



Обзор угроз для мобильных приложений и платформ.

Как удобно и мобильно потерять деньги, важную информацию и настроение.

О чём говорить не будем?

152-ФЗ

161-ФЗ

382-П

СТОБР

ФСТЭК-31

ISO/IEC 2700x

ISO/IEC 15408

ISO/IEC 17799

...

Грустные новости



Knock, Knock, Neo, The Matrix has pwned you

Photo by Sam Taylor-Wood

Evernote и Sony сдаёт «своих»;

Твиттеры первых лиц взламываются

Google docs и NTP-серверы используются для DDoS-атак;

OpenSSL «кровоточит» ([CVE-2014-0160](#));



Карты банков и реквизиты доступа к ДБО регулярно компрометируются,

Базы почтовиков бродят по сети

Telegram уязвим!



OWASP TOP-10:



- Внедрение кода
- Некорректная аутентификация и управление сессией
- Межсайтовый скриптинг (XSS)
- Небезопасные прямые ссылки на объекты
- Небезопасная конфигурация
- Утечка чувствительных данных
- Отсутствие контроля доступа к функциональному уровню
- Подделка межсайтовых запросов (CSRF)
- Использование компонентов с известными уязвимостями
- Невалидированные редиректы

Смартфонам чуть более 5 лет и мы о них мало что знаем



Do you know about Cole Wilson?

“Deadman” by Jim Jarmush

От кого: Leonid [REDACTED] <leo@[REDACTED].ru>

Дата: 26 марта 2014 г., 12:02

Тема: Re: документы по [REDACTED]

Кому: Dmitriy [REDACTED] @group-ib.ru>

Копия: Алексей [REDACTED], Evgeny [REDACTED], Александр [REDACTED]
[REDACTED], Алексей [REDACTED]

Добрый день!

Вчера запустили приложение на Android со встроенными покупками (журнал, подписка):

[https://play.google.com/store/apps/details?id=\[REDACTED\]for_android.mag](https://play.google.com/store/apps/details?id=[REDACTED]for_android.mag)

Сломали сразу же:

[http://joxi.ru/FogyU_3JTJAa\[REDACTED\]NkM](http://joxi.ru/FogyU_3JTJAa[REDACTED]NkM)

Ссылка на пост:

[http://vk.com/\[REDACTED\]?w=wall-387766_6328528](http://vk.com/[REDACTED]?w=wall-387766_6328528)

Вопрос Дмитрию, есть опыт борьбы с такими вещами, что можно сделать?



Максим Алисейко

Иван, да. Все замечательно ломается

час назад Ивану | Ответить



Иван Хромов

Максим, и скачивается?

час назад Максиму | Ответить



Максим Алисейко

Иван, как видишь



час назад Ивану | Ответить

Top 10 Mobile Risks (OWASP*):

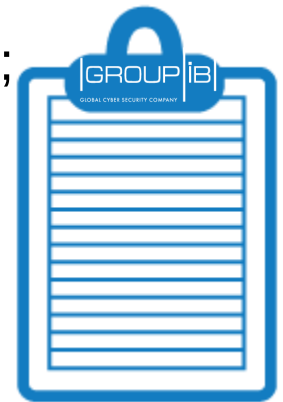
- Недостаточно защищенная серверная часть приложения;
- небезопасное хранение данных;
- Недостаточная защита данных при передаче;
- Непреднамеренная утечка данных
- Недостаточная авторизация и аутентификация
- Уязвимая реализация шифрования;
- Инъекции на клиентской стороне;
- Получение данных от недоверенных процессов;
- Неверная обработка сессии;
- Отсутствие защиты исполняемого кода.



*https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

Group-IB TOP 10++

- Отсутствие обфускации кода;
- Недостаточная проверка доверенности среды;
- Некорректная работа с системными логами и кешем;
- Отсутствие контроля перекрытия экрана;
- Отсутствие техник пиннинга сертификатов;
- «Бессмертные» сессии;
- Предсказуемые идентификаторы;
- Некорректная работа со скриншотами (iOS);
- Пренебрежение шифрованием;
- Некорректное удаление информации;
- Утечки через дополнительные аппаратные средства;
- Итд.

