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

**TTPod（ 6.6.2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 | TTPod |
| 版本 | 6.6.2 |
| 包名 | com.sds.android.ttpod |
| 域名线索 | 71条 |
| URL线索 | 80条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | apk202752.apk |
| 文件大小 | 8.55MB |
| MD5值 | d10d0291f88432a3bb11b8a0dc56b3e0 |
| SHA1值 | 355054c83e7f7acf7e9d241bbbca0c3264f2a4f1 |
| SHA256值 | eda05340ca664f1d83e5e685f5e0e573dd81b1922650284d0f3b858a4945870c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TTPod |
| 包名 | com.sds.android.ttpod |
| 主活动Activity | .EntryActivity |
| 安卓版本名称 | 6.6.2 |
| 安卓版本 | 6620 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cgi.qplus.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| testmobile.qq.com | 没有服务器地理信息. |
| weibo.com | IP: 180.149.138.246  所属国家: China  地区: Beijing  城市: Beijing |
| picdown.ttpod.cn | 没有服务器地理信息. |
| qzs.qq.com | IP: 182.254.48.69  所属国家: China  地区: Guangdong  城市: Shenzhen |
| so.ard.iyyin.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mta.oa.com | IP: 193.123.33.15  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| v2.ttus.ttpod.com | 没有服务器地理信息. |
| ttus.ttpod.com | 没有服务器地理信息. |
| openmobile.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| feedback.ttpod.itlily.com | IP: 218.205.72.4  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| v1.ard.update.itlily.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alog.umeng.co | 没有服务器地理信息. |
| openbox.mobilem.360.cn | IP: 180.163.251.81  所属国家: China  地区: Shanghai  城市: Shanghai |
| quan.dongting.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| upload.api.weibo.com | IP: 49.7.37.107  所属国家: China  地区: Beijing  城市: Beijing |
| wspeed.qq.com | 没有服务器地理信息. |
| ting.hotchanson.com | 没有服务器地理信息. |
| www.dongting.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wm.shouji.360.cn | 没有服务器地理信息. |
| appsupport.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| api.show.dongting.com | 没有服务器地理信息. |
| sdk.open.phone.igexin.com | IP: 183.131.7.102  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| webpresence.qq.com | IP: 121.51.142.60  所属国家: China  地区: Guangdong  城市: Shenzhen |
| weixin.qq.com | IP: 101.89.38.155  所属国家: China  地区: Shanghai  城市: Shanghai |
| lrc.ttpod.com | 没有服务器地理信息. |
| d1.ttpod.com | 没有服务器地理信息. |
| xmlpull.org | IP: 74.50.61.58  所属国家: United States of America  地区: Texas  城市: Dallas |
| api.skin.ttpod.com | 没有服务器地理信息. |
| ae.hotchanson.com | 没有服务器地理信息. |
| oc.umeng.co | 没有服务器地理信息. |
| t2.qpic.cn | IP: 43.137.223.97  所属国家: China  地区: Beijing  城市: Beijing |
| mta.qq.com | IP: 123.125.9.115  所属国家: China  地区: Beijing  城市: Beijing |
| api.weibo.com | IP: 49.7.37.118  所属国家: China  地区: Beijing  城市: Beijing |
| client.api.ttpod.com | 没有服务器地理信息. |
| appact.qzone.qq.com | IP: 182.254.50.22  所属国家: China  地区: Guangdong  城市: Shenzhen |
| www.tudou.com | IP: 106.11.43.158  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pingma.qq.com | IP: 119.45.78.184  所属国家: China  地区: Beijing  城市: Beijing |
| test.openmobile.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| advise.ttpod.cn | 没有服务器地理信息. |
| www.zip | 没有服务器地理信息. |
| v1.ard.y.itlily.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| graph.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| bbs.dongting.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| star.dongting.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ear.ttpod.com | 没有服务器地理信息. |
