



MoGua

永利娱乐城 5.2.22.APK 分析报告



APP名称:

永利娱乐城

包名: com.srcg.gifp1319.kwmjvui

域名线索: 57条

URL线索: 35条

邮箱线索: 0条

分析日期: 2025年7月5日

分析平台: [摸瓜APK反编译平台](#)

文件名: 4 (22).apk
文件大小: 76.82MB
MD5值: 58ce6637a1c1c95e457584f0403bf8c5
SHA1值: 3a4c7ff0550eda95e50621a5bc65ab70117db6e3
SHA256值: 089bb26d43c3d12937555ee69746da92ccd88381acb93a4b108d116977adffef

i APP 信息

App名称: 永利娱乐城
包名: com.srcg.gifp1319.kwmjvui
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 5.2.22
安卓版本: 12

🔍 域名线索

域名	服务器信息
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
smonitorsdk.s	没有服务器地理信息.
gdpr.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380

id6.me	IP: 42.123.77.138 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sonelink.s	没有服务器地理信息.
cdn.livechatinc.com	IP: 2.16.1.243 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
riskct.geetest.com	IP: 103.143.17.142 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
sconversions.s	没有服务器地理信息.
ssdk-services.s	没有服务器地理信息.
manual.sensorsdata.cn	IP: 125.39.61.77 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
app.adjust.com	IP: 185.151.204.9 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525

	经度: 13.410037
gdpr.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
subscription.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
app.adjust.net.in	IP: 185.151.204.31 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
app.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
msg.cmpassport.com	IP: 120.232.74.115 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
	IP: 74.86.226.234 所属国家: United States of America 地区: California

www.facebook.com	城市: San Jose 纬度: 37.339390 经度: -121.894958
simpression.s	没有服务器地理信息.
api.onesignal.com	IP: 104.17.111.223 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
gdpr.adjust.net.in	IP: 185.151.204.30 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
bugsnag.com	IP: 3.165.102.3 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
slaunches.s	没有服务器地理信息.
gdpr.adjust.world	IP: 185.151.204.40 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
sadrevenue.s	没有服务器地理信息.

sgcdsdk.s	没有服务器地理信息.
tools.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
subscription.adjust.world	IP: 185.151.204.44 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
scdn-ssettings.s	没有服务器地理信息.
sattr.s	没有服务器地理信息.
subscription.adjust.net.in	IP: 185.151.204.34 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
sars.s	没有服务器地理信息.
access.line.me	IP: 199.59.148.96 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
svalidate.s	没有服务器地理信息.

scdn-stestsettings.s	没有服务器地理信息.
sviap.s	没有服务器地理信息.
gdpr.adjust.com	IP: 185.151.204.51 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
docs.bugsnag.com	IP: 3.170.229.22 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
pushstat.api.engagelab.cc	IP: 188.239.42.236 所属国家: Ukraine 地区: Kyiv 城市: Kiev 纬度: 50.454659 经度: 30.523800
notify.bugsnag.com	IP: 35.186.205.6 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
sdlSDK.s	没有服务器地理信息.
app.adjust.world	IP: 185.151.204.41 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525

	经度: 13.410037
sstats.s	没有服务器地理信息.
app.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
api.line.me	IP: 199.59.149.237 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
zolz-pipe.oss-ap-southeast-1.aliyuncs.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
sessions.bugsnag.com	IP: 35.190.88.7 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
subscription.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380

sregister.s	没有服务器地理信息.
gdpr.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
dnsrepo-pub.alibaba.com	IP: 203.119.174.99 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
sapp.s	没有服务器地理信息.
sinapps.s	没有服务器地理信息.
nisportal.10010.com	IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
subscription.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
subscription.adjust.com	IP: 185.151.204.52 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525

	经度: 13.410037
app.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380
en.wikipedia.org	IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249

