Золотая цензура Китая, часть 2

Во второй части опусов про устройство "Великого китайского файервола" разберем технико-экономическую составляющую системы, и попробуем заглянуть из-за стены. Можно ли обойти "огненную информационную стену", окружающую Китай?

И сразу отвечу на вопрос, обозначенный в анонсе: стену обойти можно. Рассказ об этом есть в первой части сериала, про то, как "папа GFW" Фань Биньсинь публично продемонстрировал способ обхода на конференции в Харбине - открыл VPN и зашел на заблокированный сайт.



Правда, последний год китайские телеком-чиновники ужесточили борьбу с VPN-операторами, которых в Китае развелось видимо-невидимо, что логично. Но "борьба" ведется только с легальными сервисами, которые сделали бизнес на защите данных и приватности пользователей.

Например, только за полгода 2017-го года были закрыты десятки провайдеров, предоставляющих услуги VPN-соединений. У одного из крупнейших из них, GreenVPN, были десятки миллионов клиентов и миллионы долларов оборота в месяц.

Теперь на сайте висит объявление:



Короткий перевод:

> "Мы больше никогда не встретимся. GreenVPN закрывается с 1 июля 2017 года".

Далее идут вопросы по возврату денег за услуги и кнопка "Отказаться от абонентской платы". Причем, если вы откажетесь, то...

То вам предложат подключиться к другому сервису, который находится вне зоны юрисдикции китайской цензуры.

Ну, а кто откажется?

Представьте себе 730+ миллионов пользователей интернета, из которых уже в 2015 году о существовании такого сервиса, как VPN знали не менее половины (данные опроса, но закрыты за пейволлом, но есть еще GlobalWebIndex и журнал Wired, которые подтверждают цифру), а фактически использовали не менее трети. Посчитали? Это 243 миллиона пользователей. Прописью - двести сорок три миллиона. Даже если собрать с них по доллару в год, это уже внушительная сумма, на которую найдутся желающие, несмотря на проведение XIX съезда КПК, которое планируется осенью текущего года.

Ну, и считается, что основной способ цензурирования находится "внутри пользователя". А чтобы граждане Поднебесной не забывали, что необходимо воздержаться от скоропалительных выводов и излишне эмоциональных высказываний в социальных сетях, существует целая армия "умаодан", которые при необходимости объяснят политику партии.

Впрочем, мы опять отвлеклись на гуманитарщину, а обещана была техническая сторона.

Архитектура ChinaNet

Итак, проект Golden Shield, он же Great Firewall of China (GFW) является крупнейшей в мире системой цензурирования интернет-содержания на магистральных сетях передачи данных. Эта система изначально централизована и устроена как "фильтр-на-пути". GFW может отслеживать и "окрашивать" трафик, т.е. помечать отдельные пакеты специальным образом. Но система не может в принципе заблокировать доставку пакетов в процессе передачи от источника и до места назначения.

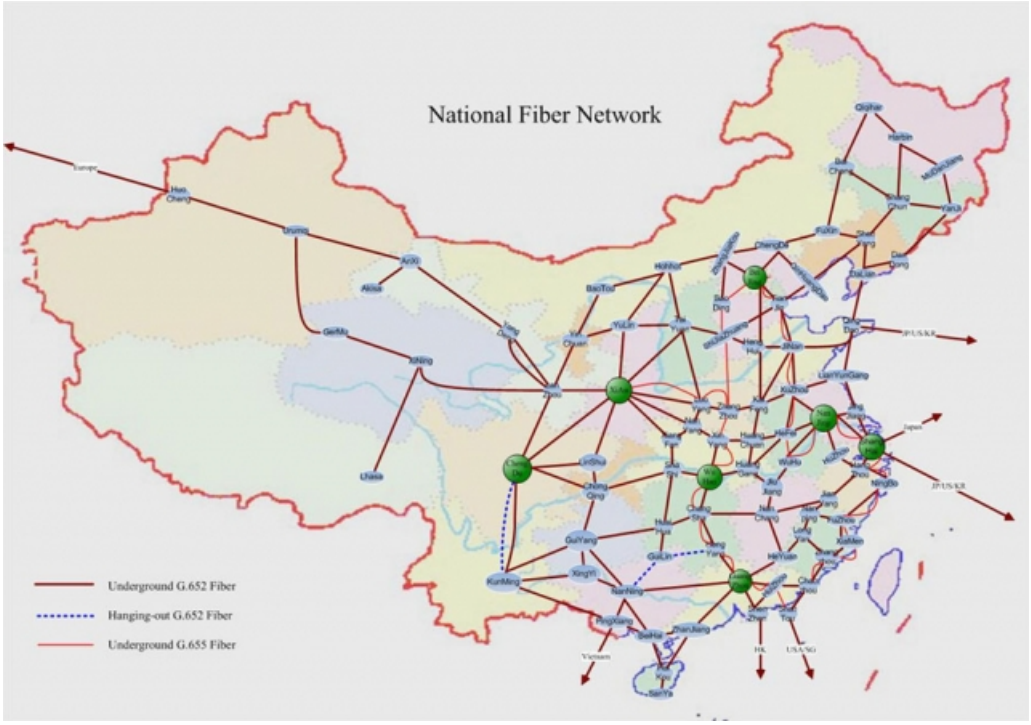
Важно понять главный архитектурный принцип "Золотого щита": это буквально firewall между "внутренним интернетом Китая" и остальным миром. Вся связь между Поднебесной и остальным миром проходит только и исключительно через "специальные серверы", установленные в

установленных законом точках обмена трафиком. И все оборудование принадлежит государственным компаниям, которых, по большому счету, две: China Telecom и China Unicom. Вот полный список организаций, которые имеют право на трансграничный трафик:

1. China Academy of Information and Communications Technology;
2. China Telecommunications Corporation (aka China Telecom);
3. China Mobile Communications Corporation (aka China Mobile);
4. China United Network Communications Group Co., Ltd. (aka China Unicom);
5. China Radio and Television Network Co., Ltd.;
6. CITIC Networks Co., Ltd.

Итого - 6 (шесть) компаний, из которых одна правительственная образовательная организация, одна правительственная медиакорпорация, а остальные, по сути, аффилированные с правительством компании.

Вот есть такая, довольно устаревшая схема сетей Китая от China Telecom:



Всё, что внутри Китая - называется ChinaNet и, так или иначе, контролируется правительством Китая. Все, что снаружи - это Global Service, и должно подключаться только и исключительно через шлюзы GFW. Глобальная связность рисуется примерно так:



Интернет-шлюзы доступа в ChinaNet делятся на несколько уровней. Базовые "национального (National) уровня" их три, и они находятся в локациях: Beijing (Пекин), Shanghai (Шанхай), Guangzhou (Гуанчжоу).

