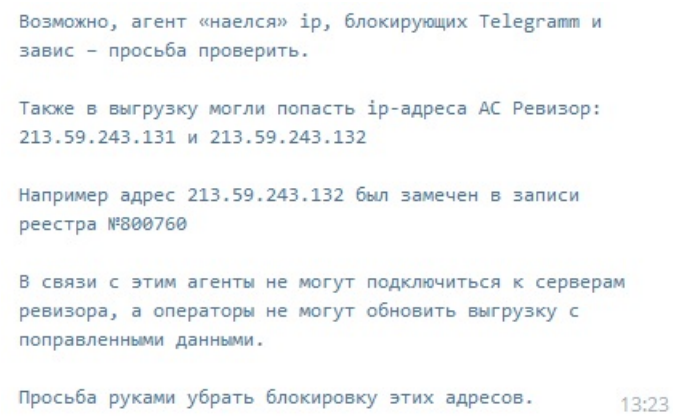
Telegram ни при чём: Роскомнадзор наступил на старые грабли

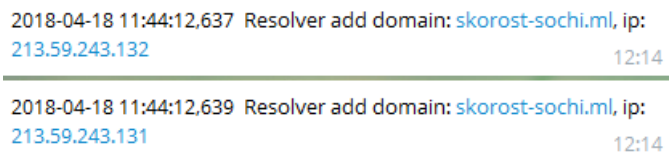
В минувшую среду, 18 апреля, Nag.ru со ссылкой на представителя одного из региональных интернет-провайдеров, сообщил о проблемах в работе Аппаратно-программного комплекса "Ревизор", а также о том, что IP-адреса сервера "Ревизор" попали под блокировку.

Как утверждал наш источник, утром 18 апреля некоторые интернет-провайдеры получили неофициальное сообщение от Роскомнадзора с настоятельной просьбой перезагрузить программно-аппаратный комплекс "Ревизор", который используется для мониторинга доступа к сайтам из реестра. Возможно, "Ревизор" завис из-за огромного количества IP-адресов, которые попали в реестр запрещенных. Также, в письме говорилось о том, что операторам необходимо проверить адреса, на которые отправляется статистика по заблокированным ресурсам. При проверке выяснилось, что оба адреса заблокированы.



Скрин сообщения Роскомнадзора

Наш источник, проштудировав выгрузку, нашел в ней запись реестра под № 800760, которая содержала домен skorost-sochi.ml. Под этим доменом и значились в списке два запрещенных IP-адреса серверов "Ревизора" (213.59.243.131 и 213.59.243.132). Посмотреть почасовую историю реестра за эти дни можно по ссылке.



Так выглядит запись в реестре

В Роскомнадзоре опровергают факт возникновения проблем с работой "Ревизора", а также попадания IP-адресов сервера в "черный список".

> "Сообщение о том, что IP сервера "Ревизора" был в id выгрузки – это ложь. "Ревизор" работал полноценно, а текст письма, приведенный на картинке, фейк. Агенты не "наедаются ip-адресами" и не зависают. В выгрузке не содержатся и не содержались ip-адреса 213.59.243.131 и 213.59.243.132. А запись реестра №800760 содержит домен skorost-sochi.ml , и не содержит (и не содержала) вышеупомянутых ip-адресов", – пояснил представитель ФГУП "РЧЦ ЦФО" Владислав Минаков.

Однако наш источник в корне не согласен с представителем Роскомнадзора и утверждает, что сообщение провайдеру поступило неофициально от местного представительства регулятора.

> "Представители нашего Роскомадзора обратились ко мне по неофициальным каналам, поэтому я никоим образом не могу подтвердить факт обращения. Но факт остается фактом. Судя по всему, из-за "косяка" в скриптах IP-адрес не удалился из блокируемых, а затем Ревизоры "отпали". Представители нашего регионального РКН написали мне о том, что они не работают, а также сообщили о том, что IP-адреса были в выгрузке. То есть, такие сообщения могли получить ограниченное число операторов. Поскольку, IP- адреса были в скором времени разблокированы", – поясняет источник.

Факт возникновения проблем в работе "Ревизоров" подтвердил и представитель другого интернет-провайдера.

> "19 апреля к нам обращались сотрудники РЧЦ с жалобами на работу ревизора в предыдущий день. Но это не было связано (и не связано сейчас) с указанными адресами,

ревизор просто глючит. Адреса не попадали в реестр напрямую, но резолвятся по записи 800760 для тех, кто резолвит.

Суть в том, что системы фильтрации бывают построены немного по-разному.

Интересное нам в этом случае деление: либо весь абонентский трафик проходит через фильтр, либо только его часть.

