MoGua

全自动记牌器 1.0.APK 分析报告

APP名称: 全自动记牌器

包名:	com.example.imageenhancementandroid
域名线索:	14条
URL线索:	24条
邮箱线索:	1条
分析日期:	2025年7月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 原始记牌器.apk
文件大小: 22.85MB
MD5值: a4945c1537e7727141ec98ba4d1f54ca
SHA1值: 36b0052112152d7b3e93b67b67c59c4328d00114
SHA256值: 32ebcdff13c217d522ab0ed7da9b3b8057273f53d106d1864d5214fc3ce03145

APP 信息

App名称: 全自动记牌器
包名: com.example.imageenhancementandroid
主活动Activity: com.example.imageenhancementandroid.StartActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
cfg.imtt.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
log.tbs.qq.com	**IP**: 124.95.231.218 **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
mp.weixin.qq.com	**IP**: 140.207.191.167 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
tbs.imtt.qq.com	**IP**: 153.99.77.59 **所属国家**: China **地区**: Jiangsu **城市**: Huai'an **纬度**: 33.588612 **经度**: 119.019173
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
mdc.html5.qq.com	**IP**: 125.39.196.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

qzd.jipaiqi.vip	**IP**: 101.43.194.99 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
open.weixin.qq.com	**IP**: 116.128.171.214 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
pms.mb.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
xian.ccwyapp.com	**IP**: 120.46.22.24 **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
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/PmobileActivity.java
http://qzd.jipaiqi.vip/api/sendsms.php	com/example/imageenhancementandroid/PmobileActivity.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/PwdActivity.java
http://qzd.jipaiqi.vip/api/sendsms.php	com/example/imageenhancementandroid/PwdActivity.java
http://qzd.jipaiqi.vip/api/sendsms.php	com/example/imageenhancementandroid/RegActivity.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/RegActivity.java
http://qzd.jipaiqi.vip/api/sendsms.php	com/example/imageenhancementandroid/LoginActivity.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/LoginActivity.java
http://qzd.jipaiqi.vip/api/about.php?id=3	com/example/imageenhancementandroid/HelpActivity.java
http://qzd.jipaiqi.vip/	com/example/imageenhancementandroid/utils/ShareWeixin.java
http://qzd.jipaiqi.vip/api/jpq.php?act=pweixin2&uid=	com/example/imageenhancementandroid/fragment/MemberFragment.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/fragment/MemberFragment.java
http://qzd.jipaiqi.vip/api/jpq.php?act=puser&uid=	com/example/imageenhancementandroid/fragment/MemberFragment.java

http://qzd.jipaiqi.vip/huodong3/	com/example/imageenhancementandroid/fragment/JiangPinFragment.java
http://qzd.jipaiqi.vip/api/about.php?id=1	com/example/imageenhancementandroid/fragment/ThreeFragment.java
http://xian.ccwyapp.com/api/about.php?id=2	com/example/imageenhancementandroid/fragment/KefuFragment.java
http://qzd.jipaiqi.vip/api/about.php?id=4	com/example/imageenhancementandroid/fragment/TwoFragment.java
http://qzd.jipaiqi.vip/huodong3/	com/example/imageenhancementandroid/fragment/TuiguangFragment.java
http://qzd.jipaiqi.vip/api/jpq.php?act=puser&uid=	com/example/imageenhancementandroid/fragment/TuiguangFragment.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/fragment/TuiguangFragment.java
http://qzd.jipaiqi.vip/api/jpq.php?act=puser2	com/example/imageenhancementandroid/fragment/MainFragment.java
http://qzd.jipaiqi.vip/api/jpq.php?act=puser&uid=	com/example/imageenhancementandroid/fragment/MainFragment.java
http://qzd.jipaiqi.vip/api/jpq.php	com/example/imageenhancementandroid/wxapi/WXEntryActivity.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java

https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.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
http://xml.apache.org/xslt	com/orhanobut/logger/LoggerPrinter.java
https://github.com/opencv/opencv/issues/16739	lib/arm64-v8a/libopencv_java4.so
https://github.com/opencv/opencv/issues/5412.	lib/arm64-v8a/libopencv_java4.so
https://github.com/opencv/opencv/issues/21326	lib/arm64-v8a/libopencv_java4.so

邮箱线索

邮箱地址	所在文件
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

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: C=zz, ST=zz, L=zz, O=zz, OU=zz, CN=zz
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-19 10:49:28+00:00
有效期至: 2050-03-13 10:49:28+00:00
发行人: C=zz, ST=zz, L=zz, O=zz, OU=zz, CN=zz
序列号: 0x4b944122
哈希算法: sha256
md5值: e3eeca241b2561d7f5aee0d1fe33657b
sha1值: 1f0b8c1be2717ef9e84efb3e5283d06c14a3b396
sha256值: 9cf6df2c434b84bec6161e51cab5a92b0f1386fefefc971893132ccaf779bf2a
sha512值: f3111f6a3c855f3ba750c563f99bda935dc5714a4772c1f977e1e787871483cfc09bfbe2e141b71b307216695c4994b855fd0366e16239d5c6d4a37804bde633
公钥算法: rsa
密钥长度: 2048
指纹: 698ef84e1ec290b86991555e21a6e816624db38b43703ea9e174ea80fd00522a

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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.permisson.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.ACCESS_SUPERUSER	未知	Unknown permission	Unknown permission from android reference

android.permission.SYSTEM_OVERLAY_WINDOW	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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

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。