Потом, по мере роста трафика, были добавлены шлюзы класса "Core Level", которые расположены в городах: Шэньян (Shenyang), Сиань (Xi"an), Чэнду (Chengdu), Ухань (Wuhan), и Нанкин (Nanjing).

Остальные точки обмена трафиком находятся на "третьем уровне" (Metropolitan Area Network) и подключаются исключительно к уровню "Core Level".

В 2015 году, из-за кратного роста трафика, Китаю пришлось построить еще семь backbone-узлов в городах Чэнду (Chengdu), Ухань (Wuhan), Сиань (Xi"an), Шэньян (Shenyang), Нанкин (Nanjing), Чунцин (Chongqing), и Ченджоу (Zhenzhou), часть из которых "подняли" с уровня "Core Level" до "National", часть построили заново.

В общем, чтоб не запутаться, сейчас (на момент написания более свежей информации не нашел) в Китае ровно 10 точек обмена трафиком между ChinaNet и "остальным миром".

Пропускаемый через эти узлы трафик - огромен. Представьте себе 730 миллионов абонентов со средней скоростью 3,7 mbps (это "внешняя" скорость - "внутренняя", в два раза выше - можно поиграться с цифрами на карте AKAMAI) и порядка 100 млн. выданных APNIC IP v4 адресов.

Стоимость строительства точек доступа - засекречена. Но оценочные суммы по эксплуатации узлов, хоть и расходятся в разы, но есть сведения (на китайском), что только на первом этапе в 2002 году, разработка проекта обошлась в 3,7 миллиарда юаней. Бюджет "до запуска" оценивался в 0,8 миллиарда долларов. Без учета, повторюсь, эксплуатационных издержек и расширения инфраструктуры.

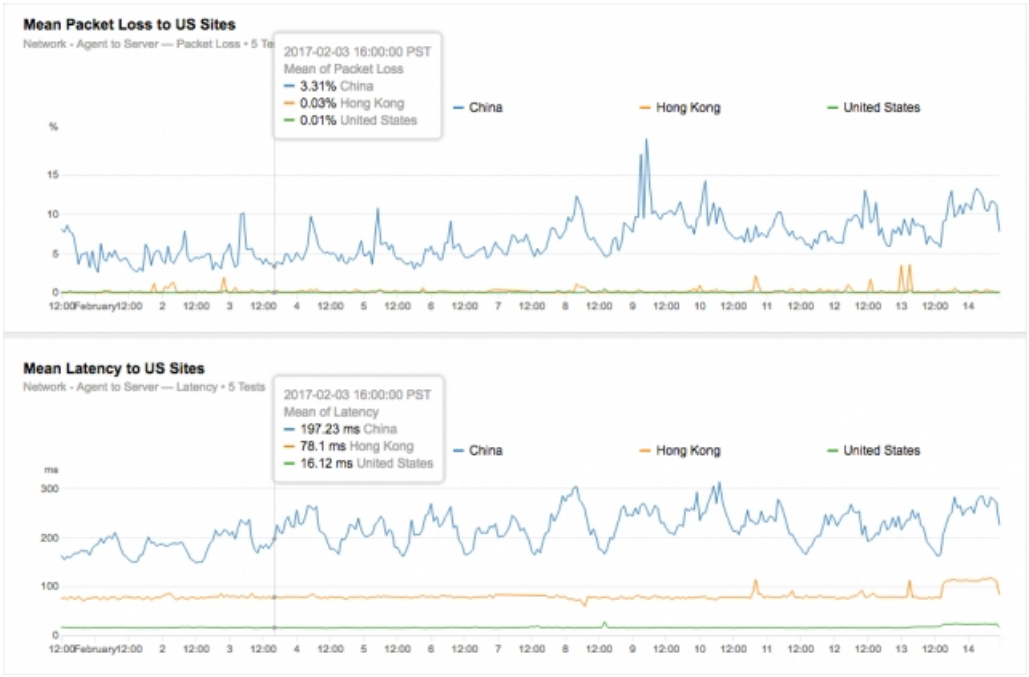
3,7 миллиарда юаней, это 32,8 миллиарда рублей, в текущих ценах.

Плюс, на последнее расширение "Core Level" узлов в 2015-ом году было оценочно выделено не менее 470 миллионов долларов.

Понятно, что за все расплачивается конечный потребитель, и для столь огромного рынка "лишний" миллиард долларов, это капля в море. Ну, распределили на всех один-два доллара затрат в год на каждого абонента. А что не так-то?

Коллатеральные потери

Но дело в том, что затраты бывают не только прямые финансовые, но и, например, вот такие:



Это потери производительности работы сети, которые измерили и в компании Tthousandeyes. То есть, для каждого пользователя Golden Shield создает накладные расходы в виде потери пакетов, роста задержек и джиттера.

Все, кто хоть раз пытался общаться по фейсбуку и скайпу с китайскими партнёрами, то наверняка отметил, что качество связи несколько хуже... Вот поэтому.

Как они это посчитали?

Весьма стандартно, с помощью специальных зондов, которые были установлены в десятках китайских городов добровольцами.



Кроме того, точно такие же зонды с аналогичными прошивками и логикой, были установлены в других городах юго-восточной Азии - в Гонконге, Японии, Индии и т.п.

Зонды совершенно стандартны. Примерно вот такие:



Вот об этих конкретно зондах я обязательно напишу в ближайшее время.

А еще, в этих приборах вы можете обнаружить сходство с "Ревизором". Но очевидно, что падение базовых параметров качества Сети в разы на "иностранных маршрутах" не просто так, а по конкретным причинам:

Network Performance to US Sites

Sorted by Countries

Countries	Network - Agent to Server **Packet Loss** Mean	Network - Agent to Server **Latency** Mean
China	6.9	217.79
Hong Kong	0.17	80.5
United States	0.04	16.59

Технология блокировки

Блокировки осуществляются с помощью трех основных методов:

1. Банальная блокировка IP-адресов (и целых IP-блоков);
2. DNS tampering and hijacking - подделка DNS;
3. Deep packet inspection - более свежая тема;
4. Фильтрация запросов;
5. Самоцензура - до сих пор самая эффективная система.

