MoGua

执法管理系统 1.0.6.APK 分析报告

APP名称:	执法管理系统

包名:	com.yookey.suzhoucg
域名线索:	27条
URL线索:	25条
邮箱线索:	0条
分析日期:	2024年12月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: SZCG.APK
文件大小: 9.89MB
MD5值: 7dbafa3eaabd2e47b025dc32d5762704
SHA1值: 698ea15681d72b232d3d520bc1870d7a132a9db7
SHA256值: 2aff06b45f77e322a6c5a0da21bf7a4dd164d14afc11e6227c2c854b5c6578d2

APP 信息

App名称: 执法管理系统
包名: com.yookey.suzhoucg
主活动Activity: com.yookey.suzhoucg.activity.SplashActivity
安卓版本名称: 1.0.6
安卓版本: 6

域名线索

域名	服务器信息
58.210.189.53	**IP**: 58.210.189.53 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311390 **经度**: 120.618057
v.map.baidu.com	**IP**: 111.206.209.185 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
d1.client.map.bdimg.com	**IP**: 101.72.203.35 **所属国家**: China **地区**: Hebei

	城市: Tangshan **纬度**: 39.633331 **经度**: 118.183327
skyhookwireless.com	IP: 96.45.82.97 **所属国家**: United States of America **地区**: Virginia **城市**: Reston **纬度**: 38.938862 **经度**: -77.346191
lba.baidu.com	没有服务器地理信息.
vector0.map.bdimg.com	IP: 101.72.203.35 **所属国家**: China **地区**: Hebei **城市**: Tangshan **纬度**: 39.633331 **经度**: 118.183327
app.navi.baidu.com	IP: 111.206.209.213 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
itsdata.map.baidu.com	IP: 111.206.209.180 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
daohang.map.baidu.com	IP: 111.206.209.190 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501

	经度: 116.397232
58.210.114.36	IP: 58.210.114.36 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311390 **经度**: 120.618057
sapi.skyhookwireless.com	IP: 3.0.127.14 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
its.map.baidu.com	IP: 153.37.235.49 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311390 **经度**: 120.618057
wp.map.baidu.com	IP: 111.206.209.185 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
map.baidu.com	IP: 111.206.208.32 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 111.206.209.186 **所属国家**: China **地区**: Beijing

sv0.map.bdimg.com	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
alog.umeng.com	IP: 223.109.148.176 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
share.imap.baidu.com	IP: 111.206.209.119 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
log.umsns.com	IP: 59.82.29.249 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
api.map.baidu.com	IP: 111.206.208.72 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
alog.umeng.co	没有服务器地理信息.
wapmap.baidu.com	IP: 111.206.209.212 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397232
client.map.baidu.com	**IP**: 111.206.209.120 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
j.map.baidu.com	**IP**: 111.206.209.187 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
loc.map.baidu.com	**IP**: 111.206.209.175 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
sv.map.baidu.com	**IP**: 111.206.209.186 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
180.149.144.31	**IP**: 180.149.144.31 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 111.206.209.171

newvector.map.baidu.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

URL线索

URL信息	Url所在文件
http://map.baidu.com/zt/client/index/?fr=sdk_[	com/baidu/mapapi/utils/OpenClientUtil.java
http://api.map.baidu.com/direction?	com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java
http://api.map.baidu.com/place/detail?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/place/search?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://app.navi.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://api.map.baidu.com/geosearch/v2/bound	com/baidu/mapapi/cloud/BoundSearchInfo.java
http://api.map.baidu.com/geosearch/v2/local	com/baidu/mapapi/cloud/LocalSearchInfo.java
http://api.map.baidu.com/geosearch/v2/detail/	com/baidu/mapapi/cloud/DetailSearchInfo.java
http://api.map.baidu.com/geosearch/v2/nearby	com/baidu/mapapi/cloud/NearbySearchInfo.java
http://lba.baidu.com/	com/baidu/location/BDLocation.java
http://%s/%s	com/baidu/location/c/a.java

