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

**思欲..加速（ 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 | 思欲..加速 |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 28条 |
| URL线索 | 31条 |
| APP图标 |  |
| 分析日期 | 2025年5月28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 | ubxDw.Blroxl.zwDHudpaBaevys.apk |
| 文件大小 | 27.24MB |
| MD5值 | 36f199a3084a08af0678143e66b492bc |
| SHA1值 | 6d07de6215e00cf0e029be4443db2a0af1a1f6de |
| SHA256值 | ede646770363d846f5b57a372832641972a03a3c3dc3135164aadf683511005c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 思欲..加速 |
| 包名 |  |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | [] |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| nrtc.netease.im | IP: 45.254.48.99 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| android.rqd.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| webtest.netease.im | IP: 111.124.202.79 所属国家: China 地区: Guizhou 城市: Zunyi  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| errnewlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| plus.google.com | IP: 128.242.240.180 所属国家: United States of America 地区: Washington 城市: Redmond  |
| 45.116.164.114 | IP: 45.116.164.114 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| errnewlog.umeng.com | IP: 223.109.148.143 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alogsus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| ulogs.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| jy.ywdianziqin.com | IP: 172.65.190.172 所属国家: United States of America 地区: California 城市: San Francisco  |
| cnlogs.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| errlog.umeng.com | IP: 223.109.148.142 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pro.bugly.qq.com | IP: 116.130.229.17 所属国家: China 地区: Beijing 城市: Beijing  |
| ucc.umeng.com | IP: 203.119.169.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| resolve.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| aspect-upush.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pslog.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/d/c.java  |
| http://webtest.netease.im/nrtcproxy/nrtc/getSdkConfig.action  | com/netease/lava/nertc/foreground/Authenticate.java  |
| https://nrtc.netease.im/nrtc/getSdkConfig.action  | com/netease/lava/nertc/foreground/Authenticate.java  |
| https://pro.bugly.qq.com  | com/tencent/bugly/proguard/q.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/q.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/dk.java  |
| https://pro.bugly.qq.com/v1/  | com/tencent/bugly/proguard/cq.java  |
| https://android.rqd.qq.com/analytics/async  | com/tencent/bugly/proguard/ft.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/dj.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/dj.java  |
| https://pro.bugly.qq.com  | com/tencent/bugly/proguard/ev.java  |
| https://pro.bugly.qq.com  | com/tencent/bugly/proguard/ef.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/aq.java  |
| https://cnlogs.umeng.com/ext\_event  | com/umeng/analytics/pro/aq.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/l.java  |
| https://resolve.umeng.com/resolve  | com/umeng/analytics/pro/bt.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/ar.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/c/b.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/c/b.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://developer.umeng.com/docs/119267/detail/118637  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| http://45.116.164.114/appapi/playPage/appkey/abc123456/did/  | h0/a.java  |
| https://plus.google.com/  | k/g.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | org/java\_websocket/AbstractWebSocket.java  |
| https://jy.ywdianziqin.com/appapi/getSharePid/appkey/3b2a8584d88c5115  | t/b.java  |
| https://jy.ywdianziqin.com/appapi/appInit/appkey/3b2a8584d88c5115  | t/b.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | i/k.java  |

### **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: True 找到 1 个唯一证书 主题: C=中国, ST=十说小字动填, L=物诗, O=Ceicoo, OU=Ceicoo, CN=Ceicoo 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-17 23:02:18+00:00 有效期至: 2124-09-23 23:02:18+00:00 发行人: C=中国, ST=十说小字动填, L=物诗, O=Ceicoo, OU=Ceicoo, CN=Ceicoo 序列号: 0x52e1c522 哈希算法: sha512 md5值: 82b3eef6986d20c9b99885b7ba29e995 sha1值: 831f582a0fad0d4a9c05551ca085a9cae5882b80 sha256值: 14238eecd5535b25e96ab2a5a2ec69f723c6015a836f9aef54495db6f05ec573 sha512值: f9b200e1c66ed1dc2f39ce69cf5d6684881e532074639fedc69a064e414bd0de8f609137b1cf4be330be3a27ec33175dcaef4fcf70a82cd74804907ca9af91fa 公钥算法: rsa 密钥长度: 2048 指纹: 45bee00654d2476da8082181776246d9f8b36eb0b1b4b203df99967a265c097d**

## **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**

## **10. 应用内通信**

**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。**