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

**超级直播助手（ 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 | 超级直播助手 |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 43条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年10月2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 | 111.apk |
| 文件大小 | 105.07MB |
| MD5值 | 9b8dc2ceb0448a58f6a2faa651719f30 |
| SHA1值 | c2157879ba2355197d028dda638fbf78b2ec3a8d |
| SHA256值 | a681862c4e236f251502f3399fa2c6e435cf1c7c63df88bf3bb2bdf1eb1b75cd |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 超级直播助手 |
| 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 |
| --- | --- |
| apkcombo.com | IP: 174.36.228.136  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| c.tile.openstreetmap.org | IP: 31.13.85.169  所属国家: Brazil  地区: Sao Paulo  城市: Sao Paulo |
| b.tile.opentopomap.org | IP: 131.188.76.144  所属国家: Germany  地区: Bayern  城市: Erlangen |
| tiles.openseamap.org | IP: 195.37.132.70  所属国家: Germany  地区: Rheinland-Pfalz  城市: Franken |
| 110.41.35.57 | IP: 110.41.35.57  所属国家: China  地区: Guangdong  城市: Guangzhou |
| dev.virtualearth.net | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| a.tile.cloudmade.com | 没有服务器地理信息. |
| stackoverflow.com | IP: 104.18.32.7  所属国家: United States of America  地区: California  城市: San Francisco |
| tiles.wmflabs.org | IP: 31.13.92.5  所属国家: Ireland  地区: Dublin  城市: Dublin |
| apkpure.net | IP: 104.22.42.111  所属国家: United States of America  地区: California  城市: San Francisco |
| www.antlr.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| auth.cloudmade.com | IP: 23.21.136.107  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| wms.chartbundle.com | 没有服务器地理信息. |
| a.tile.opentopomap.org | IP: 131.188.76.144  所属国家: Germany  地区: Bayern  城市: Erlangen |
| zsh.sourceforge.net | IP: 104.18.12.149  所属国家: United States of America  地区: California  城市: San Francisco |
| issues.apache.org | IP: 168.119.33.54  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| a.tile.openstreetmap.org | IP: 74.86.17.48  所属国家: United States of America  地区: California  城市: San Jose |
| maps.wikimedia.org | IP: 103.102.166.240  所属国家: United States of America  地区: Indiana  城市: Francisco |
| c.tile.thunderforest.com | IP: 136.243.152.14  所属国家: Germany  地区: Berlin  城市: Berlin |
| www.gnu.org | IP: 209.51.188.116  所属国家: United States of America  地区: Massachusetts  城市: Somerville |
| material.io | IP: 216.239.32.21  所属国家: United States of America  地区: California  城市: Mountain View |
| basemap.nationalmap.gov | IP: 3.168.147.110  所属国家: United States of America  地区: Washington  城市: Seattle |
| api.xposed.info | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| a.tile.thunderforest.com | IP: 136.243.152.14  所属国家: Germany  地区: Berlin  城市: Berlin |
| tiswww.case.edu | IP: 129.22.12.56  所属国家: United States of America  地区: Ohio  城市: East Cleveland |
| www.showmyip.com | IP: 104.21.49.135  所属国家: United States of America  地区: California  城市: San Francisco |
| groovy-lang.org | IP: 148.251.23.208  所属国家: Germany  地区: Berlin  城市: Berlin |
| www.multispace.fyi | 没有服务器地理信息. |
| b.tile.openstreetmap.org | IP: 157.240.1.9  所属国家: United States of America  地区: California  城市: Menlo Park |
| api.tiles.mapbox.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| picocli.info | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| c.tile.cloudmade.com | 没有服务器地理信息. |
| www.example.com | IP: 23.218.94.16  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.magelang.com | IP: 76.223.54.146  所属国家: United States of America  地区: Washington  城市: Seattle |
| b.tile.thunderforest.com | IP: 88.99.70.11  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| schemas.android.com | 没有服务器地理信息. |
