@ValdikSS
Пользователь

сегодня в 20:49

Июньская ситуация с недоступностью ресурсов из-за блокировок веб-сайтов

Регулирование IT-сектора

Все провайдеры интернета в России вынуждены блокировать ссылки, внесенные в Единый реестр запрещенных сайтов. Он представляет собой огромную свалку ссылок (в том числе не соответствующих стандартам), доменов и IP-адресов. Общей методики блокировок не существует, есть только абстрактные рекомендации от Роскомнадзора, поэтому каждый провайдер блокирует сайты по-своему, в меру понимания реестра, своей технической продвинутости и бюджета.

Подавляющее большинство провайдеров используют те или иные системы анализа трафика, чтобы блокировать конкретные URL, а не IP-адрес: аппаратные комплексы DPI, открытые DPI под Linux, прозрачные прокси-серверы. Этого вполне достаточно для блокировки ссылок в HTTP, но не все системы поддерживают анализ домена (параметра SNI) в HTTPS-трафике, из-за чего провайдерам с такими системами приходится блокировать HTTPS-ссылки реестра по IP-адресу.
Также в реестре есть сайты, внесенные по домену, без указания протокола. Некоторые провайдеры блокируют такие записи по IP-адресу, другие — только HTTP и HTTPS-протокол у этих доменов. Чтобы не создавать излишнюю нагрузку на сеть, провайдеры пропускали через DPI только известные IP-адреса заблокированных сайтов.

У каждой записи в реестре, будь то домен или ссылка, есть свой список IP-адресов. До конца января этого года провайдерам, блокирующим частично или полностью по IP-адресам, достаточно было фильтровать доступ только к IP-адресам из реестра. В конце января обновилось ПО «Ревизора» — системы, проверяющей, насколько качественно провайдер блокирует веб-сайты. Если раньше «Ревизор» пытался открыть сайт по одному IP-адресу из DNS, как любой обычный браузер или программа, то после обновления совершает запросы по всем IP-адресам и из DNS-ответа, и из реестра. Вместе с этим, провайдеров начали штрафовать за открывшиеся сайты, не было никаких поблажек и допустимого порога внезапно открывшихся сайтов.

Дабы не быть оштрафованными, провайдеры начали постоянно проверять, не появились ли на домене новые IP-адреса, и добавлять их в списки блокируемых и пропускаемых через DPI.

Веселье начинается…

Начиная с 29 мая, люди начали потихоньку скупать разделегированные домены из реестра, которые были добавлены в 2014-2016 годах, и устанавливать на них А-записи на IP-адреса популярных ресурсов. Провайдеры резолвили эти домены, добавляли IP-адреса в список блокируемых, доступ к ресурсам пропадал. Первые шутники добавили записи Вконтакте и Яндекса, из-за чего некоторые провайдеры заблокировали к ним доступ.
Роскомнадзор прислал следующее уведомление:

РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора по Центральному федеральному округу)

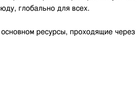
Старокоптельское шоссе, д. 2, корп.10, ГСП-7, Москва, 117997
Справочная: (495) 587-44-85 факс: (495) 249-24-16
E-mail: rsockanc77@rkn.gov.ru

Руководителю организации

01.06.2017 № 33817-09/77
На № от
О направлении информации

В соответствии с распоряжением заместителя руководителя Роскомнадзора О.А. Иванова от 01.06.2017 № 33817-09/77 **запрет блокировки** следующих сетевых адресов: 95.213.11.180, 87.240.165.82 и 5.255.255.88, отсутствующих в Перечне записей, содержащих информацию о доменных именах, указателях страниц сайтов в сети «Интернет» и сетевых адресах, позволяющих идентифицировать сайты в сети «Интернет» и (или) информационные ресурсы, содержащие информацию, доступ к которой должен быть ограничен операторами связи в порядке, установленным Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Выгрузка), предоставляемом операторам связи.

И.о.заместителя руководителя И. П. Рак



Затем последовала частичная неработоспособность Telegram и некоторых других сайтов.
При особом стечении обстоятельств, если IP-адрес ресурса добавили на домен, внесенный без URL, или на URL с HTTPS, и трафик до сайта приходил через провайдера, который реализует блокировки для транзитного трафика, сайт становился недоступен сразу отовсюду, глобально для всех.

