:337:TOC

25. *A Digital Single Market Strategy for Europe*. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192. См. также Программу единого рынка (*EU Single Market Program*) 1992 г.*EU Single Market Program 1992*. – URL: http://europa.eu/rapid/press-release_DOC-92-1_en.htm. Активная реализация «цифровой повестки» ЕС наглядно проявилась и в деятельности BEREC, о чем свидетельствует содержание упомянутой Стратегии BEREC на 2015-2017 гг. – URL: https://berec.europa.eu/eng/document_register/

subject_matter/berec/annual_work_programmes/4785-berec-strategy-2015-2017

26. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe.* – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN

27. Напомним, что речь о Директиве 2002/19/ЕС «О доступе» (*Access Directive*), Директиве 2002/20/ЕС относительно разрешений общего характера (*Authorization Directive*); Рамочной Директиве 2002/21/ЕС (*Framework Directive*) и Директиве 2002/22/ЕС об универсальных услугах (*Universal Service Directive*).

28. Так, согласно Директиве о Телекоммуникационном Кодексе, контент/содержание телевизионных программ подлежит регулированию Директивой 2010/13/ЕС Европейского Парламента и Совета от 10 марта 2010 г. о координации соответствующих положений, предусмотренных правом, законодательными нормами или административными мерами в государствах-членах, касающихся аудиовизуальных медиауслуг (Директива об аудиовизуальных медиа-услугах) (ОЖ, Право 95, 15.4.2010, с. 1).

29. BEREC Strategy 2018- 2020. – URL: https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/7310-berec-strategy-2018-2020

30. Голосование по Директиве об авторском праве и смежных правах: «за» – 348, «против» – 274 (в т.ч. (Италия, Люксембург, Нидерланды, Польша, Финляндия, Швеция и др.), «воздержавшиеся» – 36 (в т.ч. Бельгия, Словения, Эстония и др.). – URL: https://www.consilium.europa.eu/en/press/press-releases/2019/04/15/eu-adjusts-copyright-rules-to-the-digital-age/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+adjusts+copyright+rules+to+the+digital+age, а также – URL: https://www.consilium.europa.eu/en/press/press-releases/2019/04/15/eu-adjusts-copyright-rules-to-the-digital-age/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+adjusts+copyright+rules+to+the+digital+age, – URL: https://www.leadersleague.com/en/news/european-copyright-directive-the-supporters-reasoning

31. См. об этом, например, Право интеллектуальной собственности. Общие положения. Том 1. (Под общ. ред. Л. А. Новоселовой). М., Статут, 2017 // СПС КонсультантПлюс.

32. См. об этом подробнее, например, Дозорцев В. А. Интеллектуальные права: Понятие. Система. Задачи кодификации: Сб. статей. М.: Статут, 2003; а также Право интеллектуальной собственности. Указ. раб. Том 1, 2. (Под общ. ред. Л. А. Новоселовой). М.: Статут, 2017. // СПС КонсультантПлюс и др.

33. Интеграционное право в современном мире: сравнительно-правовое исследование: монография / В. А. Жбанков, П. А. Калиниченко, С. Ю. Кашкин и др.; отв. ред. С. Ю. Кашкин. Москва: Проспект, 2015. // СПС КонсультантПлюс.

34. См., например, Директиву Совета (91/250/ЕЭС) от 14 мая 1991 г. о правовой охране компьютерных программ; Директиву Совета Европейского Сообщества (92/100/ЕС) от 19 ноября 1992 г. по вопросам охраны прав проката и использования и иных прав, смежных с авторским правом, в сфере интеллектуальной собственности; Директиву Совета Европейского Сообщества (93/83/ЕС) от 27 сентября 1993 г. о согласовании ряда правил, касающихся охраны авторского права и смежных прав в сфере спутникового вещания и кабельной ретрансляции; Директиву Европейского Совета (93/98/ЕС) от 29 октября 1993 г. о согласовании сроков защиты авторских и смежных прав и др. Об этом: Юридические контуры Большой Европы. *Европейское экономическое пространство.* – URL: https://eulaw.edu.ru/spisok-dokumentov-po-pravu-evropejskogo-soyuza/direktiva-soveta-ot-14-maya-1991-g-o-pravovoj-ohrane-kompyuternyh-programm-91-250-ees-perevod-a-o-chetverikova/

35. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0029

36. Например, Директива 98/84/ЕС от 20.11.1998 г. о правовой защите услуг, с использованием условного доступа или основанных на условном доступе, Директива 2000/31/ЕС от 8 июня 2000 г. о некоторых правовых аспектах информационного общества, услугах, в частности, электронной торговли на внутреннем рынке (*E-commerce Directive*). – URL: https://ec.europa.eu/digital-single-market/en/e-commerce-directive; кроме того, действие общенормативной основы ЕС учитывает соответствующую практику Суда Справедливости ЕС (*EU Court of Justice*), международных договоров, заключенных Евросоюзом. – URL: https://ec.europa.eu/digital-single-market/en/eu-copyright-legislation

37. Речь идет о Регламенте (ЕС) 2017/1128 Европейского парламента и Совета от 14.06.2017 г. о трансграничной переносимости услуг онлайн-контента в рамках внутреннего рынка («Регламент о портативности»). *Regulation on cross-border portability of online content services in the internal market («Portability Regulation»)* – URL:https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R1128; а также о Регламенте (ЕС) 2017/1563 Европейского Парламента и Совета от 13.09.2017 г. о трансграничном обмене между ЕС и третьими странами портативными копиями некоторых произведений и иных объектов, охраняемых авторскими смежными правами в интересах слепых, слабовидящих, а также лиц с ограниченными возможностями восприятия печатной информации. (*Regulation (EU) 2017/1563 of the European Parliament and of the Council of 13 September 2017 on the cross-border exchange between the Union and third countries*

of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled) – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1563

38. Государства-члены ЕС должны направить информация о принятых национальных мерах в Еврокомиссию. Интеграционное право в современном мире: сравнительно-правовое исследование: монография / В. А. Жбанков, П. А. Калиниченко, С. Ю. Кашкин и др.; отв. ред. С. Ю. Кашкин. Москва: Проспект, 2015. // СПС КонсультантПлюс.

39. Используется разный перевод на русский язык понятия «*press publication*»: «печатная публикация», «публикация в прессе» и т.д., но более адекватным представляется используемый в настоящей статье перевод – «публикации в печатном издании», т.к. речь идет о печатном/периодическом издании.

40. См., к примеру: Your memes are safe, but these are the other fiercely opposed changes Europe is making to the internet. – URL: https://www.businessinsider.com/explained-article-15-and-article-17-2019-3; Интеллектуальная собственность в Интернете. – URL: http://lexdigital.ru/2017/121/

41. Встречается различный перевод на русский язык понятия «*online content-sharing service provider*» переводится на русский язык: интернет-провайдер контента», «поставщик контента в онлайн-режиме» и т.д.

42. См. ст. 30 Директивы об авторском праве. *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Официальный журнал ЕС, L 130/92, 17.05.2019. Помимо этого, ст. 30 возлагает на Еврокомиссию обязанность (до 7.06.2026 г.) представить обзорный доклад Европейскому Парламенту, Совету и Европейскому экономическому и социальному комитету по применению этой Директивы.

43. Законодательная резолюция от 17 апреля 2019 г. относительно предложения о принятии Регламента Европейского Парламента и Совета по предотвращению онлайнового распространения террористического контента (*Legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)*. – URL: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.html Законодательная резолюция прошла первое чтение. См. также Малов А. А. Об опыте борьбы Европейского союза с противоправным контентом // Международное публичное и частное право. 2019. № 3. С. 34-37.

44. *Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.*– URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0640

45. См. например, Klompmaker Naomi. A Social and Legal Assessment of Enhanced Action Against Terrorist Content Online. – URL: http://amsterdamlawforum.org/article/view/462

46. В проекте Регламента (Преамбула) содержится ссылка на то, что исходными положениями в целях выявления террористического контента для принятия превентивных мер является Директива (ЕС) 2017/541 О борьбе с терроризмом 2017 г. – *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.* Официальный журнал ЕС, Право 88, 31.3.2017, С. 6.

