MoGua

TGpay 1.1.9.APK 分析报告

APP名称: TGpay

包名:	com.xb.kwhsqpks.sunpay
域名线索:	24条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年1月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: tgpay.apk
文件大小: 43.39MB
MD5值: ff63a0a7673f38ef14aecece899e41bb
SHA1值: 404b8fea8e8f9346815fe36f0b000d5082d0c67a
SHA256值: c6dff374882fdaeccd99a4f54d971f61a29d1f9e94f32ae3e5cb7b058ed0d9e4

APP 信息

App名称: TGpay
包名: com.xb.kwhsqpks.sunpay
主活动Activity: com.example.pay_app.MainActivity
安卓版本名称: 1.1.9
安卓版本: 1

域名线索

域名	服务器信息
grs.dbankcloud.asia	没有服务器地理信息.
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
mobilegw.alipay.com	**IP**: 203.209.255.248 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 140.205.174.3

cloudauth.aliyuncs.com	**所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
oss.aliyuncs.com	**IP**: 118.178.29.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
cloudauth-dualstack.aliyuncs.com	**IP**: 140.205.61.35 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
grs.dbankcloud.com	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
journeyapps.com	**IP**: 13.249.59.9 **所属国家**: United States of America **地区**: Texas **城市**: Houston **纬度**: 29.763029 **经度**: -95.362061
render.alipay.com	**IP**: 220.181.135.163 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.236 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
grs.dbankcloud.cn	IP: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
oss-cn-.aliyuncs.comor	没有服务器地理信息.
mobilegw.aaa.alipay.net	没有服务器地理信息.
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
developer.android.com	IP: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
upload-z2.qiniup.com	IP: 220.181.135.136 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
mobilegw.stable.alipay.net	没有服务器地理信息.
image.cnamedomain.com	没有服务器地理信息.
ce3e75d5.jpush.cn	**IP**: 120.233.33.168 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
sdkapi-smartop.jiguang.cn	没有服务器地理信息.
cloudauth.cn-beijing.aliyuncs.com	**IP**: 101.201.182.3 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
grs.dbankcloud.eu	没有服务器地理信息.
cloudauth-dualstack.cn-beijing.aliyuncs.com	**IP**: 39.97.154.5 **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://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/PlatformViewsController.java
https://sdkapi-smartop.jiguang.cn	cn/jiguang/be/c.java
https://upload-z2.qiniup.com	cn/jiguang/bf/a.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/ax/c.java
https://ce3e75d5.jpush.cn/wi/d8n3hj	cn/jiguang/ax/c.java
https://ce3e75d5.jpush.cn/wi/op8jdu	cn/jiguang/s/c.java
https://cloudauth-dualstack.aliyuncs.com	com/aliyun/aliyunface/api/ZIMFacade.java
https://cloudauth-dualstack.cn-beijing.aliyuncs.com	com/aliyun/aliyunface/api/ZIMFacade.java
https://cloudauth.aliyuncs.com	com/aliyun/aliyunface/api/ZIMFacade.java
https://cloudauth.cn-beijing.aliyuncs.com	com/aliyun/aliyunface/api/ZIMFacade.java
https://render.alipay.com/p/f/fd-j8l9yjja/index.html	com/aliyun/aliyunface/config/NavigatePage.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/deviceid/module/x/b.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/deviceid/module/x/b.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/deviceid/module/x/b.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/deviceid/module/x/b.java
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java

http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
https://)([\\s\\S]+)	com/huawei/hms/scankit/p/C0054bd.java
https://journeyapps.com/	Mogua Engine V1
https://github.com/journeyapps/zxing-android-embedded	Mogua Engine V1
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2

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=48, ST=jincai, L=jincai, O=jincai, OU=jincai, CN=jincai
签名算法: rsassa_pkcs1v15
有效期自: 2019-07-01 11:18:59+00:00
有效期至: 2044-06-24 11:18:59+00:00
发行人: C=48, ST=jincai, L=jincai, O=jincai, OU=jincai, CN=jincai
序列号: 0xf62b6ec
哈希算法: sha256
md5值: 1ccede321520fe602c5edcbfd34ee29f
sha1值: 3e96a04e69abd0c2f128db066164cc8b96e4d84b
sha256值: 2e26f20d0bbe23bcf0899f06e357c1914ddd0257d4e5e2fdaa2e831bbc2166de
sha512值: 9a4775174fee9ad6227567fccd06dc77abfd968e600bc62ed38ad2a56ea626130ee62cc58deecd655e169aff9fec6038505983ffb6f652c92e80aab71fb5456d
公钥算法: rsa
密钥长度: 2048
指纹: 010272886d732a5e11f8c6c41400018f5680325f404dc40df23afc455abc8475

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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.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.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.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.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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.xb.kwhsqpks.sunpay.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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_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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.example.pay_app.MainActivity	Schemes: tgpay://, Hosts: orderpay,

---