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

**None（ 2.6.2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 | None |
| 版本 | 2.6.2 |
| 包名 | com.lvcha.main |
| 域名线索 | 170条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | 绿茶VPN\_2.6.2.apks |
| 文件大小 | 7.3MB |
| MD5值 | 5ddd310572bc4874130df91042a6c6de |
| SHA1值 | 90b936029088c9d4846ac262c416dd8cdb83af99 |
| SHA256值 | 10c8d077812bb5ce95fb12701a631d160a4910dc376cc49cc349916dc2d1d435 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | None |
| 包名 | com.lvcha.main |
| 主活动Activity | com.lvcha.main.activity.WelcomeActivity |
| 安卓版本名称 | 2.6.2 |
| 安卓版本 | 30 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.flickr.com | IP: 157.240.6.35  所属国家: Colombia  地区: Distrito Capital de Bogota  城市: Bogota |
| app.ejsen.cn | IP: 38.14.94.36  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| www.reddit.com | IP: 199.16.156.11  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| www.dlsite.com | IP: 104.18.3.173  所属国家: United States of America  地区: California  城市: San Francisco |
| fate-go.us | IP: 13.35.202.4  所属国家: India  地区: Telangana  城市: Hyderabad |
| app-measurement.com | IP: 114.250.65.33  所属国家: China  地区: Beijing  城市: Beijing |
| www.amazon.com | IP: 3.165.88.168  所属国家: United States of America  地区: Washington  城市: Seattle |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.huffpost.com | IP: 199.59.150.12  所属国家: United States of America  地区: California  城市: San Francisco |
| www.bbc.com | IP: 108.160.166.61  所属国家: United States of America  地区: California  城市: San Francisco |
| smodin.io | IP: 34.117.39.253  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.nexon.com | IP: 52.84.150.53  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.chatgpt.com | IP: 128.121.243.77  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.threads.net | IP: 157.240.3.8  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.drivethrucomics.com | IP: 104.21.52.78  所属国家: United States of America  地区: California  城市: San Francisco |
| www.naver.com | IP: 223.130.200.236  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| www.dmm.com | IP: 13.33.97.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.notion.so | IP: 208.103.161.2  所属国家: United States of America  地区: South Carolina  城市: Mount Pleasant |
| www.tumblr.com | IP: 199.16.156.103  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| www.booking.com | IP: 108.157.254.54  所属国家: United States of America  地区: Washington  城市: Seattle |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| 17.live | IP: 31.13.85.53  所属国家: Brazil  地区: Sao Paulo  城市: Sao Paulo |
| mixi.jp | IP: 103.97.176.73  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| zoom.us | IP: 170.114.52.2  所属国家: United States of America  地区: California  城市: San Jose |
| meet.google.com | IP: 142.250.73.110  所属国家: United States of America  地区: California  城市: Mountain View |
| google.com | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| runwayml.com | IP: 76.76.21.21  所属国家: United States of America  地区: California  城市: Walnut |
| line.me | IP: 31.13.95.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.voachinese.com | IP: 104.244.43.208  所属国家: United States of America  地区: California  城市: San Francisco |
| www.mail.com | IP: 82.165.229.59  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Strang |
| www.yahoo.com | IP: 69.147.80.12  所属国家: United States of America  地区: New York  城市: New York City |
| www.dailymotion.com | IP: 31.13.70.33  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.midjourney.com | IP: 172.64.154.39  所属国家: United States of America  地区: California  城市: San Francisco |
| time.com | IP: 154.85.102.32  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.imdb.com | IP: 13.33.92.21  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.deepl.com | IP: 104.18.39.209  所属国家: United States of America  地区: California  城市: San Francisco |
| www.facebook.com | IP: 31.13.96.195  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.sudowrite.com | IP: 216.24.57.1  所属国家: United States of America  地区: California  城市: San Francisco |
| www.marvelsuperwar.com | 没有服务器地理信息. |
| www.foxnews.com | IP: 151.101.90.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.instagram.com | IP: 103.252.115.153  所属国家: Singapore  地区: Singapore  城市: Singapore |
| tubitv.com | IP: 3.170.229.129  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.kakaocorp.com | IP: 211.249.221.227  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| firebase-settings.crashlytics.com | IP: 114.250.65.34  所属国家: China  地区: Beijing  城市: Beijing |
| tw.yahoo.com | IP: 157.240.10.41  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.cryptocompare.com | IP: 104.26.3.124  所属国家: United States of America  地区: California  城市: San Francisco |
| www.dw.com | IP: 50.117.117.42  所属国家: United States of America  地区: California  城市: Santa Clara |
| www.snapchat.com | IP: 34.149.46.130  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.feixiaohao.com | IP: 31.13.75.12  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.agedm.org | IP: 23.225.30.102  所属国家: United States of America  地区: California  城市: Los Angeles |
| copy.ai | IP: 44.229.220.222  所属国家: United States of America  地区: Oregon  城市: Portland |
| www.worldcoinindex.com | IP: 104.26.15.233  所属国家: United States of America  地区: California  城市: San Francisco |
| www.camfrog.com | IP: 104.22.63.133  所属国家: United States of America  地区: California  城市: San Francisco |
| vk.com | IP: 87.240.132.67  所属国家: Russian Federation  地区: Sankt-Peterburg  城市: Saint Petersburg |
| stablediffusionweb.com | IP: 69.63.186.31  所属国家: United States of America  地区: New York  城市: New York City |
| www.xe.com | IP: 3.169.183.18  所属国家: United States of America  地区: Washington  城市: Seattle |
| edition.cnn.com | IP: 151.101.3.5  所属国家: United States of America  地区: California  城市: San Francisco |
| www.rakuten.co.jp | IP: 199.96.62.21  所属国家: United States of America  地区: California  城市: San Francisco |