| pic.ttpod.cn | 没有服务器地理信息. |
| www.myapp.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| s.p.qq.com | IP: 14.215.158.27  所属国家: China  地区: Guangdong  城市: Shenzhen |
| open.weibo.cn | IP: 49.7.37.118  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 128.30.52.100  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| open.t.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| loc.map.baidu.com | IP: 111.206.209.174  所属国家: China  地区: Beijing  城市: Beijing |
| www.ttpod.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alog.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Beijing  城市: Beijing |
| v1.ard.q.itlily.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| collect.log.ttpod.com | 没有服务器地理信息. |
| skin.ard.ttpod.com | 没有服务器地理信息. |
| wmstat.com | IP: 101.199.103.210  所属国家: China  地区: Beijing  城市: Beijing |
| cgi.connect.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| msg.shouji.360.cn | IP: 180.163.251.69  所属国家: China  地区: Shanghai  城市: Shanghai |
| v1.ard.h.itlily.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| v1.ard.yy.itlily.com | 没有服务器地理信息. |
| so.bq.yymommy.com | 没有服务器地理信息. |
| fm.api.ttpod.com | 没有服务器地理信息. |
| v1.ard.tj.itlily.com | IP: 203.119.201.178  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ayyc.ttpod.com | 没有服务器地理信息. |
| api.busdh.com | 没有服务器地理信息. |
| oc.umeng.com | IP: 203.119.128.55  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| shouji.360.cn | IP: 180.163.237.195  所属国家: China  地区: Shanghai  城市: Shanghai |
| wx.dl.baofeng.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://alog.umeng.com/app\_logs | com/umeng/a/h.java |
| http://alog.umeng.co/app\_logs | com/umeng/a/h.java |
| http://oc.umeng.com/check\_config\_update | com/umeng/a/h.java |
| http://oc.umeng.co/check\_config\_update | com/umeng/a/h.java |
| http://msg.shouji.360.cn/getWeishiApk.php?para=%s | com/qihoo360/mobilesafe/sdk/apk/MobileSafeApkManager.java |
| http://wm.shouji.360.cn/getAdInfo | com/qihoo360/union/c/a/a.java |
| http://wmstat.com/union/other.htm | com/qihoo360/union/c/a/a.java |
| http://wmstat.com/union/down.htm | com/qihoo360/union/c/a/a.java |
| http://wmstat.com/union/install.htm | com/qihoo360/union/c/a/a.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/stat/StatConfig.java |
| http://mta.qq.com/ | com/tencent/stat/StatService.java |
| http://mta.oa.com/ | com/tencent/stat/StatService.java |
| https://open.t.qq.com/cgi-bin/oauth2/authorize?client\_id= | com/tencent/weibo/sdk/android/component/Authorize.java |
| http://www.tudou.com/programs/view/b-4VQLxwoX4/ | com/tencent/weibo/sdk/android/component/MainPage\_Activity.java |
| http://t2.qpic.cn/mblogpic/9c7e34358608bb61a696/2000 | com/tencent/weibo/sdk/android/component/MainPage\_Activity.java |
| http://t2.qpic.cn/mblogpic/9c7e34358608bb61a696/2000 | com/tencent/weibo/sdk/android/component/GeneralInterfaceActivity.java |
| http://cgi.qplus.com/report/report | com/tencent/jsutil/ReportUtils.java |
| http://cgi.connect.qq.com/qqconnectutil/sdk | com/tencent/jsutil/ReportUtils.java |
| http://s.p.qq.com/pub/check\_bizup | com/tencent/jsutil/JsConfig.java |
| http://s.p.qq.com/pub/check\_bizup?qver= | com/tencent/connect/a/b.java |
| http://qzs.qq.com/open/mobile/rate/sdk\_rate.html? | com/tencent/open/SocialApiIml.java |
| http://appact.qzone.qq.com/appstore\_activity\_task\_pcpush\_sdk | com/tencent/open/TaskGuide.java |