От транзитных блокировок пострадали в основном ресурсы, проходящие через Ростелеком и ТТК:

- Корневые DNS
- ntv.ru
- nag.ru
- avito.ru
- 3ds.sdm.ru
- acs.bspb.ru

Nag и НТВ лежали длительное время, пол дня, или около того. О неработоспособности двух последних доменов, обеспечивающих 3-D Secure (СМС-подтверждение онлайн-транзакции по карте) банков Санкт-Петербург и СДМ, не заявляли ни СМИ, ни сами банки.

https://3ds.sdm.ru (ТИЦ 0; PR:).

Проверка выполнена 5 июня 2017 года в 6:51:21 по московскому времени.

Проверить другой сайт →
Экспорт результатов проверки в Excel

Точка мониторинга	IP вашего сервера	Общее время, сек.	DNS, сек.	Соединение, сек.	Ожидание ответа, сек.	Скорость загрузки	Размер страницы
Россия, Москва, восток 1	Невозможно соединиться с указанным адресом.						
Россия, Москва, северо-восток 2	Невозможно соединиться с указанным адресом.						
Россия, Москва, центр 1	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 193.189.121.8.						
Россия, Москва, центр 2	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 193.189.121.8.						
Россия, Апатиты	Невозможно соединиться с указанным адресом.						
Россия, Калининград	Операция прервана, т.к. сервис не ответил в течение 8 секунд. Обращение производилось к IP: 193.189.121.8.						
Россия, Красноярск	Невозможно соединиться с указанным адресом.						
Россия, Нижний Новгород	Невозможно соединиться с указанным адресом.						
Россия, Новосибирск, юго-восток	Невозможно соединиться с указанным адресом.						
Россия, Петрозаводск	Операция прервана, т.к. сервис не ответил в течение 8 секунд. Обращение производилось к IP: 193.189.121.8.						
Россия, Ростов-на-Дону	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 193.189.121.8.						
Россия, Санкт-Петербург, центр 1	Операция прервана, т.к. сервис не ответил в течение 8 секунд.						
Россия, Томск, восток	Невозможно соединиться с указанным адресом.						
Россия, Тюмень	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 193.189.121.8.						
Россия, Хабаровск	Невозможно соединиться с указанным адресом.						
Россия, Химки	Операция прервана, т.к. сервис не ответил в течение 8 секунд.						

https://acs.bspb.ru (ТИЦ 0; PR:).

Проверка выполнена 5 июня 2017 года в 7:12:25 по московскому времени.

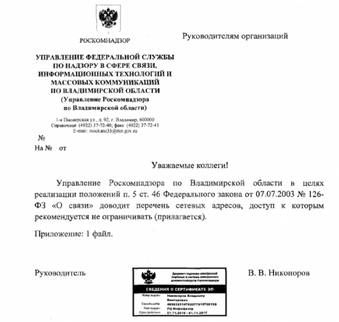
Проверить другой сайт →
Экспорт результатов проверки в Excel

Точка мониторинга	IP вашего сервера	Общее время, сек.	DNS, сек.	Соединение, сек.	Ожидание ответа, сек.	Скорость загрузки	Размер страницы
Россия, Москва, восток 1	Невозможно соединиться с указанным адресом.						
Россия, Москва, северо-восток 2	Невозможно соединиться с указанным адресом.						
Россия, Москва, центр 1	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 213.172.3.116.						
Россия, Москва, центр 2	Операция прервана, т.к. сервис не ответил в течение 8 секунд. Обращение производилось к IP: 213.172.3.116.						
Россия, Апатиты	Невозможно соединиться с указанным адресом.						
Россия, Калининград	Операция прервана, т.к. сервис не ответил в течение 8 секунд. Обращение производилось к IP: 213.172.3.116.						
Россия, Красноярск	Невозможно соединиться с указанным адресом.						
Россия, Нижний Новгород При поддержке Rostelecom	213.172.3.116	0,625152	0,252800 (40,44%)	0,023116 (3,70%)	0,024678 (3,95%)	403 Доступ запрещён	
Россия, Новосибирск, юго-восток	Невозможно соединиться с указанным адресом.						
Россия, Петрозаводск При поддержке Ростелеком	213.172.3.116	0,636606	0,119750 (18,81%)	0,031335 (4,92%)	0,032856 (5,16%)	403 Доступ запрещён	
Россия, Ростов-на-Дону При поддержке Дельта Телеком	213.172.3.116	0,835038	0,109088 (13,06%)	0,034572 (4,14%)	0,035493 (4,25%)	403 Доступ запрещён	
Россия, Санкт-Петербург, центр 1	Операция прервана, т.к. сервис не ответил в течение 8 секунд.						
Россия, Томск, восток	Невозможно соединиться с указанным адресом.						
Россия, Тюмень	Невозможно соединиться с указанным адресом. Обращение производилось к IP: 213.172.3.116.						
Россия, Хабаровск	Невозможно соединиться с указанным адресом.						
Россия, Химки	Операция прервана, т.к. сервис не ответил в течение 8 секунд.						