IP blocking

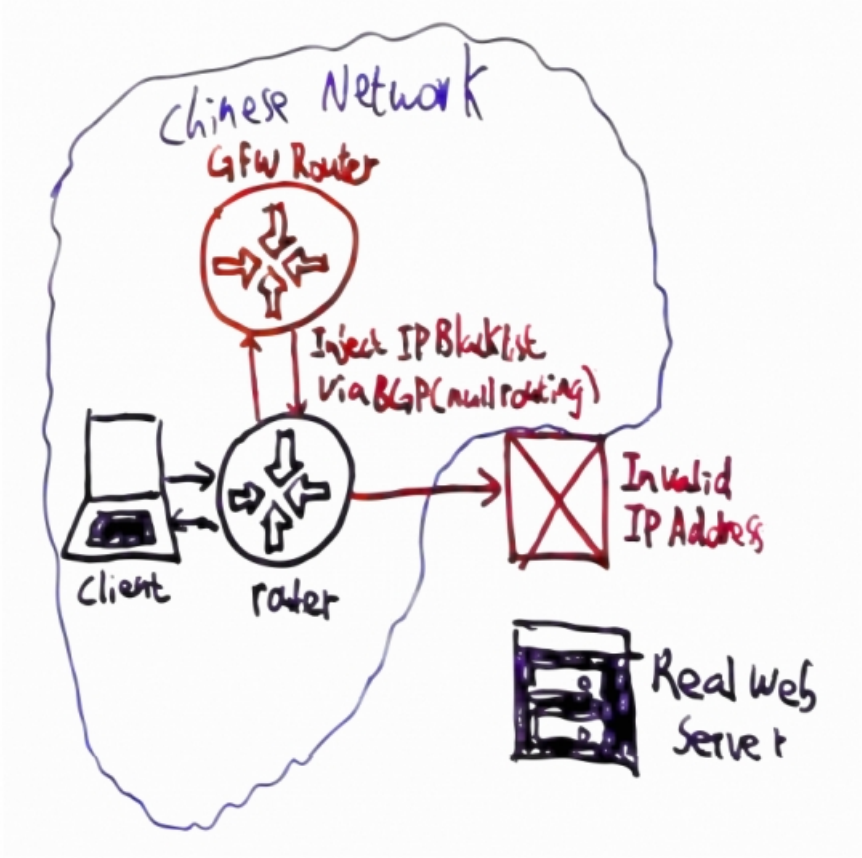
Блокировка IP-адресов - это самый простой, дешевый и доступный даже китайцам способ технической цензуры. На пограничных маршрутизаторах устанавливаем незамысловатые правила, по которым все пакеты из "черного списка" просто уходят в DROP. И самым трудоемким здесь будет как раз подготовка такового списка.

Но напомню про целую армию "умаодан" из первой части статьи, и вам станет понятно, что это как раз вообще не проблема - на сегодня размер китайского black list оценивается в 800 тысяч IP-адресов, среди которых есть и New York Times, и публичный DNS от Google (8.8.8.8). Хотя, конечно, никто точно не считал.

Кое-какая статистика [есть вот тут (а также инструменты проверки и тестирования конкретного адреса),](#) но там речь идет не о конкретных адресах, а несколько шире:



Схема блокировки IP-адресов стандартная, с использованием BGP-маршрутизаторов:



Интересная схема реализации блокировок устроена таким образом, что все пакеты, которые отправлены по IP-адресам в черном списке, просто дропаются. То есть, в отличие от российской цензурщины никто не показывает заглушек, что, дескать, "вы попытались зайти на запрещенный ресурс", а просто при обращении к заблокированным адресам вам покажет "вечную загрузку". Браузер отправил запрос, запрос прилетел до файерволла и там... потерялся. И бедный браузер будет ждать ответа, как соловей лета, пока не произойдет событие Time Out.

И это еще не всё! Дело в том, что прохождение пакетов в обратную сторону не блокируются. То есть, трафик, например, UDP вполне может приходить с заблокированных адресов. И этим какое-то время пользовались "обходчики". Но, тем не менее, для подавляющего большинства китайских пользователей это само по себе уже непреодолимое препятствие.

Блокировка по IP-адресам - самое простое цензурное решение, которое было сделано очень быстро с самого начала "открытия Интернета" Китаем. Существует централизованный черный список, который готовится без особого участия со стороны интернет-провайдеров. Маршрутизация "в ноль" осуществляется на оборудовании, к которому есть доступ только у "специально обученных людей", и таким образом гарантируется конфиденциальность как списков, так и технологии блокировки. Да и какого-то особо мощного оборудования для таких фильтров не требуется - это же базовый функционал достаточно мощного сетевого оборудования, класса "hi-end".

Вот как-то так выглядит дамп запросов к Гуглу "с той стороны файерволла":

9	1.354844	10.200.128.110	216.58.200.46	TCP	68 58013→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=44
10	1.605324	10.200.128.110	216.58.200.46	TCP	68 58014→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=44
11	1.924212	216.58.200.46	10.200.128.110	TCP	64 80→58014 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1353 SAC
12	1.924269	10.200.128.110	216.58.200.46	TCP	56 58014→80 [ACK] Seq=1 Ack=1 Win=131392 Len=0 TSval=444779035
13	1.924750	10.200.128.110	216.58.200.46	HTTP	438 GET / HTTP/1.1
14	2.122063	10.200.128.110	74.125.23.100	TCP	52 56917→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
15	2.163053	216.58.200.46	10.200.128.110	TCP	64 [TCP Out-Of-Order] 80→58014 [SYN, ACK] Seq=0 Ack=1 Win=4254
16	2.163090	10.200.128.110	216.58.200.46	TCP	56 [TCP Dup ACK 12#1] 58014→80 [ACK] Seq=383 Ack=1 Win=131392
17	2.180634	216.58.200.46	10.200.128.110	TCP	56 80→58014 [ACK] Seq=1 Ack=383 Win=43648 Len=0 TSval=335952367
18	2.190688	216.58.200.46	10.200.128.110	HTTP	596 HTTP/1.1 301 Moved Permanently (text/html)
19	2.190721	10.200.128.110	216.58.200.46	TCP	56 58014→80 [ACK] Seq=383 Ack=541 Win=130848 Len=0 TSval=444779
20	2.359679	10.200.128.110	216.58.200.46	TCP	68 [TCP Retransmission] 58013→80 [SYN] Seq=0 Win=65535 Len=0 MS
21	2.426069	10.200.128.110	74.125.23.113	TCP	52 56918→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
22	2.598143	10.200.128.110	46.82.174.68	TCP	52 56919→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
23	3.361591	10.200.128.110	216.58.200.46	TCP	68 [TCP Retransmission] 58013→80 [SYN] Seq=0 Win=65535 Len=0 MS

Кроме того, власти в момент строительства GFW сразу предусмотрели, что никаких заглушек не выдается. То есть, сэкономили даже тут - иначе пришлось бы строить вполне себе мощные серверные фермы, которые при любом обращении к Google выдавал бы страничку-предупреждение. А вы представляете, сколько раз эта страничка выдавалась бы в день, если учесть, что абонентов сотни миллионов?

