MoGua

鹤轩改机 1.2.1.APK 分析报告

APP名称:	鹤轩改机

包名:	com.android.shiwan
域名线索:	6条
URL线索:	9条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: æ”¹æœº.apk
文件大小: 11.47MB
MD5值: 32f58002f3f7922d1f9e3ae37e6b53b8
SHA1值: 76261705bd726c0fc5172da4d81cf19fbbf1fa5b
SHA256值: 7dac326771d49946ec2461df59e3cd6a8917bb6d47aaaf1030600e2f00c21cbb

APP 信息

App名称: 鹤轩改机
包名: com.android.shiwan
主活动Activity: com.gaiji.kiggaiji10.Activity.LoginActivity
安卓版本名称: 1.2.1
安卓版本: 121

域名线索

域名	服务器信息
data.yunshizhi.com	**IP**: 163.197.32.7 **所属国家**: South Africa **地区**: Gauteng **城市**: Johannesburg **纬度**: -26.202271 **经度**: 28.043631
inapps.appsflyer.com	**IP**: 99.84.50.106 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
launches.appsflyer.com	**IP**: 13.227.62.42 **所属国家**: Japan **地区**: Tokyo

	城市: Tokyo **纬度**: 35.689507 **经度**: 139.691696
193.123.249.30	**IP**: 193.123.249.30 **所属国家**: Korea (Republic of) **地区**: Seoul-teukbyeolsi **城市**: Seoul **纬度**: 37.568260 **经度**: 126.977829
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
click.hopemobi.net	**IP**: 54.70.23.234 **所属国家**: United States of America **地区**: Oregon **城市**: Portland **纬度**: 45.523449 **经度**: -122.676208

URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
http://data.yunshizhi.com	com/gaiji/kiggaiji10/Global.java
http://data.yunshizhi.com:9086	com/gaiji/kiggaiji10/Api/ApiClass.java

https://launches.appsflyer.com/api/v6.2/androidevent?app_id=com.dream.dreamtestapp&buildnumber=6.2.3	com/gaiji/kiggaiji10/Util/MyX509.java
https://data.yunshizhi.com/cansu.php	com/gaiji/kiggaiji10/Util/MyX509.java
https://click.hopemobi.net/click?id=32546045&aff=1196&ost=1631711051&click_id=4779cc01148025d47919&android_id=&gaid=84a11a1b-60ca-48d0-a866-9fd0390a114c&aff_sub=ippv	com/gaiji/kiggaiji10/Util/MyX509.java
http://data.yunshizhi.com/Apk/kig.apk	com/gaiji/kiggaiji10/Util/ApkUpdate.java
http://data.yunshizhi.com/cansu.php	com/gaiji/kiggaiji10/Util/MyX509TrustManager.java
https://inapps.appsflyer.com/api/v6.2/androidevent?app_id=com.dream.dreamtestapp&buildnumber=6.2.3	com/gaiji/kiggaiji10/Util/MyX509TrustManager.java
http://data.yunshizhi.com/html/user_terms.html	com/gaiji/kiggaiji10/Fragment/MyFragment.java
http://data.yunshizhi.com	Mogua Engine V1
http://193.123.249.30	Mogua Engine V1

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=AnHui, L=HeFei, O=Company, OU=Department, CN=PPTV, E=875646589@qq.com

签名算法: rsassa_pkcs1v15
有效期自: 2021-09-29 01:42:30+00:00
有效期至: 2049-02-14 01:42:30+00:00
发行人: C=CN, ST=AnHui, L=HeFei, O=Company, OU=Department, CN=PPTV, E=875646589@qq.com
序列号: 0xc8f96c17c8493c81
哈希算法: sha256
md5值: 0b47a6de604369dd59ca846ea0e31342
sha1值: 0d13f159c99ad225b032978ea5d575e34e88461a
sha256值: dffc2031ba23c8cc113ec3da0c7b387fd1f257f4d14387ce40e36be8c3a7347a
sha512值: 1ddf635eebb6b3287665ca5fd5454d6461338c925664175c319c6e9e25df34115a81bea046b8fb5f99f65b3cec62da58d186700aba61a7ff7c483abd76745052

硬编码敏感信息

可能的敏感信息
"LiuKe_Api_Domain" : "http://data.yunshizhi.com"
"YuGang_Api_Domain" : "http://193.123.249.30"
"deskey" : "853b5da1772f55a7710f004ae838a5fd"

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.SET_TIME	系统需要	设定时间	允许应用程序更改手机的时钟时间
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.SET_TIME_ZONE	系统需要	设置时区	允许应用程序更改手机的时区
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.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.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储器	允许应用程序格式化可移动存储
android.Manifest.permission.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用
android.Manifest.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.NET_ADMIN	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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。
com.android.shiwan.andpermission.bridge	未知	Unknown permission	Unknown permission from android reference

应用内通信
