



## ANDROID 静态分析报告



◆ 萌萝社 • v1.1

分析日期: 2024-06-06 16:06:34

i应用概览

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| 文件名称:     | d24ff8c4d33d142a760dc4204273e1beb70265dca0a7f5709831f08e37176df8.apk |
| 文件大小:     | 20.44MB                                                              |
| 应用名称:     | 萌萝社                                                                  |
| 软件包名:     | shink.mlsrj.wallc                                                    |
| 主活动:      | flc.ast.SplashActivity                                               |
| 版本号:      | 1.11                                                                 |
| 最小SDK:    | 21                                                                   |
| 目标SDK:    | 31                                                                   |
| 加固信息:     | 360加固 加固                                                             |
| 应用程序安全分数: | 42/100 (中风险)                                                         |
| 跟踪器检测:    | 3/432                                                                |
| 杀软检测:     | 6 个杀毒软件报毒                                                            |
| MD5:      | 5b051768df155be5e392553b467714d7                                     |
| SHA1:     | 3bd0d03a276f760adce1e50cb52c1711b03f3583                             |
| SHA256:   | d24ff8c4d33d142a760dc4204273e1beb70265dca0a7f5709831f08e37176df8     |

分析结果严重性分布

|    |    |    |    |    |
|----|----|----|----|----|
| 高危 | 中危 | 信息 | 安全 | 关注 |
| 4  | 2  | 1  | 1  | 17 |

四大组件导出状态统计

|                                 |
|---------------------------------|
| Activity组件: 68个, 其中export的有: 0个 |
| Service组件: 12个, 其中export的有: 0个  |
| Receiver组件: 1个, 其中export的有: 0个  |
| Provider组件: 11个, 其中export的有: 0个 |

应用签名证书信息

二进制文件已签名

v1 签名: True  
v2 签名: True  
v3 签名: True  
v4 签名: False  
主题: C=CN, ST=CN, L=CN, O=xingjishidai, OU=xingjishidai, CN=xingjishidai  
签名算法: rsassa\_pkcs1v15  
有效期自: 2022-07-25 03:59:17+00:00  
有效期至: 2047-07-19 03:59:17+00:00  
发行人: C=CN, ST=CN, L=CN, O=xingjishidai, OU=xingjishidai, CN=xingjishidai  
序列号: 0x21e191b8  
哈希算法: sha256  
证书MD5: f394fe189c50eb8fd342108d04ede0fc  
证书SHA1: b3fef0cfea2cf420e8a539add830e19422c77b84  
证书SHA256: d5a9d87be12e3d131e0f847a584140e45f602e3c93a1e51dc04bebc07f154d0  
证书SHA512: d22e356ea58d138ddac4f6ef8ebac8317c6271ecd6257042e29a24384cbdd7e522008779d44283e53b018f97f4fd4ec734b4c0a8521a21baaf914ca2f599863  
  
公钥算法: rsa  
密钥长度: 2048  
指纹: fa851b3daa461656360dc203d3ea850e073971dfac0441b2e6bd2e62b56c1d3f  
找到 1 个唯一证书

权限声明与风险分级

| 权限名称                                               | 安全等级 | 权限内容           | 权限描述                                                    |
|----------------------------------------------------|------|----------------|---------------------------------------------------------|
| android.permission.ACCESS_NETWORK_STATE            | 普通   | 获取网络状态         | 允许应用程序查看网络的状态。                                          |
| android.permission.INTERNET                        | 危险   | 完全互联网访问        | 允许应用程序创建网络套接字。                                          |
| android.permission.WAKE_LOCK                       | 危险   | 防止手机休眠         | 允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。                          |
| 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_PHONE_STATE                | 危险   | 读取手机状态和标识      | 允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。 |
| android.permission.ACCESS_WIFI_STATE               | 普通   | 查看Wi-Fi状态      | 允许应用程序查看有关Wi-Fi状态的信息。                                   |
| android.permission.REQUEST_INSTALL_PACKAGES        | 危险   | 允许安装应用程序       | Android8.0 以上系统允许安装未知来源应用程序权限。                          |
| android.permission.VIBRATE                         | 普通   | 控制振动器          | 允许应用程序控制振动器，用于消息通知振动功能。                                 |
| shink.mlsrj.wallpaperadsdk.permission.TT_PANGO_LIN | 未知   | 未知权限           | 来自 android 引用的未知权限。                                     |
| com.asus.msa.SupplementaryDID.ACCESS               | 普通   | 获取厂商oaid相关权限   | 获取设备标识信息oaid，在华硕设备上需要用到的权限。                             |
| android.permission.READ_EXTERNAL_STORAGE           | 危险   | 读取SD卡内容        | 允许应用程序从SD卡读取信息。                                         |