| goo.gl | IP: 142.250.73.110  所属国家: United States of America  地区: California  城市: Mountain View |
| www.messenger.com | IP: 202.160.130.118  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.thetrainline.com | IP: 13.35.37.46  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| www.toptoon.net | IP: 69.30.25.21  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.apkpure.net | IP: 172.67.11.98  所属国家: United States of America  地区: California  城市: San Francisco |
| www3.nhk.or.jp | IP: 23.215.160.189  所属国家: Australia  地区: South Australia  城市: Adelaide |
| www.pinterest.com | IP: 108.160.170.44  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 |
| www.afreecatv.com | IP: 61.253.217.81  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.disney.com | IP: 23.193.186.143  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.netflix.com | IP: 44.240.158.19  所属国家: United States of America  地区: Oregon  城市: Portland |
| discord.com | IP: 128.242.240.85  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.grab.com | IP: 13.35.37.58  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| sp.nicovideo.jp | IP: 128.121.146.228  所属国家: United States of America  地区: California  城市: Sacramento |
| www.walmart.com | IP: 23.219.69.182  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| zenly.com | IP: 34.120.54.238  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| twitter.com | IP: 199.59.148.247  所属国家: United States of America  地区: California  城市: San Francisco |
| mir4global.com | IP: 13.72.197.150  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.wsj.com | IP: 199.59.148.8  所属国家: United States of America  地区: California  城市: San Francisco |
| bard.google.com | IP: 142.250.73.110  所属国家: United States of America  地区: California  城市: Mountain View |
| www.pixiv.net | IP: 199.16.158.104  所属国家: United States of America  地区: California  城市: San Francisco |
| www.gocomics.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| cn.nytimes.com | IP: 108.160.163.108  所属国家: United States of America  地区: California  城市: San Francisco |
| genshin.hoyoverse.com | IP: 108.157.254.20  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.sephora.com | IP: 23.192.152.99  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.canva.com | IP: 104.16.102.112  所属国家: United States of America  地区: California  城市: San Francisco |
| www.tradingview.com | IP: 31.13.88.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.youtube.com | IP: 31.13.94.49  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.shiekhshoes.com | IP: 44.229.241.209  所属国家: United States of America  地区: Oregon  城市: Portland |
| firebase.google.com | IP: 142.250.73.78  所属国家: United States of America  地区: California  城市: Mountain View |
| zoom.earth | IP: 104.26.5.90  所属国家: United States of America  地区: California  城市: San Francisco |
| pagead2.googlesyndication.com | IP: 114.250.64.38  所属国家: China  地区: Beijing  城市: Beijing |
| www.lazada.com | IP: 163.181.35.186  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.olevod.com | IP: 157.240.2.14  所属国家: United States of America  地区: California  城市: Menlo Park |
| nikke.hotcool.tw | IP: 104.21.43.36  所属国家: United States of America  地区: California  城市: San Francisco |
| www.toranoana.jp | IP: 52.199.56.83  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| jumpshop-online.com | IP: 23.227.38.65  所属国家: Canada  地区: Ontario  城市: Ottawa |
| www.tiktok.com | IP: 199.96.59.95  所属国家: United States of America  地区: California  城市: San Francisco |
| planetix.com | IP: 172.67.207.68  所属国家: United States of America  地区: California  城市: San Francisco |
| character.ai | IP: 43.226.16.8  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| crowd1.com | IP: 104.18.0.188  所属国家: United States of America  地区: California  城市: San Francisco |
| www.gate.io | IP: 108.160.165.8  所属国家: United States of America  地区: California  城市: San Francisco |
| www.grailed.com | IP: 104.16.234.118  所属国家: United States of America  地区: California  城市: San Francisco |
| myspace.com | IP: 34.111.176.156  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| play.google.com | IP: 8.7.198.46  所属国家: United States of America  地区: Louisiana  城市: Monroe |
| youtrack.jetbrains.com | IP: 63.35.30.167  所属国家: Ireland  地区: Dublin  城市: Dublin |
| scholar.google.com | IP: 142.250.73.100  所属国家: United States of America  地区: California  城市: Mountain View |
| www.grammarly.com | IP: 108.156.144.53  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.hulu.com | IP: 104.126.37.179  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.chinatimes.com | IP: 172.66.134.48  所属国家: United States of America  地区: California  城市: San Francisco |
| store.steampowered.com | IP: 23.215.161.136  所属国家: Australia  地区: South Australia  城市: Adelaide |
| www.wikipedia.org | IP: 157.240.17.35  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| www.bing.com | IP: 202.89.233.100  所属国家: China  地区: Beijing  城市: Beijing |
| www.outwrite.com | IP: 66.33.60.34  所属国家: Canada  地区: Ontario  城市: Etobicoke |
| www.ebay.com | IP: 23.215.161.87  所属国家: Australia  地区: South Australia  城市: Adelaide |
| vimeo.com | IP: 157.240.17.35  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| www.marvel.com | IP: 13.35.37.10  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| www.mercari.com | IP: 88.191.249.183  所属国家: France  地区: Ile-de-France  城市: Paris |
| tinder.com | IP: 52.84.150.60  所属国家: United States of America  地区: Washington  城市: Seattle |
| chat.openai.com | IP: 157.240.0.18  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.dc.com | IP: 151.101.89.55  所属国家: United States of America  地区: California  城市: San Francisco |
| www.shixinfo.com | IP: 39.108.2.129  所属国家: China  地区: Guangdong  城市: Shenzhen |
| drive.google.com | IP: 199.16.156.75  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| www.binance.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| www.linkedin.com | IP: 52.130.75.155  所属国家: China  地区: Shanghai  城市: Shanghai |
