Evaluation Warning: The document was created with Spire.Doc for Python.

**户籍猎手（ 1.1.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 户籍猎手 |
| 版本 | 1.1.0 |
| 包名 | com.unizone.huji |
| 域名线索 | 98条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年6月15日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 户籍猎手\_1.1.0.apk |
| 文件大小 | 6.25MB |
| MD5值 | af7f769f3e040c7844ee2f4f73437b6c |
| SHA1值 | 16b4ca44d207893ff055ec2d29c967b63bf9ba51 |
| SHA256值 | caf3b20188c4413f2db3e4eca9a1cfa739ea0bbaac199e1bd36c0d41e0e18c58 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 户籍猎手 |
| 包名 | com.unizone.huji |
| 主活动Activity | com.iapp.app.run.mian |
| 安卓版本名称 | 1.1.0 |
| 安卓版本 | 100001 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ptlogin.4399.com | IP: 42.193.129.186 所属国家: China 地区: Beijing 城市: Beijing  |
| openapi.book118.com | IP: 222.187.225.112 所属国家: China 地区: Jiangsu 城市: Suqian  |
| ke.wooffice.net | IP: 47.111.18.15 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.hndyjyfw.gov.cn | IP: 123.6.9.140 所属国家: China 地区: Henan 城市: Zhengzhou  |
| www.wanmeiip.com | IP: 123.57.43.51 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| my.800hr.com | IP: 118.144.89.176 所属国家: China 地区: Beijing 城市: Beijing  |
| scapi.taodingding.com | IP: 120.77.198.179 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| user.chinahr.com | IP: 43.144.202.153 所属国家: China 地区: Beijing 城市: Beijing  |
| www.zbwmy.com | IP: 58.34.1.155 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.weidai.com.cn | IP: 101.71.14.21 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| edms.fcbox.com | IP: 157.148.58.35 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| mayi-api.91ants.com | IP: 208.98.43.13 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| www.yougou.com | IP: 47.93.94.129 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| jiameng.baidu.com | IP: 110.242.68.246 所属国家: China 地区: Hebei 城市: Baoding  |
| xuanhao.myyb100.com | IP: 47.113.106.97 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apiv3.tongbux.com | IP: 123.56.73.151 所属国家: China 地区: Beijing 城市: Beijing  |
| dss.xiongmaopeilian.com | IP: 47.95.70.54 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| agw.4gdh.net | IP: 47.106.112.167 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| i.zhaopin.com | IP: 116.136.189.182 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| m.haiav.com | IP: 172.247.204.111 所属国家: United States of America 地区: California 城市: Los Angeles  |
| www.chinabreed.com | IP: 1.94.73.48 所属国家: China 地区: Beijing 城市: Beijing  |
| queryservice.maka.im | IP: 8.141.27.191 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| shop.sino-life.com | IP: 113.98.237.116 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| bizapi.pezy.cn | 没有服务器地理信息.  |
| login.11h5.com | IP: 124.223.147.45 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| console2.talk-fun.com | IP: 116.136.189.188 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| m.yiwise.com | 没有服务器地理信息.  |
| bdsn.thjy2.com | 没有服务器地理信息.  |
| api.kpjushi.cn | IP: 47.93.95.48 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sso-c.souche.com | IP: 47.110.70.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.00800.com.cn | IP: 119.23.85.144 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| apps.yae920.com | IP: 47.109.179.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.ryzwz.com | IP: 46.175.135.11 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| www.tgcost.com | IP: 139.159.182.3 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.diantoushi.com | IP: 118.25.167.9 所属国家: China 地区: Beijing 城市: Beijing  |
