MoGua

LionWei 4.11.7.APK 分析报告

APP名称: LionWei

包名:	com.zlh.fishwill
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年5月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.zlh.fishwill_4.11.7.apk
文件大小: 39.47MB
MD5值: 0e202ffe3f434cdfbb092eb525e62ec6
SHA1值: 5350c8014ef71e433d40e2f8d7c6553250a3de4d
SHA256值: 9a50031fabe6467e7197b9e44b676e85e4a0f9a253603f572bc12859c01b1f1a

APP 信息

App名称: LionWei
包名: com.zlh.fishwill
主活动Activity: com.zlh.fishwill.SplashActivity
安卓版本名称: 4.11.7
安卓版本: 120

域名线索

域名	服务器信息
www.mob.com	**IP**: 180.188.26.28 **所属国家**: China **地区**: Zhejiang **城市**: Taizhou **纬度**: 28.666668 **经度**: 121.349998

URL线索

URL信息	Url所在文件
http://www.mob.com	摸瓜V1引擎

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: True
找到 1 个唯一证书
主题: C=fishwill, ST=fishwill, L=fishwill, O=fishwill, OU=fishwill, CN=fishwill
签名算法: rsassa_pkcs1v15
有效期自: 2016-01-29 08:36:48+00:00
有效期至: 3015-06-01 08:36:48+00:00
发行人: C=fishwill, ST=fishwill, L=fishwill, O=fishwill, OU=fishwill, CN=fishwill
序列号: 0x35e6bb33
哈希算法: sha256
md5值: d251248c9c6890e0720dd5e4a5283909
sha1值: 0eb564a0dec9141d31714953f676c5d6427b7be8
sha256值: 6ab4de601d093b3ef14522eafb632a28a11e9de9fa1684f62f37b985160c6b75
sha512值: 81902cac2fc037f8cce74a1bba124a0292b523f06983ec9cce0a78d116198153e7b688e897ad9d7d1387797a914ea261b745904f9a0c22be9b46703fcc02f824
公钥算法: rsa
密钥长度: 2048
指纹: 49c702aba0e6b16fdcdadfaacfa0a0c970a2bdd74e4f33d388ba7a7a2c7bea7a

硬编码敏感信息

可能的敏感信息
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"

"ssdk_weibo_oauth_regiseter" : 应用授权
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

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.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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.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.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.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.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_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.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
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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_TOP_ACTIVITY_INFO	未知	Unknown permission	Unknown permission from android reference
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.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.WRITE_CONTACTS	危险	写入联系人数	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来

		据	删除或修改您的联系人数据

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.mob.tools.MobUIShell	Schemes: line.1477692153://,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent1105522320://,

---