MoGua

# apk文件提取 1.0.7.APK 分析报告

APP名称: apk文件提取

| | |
|---|---|
| 包名: | com.lapian.appkit |
| 域名线索: | 0条 |
| URL线索: | 0条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2024年4月25日 |
| 分析平台: | 摸瓜反编译平台 |

## 文件信息

**文件名**: com.lapian.appkit107.apk
**文件大小**: 11.45MB
**MD5值**: 0eef230421c9ad64b10a0ae14a5dbdbe
**SHA1值**: e37558fdb599d9e04865d64d886f17ce048039c2
**SHA256值**: 83567a95fdfacd78ea8bb6254ed3c3925fc5f12721d3c788ef06cf0e470383db

# APP 信息

**App名称**: apk文件提取
**包名**: com.lapian.appkit
**主活动Activity**: com.lapian.appkit.ui.activity.FlashActivity
**安卓版本名称**: 1.0.7
**安卓版本**: 8

# 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=cn, L=sz, CN=lp

签名算法: rsassa_pkcs1v15
有效期自: 2020-09-04 03:21:20+00:00
有效期至: 2045-08-29 03:21:20+00:00
发行人: C=cn, L=sz, CN=lp
序列号: 0x5da27933
哈希算法: sha256
md5值: 1b61c529298569ee695c7b5db6629af1
sha1值: f50e06a10f525e53b180c1459a8772957c97f3b4
sha256值: 4e6dc296d1e718184fb769ebbb20b112c0bea28e5dbb9de16efb8762b2e1aa82
sha512值: 9b9206d71ce710b14b5ec172f1bcf5be7dbe31511e60582a3f9b94ec781fe3e28e872fc9e54728f667a9d5eb67fe704daf5e74103995367d793346ec19bc4647
公钥算法: rsa
密钥长度: 2048
指纹: 70b2a3c354faff18f1af56da9f8ebb191e80c5db29f1c83dcb6d31c33832781c

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "category_advanced_key" : "category_key" |
| "category_more_key" : "category_more" |
| "category_other_key" : "other_key" |
| "category_advanced_key" : "category_key" |
| "category_more_key" : "category_more" |
| "category_other_key" : "other_key" |

# 加壳分析

| | |
| --- | --- |

| 加壳类型 | 所属文件 |
| --- | --- |
| 360 | .appkey |
| 360 | assets/.appkey |
| 360 | libjiagu.so |
| 360 | assets/libjiagu.so |
| 360 | libjiagu_a64.so |
| 360 | libjiagu_x64.so |
| 360 | libjiagu_x86.so |

## 第三方SDK

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 360加固 | 加壳加固, 开发辅助 | https://reports.exodus-privacy.eu.org/trackers/456 |

## 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.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.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.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.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.PACKAGE_USAGE_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| 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.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.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.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.REQUEST_DELETE_PACKAGES | 正常 | | 允许应用程序请求删除包 |
| com.lapian.appkit.openadsdk.permission.TT_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

# 应用内通信

---