Для первого случая нам нужен большой и дорогой фильтр.

Во втором случае нам надо определить, какую часть абонентского трафика мы будем подавать в фильтрацию. Вот для тех, кто идет по второму пути, необходимо как-то предсказать, куда именно пойдет "Ревизор" (ну и абонент, но это не так важно). Поэтому для записей в реестре, указывающих на доменное имя или на страницу сайта, они делают резолвинг этого доменного имени через DNS. На какой IP укажет DNS – трафик на тот IP и будет "зарулен" в систему фильтрации.

И тут возникают наши злоумышленники, которые зарегистрировали свободный домен из реестра и прописали ему IP-адреса АС "Ревизор". У резолвящего оператора для этого домена выпадают адреса "головы" Ревизора, и служебный трафик Ревизора уходит в фильтры. Правда, он тоже не должен блокироваться - он просто должен пройти фильтр и выйти. Но там уже возникают разные моменты совместимости этого трафика с фильтрацией. Примерно, тоже самое происходило летом прошлого года, когда из-за злоумышленников IP-адреса многих известных интернет ресурсов попали в "черный список", – рассказал Валерий Лутошкин.

То есть, по словам наших источников, факт "зависания" Ревизоров все-таки имел место, просто это явление не имело массового характера, а было скорее локальным. Также и IP-адреса попали в "черный список" Роскомнадзора. Это явление не было связано с блокировкой мессенджера Telegram, а скорее стало эхом истории, произошедшей летом 2017 года, когда в механизме блокировок Роскомнадзора обнаружили уязвимость, благодаря которой можно внести в список запрещенных любой добропорядочный интернет-ресурс. Для этого владелец домена сайта, внесенного в "черный список", может разместить в собственных DNS-записях IP-адрес любого сайта, чем ограничит доступ к нему. Тогда это привело к массовым блокировкам интенет-ресурсов, среди которых оказался официальный портал администрации Президента РФ Kremlin.ru, и даже портал Nag.Ru

С тех пор механизм блокировок в Роскомнадзоре не изменили и продолжают "тоннами" блокировать IP-адреса, что мы видим на примере борьбы с Telegram. От этого "махания молотом" страдают все, кроме самого мессенджера.

Как сообщает Михаил Климарев в своем Telegram-канале "За Телеком", сегодня количество заблокированных IP-адресов достигло 19 миллионов.

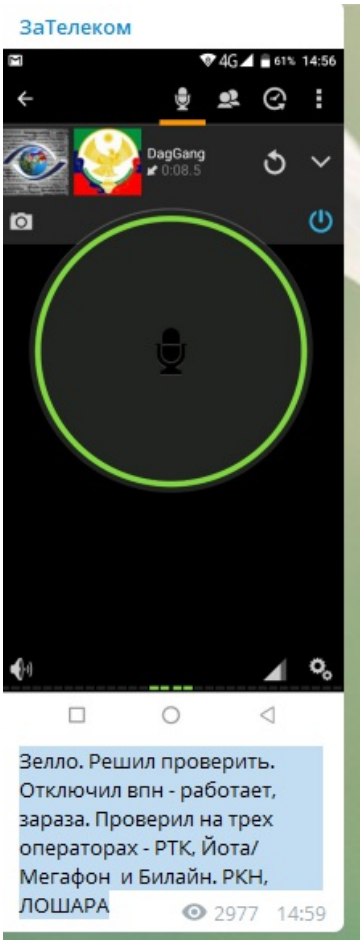
"*В связи с блокировкой мессенджера Telegram, Роскомнадзор закрыл доступ к уже почти 19 миллионам ip-адресов. Для того, чтобы были яснее масштабы происходящего, ниже мы собрали топ провайдеров, подсети которых попали под блокировку, упорядочив их по количеству доменов в зонах .ru, .su и .рф:*

1. *Hetzner – 201,4 тыс. доменов;*
2. *OVH – 94,9 тыс. доменов;*
3. *Google – 61,6 тыс. доменов;*
4. *Digital Ocean – 34,1 тыс. доменов;*
5. *Amazon – 28,6 тыс. доменов;*
6. *Microsoft – 5,4 тыс. доменов.*

Как видно из этого списка, сегодня в зоне риска находится 426 тысяч сайтов в трех зонах российских доменных имен. Если для своего проекта вы пользуетесь услугами этих провайдеров, но не испытываете проблем с доступностью, советуем не ждать и подключить проксирование заранее. Если вы уже столкнулись со сложностями, вам тем более стоит воспользоваться им", – говорится в сообщении.