Но проблема блокировки по IP вполне себе понятная и известная. Она называется DNS (тут должен

быть стикер из телеграма, посвященный РКН-тян).

Во-первых, блокировка по IP бессильна, если заблокированный сайт будет менять в А-записях адреса разрешения доменного имени. И это действительно происходило довольно часто с мелкими ресурсами, где аудитория была китайской.

Против интернет-гигантов класса Google или Facebook - это довольно эффективно оказалось, но вот против, например, сайта запрещенной в Китае секты Фалунь Дафа (на всякий случай, не буду давать адреса - на Наге есть некоторое количество неуравновешенных читателей и у них могут произойти психические срывы) это просто не срабатывало. Сайт просто менял айпишники каждый день по мере того, как умаодан вносили адреса в черные списки.

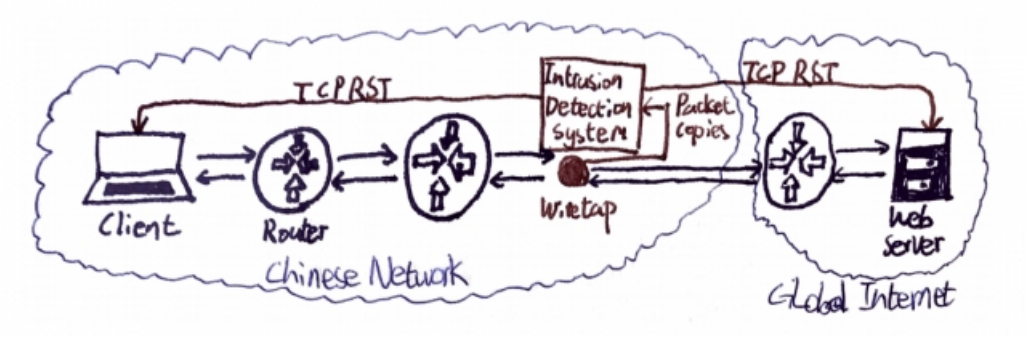
А во-вторых, когда все делается вручную, есть шанс что-то пропустить. Ну, например, все эти "атаки на ДНС", которые поразили Рунет в июне, китайцы прочувствовали еще в далеком 2008-ом году. Тот же Фалунь часто менял IP в записях DNS, а "офицеры информационной безопасности" тут же меняли блэк-листы. И в один прекрасный момент в черном списке оказался IP-адрес Массачусетского Технологического. И всё бы ничего, но как раз в этот момент проводилась какая-то важная встреча "на высшем уровне", где MIT должен был что-то там доказывать на уровне правительства и предоставил массу учебных курсов (MOOC) на китайском языке, получив от правительства Китая приличные деньги. А сайт оказался заблокированным.

Кроме того, блокировка по IP, даже когда никто не обращает внимания на коллатеральные потери в виде заблокированных целых кластеров сайтов у популярных хостеров, не самая надежная. Можно что-то пропустить по "альтернативным маршрутам". Что и произошло, опять-таки в 2008-ом, когда в Китае внезапно стал доступен YouTube по причине, что Google… просто поставил кучу Google-кэшей в Пакистане.

TCP Reset

Поскольку блокировка "по айпи" показала себя не самым лучшим образом, а также с ростом реал-тайм трафика UDP, китайские архитекторы "Стены" решили исправить систему "отправки запросов в ноль" добавлением блокировки входящих пакетов.

Для этого использовали схему, которую разрабатывали для корпоративного сегмента, а именно Intrusion Detection System. Вот так эта схема выглядит:



Суть работы такой схемы довольно простая: ключевым элементом является устройство "wiretap" - "прослушка". По сути, это обычный межсетевой экран, который направляет копии каждого пакетика на более интеллектуальную машинку IDS.

И вот уже IDS проверяет пакеты на легитимность. Если по каким-то признакам пакет не проходит, то клиенту, которому данный пакет направляется, шлется TCP Reset, то есть сброс соединения.

Поясню (для тех, кто прогуливал лекции по ПД): каждый TCP-пакет в рамках соединения несет заголовок. В каждом из них есть бит флага сброса (RST). У большинства пакетов этот бит установлен в 0 и ничего не значит, но если он установлен в 1, это значит, что получатель должен немедленно прекратить использовать данное соединение: не посылать пакетов с текущим идентификатором (на текущий порт), а также игнорировать все последующие пакеты этого соединения (согласно информации в их заголовках). По сути, сброс TCP моментально разрывает соединение.

Схема удобна тем, что если на каком-то из двух элементов системы происходит сбой, то соединение все же будет установлено. Все же приоритет в существовании "глобальной сети интернет" в том, чтоб-таки данные передавались. Но при работающей схеме пользование любым сетевым ресурсом, находящимся в "черном списке", будет очень затруднено, даже если IDS будет пропускать некоторые пакеты - сессии будут валиться, соединения прерываться.

Причем, у такой схемы есть более неприятные последствия - с некоторой долей вероятности клиент

может получить TCP Rst вообще по всем открытым в данный момент времени установленным соединениям, что несет еще и довольно неприятные воспитательные функции, когда пользователи начинают вообще опасаться каких-либо "неправильных ресурсов", поскольку связь может быть приостановлена не только в браузере, но и, например, во время мультимедийной сессии и/или телефонного разговора.

Исследования "Великой Китайской Интернет-стены" изнутри показывают, что фильтрация по похожим сценариям чаще происходит на уровнях вообще "Автономных Систем", а не на пограничных маршрутизаторах. Но не всегда. Поскольку данная схема требует огромного количества вычислительных ресурсов, то каждый пакетик из генерируемого сотнями миллионов абонентов трафика нужно проверить на кошерность.

Поэтому достаточно большое количество фильтрующих устройств класса IDS расположены в сетях на пограничных и опорных AS, которые подключаются к внешним сетям, так как они могут наиболее легко служить в качестве точек трафика.

