MoGua

桃子视频 11.5.6.APK 分析报告

APP名称: 桃子视频

包名:	com.t.v1_1_14
域名线索:	17条
URL线索:	39条
邮箱线索:	3条
分析日期:	2025年7月3日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.peach.tz.app.BaseApplication.apk
文件大小: 13.1MB
MD5值: 28fe45982d0afb1e52ad085fec6d064a
SHA1值: a53494adfae61a71711f4f8dc6db0fd3b4d27a4e
SHA256值: 90964ba778728a0e0a45d18dbd5ba78a2e999a40e310c4f003c8cea252035b7e

APP 信息

App名称: 桃子视频
包名: com.t.v1_1_14
主活动Activity: com.peach.tz.mvp.ui.activity.SplashActivity
安卓版本名称: 11.5.6
安卓版本: 56

域名线索

域名	服务器信息
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
u.20021be.pw	没有服务器地理信息.
help.kuaiyun.cloud	没有服务器地理信息.
greenrobot.org	IP: 85.13.163.69 **所属国家**: Germany **地区**: Thuringen **城市**: Friedersdorf **纬度**: 50.604919 **经度**: 11.035770
ip.zxinc.org	IP: 101.32.207.56 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
www.slf4j.org	IP: 159.100.250.151 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
api.taovideo.me	IP: 104.21.48.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
img.zcool.cn	IP: 221.204.14.66 **所属国家**: China **地区**: Shanxi

	城市: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
pagead2.googlesyndication.com	IP: 114.250.69.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.github.com	IP: 20.205.243.168 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
127.0.0.1	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.unkownwebsiteblog.me	IP: 103.224.182.215 **所属国家**: Australia **地区**: Victoria **城市**: Beaumaris **纬度**: -37.982201 **经度**: 145.038940

alj1s9j1.com	**IP**: 194.53.53.11 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
aria.laoyuyu.me	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java

http://%s:%d/%s	com/danikula/videocache3/server/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache3/server/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache3/server/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache3/server/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache3/server/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache3/server/HttpProxyCacheServer.java
http://%s:%d/%s	com/danikula/videocache3/hls/FileUtils.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/n.java
http://xml.apache.org/xslt	com/jess/arms/c/b.java
https://api.github.com/	com/jess/arms/a/b/p.java
https://img.zcool.cn/community/011ad05e27a173a801216518a5c505.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/0148fc5e27a173a8012165184aad81.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/013c7d5e27a174a80121651816e521.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01b8ac5e27a173a80120a895be4d85.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01a85d5e27a174a80120a895111b2c.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01085d5e27a174a80120a8958791c4.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01f8735e27a174a8012165188aa959.jpg	com/peach/tz/mvp/model/enity/netbean/BannerDataBean.java
http://api.taovideo.me/fast-cloud/	com/peach/tz/mvp/model/api/Api.java

https://help.kuaiyun.cloud/	com/peach/tz/mvp/model/api/Api.java
http://api.taovideo.me/fast-cloud/	com/peach/tz/mvp/model/api/a.java
http://www.unkownwebsiteblog.me	com/peach/tz/mvp/ui/fragment/agentweb/AgentWebFragment.java
https://ip.zxinc.org/api.php?type=json	com/peach/tz/utils/b1/a.java
https://u.20021be.pw/cloud-upload/upload4/posts	com/peach/tz/utils/b1/a.java
https://alj1s9j1.com/	com/re/ng/yhqp/api/ChessClient.java
http://127.0.0.1:8080/%s/%s	com/zzb/ipfssdk/m.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	e/b/a/a/a/a/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/i.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/a.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/f.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/w.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/n.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/c.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/k.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/g.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
http://www.slf4j.org/codes.html	org/slf4j/c.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/h/b.java
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/Document/execCommand	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
danikula@gmail.com	com/danikula/videocache3/server/HttpUrlSource.java
ntz876666@gmail.com	com/peach/tz/mvp/ui/activity/SplashActivity.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=taozi.jks, ST=taozi.jks, L=taozi.jks, O=taozi.jks, OU=taozi.jks, CN=taozi.jks
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-22 11:58:12+00:00
有效期至: 2046-10-16 11:58:12+00:00
发行人: C=taozi.jks, ST=taozi.jks, L=taozi.jks, O=taozi.jks, OU=taozi.jks, CN=taozi.jks
序列号: 0x6d9572c5
哈希算法: sha256
md5值: 65056ba65ed47ee17bfa0b8ae85ec711
sha1值: d74aa7e6357c3eda760c6eb97f9a12e7f1bd78e8
sha256值: 0643736bb59adc6f7ffe070d5aff01257c3cb2c4aa105f47c7c6b96a92c4cf9a
sha512值: 6e399b4ca375039006782e8c68cd90fee33c52f02e15a30bb00835b80dbadfdee74750c8fefd403e6ff7b0c15d2b04f7b7fb10f0101c77be575c2e1f09f240de
公钥算法: rsa
密钥长度: 2048
指纹: f2706e54b136f2732e5eb085ac0ab1b30bbe1bf2dff8dec76025f3f26ac8d04e

硬编码敏感信息

可能的敏感信息
"et_card_pwd_hit" : "请输入身份卡密码"
"google_api_key" : "AIzaSyClSx3CBxoiDI7V6Q62Cekak1K9xZwS3jQ"
"google_crash_reporting_api_key" : "AIzaSyClSx3CBxoiDI7V6Q62Cekak1K9xZwS3jQ"
"login_forget_pwd" : "忘记密码"
"login_mode_pwd" : "注册账号登录"

"login_toast_forget_pwd_success" : "找回密码成功。请尝试登录"
"login_toast_pwd_length" : "请输入正确密码"
"login_toast_pwd_wrong" : "密码错误"
"pwd_limit" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"token_erc" : "ERC-20"
"token_trc" : "TRC-20"
"token_type_label" : "类型"

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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
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
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像

android.permission.PERMISSIONS_STORAGE	未知	Unknown permission	Unknown permission from android reference
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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.peach.tz.mvp.ui.activity.MainActivity	Schemes: cdpk7155://,

com.peach.tz.mvp.ui.activity.SplashActivity	Schemes: cdpk7155://,

---