MoGua

周周花 1.0.0.1.APK 分析报告

APP名称:	周周花

包名:	com.kingControl.merchantId1700.zhouzhouhua
域名线索:	5条
URL线索:	3条
邮箱线索:	1条
分析日期:	2025年7月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: smzy_zhouzhouhua.apk
文件大小: 11.61MB
MD5值: 937dc73611101831da35d6c5c6b92941
SHA1值: a4fa08fb1f8e487a83ffc791ceef04270a578276
SHA256值: 2de4c94cd2745e1eeda5664c6c6742d10460e62448c7640ff21617502b8a0414

APP 信息

App名称: 周周花
包名: com.kingControl.merchantId1700.zhouzhouhua
主活动Activity: com.tech.kingControl.ui.activities.WelcomeAct
安卓版本名称: 1.0.0.1
安卓版本: 1

域名线索

域名	服务器信息
mta.oa.com	**IP**: 141.144.196.217 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
pingma.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
rqd.uu.qq.com	**IP**: 60.29.240.104 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mta.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL**信息**	Url**所在文件**
http://mta.qq.com/	com/tencent/legu/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/legu/stat/StatServiceImpl.java
http://mta.qq.com/mta/api/ctr_feedback	com/tencent/legu/stat/common/StatConstants.java
http://pingma.qq.com:80/mstat/report	com/tencent/legu/stat/common/StatConstants.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java

邮箱线索

邮箱地址	所在文件
ctwap@mycdma.cn	com/tencent/legu/mid/a/a.java

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=sdrg, ST=dfgb, L=hgbsc, O=gbsadfgvdawf, OU=rbgvsadf, CN=fwerqht
签名算法: rsassa_pkcs1v15
有效期自: 2018-08-20 10:31:47+00:00
有效期至: 2118-07-27 10:31:47+00:00
发行人: C=sdrg, ST=dfgb, L=hgbsc, O=gbsadfgvdawf, OU=rbgvsadf, CN=fwerqht
序列号: 0x3df18b9f
哈希算法: sha256
md5值: 4d216eba1d67577e3643563123361429
sha1值: 3f6baa4db3bd9f2c2610c87341c74e7bfc65afce
sha256值: 73fbfe13f4e0f9e5df4a116d36b0c2b29582a2b1839b31ae46dff727dc4b1923
sha512值: 3b540b1705d7c7e2b942cce0c3fbd337ed21cca402556eceddb7ac6ff5f55690d7b2e00a936a5fbb8a7af5e4927622bba9098e675614012865b48a38ed81848c

硬编码敏感信息

可能的敏感信息

"octopus_onekey" : "一键登录失败，请使用账号密码登录！"
"super_face_auth_pass" : "稍后再认证人脸"

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_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息，可能包括个人或私人信息

android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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_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_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_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_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_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_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.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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
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.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

应用内通信
