

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



♠ 准点点餐 1.0.3.APK

APP名称: 准点点餐

包名: com.zddc.zddc

域名线索: 0条

URL线索: 0条

邮箱线索: 0条

分析日期: 2022年2月2日 14:58

文件名: zddcan.apk 文件大小: 7.57MB

MD5值: d90f4898c5d467c0f7bf5f1b70616595

SHA1值: d5f84fc5ef25d77d83765e7331c008b4501aa64b

SHA256值: 279dc76669e2be86fff3ac5a20976b566ccfe2b317df25a1f1438afd3ecbb95c

i APP 信息

App名称: 准点点餐 包名: com.zddc.zddc

主活动**Activity:** com.zddc.zddc.activitys.StartActivity

安卓版本名称: 1.0.3

安卓版本: 4

畫此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
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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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_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.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



APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: ST=hunan, L=changsha, O=jiayu, OU=jiayu, CN=jiayu

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2019-07-01 02:17:53+00:00 Valid To: 2044-06-24 02:17:53+00:00

Issuer: ST=hunan, L=changsha, O=jiayu, OU=jiayu, CN=jiayu

Serial Number: 0x16a853d0 Hash Algorithm: sha256

md5: 13f00c610632bf544c97d38fcb40a637

sha1: 3cb3d4b28fe26820a2d0832fdd8427c25c553391

sha256: b803d591754ef9527e01f154c746c941a35fd77c5ba7087f455632bbdcb99fc5

sha512: 21a80c5b3239a3047fedde090f526dbae14b8e055f5303a2eed88c87ae4a592fa33631e9535e2459c515ac87a5d756098ccabdf477281c7d584960793958331d

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: afd52e2e98cc76201fa90821feeead691026600b4b4ceab08e617ed82b5012a3

☑应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: \ 1109591442://,

命加壳分析

文件列表	分析结果	
APK包	壳列表	详细情况
ALKE	打包	Jiagu

文件列表	分析结果			
	売列表	详细情况		
classes.dex	编译器	dexlib 2.x		
	模糊器	unreadable field names unreadable method names		

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析