Тут еще нужно оговориться, что частные и независимые провайдеры в Китае существуют. И довольно большие по европейским меркам. Ну, то есть, это не только China Telecom и China Mobile. Есть еще оператор, например, Unicom. Это "большая китайская тройка".

Но есть еще, например, оператор Great Wall Broadband Network Service Co., Ltd, который занимает нишу, схожую с российским Дом.ru. Строит сети по технологии Ethernet в крупных китайских городах на востоке и центральной части страны и имел на 2015 год 15 млн. абонентов. Штаб-квартира в Пекине. Сколько там, говорите, абонентов у "национального чемпиона"?



Существуют еще и сотни мелких провайдеров "регионального значения". И совсем какое-то огромное количество совсем мелких нишевых ИСП "одного здания". Причем, если вы бывали хоть раз на китайском, например, рынке, то можете представить эти "мелкие конторки". Они мелкие только по сравнению с гигантами класса China Telecom, а если поставить их рядом с российскими региональными операторами, то сравнивать будет даже не с чем.

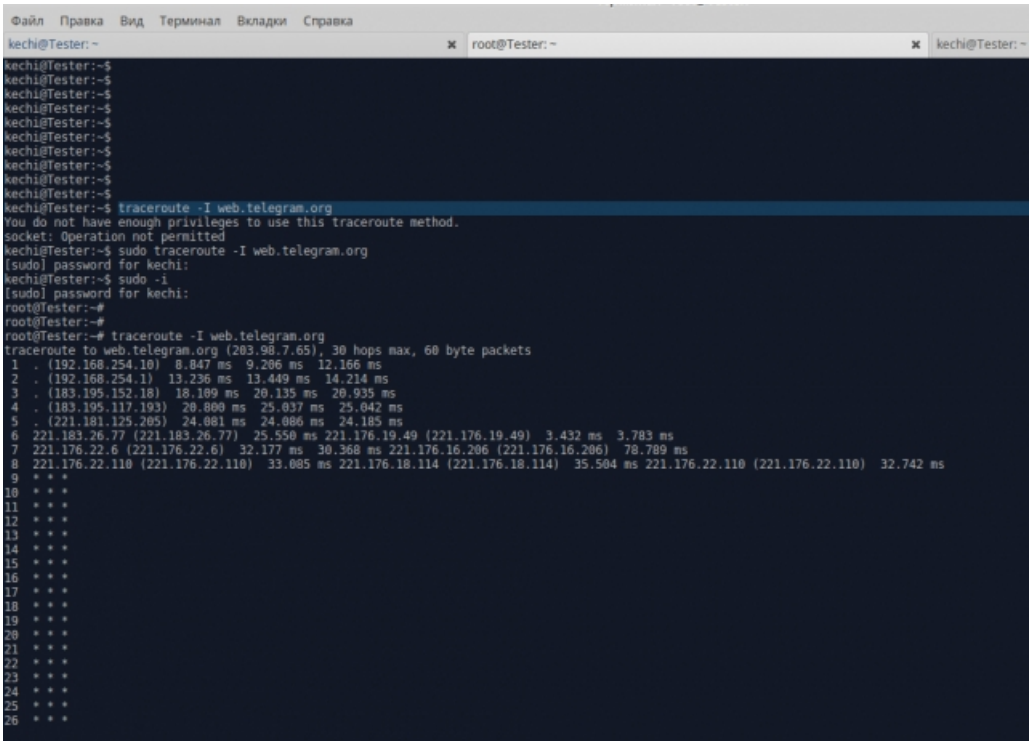
Поэтому и в схемах включения GFW имеются некоторые исключения. Вот те же два крупнейших китайских интернет-провайдера отличаются друг от друга подходами к построению цензуры. В частности, CNC Group (принадлежащая China Unicom) размещает большинство своих фильтров на магистрали. При этом ChinaNet (принадлежащая China Telecom), в силу колоссального объема всекитайского трафика, размещает фаерволлы в основном на собственных региональных сетях, которые имеют собственные "автономки".

Но, еще раз повторюсь, фильтры и все, что связано с цензурой, имеет место быть только и исключительно на сетях "большой китайской тройки". Тот же GWBN никаких фильтров у себя не устанавливает, но при этом с целью передачи трансграничного трафика имеет право подключаться только и исключительно к "тройке".

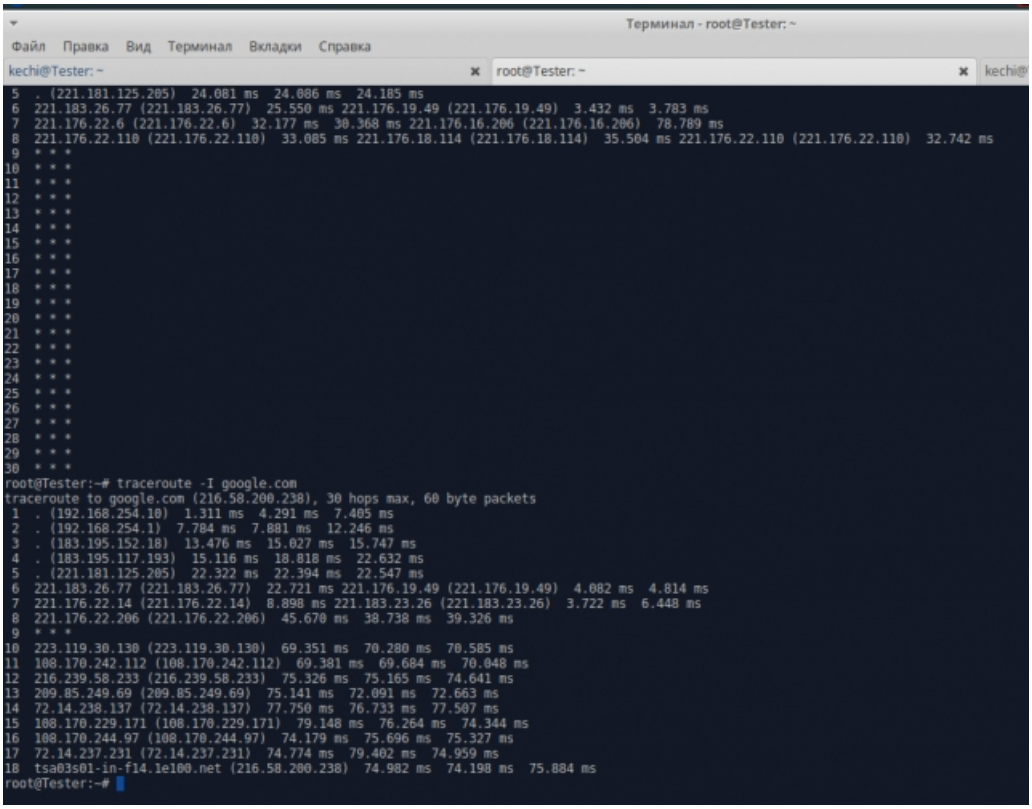
Что приводит к довольно интересным эффектам.

