MoGua

银企通 3.1.9.APK 分析报告

APP名称:	银企通

包名:	io.dcloud.H51D6B84A
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2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qct.apk
文件大小: 18.59MB
MD5值: f372df4d20783636368ce931f60029b8
SHA1值: fc159c7a4a2961b0f5f66cfa43e399c03e6824c0
SHA256值: 94ba60aae8409b61a1caa3126d24bd2af58d507dbc9ca57ebd82646f81f8a119

APP 信息

App名称: 银企通
包名: io.dcloud.H51D6B84A
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 3.1.9
安卓版本: 388

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: False
找到 1 个唯一证书
主题: C=0311, ST=sjz, L=sjz, O=rs, OU=rongshang, CN=li

签名算法: rsassa_pkcs1v15
有效期自: 2017-09-18 07:52:52+00:00
有效期至: 2072-06-21 07:52:52+00:00
发行人: C=0311, ST=sjz, L=sjz, O=rs, OU=rongshang, CN=li
序列号: 0x599b8328
哈希算法: sha256
md5值: 65a1e7eecfaf9f27d0bcea365c550d56
sha1值: f95bbacf34bd85f7690ecccd1709b27672ab33b9
sha256值: 2409b8fc4a8eb83a3b632855a1a21a2a4b5c6e050317716bed606844aa1263e3
sha512值: 1ef1f1b92d0800ba6bf68b045faa23b7231c1eb39e0964a79796a56d42a739bd1dd09588a65c916adeecffcc0092fe9a92c484b2f5d9dd87aa352dc3d12cc9e0
公钥算法: rsa
密钥长度: 2048
指纹: 51d19329be6c6d5d18a9e1aaa4e234a3905cff25d7b089ac4e16aaad96675c9f

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.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_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.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_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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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。
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.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.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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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。

应用内通信