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

**字体美化大师（ 8.8.7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 | 字体美化大师 |
| 版本 | 8.8.7 |
| 包名 | com.mylikefonts.activity |
| 域名线索 | 15条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年6月24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 | ztmhds\_138630.apk |
| 文件大小 | 61.93MB |
| MD5值 | 179878bd63548670a2e55bffba479cff |
| SHA1值 | 1100b567ab770d78ad722423f77cbcc66331d5fd |
| SHA256值 | 59f37efb21910bb83652d9515fbf72b00bbdeb99c9fefaaaec38956a056cdde6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 字体美化大师 |
| 包名 | com.mylikefonts.activity |
| 主活动Activity | com.mylikefonts.activity.IndexActivity |
| 安卓版本名称 | 8.8.7 |
| 安卓版本 | 167 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.asia | IP: 119.8.176.236 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics1.data.hicloud.com | IP: 111.202.17.12 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 113.201.107.90 所属国家: China 地区: Shaanxi 城市: Baoji  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.mob.com | IP: 45.113.201.237 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.mob.com  | Mogua Engine V1  |
| https://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.dt.dbankcloud.ru:6447  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://grs.platform.dbankcloud.ru  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| feedback@jnsdyt.com  | Mogua Engine V1  |

### **4.4 手机号线索**

## **5. 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: CN=mylikefonts 签名算法: rsassa\_pkcs1v15 有效期自: 2014-05-19 06:29:40+00:00 有效期至: 2114-04-25 06:29:40+00:00 发行人: CN=mylikefonts 序列号: 0x5379a4d4 哈希算法: sha1 md5值: cfa778638a7feaf92da8896436b511b9 sha1值: 2224e7778f1f85dc6df2cf286498fdc9b04b98d0 sha256值: 15d1292f8437edceab78d08c900a1be57030de0be47f641b14ec960a12e0ac01 sha512值: b606c4d3f31c29ccb6b9e63bb638bc68958f8313de07f257c1b2b6f42a0f93f5d1e03fe3680d39f31498a9f64b474bb394bc02ba5e83b8da8c95f2b55602e468 公钥算法: rsa 密钥长度: 1024 指纹: af768f2069ceb638d2ca7e4ed8a55900f41053179f37c2e12e79bf426ce969c8**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "consumer\_re\_password" : "确认密码"  |
| "font\_author\_apply\_1" : "美字达人可以在社区内分享自己创作或美化的字体作品。"  |
| "font\_author\_apply\_2" : "可获得专属勋章"  |
| "font\_author\_apply\_3" : "帐号需要绑定手机，可到帐号管理处绑定"  |
| "font\_author\_apply\_4" : "有字体设计或美化作品"  |
| "font\_author\_apply\_phone\_unbind" : "还没绑定手机号，是否现在去绑定？"  |
| "font\_author\_apply\_success" : "申请提交成功，审核通过后即可分享字体。"  |
| "font\_author\_secret\_unchecked" : "请确认已同意美字达人入驻协议"  |
| "font\_author\_submit" : "立即申请"  |
| "font\_author\_submit\_my" : "我要申请"  |
| "font\_author\_title" : "字体作品地址"  |
| "menu\_font\_author" : "美字达人"  |
| "menu\_font\_author\_apply" : "美字达人申请"  |
| "menu\_getpassword" : "忘记密码"  |
| "menu\_resetpassword" : "重置密码"  |
| "menu\_user" : "我的"  |
| "privateKeyP2" : "#e$r"  |
| "private\_image\_mutual" : "互相关注后才能发图片"  |
| "secret\_content" : "欢迎使用字体美化大师！我们非常重视您的个人隐私信息和本软件内容的版权信息。在使用本软件服务之前请您仔细阅读《隐私政策》《用户协议》和《免责声明》。我们将严格按照经您同意的各项条款使用您的个人信息，以便为您提供更好的服务。 1.我们会申请收集设备信息权限，用于提供对应设备的字体安装方式。 2.我们会申请位置权限，用于向你推荐该区域用户常用字体，我们仅会获取大概位置，不会获取您精确位置信息。 3.我们会申请存储权限，用于下载及缓存相关文件。 4.我们会在美图秀、更换头像等功能中申请摄像头、相册权限，用于分享图片及更换头像。 5.为实现第三方登录、信息分享、综合统计等，我们可能会调用相关功能最小必要信息。 6.我们会获取用户设备信息包括但不限于IMEI、IMSI、设备MAC地址、WIFI信息(SSID，BSSID，WIFI扫描结果)、软件安装列表、设备序列号、androidID、设备传感器等信息，用于实现服务功能及保障您的帐号、网络、运营及系统安全。 7.您可以在手机的“设置-隐私”中随时查看App获取权限情况，并对权限进行开启/关闭的管理"  |
| "secret\_no\_alert" : "字体美化大师APP需要拥有常用权限才能为您提供服务，否则字体预览、安装等功能均无法使用！"  |
| "secret\_title" : "隐私政策和免责声明"  |
| "security\_public\_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"  |
| "smssdk\_authorize\_dialog\_accept" : "同意"  |
| "smssdk\_authorize\_dialog\_reject" : "拒绝"  |
| "smssdk\_authorize\_dialog\_title" : "服务授权"  |
| "user" : "用户"  |
| "smssdk\_authorize\_dialog\_accept" : "同意"  |
| "smssdk\_authorize\_dialog\_reject" : "拒绝"  |
| "smssdk\_authorize\_dialog\_title" : "服务授权"  |
| "smssdk\_authorize\_dialog\_accept" : "Agree"  |
| "smssdk\_authorize\_dialog\_reject" : "Disagree"  |
| "smssdk\_authorize\_dialog\_title" : "Terms of Use"  |

## **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.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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\_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.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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.mylikefonts.activity.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| 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 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.mylikefonts.activity.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.mylikefonts.activity.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.mylikefonts.activity.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.action.UPDATE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.mylikefonts.activity.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.mylikefonts.activity.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.mylikefonts.activity.MainActivity | **Schemes**: mylikefonts://, **Hosts:** com.ericly.mylikefonts, **Paths:** /main,  |
| com.mylikefonts.activity.FontMainActivity | **Schemes**: mylikefonts://, **Hosts:** com.ericly.mylikefonts, **Paths:** /fontmain,  |
| com.mylikefonts.activity.RankingActivity | **Schemes**: mylikefonts://, **Hosts:** com.ericly.mylikefonts, **Paths:** /ranking,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1101351512://, tencenttencent1101351512://,  |

**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。**