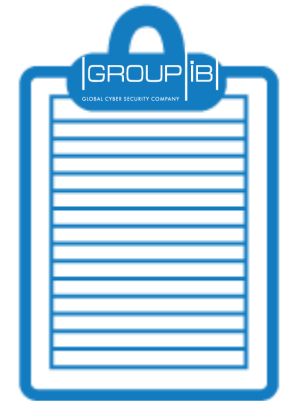


Group-IB TOP 10++

- Отсутствие обфускации кода

```
protected void onResponse(int tag, JsonElement response) {
    int v7 = 2131492888; // R.string.alert_info
    int v6 = 2130837675; // R.drawable.ic_dialog_info
    int v5 = 170393370;
    Object v0 = this.gson.fromJson(response, GSONPaymentCheck.class);
    StringBuilder v1 = new StringBuilder();
    v1.append(((GSONPaymentCheck)v0).response).append("\n");
    if(((GSONPaymentCheck)v0).response.equals("Абонент найден")) {
        v1.append("Подтвердить?").append("");
        new AlertDialog$Builder(this.getActivity()).setMessage(v1.toString()).setCancelable(false)
            .setIcon(v6).setTitle(v7).setPositiveButton(v5, new DialogInterface$OnClickListener() {
                public void onClick(DialogInterface dialog, int whichButton) {
                    dialog.dismiss();
                    if(!PaymentFragment.this.cbSave.isChecked()) {
                        PaymentFragment.this.requestJSON(0, 0, HTTPGETCreator.paymentConfirm(PaymentFragment
                            .this.service.getId(), PaymentFragment.this.ids, PaymentFragment.this
                                .params, PaymentFragment.this.accFrom.getId(), PaymentFragment.this
                                    .amount, PaymentFragment.this.cbSave.isChecked(), PaymentFragment.this
                                        .etTemplateName.getText().toString()));
                    }
                    else {
                        PaymentFragment.this.requestJSON(0, 0, HTTPGETCreator.paymentConfirm(PaymentFragment
                            .this.service.getId(), PaymentFragment.this.ids, PaymentFragment.this
                                .params, PaymentFragment.this.accFrom.getId(), PaymentFragment.this
                                    .amount, PaymentFragment.this.cbSave.isChecked(), PaymentFragment.this
                                        .etTemplateName.getText().toString()));
                    }
                }
            }).setNegativeButton(170393369, new DialogInterface$OnClickListener() {
                public void onClick(DialogInterface dialog, int whichButton) {
                }
            }).create().show();
    }
}
```

```
LocalizationDataSource
├─ fragment
│   └─ account
│       ├── AccountDetailsFragment
│       ├── AccountListFragment
│       ├── AccountSettingsFragment
│       ├── AccountStatementFragment
│       └── LoanScheduleFragment
├─ atm
│   ├── ATMinListFragment
│   ├── ATMOnMapFragment
│   └── ListAndMapFragment
├─ payment
│   ├── PaymentConfirmationFragment
│   ├── PaymentFragment
│   ├── PaymentHistoryFragment
│   ├── PaymentHistoryListFragment
│   ├── PaymentListFragment
│   ├── PaymentTemplateFragment
│   ├── PaymentsTabFragment
│   ├── ServiceListFragment
│   └── TemplateListFragment
├─ template
│   ├── HistoryTransaction
│   └── TemplateFragment
└─ transfer
    ├── Transfer2BAFragment
    ├── Transfer2OtherBankFragment
    ├── TransferAccountsFragment
    ├── TransferHistoryFragment
    ├── TransferHistoryListFragment
    ├── TransferInsideBankFragment
    ├── TransferListFragment
    ├── TransferTemplateFragment
    ├── TransferTemplateListFragment
    └── TransfersTabFragment
```



Исходный код легко читается, имена функций показывают их функционал прозрачно даже для неподготовленного пользователя.

Group-IB TOP 10++

- Наличие обфускации кода

```

private HttpURLConnection b0429m0429m0429m() throws Exception {
    HttpURLConnection v0_3;
    label_2:
    switch(1) {
        case 0: {
            goto label_2;
        }
        case 1: {
            break;
        }
        default: {
            label_3:
            switch(0) {
                case 0: {
                    goto label_5;
                }
                case 1: {
                    goto label_5;
                }
                default: {
                    goto label_5;
                }
            }
        }
    }
    label_5:
    switch(0) {
        case 0: {
            goto label_8;
        }
        case 1: {
            goto label_5;
        }
    }
    while(true) {
        switch(0) {
            case 0: {
                goto label_8;
            }
        }
    }
}