Вот буквально перед сдачей статьи в публикацию, один читатель телеграм-канала "ЗаТелеком" (подписывайтесь, кстати) прислал трейсы до разных заблокированных в Китае ресурсов.

До Телеграма путь выглядит так:



А до Google - так:



Почему так произошло?

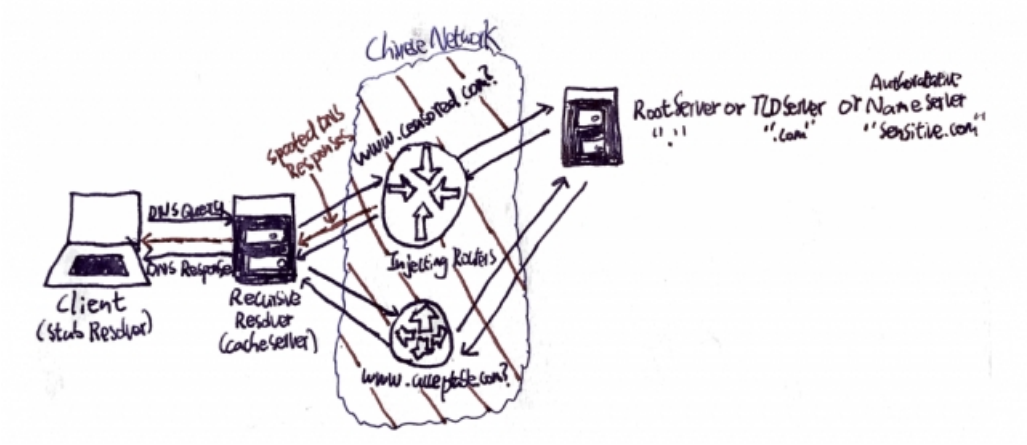
Поясняю. Сеть 183.194.0.0-183.195.255.255 принадлежит China Mobile в Шанхае. Именно там и находится инсайдер. Дальше пакеты улетают на бэкбон в Пекине, где и находится главный шлюз Чайна Мобайл из ЧайнаНет в глобальный интернет.

Только Телеграм в Китае блокирует по IP-адресам все автономки (да, у Телеграм есть собственная AS12301, базируется в Венгрии), а Google, очевидно, блокируется более хитрым способом с использованием IDS и прочего шаманства, потому что маршрут уходит на AS58453 (тоже China Mobile), а потом доходит до автономок Гугла, но со странными петлями в частных адресных пространствах.

При этом, ответ как бы приходит, но связи с Гуглом все же нет.

Блокировка по DNS

Очень похожая на "российскую цензуру" схема. Выглядит вот так:



Изменение записей A-типа в доменных именах не так уж и тривиально. Поэтому архитекторы "Великого Китайского Фаерволла" предусмотрели и такой тип блокировок. В сочетании с блокировкой IP-адресов, конечно.

В укрощении DNS используется фальсификация ответа, возвращаемого DNS-сервером, либо посредством преднамеренной конфигурации, либо буквально "отравления" DNS.

Блокируемый сервер может иметь любой IP-адрес, записанный в CNAME на корневых DNS-серверах, авторитетных для "всея Интернета". Но не в ChinaNet, где имеются собственные "корневые DNS".

В результате, при обращении пользователя, например, к подцензурному доменному имени twitter.com, пользователю выдаются ложные ответы. Чаще всего какие-нибудь опять не существующие, чтобы пользователь просто очень долго ждал ответа, но не дождался бы. Используемые вместе тактики "DNS-отравы" и "блокировка IP-адресов" позволяет довольно эффективно блокировать подцензурные сайты и серверы, как на уровне домена, так и на уровне IP.

При этом, "DNS-отрава" использовалось не только для блокировки контента, но и для продвижения "отечественного производителя". Например, в 2002 году при запросе google.cn пользователей редиректило на Baidu. Что сыграло довольно важную роль в продвижении главной поисковой системы Китая.

Но кроме тривиального вмешательства в DNS-записи, маршрутизаторы GFW еще умеют блокировать подцензурные запросы, подменяя DNS-запросы с запрещенными ключевыми словами, выдавая поддельные DNS-ответы.

Исследователи "с той стороны" обнаружили, что при запросах, которые входят в стоп-лист из примерно 15 тысяч слов, DNS на бордер-автономках делают инъекции поддельных DNS-ответов, что приводит к успешной блокировке интернет-ресурсов, даже если пользователи используют сторонние DNS-серверы за пределами страны. Это связано с тем, что умаодан тщательно просматривают IP-адреса DNS-резолверов в интернете и своевременно вносят любые подобные сервисы в блек-листы. При этом все "национальные DNS-серверы" тщательно и нежно правятся на предмет некошерных ресурсов.

Первые сообщения о DNS-инъекциях появились еще в 2002-ом году, когда выяснили, что практически все DNS-ответы подделываются и отравляются. В 2007 году DNS-отрава стала повсеместной, и появились фильтры по ключевым словам. При этом никто внутри не запрещает создавать кэширующие DNS-серверы, но корневым для кэша должен быть только "одобренный министерством общественной безопасности", из предложенного списка DNS-серверов.

Специфические детали устройства китайских DNS-отравителей можно почитать тут.

Разумеется, такая схема имеет побочные эффекты в виде коллатеральных потерь среди мирного населения. Но никто на это обычно не заморачивается - ну, заблокировали вместе с Твиттером (условно) еще пару тысяч сайтов, ну и что. Иногда случаются и факапы, как с упомянутым случаем с онлайн курсами от MIT. Но тогда вмешиваются ручным управлением, а пострадавшим ресурсам "настоятельно рекомендуют" сменить реквизиты доступа.

За процессом блокировок же следит целая армия как профессиональных военных сетевых инженеров, так и сотни тысячтрехрублевых идейных граждан.

Правда, иногда достается тем странам, которые имеют IP-транзиты через Китай. Но и это не беда, а проблемы тех стран, которые имеют IP-транзиты через Китай.

