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

**疯狂宝贝（ 3.0.1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 | 疯狂宝贝 |
| 版本 | 3.0.1 |
| 包名 | com.fkbb.zsy |
| 域名线索 | 40条 |
| URL线索 | 33条 |
| APP图标 |  |
| 分析日期 | 2024年12月3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 | h4000.apk |
| 文件大小 | 32.41MB |
| MD5值 | e461a98e90605cce1693a42d8132ed80 |
| SHA1值 | d060c09a59a98293a8a928aafce175be3cb05a09 |
| SHA256值 | 9839754e7d0ef008ec58a466172a2c61dabec0c89b3bfd52fed00bcf3d0cbd96 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 疯狂宝贝 |
| 包名 | com.fkbb.zsy |
| 主活动Activity | com.rebate.agent.privacy.PrivacyActivity |
| 安卓版本名称 | 3.0.1 |
| 安卓版本 | 30001 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| callback.sdk.quicksdk.net | IP: 106.75.99.122  所属国家: China  地区: Beijing  城市: Beijing |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| www.baidu.com | IP: 110.242.68.3  所属国家: China  地区: Hebei  城市: Baoding |
| 172.16.130.122 | IP: 172.16.130.122  所属国家: -  地区: -  城市: - |
| www.173qy.com | IP: 120.79.147.48  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cfg.imtt.qq.com | IP: 109.244.173.227  所属国家: China  地区: Beijing  城市: Beijing |
| ms.zzx9.cn | IP: 111.206.169.70  所属国家: China  地区: Beijing  城市: Beijing |
| pv.sohu.com | IP: 42.81.16.110  所属国家: China  地区: Tianjin  城市: Tianjin |
| mdc.html5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| onekey.cmpassport.com | IP: 120.197.235.28  所属国家: China  地区: Guangdong  城市: Guangzhou |
| sg2log.gotechgames.com | IP: 47.110.254.39  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| sysdk.cl2009.com | IP: 101.133.104.19  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| iospingtai.xinxinjoy.com | IP: 120.79.164.117  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| log1.cmpassport.com | IP: 36.138.255.61  所属国家: China  地区: Beijing  城市: Beijing |
| debugx5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| www.csgames.net | IP: 219.147.98.77  所属国家: China  地区: Nei Mongol  城市: Baotou |
| sy.cl2009.com | IP: 47.101.5.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| config.cmpassport.com | IP: 120.232.169.180  所属国家: China  地区: Guangdong  城市: Guangzhou |
| open.e.189.cn | IP: 42.123.76.52  所属国家: China  地区: Beijing  城市: Beijing |
| example.com | IP: 93.184.216.34  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| update.kairong5.com | IP: 219.147.98.77  所属国家: China  地区: Nei Mongol  城市: Baotou |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Shanghai  城市: Shanghai |
| 47.110.125.158 | IP: 47.110.125.158  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| debugtbs.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| log.tbs.qq.com | IP: 109.244.244.32  所属国家: China  地区: Beijing  城市: Beijing |
| passport.q1.com | IP: 39.105.141.118  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wup.imtt.qq.com | IP: 42.187.184.221  所属国家: China  地区: Beijing  城市: Beijing |
| api.sy12306.com | IP: 47.99.211.243  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| collect.ux.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| stand.alone.version | 没有服务器地理信息. |
| wap.cmpassport.com | IP: 120.197.235.27  所属国家: China  地区: Guangdong  城市: Guangzhou |
| runtime.layabox.com | IP: 221.204.166.202  所属国家: China  地区: Shanxi  城市: Taiyuan |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| pms.mb.qq.com | IP: 175.27.12.246  所属国家: China  地区: Beijing  城市: Beijing |
| lingliusdk.szyzcm.com | IP: 47.107.82.187  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| nativetest.layabox.com | IP: 111.229.219.46  所属国家: China  地区: Beijing  城市: Beijing |
| www.q1.com | IP: 219.147.98.77  所属国家: China  地区: Nei Mongol  城市: Baotou |