47. К примеру, «цифровая повестка» диктует комплекс интеграционных мероприятий, осуществляемых в рамках Евразийского экономического союза (ЕАЭС) См., об этом: Цифровая повестка ЕАЭС 2025: перспективы и рекомендации. – URL: http://www.eurasiancommission.org/ru/act/dmi/Pages/digital_agenda.aspx

Бесфайловое вредоносное программное обеспечение

Дэвид Стром (David Strom)

С течением времени авторы вредоносных программ становятся все более искусными и хитрыми, затрудняя обнаружение своего кода и предотвращение его действия. Одним из наиболее тревожных последних «достижений» стало появление «бесфайловых» вирусов. В этом случае существует весьма серьезная причина для беспокойства, поскольку такой тип атак может нанести более серьезный ущерб, а само вредоносное ПО может целыми неделями или месяцами находиться в ваших компьютерах и сетях до того момента, когда оно будет, наконец, нейтрализовано. Давайте поговорим о том, что собой представляет это вредоносное ПО, и лучше поймем его особенности с тем, чтобы попытаться вообще предотвратить его проникновение в наши сети.

С течением времени авторы вредоносных программ становятся все более искусными и хитрыми, затрудняя обнаружение своего кода и предотвращение его действия. Одним из наиболее тревожных последних «достижений» стало появление «бесфайловых» вирусов. В этом случае существует весьма серьезная причина для беспокойства, поскольку такой тип атак может нанести более серьезный ущерб, а само вредоносное ПО может целыми неделями или месяцами находиться в ваших компьютерах и сетях до того момента, когда оно будет, наконец, нейтрализовано. Давайте поговорим о том, что собой представляет это вредоносное ПО, и лучше поймем его особенности с тем, чтобы попытаться вообще предотвратить его проникновение в наши сети.

Обычно целью большинства вредоносных программ является внедрение в одной из конечных точек (сети, компьютера) чего-то «вещественного» – одного или нескольких файлов, которые содержат исполняемую программу, повреждающую ваш компьютер, превращающую его в часть ботнета или копирующую конфиденциальные данные и перемещающую их во внешнее хранилище. Со временем различные средства обнаружения научились лучше находить эти – как их называют – *остаточные следы* и блокировать их.

Однако борьба с вредоносным ПО напоминает игру в «кошки-мышки», и по мере того, как защита все лучше останавливает такие программы, их авторы совершенствуют способы ускользания от барьеров. В ранние годы развития Интернета большинство блокирующих процедур искали определенные сигнатуры либо в виде имени одной из программ, исполняющихся на вашем ПК, либо в виде конкретных паттернов поведения в рамках сети. Все эти опции работали до тех пор, пока авторы вредоносных программ не научились лучше скрывать свой характерный почерк.

И именно в этот момент в игру вступают бесфайловые вирусы. Их целью является оставление как можно меньшего количества следов, чтобы затруднить свое обнаружение антивирусными продуктами. Либо, что еще лучше, ввести их в заблуждение, маскируя свои действия под видом чего-то, что может делать незараженная операционная система.

Фактически название «бесфайловый» частично искажает смысл, поскольку такая программа все-таки кое-что после себя оставляет. Возможно, это не будет полный исполняемый файл или файл DLL, однако некоторый программный код все же используется для фактического выполнения ряда процессов, которые делают «грязную работу» вредоносной программы. Начиная с 2016 года исследователи отмечают возрастающие усилия авторов вредоносного ПО в этом направлении, и такие программы становятся все более популярными, поскольку подобный вирус может стать мощным средством заражения, которое нелегко найти или предотвратить[1].

Типы бесфайловых атак

Бесфайловое вредоносное ПО использует три разных типа атак: *возвратно-ориентированное программирование*, *атаки на базе скриптов* и *полиморфные атаки*. Каждая из них имеет свои отличия.

Первый тип атак получил название *возвратно-ориентированного программирования*, которое является наиболее популярным и может считаться «классической» версией. Такая вредоносная программа может исполнять стандартные DLL-файлы и другие последовательности кода, которые способны обеспечить несанкционированный доступ к незараженной системе. Подобный код может также входить в состав вашего веб-браузера или обычных инструментов *операционной системы* (ОС), например, приложений рабочего стола. Поскольку такой код уже присутствует в этих функциях операционной системы, не существует конкретного, фактически исполняемого «файла», который является уникальным для данной вредоносной программы.

Вместо этого автор вредоносного ПО для достижения своей цели эксплуатирует существующие в ОС методы.

Для того чтобы реализовать такой тип атак, автор должен быть знаком с программным кодом, который планируется «захватить» в злонамеренных целях, и быть уверенным в том, что в целевой конечной точке исполняется конкретная версия кода для этой операционной системы. Незначительные изменения в версиях ОС, например, переход с Windows 7 на 7.1 или с MacOS 10.12.5 на 10.12.6, могут сорвать атаку, поскольку изменилась база кода. Либо если Microsoft или Apple (в особенности учитывая их популярность и установленную базу ПО) выпустят патч для исправления потенциальной уязвимости.

Атаки на базе скриптов являются вторым типом бесфайлового вредоносного ПО. Еще один метод, позволяющий избежать обнаружения, заключается в использовании встроенных в Windows механизмов выполнения скриптов, таких как Microsoft Office, Windows *PowerShell* или Microsoft HTML Application Host. Обычно такие атаки используют преимущества привязки к процессам и не оставляют никаких файловых следов в конечной точке. Если ваша система обнаружения не видит исполнение скрипта или не понимает аргументы командной строки, то вы не сможете без промедления определить наличие вредоносного ПО.

Например, типовой вредоносный скрипт распределяет память, выбирает прикладные программные интерфейсы и загружает некоторые исполняемые файлы прямо в память целевого ПК. После проникновения в память он начинает вредоносную деятельность и использует целевой ПК для изучения локальной сети и нахождения других целей, часто запуская другие вредоносные скрипты PowerShell, которые используют эскалацию привилегий и удаленное исполнение. Все это множество операций должно избегать обнаружения и делать грязную работу для злоумышленника. Однако большая часть из этих действий выполняется «вне поля видимости» и, возможно, будет обнаружена только через несколько месяцев с помощью детального ретроспективного анализа, который способен зафиксировать последовательность событий, развернувшихся в ходе конкретной атаки.

Скриптовые атаки набирают популярность в основном по причине того, что в типовом современном ПК имеется большое количество встроенного ПО, которое может выполнять то, что требуется вредоносной программе: получать доступ к общему сетевому диску, копировать части файлов, настраивать некий инструмент мониторинга и т.д. Зачем заново «изобретать колесо», если оно уже имеется в составе среднего настольного ПК или ноутбука?

Третий метод получил название *полиморфной атаки*. Такие атаки адаптируются к широкому спектру условий, операционных систем и обстоятельств, а также пытаются избежать сканирования и средств защиты с целью заражения конечных точек. Их называют полиморфными, поскольку они меняют свои сигнатуры, методы атаки и цели, что затрудняет их идентификацию и «поимку». Злоумышленники обычно используют полиморфизм как один из множества методов обфускации (запутывания) для того, чтобы скрыть вирус от средств защиты, например, определяя, если они работают внутри *виртуальной машины* (излюбленная хитрость исследователей), или шифруют свой код для маскировки исполняемых файлов.

За последние несколько лет поставщики решений в сфере безопасности начали брать на вооружение принцип полиморфизма и превратили его в защитный маневр. Идея заключается в том, чтобы создать видимость того, что целевой веб-сервер или другая единица сетевой инфраструктуры часто изменяются, затрудняя их идентификацию и заражение. Иногда такой метод называют *защитой с помощью подвижной мишени*, что может быть синонимом некоего аспекта защиты, который изменяет природу приложений или участков кода. В число этих поставщиков входят компании Morphisec, Shape Security и Polyverse – все они стартапы. Один из таких стартапов – CyActive – добился достаточного успеха, чтобы его купила компания PayPal.

Полиморфные средства защиты могут ограничить период времени, в течение которого потенциальный злоумышленник способен вторгнуться в сеть, поскольку создается видимость того, что целевая система движется по сети или меняются ее свойства.

Исследователи рассматривают комбинации из всех трех видов атак и считают, что это сделает их еще более изощренными и трудными для отслеживания. В некоторых случаях авторы вредоносного ПО планируют сразу несколько типов атак с тем, чтобы гарантировать, что часть их кода избежит средств защиты и проникнет в вашу сеть. Как я уже упоминал ранее, все это напоминает игру в кошки-мышки.

Образцы бесфайлового вредоносного ПО

Для того чтобы проиллюстрировать различия и эволюцию, давайте взглянем на несколько недавних примеров бесфайлового вредоносного ПО.