На антизапрете долгое время есть система определения аномалий, чтобы исключать IP-адреса популярных ресурсов из списка проксирования, если владелец заблокированного домена установил А-запись на этот IP-адрес. Список IP-адресов для определения аномалий составлял сам, в него попали популярные мировые и российские сайты, корневые DNS и DNS распространенных доменных зон, технические банковские домены.
Проснувшись утром в понедельник, я обнаружил большое количество аномалий, удивился, и решил проверить доступность некоторых сервисом ping-admin.ru — результат на скриншоте выше. Не знаю, как долго они продержались и на каком домене были установлены, т.к. скрипт запускался раз в 6 часов и выдавал только список IP-адресов (сейчас я его уже модифицировал). В последующей выгрузке этих IP уже не было.

…и продолжается

7 июня, в неумелых попытках исправить ситуацию, Роскомнадзор составил и направил «белый» список сайтов провайдерам, с IP-адресами и доменами, которые лучше бы не блокировать.



РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ВЛАДИМИРСКОЙ ОБЛАСТИ
(Управление Роскомнадзора по Владимирской области)

Руководителям организаций

№
На № от

Уважаемые коллеги!

Управление Роскомнадзора по Владимирской области в целях реализации положений п. 5 ст. 46 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» доводит перечень сетевых адресов, доступ к которым рекомендуется не ограничивать (прилагается).

Приложение: 1 файл.

Руководитель В. В. Никоноров

Роскомнадзор объединил ячейки в XLS-документе так, что каждую вторую запись не было видно, и многие долго пытались понять, почему, например, одни корневые DNS-серверы в него вошли, а другие — нет. Все стало ясно, когда кто-то додумался установить высоту всех ячеек в одинаковое значение.

Весельчаки-затейники начали оставлять в DNS-записях послание Роскомнадзору и провайдерам (есть даже от 14-летнего мальчика), а также сделали собственный сервис блокирования произвольных IP-адресов!

Позже очнулись магистральные провайдеры. Поняв, что так дела не делаются, Транстелеком сначала начал проксировать все запросы к заблокированным сайтам в транзите (буквально, через squid, с изменением исходящего IP-адреса), а затем начал отключать блокирование транзитного трафика, заставляя мелких провайдеров фильтровать сайты самостоятельно.

Последняя аномалия выглядит следующим образом:

```
104.244.42.129 nudism.ga. # twitter
104.244.42.193 nudism.ga. # twitter
109.207.1.97 nudism.ga. # gosuslugi.ru
163.172.11.143 zenitbet44.com. # meduza.io
163.172.11.149 zenitbet44.com. # meduza.io
163.172.180.25 zenitbet44.com. # meduza.io
163.172.40.199 zenitbet44.com. # meduza.io
163.172.73.23 zenitbet44.com. # meduza.io
163.172.74.46 zenitbet44.com. # meduza.io
194.54.14.159 nudism.ga. # sberbank
194.67.29.100 www.segodel.com. # securepay.rb.ru
216.146.46.10 www.1Osport10t.com. #travel.s7.ru
216.146.46.10 www.betrallyru.com. #travel.s7.ru
216.146.46.11 www.1Osport10t.com. #travel.s7.ru
216.146.46.11 www.betrallyru.com. #travel.s7.ru
50.112.196.159 nudism.ga. # twitch
52.36.196.57 nudism.ga. # twitch
52.41.96.17 nudism.ga. # twitch
5.255.255.88 bethaze.ru. # yandex
5.255.255.88 dabet.ru. # yandex
5.255.255.88 zerkalo-tv.ru. # yandex
77.88.8.88 www.segodel.com. # yandex
88.212.240.172 zenitbet44.com. # meduza.io
88.212.244.68 zenitbet44.com. # meduza.io
91.227.34.40 zenitbet44.com. # meduza.io
95.167.27.74 www.segodel.com. # DNS Rostelecom
95.213.255.15 tjournal.ru. # tjournal.ru
```

Чего ждать дальше

Ау, Роскомнадзор! Может, уже что-нибудь, ну, скажете, хотя бы, если не сделаете? Вы там сдохли, что ли? Буквально несколько часов назад произошли масштабные сбои в обслуживании банковских карт.

