



挑码助手 1.0.37.APK 分析报告



APP名称:

挑码助手

包名: xiaoTong.TiaoMaZhuShou

域名线索: 17条

URL线索: 17条

邮箱线索: 0条

分析日期: 2025年6月19日

分析平台: [摸瓜APK反编译平台](#)

文件名: dh2024.apk
文件大小: 3.34MB
MD5值: 21f05a33458fa8d1ba73937d2343e1c0
SHA1值: e6ea929417a2c5c53358b2f15e769c95d68cec78
SHA256值: c4240d23fca115a05437fced32507995c443b0754fc0fb031675d25806212674

i APP 信息

App名称: 挑码助手
包名: xiaoTong.TiaoMaZhuShou
主活动Activity: xiaoTong.TiaoMaZhuShou.rg_startup_class
安卓版本名称: 1.0.37
安卓版本: 1

🔍 域名线索

域名	服务器信息
103.133.176.236	IP: 103.133.176.236 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
124.222.124.53	IP: 124.222.124.53 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
aspect-upush.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu

	城市: Nanjing 纬度: 32.061668 经度: 118.777992
gitee.com	IP: 180.76.198.77 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
alogus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
pslog.umeng.com	IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
developer.umeng.com	IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
utoken.umeng.com	IP: 223.109.148.171 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992

ulogs.umengcloud.com	IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ucc.umeng.com	IP: 203.119.169.43 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
yumao.puata.info	IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
plbslog.umeng.com	IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
alogsus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.222666b.com	IP: 154.216.191.134 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
ccs.umeng.com	IP: 110.253.189.200 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
ulogs.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
sss.umeng.com	IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

URL线索

URL信息	Url所在文件
https://pslog.umeng.com/ablog	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/c/b.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/c/b.java

http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://aspect-upush.umeng.com/occa/v1/event/report	com/umeng/analytics/pro/an.java
https://ucc.umeng.com/v2/inn/fetch	com/umeng/analytics/pro/ao.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://alogus.umeng.com	com/umeng/commonsdk/stateless/a.java
https://utoken.umeng.com	com/umeng/umzid/ZIDManager.java
https://yumao.puata.info/anti_logs	com/uyumao/c.java
https://yumao.puata.info/cc_info	com/uyumao/r.java
https://sss.umeng.com/api/v2/al	com/uyumao/q.java

https://ccs.umeng.com/ra	com/uyumao/q.java
https://yumao.puata.info/cc_info	com/uyumao/d.java
http://124.222.124.53:9527/zhusgg.htm	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/admin.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/dbkjcjx.htm	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/zssyjc.htm	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/tuku/ao.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://103.133.176.236/tuku/cs/ao.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/tuku/hk.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://103.133.176.236/tuku/cs/hk.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
https://gitee.com/hb23888/tmzs/raw/master/admin.txt	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
https://www.222666b.com:888/year/2024.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
https://www.222666b.com:888/mo-lottery/2024.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/xaomen/lskjil.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/xaomen/jnkjil.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/aomen/lskjil.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/aomen/jnkjil.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java

http://124.222.124.53:9527/xg/xglskjjl.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
http://124.222.124.53:9527/xg/xgjnkkjl.html	xiaoTong/TiaoMaZhuShou/rg_startup_class.java
https://gitee.com/hb23888/tmzs/raw/master/HKTK.txt	xiaoTong/TiaoMaZhuShou/rg_GongYongZiYuan.java

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, CN=小童
签名算法: rsassa_pkcs1v15
有效期自: 2022-02-05 07:30:53+00:00
有效期至: 2122-01-12 07:30:53+00:00
发行人: C=CN, CN=小童
序列号: 0x69a195c3
哈希算法: sha256
md5值: b1c53db29ee490fda3e035b8fae5b229
sha1值: b7c8ee26b0cbb9e2407fe6e91cc5a6ec450437ef
sha256值: 3d198d617b3962028dcb4be4ec359ecd013b3089625f14000a89ce93b75e15cf
sha512值: 4360b1ea0ef392c1ff26999cf73491e63369333a2aac838959ac59a3a1124c95cf4dd82125e174e7257beb32753916c7364c42a1377b3c3722971a9c05e7ebb5

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.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.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.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.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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

应用内通信