

Как кибербезопасникам подкинули кибернаркотики

В воскресенье, совсем не в пиковое для новостей время, Илья Сачков, гендиректор довольно известной в кругах инфобезопасников компании "Group-IB" на своей странице в Facebook опубликовал пару скриншотов и скромно их подписал: "отлично! подаем в суд=)".

А уже в понедельник об этом написали полсотни ведущих СМИ и информационных агентств, и оживленно обсуждал Рунет.

Так что же так возмутило топа одиозной киберзащитной компании? И почему это стало такой горячей темой?

Начнем с того, что Илья Сачков внезапно узнал, что Ростелеком на тот момент уже как минимум месяц блокирует их англоязычный интернет-ресурс.

Вернее, на тот момент никто из "Group-IB" не подозревал - сколько по времени находится их ресурс под такой блокировкой, это осознание пришло позже, когда "[РосКомСвобода](#)" представила анализ случившегося, в ходе которого всплыло 2 решения Госнаркоконтроля по блокировке IP-адреса, на котором и расположен непосредственно сайт кибербезопасников.

Решение по внесению соответствующей записи в Реестр запрещенных сайтов было принято дважды - еще в середине октября и касалось блокировки домена и страниц портала drugspace.info, на котором ФСКН нашла информацию по распространению наркотиков.

А как мы знаем, закон о "черных списках сайтов" 139-ФЗ, внедренный осенью прошлого года, позволяет вносить в реестр не только страницы и домены, которые запрещены надзорными ведомствами, но и соответствующие сетевые адреса. Чем и пользуются те операторы, которые осуществляют так называемую IP-блокировку, при которой подпадают под ограничение доступа до десятков тысяч других добропорядочных сайтов, расположенных на том же сетевом адресе.

Ростелеком, получив очередную подобную выписку из реестра, ограничил доступ ко всему IP-адресу. Ну и в очередной раз нарвался на более-менее известный портал, который висел на том же IP.

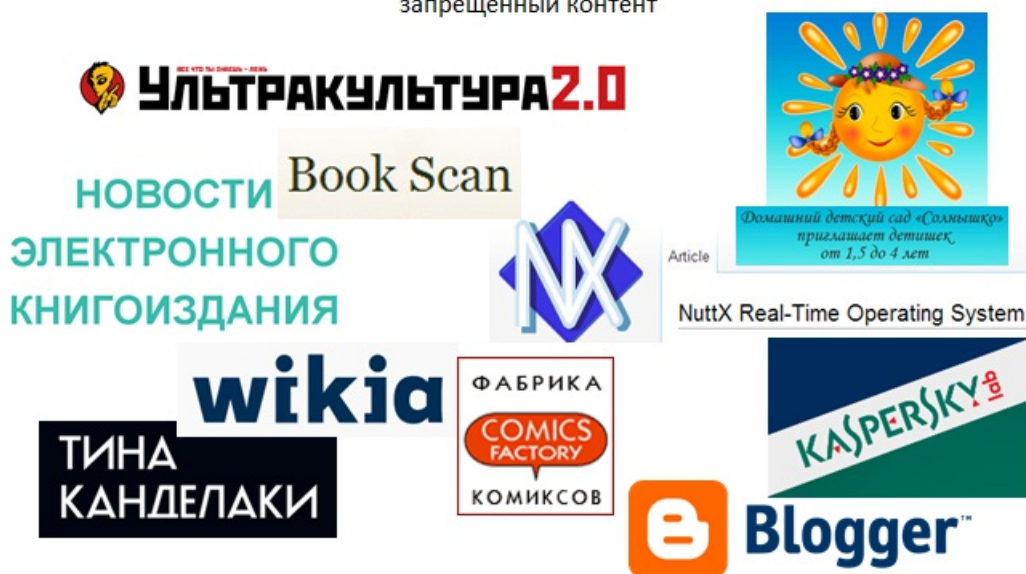
Громкими такие случаи становятся в двух случаях:

1. попадает под такую ростелекомовскую блокировку широкоизвестная или аффилированная с госструктурами компания/портал/личность;
2. владелец заблокированного таким образом интернет-ресурса подает в суд.