| www.telltale.com | IP: 173.236.159.172  所属国家: United States of America  地区: California  城市: Brea |
| plus.google.com | IP: 159.138.20.20  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.cz01.vip | IP: 45.154.214.60  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.mozilla.org | IP: 151.101.91.19  所属国家: United States of America  地区: California  城市: San Francisco |
| www.nordstrom.com | IP: 151.101.90.132  所属国家: United States of America  地区: California  城市: San Francisco |
| coinw.zendesk.com | IP: 104.18.249.37  所属国家: United States of America  地区: California  城市: San Francisco |
| mail.google.com | IP: 142.250.73.69  所属国家: United States of America  地区: California  城市: Mountain View |
| www.twitch.tv | IP: 98.159.108.58  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.zongheng.com | IP: 116.205.2.101  所属国家: China  地区: Beijing  城市: Beijing |
| www.skype.com | IP: 52.113.194.133  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.tvbanywhere.com | IP: 3.165.102.60  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.viu.com | IP: 3.165.78.245  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.nba2k.com | IP: 192.81.242.63  所属国家: United States of America  地区: New York  城市: New York City |
| sms-activate.org | IP: 172.67.73.248  所属国家: United States of America  地区: California  城市: San Francisco |
| www.coupang.com | IP: 23.215.162.7  所属国家: Australia  地区: South Australia  城市: Adelaide |
| www.taptap.io | IP: 104.18.1.19  所属国家: United States of America  地区: California  城市: San Francisco |
| wildrift.leagueoflegends.com | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.suruga-ya.com | IP: 59.188.250.54  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| slack.com | IP: 52.192.46.121  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| metamask.io | IP: 199.59.148.206  所属国家: United States of America  地区: California  城市: San Francisco |
| arabic.nsfx.com | IP: 18.197.205.127  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| ethermine.org | IP: 199.59.148.209  所属国家: United States of America  地区: California  城市: San Francisco |
| www.maxmovie.com | IP: 43.202.27.194  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| zapier.com | IP: 3.166.228.65  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.microsoft.com | IP: 221.194.156.64  所属国家: China  地区: Hebei  城市: Langfang |
| pimeyes.com | IP: 168.143.171.186  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| ani.gamer.com.tw | IP: 118.107.180.216  所属国家: Palestine, State of  地区: Hebron  城市: Hebron |
| www.potato.im | IP: 162.125.2.3  所属国家: United States of America  地区: California  城市: San Francisco |
| opensea.io | IP: 31.13.95.48  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.theguardian.com | IP: 157.240.1.33  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.whatsapp.com | IP: 104.244.46.93  所属国家: United States of America  地区: California  城市: San Francisco |
| stackoverflow.com | IP: 104.18.32.7  所属国家: United States of America  地区: California  城市: San Francisco |
| www.googleadservices.com | IP: 114.250.69.38  所属国家: China  地区: Beijing  城市: Beijing |
| web.telegram.org | IP: 98.159.108.71  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.coinbase.com | IP: 104.18.35.15  所属国家: United States of America  地区: California  城市: San Francisco |
| www.htx.com | IP: 209.95.56.60  所属国家: United States of America  地区: Utah  城市: Salt Lake City |
| www.tokenpocket.pro | IP: 163.181.228.146  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.google.com | IP: 199.59.148.229  所属国家: United States of America  地区: California  城市: San Francisco |
| lubansms.com | IP: 172.67.74.40  所属国家: United States of America  地区: California  城市: San Francisco |
| www.okx.com | IP: 169.254.0.2  所属国家: -  地区: -  城市: - |
| www.ea.com | IP: 23.215.160.165  所属国家: Australia  地区: South Australia  城市: Adelaide |
| token.im | IP: 172.67.6.50  所属国家: United States of America  地区: California  城市: San Francisco |
| www.quora.com | IP: 162.159.153.247  所属国家: United States of America  地区: California  城市: San Francisco |
| www.walgreens.com | IP: 23.218.94.231  所属国家: Australia  地区: New South Wales  城市: Sydney |
| m.iyf.tv | IP: 172.64.154.69  所属国家: United States of America  地区: California  城市: San Francisco |
| www.pubgmobile.com | IP: 173.222.248.86  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| shopee.com | IP: 143.92.82.21  所属国家: Singapore  地区: Singapore  城市: Singapore |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/FasterXML/jackson-databind/issues/2715 | com/fasterxml/jackson/databind/PropertyNamingStrategy.java |
| http://javax.xml.XMLConstants/feature/secure-processing | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| http://apache.org/xml/features/disallow-doctype-decl | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| http://javax.xml.XMLConstants/feature/secure-processing | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| http://javax.xml.XMLConstants/property/accessExternalDTD | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| https://www.tiktok.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.youtube.com\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://twitter.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.instagram.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.facebook.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://web.telegram.org\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.voachinese.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.netflix.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.amazon.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.binance.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.apkpure.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://chat.openai.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.pixiv.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.bbc.com/zhongwen/simp\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.wikipedia.