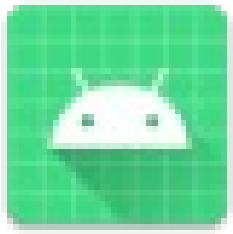
MoGua

# 老化应用8229 1.0.APK 分析报告



APP名称: 老化应用8229

| | |
|---|---|
| 包名: | com.jancar.monster |
| 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16日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: 老化应用8229_ivi-burn.apk
**文件大小**: 1.68MB
**MD5值**: 4077e07a01a026c3f2cfd9697ea5816f
**SHA1值**: 7f2261fd675f31463298eb96edcc156a83bdaba0
**SHA256值**: e4464cb038acfea02ff47de7e79c2fd132067ff1551627ce05a3ea1e9264d300

# APP 信息

**App名称**: 老化应用8229
**包名**: com.jancar.monster
**主活动Activity**: com.jancar.monster.FakeActivity
**安卓版本名称**: 1.0
**安卓版本**: 1

# 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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

签名算法: rsassa_pkcs1v15
有效期自: 2008-04-15 22:40:50+00:00
有效期至: 2035-09-01 22:40:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xb3998086d056cffa
哈希算法: md5
md5值: 8ddb342f2da5408402d7568af21e29f9
sha1值: 27196e386b875e76adf700e7ea84e4c6eee33dfa
sha256值: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
sha512值: 5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6ef602d43d1a2ebae9f002a6598e72fd2d83
公钥算法: rsa
密钥长度: 2048
指纹: 65ba0830722d5767f8779e37d0d9c67562f03ec63a2889af655ee9c59effb434

# 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.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_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.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.REBOOT | 系统需要 | 强制手机重启 | 允许应用强制手机重启 |

# 应用内通信