| user.daojia.com | IP: 47.94.171.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| my.baihe.com | IP: 120.53.78.42 所属国家: China 地区: Beijing 城市: Beijing  |
| hxg-api.yd.com.cn | IP: 116.205.76.178 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| m.tk.cn | IP: 120.53.66.36 所属国家: China 地区: Beijing 城市: Beijing  |
| m.egou.com | IP: 125.39.27.204 所属国家: China 地区: Tianjin 城市: Tianjin  |
| test2.p10155.cn | 没有服务器地理信息.  |
| www.tanwan.com | IP: 42.59.4.237 所属国家: China 地区: Liaoning 城市: Dalian  |
| j.xy860.com | 没有服务器地理信息.  |
| lianghao.myyb100.com | IP: 47.115.82.198 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| shop.pinming.cn | IP: 47.110.189.113 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| user.qunar.com | IP: 123.59.180.212 所属国家: China 地区: Beijing 城市: Beijing  |
| m.mxj.com.cn | IP: 47.92.72.34 所属国家: China 地区: Beijing 城市: Beijing  |
| jmwap.ctdsb.net | IP: 61.48.83.229 所属国家: China 地区: Beijing 城市: Beijing  |
| hr.xfcbank.com | 没有服务器地理信息.  |
| www.xxwolo.com | IP: 81.70.125.124 所属国家: China 地区: Beijing 城市: Beijing  |
| w4.duoyi.com | 没有服务器地理信息.  |
| admin.schdmi.com | IP: 47.104.68.216 所属国家: China 地区: Shandong 城市: Qingdao  |
| www.52fzlt.cn | IP: 154.214.132.111 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.pmax.cn | IP: 111.230.153.198 所属国家: China 地区: Beijing 城市: Beijing  |
| cd.abiz.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mp.sfccn.com | IP: 116.198.151.99 所属国家: China 地区: Beijing 城市: Beijing  |
| m.qiuyi.cn | IP: 123.58.224.35 所属国家: China 地区: Beijing 城市: Beijing  |
| www.longone.com.cn | IP: 122.195.53.83 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.jiandan001.com | IP: 172.247.49.243 所属国家: United States of America 地区: California 城市: Los Angeles  |
| console.ytx.net | IP: 101.201.100.172 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| card.10010.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.donews.com | IP: 123.125.216.219 所属国家: China 地区: Beijing 城市: Beijing  |
| passport.fang.com | IP: 124.251.47.96 所属国家: China 地区: Beijing 城市: Beijing  |
| cms.51fenmi.com | IP: 39.98.56.66 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobile.iqihang.com | IP: 123.206.4.208 所属国家: China 地区: Beijing 城市: Beijing  |
| www.12chu.com | IP: 46.175.135.11 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| m.fanli.com | IP: 124.70.121.4 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| gw.aoscdn.com | IP: 125.38.11.91 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.xd.com | IP: 203.107.33.10 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| splus.bianfeng.com | IP: 115.238.30.10 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tel.kuaishang.cn | IP: 45.117.11.51 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| sso1.nlc.cn | IP: 202.96.31.48 所属国家: China 地区: Beijing 城市: Beijing  |
| account.bol.wo.cn | IP: 111.202.245.4 所属国家: China 地区: Beijing 城市: Beijing  |
| www.lanniuh.com | IP: 121.43.193.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m.mop.com | 没有服务器地理信息.  |
| api.zhaotu.com | IP: 47.93.241.251 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.passport.pptv.com | IP: 223.68.136.250 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| user.zixia.com | IP: 47.96.98.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| member.stockstar.com | IP: 119.188.209.65 所属国家: China 地区: Shandong 城市: Zaozhuang  |