В 2014 году компания-ретейлер Target подверглась ставшему печально известным взлому. Оказалось, что вредоносное ПО попало в ее сеть с помощью очень простой стратегии: были раскрыты и скопированы реквизиты доступа в сеть одного из пользователей – в данном случае это оказался сотрудник поставщика систем отопления. Эта атака оказалась примечательна своей простотой и тем фактом, что топология сети Target была совершенно «плоской», без использования *виртуальных локальных сетей* (vLAN) или другой сегментации. Этот пример напоминает о том, что плохой дизайн сетевой инфраструктуры может сделать опасным любой вид вредоносного ПО – является ли оно бесфайловым или нет. Брайан Кребс (Brian Krebs) изучил обстоятельства и то, что пошло неправильно, написав об этой атаке в своём блоге[2].

Как большинство из вас уже знает, в 2016 году был взломан *Национальный комитет демократической партии США* (DNC). В ходе атаки была задействована бесфайловая вредоносная программа, которая воспользовалась средствами PowerShell и *Windows Management Instrumentation* (WMI) для того, чтобы «получить плацдарм» в системах политической партии.

Инструментарий WMI обычно используется в каждодневных задачах управления, таких как развертывание скриптов автоматизации, выполнение процесса в определенное время либо получение информации об установленных приложениях или аппаратном обеспечении.

Вредоносное ПО, проникшее в системы DNC, также использовало (инструмент написания скриптов) PowerShell в качестве инсценировочного инструмента для выполнения других скриптов, обеспечивающих взлом системы. Эта вредоносная программа использовала WMI для установки бэкдоров (программных закладок), которые обеспечивали злоумышленникам длительный доступ за счет автоматического запуска вредоносного кода через определенный период функционирования системы либо по специальному графику. Опять же, вредоносное ПО использовало все эти тактики для того, чтобы избежать обнаружения[3].

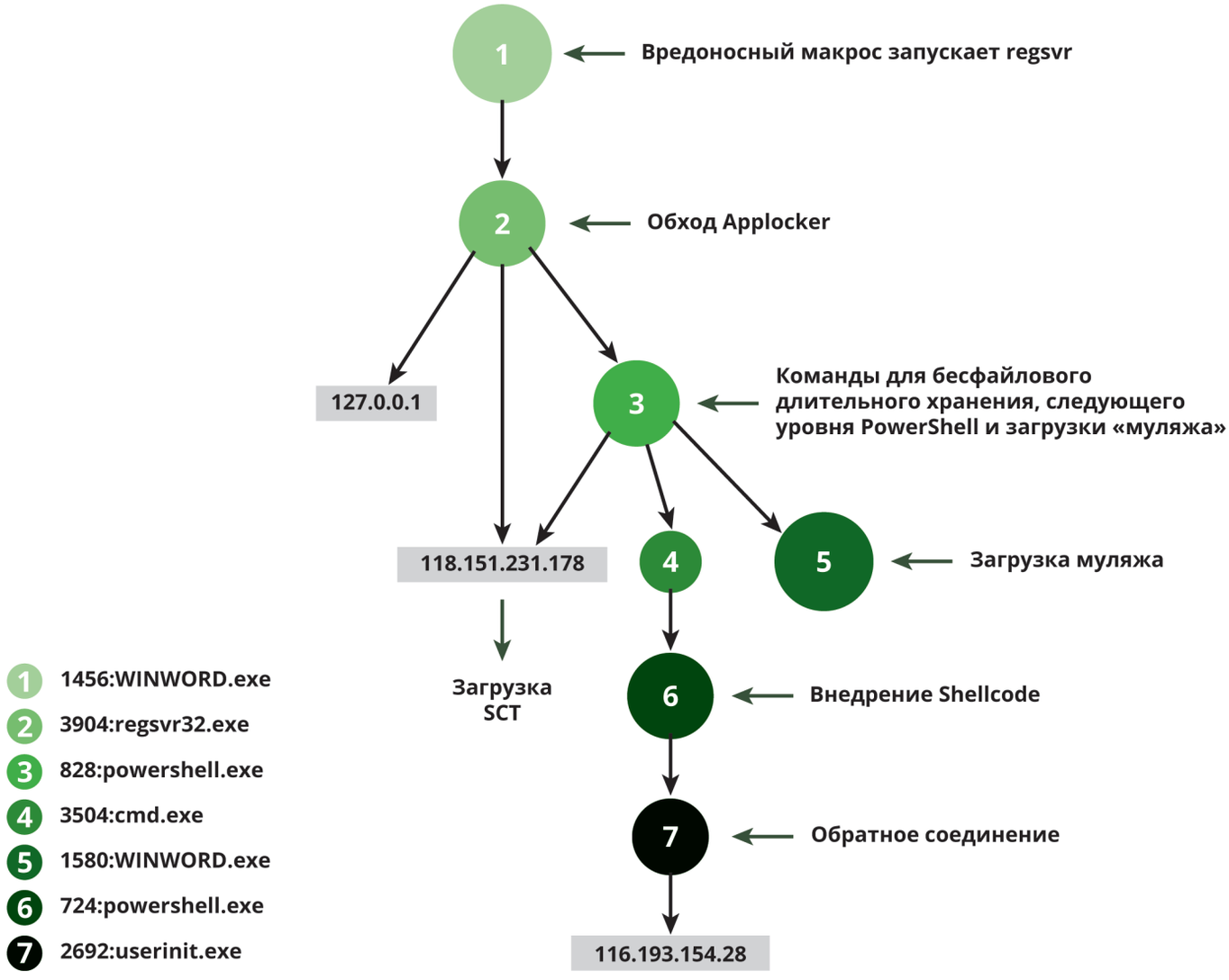
Вредоносная программа *August Stealer* была обнаружена в конце 2016 года и приписывается преступной группе TA530. Нацеленная на службы поддержки клиентов и персонал кол-центров, она использует зараженные макросы Word и скрипты PowerShell, доставленные через фишинговые электронные письма. Подобные электронные письма специально создаются так, чтобы выглядеть как запросы от пользователей по вопросам поддержки, и используют разнообразные темы, например, перечисленные ниже:

- Ошибочные платежи от [домен получателя]
- [домен получателя] Помогите: продукты исчезают из корзины до оформления и оплаты заказа
- [домен получателя] Поддержка: продукты исчезают из корзины во время оформления заказа
- Необходима помощь с заказом [домен получателя]
- Двойная плата за продукт [домен получателя]

Вредоносная программа *August Stealer* содержит функции для кражи из зараженных компьютеров идентификационных данных, бумажников криптовалют и конфиденциальных документов[4].

Обнаруженная в начале 2017 года вредоносная программа *Duqu2* – это еще один хороший пример первых бесфайловых вредоносов. Эта программа была обнаружена в более

Рис. 1. Модули Poison Ivy.



чем 140 корпоративных сетях, принадлежащих банкам, государственным организациям, телекоммуникационным компаниям в 40 разных странах.

Она принимает форму вредоносного скрипта PowerShell и набора значений системного реестра Windows, которые на тот момент были уникальными для программы и использовались для идентификации зараженных систем:

- **HKLM\SYSTEM\ControlSet001\services** – путь меняется после использования утилиты SC
- **HKLM\SYSTEM\ControlSet001\services\PortProxy\v4tov4\tcp** – путь меняется после использования утилиты NETSH

После того, как программа проникла на целевой жесткий диск, она запускается через вредоносный установщик Windows или файл MSI, который затем удаляет себя и переименовывает различные файлы для сокрытия своих действий. После того, как вредоносная программа будет установлена на ПК, она просто работает в памяти этого ПК.

«Вот почему ретроспективный анализ памяти критически важен для исследования вредоносного ПО и его функций. Фактически обнаружение такой атаки возможно только в памяти, сети и системном реестре Windows», - говорит один из участников группы исследователей Kaspersky Labs, который изучал действия вредоноса[5]. Очевидно, что работа в памяти означает, что вредоносная программа Duqu2 не переживет перезагрузки ПК – это один из недостатков многих бесфайловых продуктов.

Вредоносная программа *Poison Ivy*, также обнаруженная в начале 2017 года, является еще одним примером бесфайлового вредоносного ПО, она использовалась для заражения конкретной цели, в данном случае компьютеров, принадлежащих чиновникам монгольского правительства. Она имеет форму вредоносного макроса Microsoft Word. Если целевой ПК разрешает макросы – что является типичным параметром настройки для большинства пользователей, – то программа запускается и создает соединение удаленного доступа для регистрации нажатия клавиш и записи экранов и видео с этого ПК. Все эти действия выполняются из располагающихся в памяти программ, которые пользуются возможностями определенных последовательностей команд PowerShell. На рис. 1 показаны различные модули этого вредоноса (с разрешения FireEye).