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://line.me/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.twitch.tv/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://store.steampowered.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://play.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://github.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.disney.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.hulu.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.chatgpt.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://character.ai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://bard.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://runwayml.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grammarly.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.midjourney.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.sudowrite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.outwrite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://copy.ai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.canva.com/design/play\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.notion.so/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zapier.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://smodin.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://stablediffusionweb.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://github.com/features/copilot\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://vimeo.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tvbanywhere.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.olevod.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.viu.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.imdb.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://m.iyf.tv/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tubitv.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.cz01.vip/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://17.live/en\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.afreecatv.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.maxmovie.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dailymotion.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dlsite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://jumpshop-online.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://ani.gamer.com.tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://sp.nicovideo.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.suruga-ya.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.toptoon.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dmm.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.agedm.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dc.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.marvel.com/unlimited\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.amazon.com/kindle-dbs/comics-store/home\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.drivethrucomics.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.toranoana.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.gocomics.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.zongheng.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.chinatimes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tw.yahoo.com/?p=dnr\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://cn.nytimes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.quora.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dw.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.foxnews.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www3.nhk.or.jp/nhkworld/zh/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.reddit.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://edition.cnn.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://time.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.theguardian.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.huffpost.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.wsj.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.threads.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://web.telegram.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.whatsapp.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tinder.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.potato.im/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mixi.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.kakaocorp.com/page/?lang=ENG\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.messenger.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://vk.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.camfrog.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.snapchat.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.pinterest.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tumblr.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zenly.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.flickr.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://myspace.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://nikke.hotcool.tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://discord.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.taptap.io/app/154140\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://genshin.hoyoverse.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://wildrift.leagueoflegends.com/zh-tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.ea.com/en-gb/games/apex-legends\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mir4global.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.pubgmobile.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://fate-go.us/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nexon.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.marvelsuperwar.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.telltale.com/batman-a-telltale-story/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nba2k.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tradingview.