Применение закона «о чёрных списках сайтов»

А что блокируется заодно?

только потому, что данные ресурсы находятся на том же IP-адресе, что и запрещенный контент



По первому варианту такие случаи уже не редкость, например, под такую блокировку попадал один из ресурсов "Лаборатории Касперского", сайт Тины Канделаки, социальная сеть "Мир Тесен", блог-

платформы Blogger и Wordpress.com, многие электронные библиотеки, ряд ресурсов Google также страдали от такого вида блокировки и т.д.

Насчет судебных процессов - на данный момент самый резонансный - это отстаивание владельцем ресурса электронного книгоиздания Владимиром Харитоновым права на доступ к своему portalу www.digital-books.ru, который также подвергнулся блокировке по IP-адресу "за компанию". На данный момент [готовится жалоба](#) в "Европейский суд по правам человека", т.к. Мосгорсуд встал на сторону наших госорганов и впоследствии отклонил и апелляцию по делу.

И вот в данном случае п.1 совпал с п.2: мало того, что компания "Group-IB", известная в своих кругах, поддерживает многие государственные начинания, равнодушна к одиозной "Лиге безопасного интернета" (зачинщицей и евангелистом самих "черных списков сайтов"), получила на днях "Премия Рунета" в категории "Безопасный Рунет", спонсируемой всё той же ЛБИ, так еще и намерилась на всем этом фоне все-таки судиться с правоприменительной практикой блокировки, под которую сами попали.

Фантазмагория и гротеск!

Цитата:

"Г-н Сачков считает, что посетители могли ассоциировать сайт с незаконной деятельностью, и оценивает ущерб, нанесенный компании, в 3-5 млн долл. Юристы считают, что Group-IB может выиграть дело.

Методику оценки ущерба именно в эту сумму г-н Сачков не поясняет так же, как не готов пока сказать, к кому именно будет иск - к "Ростелекому" или Роскомнадзору, но считает, что произошедший инцидент показывает недоработки действующего закона. "Технически закон надо доработать так, чтобы от его действия не страдали честные компании. Мы решили подать в суд, потому что блокировка сайта негативно отразилась на репутации компании. При этом ресурс, который послужил главной причиной этой блокировки, просто поменял IP-адрес и работает до сих пор"" (из интервью [РБК daily](#))

Интересное [общение](#) развернулось между представителями компании и Ростелекомом в твиттере. Выжимка:

"Известия": Для снятия блокировки сайта компании Group-IB, "Ростелеком" рекомендовал сменить IP-адрес

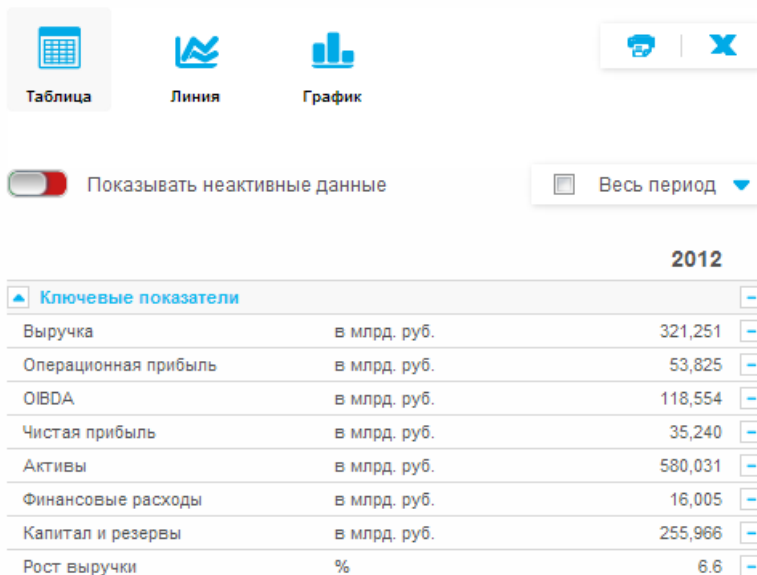
"Group-IB": пусть наркоторговцы меняют IP

"Ростелеком": IP в реестре eais.rkn.gov.ru, можете обжаловать решение ФСКН и Роскомнадзора в установленном порядке

"Group-IB": судебный процес научит Ростелеком в 21м веке блокировать ресурсы по url

"Ростелеком": Мы готовы выслушать ваши предложения по бюджетному внедрению DPI в масштабах всей страны.

