MoGua

龙年优选 1.0.0.APK 分析报告

APP名称:	龙年优选

包名:	com.kydqrj.klpkkwe
域名线索:	29条
URL线索:	27条
邮箱线索:	2条
分析日期:	2025年6月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: longnianyx_android.apk
文件大小: 7.7MB
MD5值: 504ac308b136a3f04eec944851476181

SHA1值: 4063e741d16143455a30a9b0a5ca4dbb7c457958
SHA256值: 76571d54c2f12a243c065dce4f6de87243433850d01763029296ea420bf3f0fc

APP 信息

App名称: 龙年优选
包名: com.kydqrj.klpkkwe
主活动Activity: com.bslyun.app.activity.MainActivity
安卓版本名称: 1.0.0
安卓版本: 5

域名线索

域名	服务器信息
testdatalbs.sparta.html5.qq.com	**IP**: 157.255.4.30 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
com.thoughtworks.xstream	没有服务器地理信息.
adblocker.appbsl.net	没有服务器地理信息.
rttgpsreport.map.qq.com	**IP**: 60.28.215.71 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 156.245.67.29 **所属国家**: Hong Kong **地区**: Hong Kong

www.appk6.com	**城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
nlp.map.qq.com	IP: 125.36.181.163 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
api.appbsl.net	IP: 61.48.83.207 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
auth.appbsl.com	没有服务器地理信息.
analytics.map.qq.com	IP: 125.36.181.142 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
log.tbs.qq.com	IP: 124.95.231.218 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
cs.map.qq.com	IP: 125.36.181.142 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

mdc.html5.qq.com	IP: 125.39.196.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
maps.google.com	IP: 142.250.69.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
tbs.imtt.qq.com	IP: 124.163.196.146 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
xml.org	IP: 104.239.142.8 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
debugtbs.qq.com	IP: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ue.indoorloc.map.qq.com	IP: 116.130.224.171 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

schemas.android.com	没有服务器地理信息.
work.weixin.qq.com	**IP**: 106.55.127.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
wx.tenpay.com	**IP**: 220.196.148.65 **所属国家**: China **地区**: Jiangsu **城市**: Yancheng **纬度**: 33.385559 **经度**: 120.125282
api.weibo.com	**IP**: 116.133.8.18 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cc.map.qq.com	**IP**: 125.36.181.145 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
cfg.imtt.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 127.0.0.1 **所属国家**: - **地区**: -

my.wlwx.com	**城市**: - **纬度**: 0.000000 **经度**: 0.000000
apis.map.qq.com	IP: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
lstest.map.qq.com	IP: 116.130.223.83 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
debugx5.qq.com	IP: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ns.adobe.com	没有服务器地理信息.
pms.mb.qq.com	IP: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL**信息**	Url**所在文件**

http://ns.adobe.com/xap/1.0/\u0000	a/e/a/a.java
https://lstest.map.qq.com/nlpdr?sf	c/t/m/g/j.java
https://nlp.map.qq.com/?sf	c/t/m/g/j.java
https://testdatalbs.sparta.html5.qq.com/tr?sf	c/t/m/g/j.java
https://analytics.map.qq.com/?sf	c/t/m/g/j.java
https://cs.map.qq.com/atta?type=1&multi=0	c/t/m/g/s3.java
https://analytics.map.qq.com/tr?mllc	c/t/m/g/s3.java
https://cs.map.qq.com/key	c/t/m/g/r0.java
https://analytics.map.qq.com/tr?mllc	c/t/m/g/r6.java
https://rttgpsreport.map.qq.com/report?type=sdk&key=5e1fe70424035ee83066ac22b24f31dc	c/t/m/g/f.java
https://cc.map.qq.com/?get_c3	c/t/m/g/m0.java
https://ue.indoorloc.map.qq.com/?wl	c/t/m/g/u4.java
https://testdatalbs.sparta.html5.qq.com/tr?wf4	c/t/m/g/h.java
https://analytics.map.qq.com/?wf4	c/t/m/g/h.java
https://testdatalbs.sparta.html5.qq.com/tr?utr	c/t/m/g/g.java
https://analytics.map.qq.com/tr?utr	c/t/m/g/g.java
https://apis.map.qq.com/ws/geocoder/v1/?location=	c/t/m/g/p4.java
http://www.appk6.com	com/bslyun/app/MainApplication.java