```

```

while(true) {
    switch(1) {
        case 0: {
            goto label_51;
        }
        case 1: {
            goto label_54;
        }
    }
}

label_54:
this.ba04300430aa04300430(arg8.b0436043604360436m(mmmmp.a0436043604360436m(v0, v1, v6)));
this.ba0430a0430a04300430(arg8.b0436043604360436m(mmmmp.mb_string_decrypt("e8888888888888888888888888888888",
    '1', '8', '\u0000')));
this.baaaa043004300430(arg8.b043604360436m(mmmmp.a0436043604360436m("e8888888888888888888888888888888",
    '8', '\u0000')));
this.b0430aaa043004300430(arg8.b043604360436m(mmmmp.a0436043604360436m("e8888888888888888888888888888888",
    'U', '\u0000')));
}

public void b0417041755504175(String arg4) {
    label_2:
    switch(0) {
        case 0: {
            goto label_5;
        }
        case 1: {
            goto label_5;
        }
        default: {
            goto label_5;
        }
    }
    label_5:
    switch(1) {
        case 0: {
            goto label_2;
        }
        case 1: {
            goto label_5;
        }
        default: {
            goto label_3;
        }
    }
}

```

Имена функций и строки
шифрованы, добавлены
пустые переходы, код
«отравлен» и его изучение
осложнено даже для
профессионального аудитора

Group-IB TOP 10++

- Недостаточная проверка доверенности среды;

```
public static boolean findBinary(String binaryName) {
    boolean v1 = false;
    if(0 == 0) {
        String[] v0 = new String[]{"/sbin/", "/system/bin/", "/system/xbin/", "/data/local/xbin/",
            "/data/local/bin/", "/system/sd/xbin/", "/system/bin/failsafe/", "/data/local/"};
        int v3 = v0.length;
        int v2 = 0;
        while(v2 < v3) {
            if(new File(v0[v2] + binaryName).exists()) {
                v1 = true;
            }
            else {
                ++v2;
                continue;
            }
        }
        return v1;
    }
}

return v1;
}

private static boolean isRooted() {
    return Splash.findBinary("su");
}

public void onCreate(Bundle savedInstanceState) {
    long v2 = 5000;
    // ...
    float v4 = 10f;
    super.onCreate(savedInstanceState);
    this.showActionBar();
    this.setContentView(2130903063);
    FragmentTransaction v7 = this.getSupportFragmentManager().beginTransaction();
    v7.add(2131361882, new MainFragment());
    v7.commit();
    if(Splash.isRooted()) {
        this.alertbox("", "");
    }
}
```

Наличие root-прав проверяется
всего одним способом.
Этого мало



- Недостаточная проверка доверенности среды;



14

Group-IB TOP 10++

- Некорректная работа с системными логами и кешем;

