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

**Folo（ 0.2.2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 | Folo |
| 版本 | 0.2.2 |
| 包名 | is.follow |
| 域名线索 | 26条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | Folo\_0.2.2\_apkcombo.com.xapk |
| 文件大小 | 52.52MB |
| MD5值 | 488e4d07a2758ffabdf8577aea3eeea6 |
| SHA1值 | e60f7381f5eab29f9044f575201dede995ba0235 |
| SHA256值 | 4cf7c4305ebea0e212b31c932e1fadc07003230c7c188948147688abe7cdd6ed |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Folo |
| 包名 | is.follow |
| 主活动Activity | is.follow.MainActivity |
| 安卓版本名称 | 0.2.2 |
| 安卓版本 | 17 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| docs.expo.dev | IP: 104.18.4.104 所属国家: United States of America 地区: California 城市: San Francisco  |
| .css | 没有服务器地理信息.  |
| www.years | 没有服务器地理信息.  |
| expo.fyi | IP: 216.150.1.1 所属国家: Canada 地区: Ontario 城市: Etobicoke  |
| shopify.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| .jpg | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.text-decoration | 没有服务器地理信息.  |
| www.hortcut | 没有服务器地理信息.  |
| www.a | 没有服务器地理信息.  |
| www.icon | 没有服务器地理信息.  |
| expo.dev | IP: 104.18.4.104 所属国家: United States of America 地区: California 城市: San Francisco  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.style | IP: 99.83.155.228 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.css | 没有服务器地理信息.  |
| www.wencodeuricomponent | 没有服务器地理信息.  |
| www.recent | 没有服务器地理信息.  |
| www.world | IP: 75.2.38.108 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.interpretation | 没有服务器地理信息.  |
| www.language | 没有服务器地理信息.  |
| www.lia | 没有服务器地理信息.  |
| docs.swmansion.com | IP: 172.67.142.188 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| filesystem.local | 没有服务器地理信息.  |
| www.c | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xmlpull.org/v1/doc/features.html  | com/caverock/androidsvg/SVGParser.java  |
| http://xml.org/sax/features/external-general-entities  | com/caverock/androidsvg/SVGParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/caverock/androidsvg/SVGParser.java  |
| http://xml.org/sax/properties/lexical-handler  | com/caverock/androidsvg/SVGParser.java  |
| https://shopify.github.io/flash-list/docs/usage  | com/shopify/reactnative/flash\_list/AutoLayoutView.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues  | com/swmansion/rnscreens/InsetsObserverProxy.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenModalFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues  | com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java  |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot  | com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java  |
| https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting  | com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java  |
| https://github.com/c19354837/react-native-system-setting/issues/48  | com/reactnativevolumemanager/VolumeManagerModule.java  |
| http://filesystem.local  | expo/modules/fetch/OkHttpFileUrlInterceptorKt.java  |
| http://filesystem.local  | expo/modules/fetch/OkHttpFileUrlInterceptor.java  |
| https://expo.fyi/android-r.  | expo/modules/medialibrary/albums/AddAssetsToAlbum.java  |
| https://docs.expo.dev/push-notifications/fcm-credentials/  | expo/modules/notifications/tokens/PushTokenModule.java  |
| https://github.com/expo/expo.  | expo/modules/securestore/encryptors/HybridAESEncryptor.java  |
| https://expo.dev  | expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java  |
| http://dictionaryperceptionrevolutionfoundationpx;height:successfulsupportersmillenniumhis  | org/brotli/dec/Dictionary.java  |
| http://mathematicsmargin-top:eventually  | org/brotli/dec/Dictionary.java  |
| http://Descriptionrelatively  | org/brotli/dec/Dictionary.java  |
| http://applicationslink\  | org/brotli/dec/Dictionary.java  |
| http://navigation\  | org/brotli/dec/Dictionary.java  |
| http://px;  | org/brotli/dec/Dictionary.java  |
| https://www.World  | org/brotli/dec/Dictionary.java  |
| http://www.years  | org/brotli/dec/Dictionary.java  |
| http://interested  | org/brotli/dec/Dictionary.java  |
| http://familiar  | org/brotli/dec/Dictionary.java  |
| https://was  | org/brotli/dec/Dictionary.java  |
| https://aIn  | org/brotli/dec/Dictionary.java  |
| http://whether  | org/brotli/dec/Dictionary.java  |
