MoGua

澳门新葡京 3.8.40.APK 分析报告

APP名称:	澳门新葡京

包名:	com.asdasdasdwww.liveandroid
域名线索:	33条
URL线索:	46条
邮箱线索:	2条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 153923151.apk
文件大小: 153.53MB
MD5值: e91bdb42903a2b32ab04fe118f71a1c2
SHA1值: fc9353fc98aaa4af2670fd4353a0cbe89f354261
SHA256值: 0c855994c46dbc73939f07731d936010be3ab6defe21586a877a33a94de6f53d

APP 信息

App名称: 澳门新葡京
包名: com.asdasdasdwww.liveandroid
主活动Activity: com.sport.SplashActivity
安卓版本名称: 3.8.40
安卓版本: 382

域名线索

域名	服务器信息
acstatic-dun.126.net	**IP**: 221.195.209.99 **所属国家**: China **地区**: Hebei **城市**: Cangzhou **纬度**: 38.316669 **经度**: 116.866669
imweb.xxx.com	**IP**: 130.211.15.150 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mcgw.alipay.com	**IP**: 116.142.245.205 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
imweb.imsystestaedoh.com	没有服务器地理信息.
www.slf4j.org	**IP**: 195.15.222.169 **所属国家**: Switzerland **地区**: Geneve **城市**: Carouge **纬度**: 46.180931 **经度**: 6.138709
www.google.com	**IP**: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
mclient.alipay.com	**IP**: 116.142.245.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
h5.btesth5aogho.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
h5.8btest6aht7uok.com	没有服务器地理信息.

mobilegw-1-64.test.alipay.net	没有服务器地理信息.
da.dun.163.com	**IP**: 59.111.248.82 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
mobilegw.alipay.com	**IP**: 203.209.243.27 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mobilegw.aaa.alipay.net	没有服务器地理信息.
wappaygw.alipay.com	**IP**: 116.142.245.205 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

wbimgsgame.oss-cn-hongkong.aliyuncs.com	**IP**: 47.79.64.227 **所属国家**: United States of America **地区**: California **城市**: San Mateo **纬度**: 37.547424 **经度**: -122.330589
cstaticdun.126.net	**IP**: 111.202.6.32 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobilegw.stable.alipay.net	没有服务器地理信息.
h.trace.qq.com	**IP**: 113.56.189.246 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
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
www.baidu.com	**IP**: 110.242.69.21 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
	IP: 61.240.144.198

h5.m.taobao.com	**所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
en.wikipedia.org	IP: 199.16.158.12 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
playready.directtaps.net	IP: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
schemas.microsoft.com	IP: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
m.alipay.com	IP: 203.209.245.74 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
loggw-exsdk.alipay.com	IP: 110.76.6.82 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

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
soft.imtt.qq.com	**IP**: 61.240.220.107 **所属国家**: China **地区**: Hunan **城市**: Chenzhou **纬度**: 25.799999 **经度**: 113.033333
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

URL线索

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java

http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/util/b.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
https://github.com/yyued/SVGAPlayer-Android	com/opensource/svgaplayer/SVGAParser.java
https://cstaticdun.126.net/api/v2/mobile.v2.10.1.html	com/netease/nis/captcha/CaptchaConfiguration.java
https://da.dun.163.com/sn.gif?d=	com/netease/nis/captcha/h.java
http://acstatic-dun.126.net/tool.min.js	com/netease/nis/captcha/CaptchaWebView.java

http://cstaticdun.126.net/2.14.2/core.v2.14.2.min.js	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net/2.14.2/light.v2.14.2.min.js	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net//2.14.2/images/tipBg@2x.c7a9593.png	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net//2.14.2/images/icon_light@2x.9386248.png	com/netease/nis/captcha/CaptchaWebView.java
https://en.wikipedia.org/wiki/Blend_modes\n//	com/tencent/ugc/videoprocessor/transitions/StereoViewerFilter.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://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://imweb.imsystestaedoh.com:443/im_sys	com/wb/base/bean/user/AppConfigBean.java
http://schemas.android.com/apk/res/android	com/wb/base/widget/cutomertab/SlidingTabLayoutTopConer.java
http://schemas.android.com/apk/res/android	com/wb/base/widget/cutomertab/SlidingTabLayoutGuide.java
http://schemas.android.com/apk/res/android	com/wb/base/widget/cutomertab/MySlidingTabLayout.java
https://wbimgsgame.oss-cn-hongkong.aliyuncs.com/wtfk/upload/1656689067110.png	com/wb/customer/ChatActivity.java
http://soft.imtt.qq.com/browser/tes/feedback.html	com/wb/main/ui/activity/HomeTestActivity.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://mobilegw.alipaydev.com/mgw.htm	i0/i.java

http://www.slf4j.org/codes.html	org/slf4j/a.java
http://schemas.android.com/apk/res/android	r2/r.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/c.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	v7/h.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	v7/s.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	v7/e.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	v7/a.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	v7/l.java
https://www.google.com	w6/c.java
https://mobilegw.alipay.com/mgw.htm	y/a.java
http://xml.apache.org/xslt	y0/f.java
http://xml.apache.org/xslt	k1/a.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	ib/a.java

https://h5.m.taobao.com/mlapp/olist.html	z/a.java
https://www.baidu.com	g7/b.java
https://mcgw.alipay.com/sdklog.do	e0/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	e0/d.java
http://h5.btesth5aogho.com/	t4/d.java
https://h5.8btest6aht7uok.com/	t4/d.java
https://www.baidu.com/	t4/d.java
https://imweb.xxx.com/im_sys/	t4/d.java

邮箱线索

邮箱地址	所在文件
tipbg@2x.c7a9593 icon_light@2x.9386248	com/netease/nis/captcha/CaptchaWebView.java
xxx@email.elided	com/tencent/liteav/base/PiiElider.java

手机线索

手机号	所在文件
	com/tencent/ugc/videoprocessor/transitions/BounceFilter.java

14159265358	
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-08 07:29:28+00:00
有效期至: 2080-04-10 07:29:28+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x7c639cfbdc36df95
哈希算法: sha256
md5值: 30d1653cafba71f76f1a0cddb331ed65
sha1值: 4ed69070ab651eaa674b0e2a39ea77ad8ce87379
sha256值: 9fbb0374fe9c499cdcd3338228b94d270d84733120b3f5305fc68704ffe6e038
sha512值: 59b907c4afe887fac62941ce9a7eb18abf7d57b8930fa4fe78e27d2d91f3f990aca887268f00501849aa1d0c71d97267770302dc0b4a2524c251f5248018ac0d
公钥算法: rsa
密钥长度: 2048
指纹: 2e09806b66f4c90ce7bf86c7e5d45ee51db3db8ec08e977defa5cc97e99470a5

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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.WRITE_MEDIA_STORAGE	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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.READ_MEDIA_IMAGES	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_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	正	防止手机睡眠	允许应用程序防止手机进入睡眠状态

	常		
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.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。
com.asdasdasdwww.liveandroid.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.vivo.notification.permission.BADGE_ICON	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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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
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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference

应用内通信