

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



Heart Gears 2.0.APK

APP名称: Heart Gears

包名: com.world_date.advent

域名线索: 1条

URL线索: 2条

邮箱线索: 0条

分析日期: 2022年1月28日 22:20

文件名: heartgears539728.apk

文件大小: 5.17MB

MD5值: 791d59f3223209b2a5e162cbb650f715

SHA1值: 9592778b90b3f4176553a1ad629beaf33c523c88

\$HA256值: 7c313be9dbd7ac8a8fde38b58a876a850679b27b3ee15d64e7385fab9d146f76

i APP 信息

App名称: Heart Gears

包名: com.world_date.advent

主活动**Activity:** com.world_date.advent.ui.MainActivity

安卓版本名称: 2.0 安卓版本: 2

0 域名线索

| 域名 | 是否危险域名 | 服务器信息 |
|-----------------------|--------|------------|
| id249.whitelist.world | good | 没有服务器地理信息. |

URL线索

| URL信息 | Url所在文件 |
|--------------------------------|---|
| https://id249.whitelist.world/ | com/world_date/advent/data/net/NetImpl.java |

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_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.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.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.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.FOREGROUND_SERVICE | 正常 | | 允许常规应用程序使用 Service.startForeground。 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |



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

Found 1 unique certificates Subject: CN=Dann Molke

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-05-02 07:50:23+00:00 Valid To: 2045-04-26 07:50:23+00:00

Issuer: CN=Dann Molke

Serial Number: 0x3a1f0f88 Hash Algorithm: sha256

md5: a986acbfadb453f3b94d88ca29be4d46

sha1: 79c30eed57a3ed40adee91e5292632ae7c8f5184

sha256; cb6e9d4158047067e1f8043608320713463cb3b7325e20c19412ef68e54f767f

sha512: bac81ae1e2a7bf432dd65b3230703209fd005eab929154f4189848d56cec5459cee5af485e8b16748ae0184d2e6642f0f7e5ccc2101ec97f9f9d7126872d283f

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: be40489ab6066d44b617cb0b6699a18aab98513475d57399c96c9af6a20cc0d6



₽ 硬编码敏感信息

可能的敏感信息

"remember_password" : "Забыли пароль?"

"remember_password": "Passwort vergessen?"

"remember_password": "Forgot your password?"



文件列表 分析结果

| 文件列表 | 分析结果 | | | | |
|-------------|------|------------|--------------------------|--|--|
| classes.dex | 壳 | | 详细情况 | | |
| | 反 | 反虚拟机 | Build.MANUFACTURER check | | |
| | 编计 | 扁译器 | r8 | | |
| | | | | | |
| | | | | | |

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