Тяжелее приходится блокировать ресурсы, которые используют DNSSec. Но поскольку пока эта технология не сильно-то и распространена (на клиентской части - а так-то все ОК), то решать эту проблему не спешат.

Точно также, как и проблему HTTPS.

Более сложные схемы цензуры

Материал получается слишком объемным, и многие уже устали вникать в подробности технической реализации китайской цензуры. Понимаю.

Но осталось совсем чуть-чуть.

Процессы блокировки с помощью DPI, на самом деле, мы уже описали в разделе TCP Reset. Это, собственно, и есть DPI в light-версии. Разумеется, никому и в голову не приходит молотить ВЕСЬ китайский трансграничный трафик. Это только Роскомнадзору может прийти в голову.

Все намного проще. Прослушки (упомянутые уже Wiretap’s) установлены на практически всех крупных бордерах автономных систем. Их задача - как раз слушать. Совсем не обязательно блокировать ВСЕ tcp-соединения 730 миллионов китайцев.

Достаточно доставить особо любопытным персонажам немного неприятностей, которые доставляются простым, но эффективным способом "сброса всех TCP-соединений", как только любопытный полезет куда-то не туда.

А как определить "не туда"?

Правильно. По ключевым словам. Тем более что иероглифический китайский язык позволяет делать это очень эффективно.

Существует специально разработанный список слов, на которые цербер IDS тут же сбросит вам соединения. Он большой, и, кстати, включает и английские слова - из ограниченного перечня, конечно.

Список есть не только у IDS, но и у крупнейших китайских ресурсов с юзер-генерейт контентом. У Байду, Сино, Тенсент и Вейбо. Кажется, я перечислил все крупнейшие китайские интернет-медиа конгломераты. А! Еще Алибаба, конечно.

Список, разумеется, секретный. Но пользователи сумели распознать часть этого словаря. А как иначе-то? После некоторых неудобств и банов начнешь понимать, что к чему.

Хочу сразу предупредить сотрудников Роскомнадзора и Минкомсвязи, которые, я уверен, прочитают эту статью, что в России такая схема работать не будет. И даже не потому, что "россияне - свободные люди и привыкли говорить прямо и открыто". Нет, дело в лингвистических различиях китайского и русского. Русский язык омофоничен не больше китайского, конечно. Но вот с омографией - в русском языке беда. Все эти "оскорблять", "шумахер" и прочие словообразования очень вредят цензуре. Почитайте обязательно Википедию про матерные слова.

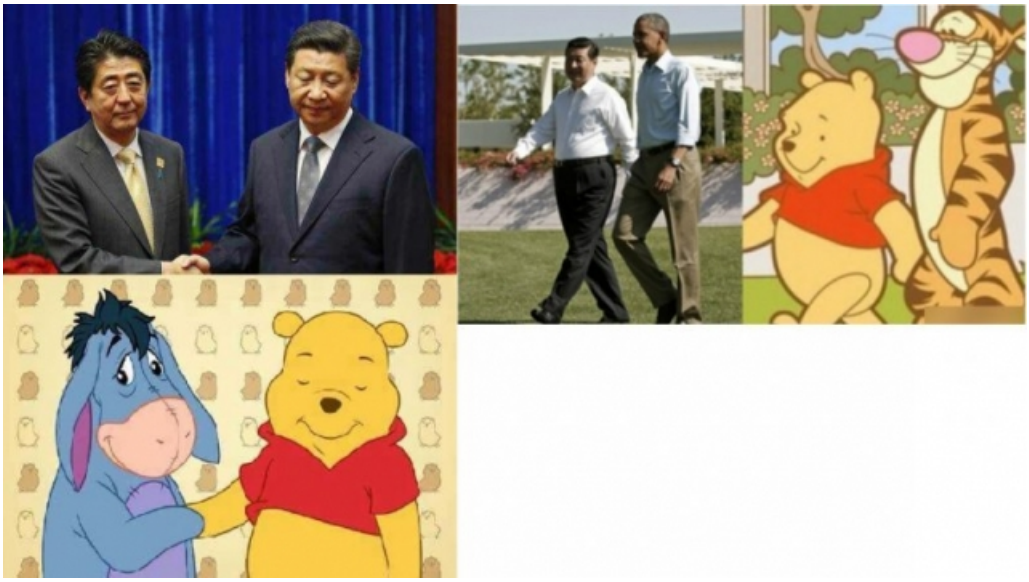
Там много имен собственных, связанных с политикой. Всяческие "Тяньаньмень", "Вэнь Цзябао" и тому подобное. Я не буду писать этих страшных слов, потому что, вдруг, прочитает кто-то из "китайских товарищей", да и заблокируют Наг.

Английских же слов не так много - это, прежде всего, porn, tits и boobs. Откуда становится понятным, почему китайские туристы, попадающие в страны со свободным интернетом, тут же скачивают гигабайты на флешки. Это мне в мобильных операторах рассказали - они сперва понять не могли, почему такой ажиотаж на трафик в первые дни у новоприбывших. Оказалось, что потом этими флешками просто торгуют уже внутри Поднебесной.

Ну, и вот из последних казусов, пожалуй, можно привести примеры:



Буквально на неделе, в Китае заблокировали Винни-Пуха.