| http://wspeed.qq.com/w.cgi | com/tencent/open/cgireport/ReportManager.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com/open/mobile/brag/sdk\_brag.html? | com/tencent/sdkutil/ServerSetting.java |
| https://openmobile.qq.com/ | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/sdkutil/ServerSetting.java |
| http://wspeed.qq.com/w.cgi | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/sdkutil/ServerSetting.java |
| http://qzs.qq.com/open/mobile/not\_support.html? | com/tencent/sdkutil/ServerSetting.java |
| https://test.openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/sdkutil/ServerSetting.java |
| http://testmobile.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/sdkutil/ServerSetting.java |
| http://testmobile.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/sdkutil/ServerSetting.java |
| https://test.openmobile.qq.com/ | com/tencent/sdkutil/ServerSetting.java |
| http://testmobile.qq.com/open/mobile/brag/sdk\_brag.html? | com/tencent/sdkutil/ServerSetting.java |
| http://testmobile.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/sdkutil/ServerSetting.java |
| http://test.openmobile.qq.com | com/tencent/sdkutil/ServerSetting.java |
| http://www.myapp.com/forward/a/45592?g\_f=990935 | com/tencent/tauth/Tencent.java |
| http://webpresence.qq.com/getonline?Type=1& | com/tencent/tauth/Tencent.java |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/tauth/Tencent.java |
| https://openmobile.qq.com/ | com/tencent/tauth/Constants.java |
| https://openmobile.qq.com/weiyun/download\_music | com/tencent/tauth/DownloadFileFromWeiyun.java |
| https://openmobile.qq.com/weiyun/download\_photo | com/tencent/tauth/DownloadFileFromWeiyun.java |
| https://openmobile.qq.com/weiyun/get\_photo\_thumb | com/tencent/tauth/DownloadFileFromWeiyun.java |
| https://openmobile.qq.com/weiyun/download\_video | com/tencent/tauth/DownloadFileFromWeiyun.java |
| http://loc.map.baidu.com/sdk.php | com/baidu/location/LocationClient.java |
| http://loc.map.baidu.com/sdk\_ep.php | com/baidu/location/j.java |
| http://loc.map.baidu.com/sdk.php | com/baidu/location/j.java |
| https://graph.qq.com/oauth2.0/authorize?scope=upload\_pic,add\_topic,get\_user\_info&client\_id=100240447&display=mobile&response\_type=code&redirect\_uri=ttus.ttpod.com/thirdlogin/qq | com/sds/android/sdk/core/usersystem/Authorize.java |
| https://api.weibo.com/oauth2/authorize?scope=follow\_app\_official\_microblog&forcelogin=true&client\_id=3374293008&display=mobile&redirect\_uri=http://ttus.ttpod.com/thirdlogin/sina | com/sds/android/sdk/core/usersystem/Authorize.java |
| http://ttus.ttpod.com/ | com/sds/android/sdk/core/usersystem/Authorize.java |
| http://feedback.ttpod.itlily.com/bug | com/sds/android/sdk/core/b/a.java |
| http://collect.log.ttpod.com/ttpod\_client/index.html | com/sds/android/sdk/core/statistic/IStatisticCommit.java |
| http://v1.ard.update.itlily.com/version | com/sds/android/ttpod/app/modules/version/VersionUpdateModule.java |
| http://v1.ard.tj.itlily.com/ttpod?a=getnewttpod | com/sds/android/ttpod/app/modules/b/a.java |
| http://v1.ard.tj.itlily.com/indexchannel/list?sv=6.0 | com/sds/android/ttpod/app/modules/b/a.java |
| http://so.ard.iyyin.com/v2/songs/singersearch | com/sds/android/ttpod/app/modules/b/a.java |
| http://fm.api.ttpod.com | com/sds/android/ttpod/app/modules/b/a.java |
| http://v1.ard.h.itlily.com/new/plaza | com/sds/android/ttpod/app/modules/b/a.java |
| http://api.show.dongting.com/public/room\_list?size=32 | com/sds/android/ttpod/app/modules/c/b.java |
