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

**快柠檬（ 1.09.0102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 | 快柠檬 |
| 版本 | 1.09.0102 |
| 包名 | com.falemon.fastlemon |
| 域名线索 | 47条 |
| URL线索 | 14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 | 4\_5798820944751366281.apk |
| 文件大小 | 36.12MB |
| MD5值 | f19cd538837c94d99f8274ae4e821444 |
| SHA1值 | 3c2685ddae7eaf673f6cb7e8d3358633f19552f2 |
| SHA256值 | 7cf3afea9272229d2d2dee65e9cb8f0d84755b66f733861978b4d9ebd3d174f2 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 快柠檬 |
| 包名 | com.falemon.fastlemon |
| 主活动Activity | com.faultyworld.walkthrough.MainActivity |
| 安卓版本名称 | 1.09.0102 |
| 安卓版本 | 109 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| falm.shop | IP: 172.67.165.250 所属国家: United States of America 地区: California 城市: San Francisco  |
| vm483584.stark-industries.solutions | 没有服务器地理信息.  |
| www.google.com | IP: 199.59.148.20 所属国家: United States of America 地区: California 城市: San Francisco  |
| 172-105-201-193.ip.linodeusercontent.com | IP: 172.105.201.193 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| vm485596.stark-industries.solutions | 没有服务器地理信息.  |
| api.falm.cc | IP: 172.67.156.39 所属国家: United States of America 地区: California 城市: San Francisco  |
| knmvd.com | IP: 104.21.96.127 所属国家: United States of America 地区: California 城市: San Francisco  |
| aomedia.org | IP: 199.59.150.39 所属国家: United States of America 地区: California 城市: San Francisco  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| 139-144-123-209.ip.linodeusercontent.com | IP: 139.144.123.209 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ghproxy.com | IP: 144.24.81.189 所属国家: Korea (Republic of) 地区: Gangwon-do 城市: Chuncheon  |
| client.relay.crisp.chat | IP: 159.65.139.183 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| connectivitycheck.gstatic.com | IP: 203.208.43.98 所属国家: China 地区: Beijing 城市: Beijing  |
| vm869667.stark-industries.solutions | 没有服务器地理信息.  |
| pub.dev | IP: 34.36.0.14 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| knmva.store | IP: 103.224.212.109 所属国家: Australia 地区: Victoria 城市: Beaumaris  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 172-105-212-236.ip.linodeusercontent.com | IP: 172.105.212.236 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| developer.android.com | IP: 142.250.73.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.google-analytics.com | IP: 216.239.34.178 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.gstatic.com | IP: 203.208.50.34 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| knmvb.site | IP: 172.67.195.209 所属国家: United States of America 地区: California 城市: San Francisco  |
| default.url | 没有服务器地理信息.  |
| c.tenor.com | IP: 108.160.169.171 所属国家: United States of America 地区: California 城市: San Francisco  |
| client.crisp.chat | IP: 104.18.29.104 所属国家: United States of America 地区: California 城市: San Francisco  |
| abs.twimg.com | IP: 151.101.88.159 所属国家: United States of America 地区: California 城市: San Francisco  |
| main-so-b9gyd9ejdhe4f3gj.z01.azurefd.net | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| static.cloudflareinsights.com | IP: 104.16.80.73 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.apple.com | IP: 17.253.87.198 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| vm496390.stark-industries.solutions | 没有服务器地理信息.  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| cs510.wpc.edgecastcdn.net | IP: 208.43.170.231 所属国家: United States of America 地区: Texas 城市: Dallas  |
| vm496402.stark-industries.solutions | 没有服务器地理信息.  |
| raw.githubusercontent.com | IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.googletagmanager.com | IP: 114.250.67.41 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| twitter.com | IP: 174.36.228.136 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| googlehosted.l.googleusercontent.com | IP: 142.250.69.161 所属国家: United States of America 地区: California 城市: Mountain View  |
| 172-104-64-244.ip.linodeusercontent.com | IP: 172.104.64.244 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| falm.cc | IP: 172.67.156.39 所属国家: United States of America 地区: California 城市: San Francisco  |
| 121.196.147.118 | IP: 121.196.147.118 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| https://www.google.com  | com/faultyworld/walkthrough/MainActivity.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | i2/u0.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | e4/z.java  |
| https://x</LA\_URL>  | m2/k0.java  |
| https://default.url  | m2/k0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | m2/l0.java  |
| http://dashif.org/guidelines/last-segment-number  | o3/d.java  |
| http://dashif.org/guidelines/trickmode  | o3/d.java  |
| http://dashif.org/thumbnail\_tile  | o3/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | o3/d.java  |
| http://ns.adobe.com/xap/1.0/  | s2/a.java  |
| https://aomedia.org/emsg/ID3  | c3/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | c3/a.java  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| https://github.com/apvarun/toastify-js  | 摸瓜V2引擎  |
| falm.shop  | 摸瓜V3引擎  |
| vm483584.stark-industries.solutions  | 摸瓜V3引擎  |
| 172-105-201-193.ip.linodeusercontent.com  | 摸瓜V3引擎  |
| vm485596.stark-industries.solutions  | 摸瓜V3引擎  |
| api.falm.cc  | 摸瓜V3引擎  |
| knmvd.com  | 摸瓜V3引擎  |
| 139-144-123-209.ip.linodeusercontent.com  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| client.relay.crisp.chat  | 摸瓜V3引擎  |
| connectivitycheck.gstatic.com  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| vm869667.stark-industries.solutions  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| knmva.store  | 摸瓜V3引擎  |
| firebaseinstallations.googleapis.com  | 摸瓜V3引擎  |
| 172-105-212-236.ip.linodeusercontent.com  | 摸瓜V3引擎  |
| www.google-analytics.com  | 摸瓜V3引擎  |
| www.gstatic.com  | 摸瓜V3引擎  |
| instantmessaging-pa.googleapis.com  | 摸瓜V3引擎  |
| knmvb.site  | 摸瓜V3引擎  |
| android.googleapis.com  | 摸瓜V3引擎  |
| c.tenor.com  | 摸瓜V3引擎  |
| client.crisp.chat  | 摸瓜V3引擎  |
| abs.twimg.com  | 摸瓜V3引擎  |
| gmscompliance-pa.googleapis.com  | 摸瓜V3引擎  |
| static.cloudflareinsights.com  | 摸瓜V3引擎  |
| vm496390.stark-industries.solutions  | 摸瓜V3引擎  |
| cs510.wpc.edgecastcdn.net  | 摸瓜V3引擎  |
| vm496402.stark-industries.solutions  | 摸瓜V3引擎  |
| www.googletagmanager.com  | 摸瓜V3引擎  |
| twitter.com  | 摸瓜V3引擎  |
| googlehosted.l.googleusercontent.com  | 摸瓜V3引擎  |
| 172-104-64-244.ip.linodeusercontent.com  | 摸瓜V3引擎  |
| https://raw.githubusercontent.com/Faalemon/cloud/main/api.json  | lib/armeabi-v7a/libapp.so  |
| https://main-so-b9gyd9ejdhe4f3gj.z01.azurefd.net/system/3rdparty/cloud/api.json  | lib/armeabi-v7a/libapp.so  |
| http://127.0.0.1:  | lib/armeabi-v7a/libapp.so  |
| https://api.falm.cc  | lib/armeabi-v7a/libapp.so  |
| https://falm.cc/p/downloads  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| https://knmvd.com/system/3rdparty/cloud/api.json  | lib/armeabi-v7a/libapp.so  |
| http://121.196.147.118:38080/api.json  | lib/armeabi-v7a/libapp.so  |
| https://ghproxy.com/https://raw.githubusercontent.com/Faalemon/cloud/main/api.json  | lib/armeabi-v7a/libapp.so  |
| https://pub.dev/packages/dart\_ping  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| \_httpparser@13463476.responsepa \_double@0150898.fromintege .\_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat c\_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec -\_list@0150898.\_ofarray z\_timer@1026248.periodic m\_growablelist@0150898.\_literal2 g\_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_casterror@0150898.\_create l\_invocationmirror@0150898.\_withtype i\_rawsocket@14069316.\_writepipe 5\_nativesocket@14069316.watchsigna \_growablelist@0150898.\_literal1 4\_uri@0150898.file q\_imagefilter@16065589.blur \_growablelist@0150898.\_literal4 bb\_growablelist@0150898.\_ofgrowabl x\_growablelist@0150898.of \_nativesocket@14069316.pipe velocitytrackermixin@340039605.withkind \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_list@0150898.of \_list@0150898.generate n\_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 u\_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe storationinformation@1155124995.fromserial \_socket@14069316.\_readpipe \_list@0150898.\_ofother eo\_bytebuffer@7027147.\_new ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create av\_nativesocket@14069316.normal lectiontoolbarbutton@879113492.text \_uri@0150898.directory qd\_growablelist@0150898.\_literal8 v\_file@14069316.fromrawpat lectiontoolbarbutton@759392285.text gh\_growablelist@0150898.generate \_uri@0150898.notsimple 7u\_growablelist@0150898.\_literal7 \_\_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| go-tun2socks@v1.16  | lib/armeabi-v7a/libgojni.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | k4/a.java  |
| 15222222222  | t2/e.java  |