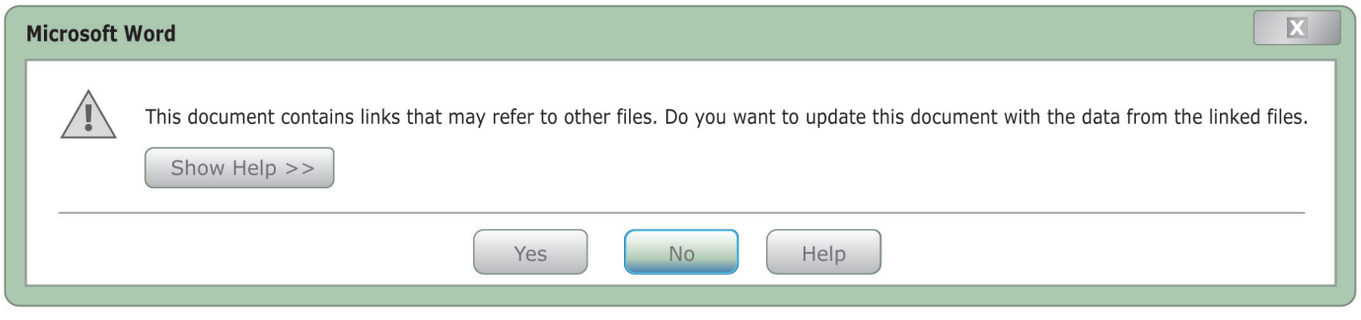
Poison Ivy также пытается избежать обнаружения системой защиты Microsoft *AppLocker*, вставляя ссылку на себя в список имеющих аккредитацию приложений AppLocker с помощью ряда программ и скриптов Windows. Кроме того, эта программа изготавливает копию отвлекающих документов для того, чтобы создать видимость безвредности своих действий для зараженного пользователя. Как видите, она отличается большой сложностью, а также включает несколько этапов и методов для проникновения в ПК пользователя. Этот вредонос также использовался в некоторых других случаях помимо монгольских организаций[6].

Другие случаи целевого использования бесфайловых вредоносных программ, например, атака с помощью *OilRig*[7], приписывалась злоумышленникам, спонсируемым иранским правительством. Эта атака была нацелена на 250 аккаунтов электронной почты, принадлежащих различным гражданам Израиля, включая, что весьма иронично, исследователей проблем кибербезопасности из Университета имени Бен-Гуриона. Хотя в апреле 2017 года компания Microsoft выпустила патч, который предотвращает распространение этой вредоносной программы, однако многие организации до сих пор его не установили. По иронии судьбы (опять) авторы этого вредоноса использовали данные из опубликованного концептуального исследования для разработки своих инструментов.

Эта конкретная вредоносная программа использовала зараженный документ Word, который отправлялся в качестве вложения в письмо и использовался для кражи информации с целевого ПК. Она использовала специализированную бесфайловую версию трояна Helminth Trojan. Более ранние версии OilRig использовали зараженные макросы, однако в ходе данной атаки была задействована вложенная веб-ссылка, использующая исполняемый файл **.HTA**. Такой тип файла автоматически исполняется входящей в состав ОС Windows программой **MSHTA.EXE** (для HTML-приложений Microsoft). Обычно при исполнении этой программой файла .HTA отображается предупреждающее сообщение (см. рис 2).

Однако данный вредонос ожидает такую ситуацию и автоматически отправляет команду «Ввод». В результате окно с предупреждением быстро убирается и вредоносная программа продолжает свою работу. Другие подобные целевые атаки включают атаку, направленную на компьюте-

Рис. 2. Это предупреждение о разрешении исполнения файла Windows на короткое время показывает пользователям, когда они щелкают зараженный файл.



ры американского ресторана с использованием вредоноса *Fin7*[8]. В прошлом эта вредоносная программа атаковала банки и государственные финансовые документы. Подобно другим бесфайловым вредоносам, эта программа скрывается внутри документа Microsoft Word, который вложен в фишинговое электронное письмо. Одной из новых особенностей атаки на рестораны с помощью Fin7 стало то, что вредоносный код полностью располагался и исполнялся в памяти без использования каких-либо команд PowerShell.

Еще один метод обфускации получил название *DoubleAgent*. Он использует незадокументированную функцию Microsoft Application Verifier. Этот верификатор представляет собой код, который присутствовал в ОС со времен как минимум Windows XP, и является утилитой Windows, которая позволяет разработчикам проверять исполнение своих приложений с целью нахождения и устранения проблем с безопасностью.

К сожалению, данный верификатор имеет в своём составе незадокументированную функцию, которую обнаружили исследователи из компании Cybellum. Эта функция позволяет злоумышленникам заменить законный верификатор на поддельный и получить полный контроль над приложением. Представитель Cybellum отметил: «DoubleAgent дает возможность злоумышленнику контролировать AV (Application Verifier) и выполнять все вышеперечисленные операции без риска обнаружения, сохраняя при этом иллюзию того, что AV работает нормально»[9].

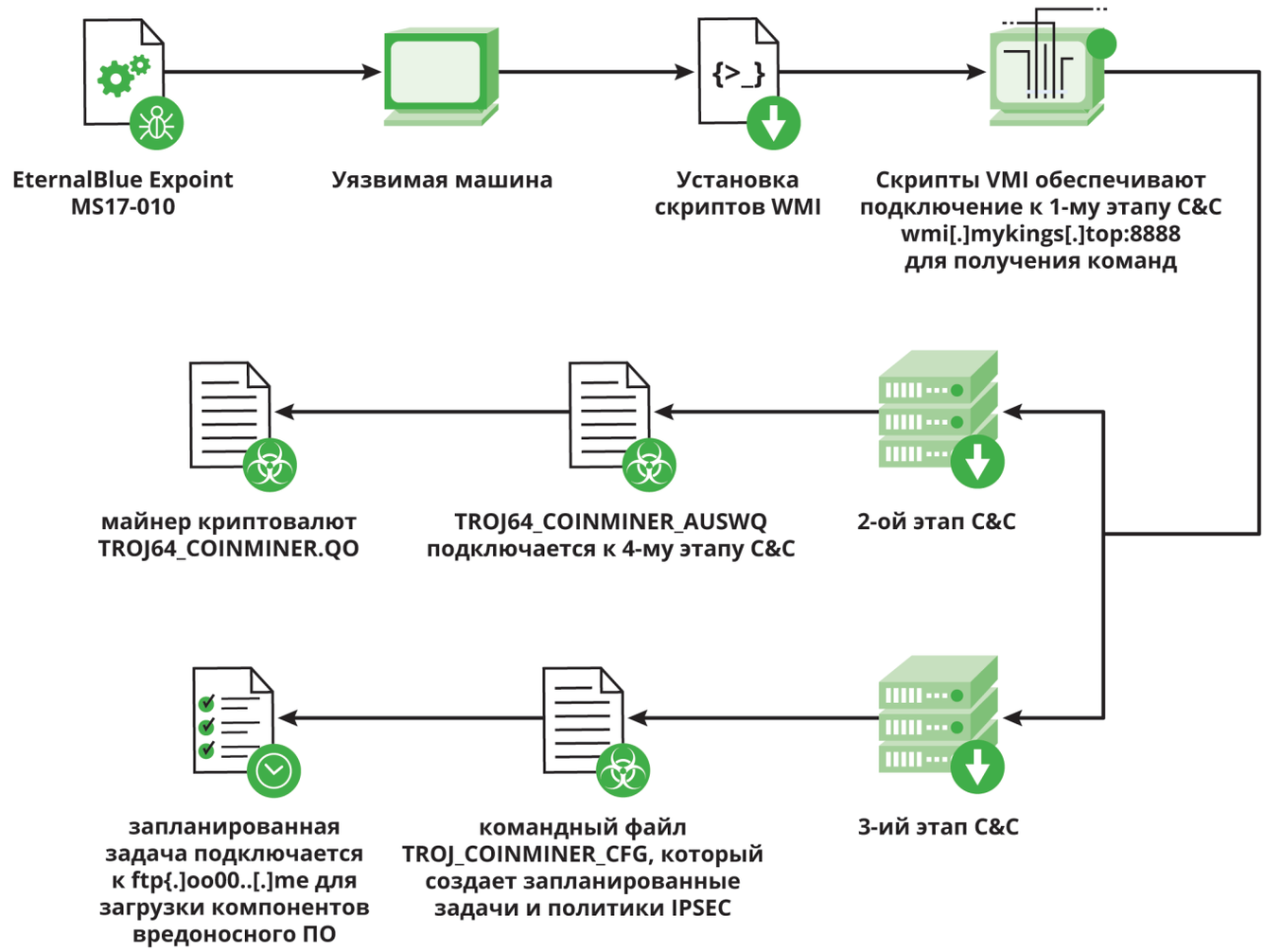
Поставщики решений безопасности недавно выпустили патчи для исправления этой уязвимости, однако данный пример демонстрирует, что создатели вредоносов все лучше находят подобные типы скрытых механизмов для того, чтобы избежать обнаружения и блокирования.

