MoGua

R-meta 3.1.0.APK 分析报告



APP名称:	R-meta

包名:	applo.com.shixiyulololoman
域名线索:	20条
URL线索:	25条
邮箱线索:	1条
分析日期:	2024年3月29日
分析平台:	摸瓜反编译平台

文件信息

文件名: 1.apk
文件大小: 93.93MB
MD5值: 34536fa90b34de12853deac657292169
SHA1值: e6945291611efe5435e158ab408d3e4a4026e67a
SHA256值: 9bde9d300c14b091c6f4cb95a47b23f2b4e48a99fb824f35c0fb3903df7b4e51

APP 信息

App名称: R-meta
包名: applo.com.shixiyulololoman
主活动Activity: applo.com.shixiyulololoman.MainActivity
安卓版本名称: 3.1.0
安卓版本: 5

域名线索

域名	服务器信息
api-cn.faceplusplus.com	**IP**: 60.205.234.99 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
stackoverflow.com	**IP**: 151.101.65.69 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
stats.cn.ronghub.com	**IP**: 47.94.172.98 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
s3.amazonaws.com	**IP**: 52.216.89.21 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
www.ietf.org	**IP**: 104.16.45.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api-us.faceplusplus.com	**IP**: 3.97.29.30 **所属国家**: Canada **地区**: Quebec **城市**: Montreal **纬度**: 45.508839 **经度**: -73.587807
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
feedback.cn.ronghub.com	**IP**: 101.200.58.95 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 39.106.1.81

nav.cn.ronghub.com	**所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.webrtc.org	**IP**: 172.217.163.46 **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
dev.w3.org	**IP**: 128.30.52.30 **所属国家**: United States of America **地区**: Massachusetts **城市**: Cambridge **纬度**: 42.365078 **经度**: -71.104523
developer.android.com	**IP**: 172.217.160.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568

data.facegl.com	**IP**: 47.104.165.23 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
tools.ietf.org	**IP**: 104.16.45.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
paulbakaus.com	**IP**: 167.172.18.193 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
api.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
nav2-cn.ronghub.com	**IP**: 139.196.191.67 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
www.gnu.org	**IP**: 209.51.188.116 **所属国家**: United States of America **地区**: Massachusetts **城市**: Somerville

	纬度: 42.387600 **经度**: -71.099503

URL线索

URL信息	Url所在文件
https://stats.cn.ronghub.com/active.json	io/rong/imlib/RongCoreClientImpl.java
http://%s/active.json	io/rong/imlib/RongCoreClientImpl.java
https://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
http://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
https://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
http://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
https://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationDataHolder.java
https://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationDataHolder.java
http://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationDataHolder.java
http://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationDataHolder.java
http://%s	io/rong/imlib/httpdns/HttpDnsClient.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/MinioSliceCompleteRequest.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/StcSliceCompleteRequest.java

http://%s/	io/rong/rtlog/upload/RtLogUploadManager.java
http://%s/	io/rong/rtlog/upload/RtLogTimingUploadConfig.java
https://stats.cn.ronghub.com	io/rong/libcore/BuildConfig.java
http://nav.cn.ronghub.com/navipush.json	io/rong/push/common/PushConst.java
https://feedback.cn.ronghub.com	io/rong/common/dlog/LogEntity.java
https://feedback.cn.ronghub.com	io/rong/common/rlog/RLogConfig.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
https://api-cn.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utils/f.java
https://api-us.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utils/f.java
https://data.facegl.com/appapi/Sticker/index	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/Sticker/high	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/mask/index	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/mask/high	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/gift/index	com/meihu/beautylibrary/constant/a.java
http://data.facegl.com/appapi/face/index	com/meihu/beautylibrary/constant/b.java
http://paulbakaus.com/tutorials/html5/web-audio-on-ios/	Mogua Engine V2
http://stackoverflow.com/questions/24119684	Mogua Engine V2

http://dev.w3.org/html5/spec-author-view/spec.html	Mogua Engine V2
https://www.gnu.org/licenses/>.	Mogua Engine V2
https://www.gnu.org/licenses/>.	Mogua Engine V2
https://www.gnu.org/licenses/>.	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	Mogua Engine V2
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-01	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	lib/x86/libRongRTCLib.so
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/video-content-type	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/video-timing	lib/x86/libRongRTCLib.so
http://tools.ietf.org/html/draft-ietf-avtext-framemarking-07	lib/x86/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdrext/color-space	lib/x86/libRongRTCLib.so
http://www.w3.org/XML/1998/namespace	lib/arm64-v8a/libflutter.so

http://www.w3.org/2000/xmlns/	lib/arm64-v8a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so

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: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2022-12-21 16:02:56+00:00
有效期至: 2052-12-13 16:02:56+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
md5值: 10bd6f9eacb4970edfac75633e559833

sha1值: 4c13565a7476086f01fb82a71b6b788f773f936b
sha256值: 1ad983793f064894bcf4a5d0880e8ae98d195854d9efb06d2c278ae64b88dc9c
sha512值: 56613b9ee9bee211df19f51a58422c0b938db80e9bb2f4f169cd959b6ab0ed871ce44247ed66ebebae8e6669e0fbf284b76e8a18c7fcc52442796b651152bf0f
公钥算法: rsa
密钥长度: 2048
指纹: 16388dfa262647e393186970e11137173f23c4b14632a96efee419a6158e020c

硬编码敏感信息

加壳分析

第三方SDK

名称	分类	URL链接
Flutter	加壳加固, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/449
glide图库	开发辅助	https://reports.exodus-privacy.eu.org/trackers/469

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.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

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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.ACCESS_MEDIA_LOCATION	危险	访问的任何地理位置	允许应用程序访问的任何地理位置持久保存在用户的共享集合
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.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.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.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.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

Manifest.permission.CAPTURE_AUDIO_OUTPUT	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.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.POST_NOTIFICATIONS	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.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
applo.com.shixiyuloloman.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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
applo.com.shixiyuloloman.permission.RONG_ACCESS_RECEIVER	未知	Unknown permission	Unknown permission from android reference

应用内通信

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。