## **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: C=FL, ST=FL, L=FL, O=falemon, OU=FastLemon, CN=Fast 签名算法: rsassa\_pkcs1v15 有效期自: 2022-03-26 13:07:39+00:00 有效期至: 2049-08-11 13:07:39+00:00 发行人: C=FL, ST=FL, L=FL, O=falemon, OU=FastLemon, CN=Fast 序列号: 0x67925f1f70b5feb7 哈希算法: sha256 md5值: 1f2034d8cfdb65b43fe2514aca7b7c5e sha1值: 3973a1e660139ec572534fbb90b5204913b64f0f sha256值: bbd8137e15cb07363f71c25d2b72875c179d534c27f73391820a72f2586b4a83 sha512值: 61bf5e5a5391cd23bc3fdc4d1a09d2f8fa10aaa04dbeeccec3c2bc3cab966af5db8ec96c89590187c4cbbddcccd5ccaf312480bbc40304f16cbcb62a836b24f4 公钥算法: rsa 密钥长度: 2048 指纹: 5520b2afa346e5d33a749d118774128a454da7c42ad5744af09808fca51751e3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "password" : "Password"  |
| "verify\_certificate" : "Verify Certificate"  |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.POST\_NOTIFICATIONS | 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.falemon.fastlemon.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |

## **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。**