MoGua

牧兰优选 1.1.6.APK 分析报告

牧兰优选

APP名称:	牧兰优选

包名:	com.dbzvgk.stfttw
域名线索:	11条
URL线索:	8条
邮箱线索:	0条
分析日期:	2025年2月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: mlyx.apk
文件大小: 22.18MB
MD5值: ee2a179b466b788c2284eed6f125ca7e
SHA1值: 5fd4499f0815d9129ce3e01ac84cefac2ea6cacf
SHA256值: 4490edd11bb1763958aed4fff87eddcbbcdb24ce7eb4106c56f7990ae39f7fd5

APP 信息

App名称: 牧兰优选
包名: com.dbzvgk.stfttw
主活动Activity: com.googlecnx.androidcnx.MainActivity
安卓版本名称: 1.1.6
安卓版本: 3

域名线索

域名	服务器信息
log.tbs.qq.com	**IP**: 109.244.244.32 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
h5.mulanny.com	**IP**: 211.149.185.85 **所属国家**: China **地区**: Sichuan **城市**: Chengdu **纬度**: 30.666670 **经度**: 104.066673
tbsrecovery.imtt.qq.com	**IP**: 109.244.244.237 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397232
soft.tbs.imtt.qq.com	IP: 119.167.147.86 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
cfg.imtt.qq.com	IP: 109.244.173.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mqqad.html5.qq.com	IP: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
debugx5.qq.com	IP: 175.27.9.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
debugtbs.qq.com	IP: 175.27.9.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 109.244.173.227

pms.mb.qq.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mdc.html5.qq.com	**IP**: 175.27.9.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
china-dna.com	**IP**: 116.62.238.180 **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
https://china-dna.com	com/googlecnx/androidcnx/MainActivityX.java
http://h5.mulanny.com	com/googlecnx/androidcnx/MainActivity.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java

https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/m.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.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: False
找到 1 个唯一证书
主题: C=20bd0f88, ST=20bd0f88, L=20bd0f88, O=20bd0f88, OU=20bd0f88, CN=20bd0f88
签名算法: rsassa_pkcs1v15
有效期自: 2023-03-25 02:00:13+00:00
有效期至: 2023-06-23 02:00:13+00:00
发行人: C=20bd0f88, ST=20bd0f88, L=20bd0f88, O=20bd0f88, OU=20bd0f88, CN=20bd0f88
序列号: 0x14f3cd40
哈希算法: sha256
md5值: 0067773a447159cd34ca4f101bbbee63
sha1值: af71f1e5b868acb77367f04f54a9f55989ba4e1d
sha256值: 451ad875db773a07273eddbbb7e852718d9622f8a78a3498852c84968d121cb1
sha512值: 83dd46bf6cd0013d930faa033bd35cffe9053714c6c9dc6bbb54363a49d22455a2229ae5e41119cdac05549979f590505b51390225674c970430c2363f2938f7
公钥算法: rsa
密钥长度: 2048
指纹: d99ebf28b953c2ff5ceddd2021ed06f1bd5cc880c0c296ceef63163c9c297cea

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.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.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.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

应用内通信