| m.10010.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.yichuangtianji.com | IP: 156.250.169.114 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| kingcard.dgunicom.com | IP: 211.95.193.53 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.zoneidc.com | IP: 43.248.189.120 所属国家: China 地区: Jiangsu 城市: Suqian  |
| service.wzhxlx.com | IP: 120.79.7.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| changliao.myyb100.com | IP: 112.74.39.132 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| www.musicdo.cn | IP: 120.79.103.106 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| shop.usr.cn | IP: 61.48.83.207 所属国家: China 地区: Beijing 城市: Beijing  |
| api.qingmang.me | IP: 172.67.194.151 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.lu.com | IP: 101.89.64.50 所属国家: China 地区: Shanghai 城市: Shanghai  |
| slb-sport.vesal.cn | IP: 39.107.84.106 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.365liye.com | IP: 82.157.3.241 所属国家: China 地区: Beijing 城市: Beijing  |
| store.wanmeicun.com | IP: 47.106.147.245 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| u.house.ifeng.com | IP: 8.140.128.31 所属国家: China 地区: Beijing 城市: Beijing  |
| www.hezon.cn | IP: 115.29.240.4 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| elove.darryring.com | IP: 112.84.222.42 所属国家: China 地区: Jiangsu 城市: Huai'an  |
| codingle.cn | IP: 140.143.213.212 所属国家: China 地区: Beijing 城市: Beijing  |
| reg.qun.hk | IP: 81.71.82.151 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/f.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://member.stockstar.com/loginm/Account/SendValidateCode  | 摸瓜V3引擎  |
| http://www.yichuangtianji.com/member.php?a=sms&\_=1445158338&dianhua=  | 摸瓜V3引擎  |
| https://scapi.taodingding.com/getCode?phone=18663841916&token=123&server=0&scene=1  | 摸瓜V3引擎  |
| https://www.donews.com/login/getcode?tel=  | 摸瓜V3引擎  |
| https://my.800hr.com/inc/checkcode/?width=60&high=30&size=12&tm=21m25s13&type=1&channel=2&act=getpho  | 摸瓜V3引擎  |
| http://w4.duoyi.com/p\_user/DoNewActCards.aspx?gate=sw&jsoncallback=jQuery18303232165043277003\_148385  | 摸瓜V3引擎  |
| https://jiameng.baidu.com/portal/com/captcha?ajax=1&device=pc  | 摸瓜V3引擎  |
| http://www.tanwan.com/api/reg\_json\_2019.php?act=3&phone=  | 摸瓜V3引擎  |
| http://m.haiav.com/index.php?m=site&c=public&a=send\_mobile\_code&mobile=  | 摸瓜V3引擎  |
| https://kingcard.dgunicom.com/lsd-message/send/captcha/phone/v1?phoneNumber=  | 摸瓜V3引擎  |
| https://m.lu.com/user/service/login/otp-login-pre-check  | 摸瓜V3引擎  |
| https://account.bol.wo.cn/cuuser/cuauth/smscode?smsType=2&clientId=woemail&mobile=  | 摸瓜V3引擎  |
| http://j.xy860.com/android/invite/getcode/?callback=success\_jsonpCallback&mobile=  | 摸瓜V3引擎  |
| http://www.ryzwz.com/index.php?hm=  | 摸瓜V3引擎  |
| https://www.chinabreed.com/index.php?s=/home/index/getcode.html  | 摸瓜V3引擎  |
| http://edms.fcbox.com/hibox/weixin/getVerifyCode?mobilePhone=  | 摸瓜V3引擎  |
| http://cd.abiz.com/v3validcode?t=1604046053252&currentFindType=1&pageType=7&pn=abiz&validateCode=cur  | 摸瓜V3引擎  |
| https://u.house.ifeng.com/getVerifyCode?\_=0.38838852170651417&\_t=1565612980&verifyCode=  | 摸瓜V3引擎  |
| http://www.xd.com/users/sendWebRegCode?callback=jQuery110208424835141365408\_1600270044866&mobile=  | 摸瓜V3引擎  |
| https://www.yougou.com/my/getMobileCodes.jhtml  | 摸瓜V3引擎  |
| https://ke.wooffice.net/api3/h5/sms\_code?mobile=  | 摸瓜V3引擎  |
| http://sso1.nlc.cn/sso/currency/sendCodeToMobile?mobile=  | 摸瓜V3引擎  |