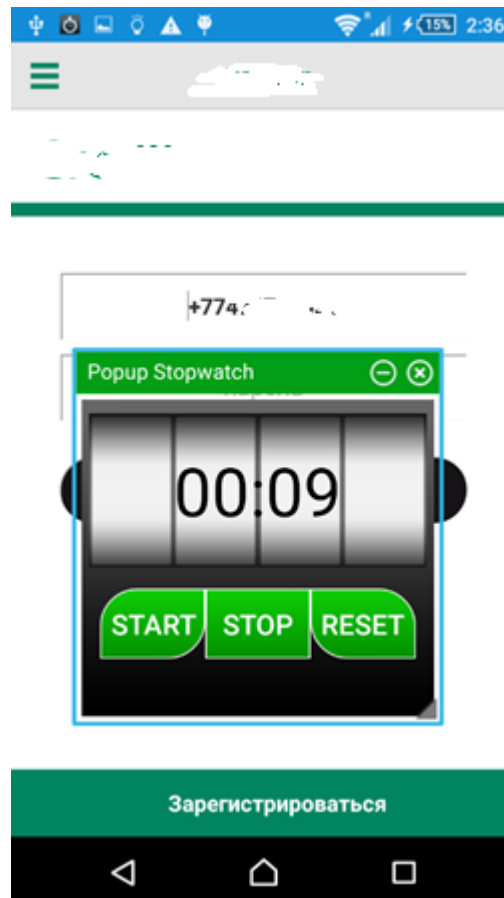
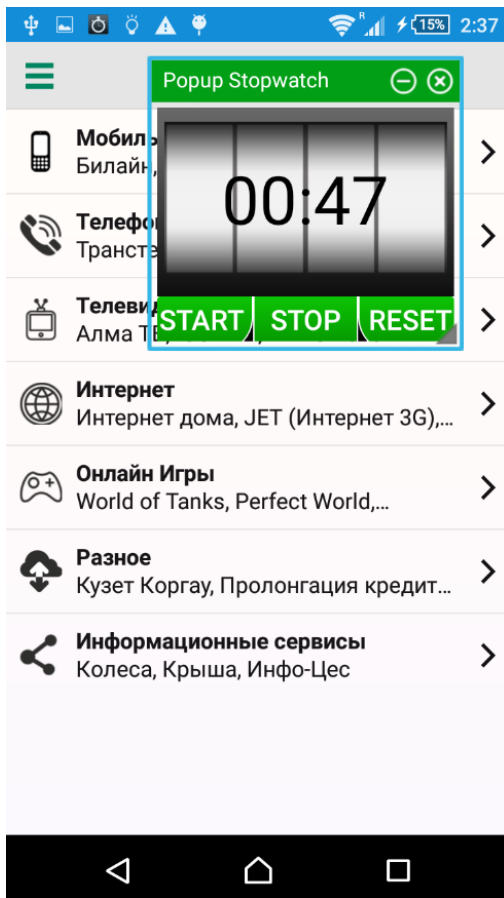
```
View - logcat.txt
File Edit View Help
2014-12-17 17:43:38.246 I 31930/System.out: 3 +7[ 2]715-
2014-12-17 17:43:38.246 I 31930/System.out: 3 3
2014-12-17 17:43:38.246 I 31930/System.out: 3 +7[ 2]715-
2014-12-17 17:43:38.246 I 31930/System.out: 12 12
2014-12-17 17:43:38.246 I 31930/System.out: 12 +7[ 2]715-
2014-12-17 17:43:39.277 E 1885/wpa_supplicant: RX ctrl_iface - hexdump
2014-12-17 17:43:39.277 E 1885/wpa_supplicant: 3 49 4: fe 41 4c 5f
2014-12-17 17:43:39.277 D 1885/wpa_supplicant: Command received: SIG
2014-12-17 17:43:39.277 D 1885/wpa_supplicant: nl 211: si vey data m
2014-12-17 17:43:40.568 D 2110/dalvikvm: GC_FOR_LLLOC freed 710K, 1
2014-12-17 17:43:40.628 I 31930/System.out: 0 0
2014-12-17 17:43:40.628 I 31930/System.out: 3 0
2014-12-17 17:43:40.628 I 31930/System.out: 3 +7[7 715-3
2014-12-17 17:43:40.628 I 31930/System.out: 3 3
2014-12-17 17:43:40.628 I 31930/System.out: 3 +7[70 715-3
2014-12-17 17:43:40.628 I 31930/System.out: 13 13
2014-12-17 17:43:40.628 I 31930/System.out: 13 +7[7 715- |
2014-12-17 17:43:40.628 I 31930/System.out: 14 14
2014-12-17 17:43:40.628 I 31930/System.out: 14 +7[7 715- |
2014-12-17 17:43:40.748 D 2110/dalvikvm: GC_FOR_LLLOC freed 715K, 1
2014-12-17 17:43:40.858 I 31930/System.out: 0 0
2014-12-17 17:43:40.858 I 31930/System.out: 3 0
2014-12-17 17:43:40.858 I 31930/System.out: 3 +7[7 715-31 |
2014-12-17 17:43:40.869 I 31930/System.out: 3 3
2014-12-17 17:43:40.869 I 31930/System.out: 3 +7[7 715-31
2014-12-17 17:43:40.869 I 31930/System.out: 15 15
2014-12-17 17:43:40.869 I 31930/System.out: 15 +7[ 2]715-3 1
2014-12-17 17:43:41.049 D 2110/dalvikvm: GC_FOR_LLLOC freed 710K, 1
2014-12-17 17:43:41.129 I 31930/System.out: 0 0
2014-12-17 17:43:41.139 I 31930/System.out: 3 0
2014-12-17 17:43:41.139 I 31930/System.out: 3 +7[7 715-
2014-12-17 17:43:41.139 I 31930/System.out: 3 3
2014-12-17 17:43:41.139 I 31930/System.out: 3 +7[7 715-
2014-12-17 17:43:41.139 I 31930/System.out: 16 16
2014-12-17 17:43:41.139 I 31930/System.out: 16 +7[ 2]715-31-14
2014-12-17 17:43:41.739 D 2110/dalvikvm: GC_FOR_LLLOC freed 918K, 1
2014-12-17 17:43:42.270 E 1885/wpa_supplicant: RX ctrl_iface - hexdump
2014-12-17 17:43:42.270 E 1885/wpa_supplicant: 53 49 47 4e 41 4c 5f
2014-12-17 17:43:42.270 D 1885/wpa_supplicant: Command received: SIG
```



Системный лог содержит
множество отладочных данных

Group-IB TOP 10++

- Отсутствие контроля перекрытия экрана;