网络通信安全风险分析

高危: 3 | 警告: 1 | 信息: 0 | 安全: 0

| 序号 | 范围 | 严重级别 | 描述 |
|----|----|------|----|
|----|----|------|----|

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |                            |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----------------------------|
| 1 | *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 高危 | 基本配置不安全地配置为允许到所有域的明文流量。    |
| 2 | i.snssdk.com<br>is.snssdk.com<br>pangolin.snssdk.com<br>extlog.snssdk.com<br>sf3-ttcdn-tos.pstatp.com<br>bds.snssdk.com<br>dig.bdurl.net<br>api-access.pangolin-sdk-to<br>utiao.com<br>sf1-fe-tos.pglstatp-toutiao.<br>com<br>sf1-be-pack.pglstatp-toutia<br>o.com<br>sf3-fe-tos.pglstatp-toutiao.<br>com<br>log-api.pangolin-sdk-toutia<br>o.com<br>s3-fe-scm.pglstatp-toutiao.<br>com<br>s3a.pstatp.com<br>api-access.pangolin-sdk-to<br>utiao-b.com<br>log-api.pangolin-sdk-toutia<br>o-b.com<br>dm.pstatp.com<br>toblog.ctobsnssdk.com<br>sdfp.snssdk.com<br>tosv.byted.org<br>sf1-ttcdn-tos.pstatp.com<br>sf6-fe-tos.pglstatp-toutiao.<br>com<br>log.snssdk.com<br>tosv.boe.byted.org<br>dm.toutiao.com<br>dm.bytedance.com<br>snssdk.com<br>open.snssdk.com<br>mercury-sdk.snssdk.com<br>open.toutiao.com<br>open-hl.toutiao.com<br>test-open.snssdk.com<br>pstatp.com<br>s3.pstatp.com<br>mcs.snssdk.com<br>dm-hl.toutiao.com<br>dm-log.toutiao.com<br>webcastopen.douyin.com<br>plugin-patch-api.bytedan<br>ce.com<br>127.0.0.1 | 高危 | 域配置不安全地配置为允许明文流量到达范围内的这些域。 |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |                  |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|------------------|
| 3 | i.snssdk.com<br>is.snssdk.com<br>pangolin.snssdk.com<br>extlog.snssdk.com<br>sf3-ttcdn-tos.pstatp.com<br>bds.snssdk.com<br>dig.bdurl.net<br>api-access.pangolin-sdk-to<br>utiao.com<br>sf1-fe-tos.pglstatp-toutiao.<br>com<br>sf1-be-pack.pglstatp-toutia<br>o.com<br>sf3-fe-tos.pglstatp-toutiao.<br>com<br>log-api.pangolin-sdk-toutia<br>o.com<br>s3-fe-scm.pglstatp-toutiao.<br>com<br>s3a.pstatp.com<br>api-access.pangolin-sdk-to<br>utiao-b.com<br>log-api.pangolin-sdk-toutia<br>o-b.com<br>dm.pstatp.com<br>toblog.ctobsnssdk.com<br>sdfp.snssdk.com<br>tosv.byted.org<br>sf1-ttcdn-tos.pstatp.com<br>sf6-fe-tos.pglstatp-toutiao.<br>com<br>log.snssdk.com<br>tosv.boe.byted.org<br>dm.toutiao.com<br>dm.bytedance.com<br>snssdk.com<br>open.snssdk.com<br>mercury-sdk.snssdk.com<br>open.toutiao.com<br>open-hl.toutiao.com<br>test-open.snssdk.com<br>pstatp.com<br>s3.pstatp.com<br>mcs.snssdk.com<br>dm-hl.toutiao.com<br>dm-lq.toutiao.com<br>webcast-open.douyin.com<br>plugin_patch-api.bytedanc<br>e.com<br>127.0.0.1 | 高危 | 域配置配置为信任用户安装时证书。 |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|------------------|

