MoGua

消消达人 1.0.APK 分析报告

APP名称:	消消达人

包名:	com.xxdr
域名线索:	8条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年9月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app-release.apk

文件大小: 10.13MB
MD5值: ad982d40389789519e87381591b840cc
SHA1值: cee3e73da30274a3c27da247b79241f8788d7ab4
SHA256值: 1a7ff65f0547ffc40e65a7e9764508b8f0709f8e46838514154151149f19ffd6

APP 信息

App名称: 消消达人
包名: com.xxdr
主活动Activity: mobi.popsoft.popanimal.popfarm
安卓版本名称: 1.0
安卓版本: 10

域名线索

域名	服务器信息
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.apple.com	**IP**: 106.4.158.58 **所属国家**: China **地区**: Jiangxi **城市**: Jingdezhen **纬度**: 29.294701 **经度**: 117.207893
www.soulgame.mobi	**IP**: 193.112.109.171 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
pay.newcreatesoft.com	IP: 116.198.202.148 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
popjewels2.soulgame.mobi	IP: 112.124.109.22 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
apifox.com	IP: 121.199.72.199 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
sock.ianpei.com	IP: 172.86.117.49 **所属国家**: United States of America **地区**: Michigan **城市**: Detroit **纬度**: 42.331429 **经度**: -83.045753
weixin.qq.com	IP: 140.207.122.204 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

URL线索

URL信息	Url所在文件
http://weixin.qq.com/r/NXTg77jEpobZh6mMnyER	org/cocos2dx/lib/Cocos2dxHelper.java
https://pay.newcreatesoft.com:7007/app_api/api/anon/payOrders	org/cocos2dx/exten/PSAppUtils.java
https://apifox.com)	org/cocos2dx/exten/PSAppUtils.java
http://www.soulgame.mobi/popsoft/popfarm	lib/armeabi-v7a/libpopfarm.so
http://popjewels2.soulgame.mobi/exchangecode.php	lib/armeabi-v7a/libpopfarm.so
http://popjewels2.soulgame.mobi/uploadappinfo.php	lib/armeabi-v7a/libpopfarm.so
http://popjewels2.soulgame.mobi/uploadsocial.php	lib/armeabi-v7a/libpopfarm.so
http://popjewels2.soulgame.mobi/uploadscore_v2.php	lib/armeabi-v7a/libpopfarm.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libpopfarm.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libpopfarm.so
https://sock.ianpei.com/stat/os	lib/armeabi-v7a/libnative-lib.so

邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/armeabi-v7a/libpopfarm.so

ftp@example.com	lib/armeabi-v7a/libpopiarm.so

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=china, ST=henan, L=nanyang, O=xcy, OU=xcy, CN=xcy
签名算法: rsassa_pkcs1v15
有效期自: 2018-03-16 05:56:45+00:00
有效期至: 2045-08-01 05:56:45+00:00
发行人: C=china, ST=henan, L=nanyang, O=xcy, OU=xcy, CN=xcy
序列号: 0xec668ce
哈希算法: sha256
md5值: 6f3162db8b1c8a0b7c708f0d30911df5
sha1值: 60709e85388d7cb02644c34cc753c951da70904a
sha256值: 50611d6ac7a33e6df23239637d7255ece10e44fb5cc29695817da2ebfc06a0ee
sha512值: 73517766d27ef19f820825099aea26e4cd98605126fc89722b93927b511671c0d9c1c9bef100b9b52d45d6314ea10920bcf91df0c53e57ec04a2c7ef944c329a
公钥算法: rsa
密钥长度: 2048
指纹: 777eb0a79b9eba6f8685e8ad5793c2da8075ff5bd49d7cca99a39e059062f1d2

硬编码敏感信息

可能的敏感信息
"gc_gamepad_input_pwd_tip" : "请输入您的支付密码:"

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

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。