



MoGua

LuckyBear 1.0.2.APK 分析报告



APP名称:

LuckyBear

包名:	com.prize.game.plus
域名线索:	21条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件名: com.luckybear.pro.apk
文件大小: 9.74MB
MD5值: c7f642479669ba3c0cc4f6ea3839f508
SHA1值: a20a9e2de681778bbb32966a95cb81ec85e4698a
SHA256值: 61a989862d45e354a1d46c241aaf8561e62e9062830751e8e2e4e95488107673

i APP 信息

App名称: LuckyBear
包名: com.prize.game.plus
主活动Activity: com.prize.game.plus.MainActivity
安卓版本名称: 1.0.2
安卓版本: 3

🔍 域名线索

域名	服务器信息
smonitorsdk.s	没有服务器地理信息.
sadrevenue.s	没有服务器地理信息.
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
sapp.s	没有服务器地理信息.
sars.s	没有服务器地理信息.
sconversions.s	没有服务器地理信息.

scdn-settings.s	没有服务器地理信息.
sregister.s	没有服务器地理信息.
scdn-testsettings.s	没有服务器地理信息.
api.luckybear.online	IP: 156.229.17.236 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
sSDK-services.s	没有服务器地理信息.
sdlSDK.s	没有服务器地理信息.
svalidate.s	没有服务器地理信息.
sattr.s	没有服务器地理信息.
slaunches.s	没有服务器地理信息.
sviap.s	没有服务器地理信息.
sinapps.s	没有服务器地理信息.
simpression.s	没有服务器地理信息.
sgcdSDK.s	没有服务器地理信息.
sstats.s	没有服务器地理信息.
sonelink.s	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://api.luckybear.online/lucky_bear/native_app/af_report	com/prize/game/plus/MainActivity.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True

v3 签名: False
找到 1 个唯一证书
主题: CN=prizeplus, OU=prizeplus, O=prizeplus, L=prizeplus, ST=prizeplus, C=ru
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-08 11:36:48+00:00
有效期至: 2050-04-02 11:36:48+00:00
发行人: CN=prizeplus, OU=prizeplus, O=prizeplus, L=prizeplus, ST=prizeplus, C=ru
序列号: 0x1
哈希算法: sha256
md5值: 7dbd35d5d41d1cb0d0596569df8e2664
sha1值: d12f6cc261cdb26f50a6dc532e3dd75812a9c5db
sha256值: 432b68eb3f55d0bac0ebc8d80ee00077715c754bbbbfe125753229ce8dc8aa3a
sha512值: adc80b5cd4069c0b1acd6181e9bc1d6c1925bcccb07302cdb9ac182562efff64f1691871539f15bd201fd129d7c4664cef3b80c2a787744a3edc782cd0228b26
公钥算法: rsa
密钥长度: 2048
指纹: f65e06cecfb9744e87338a88bd8ecaf4ce9f358cf3a1113efac84a04db96c7a6

 硬编码敏感信息

 加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

 第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

☰ 此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.prize.game.plus.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

📱 应用内通信

活动(ACTIVITY)	通信(INTENT)
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,