



MoGua

AKPay v1.23.APK 分析报告



APP名称:

AKPay

包名:	xyz.akpay.app
域名线索:	15条
URL线索:	19条
邮箱线索:	0条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件名: AKPay.apk
文件大小: 4.53MB
MD5值: e353749d13fc7bc1139e70a1a5dfd576
SHA1值: e57e6fcae0b403435735ee0d8265dd0eae4b40d0
SHA256值: 4a68bc07c08981ee13c602183341906e3800e7b86c4eb44b03dac7163ebb85a8

i APP 信息

App名称: AKPay
包名: xyz.akpay.app
主活动Activity: xyz.indianx.app.ui.LauncherActivity
安卓版本名称: v1.23
安卓版本: 23

🔍 域名线索

域名	服务器信息
h.trace.qq.com	IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
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
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.774929 经度: -122.419418
schemas.android.com	没有服务器地理信息.
issuetracker.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
android.bugly.qq.com	IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
ns.adobe.com	没有服务器地理信息.
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
youtrack.jetbrains.com	IP: 63.33.88.220 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
api.ak-pay.xyz	IP: 13.126.137.25 所属国家: India 地区: Maharashtra

	城市: Mumbai 纬度: 19.075975 经度: 72.877380
www.mobikwik.com	IP: 104.18.0.215 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
astat.bugly.qcloud.com	IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.freecharge.in	IP: 23.54.122.154 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
api.whatsapp.com	IP: 185.45.7.185 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740

URL线索

URL信息	Url所在文件
https://github.com/google/gson/blob/main/Troubleshooting.md	A/g.java
http://schemas.android.com/apk/res/android	N/b.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://api.ak-pay.xyz	G0/w.java
https://youtrack.jetbrains.com/issue/KT-55980	h3/m.java
https://issuetracker.google.com/issues/116541301	g0/AbstractC0456h.java
https://github.com/google/gson/blob/main/Troubleshooting.md	u2/C0818a.java
https://github.com/google/gson/blob/main/Troubleshooting.md	p2/G.java
https://github.com/google/gson/blob/main/Troubleshooting.md	p2/C0735t.java
http://ns.adobe.com/xap/1.0/u0000	m0/g.java
https://www.freecharge.in/services	xyz/indianx/app/ui/tool/ToolWebActivity.java
https://www.mobikwik.com	xyz/indianx/app/ui/tool/ToolWebActivity.java

https://github.com/google/gson/blob/main/Troubleshooting.md	t2/a.java
https://api.ak-pay.xyz	J2/d.java
https://t.me/	b4/AbstractC0212a.java
https://play.google.com/store/apps/details?id=	b4/AbstractC0212a.java
https://api.whatsapp.com/send?phone=	i4/c.java
https://github.com/google/gson/blob/main/Troubleshooting.md	r2/c.java
https://play.google.com/store/apps/details?id=	A4/b.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: CN=keystore, OU=keystore, O=keystore, L=keystore, ST=keystore, C=keystore
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-01 16:15:41+00:00
有效期至: 2049-06-25 16:15:41+00:00
发行人: CN=keystore, OU=keystore, O=keystore, L=keystore, ST=keystore, C=keystore
序列号: 0x1
哈希算法: sha256

md5值: 81ae9fba58997947b2dc9210ff12cb24
sha1值: 4129d17deb72627b526ff00d386fa7ce306c3bcf
sha256值: 82a156c588a75a47310fde351398a85c4f9382fa1c4af5b60904cc918c848c26
sha512值: 21158e7d0e63214ad53c0a75d8a858592f4941ffa961bfb9c79e15477ac56e705773e6ce96f96aeae14bb73fb0aa5c4ce722f00de85720889b6224b27c196b1c
公钥算法: rsa
密钥长度: 2048
指纹: 2378ec8892e1af2e75e10acf01c82e84ecc7220cbc713f55cc13676856449d1f

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	类型	详细情况

	险		
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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.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.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
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
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.VIBRATE	正常	可控震源	允许应用程序控制振动器

android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
xyz.akpay.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

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。