MoGua

智会通 xabmait0.APK 分析报告

APP名称: 智会通

包名:	qion86eu20.fvr2zgdhns.pdr8lp73yz
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qion86eu20.fvr2zgdhns.pdr8lp73yz.apk
文件大小: 23.43MB

MD5值: 6d639e7d28eba308bc2a59165eaae704
SHA1值: 0f8a4f214620b612ca62eba3deeee8541ae006d9
SHA256值: fb10f73070b1c6e2800d0230a3db2f2296f59346034fefeeeb0c4d34f23c2b2f

APP 信息

App名称: 智会通
包名: qion86eu20.fvr2zgdhns.pdr8lp73yz
主活动Activity: qion86eu20.fvr2zgdhns.pdr8lp73yz.MainActivity
安卓版本名称: xabmait0
安卓版本: 89316054

域名线索

URL线索

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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-24 08:06:56+00:00
有效期至: 2125-05-31 08:06:56+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x33554fbb796acf2a
哈希算法: sha384
md5值: a5826f40ab12b896713fe3535f110a69
sha1值: ac1a37f25f0bc103b65a85385887f300861ff298
sha256值: 57555b561626b93bf8a1e8ee12a049e32b1736642c92df67796543c4e18243ba
sha512值: e40ed01e455e96cffb018ea4d326b280b9c991afe630a2e2cef7867ad1a58d75851b77882948c1946c9bd52aed12ff2d31d7737994b32f238706665a889241a0
公钥算法: rsa
密钥长度: 2048
指纹: 12048e06e9555644198952f332f44573b9d1c863ebaca3e405e2f2a59868549b

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

	是否		

向手机申请的权限	危险	类型	详细情况
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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
qion86eu20.fvr2zgdhns.pdr8lp73yz.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
qion86eu20.fvr2zgdhns.pdr8lp73yz.MainActivity	Schemes: cthjrawo://,

---