MoGua

LM_SQPlayer 1.0.17.APK 分析报告

APP名称:	LM_SQPlayer

包名:	com.github.tvbox.osc.lemon.mobile
域名线索:	14条
URL线索:	19条
邮箱线索:	0条
分析日期:	2025年6月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: LMplayer-v1.0.17.apk
文件大小: 35.93MB
MD5值: 4128b6fbf00d85044033d9e056916fc5
SHA1值: 1795b4bd58b0ea5eddfc3d09108fa1a9087c917c
SHA256值: 12394330f8b0a28fce44a142b46588110c48d0232280a629a0704365434bdeaf

APP 信息

App名称: LM_SQPlayer
包名: com.github.tvbox.osc.lemon.mobile
主活动Activity: com.example.lemon_os.MainActivity
安卓版本名称: 1.0.17
安卓版本: 1017

域名线索

域名	服务器信息
aomedia.org	**IP**: 4.78.139.54 **所属国家**: United States of America **地区**: New Jersey **城市**: Newark **纬度**: 40.732277 **经度**: -74.173576
tdsdk.cpatrk.net	**IP**: 116.198.16.249 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
me.cpatrk.net	**IP**: 116.198.14.180 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
issuetracker.google.com	**IP**: 142.250.73.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dashif.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
developer.apple.com	**IP**: 17.253.87.204 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
developer.android.com	**IP**: 142.251.215.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
	IP: 119.29.29.229

dns.qq.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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
docs.flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
ns.adobe.com	没有服务器地理信息.
g.co	**IP**: 142.250.73.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
api.talkingdata.com	**IP**: 116.196.64.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
https://docs.flutter.dev/deployment/android	O2/b.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	Y/u.java
http://g.co/dev/packagevisibility.	Y/A.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	a0/C0154I.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	I/C0074s.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	I/N.java
https://issuetracker.google.com/issues/241760537	I/b0.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	I/C0075t.java
http://ns.adobe.com/xap/1.0/\u0000	N/g.java
https://tdsdk.cpatrk.net/n/a/v1	com/tendcloud/tenddata/aa.java
https://me.cpatrk.net	com/tendcloud/tenddata/a.java
https://api.talkingdata.com/adt/openapi/rest/socialSharing/getShortUrl/v2	com/tendcloud/tenddata/bc.java
https://api.talkingdata.com/adt/openapi/rest/socialSharing/getShortUrl/v2?sign=	com/tendcloud/tenddata/bc.java
https://dns.qq.com	com/tendcloud/tenddata/aj.java
https://dns.qq.com/d?dn=	com/tendcloud/tenddata/aj.java
http://ns.adobe.com/xap/1.0/	G0/a.java

https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/l.java
http://dashif.org/guidelines/trickmode	d0/C0276b.java
http://dashif.org/guidelines/trickmode	e0/C0291e.java
http://dashif.org/guidelines/last-segment-number	e0/C0291e.java
https://github.com/Baseflow/flutter-permission-handler/issues	F1/e.java
https://aomedia.org/emsg/ID3	J0/a.java
https://developer.apple.com/streaming/emsg-id3	J0/a.java

邮箱线索

手机线索

手机号	所在文件
17512775099	v2/AbstractC0757a.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=CN

签名算法: rsassa_pkcs1v15
有效期自: 2025-06-14 04:40:43+00:00
有效期至: 2050-06-08 04:40:43+00:00
发行人: C=CN
序列号: 0x94588ea
哈希算法: sha256
md5值: d619a96ce67d684adc2be8b38dd3ecdf
sha1值: 8b2ed51b71a4346156c529fec44fe62641aa2e0f
sha256值: e7cf940641527eeefbd3dade00b64e5c447453c80948c81bbe5569af10934060
sha512值: 7c2a69dcf4a3e65f258c46bb8b61638c6be481c2a8215087a99c699620c312157d24d897b0b3959bcc2a182934094c9f36823a4412d5c8a71dc0b502ca151d5c
公钥算法: rsa
密钥长度: 2048
指纹: a77238f327be2cf431d2022980ad29b863dc8f585b29f85ef32409115f1a89c1

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_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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_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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
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.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.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。
com.github.tvbox.osc.lemon.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信