| http://jmwap.ctdsb.net:8089/amc/client/getAuthCode?mobilephone=  | 摸瓜V3引擎  |
| https://api.passport.pptv.com/snsms/sendcode?\_source=ppsports&apptype=android&appversion=1.0.7.1&dev  | 摸瓜V3引擎  |
| http://www.longone.com.cn/servlet/user/Register?&function=AjaxGetPin1&mo=  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://m.mxj.com.cn/login/getIntentionCode?mobile=  | 摸瓜V3引擎  |
| http://m.egou.com/validate\_phone.htm?phone=  | 摸瓜V3引擎  |
| https://api.kpjushi.cn/union/sendInvalidCodeSms?phone=  | 摸瓜V3引擎  |
| https://www.wanmeiip.com/source/class/captcha/captcha.php?0.41730894602711244validate=  | 摸瓜V3引擎  |
| http://api.qingmang.me/v1/account.sendVerification?&phone=%2B8  | 摸瓜V3引擎  |
| http://lianghao.myyb100.com/webapi/geticode.jsp?userid=  | 摸瓜V3引擎  |
| https://m.tk.cn/member\_api/  | 摸瓜V3引擎  |
| https://login.11h5.com/account/api2.php  | 摸瓜V3引擎  |
| https://sso-c.souche.com/loginApi/getCaptchaUrlByPhone.json?app=tangeche&phone=  | 摸瓜V3引擎  |
| https://apps.yae920.com/login/sendSMS  | 摸瓜V3引擎  |
| http://hr.xfcbank.com/ajax/wap.php?action=get\_authcode&mobile=  | 摸瓜V3引擎  |
| http://www.musicdo.cn/MiniPhone/ashx/Foundation.ashx?MethodName=GetVerificationCode&phoneNumber=  | 摸瓜V3引擎  |
| https://www.weidai.com.cn/regs/mobileCode.json?\_api=reg.mobileCode&\_mock=false&\_stamp=1639512275611&  | 摸瓜V3引擎  |
| http://www.zoneidc.com/user/sendmobi.asp?mobi=  | 摸瓜V3引擎  |
| https://www.xxwolo.com/ccsrv/apph5/sendShortMsg?phone=  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| http://www.365liye.com/API/Site/Member/SendCode?tel=  | 摸瓜V3引擎  |
| https://gw.aoscdn.com/base/passport/v1/api/captcha  | 摸瓜V3引擎  |
| http://api.qingmang.me/v1/account.sendVerification?token=&phone=%2B86  | 摸瓜V3引擎  |
| http://xuanhao.myyb100.com//webapi/geticode.jsp?userid=  | 摸瓜V3引擎  |
| https://www.tgcost.com/myFiles/openLogin/check\_mobile.json?mobile=  | 摸瓜V3引擎  |
| https://store.wanmeicun.com/api/v2/mall/sms  | 摸瓜V3引擎  |
| http://www.zbwmy.com/zbwuser/sendCode/reg?phone=  | 摸瓜V3引擎  |
| http://m.fanli.com/invite/sendverifycode?jsoncallback=jsonp2&pos=601&t=1488608297799&mobile=  | 摸瓜V3引擎  |
| http://mobile.iqihang.com/api/v2/user/send-sms?phone=  | 摸瓜V3引擎  |
| https://card.10010.com/ko-order/messageCaptcha/send?phoneVal=  | 摸瓜V3引擎  |
| https://openapi.book118.com/index.php/api/code/getmobilecode.html?mobile=  | 摸瓜V3引擎  |
| https://api.hndyjyfw.gov.cn/djapi/mobileVerify  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| https://dss.xiongmaopeilian.com/student\_wx/student/send\_sms\_code?country\_code=86&mobile=  | 摸瓜V3引擎  |
| http://m.qiuyi.cn/dengta/Sendmessage/sendCode?mobile=  | 摸瓜V3引擎  |
| http://mayi-api.91ants.com/shared/sms/code?mobile=  | 摸瓜V3引擎  |
| http://bdsn.thjy2.com/index.php?a=getPhoneCode  | 摸瓜V3引擎  |
| https://www.diantoushi.com/user/v2/captcha?mobile=  | 摸瓜V3引擎  |
| http://cms.51fenmi.com/api/base/public/getCode?mobile=  | 摸瓜V3引擎  |
| http://splus.bianfeng.com/index.php?r=findAccount/SendCode&rnd=&a=  | 摸瓜V3引擎  |
| http://bizapi.pezy.cn/qknode/sms/reqSmsCode?df=android&publishid=1003&deviceId=8812baafc8de4fe4&vt=5  | 摸瓜V3引擎  |
| http://shop.sino-life.com/SL\_EFS/memberRegister/sendRegistSmsCode.do?mobile=  | 摸瓜V3引擎  |
| http://www.12chu.com/reg/sendCode.jhtml?mobile=  | 摸瓜V3引擎  |
| https://ptlogin.4399.com/ptlogin/sendPhoneLoginCode.do?phone=  | 摸瓜V3引擎  |
| http://slb-sport.vesal.cn/vesal-sport-prod/v1/app/member/getCode?tellAndEmail=  | 摸瓜V3引擎  |
| https://admin.schdmi.com/api/app/smsCode  | 摸瓜V3引擎  |
| http://tel.kuaishang.cn/cl.php?tel=  | 摸瓜V3引擎  |
