MoGua

YPT 2.0.1.APK 分析报告

APP名称: YPT

包名:	com.ypt.pay
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19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ypt.apk
文件大小: 129.41MB
MD5值: 69db05bca23b19f3c7c6637a4d82b695
SHA1值: 82d1cf248c8956d4c43db5ef59bb2dbe01e8d346
SHA256值: c54f1d2b186a0cbf45fafb51fc98dc57f5af3c248fcfbe239e01defef05694bb

APP 信息

App名称: YPT
包名: com.ypt.pay
主活动Activity: com.ypt.pay.MainActivity
安卓版本名称: 2.0.1
安卓版本: 24

域名线索

域名	服务器信息
expo.dev	**IP**: 104.18.4.104 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
dev-in.sumsub.com	**IP**: 10.220.13.238 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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
xml.org	IP: 104.239.142.8 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
filesystem.local	没有服务器地理信息.
docs.swmansion.com	IP: 172.67.142.188 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.sumsub.com	IP: 104.18.35.3 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
docs.sumsub.com	IP: 104.16.241.118 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
docs.expo.dev	IP: 104.18.5.104 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
android.asset	没有服务器地理信息.
expo.fyi	**IP**: 216.150.16.1 **所属国家**: Canada **地区**: Ontario **城市**: Etobicoke **纬度**: 43.623768 **经度**: -79.559723
support.sumsub.com	**IP**: 46.51.152.13 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
xmlpull.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
sentry.sumsub.com	**IP**: 172.64.152.253 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-general-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-parameter-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/properties/lexical-handler	com/caverock/androidsvg/SVGParser.java
https://sentry.sumsub.com/	com/sumsub/sns/a.java
https://api.sumsub.com/	com/sumsub/sns/core/SNSMobileSDK.java
https://docs.sumsub.com/docs/customization-android	com/sumsub/sns/core/SNSMobileSDK.java
https://support.sumsub.com/hc/	com/sumsub/sns/internal/features/domain/i.java
http://dev-in.sumsub.com/\	com/sumsub/sns/internal/ff/a.java
https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/InsetsObserverProxy.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenModalFragment.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenStackFragment.java

https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
http://filesystem.local	expo/modules/fetch/OkHttpFileUrlInterceptorKt.java
http://filesystem.local	expo/modules/fetch/OkHttpFileUrlInterceptor.java
https://expo.fyi/android-r.	expo/modules/medialibrary/albums/AddAssetsToAlbum.java
https://docs.expo.dev/push-notifications/fcm-credentials/	expo/modules/notifications/tokens/PushTokenModule.java
https://expo.dev	expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java
https://android.asset/	io/noties/markwon/image/destination/ImageDestinationProcessorAssets.java

邮箱线索

手机线索

手机号	所在文件
17179869184	com/caverock/androidsvg/SVGParser.java
17179869184	com/caverock/androidsvg/SVG.java
17179869184	com/caverock/androidsvg/SVGAndroidRenderer.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: CN=spiderpay, OU=100
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-08 13:59:10+00:00
有效期至: 2050-01-02 13:59:10+00:00
发行人: CN=spiderpay, OU=100
序列号: 0x1
哈希算法: sha256
md5值: 0b1d2032147d1f922ddced367cb33fce
sha1值: e679724112651bb026e50598f0dde59ce140e6e4
sha256值: 8c9747a90ce3c6729f324d6923a64420a5f5cfa797555faed796f104023fe54c
sha512值: 950a45fcd42b9ecee2bdd4a4abe861bfa22638bf531dba985ac76cafcdab07b1a4f5f8badc24635ebb5776a84044f74f13034d647d0400f5f328d61ea23a6792
公钥算法: rsa
密钥长度: 2048
指纹: 23aa450f43b76bf0159edc91dc86b2f2d2d1af634e7dd7a156faa95bca7d1c47

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**

登陆搜瓜网站后查看		

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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_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
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.ypt.pay.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未	Unknown	Unknown permission from android reference

	知	permission	
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
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。

com.huawei.android.launcher.permission.READ_SETTINGS	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
com.huawei.android.launcher.permission.WRITE_SETTINGS	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.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.ypt.pay.MainActivity	Schemes: ypt://, exp+ypt://,

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。