Возможность
перекрытия экрана
для финансового
приложения —
преступление

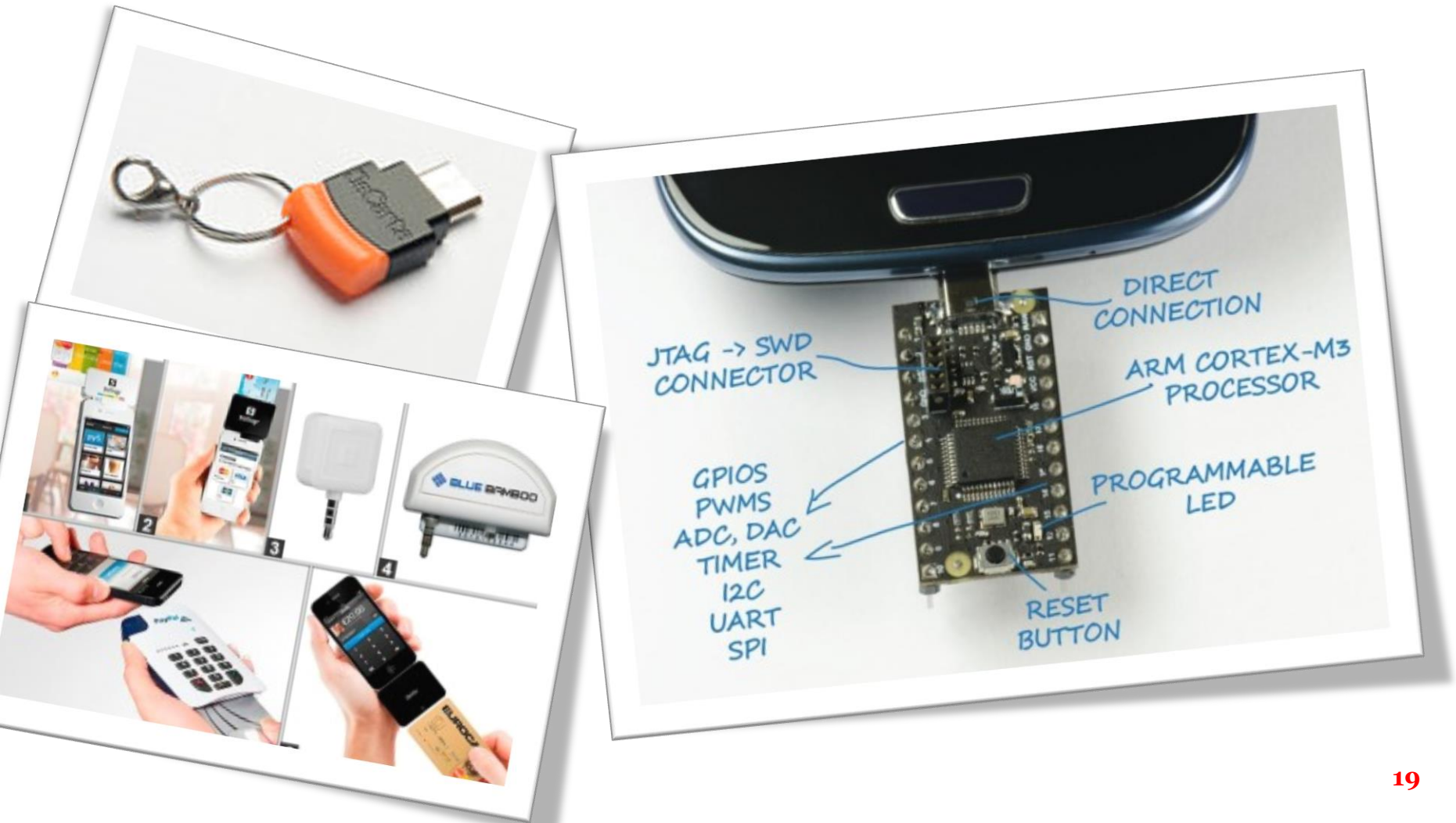
Защищённые мессенджеры



Защищённые телефоны и корпоративное использование



Токены и mPOS



Линейка продуктов для проактивной защиты от киберугроз



Bot-Trek Intelligence



Bot-Trek TDS



Bot-Trek Secure Bank



Bot-Trek Secure Portal



**Андрей
Брызгин**

+7 (495) 984-33-64 **доб.511**

+7 929 597 1223

bryzgin@group-ib.ru



+7 (495) 984 33 64



www.group-ib.ru



info@group-ib.ru



facebook.com/group-ib



twitter.com/group-ib