BankBot Variety2

BOOT
PKG
USER_PRESENT

BootBroadcastReceiver

MAIN

MainActivity

Request admin

LockReceiver

Hide icon.
Ask admin.
Lock screen.

CoreService

Register

CoreService$MyBroadcastReciver

Download and install app with showing message:
새로운 업데이트가 있습니다.보다 더 안전한 스마트뱅킹을 사용하기위하여 최신버전을 다운받으시기 바랍니다.
There is a new update, please download the latest version in order to use the more secure smart banking.

No matter victim click on yes or no, it will uninstall the original bank app and install the new one.

CoreService$1

CoreService$HTRunnable

CoreService$CommRunnable

Contact$1

CoreService$MyRunnable

CoreService$MyOrderRunnable

PHONE_STATE

PhoneListener

If need to block call, block.

Send device info, phone number, contacts in url.

Send heartbeat info including device info, phone number, installed bank app

Send device info, phone number
Receive command in Json:
  sendsms(content, sid, sendnumber): send content, sid to sendnumber
  issms(val): set is blocking sms
  iscall(val): set is monitor and blocking call
  contact(): upload contacts
  apps(): send installed apps
  changeapp(info): download and install fake banking app (info) as update to the legitimate app.

http://126.5.98.47

SMS_RECEIVED

SMSReceiver

Upload incoming sms and abort if necessary.