https://wx.tenpay.com/	com/bslyun/app/browser/WebViewUtils.java
http://maps.google.com/maps?saddr=	com/bslyun/app/browser/Bridge.java
https://work.weixin.qq.com/kfid/	com/bslyun/app/browser/Bridge.java
https://api.weibo.com/2/users/	com/bslyun/app/component/WeiboComponent.java
https://my.wlwx.com:6016	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://auth.appbsl.com	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
https://wx.tenpay.com/	com/bslyun/app/fragment/WebFragment.java
http://api.appbsl.net/adv/index/appcount?mark=7&type=100	com/bslyun/app/e/a.java
https://adblocker.appbsl.net/index.php?g=port&m=unionadvblock&a=get	com/bslyun/app/service/UpdateFilterIpService.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java

https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
http://com.thoughtworks.xstream/sax/property/configured-xstream	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespaces	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespace-prefixes	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/configured-xstream\	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list\	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/XStreamSource/feature	com/thoughtworks/xstream/io/xml/TraxSource.java
http://schemas.android.com/apk/res/android	com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java

邮箱线索

邮箱地址	所在文件
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java
null@null.xml	com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java

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, O=������������, OU=������������, CN=134422
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-20 05:02:26+00:00
有效期至: 2122-09-14 05:02:26+00:00
发行人: C=CN, O=������������, OU=������������, CN=134422
序列号: 0x400d4482
哈希算法: sha256
md5值: c1a01fb730bdfaecbdddbcc0a7d50a4b
sha1值: f5876f6ef3bd80a8206f2333373c004c7e2c569f
sha256值: bf101544ff9ad7929f8ac9dd4a8d46c3d5c5a711bff51446865a8fcb910f1f35
sha512值: 8b8059b36e57e0a0b7d9952fe63cdd03aaaa7b336a9daf12f113b155524d30ce40c86b144e96cff9f66d284d874b488e3b12e0c8291021b2f6a42d87c503e34f
公钥算法: rsa
密钥长度: 2048
指纹: 396cdd3ccd3943b867697692d196105416dfd890d5273e165591dbf9c3d2207e

硬编码敏感信息

可能的敏感信息
"QQ_AppSecret" : "_QQ_AppSecret"
"SINA_APP_KEY" : "_SINA_APP_KEY"
"WX_AppSecret" : "_WX_AppSecret"
"adset_app_key" : ""
"ali_login_secret_key" : ""

"baid_ai_app_key" : "_baid_ai_app_key"
"baid_ai_secret_key" : "_baid_ai_secret_key"
"baidu_face_api_key" : ""
"baidu_face_secret_key" : ""
"hw_app_key" : "_hw_app_key"
"lebo_app_secret" : "_lebo_app_secret"
"linked_me_key" : ""
"meiqia_app_key" : ""
"mi_app_key" : "_mi_app_key"
"my_app_secret" : ""
"my_master_secret" : ""
"oppo_app_key" : ""
"rongyun_appkey" : ""
"tx_tts_secret_id" : ""
"tx_tts_secret_key" : ""
"umeng_app_key" : ""
"zb_license_key" : ""

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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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
	正	查看Wi-Fi	

android.permission.ACCESS_WIFI_STATE	常	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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.READ_MEDIA_IMAGES	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
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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

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.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.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.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.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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.CLEAR_APP_CACHE	系统需要	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
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.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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	未知	Unknown permission	Unknown permission from android reference

com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.bslyun.app.activity.MainActivity	Schemes: @string/wx_app_id://, @string/u_link_scheme://, um.622017db317aa87760767d8c://, mtjç¦\u0081æ¢å\u0088 é\u0099¤://,
com.bslyun.app.activity.HtmlOpenApp	Schemes: bslapp://,