http://180.149.144.31:8091/offline_loc	com/baidu/location/c/d.java
http://loc.map.baidu.com/offline_loc	com/baidu/location/c/d.java
https://sapi.skyhookwireless.com/wps2/reverse-geo	com/baidu/location/g/b.java
http://skyhookwireless.com/wps/2005\	com/baidu/location/g/b.java
http://loc.map.baidu.com/cc.php	com/baidu/location/e/h.java
http://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/e/h.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/wloc	com/baidu/location/b/k.java
https://sapi.skyhookwireless.com/wps2/location	com/baidu/location/b/k.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/statloc	com/baidu/location/b/o.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/h.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java

http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://log.umsns.com/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://58.210.189.53:4000	com/yookey/suzhoucg/activity/AboutUsActivity.java
http://58.210.114.36:2088/Authorize/Index	com/yookey/suzhoucg/entity/constants/Constants.java
http://client.map.baidu.com/	lib/armeabi/libBaiduMapSDK_base_v4_0_0.so
http://api.map.baidu.com/s	lib/armeabi/libBaiduMapSDK_base_v4_0_0.so
http://api.map.baidu.com/	lib/armeabi/libBaiduMapSDK_base_v4_0_0.so
http://client.map.baidu.com/phpui2/	lib/armeabi/libBaiduMapSDK_base_v4_0_0.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_base_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/RadarService/	lib/armeabi/libBaiduMapSDK_radar_v4_0_0.so
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://v.map.baidu.com/low/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://v.map.baidu.com/indoorinside/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://v.map.baidu.com/high/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://newvector.map.baidu.com/grid_vc/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://vector0.map.bdimg.com/vecdata/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so

http://its.map.baidu.com:8003/its.php	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://wp.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://client.map.baidu.com/footmap/image.php?	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://sv.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://sv0.map.bdimg.com/	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://client.map.baidu.com/phpui2/?	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://client.map.baidu.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://d1.client.map.bdimg.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_map_v4_0_0.so
http://map.baidu.com/su	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://client.map.baidu.com/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui/v1/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://share.imap.baidu.com/ps	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://j.map.baidu.com/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://wapmap.baidu.com/s	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so

http://map.baidu.com/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/s	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui2/v1/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkws/place/v2/detail	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/indoor/v1/	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/direction/v1	lib/armeabi/libBaiduMapSDK_search_v4_0_0.so

邮箱线索

手机线索

手机号	所在文件
15778800000	org/joda/time/chrono/BasicFixedMonthChronology.java
15778800000	org/joda/time/chrono/JulianChronology.java
15778476000	org/joda/time/chrono/GregorianChronology.java
15308640144	org/joda/time/chrono/IslamicChronology.java
18345352118	com/baidu/platform/comapi/util/b.java
13915584075	com/yookey/suzhoucg/activity/ContacterActivity.java

13915584076	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584072	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584077	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584078	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584079	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584070	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584080	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584084	com/yookey/suzhoucg/activity/ContacterActivity.java
13915584098	com/yookey/suzhoucg/activity/ContacterActivity.java

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: OU=yookey
签名算法: rsassa_pkcs1v15
有效期自: 2015-11-24 01:06:39+00:00
有效期至: 2040-11-17 01:06:39+00:00
发行人: OU=yookey
序列号: 0x5653b81f
哈希算法: sha1
md5值: 680db3bb52cd40ba5465a0050e44190d
sha1值: 1301f229f24c1253f037c57f48a58458b5b74923
sha256值: 175d2974135a9b96ffb354e500f561703c369c60082323e78d35a0bb292b39ac

sha512值: 55b67481eb22bb2ec69a9105d25560a424522131a23873262453c7b06200695a2056d172a36d5f902e28a26bdf6f8ca8bb60c170fa0e7511d04e16fe9a7955b4
公钥算法: rsa
密钥长度: 1024
指纹: d4a394155c4a69f58e6b18d75fce8d541b28be55e725530d73688f038d3fce0b

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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
com.android.launcher.permission.READ_SETTINGS	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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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_FINE_LOCATION	危险	精细定位	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

		（GPS）	确定您的位置,并可能消耗额外的电池电量
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.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
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_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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.BAIDU_LOCATION_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码

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
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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

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。