| http://api.busdh.com/market-api | com/sds/android/ttpod/app/modules/c/b.java |
| http://v1.ard.tj.itlily.com/screen | com/sds/android/ttpod/app/modules/e/d.java |
| http://v1.ard.h.itlily.com/favorites | com/sds/android/ttpod/app/modules/a/c.java |
| http://v1.ard.y.itlily.com/favorites | com/sds/android/ttpod/app/modules/a/c.java |
| http://v1.ard.y.itlily.com/friends | com/sds/android/ttpod/app/modules/d/b.java |
| http://v1.ard.tj.itlily.com/recommend | com/sds/android/ttpod/app/modules/d/c.java |
| http://v1.ard.yy.itlily.com/shake | com/sds/android/ttpod/app/modules/d/c.java |
| http://v1.ard.y.itlily.com/user | com/sds/android/ttpod/app/modules/d/c.java |
| http://v2.ttus.ttpod.com | com/sds/android/ttpod/app/modules/d/c.java |
| http://v2.ttus.ttpod.com/ttus/user | com/sds/android/ttpod/app/modules/d/c.java |
| http://v1.ard.y.itlily.com/friends | com/sds/android/ttpod/app/modules/d/c.java |
| http://v1.ard.q.itlily.com/notice | com/sds/android/ttpod/app/modules/d/c.java |
| http://v1.ard.q.itlily.com/collect | com/sds/android/ttpod/app/modules/d/a.java |
| http://so.ard.iyyin.com/albums | com/sds/android/ttpod/app/modules/search/a.java |
| http://ayyc.ttpod.com | com/sds/android/ttpod/app/modules/search/a.java |
| http://so.ard.iyyin.com/suggest.do | com/sds/android/ttpod/app/modules/search/a.java |
| http://xmlpull.org/v1/doc/ | com/sds/android/ttpod/app/modules/search/a/a.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/sds/android/ttpod/app/modules/search/a/a.java |
| http://www.w3.org/XML/1998/namespace | com/sds/android/ttpod/app/modules/search/a/a.java |
| http://www.w3.org/2000/xmlns/ | com/sds/android/ttpod/app/modules/search/a/a.java |
| www.zip | com/sds/android/ttpod/app/modules/core/c/b/e.java |
| http://v2.ttus.ttpod.com/ttus/user | com/sds/android/ttpod/app/modules/core/e/a.java |
| http://ttus.ttpod.com/third/login/qq | com/sds/android/ttpod/app/modules/core/e/a.java |
| http://ttus.ttpod.com/third/login/sina | com/sds/android/ttpod/app/modules/core/e/a.java |
| http://ae.hotchanson.com/user/info/ | com/sds/android/ttpod/app/modules/core/audioeffect/c.java |
| http://ae.hotchanson.com/public/query\_by\_song\_id | com/sds/android/ttpod/app/modules/core/audioeffect/c.java |
| http://ae.hotchanson.com/ae/pick/ | com/sds/android/ttpod/app/modules/core/audioeffect/c.java |
| http://ae.hotchanson.com/ae/bind/ | com/sds/android/ttpod/app/modules/core/audioeffect/c.java |
| http://lrc.ttpod.com/down? | com/sds/android/ttpod/app/support/search/task/b.java |
| http://lrc.ttpod.com/search? | com/sds/android/ttpod/app/support/search/task/b.java |
| http://picdown.ttpod.cn/picsearch? | com/sds/android/ttpod/app/support/search/task/c.java |
| http://lrc.ttpod.com/report? | com/sds/android/ttpod/app/support/search/task/d.java |
| http://picdown.ttpod.cn/picreport? | com/sds/android/ttpod/app/support/search/task/d.java |
| www.ttpod.com | com/sds/android/ttpod/activities/SkinInfoActivity.java |
| http://advise.ttpod.cn/m.do | com/sds/android/ttpod/activities/setting/FeedbackActivity.java |
| http://quan.dongting.com | com/sds/android/ttpod/activities/setting/AboutActivity.java |
| http://weibo.com/ittpod | com/sds/android/ttpod/activities/setting/AboutActivity.java |
| http://weixin.qq.com/r/YHXPwBXE8iuNhwSjnyBE | com/sds/android/ttpod/activities/setting/AboutActivity.java |
| http://bbs.dongting.com | com/sds/android/ttpod/activities/setting/AboutActivity.java |
