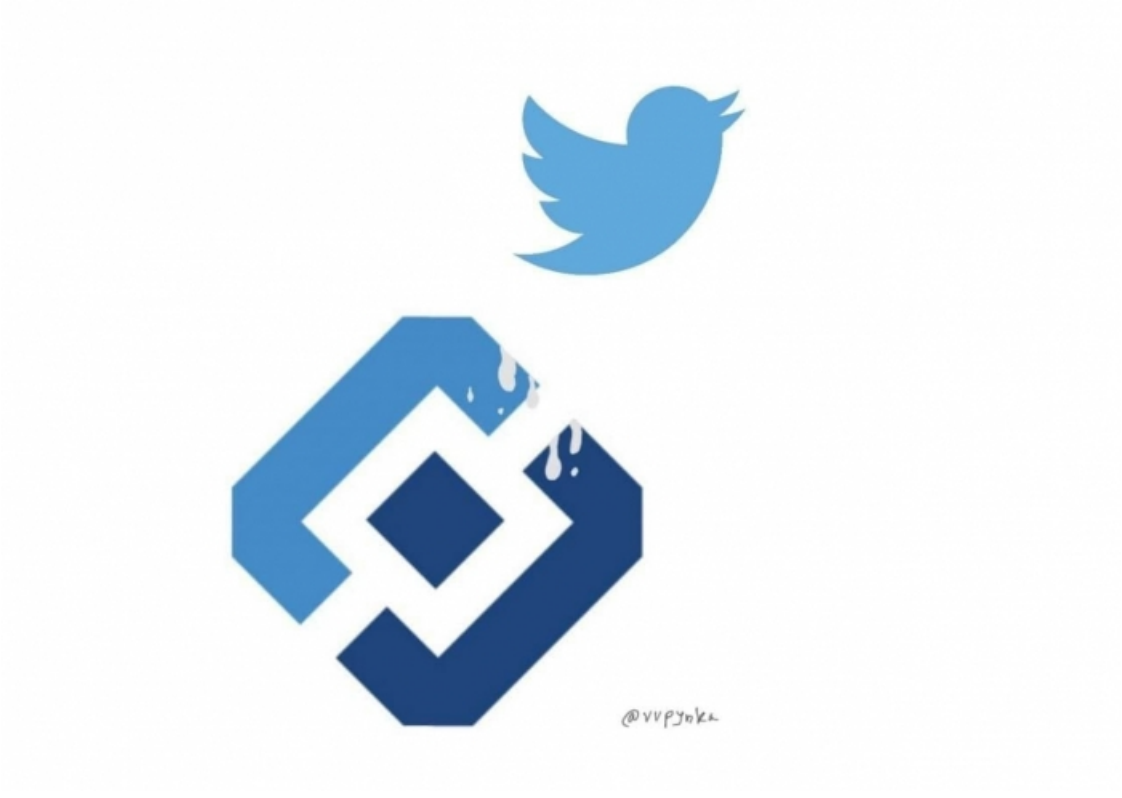
Разведка боем: борьба РКН с Twitter - лишь начало

Март 2021 года вместе с потеплением и запахами весны принес с собой и ностальгические нотки о весне 2018 года. Тогда Роскомнадзор, возглавляемым Александром Жаровым, объявил войну мессенджеру Telegram. Уверенный в себе и своих подопечных из РКН, Жаров решил раз и навсегда убрать из смартфонов россиян непокорный мессенджер, попутно объявив Павла Дурова врагом и даже пособником террористов (во всяком случае, так говорилось на многих телеканалах). Тогда на мессенджер ополчились все - от политиков до звезд государственной пропаганды. РКН своими неумелыми действиями порушил половину рунета, не нанеся, при этом, никакого урона Telegram. В результате, Telegram спокойно работает и от него уже отстали. У пропагандистов теперь новые враги, о чем они сообщают подписчикам в некогда запрещенном мессенджере, а Жаров ушел в "Газпром-Медиа", создавать российский аналог YouTube. Но дело его живет.

Роскомнадзор 10 марта объявил о том, что начал замедлять интернет-трафик Twitter. Выяснилось, что у регулятора попросту накипело: ведь социальная сеть систематически не исполняет требования Роскомнадзора, попросту игнорируя их. По словам представителя ведомства, Twitter с 2017 года не исполняет указания регулятора по удалению противоправного контента. Роскомнадзор нашел на страницах социальной сети более 3 тысяч публикаций, содержащих призывы к самоубийству, детскую порнографию и пропаганду наркотиков.