В июле 2017 года была обнаружена новая бесфайловая вредоносная программа, названная *CoinMiner*[10], которая главным образом распространяется в Японии и Индонезии. Целью этого вредоноса является создание скрытого приложения по майнингу биткоинов, генерирующего криптовалюту для злоумышленника. Он использует WMI для продления своего существования после перезагрузки компьютера и исполняет набор скриптов. CoinMiner атакует ПК через эксплойт *EternalBlue*[11], что совпадает с методом, использовавшимся червем *WannaCry*. На рис. 3 приведена схема его логического потока (с разрешения Trend Micro):

Общие методы по предотвращению опасности

Принимая во внимание масштабы этих эксплойтов, ниже мы перечислили несколько вариантов по предотвращению заражения в рамках вашей сети:

Рис. 3. Логический поток CoinMiner.



- Необходимо устанавливать патчи быстро и на все системы. Компания Microsoft выпускает регулярные патчи для Windows, а разработчики других операционных систем делают это для своих ОС. Не откладывайте обновление, поскольку некоторые злоумышленники используют это для того, чтобы заразить непропатченные системы своим вредоносным ПО. Хорошим примером является эксплойт EternalBlue: патч, предотвращающий эту атаку, был доступен больше месяца, прежде чем данный эксплойт стали использовать злоумышленники.

- Тщательно сегментируйте свою сеть, убедитесь в том, что вы понимаете права доступа, особенно те, которые предоставляются третьим лицам.

- Ограничьте права администратора до минимального количества систем. Многие эксплойты на базе WMI полагаются на обильное использование прав администратора, которые не являются необходимыми.

- Отключите не требующиеся вам программы Windows, например, WMI, PowerShell, а также поддержку старых протоколов, таких как *Server Message Block* (SMB) v1.

- Создайте список аккредитованных приложений с тем, чтобы еще больше ограничить набор программ, разрешенных к исполнению в большинстве конечных точек.

Заключение

Как видите, «плохие парни» усовершенствовались в своём ремесле и благодаря использованию бесфайловых методов они делают обнаружение вредоносного ПО и защиту от него все более трудным делом. К счастью, изучив некоторые из этих примеров из прошлого, вы можете соответствующим образом настроить свою защиту и более эффективно предотвращать заражения.

Об авторе

Дэвид Стром ранее являлся одним из авторов журнала *The Internet Protocol Journal*, публикуя статьи на тему электронной почты; он ведет информационный бюллетень по безопасности для *Inside.com*. Он был одним из основателей и ответственных редакторов журнала *Network Computing* (USA), а также является соавтором вышедшей в 1998 году книги *The Internet Message: Closing the Book with Electronic Mail* (совместно с Marshall T. Rose).

Ссылки

1. Ericka Chickowski, "Fileless Malware Takes 2016 By Storm", DarkReading, December 2016. http://www.darkreading.com/vulnerabilities---threats/fileless-malware-takes-2016-by-storm/d/d-id/1327796

2. "Target Hackers Broke in Via HVAC Company", Krebs on Security blog, February 2014. https://krebsonsecurity.com/2014/02/target-hackersbroke-in-via-hvac-company/

3. "DNC Hack Exhibits One of 3 Attack Trends To Watch for in 2017", Crowdstrike blog, January 2017. https://www.crowdstrike.com/blog/dnc-hack-exhibitsone-of-3-attack-trends-to-watch-for-in-2017/

4. "August in November: New Information Stealer Hits the Scene", Proofpoint, December 2016. https://www.proofpoint.com/us/threat-insight/post/august-in-december-new-information-stealer-hits-thescene

5. "Fileless attacks against enterprise networks", Securelist, February 2017. https://securelist.com/fileless-attacks-againstenterprise-networks/77403/

6. "Poison Ivy: Assessing Damage and Extracting Intelligence", FireEye Special Report, 2014. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

7. Michael Gorelik, "Iranian Fileless Attack Infiltrates Israeli Organizations", Morphisec Cyber Security Blog, April 2017. http://blog.morphisec.com/iranian-filelesscyberattack-on-israel-word-vulnerability

8. Michael Gorelik, "FIN7 Takes Another Bite at the Restaurant Industry", Morphisec Cyber Security Blog, June 2017. http://blog.morphisec.com/fin7-attacks-restaurantindustry

9. Michael Engstler, "DoubleAgent: Zero-Day Code Injection and Persistence Technique", Cybellum blog, March 2017. https://cybellum.com/doubleagentzero-day-codeinjection-and-persistence-technique/

10. Buddy Tancio, "Cryptocurrency Miner Uses WMI and EternalBlue To Spread Filelessly," TrendLabs Security Intelligence Blog, August 2017. http://blog.trendmicro.com/trendlabs-securityintelligence/cryptocurrency-miner-uses-wmieternalblue-spread-filelessly/

11. "EternalBlue," Wikipedia article, https://en.wikipedia.org/wiki/EternalBlue

Источник: The Internet Protocol Journal, Volume 21, Number 2, http://ipj.dreamhosters.com/wp-content/uploads/2018/08/ipj212.pdf

20 лет CENTR

Павел Храмцов

В 2019 году исполняется 20 лет Ассоциации европейских национальных регистратур доменов верхнего уровня – CENTR. К этой дате CENTR выпустила несколько любопытных аналитических материалов. Один из них называется «От измерения рынка к его пониманию»[1]. Автором является Патрик Майлз (Patrick Myles).

Майлз исследует развитие европейских доменных имен от конца 1990-х и до наших дней. Отмечается, что многие из этих доменов в начале своего существования были абсолютно бесплатными, раздавались по несколько штук «в одни руки» и предназначались в основном учебным заведениям и исследовательским институтам.

С самого начала управляли этим ресурсом некоммерческие организации, т.к. в то время никто еще не мог предполагать огромный коммерческий потенциал рынка доменных имен.

До сих пор традиционно в Европе 84% всех администраторов ccTLD (Country Code Top Level Domain) – это некоммерческие организации.

В настоящее время, отмечает Майлз, несмотря на свою важность в качестве человеко-машинного интерфейса, «видимость» доменных имен для широкой публики падает. Видимо, эпоха десктопов и World Wide Web потихоньку сходит на нет и социальные сети и мобильные приложения постепенно захватывают все больше и больше «места под солнцем».

Темпы роста количества доменных имен в европейских реестрах доменных имен за последние пару лет являются самыми низкими за все время их существования.

В этой связи Майлз считает главной задачей национальных регистратур внедрение технологий, упрощающих создание сайтов. Речь идет о конструкторах сайтов нового поколения, которые давали бы точно такой же функционал размещения контента и социализацию групп пользователей, что и инструменты социальных сетей.

Довольно сомнительная с точки зрения успеха перспектива. Платформы социальных сетей специально разрабатывались в качестве контент-хаба и средства коммуникации. Конкурировать на этом поле – это заведомо проиграть.

И еще одно интересное наблюдение Майлза. В его обзоре есть любопытная картинка роста количества регистраций gTLD за период с 2011 по 2019 год (рис. 1).

Что в ней любопытно, так это то, что программа new gTLD хоть и привела к кратковременному ажиотажу на рынке доменных имен, но не повлияла существенным образом на долгосрочную тенденцию – прирост количества доменов замедляется.

Тем не менее, отчаиваться не следует. Сила доменного имени в том, что оно заложено в спецификацию URI (Uniform Resource Identifier[2]), которая используется во многих протоколах и стандартах Сети. Доменные имена, читаемые человеком, нужны не только для получения IP-адресов, но и для удостоверения прав управления информационными ресурсами или в URL информационных страниц, на которые ссылаются поисковые машины. Умрут доменные имена, могут умереть и поисковые машины.

К слову сказать, всплеск регистраций в new gTLD был во многом обусловлен не технологическими новациями, а вопросами защиты прав интеллектуальной собственности, а точнее, средств индивидуализации, которыми являются доменные имена. Прирост регистраций дали владельцы товарных знаков.

World Wide Web Consortium (W3C) и DID

Не только CENTR отмечает в этом году юбилей. В 1989 году Тим Бернерс Ли изобрел World Wide Web. Роль веба в популяризации Интернета трудно переоценить. Паутина дала толчок развитию и популяризации массе интернет-технологий. Уже отмечалось, что именно Паутина дала толчок развитию доменной индустрии. Именно высокие доходы Network Solutions от домена .com не давали «спокойно спать» «доменным инвесторам» и привели к образованию в 1998 году ICANN[3].

