Evaluation Warning: The document was created with Spire.Doc for Python.

**微聊天记录器（ 2.1.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 微聊天记录器 |
| 版本 | 2.1.0 |
| 包名 | cn.zhilianda.chat.recovery.manager |
| 域名线索 | 5条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年1月20日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | manager.apk |
| 文件大小 | 19.22MB |
| MD5值 | 9c30686bb36db384b6f17a517e7c1beb |
| SHA1值 | 08dc02e6b392a9716989e1211b20009a16697343 |
| SHA256值 | 6f6fbc5cf006c4822c99c66abf10944bc4f80fa77c74e92e7c59fa3d68f1ca12 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 微聊天记录器 |
| 包名 | cn.zhilianda.chat.recovery.manager |
| 主活动Activity | cn.zhilianda.chat.recovery.manager.ui.other.WelActivity |
| 安卓版本名称 | 2.1.0 |
| 安卓版本 | 210 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| errlog.umeng.com | IP: 223.109.148.142 所属国家: China 地区: Beijing 城市: Beijing  |
| www.zetetic.net | IP: 13.225.165.105 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| gjapplog.ucweb.com | IP: 168.235.204.12 所属国家: United States of America 地区: California 城市: Monrovia  |
| applog.uc.cn | IP: 123.182.50.230 所属国家: China 地区: Hebei 城市: Zhangjiakou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.zetetic.net/sqlcipher/  | Mogua Engine V1  |
| https://www.zetetic.net/sqlcipher/license/  | Mogua Engine V1  |
| https://github.com/sqlcipher/android-database-sqlcipher  | Mogua Engine V1  |
| https://applog.uc.cn/collect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://gjapplog.ucweb.com/collect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 旋转线条@2x.png 透明@2x.png  | Mogua Engine V2  |
| 旋转线条@2x.png 透明@2x.png  | Mogua Engine V2  |
| 搜索@2x.png 文件@2x.png  | Mogua Engine V2  |
| 无障碍@2x.png 图层1@2x.png 图层2@2x.png 图层3@2x.png 图层5@2x.png  | Mogua Engine V2  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: CN=zhilianda 签名算法: rsassa\_pkcs1v15 有效期自: 2021-08-02 01:51:55+00:00 有效期至: 2046-07-27 01:51:55+00:00 发行人: CN=zhilianda 序列号: 0x640ca91c 哈希算法: sha256 md5值: 26c42fb2b058a4440e730de887a127f9 sha1值: b0697d8d2052e6aa01b9d9546416ebc52a709fc1 sha256值: 1175442cf2cfb21aa9d4cdbb2e68e64d4a6b95dfe9aae3eec4ac08ba533b790b sha512值: 488ef86573287394c2601b921f61765376feca7294338d7ec58420dc8d216f77f55b4cb497ba0deb261977d64992785a4e524c633715a302d8f50a49b97ad72a**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "hit\_del\_user" : "确定注销吗？"  |
| "library\_android\_database\_sqlcipher\_author" : "Zetetic, LLC"  |
| "library\_android\_database\_sqlcipher\_authorWebsite" : "https://www.zetetic.net/sqlcipher/"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_SUPERUSER | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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.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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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 |
| cn.zhilianda.chat.recovery.manager.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| cn.zhilianda.chat.recovery.manager.ui.login.AccountActivity | **Schemes**: scheme://, **Hosts:** zld-chat-recovery, **Paths:** /loginActy,  |
| cn.zhilianda.chat.recovery.manager.ui.my.activity.BuyVipActivity | **Schemes**: scheme://, **Hosts:** zld-chat-recovery, **Paths:** /vipCombo,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent101966790://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**