Современные угрозы в мире non-windows или как ломают IoT

Виктор Чебышев,

Ведущий исследователь безопасности Kaspersky

kaspersky

About

What?

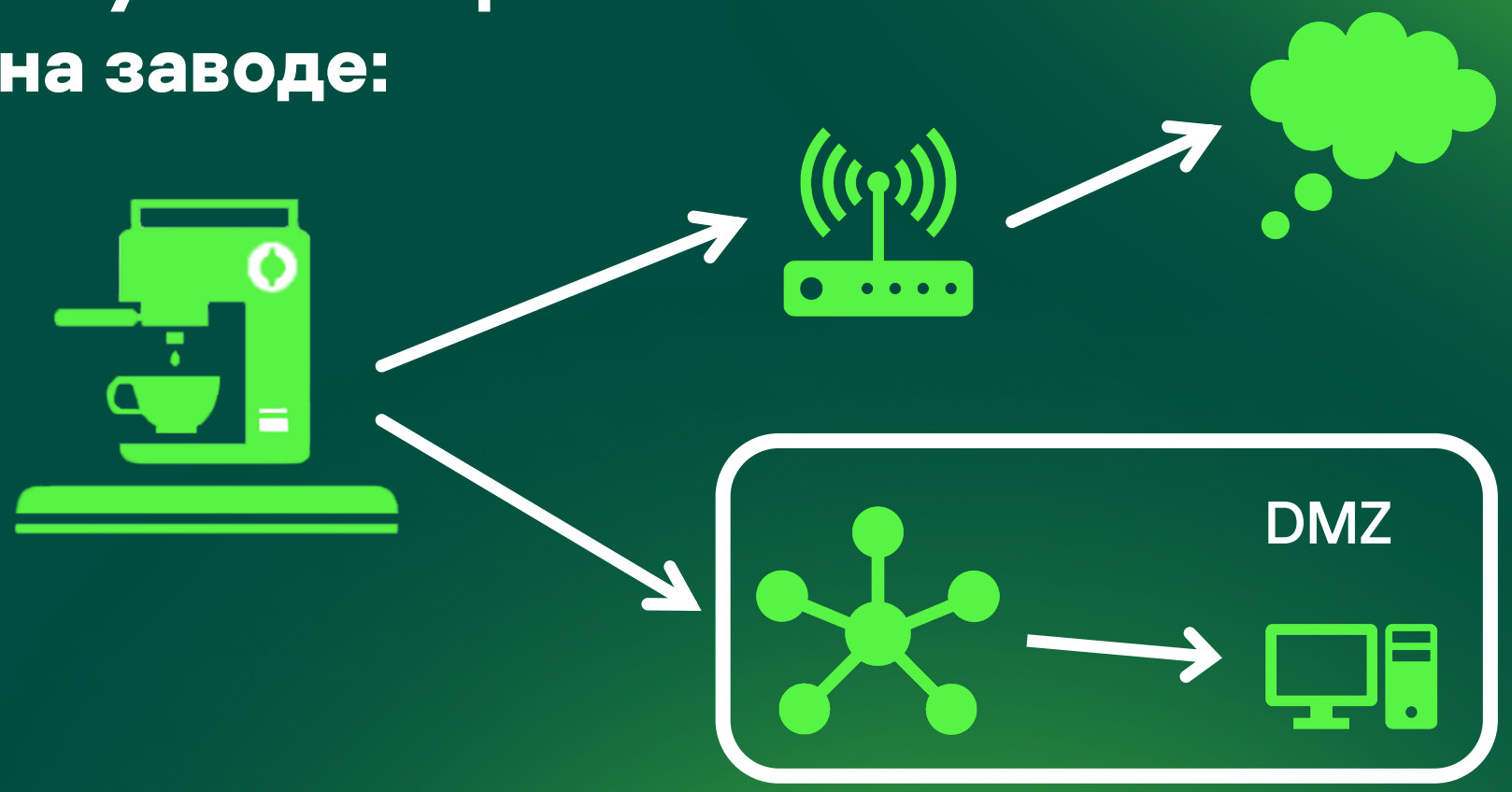
А что такое Internet of Things вообще?

What for?

Зачем атаковать кофеварку, чайник, камеру ?