| http://pic.ttpod.cn/singerpic | com/sds/android/ttpod/b/b.java |
| http://quan.dongting.com/do.html?m=music&a=details&id= | com/sds/android/ttpod/b/k.java |
| http://ttus.ttpod.com/thirdlogin/sina?code=6aef2d447c0e33be42045115551fbcc4 | com/sds/android/ttpod/share/b/f.java |
| https://open.weibo.cn/oauth2/authorize | com/sds/android/ttpod/share/b/f.java |
| http://ttus.ttpod.com/thirdlogin/qq?code=beed767ac431765bb6f66c4a9a437029 | com/sds/android/ttpod/share/b/e.java |
| https://openmobile.qq.com/oauth2.0/authorize | com/sds/android/ttpod/share/b/e.java |
| http://www.ttpod.com/ | com/sds/android/ttpod/share/b/d.java |
| https://open.t.qq.com/cgi-bin/oauth2/authorize | com/sds/android/ttpod/share/b/d.java |
| http://pic.ttpod.cn/singerpic | com/sds/android/ttpod/share/c/d.java |
| https://open.t.qq.com/api/t/add\_pic | com/sds/android/ttpod/share/a/f.java |
| http://www.ttpod.com | com/sds/android/ttpod/share/a/g.java |
| https://graph.qq.com/share/add\_share | com/sds/android/ttpod/share/a/g.java |
| https://upload.api.weibo.com/2/statuses/update.json | com/sds/android/ttpod/share/a/i.java |
| https://upload.api.weibo.com/2/statuses/upload.json | com/sds/android/ttpod/share/a/i.java |
| https://api.weibo.com/2/friendships/show.json | com/sds/android/ttpod/share/a/i.java |
| https://api.weibo.com/2/friendships/create.json | com/sds/android/ttpod/share/a/i.java |
| http://www.dongting.com/?song\_id= | com/sds/android/ttpod/share/d/b.java |
| http://www.dongting.com/#a=searchlist&q= | com/sds/android/ttpod/share/d/b.java |
| http://wx.dl.baofeng.com/mobile/ttpod/AndroidStorm\_DEVICE\_CPU\_TYPE.apk | com/sds/android/ttpod/component/video/VideoPlayManager.java |
| http://bbs.dongting.com | com/sds/android/ttpod/component/c/a/m.java |
| http://api.busdh.com/market-api/api/sdk?sdk\_category=%d&version=%s | com/sds/android/ttpod/component/advertisement/b.java |
| http://xmlpull.org/v1/doc/features.html#indent-output | com/sds/android/ttpod/component/g/b.java |
| http://picdown.ttpod.cn/picsearch? | com/sds/android/ttpod/adapter/PictureManagerAdapter.java |
| http://shouji.360.cn/360safe/101153/360MobileSafe.apk | com/sds/android/ttpod/ThirdParty/liangdian/App360Manager.java |
| http://openbox.mobilem.360.cn/channel/getUrl?src=430641&app=360box | com/sds/android/ttpod/ThirdParty/guide/GuidePage.java |
| http://so.bq.yymommy.com/appsearch/#a=ss&q= | com/sds/android/ttpod/fragment/main/SearchResultFragment.java |
| http://ear.ttpod.com/ | com/sds/android/ttpod/fragment/main/market/HeadsetFragment.java |
| http://d1.ttpod.com/download/android/f40/TTShow\_Android.apk | com/sds/android/ttpod/fragment/main/market/BeautyFragment.java |
| http://v2.ttus.ttpod.com/ttus/user | com/sds/android/ttpod/fragment/musiccircle/HeaderPostListFragment.java |
| http://skin.ard.ttpod.com/mobile/skin.html? | com/sds/android/ttpod/fragment/skinmanager/WebSkinFragment.java |
| http://ae.hotchanson.com/public/query\_by\_song\_info | com/sds/android/cloudapi/ttpod/a/b.java |
| http://ae.hotchanson.com/ae/create/ | com/sds/android/cloudapi/ttpod/a/b.java |
| http://v1.ard.q.itlily.com/privatemsg | com/sds/android/cloudapi/ttpod/a/k.java |
| http://v1.ard.q.itlily.com/collect | com/sds/android/cloudapi/ttpod/a/f.java |
| http://ting.hotchanson.com/v2/songs | com/sds/android/cloudapi/ttpod/a/h.java |
| http://v1.ard.q.itlily.com/notice | com/sds/android/cloudapi/ttpod/a/g.java |