URL线索

URL信息	Url所在文件
https://app.adjust.com	com/adjust/sdk/Constants.java
https://gdpr.adjust.com	com/adjust/sdk/Constants.java
https://subscription.adjust.com	com/adjust/sdk/Constants.java
https://github.com/adjust/android_sdk	com/adjust/sdk/ActivityHandler.java
https://app.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://app.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java

https://app.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://subscription.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://subscription.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermData	com/alibaba/pdns/g.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData	com/alibaba/pdns/g.java
https://zoloz-pipe.oss-ap-southeast-1.aliyuncs.com/zmodel/	com/ap/zoloz/hot/download/impl/ModelLoadServiceImpl.java
https://notify.bugsnag.com	com/bugsnag/android/s0.java
https://sessions.bugsnag.com	com/bugsnag/android/s0.java
https://bugsnag.com	com/bugsnag/android/b2.java

https://docs.bugsnag.com/platforms/android/	com/bugsnag/android/p.java
https://docs.bugsnag.com/platforms/android/ndk-link-errors	com/bugsnag/android/NdkPlugin.java
https://docs.bugsnag.com/platforms/android/anr-link-errors	com/bugsnag/android/AnrPlugin.java
https://riskct.geetest.com/g2/api/v1/client_report	com/geetest/core/e.java
https://riskct.geetest.com/g2/api/v1/client_report	com/geetest/core/GeeGuard.java
https://nisportal.10010.com:9001/api?	com/geetest/core/g6.java
https://msg.cmpassport.com/h5/getMobile	com/geetest/core/g6.java
https://id6.me/gw/preuniq.do	com/geetest/core/g6.java
https://riskct.geetest.com/g2/api/v1/client_report	com/geetest/gtc4/b.java
https://api.onesignal.com/	com/onesignal/q3.java
https://access.line.me/.well-known/openid-configuration	com/linecorp/linesdk/api/LineApiClientBuilder.java
https://api.line.me/	com/linecorp/linesdk/api/LineApiClientBuilder.java
https://access.line.me/.well-known/openid-configuration	com/linecorp/linesdk/auth/LineAuthenticationConfig.java
https://api.line.me/	com/linecorp/linesdk/auth/LineAuthenticationConfig.java
https://access.line.me/oauth2/v2.1/login	com/linecorp/linesdk/auth/LineAuthenticationConfig.java
https://en.wikipedia.org/wiki/Hostname	com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java
https://manual.sensorsdata.cn/sa/latest/flutter-22257963.html	com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java

https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_use-7545346.html\	com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java
https://cdn.livechatinc.com/app/mobile/urls.json	com/livechatinc/inappchat/ChatWindowViewImpl.java
https://.+facebook.+(/dialog/oauth\\?	com/livechatinc/inappchat/ChatWindowViewImpl.java
https://www.facebook.com/dialog/return/arbitr	com/livechatinc/inappchat/ChatWindowViewImpl.java
https://tools.ietf.org/html/rfc7518	io/jsonwebtoken/SignatureAlgorithm.java
https://tools.ietf.org/html/rfc7518	io/jsonwebtoken/security/Keys.java
https://pushstat.api.engagelab.cc	b0/a.java

 邮箱线索

 手机线索

手机号	所在文件
15552000000	p0/h.java
19634136210	r4/g1.java

 签名证书

无法读取代码签名证书.

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

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.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.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_AUDIO	未知	Unknown permission	Unknown permission from android reference
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.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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.srcg.gifp1319.kwmjvui.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置 (如果可用)。恶意应用程序可以使用它来确定您的大致位置
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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.cocos2dx.javascript.AppActivity	Schemes: wgwkgwkg1319://, Hosts: wgwkgwkg,

	Path Prefixes: /open,
com.facebook.CustomTabActivity	Schemes: fb\${facebookAppId}://, fbconnect://, Hosts: cct.com.srcg.gifp1319.kwmjvui,
com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity	Schemes: lineauth://,

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。