Делайте выводы.

роскомнадзор, ревизор, блокировки сайтов, блокировки

+14 1,1k 5

@ValdikSS карма 408,5 рейтинг 8,1

ПОХОЖИЕ ПУБЛИКАЦИИ

12 февраля 2016 в 19:56
Правообладатели предлагают штрафовать за инструкцию обхода блокировки на 50 тысяч рублей
+33 25,1k 17 297

12 февраля 2016 в 13:45
Роскомнадзор поддерживает блокировку «Роскомсвободы» за инструкцию обхода блокировки сайтов
+13 10,8k 4 61

25 января 2016 в 00:29
Роскомнадзор начал блокировать сайты, продающие хамон, прошутто и другие санкционные продукты
+13 12,1k 9 39

САМОЕ ЧИТАЕМОЕ

Сейчас | Сутки | Неделя | Месяц

Светодиодные лампы IKEA 2017 года
+16 3,1k 15 8

Июньская ситуация с недоступностью ресурсов из-за блокировок веб-сайтов
+12 1,1k 5 3

Почему игра «Mass Effect: Andromeda» получилась такой, как получилась: разработчики рассказывают о проблемах
+2 1,4k 6 17

Softbank купила у Google Boston Dynamics
+2 898 1 3

Отдельные тонкости в работе полупроводниковой индустрии
+21 5,7k 4 16

Комментарии (3)

lolipop 9 июня 2017 в 20:55 +1

Жаль, что РКН скорее всего и себя в белый список IP внёс.

ValdikSS 9 июня 2017 в 20:55 +1

Внес, это давно еще было, даже не в прошлом месяце.

darkk 9 июня 2017 в 21:04 +3

> Транстелеком сначала начал проксировать все запросы к заблокированным сайтам в транзите

Мне больше интересно, что произойдет с подобными фильтрами на транзите, если количество IP-адресов в которые резольвятся доменные имена из реестра подербётся к размерам TCAM на маршрутизаторах. Если я верно понимаю Ig, то домены в роуты /32 резольвит не только ТТК, но и, например, Ростелеком.

Если каждый хулиганский домен отдаст по 4000 рандомных устаревших IPv4 адресов и по 2300 современных IP (примерно столько помещается в DNS-ответ максимального размера), то для выжирания TCAM с 512к записями, если я не обсчитался, достаточно будет примерно 60 доменов. У одних только граней.ру их в 10 раз больше. Disclaimer: *.rnd.darkk.net.ru. в реестре нет, это я поведение резольверов с большими ответами тестирую в рамках ООН и трафик на этот домен логируется.

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

ЧТО ОБСУЖДАЮТ

Сейчас | Вчера | Неделя

Светодиодные лампы IKEA 2017 года
3,1k 10

Взял видеоинтервью у вице-президента Ардуино и обсудил с ней преподавание школьникам ПЛИС-ов / FPGA и языка Verilog
5,9k 194

Роботакси могут сделать владение собственным автомобилем бессмысленным
9,5k 163

Социокибериженерия Жака Фреско
8,9k 79

В Думу внесли законопроект о запрете анонимайзеров и сервисов VPN
36,5k 590

ИНТЕРЕСНЫЕ ПУБЛИКАЦИИ

Июньская ситуация с недоступностью ресурсов из-за блокировок веб-сайтов
+12 910 5 3

Security Week 23: EternalBlue портировали на Win10, ЦРУ атакует с файлсерверов, маркетологи незаметно заразили весь мир Хабр
+5 386 3 0

О новых интересных законах или «Тварь ли я дрожащая или всё-таки сообщество» Хабр
+11 2,7k 7 32

Гейзенбаг 2.0: как прошла в Петербурге конференция по тестированию Хабр
+16 631 7 1

Светодиодные лампы IKEA 2017 года
+16 3k 15 7