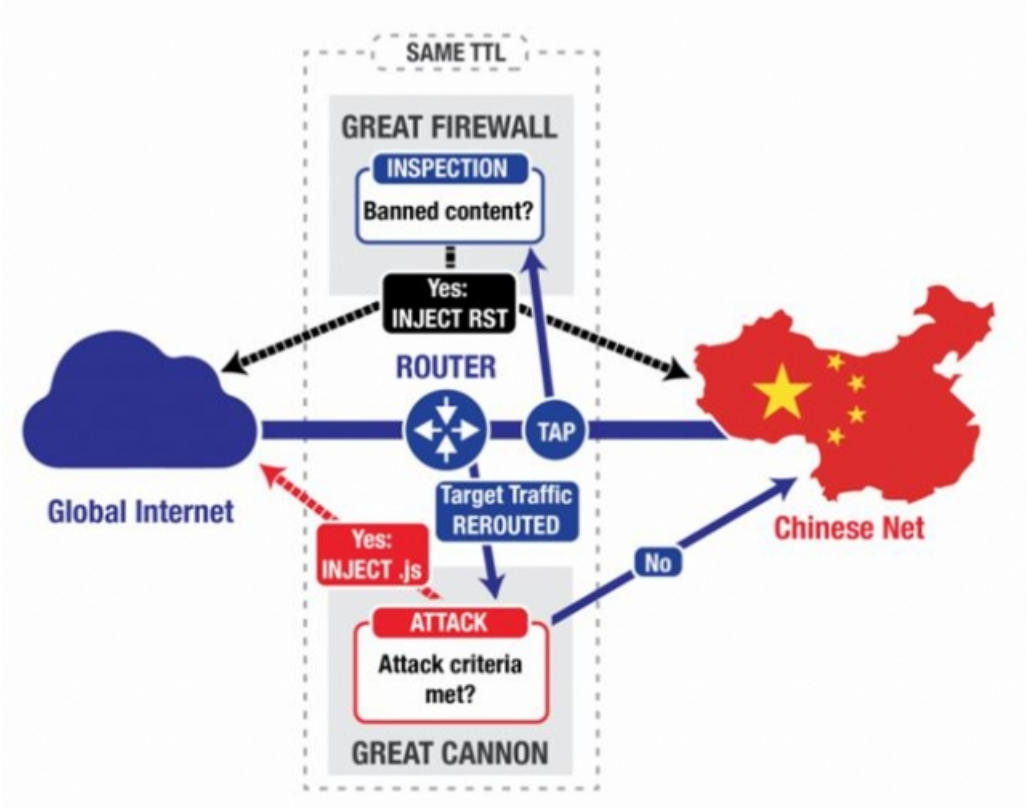


В общем-то, есть некоторое сходство, да.

Вот тут, в китайской Википедии есть очень неполный список этих страшных слов. Никогда их не пишите - потому что, если вы думаете, что китайская цензура может не только "защищать китайскую идентичность" пассивными фильтрами, но и вполне себе ударить.

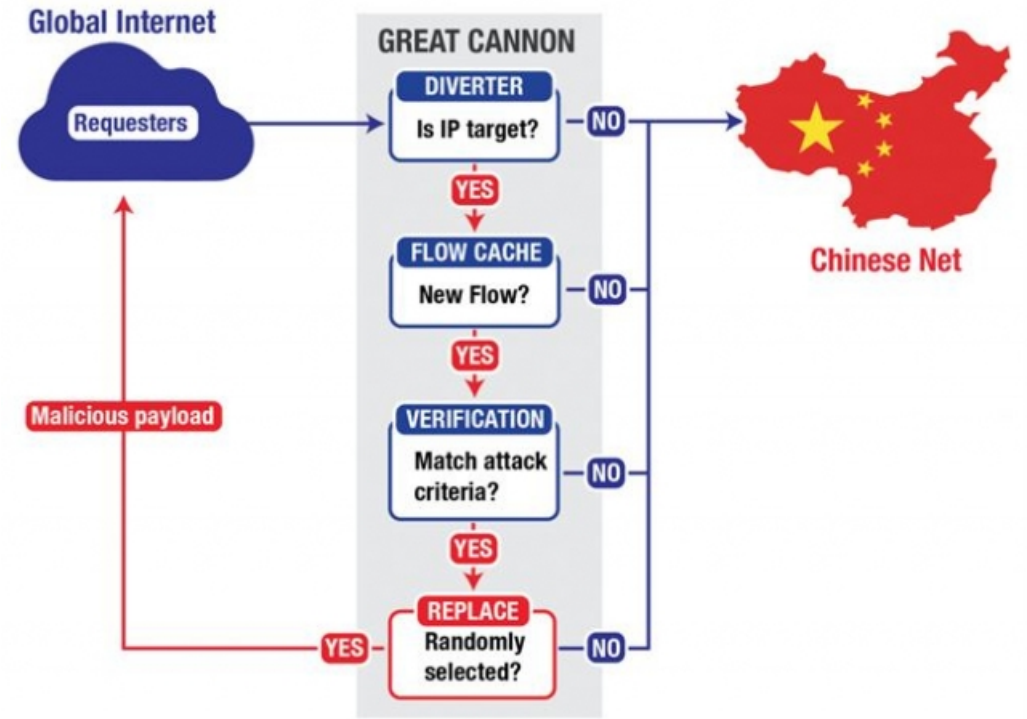
Напомню, что Сунь-Цзы - это самый первый в мире теоретик войны. И он - китайский. И он говорил, что "лучшая оборона - это нападение" (не уверен в корректности цитирования - самостоятельно гуглите).

Так вот. С недавнего времени, кроме "большой китайской интернет-стены" появилась не менее большая "китайская интернет-пушка". Низкоорбитальная.



Работает она так: если появляется некий интернет-ресурс, который не очень-то реагирует на сигналы китайской цензуры, при этом как бы еще всячески противодействует блокировкам (та же смена DNS или зеркала-домены) и/или полезен вообще для китайской общественности, то в него просто стреляют DDoS-атакой.

Просто, но эффективно. Существует целый алгоритм по выявлению цели и нацеливанию "пушки".



А собственно "стреляют" уже те самые миллионы китайских интернет-пользователей, причем, сами того не ведая. По команде "Огонь!" большинство китайских интернет-гигантов (Baidu в первую очередь) активируют небольшой JS-код на всех своих страницах, который и включает вполне себе легитимный запрос к атакуемому ресурсу. Но поскольку, я напомню, китайских пользователей сотни миллионов, то все они создают такой поток трафика, что положить под Deny of Service можно что угодно.

Другой вариант еще более коварен. У Baidu, как и у любого поискового сервиса есть собственная служба аналитики. То есть, счетчики, которые в виде обращения к JS-скрипту имплементируются на

странички большого количества сайтов. Добровольно. Так вот, если в ряде случаев (не всегда!) подменять JS-код счетчика на JS-код ботнета, то можно создать еще более страшный поток запросов к несчастному ресурсу.

Пока зафиксированы два случая реального применения этого оружия. Один раз против GitHub, где были выложены хорошие годные материалы по обходу GFW на прекрасном китайском языке, а также против ресурса greatfire.org, примерно схожей тематики.

Нужно отметить, что такие атаки могут продолжаться сколь угодно долго и с поддержкой на государственном уровне, и, напомню, при поддержке систем блокировки "обратного трафика" в виде IDS, что снижает ресурсоемкость таких атак в разы и позволяет не бояться "обратки".

Так что, если тот же Google попытается провернуть что-то подобное (вряд ли вероятность такого приближается к нулю), то "уронить" китайские ресурсы надолго вряд ли удастся - мусорные запросы будут заблокированы еще "на полете" на бордерах всех китайских автономок.

Вот так китайцы могут стрелять:

[Золотая цензура Китая, часть 2]