



MoGua

绿巨人 1.0.6.APK 分析报告



APP名称:

绿巨人

包名:	app.lvjuren888
域名线索:	21条
URL线索:	56条
邮箱线索:	2条
分析日期:	2025年6月14日
分析平台:	摸瓜APK反编译平台

文件名: ljr106.apk
文件大小: 15.97MB
MD5值: 5998ca7f49ecb0aa8b706ab6b13e8a0c
SHA1值: 7525221909e40e7e005e1d17ab38e36df8a24285
SHA256值: eacc42ff885b048d27198fb7fdae6ffaf1b586c79cc74a7f466b157f97d65e17

i APP 信息

App名称: 绿巨人
包名: app.lvjuren888
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.6
安卓版本: 106

🔍 域名线索

域名	服务器信息
quilljs.com	IP: 216.24.57.253 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.982034.xyz	IP: 103.82.140.152 所属国家: Malaysia 地区: Sabah 城市: Kuala 纬度: 5.633330 经度: 115.949997
ns.adobe.com	没有服务器地理信息.
	IP: 216.239.32.29

crbug.com	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
apis.map.qq.com	IP: 109.244.244.223 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
er.dcloud.io	没有服务器地理信息.
m3w.cn	IP: 220.181.125.253 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ask.dcloud.net.cn	IP: 220.181.125.242 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.google.com	IP: 31.13.81.4 所属国家: Poland 地区: Mazowieckie 城市: Warsaw 纬度: 52.229771 经度: 21.011780
lame.sf.net	IP: 104.18.34.154 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
vq1.biokd.net	IP: 169.254.254.254 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
at.alicdn.com	IP: 106.119.193.229 所属国家: China 地区: Hebei 城市: Tangshan 纬度: 39.633331 经度: 118.183327
er.dcloud.net.cn	IP: 123.207.69.251 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
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

api.974535.xyz	IP: 103.82.140.174 所属国家: Malaysia 地区: Sabah 城市: Kuala 纬度: 5.633330 经度: 115.949997
schemas.android.com	没有服务器地理信息.
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
www.openssl.org	IP: 23.222.143.22 所属国家: Malaysia 地区: Selangor 城市: Cyberjaya 纬度: 2.922500 经度: 101.654999
img.kaiyanapp.com	IP: 220.181.158.230 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
service.dcloud.net.cn	IP: 47.111.67.154 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java

https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://feross.org/opensource >	Mogua Engine V2
https://api.974535.xyz:9002/	Mogua Engine V2
https://api.982034.xyz:9002/	Mogua Engine V2
http://feross.org >	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2
https://quilljs.com	Mogua Engine V2

http://www.w3.org/2000/svg	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
http://img.kaiyanapp.com/255365dbfc2622930eb0cdb33e43abf0.jpeg?imageMogr2/quality/60/format/jpg	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2

https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
http://vq1.biokd.net/live/xiaonaimaoremen.txt	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
http://vq1.biokd.net/live/xiaonaimaoremen.txt	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	Mogua Engine V2
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	Mogua Engine V2
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: CN=lvjuren, OU=lvjuren, O=lvjuren, L=beijing, ST=feijing, C=100000
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-04 04:02:31+00:00
有效期至: 2048-04-27 04:02:31+00:00

发行人: CN=lvjuren, OU=lvjuren, O=lvjuren, L=bejing, ST=feijing, C=100000
 序列号: 0x1
 哈希算法: sha256
 md5值: ee8706e504e2b371594c227fe7011b86
 sha1值: 1715a4a305f318880e9a52151de214f60349122c
 sha256值: f7ef42b064c03f843bcf519e4eeb24c6ca1eb7291d77cd593526ee33312953e0
 sha512值: a446e1da910246ca754942f670c309926615d1597c66fbfc89174206990576f35920af772d07e37e72ddbf72d80015ac147525915fc41d99a338847af5c9974d
 公钥算法: rsa
 密钥长度: 2048
 指纹: 962fa5f823d6a68b3b6075b3e03bc65dc07d82b0955c302586a5b1ba5f118a79

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"

"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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.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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: ctaon8://,

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。