- Вытянуть данные, кредитку, если есть
- Устроить DDOS, она же постоянно подключена
- Шпионить за ситуацией в сети, атаковать соседние устройства
- Устроить саботаж – поджечь устройство

Случай с кофемашиной на заводе:



Internet

Компьютеры предприятия

https://www.reddit.com/r/talesfromtechsupport/comments/6ovy0h/how_the_coffeemachine_took_down_a_factories/

Examples

Случай с пылесосом:

Оказалось, что у него WIFI с простым паролем

Кто угодно может аутентифицироваться и просматривать live видео и делать фото, кататься по помещению.

Случай с утюгом

Оказалось, что передаваемые данные между утюгом и инфраструктурой не зашифрованные

Нам удалось выключить утюг

Включение на данный момент не реализовано в коде

AV Ресивер

Оказалось что ресивером можно управлять через его WEB интерфейс

Можно вывести звук

Можно «задрать» громкость

What for?

Зачем атаковать умный автомобиль (connected car)?

Шпионаж

Терроризм

Кража личных вещей

Угон

Кейс с Nissan Leaf

```
GET https://[redacted].com/orchestration_1111/gdc/BatteryStatusRecordsRequest.php?
RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX&tz=Europe/Paris&TimeFrom=2014-09-
27T09:15:21
```

Достаточно было отправить запрос к серверам инфраструктуры Nissan после чего в машине стартовал кондиционер.

- Никакой авторизации
- Нужен только VIN

https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Кейс с Tesla

Возможности connected-car с каждым днём совершенствуются.

В погоне за маркетинговыми фишками разработчики ПО забывают про безопасность и человеческий фактор.

В данном случае авто позволяло уехать на нём без ключа.

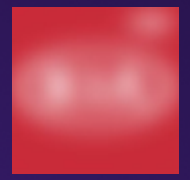
https://promon.co/blog/tesla-cars-can-be-stolen-by-hacking-the-app/

Кейсы с другими заводами автомобилей

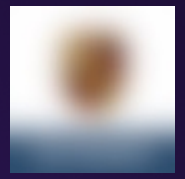
Миллионы людей используют возможности умных автомобилей