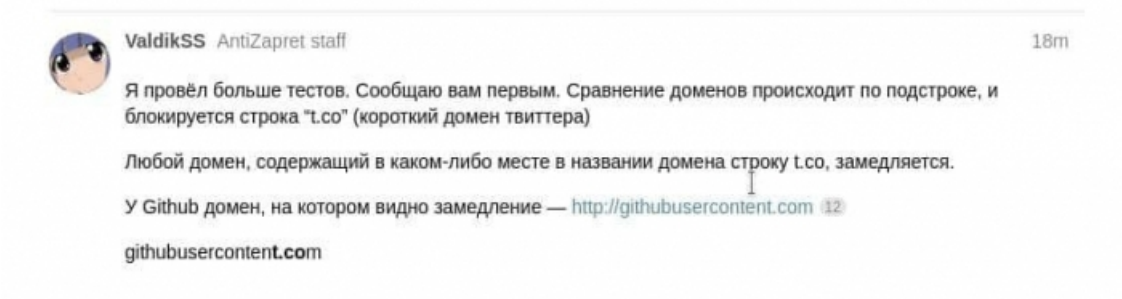
В Роскомнадзоре пояснили, что с 10 марта замедление работы социальной сети реализовано на 100% мобильных устройств и 50% стационарных. Не знаю, заметили ли пользователи реальное замедление работы Twitter, но лично автор этих строк никаких проблем при работе с социальной сетью не почувствовал. Однако, весь рунет заметил другие, более серьезные проблемы, которые начались в аккурат со старта действий РКН против Twitter.



В тот же день 10 марта начались проблемы с работой ряда ресурсов государственной власти - перебой в работе наблюдались у сайтов Правительства, Госдумы, Совета Федерации, МВД и даже самого Роскомнадзора. Также подключиться к сети не могли до 90% пользователей "Ростелекома". Проблемы были у "Почты России", ряда банков и так далее. И это Роскомнадзор еще не начал полностью блокировать Twitter, а лишь попытался немного притормозить работу сети.

Роскомнадзор, судя по всему, решил избрать иной путь для осложнения работы Twitter, нежели использовал при блокировках Telegram. Теперь банальный бан по IP-адресам был отложен на полочку, и за дело взялись современные системы по фильтрации трафика (DPI), которые установлены на сетях всех операторов связи.

Как удалось выяснить одному из IT-энтузиастов, чтобы замедлить работу Twitter, оборудование DPI анализирует трафик и тормозит работу доменов, имеющих в своем имени строку t.co. Это короткий домен Twitter. Но беда в том, что в доменных именах тысяч интернет-ресурсов может содержаться аналогичная комбинация знаков.



Так, автор Telegram-канала "ЗаТелеком" Михаил Климарев привел лишь сотню самых популярных ресурсов с аналогичным набором знаков в доменном имени, которые пострадали от действий РКН. Там оказались популярные ресурсы для геймеров и владельцев компьютеров от Apple.

ЗаТелеком
Сайты, которые попали по коллатеральные ЗАМЕДЛЕНИЯ от РКН. Отсортированы по популярности. Автор списка — ValdikSS

9,pinterest.com,84
10,microsoft.com,82
18,enable-javascript.com,79
48,blogspot.com,75
60,bluehost.com,72
71,mydomaincontact.com,70
72,reddit.com,70
78,namebright.com,70
79,dreamhost.com,70
84,t.co,69
112,akismet.com,
140,trustpilot.com,
159,dynadot.com,
193,constantcontact.com,
245,hubspot.com,
247,cointernet.com.co,
254,getpocket.com,
256,washingtonpost.com,
286,opencart.com,
301,sciencedirect.com,
314,shinystat.com,
318,huffingtonpost.com,
351,snapchat.com,
352,proofpoint.com,
354,googleusercontent.com,
389,pinterest.co.uk,
434,cnet.com,
463,format.com,
472,cookiebot.com,
486,onetrust.com,
495,independent.co.uk,
504,ewebdevelopment.com,
526,matterport.com,
532,deviantart.com,
537,indiamart.com,
538,blogspot.co.uk,
542,quantcast.com,
578,ft.com,
579,angieslist.com,
584,blogspot.com.es,
585,mapquest.com,
591,xinhuanet.com,
610,sharepoint.com,

Автора телеграм-канала "IT уголовные дела СОРМ Россиюшка" Владислав Здольников так описывает причины, по которым при замедлении работы Twitter пострадала весомая часть рунета.