Также по сведениям Михаила Климарева, вновь стала доступна интернет-рация Zello, которую ранее заблокировал "Роскомнадзор".



В качестве итога ко всему вышесказанному процитирую хорошо известного сообществу Nag.Ru, Алексея Павлюца:

"Почему все попытки РКН не сработают, а приведут только к отрицательным последствиям? Тут есть системные причины, по которым такие фокусы не пройдут не только у РКН, но и вообще у кого бы то ни было другого, и нигде в мире.

Хотел было написать на эту тему большую подробную статью, но лень. Обойдусь коротким (сравнительно) тезисным постом.

Оставляя за кадром тот факт, что квалификация нукеров Жарова невысока, а сам он вообще не представляет как что устроено, к этому есть серьезные системные причины.

Дело в том, что Интернет и ИТ сильно изменились, последние лет минимум десять вся индустрия работала над тем, чтобы привнести динамику туда, где раньше все было очень статично. Парадигма "вот есть днс, есть сервер, оно работает" действует только для небольших проектов. И да, они сравнительно статичны. Потому что изменения в них производят люди.

Все, что вырастает чуть больше размером - выходит на новый уровень, на котором масштабирование и управление изменениями автоматизировано в высокой степени. Серверы появляются и исчезают без участия человека в зависимости от нагрузки, положения звезд, распределения юзверей по географии и времени суток и так далее. Для такой системы фактор избирательного нарушения связности, частным случаем которого являются блокировки - просто еще один фактор, который надо включить в алгоритмику.

Мякотка тут в том, что скорость этих изменений на сегодня - далеко, на порядки превышает скорость обращения цикла "обнаружил-проанализировал-выкатил в бан-заблочено". Это раз.

Второе, скорость изменений ВСЕГДА будет выше скорости цикла подавления, чтобы там не изобретал РКН, и даже если они начнут напрямую вмешиваться в маршрутизацию через blackhole - это ничего не изменит. Ну, не допрыгнут через пропасть не два метра, а метр восемьдесят.

Все предыдущие успехи по блокированию - это не заслуга РКН, а недоработка блокируемых в том смысле, что они и не ставили себе цели остаться доступными. Типа - ну и хрен с вами, не рынок-то в РФ и был. Можно сказать, что Телега первая, кто НЕ согласился и не встал под блок добровольно. Исключая, конечно, кучу проектов разной степени криминальности, которые РКН рутинно блокирует, а они так же рутинно объявляются в новом месте с новым лицом.

Таким образом, на уровне технологий стабильная блокировка тупо невозможна, все это превращается в вечный бой, в котором можно только на непродолжительное время лишить сервиса какую-то небольшую часть клиентов. При этом большая часть ударов будет приходиться уже в пустоту и по тем, кому просто не повезло оказаться рядом.

Парадокс здесь в том, что все сказанное выше - это не злые козни, а объективная реальность бытия, обусловленная развитием технологий. И этот фарш взад не провернуть.

Я не знаю, хорошие ли это новости, потому что по факту они ставят "блокировщиков" перед нехитрым выбором: урезать свои аппетиты, унять амбиции и договариваться с крупными сервисами как равными, либо брать топор и рубить кабели по границе РФ.

Причем именно так, единственный файрвол, который точно будет работать - это воздушный зазор. Все остальное - проходимо, это вопрос ресурсов и квалификации.

И последнее. "Китайский вариант" - не сработает. Инкапсуляция Китая обусловлена не только усилиями правительства, но и культурной составляющей, их языковое и культурное пространство весьма замкнуто по своей природе. И да, все, кому действительно нужно - проходят за "золотой щит". Вариант "белых трансграничных списков" - это вообще трэш, он в принципе нерабочий. По сути, это почти то же самое, что топором по кабелю.

Вот, собственно, и все. Вопрос только в том, понимают ли это все те, кто принимает решения.

Боюсь, что не понимают. И вот это - по-настоящему плохая новость".

Напомним, что 16 апреля, Роскомнадзор начал процедуру блокировки Telegram. В результате под "топор" регулятора попало более 16 миллионов IP-адресов, связанных с Amazon и Google.

Подробнее об этой истории можно узнать в следующих материалах:

- Telegram. Суд. Блокировка
- В погоне за Telegram Роскомнадзор заблокировал более 2 миллионов IP-адресов, что не повлияло на работу мессенджера
- Блокировки Роскомнадзора вызвали пробки в аэропортах и проблемы в банковском секторе
- Блокировка Telegram может привести к уходу Amazon из России
- Роскомнадзор в погоне за Telegram заблокировал "Ревизор"