Evaluation Warning: The document was created with Spire.Doc for Python.

**夜色三國（ 1.0.1版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 夜色三國 |
| 版本 | 1.0.1 |
| 包名 | com.hgame.sanguo.lybq.channel |
| 域名线索 | 9条 |
| URL线索 | 16条 |
| APP图标 |  |
| 分析日期 | 2025年6月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 20250108\_232922yssg\_26.apk |
| 文件大小 | 1225.25MB |
| MD5值 | 170493942ad08f4a6a1f4b552d20c821 |
| SHA1值 | b96c8a94a28acfa75c8a4af82279c8832f8a457c |
| SHA256值 | 3057ab6721c7dbab45bc0aaed07e1035863205632de89920ccada05d24e6230d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| sdk-interface.scbgds.com | IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle  |
| sdk-interface.rjrgc.com | IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle  |
| sdk-static.xlxtop.com | IP: 18.167.82.124 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| example.com | IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo  |
| sdk-interface.fjkwx.com | IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle  |
| sdk-interface.slzth.com | IP: 75.2.47.185 所属国家: United States of America 地区: Washington 城市: Seattle  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| greenrobot.org | IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf  |

### **4.2 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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| x3@tj2.pnq j@njfp.ʉb hzo@v1.as  | 摸瓜V2引擎  |
| rk@n.2mìܕbvs rr@y.54 no@5.ʦj 8@1v.nk  | 摸瓜V2引擎  |
| g@ࢬn.ӹe8d 06@t0ewr.69 mrdӫy.a@z.h8w 㝠@w.rgpm ixo@h6.ptv  | 摸瓜V2引擎  |
| o@5.lvl  | 摸瓜V2引擎  |
| d@f.wzlsʜ exɫϐo@27.qzρc kŝ@-.ƶo  | 摸瓜V2引擎  |
| g@wʬpfi.xq2k0h  | 摸瓜V2引擎  |
| 1zdsa@vk.r12  | 摸瓜V2引擎  |
| q@daǖy.dn 5h3@m.ͷo  | 摸瓜V2引擎  |
| g@wʬpfi.xq2k0h  | 摸瓜V2引擎  |
| i0ܯy@d.pi gr-@ҟ.at  | 摸瓜V2引擎  |
| t@qb.sa  | 摸瓜V2引擎  |
| ru@پ.ӌuwyy ó@w.gz  | 摸瓜V2引擎  |
| s@68u.7k棓d þ@aybc6.xkq  | 摸瓜V2引擎  |
| ծ@rtytv.pi s2@r.a7 lz@g.onkő  | 摸瓜V2引擎  |
| v7\_@luuy.ee  | 摸瓜V2引擎  |
| ǥ@vww.ur  | 摸瓜V2引擎  |
| r@8.rmd  | 摸瓜V2引擎  |
| s0z@ueaי.ddo i@j-m.sw \_@uy.31  | 摸瓜V2引擎  |
| e@ͽ.79  | 摸瓜V2引擎  |
| n@7cch.rcղ8xϔw  | 摸瓜V2引擎  |
| g@ࢬn.ӹe8d 06@t0ewr.69 mrdӫy.a@z.h8w 㝠@w.rgpm ixo@h6.ptv  | 摸瓜V2引擎  |
| b\_vi@h7mpi.ptj  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **5. 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**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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。 |

## **10. 应用内通信**

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