MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

拆豆豆 1.0.8.APK

APP名称:	拆豆豆
包名:	chaiduoduo.top
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2022年1月22日 17:43

文件信息

文件名: cddou.apk
文件大小: 7.84MB
MD5值: adc1270f75e53702db220c6dd92ddb9f
SHA1值: 8957e4aade0532dbbfaf215cb839319b3a21f799
SHA256值: 740065fe83d2ae5bec5602668c26e7c1ea88e344cef0d9e78656cbb70cce0b63

APP 信息

App名称: 拆豆豆
包名: chaiduoduo.top
主活动**Activity:** chaiduoduo.top.StartPageActivity
安卓版本名称: 1.0.8
安卓版本: 10002

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.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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.DELETE_CACHE_FILES	系统需要	删除其他应用程序缓存	允许应用程序删除缓存文件
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=20000, ST=上海, L=上海, O=上海彩兜兜网络科技有限公司, OU=上海彩兜兜网络科技有限公司, CN=彩兜兜
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-20 08:47:03+00:00
Valid To: 2046-07-14 08:47:03+00:00
Issuer: C=20000, ST=上海, L=上海, O=上海彩兜兜网络科技有限公司, OU=上海彩兜兜网络科技有限公司, CN=彩兜兜
Serial Number: 0xd645bb0
Hash Algorithm: sha256
md5: f799c27d05380e7bef8d24a20ba5a5b3
sha1: c2a3f8150314fd17c54caab24111fba51d90a131
sha256: 57f2e8f6c82e0006fab653d8a6d75f80f9fe0bac730259818ed67474239d9e10
sha512: 7c62ab842833802f8ceb28cce5f8e7c247af89e54a58048cb1b029a882ca3a45cb2120455068a724fe95ad1f2a0f54ec6e82a013494c4311b402f45a591165f8

应用内通信

活动(ACTIVITY)	通信(INTENT)
chaiduoduo.top.MainActivity	Schemes: chaiduoduo://, Hosts: cdd,

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>Tencent's Legu</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>防止反汇编</td><td>non-zero link size
non-zero link offset</td></tr>
<tr><td>打包</td><td>Mobile Tencent Protect</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

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