> "Дело в том, что через оборудование DPI, которое устанавливает Роскомнадзор, проходит весь трафик всех пользователей, даже если он никак не ограничивается.
>
> Это оборудование производит компания РДП.РУ и называется оно ЭкоDPI. Операторы давно, по своей воле и за свои деньги, используют оборудование этой фирмы для решения внутренних задач, вроде NAT или тех же блокировок. То есть, оборудование достаточно проверенное и работает в целом качественно.
>
> Но оно никогда не использовалось на деле так, как сегодня: для ограничения скорости от конкретного популярного ресурса, с настоящей нагрузкой в сотни тысяч пользователей. Поэтому, софт на оборудовании дал сбой, и так как через него проходит весь трафик, интернет раскорячило.
>
> Напомню, что закон, по которому устанавливается оборудование DPI, принят для "защиты рунета от внешних угроз", но почему-то по этому закону и этим оборудованием ломает рунет администрация президента и Роскомнадзор", - пишет Здольников в своем Telegram-канале.

По словам начальника проектного отдела сетевого оборудования компании НАГ Андрея Шепелева, для того чтобы замедлять трафик куда угодно, Роскомнадзор должен иметь доступ к оборудованию, которое стоит в точке консолидации этого самого трафика - например, на аплинке провайдера или просто в каком-то похожем месте. Далее трафик анализируется по каким-либо отличительным признакам до сервера Twitter.

> "Это может быть все что угодно: от банального конечного адреса и заканчивая какими-то особенностями самого потока до социальной сети. Так как их все ругают за t.co, возможно они искали в пакете совпадение с подобной маской или что-то такое. Если находили, то ограничивали скорость работы данных потоков любым шейпером. В целом все банально.

> Когда происходят подобные вещи, просто криво настроены правила отбора сетевых потоков и туда попадают легитимные данные", - отметил Андрей Шепелев.

Интересно, что на фоне действия РКН, акции Twitter просели на 4%, а в самой социальной сети заявили, что обеспокоены "попытками блокировать общественный диалог в сети". По данным Brand Analytics, сообщения в Twitter в России активно публикуют около 690 тыс. человек – по этому показателю сервис осенью 2020 года занимал седьмое место в рейтинге социальных медиа. По данным SimilarWeb, сайт Twitter - 21-й по популярности в России.

В Роскомнадзоре подчеркнули, что Twitter до сих пор никак не отреагировал на призывы Роскомнадзора исполнять требования российского законодательства. При этом, российские власти готовы к открытому и честному диалогу с администрацией социальной сети.

По словам Михаила Климарева, действия Роскомнадзора могут существенно ухудшить работу рунета в целом, ведь теперь каждый пакет интернет-трафика нужно досматривать и отслеживать: а не бежит ли он в сторону Twitter? Все это замедляет загрузку ресурсов и ухудшает качество связи.

В целом же, многие эксперты сходятся во мнении, что текущие действия Роскомнадзора - это некая проверка боем, и дальше нас ждет еще большее усиление конфронтации между регулятором и крупнейшими интернет-площадками мира. Сейчас РКН лишь тестирует возможности и ищет подходы, поэтому для атаки и был выбран именно Twitter, который имеет не самую высокую популярность в России, да и трафик на социальную сеть, где публикуются лишь короткие тексты и картинки, не такой уж тяжелый. В дальнейшем, Роскомнадзор предпримет попытку полностью блокировать Twitter на территории России и уже тогда обрушится на Facebook.

Впрочем, и в самом Роскомнадзоре уже заявили, что готовы полностью блокировать Twitter, если там продолжат игнорировать требования регулятора. Судя по всему, противостояние российских властей и крупнейших западных интернет-площадок вступает в более острую фазу, и в скором времени нас ждет еще больше интересных событий. Ясней становится и необходимость закона о "суверенном интернете", который, как нас всех убеждали" еще год назад, вовсе не предназначен для блокировок и цензуре в сети, а нужен лишь для сохранения работоспособности отечественного сегмента сети.