Installs
500,000 - 1,000,000

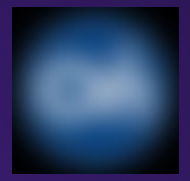
Installs
100,000 - 500,000



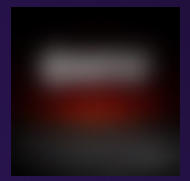
Installs
50,000 - 100,000



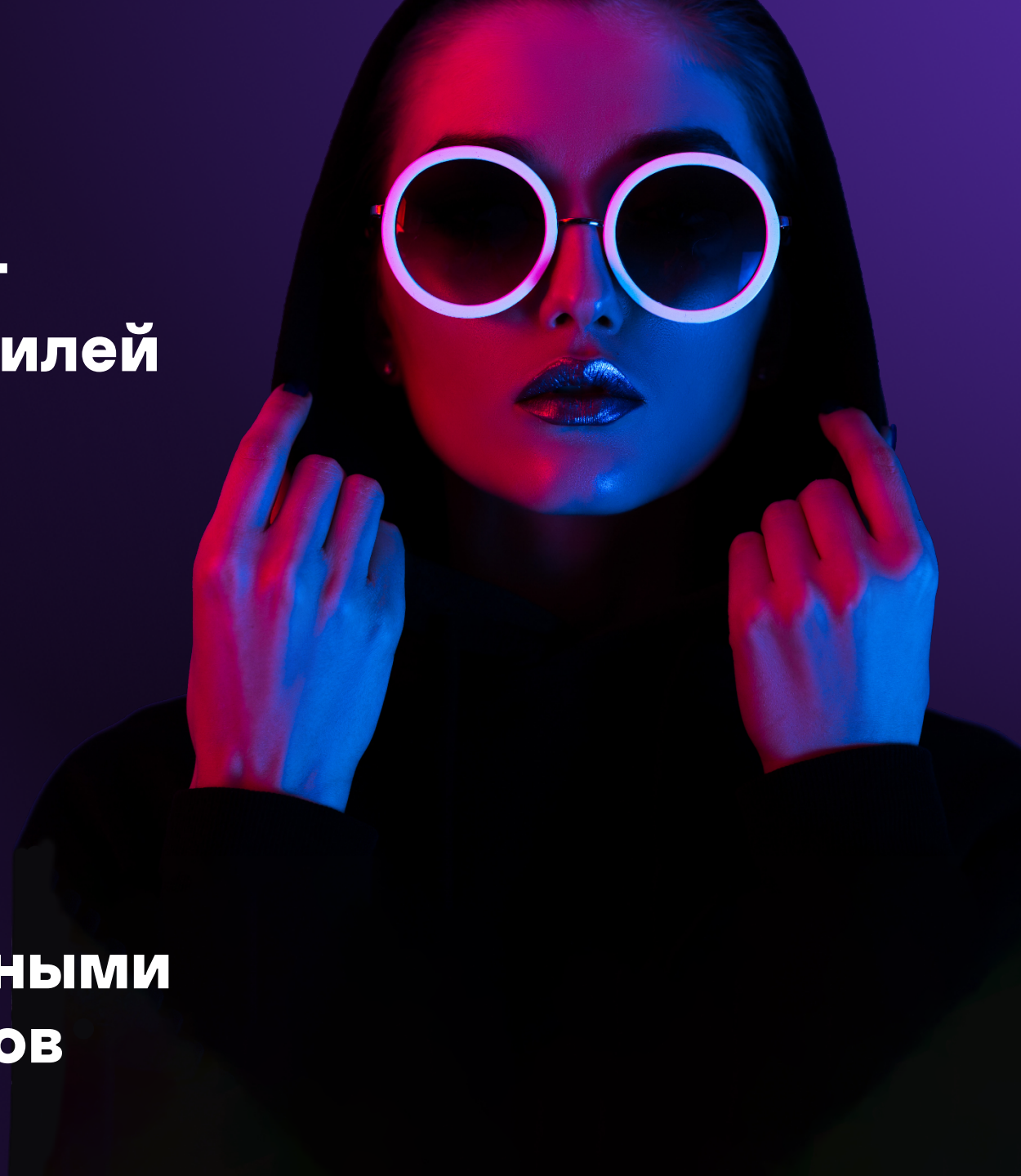
Installs
10,000 - 50,000



Installs
1,000,000 - 5,000,000



Installs
100,000 - 500,000



Все они являются потенциальными целями для киберпреступников

В большинстве приложений была возможность:

- Открыть двери
- Включить климатическую систему
- В некоторых был и запуск двигателя.

В darknet можно встретить объявления о покупке логинов и паролей от умных автомобилей.

Hello all users from [redacted].
I am looking for a [redacted] and [redacted] accounts
Paying around 200-300$ for this.
♥ I need
*USA
*All user data
*All pin numbers, Vins
*Only activated

[redacted] like this.

I've decided to start selling those awesome CRA accounts

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Refund policy.
no refund policy

Prices
- [redacted] 250$
- [redacted] 850$
- [redacted] 300$
- [redacted] 600$
- [redacted] 150$
- [redacted] 100$

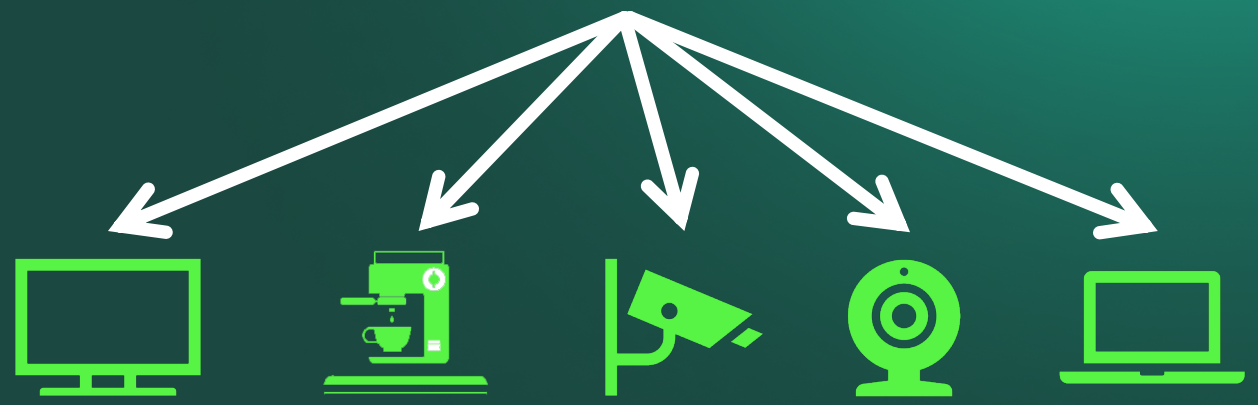
All in
Login:Password:Email:Vin:Pin

Attack vectors

Smart devices

Phon
e

Router



Что объединяет умный телевизор, умную кофеварку, умный пылесос?