| configcdn.quicksdk.net | IP: 106.75.31.55  所属国家: China  地区: Shanghai  城市: Shanghai |
| dnf.fggood.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.sy12306.com/channel/geturl | sdk/zhaosy/sdk/Login.java |
| https://api.sy12306.com/channel/geturl | sdk/zhaosy/sdk/Pay.java |
| http://pv.sohu.com/cityjson?ie=utf-8 | sdk/zhaosy/sdk/zhaosySDK.java |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | cn/com/chinatelecom/account/api/c/a.java |
| https://collect.ux.21cn.com/collect/custom/accountMsg | cn/com/chinatelecom/account/a/c.java |
| http://iospingtai.xinxinjoy.com:8084/outerinterface/ | com/org/suspension/zk/model/HttpUtils.java |
| http://iospingtai.xinxinjoy.com:8084/outerinterface/getlianxi.php | com/org/suspension/zk/model/HttpUtils.java |
| http://iospingtai.xinxinjoy.com:8084/outerinterface/getuserinfo.php | com/org/suspension/zk/model/HttpUtils.java |
| http://iospingtai.xinxinjoy.com:8084/outerinterface/andsetname.php | com/org/suspension/zk/model/HttpUtils.java |
| http://lingliusdk.szyzcm.com:8182/init.php?gameparam=replace | com/rebate/agent/sdk/AsdkActivity.java |
| http://lingliusdk.szyzcm.com:8182/hbinit.php?pub= | com/rebate/agent/sdk/SkipActivity.java |
| http://lingliusdk.szyzcm.com:8188/shanping.php?pub= | com/rebate/agent/aidl/LingliuSdk.java |
| http://sg2log.gotechgames.com:5201/ActiveGame | com/rebate/agent/tools/HttpUtils.java |
| http://www.baidu.com | com/rebate/agent/tools/PhoneTool.java |
| http://onekey.cmpassport.com/unisdk/ | com/cmic/sso/sdk/utils/d.java |
| https://config.cmpassport.com/client/uniConfig | com/cmic/sso/sdk/utils/d.java |
| https://log1.cmpassport.com:9443/log/logReport | com/cmic/sso/sdk/utils/x.java |
| https://onekey.cmpassport.com:443/unisdk/ | com/cmic/sso/sdk/utils/x.java |
| http://onekey.cmpassport.com/unisdk/ | com/cmic/sso/sdk/utils/x.java |
| https://e.189.cn/sdk/agreement/detail.do | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://config.cmpassport.com/client/uniConfig | com/cmic/sso/sdk/b/b/a.java |
| http://appdata.4g.q1. | com/q1/sdk/http/Router.java |
| https://appdata-ea.q1. | com/q1/sdk/http/Router.java |
| https://appdata-review.q1. | com/q1/sdk/http/Router.java |
| https://appdata-sa.q1. | com/q1/sdk/http/Router.java |
| https://appdata. | com/q1/sdk/http/Router.java |
| http://sdkapi.4g.q1. | com/q1/sdk/http/Router.java |
| https://ops-api.q1. | com/q1/sdk/http/Router.java |
| http://bulletin-api.test.q1oa. | com/q1/sdk/http/Router.java |
| https://sdkapi. | com/q1/sdk/http/Router.java |
| https://sdkapi.q1. | com/q1/sdk/http/Router.java |
| https://www.q1.com/PrivacyChildren.html | com/q1/sdk/entity/ConfigEntity.java |
| https://www.q1.com/PrivacyPolicy.html | com/q1/sdk/entity/ConfigEntity.java |
| https://www.q1.com/UserProtocol.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.173qy.com/PrivacyChildren.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.173qy.com/PrivacyPolicy.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.173qy.com/UserProtocol.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.csgames.net/PrivacyChildren.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.csgames.net/PrivacyPolicy.html | com/q1/sdk/entity/ConfigEntity.java |
| http://www.csgames.net/UserProtocol.html | com/q1/sdk/entity/ConfigEntity.java |
| https://passport.q1.com/Validate/LogOn | com/q1/sdk/entity/ConfigEntity.java |
| https://data. | com/q1/sdk/entity/Q1Configuration.java |
| https://www.q1.com/PrivacyChildren.html | com/q1/sdk/service/impl/ConfigServiceImpl.java |
| https://www.q1.com/PrivacyPolicy.html | com/q1/sdk/service/impl/ConfigServiceImpl.java |