И вот в 2019 году W3C объявляет о новой инициативе - Decentralized Identifier (DID)[4]. При этом разъясняется, что современные URL, базирующиеся на спецификации URI, требуют централизованного удостоверения регистратором (отсылка к системе доменных имен). Но это «нестильно, немодно и немолодежно».

Сегодня технологии Blockchain и Decentralized Ledger Technologies позволяю строить новые децентрализованные URI. Для унификации обращения к объектам этих глобальных децентрализованных баз данных предлагается применять спецификацию DID. В общем виде запись идентификатора выглядит следующим образом (рис. 2):

DID-метод в этой схеме определяет способ обращения к конкретному blockchain. Глобальная база данных DID предполагается как БД вида «ключ:значение», где «ключ» – это DID, а «значение» - это DID-документ.

Из сказанного выше непонятно, как идентификатор может быть привязан к физической сети, где располагаются

Рис. 1. Рост количества регистраций в gTLD.

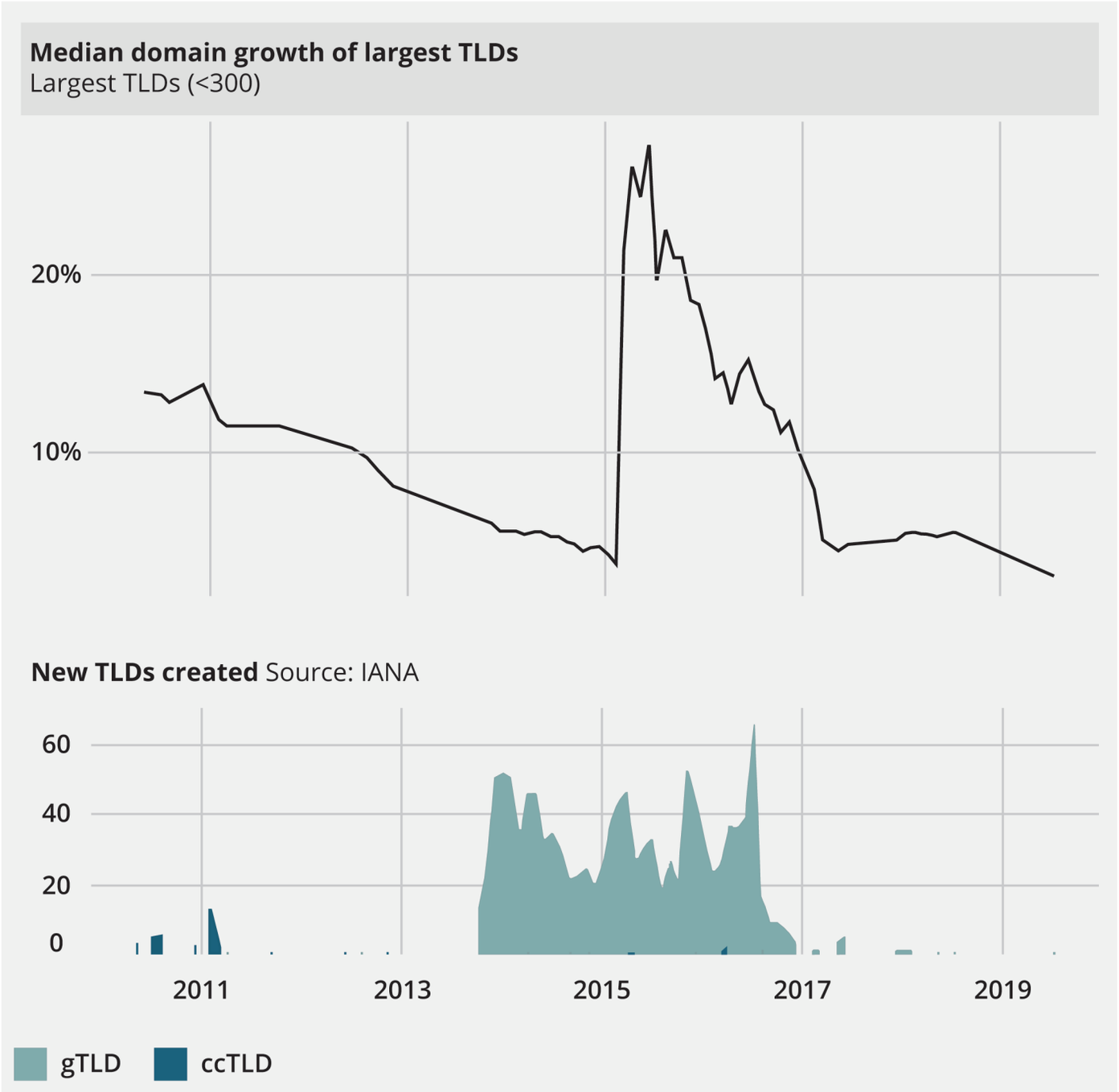


Рис. 2. Общая схема записи DID.

собственно сами информационные ресурсы. Так вот, эта привязка осуществляется через DID-документ, через спецификацию так называемого набора service endpoints.

Пока разработка этого «убийцы традиционного URL» еще в самом начале пути – создана только соответствующая рабочая группа (в сентябре 2019), но как говориться, «лиха беда начало».

Конечно, W3C не одиноки в своем порыве использовать новые технологии. Так, компания Alibaba решила скрестить доменные имена с blockchain и запатентовать результат такого скрещивания[5]. Впрочем, тексты патентов, видимо, должны читать специально обученные люди, т.к. из приведенного текста и иллюстраций можно сделать какие угодно выводы. То ли речь идет об имени блока, то ли об удостоверении доменного имени в блоке.

Солидарна с «Алибабой» и IBM, которая предлагает на основе своего патента разработать веб-браузер[6], который позволит не только хранить всю пользовательскую информацию в облачной БД на основе блоков, но и обеспечит безопасность финансовых транзакций пользователя.

DoH и все-все-все

Но не только кардинально новые технологии угрожают системе DNS и бизнесам вокруг нее. Не утихают дискуссии вокруг DoH (DNS over HTTP). Более подробно о технологии DoH и централизованной модели ее внедрения читайте в статье «DoH, или DNS, похожий на веб» в этом номере.

На 105 встрече IETF в Монреале Mozilla и Google представили планы по внедрению спецификации DoH в свои продукты. Концепции этих продуктов близки, но имеют существенные различия.

Mozilla по умолчанию включает поддержку DoH. Если пользователь или провайдер не согласны с такой постановкой вопроса, то они должны в явном виде просигнализировать об этом браузеру.

В общем, это все выглядит, как продолжение политики «принуждения силой», начатой DNS flag day 2019. Оправдание, которое приводит Mozilla – DNS пытаются использовать в атаках в качестве канала управления, и противодействовать этому можно, только перекрыв этот канал.

Призывы отдать управление резолвингом конечному пользователю парируются утверждением о том, что конечный пользователь не заботится о безопасности и, следовательно, ему нужно «помочь», исключив его самого из процесса принятия решения.

Google менее радикален в своих планах внедрения DoH. В корпорации предполагают длительный период тестирования и полноценный запуск технологии только после того, как она будет обкатана на готовых к тестам ISP. При этом Google печется и об интересах правоохранителей.

К слову, ISP не против DoH как такового. Они за то, чтобы их DoH-резолверы обслуживали конечного клиента.

И «вишенка на торте» – а нет ли других технологий для резолвинга имен, например, в рамках самого веб-приложения, без привлечения «транслятора» DNS?

Источник: «From measuring the market to understanding it», Patrick Myles, https://www.centr.org/library/library/educational-promotional-material/20th-anniversary-paper-from-measuring-the-market-to-understanding-it.html

Выводы

В общем, это все выглядит, как продолжение политики «принуждения силой», начатой DNS flag day 2019. Оправдание, которое приводит Mozilla – DNS пытаются использовать в атаках в качестве канала управления, и противодействовать этому можно, только перекрыв этот канал.Призывы отдать управление резолвингом конечному пользователю парируются утверждением о том, что конечный пользователь не заботится о безопасности и, следовательно, ему нужно «помочь», исключив его самого из процесса принятия решения.Google менее радикален в своих планах внедрения DoH. В корпорации предполагают длительный период тестирования и полноценный запуск технологии только после того, как она будет обкатана на готовых к тестам ISP. При этом Google печется и об интересах правоохранителей.