| openptmap.org | IP: 88.99.141.112  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| c.tile.opentopomap.org | IP: 131.188.76.144  所属国家: Germany  地区: Bayern  城市: Erlangen |
| api.mapbox.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| b.tile.cloudmade.com | 没有服务器地理信息. |
| overlay.openstreetmap.nl | IP: 93.186.176.173  所属国家: Netherlands  地区: Zuid-Holland  城市: Rotterdam |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://api.xposed.info/using.html | aliucord/hook/XposedModule.java |
| https://material.io/design/components/dialogs.html | com/afollestad/materialdialogs/o0O0Oo0O.java |
| http://www.ANTLR.org\ | groovyjarjarantlr/HTMLCodeGenerator.java |
| http://www.magelang.com\ | groovyjarjarantlr/HTMLCodeGenerator.java |
| http://www.ANTLR.org/\ | groovyjarjarantlr/DocBookCodeGenerator.java |
| http://schemas.android.com/apk/res/android | o00oo0O/o00oo0.java |
| http://schemas.android.com/apk/res/android | o00oo0Oo/o00oo0O0.java |
| http://schemas.android.com/apk/res/android | o0O0oOo0/o00oo0O0.java |
| https://www.showmyip.com/ | o0OO0o00/o0O0Oo.java |
| https://www.example.com | o0O0OooO/o0O00OO.java |
| https://issues.apache.org/jira/browse/GROOVY | org/codehaus/groovy/classgen/asm/sc/StaticTypesCallSiteWriter.java |
| https://issues.apache.org/jira/browse/GROOVY | org/codehaus/groovy/classgen/asm/indy/IndyCallSiteWriter.java |
| https://groovy-lang.org/ | org/codehaus/groovy/tools/FileSystemCompiler.java |
| https://a.tile.thunderforest.com/ | org/osmdroid/tileprovider/tilesource/ThunderforestTileSource.java |
| https://b.tile.thunderforest.com/ | org/osmdroid/tileprovider/tilesource/ThunderforestTileSource.java |
| https://c.tile.thunderforest.com/ | org/osmdroid/tileprovider/tilesource/ThunderforestTileSource.java |
| https://api.mapbox.com/v4/ | org/osmdroid/tileprovider/tilesource/MapBoxTileSource.java |
| http://1. | org/osmdroid/tileprovider/tilesource/HEREWeGoTileSource.java |
| http://2. | org/osmdroid/tileprovider/tilesource/HEREWeGoTileSource.java |
| http://3. | org/osmdroid/tileprovider/tilesource/HEREWeGoTileSource.java |
| http://4. | org/osmdroid/tileprovider/tilesource/HEREWeGoTileSource.java |
| http://api.tiles.mapbox.com/v4/ | org/osmdroid/tileprovider/tilesource/MapQuestTileSource.java |
| https://a.tile.openstreetmap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://b.tile.openstreetmap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://c.tile.openstreetmap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://maps.wikimedia.org/osm-intl/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| http://openptmap.org/tiles/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| http://a.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| http://b.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| http://c.tile.cloudmade.com/%s/%d/%d/%d/%d/%d%s?token=%s | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://overlay.openstreetmap.nl/openfietskaart-overlay/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://overlay.openstreetmap.nl/basemap/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://overlay.openstreetmap.nl/roads/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://tiles.wmflabs.org/hikebike/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://tiles.openseamap.org/seamark/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://basemap.nationalmap.gov/arcgis/rest/services/USGSTopo/MapServer/tile/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://basemap.nationalmap.gov/arcgis/rest/services/USGSImageryTopo/MapServer/tile/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://wms.chartbundle.com/tms/v1.0/wac/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://wms.chartbundle.com/tms/v1.0/enrh/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://wms.chartbundle.com/tms/v1.0/enrl/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://a.tile.opentopomap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://b.tile.opentopomap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://c.tile.opentopomap.org/ | org/osmdroid/tileprovider/tilesource/TileSourceFactory.java |