IoT
Devices

Кейс с Mirai

Атака проводилась на устройства с заводским, несброшенным паролем.

Более 500 000 устройств по всему миру могут быть уязвимы

Атака с помощью бот сети на Dyn DNS сделала недоступными крупные WEB ресурсы

Мощность DDOS атаки с помощью Mirai была 620 Гбит/с

admin/123456	ACTi IP Camera
root/anko	ANKO Products DVR
root/pass	Axis IP Camera, et. al
root/vizxv	Dahua Camera
root/888888	Dahua DVR
root/666666	Dahua DVR
root/7ujMko0vizxv	Dahua IP Camera
root/7ujMko0admin	Dahua IP Camera
666666/666666	Dahua IP Camera
root/dreambox	Dreambox TV receiver
root/zlxx	EV ZLX Two-way Speaker?
root/juantech	Guangzhou Juan Optical
root/xc3511	H.264 - Chinese DVR
root/hi3518	HiSilicon IP Camera
root/klv123	HiSilicon IP Camera
root/klv1234	HiSilicon IP Camera
root/jvbzd	HiSilicon IP Camera
root/admin	IPX-DDK Network Camera

Симптомы

1) Снижение скорости Internet
2) Блокировка оператором канала в целом

Лечение

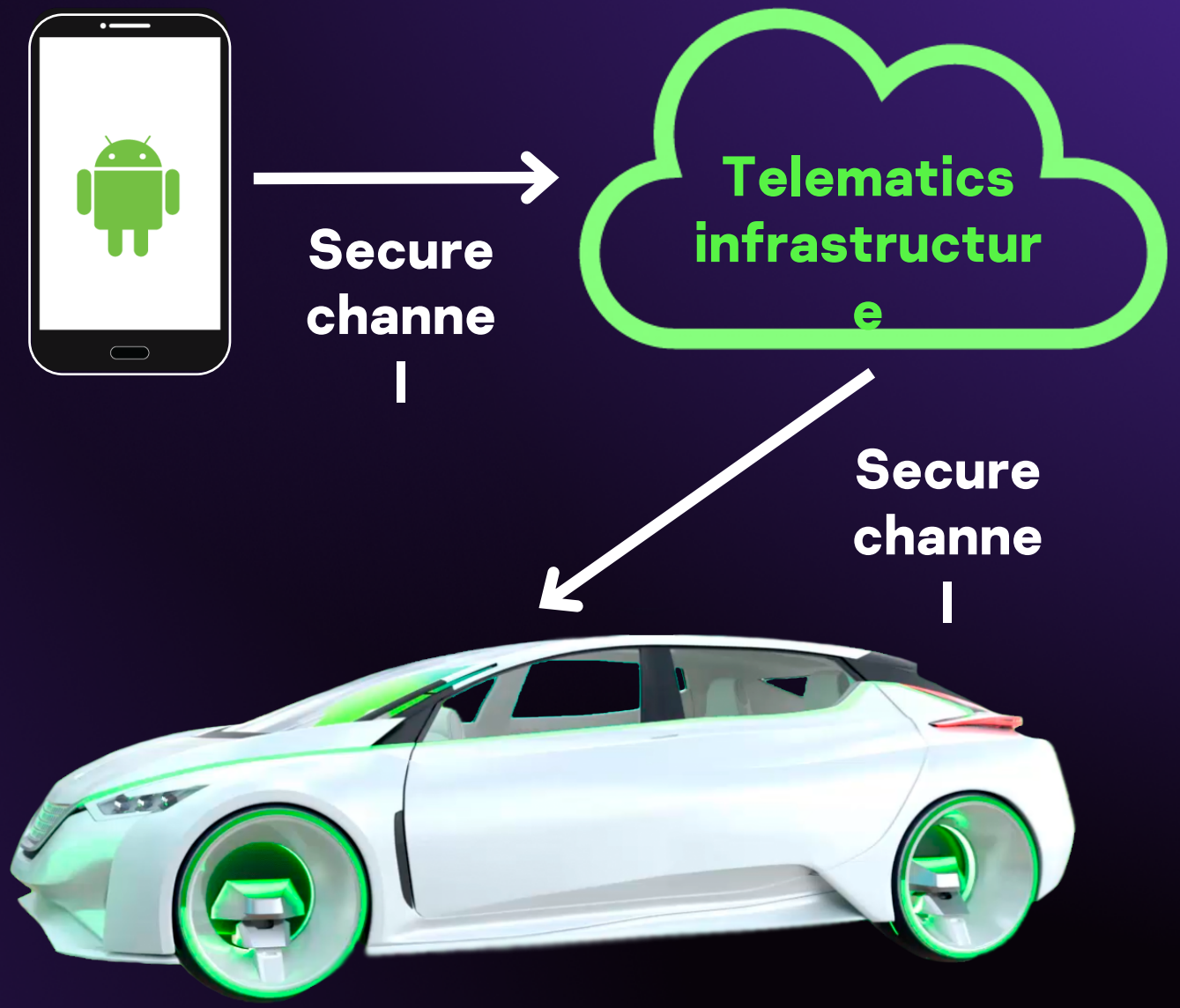
1) Перезагрузка
2) Обновление (если нет обновлений возможно есть сторонние прошивки dd-wrt/open wrt например)