Ссылки

1. «From measurement the market to understanding it», https://www.centr.org/library/library/educational-promotional-material/20th-anniversary-paper-from-measuring-the-market-to-understanding-it.html

2. https://tools.ietf.org/html/rfc3986

3. https://www.icann.org/

4. https://www.w3.org/2019/09/did-wg-charter.html

5. https://domainnamewire.com/wp-content/alibaba-blockchain-domain-patent.pdf

6. http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=10&f=G&l=50&co1=AND&d=PTXT&s1=browser&s2=blockchain&OS=browser+AND+blockchain&RS=browser+AND+blockchain

Новости доменной индустрии

Важные события 2019

TLDCON - 2019

11-12 сентября 2019 года в столице Литвы Вильнюсе состоялась 12-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы TLDCON 2019. Конференция собрала 120 участников из 20 стран мира. Конференция организована Координационным центром доменов .RU/.РФ при поддержке DOMREG.LT (принимающая сторона), «Технического центра Интернет» (генеральный партнер), ICANN и Конгресс-бюро Вильнюса.

Интересные статистические данные привел в своем выступлении генеральный директор ТЦИ Алексей Рогдев. Он отметил, что эксперты, которые в 2017 году прогнозировали падение количества доменов в зоне .ru не менее 20%, оказались неправы. Реальное падение составило всего около 6%. При этом количество регистраций новых доменов не снижается, а число удаляемых доменов, напротив, уменьшается с каждым месяцем. Доля продлеваемых доменов растет с осени 2016 года вместе с их возрастом. «Доля «мертвых» доменов, не использующих почту или сайт, а также «припаркованных» доменов падает. Все это говорит о высокой «чистоте» доменной зоны и востребованности зарегистрированных доменов», – резюмировал Алексей Рогдев.

Рабочую программу TLDCON 2019 открыла секция «Безопасность: как регистратуры взаимодействуют с правоохранителями», участники которой поделились своим опытом работы с органами защиты правопорядка. Вел секцию **Михаил Анисимов** (Координационный центр доменов .RU/.РФ). Оказалось, что несмотря на разницу в законодательстве и подходах, у регистратур всех стран есть общая проблема – подавляющее большинство представителей правоохранительных органов не представляет себе, как работает Интернет. Об этом говорили **Джон Крейн** (ICANN) и **Ричард Лининг** (RIPE NCC), который заметил, что «расследование киберпреступления всегда начинается с объяснения того, как работает Интернет и почему им управляют все и никто». Также в секции участвовали **Бенедикт Аддис** (Shadowserver), **Хильда Тунем** (UNINETT Norid AS), **Ольга Баскакова** (Координационный центр доменов .RU/.РФ) и **Кирилл Мордань** (ОАЦ при президенте Республики Беларусь).

На секции «Правовые проблемы регистрации доменов» участники из разных стран рассказали о том, как формируются отношения между представителями доменной индустрии и правообладателями и какие факторы влияют на этот процесс. **Мзия Гогилашвили** (Национальная комиссия по коммуникациям Грузии) и **Катерина Олейник** (Arzinger) рассказали о подходах национальных регистратур Грузии и Украины к этому вопросу и поделились опытом построения этих взаимоотношений в своих странах. На секции выступила и представитель правообладателей – **Екатерина Калиничева** (юридическая компания Semenov&Pevzner). Она уже во второй раз стала спикером TLDCON и, как и в прошлом году, горячо защищала правообладателей и их права на доменные имена. Оппонентом Екатерины Калиничевой вновь стал модератор секции **Сергей Копылов** (Координационный центр доменов .RU/.РФ), а в качестве третейского судьи выступил представитель ВОИС **Гонсало Мануэль Бледа**.

Новые технологии и процессы, влияющие на применение доменов в интернет-индустрии, стали основными темами секции «Есть ли будущее у доменных имен?», которую вела генеральный директор MSK-IX **Елена Воронина**. Ведущие эксперты доменного рынка напомнили путь, который прошла система доменных имен, а также представили свое видение будущего доменов и веб-приложений. **Дмитрий Белявский** (ТЦИ) рассказал о разработанном по инициативе Координационного центра доменов .RU/.РФ патче к OpenSSL, который реализует поддержку международных email-адресов (EAI) в сертификатах электронной подписи. Эта разработка помогает сделать IDN-домены «равноправными игроками» на доменном рынке и тем самым способствует развитию системы доменных имен в направлении Universal Acceptance.

Следующая конференция – TLDCON 2020 – пройдет в сентябре 2020 года в Таллине. Присоединяйтесь!

УЧАСТВОВАТЬ В УПРАВЛЕНИИ ИНТЕРНЕТОМ МОЖЕТ КАЖДЫЙ

16-19 июля 2019 года во Владивостоке в Дальневосточном федеральном университете прошел Азиатско-Тихоокеанский форум по управлению интернетом APrIGF 2019. Форум собрал почти 300 участников из 50 стран мира, в течение трех дней на заседаниях, секция и круглых столах выступили более 100 докладчиков. Координационный центр доменов .RU/.РФ стал принимающей стороной этого международного форума.

Открывая форум, директор Координационного центра доменов .RU/.РФ **Андрей Воробьев** отметил, что 2019 год стал юбилейным и для APrIGF, который отмечает свое 10-летие, и для Российского форума по управлению Интернетом, который в этом году был проведен тоже в 10-й раз, и для национального российского домена .ru, которому в 2019 году исполнилось 25 лет.

На секции, посвященной вопросам Universal Acceptance («всеобщее признание», UA), обсуждались вопросы использования Интернета на разных языках. Концепция Universal Acceptance гарантирует, что конечные пользователи смогут успешно использовать Интернет на своих языках, и обеспечивает подключение к сети различных групп населения, чтобы пользователи могли использовать потенциальные возможности Интернета для личных, деловых, общественных или семейных целей. Российский опыт по управлению и развитию национального кириллического домена .рф востребован сегодня многими регистратурами.

Одной из центральных тем второго дня APrIGF 2019 стала сессия «Локализация Интернета: две стороны одной медали». Эксперты из стран АТР обсудили вопросы распределения трафика, а также влияние «границ» в Интернете на управление и связность Сети. Главными проблемами участники назвали попытки локализации трафика на национальном уровне, распространение «тяжелого» контента через CDN, что меняет и экономику распространения контента, когда в проигрыше остаются транзитные операторы, а также растущий интерес к управлению международными потоками данных и контролю над ними на национальном уровне.

Важным событием третьего, заключительного дня работы Азиатско-Тихоокеанского форума по управлению Интернетом APrIGF 2019 стало заседание, посвященное 25-летию национального российского домена верхнего уровня .ru и 10-летию Российского форума по управлению Интернетом (RIGF). Представители международных организаций ICANN, ISOC, APTLD совместно с Координационным центром доменов .RU/.РФ и участниками APrIGF 2019 из разных стран обсудили, может ли опыт российского IGF, накопленный за эти десять лет, быть реализован другими странами и поднят на региональный и даже глобальный уровень.

Азиатско-Тихоокеанский форум по управлению Интернетом организован совместно регистратурой домена .asia и Координационным центром доменов .RU/.РФ при поддержке международной корпорации ICANN и Ассоциации регистратур национальных доменов стран Азиатско-Тихоокеанского региона APTLD. Также поддержку форуму оказали «Сообщество Интернета» (ISOC), APNIC и секретариат Глобального форума по управлению интернетом про Организации Объединенных Наций.

ВЗАИМОДЕЙСТВИЕ НАЦИОНАЛЬНЫХ РЕГИСТРАТУР РОССИИ И ВЬЕТНАМА БУДЕТ ПРОДОЛЖЕНО

24 августа во время рабочего визита делегации Координационного центра доменов .RU/.РФ во Вьетнам состоялось торжественное подписание Меморандума о взаимопонимании между регистратурами национальных российских доменов .ru и .рф и национального домена Республики Вьетнам .vn. Документ подписали директор Координационного центра доменов .RU/.РФ Андрей Воробьев и директор VNNIC Тран Мин Тан (Tran Minh Tan).

Меморандум предусматривает обмен опытом в области развития доменов на национальных языках, статистики, развития инфраструктуры и информационной безопасности, а также совместную работу над международными проектами в рамках членства в отраслевых организациях (ICANN, APTLD и других).

«Подписание меморандума открывает перед нами широкие возможности для сотрудничества как напрямую, так и при совместной работе внутри различных международных групп и организаций. Для регистратур национальных доменов сегодня очень важно вырабатывать общие подходы и общую политику в области развития национальных доменных пространств, и мы очень рады вести эти работу совместно с регистратурой национального домена Вьетнама .vn. Тему сотрудничества национальных регистратур Координационный центр поднимает регулярно – например, буквально через две недели в столице Литвы Вильнюсе пройдет 12-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы, где также будет обсуждаться взаимодействие регистратур разных стран», – сказал директор Координационного центра доменов .RU/.РФ **Андрей Воробьев**.