| https://www.q1.com/UserProtocol.html | com/q1/sdk/service/impl/ConfigServiceImpl.java |
| http://callback.sdk.quicksdk.net/callback/ | com/quicksdk/apiadapter/zhaoshouyou/PayAdapter.java |
| http://configcdn.quicksdk.net | com/quicksdk/net/a.java |
| https://sysdk.cl2009.com/ | com/chuanglan/shanyan\_sdk/a.java |
| https://sy.cl2009.com/ | com/chuanglan/shanyan\_sdk/a.java |
| https://sy.cl2009.com/flash/accountInit/v3 | com/chuanglan/shanyan\_sdk/b.java |
| https://sy.cl2009.com/flash/accountInit/v4 | com/chuanglan/shanyan\_sdk/b.java |
| https://sysdk.cl2009.com/flash/fdr/v3 | com/chuanglan/shanyan\_sdk/b.java |
| https://sy.cl2009.com/ | com/chuanglan/shanyan\_sdk/b.java |
| https://sysdk.cl2009.com/ | com/chuanglan/shanyan\_sdk/b.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/chuanglan/shanyan\_sdk/b.java |
| http://wap.cmpassport.com/resources/html/contract.html | com/chuanglan/shanyan\_sdk/b.java |
| https://ms.zzx9.cn/html/oauth/protocol2.html | com/chuanglan/shanyan\_sdk/b.java |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/j.java |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/x.java |
| http://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/x.java |
| http://wup.imtt.qq.com:8080 | com/tencent/smtt/utils/x.java |
| http://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/x.java |
| http://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/x.java |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/x.java |
| http://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/x.java |
| http://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/x.java |
| http://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| http://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/ac.java |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/a/d.java |
| http://example.com/ | cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java |
| http://dnf.fggood.com | Mogua Engine V1 |
| http://172.16.130.122:82/apk\_test/app-update.json | Mogua Engine V2 |
| http://update.kairong5.com/version | Mogua Engine V2 |
| http://172.16.130.122:82/apk\_test/version | Mogua Engine V2 |
| http://47.110.125.158:8081/api/client\_log/write\_log | Mogua Engine V2 |
| http://update.kairong5.com/version | Mogua Engine V2 |
| http://update.kairong5.com/apk\_update | Mogua Engine V2 |
| http://47.110.125.158:8081/api/client\_log/write\_log | Mogua Engine V2 |
| http://runtime.layabox.com/font/simhei.ttf', | Mogua Engine V2 |
| http://stand.alone.version') | Mogua Engine V2 |
| http://stand.alone.version/index.js'; | Mogua Engine V2 |
| http://nativetest.layabox.com/layaplayer2.0.1/index.js | Mogua Engine V2 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=86, ST=Beijing, L=Beijing, O=Youyi, OU=Youyi, CN=You Yi 签名算法: rsassa\_pkcs1v15 有效期自: 2019-06-24 07:30:01+00:00 有效期至: 2119-05-31 07:30:01+00:00 发行人: C=86, ST=Beijing, L=Beijing, O=Youyi, OU=Youyi, CN=You Yi 序列号: 0x598ff25b 哈希算法: sha256 md5值: bf0234801947f6fbca1b0393d9d92dd4 sha1值: a4fd9fc116ce7ea16c730f11fec3285fdce282bc sha256值: 1915463f9089cf8f705524251ca5791e4f51c143778f30ad64bd97848a85ca69 sha512值: 279857786fb48be7eda291cbdded16daa465e3403196bb59bc07285f1fc633833498c72802c996e99bf3e2a5b53ba738c4d9a16512f5ccfa4511dddf6e8dabb2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_password" : "密码:" |
| "remember\_password" : "记住密码" |
| "pinputusername" : "请输入手机号/用户名" |
| "inputpwd" : "请输入游戏密码" |

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| 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.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |

## **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。**