



MoGua

Y助手 M.4.9.APK 分析报告



APP名称:

Y助手

包名: c18.semag.sulpo.moc.af066b4.m0

域名线索: 17条

URL线索: 11条

邮箱线索: 0条

分析日期: 2025年7月7日

分析平台: [摸瓜APK反编译平台](#)

文件名: base.apk
文件大小: 14.89MB
MD5值: 52d4125c08372ba5639a6e2db0bf513b
SHA1值: d6f52e56f052c368595d94ee1af64b57f8ed8a06
SHA256值: fc453b456ab6daf9e16631d629e3551d8a92da7fe04b295070a3e83913e757dd

i APP 信息

App名称: Y助手
包名: c18.semag.sulpo.moc.af066b4.m0
主活动Activity: com.yyong.mirror.plugin.MainActivity
安卓版本名称: M.4.9
安卓版本: 39

🔍 域名线索

域名	服务器信息
cnlogs.umeng.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
cdndy.multiopen.cn	IP: 222.134.1.29 所属国家: China 地区: Shandong 城市: Binzhou 纬度: 37.366619 经度: 118.015182
	IP: 106.75.76.62 所属国家: China 地区: Shanghai

lrqd.wasair.com	城市: Shanghai 纬度: 31.224333 经度: 121.468948
infotrack.gdt.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
developer.umeng.com	IP: 59.82.31.92 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
ulogs.umeng.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
pslog.umeng.com	IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
alogus.umeng.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

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
aspect-upush.umeng.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
alogsus.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
mix.pangolin-sdk-toutiao.com	IP: 175.19.126.234 所属国家: China 地区: Jilin 城市: Changchun 纬度: 43.880001 经度: 125.322777
resolve.umeng.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
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
upd.donapp.cn	IP: 121.199.60.204 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
beian.miit.gov.cn	IP: 112.84.222.56 所属国家: China 地区: Jiangsu 城市: Huai'an 纬度: 33.588612 经度: 119.019173

 URL线索

URL信息	Url所在文件
https://upd.donapp.cn/chkversion.php	com/yyong/mirror/plugin/b/b.java
https://lrqd.wasair.com/?signDirect=1	com/yyong/mirror/plugin/b/b.java
http://infotrack.gdt.qq.com/game_center	com/yyong/mirror/plugin/b/b.java
https://cdndy.multiopen.cn/static_api/1/pkgBroadcastNum.json	com/yyong/mirror/plugin/b/b.java

https://mix.pangolin-sdk-toutiao.com/api/hybrid/v1/event	com/yyong/mirror/plugin/b/b.java
https://beian.miit.gov.cn/	com/yyong/mirror/plugin/b/b.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/l.java
https://aspect-upush.umeng.com/occa/v1/event/report	com/umeng/analytics/pro/aq.java
https://cnlogs.umeng.com/ext_event	com/umeng/analytics/pro/aq.java
https://cnlogs.umeng.com/uapp_ekverr_logs	com/umeng/analytics/pro/aq.java
https://resolve.umeng.com/resolve	com/umeng/analytics/pro/by.java
https://ucc.umeng.com/v2/inn/fetch	com/umeng/analytics/pro/ar.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.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/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://developer.umeng.com/docs/119267/detail/118637	com/umeng/commonsdk/debug/UMLogCommon.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.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

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: True
找到 1 个唯一证书
主题: C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-29 07:12:39+00:00
有效期至: 2050-06-23 07:12:39+00:00
发行人: C=CN
序列号: 0x1e7d1fad
哈希算法: sha256
md5值: b9e0ad65fbb549591281204d4c6434ca
sha1值: 59ef9f4d63d486eb5e84f13cf136a5bdcf97d4bd
sha256值: 22fff31db659acd5530114351e9d2140214fbd9b79f82064ade7fb3f7d2bf37a
sha512值: 3ca39e63b4fee57c3370531a960bbe0e125a0fadebc06650d4757f639c12630896b82fc6a43862110c3720074b1ed8760e7994e0c916b923842a7cbc09ba6fdb
公钥算法: rsa
密钥长度: 2048
指纹: 1517b5629d7c2145741a3c251577e1740621c5b5b2c60526d024e0211fd0d538

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

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。