MoGua

红客安全助手 1.0.3.APK 分析报告

HarSine

APP名称:	红客安全助手

包名:	com.hongke.tool
域名线索:	26条
URL线索:	26条
邮箱线索:	0条
分析日期:	2025年2月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 红客安全助手1.0.3.apk

文件大小: 12.13MB
MD5值: 1635262fa291647a903663956e71dc1c
SHA1值: 380b532b241051d9dba29f80d2874ff23f9ad60b
SHA256值: 4df4db6a364bb990bd849de20a1da92d075bfcce6f6a95add8fba1bb94c165e6

APP 信息

App名称: 红客安全助手
包名: com.hongke.tool
主活动Activity: com.hongke.tool.ui.activity.SplashActivity
安卓版本名称: 1.0.3
安卓版本: 103

域名线索

域名	服务器信息
h5.m.taobao.com	**IP**: 125.39.155.189 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
dev.mi.com	**IP**: 123.125.102.202 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
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
mobilegw.alipay.com	IP: 203.209.243.98 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
long.open.weixin.qq.com	IP: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
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: 110.76.6.75

loggw-exsdk.alipay.com	**所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
open.weixin.qq.com	**IP**: 140.207.121.14 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
mobilegw.dl.alipaydev.com	**IP**: 110.75.132.25 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
render.alipay.com	**IP**: 116.136.135.168 **所属国家**: China **地区**: Nei Mongol **城市**: Ordos **纬度**: 39.599998 **经度**: 109.783333
mp.weixin.qq.com	**IP**: 140.207.176.25 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

mobilegwpre.alipay.com	**IP**: 110.75.138.35 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
www.whitehouse.gov	**IP**: 192.0.66.51 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.748425 **经度**: -122.413673
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
share.harsine.com	**IP**: 120.221.212.144 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
www.slf4j.org	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: -

	纬度: 0.000000 **经度**: 0.000000
wappaygw.alipay.com	**IP**: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mcgw.alipay.com	**IP**: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
api.app.harsine.com	**IP**: 120.221.212.144 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
schemas.android.com	没有服务器地理信息.
open.work.weixin.qq.com	**IP**: 157.148.41.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

URL线索

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mobilegw.dl.alipaydev.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/l/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/l/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/m/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.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://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
http://schemas.android.com/apk/res/android	com/hbb20/CountryCodePicker.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://api.app.harsine.com/	com/hongke/tool/BuildConfig.java
https://www.whitehouse.gov	com/hongke/tool/page/StressTestActivity.java
https://share.harsine.com/	com/hongke/tool/ui/xpop/ShareDialog.java
https://mail.	com/hongke/tool/ui/activity/RegisterStep4Activity.java
https://api.app.harsine.com/provision?code=	com/hongke/tool/ui/activity/BrowserActivity.java
https://mail.	com/hongke/tool/ui/activity/PasswordResetActivity.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java

https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s	com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java
https://open.work.weixin.qq.com/native/sso/auth/guide?appid=	com/tencent/wework/api/WWAPIImplLocal.java
https://open.work.weixin.qq.com/sdk/opendata/init_open_data	com/tencent/wework/api/WWAPIImpl.java
https://open.work.weixin.qq.com/sdk/opendata/get_open_data	com/tencent/wework/api/WWAPIImpl.java
https://open.work.weixin.qq.com/native/sso/auth/guide?appid=	com/tencent/wework/api/WWAPIImpl.java
https://www.baidu.com	com/uyl/duser/manager/VersionManager.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
https://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
https://dev.mi.com/console/doc/detail?pId=1822	摸瓜V1引擎

邮箱线索

手机线索

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: CN=hong, OU=ke, O=ke, L=ke, ST=ke, C=ke
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-05 08:37:57+00:00
有效期至: 2050-01-30 08:37:57+00:00
发行人: CN=hong, OU=ke, O=ke, L=ke, ST=ke, C=ke
序列号: 0x1
哈希算法: sha256
md5值: 66a1ad86a008e176484cd764a604549e
sha1值: d3c139cd1b8516e72bf051ef1b06b7e556c0f95c
sha256值: 9ae3cfaa278572d9f656714e45a42998a2bb6a8399e678cb0c76e5116a08979b
sha512值: d144116decf878035df6211dbd794dc8120691bd0a7f28d958893fe933dcd6ee3520a1b5e63ffdaac8ff6ca0dbf653b1d5290e0a27d6683ed1cd656a1cf61527
公钥算法: rsa
密钥长度: 2048
指纹: f094969da6d8880536d8a01a95517d31f4fc71d9a1338c256a9981bc73989ed0

🔑 硬编码敏感信息

可能的敏感信息
"about_author" : "Android yilanyun"
"loading_go_auth" : "Go to Alipay for authorization"
"login_key" : "密钥恢复"
"theme_s3" : "墨绿色"
"loading_go_auth" : "前往支付寶授權"
"loading_go_auth" : "去支付寶授權"
"loading_go_auth" : "去支付宝授权"

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.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.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
	正		

android.permission.ACCESS_WIFI_STATE	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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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_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.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.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。
	危		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

android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	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_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.READ_CLIPBOARD	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
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.hongke.tool.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信