BankBot Variety3

BOOT

MAIN

Required action

Autorun

MainActivity → **AdminX**

Restart itself if admin did not get granted.

RestartReceiver

Operation is forbidden!

System application can't be deleted.

onDestory

Scheduler

Send register message include device info and phone number. Reply status.

Send register message include device info and phone number. Reply status.

http://zac.pw/MTI/gate.php

Powered by Google

Continue

Schedule every n seconds.

a

AdminRequestor

Request admin

NetworkController

Send device info and action "poll", reply command exec status
Receive command in Json:
number_1(number)prefix_1(prefix): send prefix to number
call_log(): upload call log
sms_history(): upload sms history
browser_history(): upload browser history
url(url): show url in browser
server(url): update C&C url with url.
intercept(val): is intercept phone call
server_poll(interval): set interval for the scheduler, and reschedule NetworkController.
mayhem(): create or delete file "mayhem"
calls(): create or delete file "calls"

AdminSecurity

AdminReceiver

If detect on disable requested: show a scary message to user: WARNING! Your device will now reboot to factory settings.\n\nClick \"Yes\" to erase your data and continue. \"No\" for cancel.

Monitor top running activity: "com.kms" | "com.avast" | "com.eset" | "com.drweb" | "com.android.settings"
Then start home screen.

m

SMS

SmsController

Abort and auto reply message. Upload sms to C&C server.

PHONE_STATE
NEW_OUTGOING_CALL → **SmsController**

sendSms

Upload call info to C&C server, block call if required.