MoGua

T1ALauncher T1A_HL1.020700.00.200214.APK 分析报告

APP名称:	T1ALauncher
包名:	com.chery.launcher
域名线索:	2条
URL线索:	1条
邮箱线索:	0条
分析日期:	2024年9月25日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: T_new.apk
文件大小: 4.33MB
MD5值: eba1efcbee3862327443297674c726a2
SHA1值: 0ee1cd1fdd16f5abf686321dd21806e59ede7f02
SHA256值: 5e9db7cf90f84d94f22af84c745a00be7a7a0dc7061aa83dd01245b7016996d0

APP 信息

App名称: T1ALauncher
包名: com.chery.launcher
主活动Activity: com.chery.launcher.MainActivity
安卓版本名称: T1A_HL1.020700.00.200214
安卓版本: 150

域名线索

域名	服务器信息
mobi.kuwo.cn	**IP**: 175.102.178.59 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
artistpicserver.kuwo.cn	**IP**: 175.102.178.59 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

URL线索

URL信息	Url所在文件
http://mobi.kuwo.cn/mobi.s?f=kuwo&q=	cn/kuwo/autosdk/utils/k.java
http://artistpicserver.kuwo.cn/pic.web?	cn/kuwo/autosdk/utils/k.java

邮箱线索

手机线索

手机号	所在文件
17179869184	cn/kuwo/autosdk/utils/d.java

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@freescale.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-07-14 17:28:51+00:00
Valid To: 2038-11-29 17:28:51+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@freescale.com
Serial Number: 0xd2cba57296ebebe2

Hash Algorithm: sha1
md5: 748a35b8c2e489de57f2d360315efe3d
sha1: 3e0caf3d799fbaec566facbe1a67fb250bdefd93
sha256: 7fbae817b7db24642d8959c347b561c003c6cfde2cb10f909c932f21a4d6d804
sha512: d49b3844b71f56fc7ea0b63f0c6a8b9bf414639137968a465d79fd58f47e8c6bff7be4d520220bea51df1a478974177942dee48c01c88201f430f97d1b0433f4

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.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.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.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.READ_SYNC_SETTINGS	正常	读取同步设置	允许应用程序读取同步设置,例如是否为联系人启用同步
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.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference

应用内通信