



MoGua

TEST0627 1.2.1.APK 分析报告



APP名称:

TEST0627

包名:	com.qxco3.baxe69lr
域名线索:	21条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件名: TEST0627_2.apk
文件大小: 2.43MB
MD5值: 261ab27365a4b9bee0592572bd1e97c4
SHA1值: 998436fd0235c04dd3c542b6d30e419b01ffde0d
SHA256值: 5abd2904951885b826b02b6ff13820fe1a14a3379d0907e274516becd3323828

i APP 信息

App名称: TEST0627
包名: com.qxco3.baxe69lr
主活动Activity: com.example.myapplication.ui.webviewstudy.GameActivity
安卓版本名称: 1.2.1
安卓版本: 4

🔍 域名线索

域名	服务器信息
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
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
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
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
app.adjust.cn	IP: 47.104.30.117 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
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
schemas.android.com	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
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
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
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
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
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
	IP: 185.151.204.44 所属国家: Germany

subscription.adjust.world	地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
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
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
app.adjust.world	IP: 185.151.204.43 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
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
gdpr.adjust.com	IP: 185.151.204.50 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
-------------------	---

 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.adjust.cn	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.adjust.com	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.adjust.com	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
http://schemas.android.com/apk/res/android	s/h.java

 邮箱线索

 手机线索

 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: C='CN', ST='Beijing', L='Beijing', O='MyOrganization', OU='IT', CN='CN'
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-12 12:37:28+00:00
有效期至: 2124-09-18 12:37:28+00:00
发行人: C='CN', ST='Beijing', L='Beijing', O='MyOrganization', OU='IT', CN='CN'
序列号: 0x6a98273868e4065
哈希算法: sha256
md5值: 6c0f44d57e342c3f36dd0c41e34ee67c
sha1值: 15fcc99ec2f6885b8305c091ca8046fa258b00a4
sha256值: e92f19d675acbffec79edaebd8367570ea6fc95fae7d826855935848bfce0d77
sha512值: 94ffd254adf8b71348d7698f865025e8aa2c0900a1d5bda77b1211e7336492f286757937bcf2417d83d6ed50bf4c472e662d8e60b654f97bada3c532c3022c19
公钥算法: rsa
密钥长度: 2048
指纹: cf7128712b66ed15542165e62fef946c9e50ebe6440f1863a7637224cb935db7

 硬编码敏感信息

可能的敏感信息
"ENGAGELAB_PRIVATES_CHANNEL_high" : "HIGH"
"ENGAGELAB_PRIVATES_CHANNEL_low" : "LOW"
"ENGAGELAB_PRIVATES_CHANNEL_normal" : "NORMAL"
"ENGAGELAB_PRIVATES_CHANNEL_silence" : "SILENCE"
"google_api_key" : "AlzaSyAQg2m49WtDGBY9WJZCCKN6rq1YYzkfBA"
"google_crash_reporting_api_key" : "AlzaSyAQg2m49WtDGBY9WJZCCKN6rq1YYzkfBA"
"ENGAGELAB_PRIVATES_CHANNEL_high" : "重要"

"ENGAGELAB_PRIVATES_CHANNEL_low" : "不重要"
"ENGAGELAB_PRIVATES_CHANNEL_normal" : "普通"
"ENGAGELAB_PRIVATES_CHANNEL_silence" : "静默"

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_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.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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.example.myapplication.ui.webviewstudy.GameActivity	Schemes: panda_2://, Hosts: open,