



麦高证券 3.1.8.APK 分析报告



APP名称:

麦高证券

包名:	maigaosec.apk
域名线索:	2条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件名: maigaosec.apk
文件大小: 81.89MB
MD5值: 70226baf15d5a7b2cd9158683bd21975
SHA1值: c10a8fe5ddb5d8fd4dd7a3a726bcd22a44d20cad
SHA256值: 58c96c47f3363979f986bda300843229cbf69cf7fc1221849ba448c0b1b04a8a

i APP 信息

App名称: 麦高证券
包名: maigaosec.apk
主活动Activity: []
安卓版本名称: 3.1.8
安卓版本: 318

🔍 域名线索

域名	服务器信息
www.mob.com	IP: 45.120.103.158 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
www.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

🌐 URL线索

URL信息	Url所在文件
http://www.mob.com/policy/en>http://www.mob.com/policy/en.	Mogua Engine V1
http://www.mob.com/about/policy>http://www.mob.com/about/policy	Mogua Engine V1
https://www.mob.com	Mogua Engine V1
http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en.If	Mogua Engine V1
http://www.mob.com/policy/zh>http://www.mob.com/policy/zh	Mogua Engine V1
http://www.apache.org/licenses/LICENSE-2.0	Mogua Engine V2

邮箱线索

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=086, ST=GUANGDONG, L=SHENZHEN, O=Thinkive, OU=Thinkive, CN=Thinkive
签名算法: rsassa_pkcs1v15
有效期自: 2013-12-21 11:44:17+00:00
有效期至: 2113-11-27 11:44:17+00:00
发行人: C=086, ST=GUANGDONG, L=SHENZHEN, O=Thinkive, OU=Thinkive, CN=Thinkive
序列号: 0x119bdfd8
哈希算法: sha256

md5值: 864bababd26bb694fbd90c08476c88dc
sha1值: 5800a6425ddccdb997322af0dc817cdab77e3a77
sha256值: 3ddf1a3a07f9f720a99dea2021782718929136a3a1fd7e73a3e29474650f7956
sha512值: fb1a660e373dbb5228fae5dfb6f1cc1d3f0915869183353c7bf322dfdf808cc360e3384be8f57d4209d71ece58a15363cf72a818500883cddba1f284ad44718a
公钥算法: rsa
密钥长度: 2048
指纹: 9148802f511ed712907eb2a3442645e0bb4a0ecbf5dafe36b1fabafcc737891a

硬编码敏感信息

可能的敏感信息
"app_function_push_token" : "手机号码"
"forget_gesture_pwd" : "忘记手势密码"
"login_password" : "请输入交易密码"
"login_remember_password" : "记住"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobdemo_authorize_dialog_title" : "服务授权"

"pwd_expired" : "您当前交易密码已变更，本设备指纹登录暂时关闭，请您使用密码登录。如需重新开启指纹登录，请您至"交易首页-指纹登录"重新开通"
"reset_gesture_pwd" : "重新设置手势密码"
"set_gesture_pwd" : "设置手势密码"
"set_gesture_pwd_reason" : "设置手势密码，防止他人未经授权查看"
"set_gesture_pwd_suc" : "设置手势密码成功"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy/en.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_auth_title" : "Service Authority"

"ssak_cmcc_login_one_key" : "Pnonenum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见 http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"</td'>
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

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.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
com.thinkive.android.invest_ha.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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_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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	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.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.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
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（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_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
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.thinkive.investwangxinsec.permission.TKPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.thinkive.investwangxinsec.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.thinkive.im.pushdemo.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.thinkive.investwangxinsec.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.thinkive.android.investwangxinsec.ui.activitys.LauncherActivity	Schemes: wx3d01813e79135a40://, browser://, Hosts: com.thinkive.android.invest_ha, Path Prefixes: /LauncherActivity,
com.thinkive.android.investwangxinsec.ui.activitys.MainActivity	Schemes: talkingdata.f2bd8c577c1a4392be9fcb5af8934f13://, Hosts: token,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent1104542729://,

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。