Обновление нужно производить оперативно, следующая успешная атака может случится через 90 секунд.

Cars

Инфраструктура connected-car

Как в случае с инфраструктурой, так и в случае мобильного телефона, атаки одинаково успешны.



Через мобильное устройство

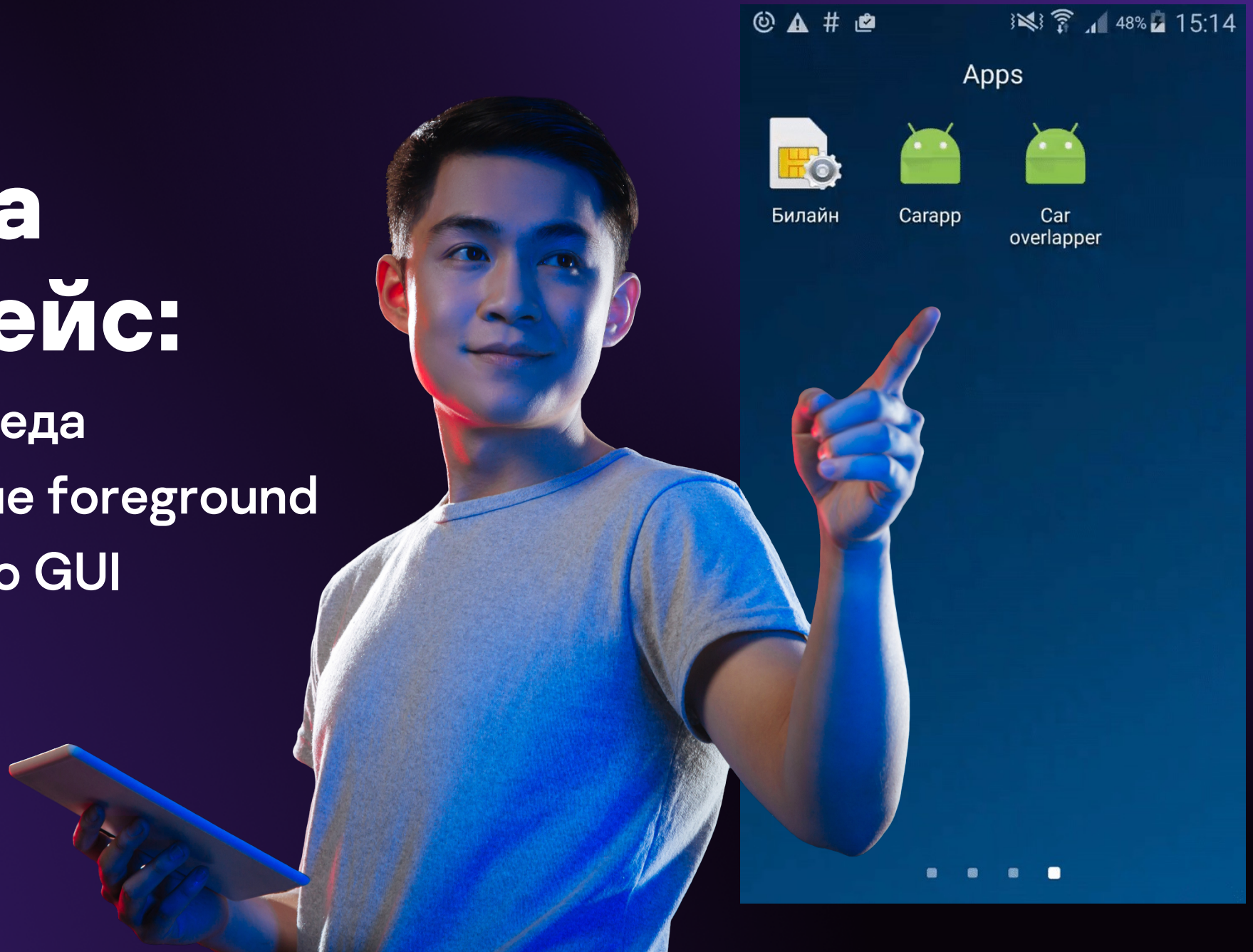
В идеальном мире на мобильное устройство без ведома пользователя:

1) Нельзя обратится к защищённым хранилищами других приложений
2) Нельзя ничего скачать
3) Нельзя ничего установить
4) Нельзя ничего запустить

Но с root правами все эти действия выполнить очень легко

Атака на интерфейс:

1) Запуск зловреда
2) Отслеживание foreground
3) Запуск своего GUI



Атака на локальные данные приложения

credentials.xml

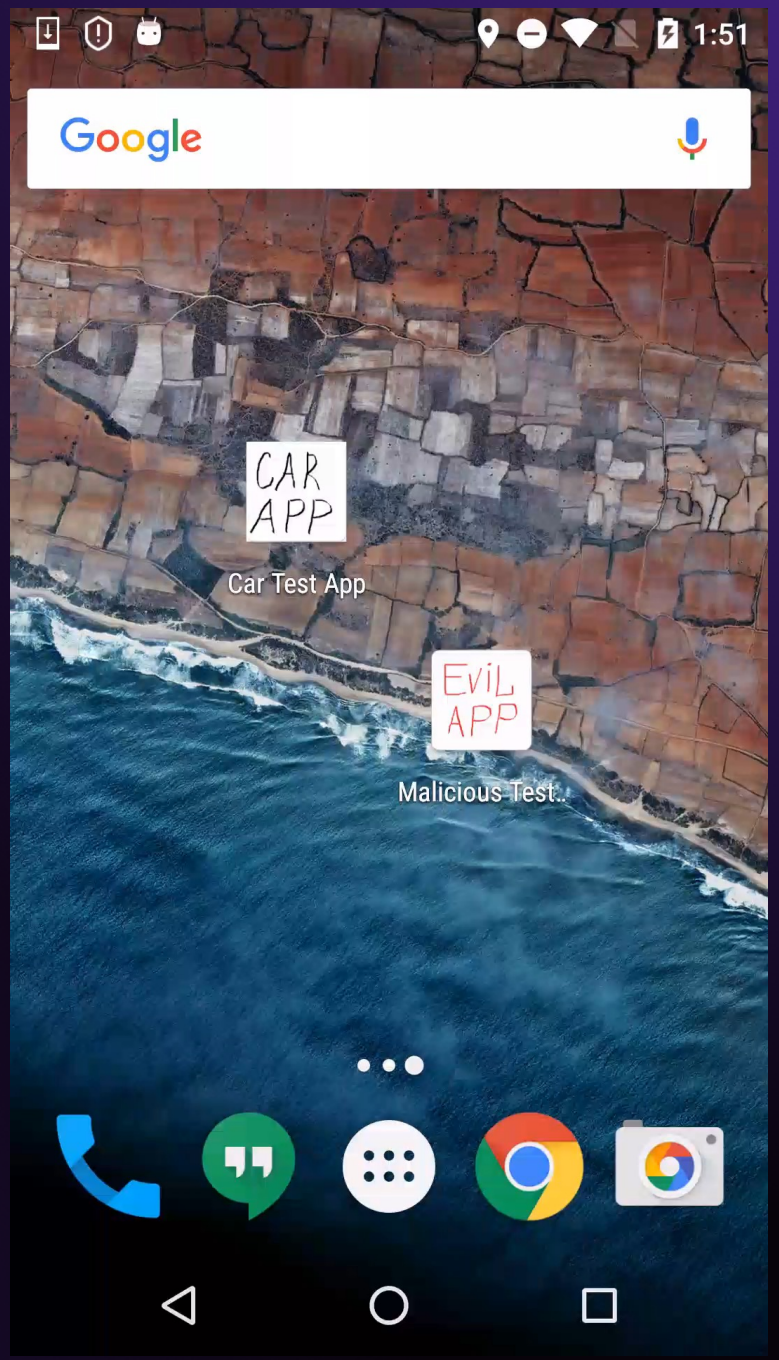
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="pref.userstore.msgflag" value="0" />
    <int name="pref.userstore.group" value="7" />
    <string name="pref.userstore.pincode">703356</string>
    <string name="dcsauthkey">[redacted]</string>
    <string name="pref.userstore.measurement">Imperial</string>
    <string name="pwd">[redacted]</string>
    <int name="pref.userstore.usercode" value="845866" />
    <string name="user_first_name">Ben</string>
    <string name="dcssessid">2[redacted]</string>
    <string name="pref.userstore.language">English</string>
    <string name="pref.userstore.lastname">[redacted]</string>
    <string name="sessionid">[redacted]</string>
    <string name="pref.userstore.accountid">315324</string>
    <string name="username">[redacted]ru</string>
    <string name="pref.userstore.accountname">[redacted]@mail.ru</string>
    <string name="pref.userstore.email">[redacted]@mail.ru</string>
    <string name="user_last_name">[redacted]</string>
    <long name="pref.userstore.id" value="579509" />
    <string name="pref.userstore.username">[redacted] ru</string>
    <string name="pref.userstore.firstname">[redacted]string>
    <string name="pref.userstore.timezone"></string>
    <string name="pref.userstore.phone"></string>
</map>
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="USERNAME">[redacted]</string>
    <boolean name="VERIFIED" value="true" />
    <boolean name="CRMExportDone" value="true" />
    <string name="HOME_COUNTRY_ISO_CODE">GB</string>