Финансовые показатели



(Финансовые показатели "Ростелеком" за 2012 г., [источник](#))

На данный момент закончилось все тем, что Роскомнадзор внезапно узнал, что запрещенный ресурс [drugspace.info](#) из-за которого и закатился весь этот сыр-бор уже давно мигрировал на другой IP-адрес и исключил злосчастный IP из реестра и соответственно дал добро операторам не блокировать его.

Ситуация становится еще более пикантной: Ростелекомом блокировался IP-адрес, на котором уже и не было запрещенного ресурса.

НИ ОДНОГО запрещенного!

Только 441 добропорядочных доменов самой разной тематики (по результату проверки на портале [www.yougetsignal.com](#)):

www.iurwastash.us	www.iurwastash.com
www.freebooksf.mobi	www.fueled4health.com
www.fullsteamlabs.com	www.fushanlang.com
www.gameactors.com	www.gamuting.com
www.gardengrove.net	www.gavinchester.com
www.getchu.co	www.gibbs-inc.com
www.glidenote.com	www.goloud.net
www.group-ib.com	www.haileysasha.com
www.hairsalonportjeffersonstation.com	www.haohuifen.com
www.hardinfo.it	www.hariritea.com
www.hdmacyayinlari.com	www.healthydiaries.com
www.hepatitis.cl	www.herringbonebindery.com
www.hnrecords.co.uk	www.hockeylog.com
www.hollywoodindieslittleleague.org	www.homeimprovementrocksprings.com

Интересные выводы:

1. Компания, которая позиционирует себя, как "одну из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий" располагается на т.н. "shared IP hosting", вместе с другими доменами, явно не принадлежащими данной ИБ-компании.
2. Реестр продолжает функционировать только в ручном режиме, автоматом только рассылаются выписки из "черных списков сайтов", а контроль и реакция на неправомерные блокировки происходит только когда становится уже "совсем жарко".
3. Продолжается практика блокирования IP-адресов даже после миграции запрещенных доменов с них, выявленный случай далеко не первый.
4. Компания, которая положительно высказывалась относительно практики ограничения доступа к интернет-ресурсам со стороны госорганов и внедрения "черных списков", сама столкнулась со своей блокировкой и готова подавать в суд на это.
5. Портал "DrugSpace", который послужил косвенной причиной блокировки "Group-IB" снова доступен и радует глаз своих прихожан. Кстати если внимательно ознакомиться с содержимым сайта - то там идет просто общение наркозависимых, а не является форумом по продаже препаратов, да и в их правилах записано, что в числе прочего "строго запрещено: пропаганда

наркотиков, любые попытки продать/купить ПАВ".

Одним словом, одни, так или иначе, пострадали материально, другие - репутационно, третьи - изображают бурную деятельность, четвертые - не следят за наполнением и содержанием реестра, пятые - наплеватьски относятся к своим клиентам и к своим обязанностям и т.д.

Все, что угодно, но только все это никоим образом не касается защищенности наших детей, как то было заявлено при внедрении закона по внесудебной блокировке интернет-ресурсов и под прикрытием чего это происходит уже больше года.

А ведь всем нам хотят навязать новые категории запрещенной информации, подобные законопроекты уже внесены в Госдуму и ждут своего часа.

Абсурд продолжается, и будет только увеличиваться.

Но, посмотрим как будет разворачиваться судебный процесс, если только сама компания не откажется от своих слов и после консультаций во властных коридорах не заиграет тему.