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://app.ejsen.cn/index1.html\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.shixinfo.com/download/ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://coinw.zendesk.com/hc/zh-cn\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.okx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.feixiaohao.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://opensea.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tokenpocket.pro/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://planetix.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.gate.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.htx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://metamask.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://token.im/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://ethermine.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.cryptocompare.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.worldcoinindex.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.coinbase.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://arabic.nsfx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://shopee.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.coupang.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mercari.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.lazada.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.rakuten.co.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.ebay.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.sephora.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nordstrom.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grailed.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.walgreens.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.shiekhshoes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.walmart.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.deepl.com/translator\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.linkedin.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mail.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://scholar.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://stackoverflow.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zoom.us/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://meet.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://crowd1.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://drive.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://slack.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.microsoft.com/en-sg/microsoft-teams/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.skype.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/maps/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.xe.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.booking.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.thetrainline.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grab.com/cn/xia-zai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://pimeyes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.yahoo.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/chrome/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.bing.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zoom.earth/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mozilla.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.naver.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mail.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://lubansms.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://sms-activate.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://plus.google.com/ | defpackage/bp3.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | defpackage/d82.java |
| https://app-measurement.com/s/d | defpackage/yj3.java |
| https://app-measurement.com/a | defpackage/yj3.java |
| https://youtrack.jetbrains.com/issue/KT-55980 | defpackage/l91.java |
| https://firebase.google.com/docs/analytics | defpackage/hq2.java |
| https://google.com/search? | defpackage/yd3.java |
| https://www.google.com | defpackage/qn3.java |
| https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s | defpackage/qn3.java |
| https://goo.gl/NAOOOI. | defpackage/qn3.java |
| https://goo.gl/NAOOOI | defpackage/qn3.java |
| https://firebase.google.com/docs/crashlytics/get-started?platform=android | defpackage/xq.java |
| https://firebase.google.com/support/privacy/init-options. | defpackage/l60.java |
| https://app-measurement.com/a | defpackage/ef2.java |
| https://app-measurement.com/s/d | defpackage/ef2.java |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings | defpackage/ik1.java |
| https://firebase.google.com/support/guides/disable-analytics | defpackage/ux2.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0  u0013android@android.com | defpackage/l33.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15552000000 | defpackage/t83.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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2024-07-14 18:03:35+00:00 有效期至: 2054-07-14 18:03:35+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xe54213c072331c3ac9faadbf3f1f08475b7b18a7 哈希算法: sha256 md5值: 67d39b068440e1c4959ac577663431de sha1值: eb9a5f0f9e519cc45b0328f29e1878ce50574997 sha256值: 2f8deaf7bf3056232dbbbad7788212ff514ec637f6e351936f0449b88add8e40 sha512值: e69eb40ce895ef7b0f6cc098bb6a8f2cda44671f6ea2f4bb642db48ceecd72d4163d31e699c3a7a5d97cdd60d6fb3e25274d0820517a475c19a154b650514dd8 公钥算法: rsa 密钥长度: 4096 指纹: eb3b48e865c4ef0f41e68baa01ae46f7befe3966551ae1aea73da41628473eeb**

## **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.FOREGROUND\_SERVICE\_SYSTEM\_EXEMPTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.android.vending.BILLING | 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| 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 |
| 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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.lvcha.main.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**