MoGua

搞笑世界 7.9.0.APK 分析报告

APP名称:	搞笑世界

包名:	com.jiuyifangdu.release
域名线索:	9条
URL线索:	8条
邮箱线索:	2条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gamecenter_release_android_jiuyi_5520_548c135dc8f58dc39df6c59529e2cd21.apk
文件大小: 69.15MB
MD5值: f7be6c067f7f3bcf2418755fa0b10715
SHA1值: 680451198f420108297750ca7b53165ac3c7b0c4
SHA256值: 53055b60952a68fc9c122c64a81bd6bb7a30b46b37277887ceb010dfb7e69342

APP 信息

App名称: 搞笑世界
包名: com.jiuyifangdu.release
主活动Activity: com.jiuyifangdu.main.MainGameActivity
安卓版本名称: 7.9.0
安卓版本: 790

域名线索

域名	服务器信息
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
pay.po124.com	**IP**: 34.96.237.34 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
open.weixin.qq.com	**IP**: 116.128.171.214 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
www.smpte-ra.org	**IP**: 52.20.185.129 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
long.open.weixin.qq.com	**IP**: 112.65.193.170 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

astat.bugly.cros.wr.pvp.net	**IP**: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418

URL线索

URL信息	Url所在文件
https://pay.po124.com/api/upload_certT	com/ccsdk/activity/WebViewFragment.java
https://pay.po124.com/api/upload_certT	com/ccsdk/activity/WebViewActivity.java
http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/D.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java

邮箱线索

邮箱地址	所在文件
21b3aa9e106ae4450662@gmail.com	chat/ccsdk/com/chat/utils/a/a/c.java
p1@zki.x9	摸瓜V2引擎

手机线索

手机号	所在文件
15555215554	com/jiuyifangdu/util/FindEmulator.java
15555215556	com/jiuyifangdu/util/FindEmulator.java
15555215558	com/jiuyifangdu/util/FindEmulator.java
15555215560	com/jiuyifangdu/util/FindEmulator.java
15555215562	com/jiuyifangdu/util/FindEmulator.java
15555215564	com/jiuyifangdu/util/FindEmulator.java
15555215566	com/jiuyifangdu/util/FindEmulator.java
15555215568	com/jiuyifangdu/util/FindEmulator.java
15555215570	com/jiuyifangdu/util/FindEmulator.java
15555215572	com/jiuyifangdu/util/FindEmulator.java
15555215574	com/jiuyifangdu/util/FindEmulator.java

15555215576	com/jiuyifangdu/util/FindEmulator.java
15555215578	com/jiuyifangdu/util/FindEmulator.java
15555215580	com/jiuyifangdu/util/FindEmulator.java
15555215582	com/jiuyifangdu/util/FindEmulator.java
15555215584	com/jiuyifangdu/util/FindEmulator.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=JiuYi, OU=JiuYi, O=JiuYi
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-28 12:35:47+00:00
有效期至: 2049-12-22 12:35:47+00:00
发行人: CN=JiuYi, OU=JiuYi, O=JiuYi
序列号: 0x1
哈希算法: sha256
md5值: 4f3d61d263779a4eb8b1664edf9f1cf3
sha1值: 6b5e18ad888dc4b4d00c89eeab17aaf613ca48c7
sha256值: 761d14dc7c8a7b5bd015697239ffda9516febc2dd38ef116a317ef510fb9a558
sha512值: dbca5458e832141c6553e81a454855932107c08890197c2e9b9fa89411353f7ce61de30419cd46d36dfee6029d6dbc0af618a3f6ace3410f4e0f9bdf8a420640
公钥算法: rsa
密钥长度: 2048
指纹: c819a711b2429238800016d4e519bc97c8d9a6a0d7b1c207e28e8c1da44bf4f8

硬编码敏感信息

可能的敏感信息
"net_connecting2_sessionlist" : "连接中.."
"net_connecting3_sessionlist" : "连接中..."
"net_connecting_sessionlist" : "连接中."
"open_session_failed_forbidden" : "该闪付专员已离开地球，请尝试联系其他专员"

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

	是否		

向手机申请的权限	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.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.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.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.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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

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。
android.permission.MANAGE_DOCUMENTS	合法		允许应用程序管理对文档的访问,通常作为文档选择器的一部分
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章

com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference

应用内通信