    <string name="LastName">Rojers</string>
    <string name="PASSWORD">[redacted]</string>
    <string name="TOKENID">i6rq/YyUexko9K4j/MqDgbCW8k0EDzrqBJEHZGHV
sG+vTPWDQ4lxCDf1McDHRQMZG6CiQ/4VcVUePHdse7+RSMkKsNEgy1f8Mtkdce5s0ZD
uilSh0=</string>
    <boolean name="PrivacyWarningShown" value="true" />
    <string name="PASSWORDHASH_">WwJheOfI0r5rIrEiFQEFpSglIUiTILjYT9
    <string name="MSGTOKENID">dS0cCR0eO3Ee2nTmA12EcO/ho7NjvRZij/Q8Y
    <string name="FirstName">Ben</string>
    <boolean name="PASSWORD_POLICY_CONFORM" value="true" />
    <long name="LAST_SYNC" value="1467120065944" />
    <string name="USERID">W242860260</string>
    <int name="currentDashboardPage" value="1" />
</map>
```

DEMO

Атака на локальные данные

1) Запуск чистого приложения
2) Ввод данных и сохранение в локальное хранилище
3) Перехват данных зловредом



В случае с приложением для автомобиля

- Мы декомпилировали
- Изменили код
- Собрали заново
- Оно запустилось

```
private void loginWithCredentials() {
    String v0 = this.mUsernameView.getText().toString();
    String v1 = this.mPasswordView.getText().toString();
    Toast.makeText(this.getApplicationContext(), v0 + v1, 0).show();
    this.performLogin(v0, v1);
}
```

Не было контроля целостности

```
label_49:
    AppTracking.trackActionStarted("login");
    String v2 = this.userName;
    String v3 = this.password;
    Toast.makeText(this.getApplicationContext(), v2 + v3, 0).show();
    this.runInBackground(new LoginTask(((BaseActivity)this), v2, v3, this.permanentState));
}
```

Conclusions

Всё плохо

- Нет стандартов безопасности при разработке IoT устройств
- За устройствами не следят, не выпускают прошивок, не обновляют
- Для совершения атаки порой не нужны сверх познания, всё на поверхности
- Тем не менее всё больше и больше разных устройств, которые упрощают нашу жизнь

Будьте внимательными к окружающим Вас гаджетам.

MAY THE FORCE BE WITH YOU

Вопросы?

kaspersky