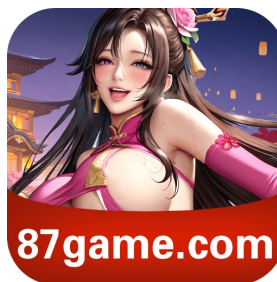




MoGua

夜色三國 1.0.1.APK 分析报告



APP名称:

夜色三國

包名: com.hgame.sanguo.lybq.channel

域名线索: 9条

URL线索: 16条

邮箱线索: 22条

分析日期: 2025年6月17日

分析平台: [摸瓜APK反编译平台](#)

文件名: 20250108_232922yssg_26.apk
文件大小: 1225.25MB
MD5值: 170493942ad08f4a6a1f4b552d20c821
SHA1值: b96c8a94a28acfa75c8a4af82279c8832f8a457c
SHA256值: 3057ab6721c7dbab45bc0aaed07e1035863205632de89920ccada05d24e6230d

i APP 信息

App名称: 夜色三國
包名: com.hgame.sanguo.lybq.channel
主活动Activity: com.hgame.sdk_ly_bq.SdkActivity
安卓版本名称: 1.0.1
安卓版本: 1

🔍 域名线索

域名	服务器信息
sdk-interface.dxsc18.com	IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
sdk-interface.scbgds.com	IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
sdk-interface.rjrgc.com	IP: 75.2.47.185 所属国家: United States of America 地区: Washington

	城市: Seattle 纬度: 47.604309 经度: -122.329842
sdk-static.xlxtop.com	IP: 18.167.82.124 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
example.com	IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580
sdk-interface.fjkwx.com	IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
sdk-interface.slzth.com	IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
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
	IP: 85.13.163.69

greenrobot.org	所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770
----------------	--

URL线索

URL信息	Url所在文件
https://sdk-static.xlxtop.com/login	com/bqgame/sdk/BqGameAgent.java
https://sdk-static.xlxtop.com/recharge-center?token=	com/bqgame/sdk/BqGameAgent.java
https://sdk-static.xlxtop.com/login	com/bqgame/sdk/a.java
https://sdk-static.xlxtop.com	com/bqgame/sdk/a.java
https://sdk-static.xlxtop.com/login	com/bqgame/sdk/ui/BaseHyActivity.java
https://sdk-interface.scbgds.com	com/bqgame/sdk/helper/c.java
https://sdk-interface.dxsc18.com	com/bqgame/sdk/helper/c.java
https://sdk-interface.slzth.com	com/bqgame/sdk/helper/c.java
https://sdk-interface.fjkwx.com	com/bqgame/sdk/helper/c.java
https://sdk-interface.rjrgc.com	com/bqgame/sdk/helper/c.java
http://example.com/	cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
https://sdk-static.xlxtop.com/login	d/c.java
https://sdk-static.xlxtop.com/login	d/a.java

 邮箱线索

邮箱地址	所在文件
x3@tj2.pnq j@njfp.ᄃb hzo@v1.as	摸瓜V2引擎
rk@n.2mᄃbvs rr@y.54 no@5.tsj 8@1v.nk	摸瓜V2引擎
g@ᄃn.ᄃie8d 06@t0ᄃwr 69	

00@t00m.00 mrdëy.a@z.h8w 冥@w.rgpm ixo@h6.ptv	摸瓜V2引擎
o@5.lvl	摸瓜V2引擎
d@f.wzlsH ext†0@27.qzpc kŒ@-.zo	摸瓜V2引擎
g@wŵpfi.xq2k0h	摸瓜V2引擎
1zdsa@vk.r12	摸瓜V2引擎
q@daũy.dn 5h3@m.иo	摸瓜V2引擎
g@wŵpfi.xq2k0h	摸瓜V2引擎
i0ṗy@d.pi gr-@k.at	摸瓜V2引擎
t@qb.sa	摸瓜V2引擎
ru@ṗ.ṗuwyy ó@w.gz	摸瓜V2引擎
s@68u.7k梃d p@aybc6.xkq	摸瓜V2引擎
đ@rtytv.pi s2@r.a7 lz@g.onkő	摸瓜V2引擎
v7_@luuy.ee	摸瓜V2引擎

g@vww.ur	摸瓜V2引擎
r@8.rmd	摸瓜V2引擎
s0z@uea'.ddo i@j-m.sw _@uy.31	摸瓜V2引擎
e@ᄁ.79	摸瓜V2引擎
n@7cch.rcŋ8xřw	摸瓜V2引擎
g@□n.ĭie8d 06@t0ewr.69 mrdëy.a@z.h8w 冥@w.rgpm ixo@h6.ptv	摸瓜V2引擎
b_vi@h7mpi.ptj	摸瓜V2引擎

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-04 11:19:05+00:00
有效期至: 2049-11-28 11:19:05+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1

序列号: 0x246b0d3d
哈希算法: sha256
md5值: c74909cbdc85300179738a71742966e1
sha1值: 8b5d07355615c889e3a8368c81248b26c61050fb
sha256值: 54ca460e5465cd74057448635b8028e19a61a9c8f83279b5fd045b782c249867
sha512值: d3cbabe30856518dfb66dc9c452d6d5cb9bc032dfbd15d7e515269f071657e83f3f44ef0baa618bdb03d4a1b207a8e780a39349b7728b7b4fb3bbd36f81c7990
公钥算法: rsa
密钥长度: 2048
指纹: 694dbd11af18dff41065ab333998fd9585f83ec0a98c2b61b09fdf1f076ef129

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	类型	详细情况

	危险		
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.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。