| http://interpreted  | org/brotli/dec/Dictionary.java  |
| http://\  | org/brotli/dec/Dictionary.java  |
| http://);  | org/brotli/dec/Dictionary.java  |
| http://addEventListenerresponsible  | org/brotli/dec/Dictionary.java  |
| http://.jpg  | org/brotli/dec/Dictionary.java  |
| http://<a  | org/brotli/dec/Dictionary.java  |
| https://<div  | org/brotli/dec/Dictionary.java  |
| http://according  | org/brotli/dec/Dictionary.java  |
| http://www.interpretation  | org/brotli/dec/Dictionary.java  |
| http://s;text-align:centerfont-weight:  | org/brotli/dec/Dictionary.java  |
| http://html4/loose.dtd\  | org/brotli/dec/Dictionary.java  |
| http://style=\  | org/brotli/dec/Dictionary.java  |
| http://staticsuggested  | org/brotli/dec/Dictionary.java  |
| http://www.a  | org/brotli/dec/Dictionary.java  |
| http://An  | org/brotli/dec/Dictionary.java  |
| https://www.recent  | org/brotli/dec/Dictionary.java  |
| http://In  | org/brotli/dec/Dictionary.java  |
| http://www./div></div><div  | org/brotli/dec/Dictionary.java  |
| http://cript\  | org/brotli/dec/Dictionary.java  |
| http://\n<script  | org/brotli/dec/Dictionary.java  |
| http://www.wencodeURIComponent(\  | org/brotli/dec/Dictionary.java  |
| http://encoding=\  | org/brotli/dec/Dictionary.java  |
| http://www.icon\  | org/brotli/dec/Dictionary.java  |
| http://imEnglish  | org/brotli/dec/Dictionary.java  |
| http://i  | org/brotli/dec/Dictionary.java  |
| http://www.<li><a  | org/brotli/dec/Dictionary.java  |
| http://site\_name\  | org/brotli/dec/Dictionary.java  |
| http://www.hortcut  | org/brotli/dec/Dictionary.java  |
| http://</a></li><li  | org/brotli/dec/Dictionary.java  |
| http://<div  | org/brotli/dec/Dictionary.java  |
| http://iparticipation  | org/brotli/dec/Dictionary.java  |
| http://www.\  | org/brotli/dec/Dictionary.java  |
| http://xt/css\  | org/brotli/dec/Dictionary.java  |
| http://link  | org/brotli/dec/Dictionary.java  |
| http://www.text-decoration:underthe  | org/brotli/dec/Dictionary.java  |
| http://option><option  | org/brotli/dec/Dictionary.java  |
| http://www</a><a  | org/brotli/dec/Dictionary.java  |
| http://w  | org/brotli/dec/Dictionary.java  |
| http://.css\  | org/brotli/dec/Dictionary.java  |
| http://www.style=\  | org/brotli/dec/Dictionary.java  |
| http://www.css\  | org/brotli/dec/Dictionary.java  |
| http://ator\  | org/brotli/dec/Dictionary.java  |
| http://www.language=\  | org/brotli/dec/Dictionary.java  |
| http://www-//W3C//DTD  | org/brotli/dec/Dictionary.java  |
| http://UA-Compatible\  | org/brotli/dec/Dictionary.java  |
| http://www.C//DTD  | org/brotli/dec/Dictionary.java  |
| http://www.  | org/brotli/dec/Dictionary.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/caverock/androidsvg/SVGParser.java  |
| 17179869184  | com/caverock/androidsvg/SVG.java  |
| 17179869184  | com/caverock/androidsvg/SVGAndroidRenderer.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-07 03:11:41+00:00 有效期至: 2055-04-07 03:11:41+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0x6a1afa27b1e7122a88c6283077035df5f0c7b164 哈希算法: sha256 md5值: fac4759b701292d10e7078e4c05fc32a sha1值: 3e9112719fb00c27a56f070f0c81828c7ebae01f sha256值: 2a0a7d26ed05f5a577fb9c0ced28972a65358793339f88a3cce4c0a8b9a7f99d sha512值: 7db06dc99f56a20ab6a41960292d7b2320dca7b586685b60f31c47c248f52eea39493069a9b8b4fbf9165651b8ff26390dcc5aeba30e5e9fe095f6bbf8f21066 公钥算法: rsa 密钥长度: 4096 指纹: c02d87b0ad5b9a46bab486fbb8b708311f9209a374bcac7d4de78428ce9b148b**

## **6. 硬编码敏感信息**

## **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\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| is.follow.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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.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.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.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| 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。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 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 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 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.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| is.follow.MainActivity | **Schemes**: follow://, folo://, exp+follow://,  |

**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。**