| https://dev.virtualearth.net/REST/V1/Imagery/Metadata/%s?mapVersion=v1&output=json&uriScheme=https&key=%s | org/osmdroid/tileprovider/tilesource/bing/BingMapTileSource.java |
| https://auth.cloudmade.com/token/ | org/osmdroid/tileprovider/util/CloudmadeUtil.java |
| http://picocli.info/) | groovyjarjarpicocli/AutoComplete.java |
| https://github.com/scop/bash-completion) | groovyjarjarpicocli/AutoComplete.java |
| http://stackoverflow.com/a/12495480/1440785\n | groovyjarjarpicocli/AutoComplete.java |
| http://tiswww.case.edu/php/chet/bash/FAQ\n | groovyjarjarpicocli/AutoComplete.java |
| https://www.gnu.org/software/bash/manual/html\_node/The-Shopt-Builtin.html\n | groovyjarjarpicocli/AutoComplete.java |
| http://zsh.sourceforge.net/Doc/Release/Options.html | groovyjarjarpicocli/AutoComplete.java |
| https://stackoverflow.com/questions/17042057/bash-check-element-in-array-for-elements-in-another-array/17042655 | groovyjarjarpicocli/AutoComplete.java |
| https://www.gnu.org/software/bash/manual/html\_node/Programmable-Completion.html | groovyjarjarpicocli/AutoComplete.java |
| https://stackoverflow.com/questions/3249432/can-a-bash-tab-completion-script-be-used-in-zsh/27853970 | groovyjarjarpicocli/AutoComplete.java |
| https://github.com/L-JINBIN/ApkSignatureKillerEx | bin/mt/signature/KillerApplication.java |
| http://110.41.35.57/up | o0OO0/o0O0OOoO.java |
| http://www.multispace.fyi/update/vcam/up.txt | o0OO0/o0O0OOoO.java |
| https://github.com/andvipgroup/VCamera | o0OO00o/o0O0OOoO.java |
| https://apkcombo.com | o0OO00o/o0O0OOoO.java |
| https://apkpure.net | o0OO00o/o0O0OOoO.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| parrt@antlr.org | groovyjarjarantlr/Tool.java |
| thetick@magelang.com | groovyjarjarantlr/debug/LLkDebuggingParser.java |
| irvinfabian97@gmail.com | o0OO00o/o0O0OOoO.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869192 | groovyjarjarantlr/ANTLRTokdefLexer.java |
| 17179869192 | groovyjarjarantlr/ANTLRLexer.java |
| 17179869192 | groovyjarjarantlr/preprocessor/PreprocessorLexer.java |
| 17179869192 | groovyjarjarantlr/actions/cpp/ActionLexer.java |
| 17179869192 | groovyjarjarantlr/actions/csharp/ActionLexer.java |
| 17179869192 | groovyjarjarantlr/actions/java/ActionLexer.java |
| 17179869192 | groovyjarjarantlr/actions/python/ActionLexer.java |
| 17179869184 | groovyjarjarantlr4/v4/parse/ANTLRParser.java |
| 17179870210 | org/codehaus/groovy/antlr/java/JavaRecognizer.java |
| 17179878408 | org/codehaus/groovy/antlr/java/JavaLexer.java |
| 16706960926 | org/codehaus/groovy/antlr/parser/GroovyRecognizer.java |
| 15569256464 | org/codehaus/groovy/antlr/parser/GroovyRecognizer.java |
| 17179869185 | org/codehaus/groovy/antlr/parser/GroovyLexer.java |

## **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=CN, ST=aaaaa, L=aaaaa, O=aaaaa, OU=aaaaa, CN=aaaaa 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-20 04:37:55+00:00 有效期至: 2050-04-14 04:37:55+00:00 发行人: C=CN, ST=aaaaa, L=aaaaa, O=aaaaa, OU=aaaaa, CN=aaaaa 序列号: 0x2b0b90e7 哈希算法: sha256 md5值: 2d25aeb3559101590234a7e9e0d2583d sha1值: b115554764220888626203fc241e2a0de97d1abd sha256值: cc94d84c40a2d10547228de54ae1b55326d27428380fc1bb091546f26de43d5b sha512值: ec2a896d328137a82f5a80928524e16618a461ac719edd561c3c516a46dcb7b94d7f974c18d43071adbfed161dba04b3a44e9a787773785582ff7fd24bb9b063 公钥算法: rsa 密钥长度: 2048 指纹: 32f41b765f918d0bc152dc91dcc7a0407925820703ca0e816047418d01efc13f**

## **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。**