Malware Discovery Form

Name of application: FlashBang

Time to find malware (hours): XXX

Location (filenames and line numbers): all lines

Trigger (conditions/events needed to trigger malware): This malware is executed when the application is installed.

Malicious Effects:

The application can:

- Download and execute files
- Steal contacts list
- Report system information
  - International Mobile Equipment Identity (IMEI)
  - Subscriber ID
  - Installed applications
  - Phone number
  - Phone model
  - Phone manufacturer
  - Operating system
- Make phone calls
- Send SMS messages
- Monitor and record SMS messages
- Show notifications
- Uninstall applications

Additional Notes (optional):
This malware was decompiled from the original Stels malware sample (1) using the technique outlined at (2). The packages were renamed to “ru.flashbang” and some broken decompiled functionalities were removed. The C&C server was replaced with liveartlu.com.

1) http://www.secureworks.com/cyber-threat-intelligence/threats/stels-android-trojan-malware-analysis/
2) https://kkinder.com/2011/11/27/so-you-want-to-reverse-engineer-an-android-app-apk/