| http://v2.ttus.ttpod.com/ttus/user | com/sds/android/cloudapi/ttpod/a/l.java |
| http://api.busdh.com/market-api | com/sds/android/cloudapi/ttpod/a/e.java |
| http://v1.ard.y.itlily.com/friends | com/sds/android/cloudapi/ttpod/a/c.java |
| http://v1.ard.q.itlily.com/share | com/sds/android/cloudapi/ttpod/a/j.java |
| http://star.dongting.com/uploads | com/sds/android/cloudapi/ttpod/a/j.java |
| http://collect.log.ttpod.com/error/searchsong/index.html | com/sds/android/cloudapi/ttpod/a/i.java |
| http://so.ard.iyyin.com/v2 | com/sds/android/cloudapi/ttpod/a/i.java |
| http://client.api.ttpod.com/global | com/sds/android/cloudapi/ttpod/a/d.java |
| http://openbox.mobilem.360.cn/channel/getUrl?src=440001&app=360box | com/qihoo/appstore/updatelib/AppInfo.java |
| http://openbox.mobilem.360.cn/AppStore/info? | com/qihoo/appstore/updatelib/i.java |
| http://openbox.mobilem.360.cn/index/upgrade? | com/qihoo/appstore/updatelib/i.java |
| http://sdk.open.phone.igexin.com/api.php | sdk/b/a/a/c/d.java |
| http://sdk.open.phone.igexin.com:8003/api.php | sdk/b/a/a/c/d.java |
| http://api.skin.ttpod.com/skin | Android String Resource |
| http://quan.dongting.com | Android String Resource |
| http://weibo.com/ittpod | Android String Resource |
| http://bbs.dongting.com | Android String Resource |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| support@ttpod.com | com/sds/android/ttpod/activities/SkinInfoActivity.java |
| support@ttpod.com  market@ttpod.com | com/sds/android/ttpod/activities/setting/AboutActivity.java |
| support@ttpod.com  market@ttpod.com | Android String Resource |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: False v3 signature: False Found 1 unique certificates Subject: C=zh, ST=shanghai, L=shanghai, O=ttpod, OU=ttpod, CN=ttpod Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2010-03-23 10:20:49+00:00 Valid To: 2035-03-17 10:20:49+00:00 Issuer: C=zh, ST=shanghai, L=shanghai, O=ttpod, OU=ttpod, CN=ttpod Serial Number: 0x4ba89601 Hash Algorithm: sha1 md5: 6e3ff75c1c14350e041de6487b444a1d sha1: 6783bd810dcbd650971b9f8013465ea5f3fa76a1 sha256: ef36b110e2ef5f53981932bb44e82c160409525d1d4d18ebdacd772e1711daab sha512: 4133b4f7ad81a91e9c4c753be242f95e7f7220aa5e617fddb95a3f32f743072c06478a061f13061f897c3d94eb72f8a6101fc268c6e4a8d8fddac2048965c395**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "forget\_password" : "forget the password" |
| "register\_user" : "register user" |
| "find\_password" : "find password" |
| "userinfo\_password" : "Password" |
| "userinfo\_access\_token\_invalid" : "Authentication failed, please login!" |
| "userinfo\_input\_password" : "Input your password here." |
| "forget\_password" : "忘记密码?" |
| "register\_user" : "注册用户" |
| "find\_password" : "找回密码" |
| "userinfo\_password" : "密码" |
| "userinfo\_access\_token\_invalid" : "身份验证失败，请重新登录！" |
| "userinfo\_input\_password" : "设置密码" |

## **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.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.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\_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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| com.baidu.appsearch.extinvoker.LAUNCH | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| .EntryActivity | **Schemes**: ttpod://, |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent100240447://, |

**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。**