



MoGua

信和 1.0.APK 分析报告



APP名称:

信和

包名:	plus.H555A5127
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件名: ces.apk

文件大小: 14.5MB

MD5值: f4d6160eb5d6f5f69a4079a8d0490682

SHA1值: 2afcb0af5c9e0448789493e205e36c6072955dda

SHA256值: 6c870c0aac06e59e062c21d591dcc79920797f67cbe599aa8db9aa155a506442

i APP 信息

App名称: 信和

包名: plus.H555A5127

主活动Activity: io.dcloud.PandoraEntry

安卓版本名称: 1.0

安卓版本: 100

🔍 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=adminy5ugmr, ST=adminy5ugmr, L=adminy5ugmr, O=adminy5ugmr, OU=adminy5ugmr, CN=adminy5ugmr

签名算法: rsassa_pkcs1v15
 有效期自: 2025-07-05 03:18:47+00:00
 有效期至: 2125-06-11 03:18:47+00:00
 发行人: C=adminy5ugmr, ST=adminy5ugmr, L=adminy5ugmr, O=adminy5ugmr, OU=adminy5ugmr, CN=adminy5ugmr
 序列号: 0x869b80a
 哈希算法: sha256
 md5值: 35be4906d5013309ecfd56dc7467ebeb
 sha1值: 0c184dce5cc3e37ba2cb0b13dac5b7693301de6a
 sha256值: 2a3dc6d4200a034d9b21da1f0e20aa8368329019d588b936bf7fe636ca5ad15d
 sha512值: 42afbfff684610a6907a724f835686151368601e75adbb636267ecebcf60ee4d61194a6739c2ceedc1441b73164029b20cbf66ab14c10cbd185a14bb6c8fd4a3a
 公钥算法: rsa
 密钥长度: 1024
 指纹: 4d0b4b6756e80cd3294dfae6da79032f37321b8fa00b3c4a9f3b1c01273276c7

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

向手机申请的权限	是否危险	类型	详细情况
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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.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.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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h555a5127://,