Календарь событий: 2019 год

Международные события

14-18 октября
RIPE79,
Роттердам, Нидерланды

Встречи RIPE проводятся два раза в год и собирают более 700 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Встреча длится пять дней и начинается с двухдневной пленарной программы, за которой следуют несколько параллельных сессий заседаний рабочих групп. Прием докладов закончен, но у вас есть возможность предложить «блиц-доклад».
https://ripe79.ripe.net/

20-22 октября
Euro-IX Forum 35,
Заандам, Нидерланды

Euro-IX является ассоциацией точек обмена трафиком (IXP), координирующей различную коллективную деятельность между участниками и предоставляющей информационные услуги, такие как база данных IXP по всему миру. Два раза в год Euro-IX организует встречу участников и всех, кому интересны вопросы обмена трафиком, создания и обслуживания IXP. Это прекрасная возможность обменяться опытом, расширить свою профессиональную сеть и установить новые деловые отношения.
https://www.euro-ix.net/en/events/fora/35th-euro-ix-forum/

28-30 октября
NANOG 77,
Остин (Техас), США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG на технологиях и системах, обеспечивающих работу Интернета. Поскольку инженерные вопросы NANOG имеют глобальный характер, участие в списке рассылки и конференциях может быть полезно широкому кругу технических специалистов в области сетевых технологий Интернета. Прием докладов закончен, но у вас есть возможность предложить «блиц-доклад». https://www.nanog.org/meetings/nanog-77/

31 октября - 1 ноября
DNS-OARC 31,
Остин (Техас), США

DNS-OARC - некоммерческая организация, целью которой является улучшение безопасности и стабильности инфраструктуры DNS, а также исследование работы этой глобальной системы. Семинары DNS-OARC открыты для членов OARC и для всех других участников, заинтересованных в работе и исследованиях DNS. В этот раз семинар пройдет параллельно со встречей ARIN - североамериканской интернет-регистратуры. https://indico.dns-oarc.net/event/32/

2-7 ноября
ICANN 66,
Монреаль, Канада

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. Участие во встречах ICANN бесплатно.
https://meetings.icann.org/en/montreal66

16-22 ноября
IETF 106,
Сингапур

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания. Это хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке. В выходные перед началом совещаний пройдет IETF Hackathon, посвященный практическому воплощению стандартов IETF, и IETF Codesprint по доработке приложения datatracker - важного инструментария IETF. https://www.ietf.org/how/meetings/106/

25-29 ноября
IGF,
Берлин, Германия

IGF является глобальной платформой со множеством заинтересованных сторон, которая облегчает обсуждение вопросов государственной политики, касающихся Интернета. Этот форум был создан по решению Генерального секретаря ООН в 2006 году и с тех пор проводится ежегодно. В дискуссиях принимают представители частного сектора, правительств, гражданского общества и технического сообщества. Участники обсуждают технические, организационные и правовые вопросы использования и развития Интернета.
https://www.intgovforum.org/multilingual/ru/content/igf-2019

В России

12-13 ноября
Санкт-Петербург,
A2 Green Concert

ZeroNights 2019
Уже несколько лет подряд ZeroNights собирает более двух тысяч экспертов, специалистов-практиков по ИБ, администраторов, пентестеров, аналитиков и хакеров со всего мира. На конференции будут представлены доклады ведущих российских и зарубежных экспертов в области ИБ. Посетители узнают об актуальных проблемах, новых атаках и реальных угрозах, а также познакомятся с нестандартными методами решения задач информационной безопасности. https://zeronights.ru/

20 ноября
Санкт-Петербург,
Holiday Inn
«Московские ворота»

BIS-2019
Международный форум «Современная инженерная инфраструктура. Вокруг автоматизации. Вокруг ЦОД» (или BIS-2019) соберет лучших представителей ИКТ-сообщества и бизнес-среды региона. В тематику форума входят следующие направления: ЦОД и технологии для их построения, работы и обслуживания; инфраструктурные и инженерные элементы дата-центров и серверных; автоматизация производства и бизнес-систем, Индустрия 4.0; структурированные кабельные системы, IT-инфраструктура зданий, умный дом; вопросы импортозамещения в IT и взаимодействия с госструктурами.
https://sankt-peterburg-bis-2019.ciseventsgroup.com/

В Москве

14 ноября
Holiday Inn
Suschevsky

II Всероссийский бизнес-форум «Развитие сетей беспроводной связи в России – 5G Future Russia 2019»
В конференции примут участие представители государственных регулирующих органов, операторов связи, IoT-компаний, производителей информационно-телекоммуникационного оборудования и абонентских устройств, системные интеграторы и поставщики решений, разработчики и поставщики программного обеспечения, подразделений и служб связи, IT и ИБ из различных секторов экономики, консультанты и эксперты отрасли, отраслевые СМИ. Организатор - информационно-аналитическое агентство TelecomDaily в партнерстве с ПАО «Ростелеком», при поддержке и участии Международного консорциума 3GPP.
http://www.tmtconferences.ru/5g2019.html

19–20 ноября
Radisson Collection Hotel

SOC Forum 2019
V SOC Forum: Практика противодействия компьютерным атакам и построения центров мониторинга ИБ, организуется ФСБ и ФСТЭК при поддержке Центробанка России. Традиционно на SOC-Форуме происходит обмен опытом и мнениями ведущих экспертов отрасли, обсуждаются практика построения центров мониторинга и управления инцидентами ИБ, вопросы выполнения требований к организациям-субъектам критической информационной инфраструктуры, особенности функционирования центров ГосСОПКА и организации взаимодействия в сфере выявления и анализа компьютерных инцидентов, новинки технологической базы, сценарии использования и повышения эффективности центров мониторинга.
https://soc-forum.ib-bank.ru/

21 ноября
«Хилтон Гарден Инн
Москва Красносельская»

Broadband Russia Forum
IX Международный форум «Broadband Russia Forum: эволюция сетей широкополосного доступа в эпоху цифровой экономики, распределенных дата-центров и облачных услуг накануне запуска 5G» – крупнейшее событие рынка ШПД в России. Участники: операторы фиксированной, мобильной и спутниковой связи, представители органов государственной власти и международных отраслевых ассоциаций и бизнес-сообществ, производители телекоммуникационного оборудования, разработчики цифровых решений и сервисов, системные интеграторы, контент-провайдеры, консультанты и эксперты отрасли, журналисты деловых и отраслевых СМИ. http://www.comnews-conferences.ru/ru/conference/bb2019

5 декабря
Центр международной
торговли

XV ПИРИНГОВЫЙ ФОРУМ 2019
Форум проводится для клиентов, партнеров и друзей MSK-IX – для тех, чья работа связана с развитием сетей и сервисных платформ в Интернете. Вы сможете ощутить пульс рынка, узнать, как развиваются сетевые технологии, пообщаться с партнерами и коллегами. В 2019 году форум пройдет в 15-й раз и соберет 700+ участников. Главные темы программы: пиринг, новости развития MSK-IX и приглашенных IXP; лучшие практики проектирования, эксплуатации и автоматизации сетей; безопасность маршрутизации и обмена данными; блокировки и другие технические аспекты регулирования отрасли связи; доставка телесигналов и OTT-видео через Интернет; исследования и макроизмерения сетевой связности. Участие бесплатное, но необходимо зарегистрироваться на сайте и получить приглашение.
https://peering-forum.ru

MSK IX

10 ГОРОДОВ

500+ УЧАСТНИКОВ

42 ПЛОЩАДКИ

21 УЗЛЕЛ DNS-СЕТИ

ПОДКЛЮЧЕНИЯ ДО **100G**

ТРАФИК **3,3Тбит/с**

MSK-IX ускоряет коммуникации между интернет-компаниями, предоставляя нейтральную платформу Internet eXchange для обмена IP-трафиком между сетями и глобальную распределенную сеть DNS-серверов для поддержки корневых доменных зон.

Более 500 организаций используют сервисы MSK-IX для развития сетевого присутствия в 10 городах. К MSK-IX подключены операторы связи, социальные сети, поисковые системы, видеопорталы, провайдеры облачных сервисов, корпоративные и научно-образовательные сети.

127083, г. Москва, ул. 8 Марта, д. 1, стр. 12
тел.: +7 495 737-92-95
www.msk-ix.ru

+7 495 737-92-95

WWW.MSK-IX.RU

Интернет изнутри

2019