| http://shop.usr.cn/index.php?m=Home&c=Api&a=send\_validate\_code&t=0.5346434143828589  | 摸瓜V3引擎  |
| https://mp.sfccn.com/dynamic/user/SMScheck  | 摸瓜V3引擎  |
| https://console.ytx.net/Login/SendPhoneCode  | 摸瓜V3引擎  |
| http://test2.p10155.cn:8075/sendCode.ashx?phonenum=  | 摸瓜V3引擎  |
| https://m.yiwise.com/apiPlatform/verificationCode/send?phoneNumber=  | 摸瓜V3引擎  |
| https://api.zhaotu.com/register/sms.html  | 摸瓜V3引擎  |
| https://hxg-api.yd.com.cn/api/hxg/v2/sms  | 摸瓜V3引擎  |
| http://m.mop.com/phoneValidatemobileNo=  | 摸瓜V3引擎  |
| http://my.baihe.com/Getinterregist/getPhoneVerifyCode?jsonCallBack=jQuery18306001467584540825\_143970  | 摸瓜V3引擎  |
| http://www.52fzlt.cn/api.php?hm=  | 摸瓜V3引擎  |
| https://console2.talk-fun.com/sms/send/captcha  | 摸瓜V3引擎  |
| http://changliao.myyb100.com/webapi/geticode.jsp?userid=  | 摸瓜V3引擎  |
| https://apiv3.tongbux.com/login/send\_SMS?phone=  | 摸瓜V3引擎  |
| http://codingle.cn/api/user/register/tel\_verify?tel=  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| http://user.daojia.com/mobile/getcode?mobile=  | 摸瓜V3引擎  |
| https://queryservice.maka.im/api/v1/verifycodes?type=login&mobile=  | 摸瓜V3引擎  |
| https://reg.qun.hk/v2/captcha/send?phone=  | 摸瓜V3引擎  |
| http://www.pmax.cn/Home/Index/sendcaptcha.html?user=  | 摸瓜V3引擎  |
| https://shop.pinming.cn/mall/api/mall/sendSmsCodeForLogin.htm  | 摸瓜V3引擎  |
| https://service.wzhxlx.com/wwyy/ceping/sendCode?channelId=99&mobile=  | 摸瓜V3引擎  |
| http://i.zhaopin.com/Login/LoginApi/SendBindSms?jsoncallback=jQuery16402676061029242586\_145414394843  | 摸瓜V3引擎  |
| http://m.10010.com/mall-mobile/CheckMessage/captcha?phoneVal=  | 摸瓜V3引擎  |
| https://user.zixia.com/class/CAP/codeshow.php?sid=2090&quhao=86appname=cellphonereg&action=sendcode&  | 摸瓜V3引擎  |
| http://agw.4gdh.net:2001/1.0/4g/account/check\_and\_code?auth\_type=key&data=phone%3D  | 摸瓜V3引擎  |
| https://www.hezon.cn/api/sendjoinvalidatecodebymobile.htm?mb=  | 摸瓜V3引擎  |
| https://elove.darryring.com/api/crm/newGwLogin/getSMSValidCode?phone=  | 摸瓜V3引擎  |
| https://www.lanniuh.com/web-bin/m/weChat/weChatPublic/get\_message\_info?phone=  | 摸瓜V3引擎  |
| https://user.qunar.com/webApi/logincode.jsp  | 摸瓜V3引擎  |
| https://user.chinahr.com/cppt/open/msg/send/smsCode?mobile=  | 摸瓜V3引擎  |
| http://passport.fang.com/loginsendmsm.api?callback=jsonp1475917947591&Service=home-club-web&backurl=  | 摸瓜V3引擎  |
| http://www.00800.com.cn/cnhs/wqproject/index.php?app=public&mod=Passport&act=sendmsg&area\_code=%2B86  | 摸瓜V3引擎  |
| https://account.bol.wo.cn/cuuser/cuauth/smscode  | 摸瓜V3引擎  |
| https://www.jiandan001.com/rest/yonghubiao/ca/register.json  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| pat@pat.net  | bsh/Interpreter.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179878401  | bsh/ParserTokenManager.java  |
| 17179869184  | bsh/ParserTokenManager.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 签名算法: rsassa\_pkcs1v15 有效期自: 2016-07-02 11:43:26+00:00 有效期至: 2098-08-21 11:43:26+00:00 发行人: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 序列号: 0x3435f5c4 哈希算法: sha256 md5值: c118816b9a0f406ba5ba053c67638185 sha1值: ae773917cc7a7523b41e1eb95bed61cf0aa8e3b0 sha256值: ac0d0777ca24956f8d584c69a7fd5d2e4fb88e276d953aec9e29ceeb9aa78e32 sha512值: 4667da273fe54297d8c90136e189f721a4bf15ba360aac00f095756e2ed09e59edcf69e08cddd20c379bff78f3b4d59c0fcb3ad5ed3c93dc472c8a85a40a21f5 公钥算法: rsa 密钥长度: 2048 指纹: 8bbf61332bce2af8264b5b6a580609a347650411f6732d955346f9f5fe76cf86**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**