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |               |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---------------|
| 4 | i.snssdk.com<br>is.snssdk.com<br>pangolin.snssdk.com<br>extlog.snssdk.com<br>sf3-ttcdn-tos.pstatp.com<br>bds.snssdk.com<br>dig.bdurl.net<br>api-access.pangolin-sdk-to<br>utiao.com<br>sf1-fe-tos.pglstatp-toutiao.<br>com<br>sf1-be-pack.pglstatp-toutia<br>o.com<br>sf3-fe-tos.pglstatp-toutiao.<br>com<br>log-api.pangolin-sdk-toutia<br>o.com<br>s3-fe-scm.pglstatp-toutiao.<br>com<br>s3a.pstatp.com<br>api-access.pangolin-sdk-to<br>utiao-b.com<br>log-api.pangolin-sdk-toutia<br>o-b.com<br>dm.pstatp.com<br>toblog.ctobsnssdk.com<br>sdfp.snssdk.com<br>tosv.byted.org<br>sf1-ttcdn-tos.pstatp.com<br>sf6-fe-tos.pglstatp-toutiao.<br>com<br>log.snssdk.com<br>tosv.boe.byted.org<br>dm.toutiao.com<br>dm.bytedance.com<br>snssdk.com<br>open.snssdk.com<br>mercury-sdk.snssdk.com<br>open.toutiao.com<br>open-hl.toutiao.com<br>test-open.snssdk.com<br>pstatp.com<br>s3.pstatp.com<br>mcs.snssdk.com<br>dm-hl.toutiao.com<br>dm-lq.toutiao.com<br>webcast-open.douyin.com<br>plugin-patch-api.bytedanc<br>e.com<br>127.0.0.1 | 警告 | 域配置配置为信任系统证书。 |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|---------------|

证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

| 标题    | 严重程度 | 描述信息              |
|-------|------|-------------------|
| 已签名应用 | 信息   | 应用程序已使用代码签名证书进行签名 |

Manifest 配置安全分析

高危: 0 | 警告: 1 | 信息: 0 | 屏蔽: 0

| 序号 | 问题                                                                      | 严重程度 | 描述信息                                                                                              |
|----|-------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------------------|
| 1  | 应用程序可以安装在有漏洞的已更新 Android 版本上<br>Android 5.0-5.0.2, [minSdk=21]          | 信息   | 该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。 |
| 2  | 应用程序具有网络安全配置<br>[android:networkSecurityConfig=@xml/stk_network_config] | 信息   | 网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。               |
| 3  | 应用程序数据可以被备份<br>[android:allowBackup=true]                               | 警告   | 这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。                                            |

</> 代码安全漏洞检测

高危: 1 | 警告: 8 | 信息: 1 | 安全: 1 | 屏蔽: 0

| 序号 | 问题                                                      | 等级 | 参考标准                                                                                                         | 文件位置                         |
|----|---------------------------------------------------------|----|--------------------------------------------------------------------------------------------------------------|------------------------------|
| 1  | <a href="#">应用程序记录日志信息,不得记录敏感信息</a>                     | 信息 | CWE: CWE-532: 通过日志文件的信息暴露<br>OWASP MASVS: MSTG-STORAGE-3                                                     | <a href="#">升级会员: 解锁高级权限</a> |
| 2  | <a href="#">应用程序使用不安全的随机数生成器</a>                        | 警告 | CWE: CWE-330: 使用不充分的随机数<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6         | <a href="#">升级会员: 解锁高级权限</a> |
| 3  | <a href="#">文件可能包含硬编码的敏感信息,如用户名、密码、密钥等</a>              | 警告 | CWE: CWE-312: 明文存储敏感信息<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14              | <a href="#">升级会员: 解锁高级权限</a> |
| 4  | <a href="#">应用程序可以读取/写入外部存储器,任何应用程序都可以读取写入外部存储器的数据</a>  | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2              | <a href="#">升级会员: 解锁高级权限</a> |
| 5  | <a href="#">SHA-1是已存在在哈希冲突的弱哈希</a>                      | 警告 | CWE: CWE-327: 使用已被攻破或存在风险的密码学算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | <a href="#">升级会员: 解锁高级权限</a> |
| 6  | <a href="#">此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击</a> | 安全 | OWASP MASVS: MSTG-NETWORK-4                                                                                  | <a href="#">升级会员: 解锁高级权限</a> |

|    |                                                                                      |    |                                                                                                              |                              |
|----|--------------------------------------------------------------------------------------|----|--------------------------------------------------------------------------------------------------------------|------------------------------|
| 7  | <a href="#">应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库</a> | 警告 | CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当 ('SQL 注入')<br>OWASP Top 10: M7: Client Code Quality                        | <a href="#">升级会员: 解锁高级权限</a> |
| 8  | <a href="#">MD5是已知存在哈希冲突的弱哈希</a>                                                     | 警告 | CWE: CWE-327: 使用已被攻破或存在风险的密码学算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | <a href="#">升级会员: 解锁高级权限</a> |
| 9  | IP地址泄露                                                                               | 警告 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2                                                               | <a href="#">升级会员: 解锁高级权限</a> |
| 10 | <a href="#">该文件是World Writable。任何应用程序都可以写入文件</a>                                     | 高危 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2              | <a href="#">升级会员: 解锁高级权限</a> |
| 11 | 应用程序创建临时文件。敏感信息永远不应该被写进临时文件                                                          | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2              | <a href="#">升级会员: 解锁高级权限</a> |

🚩 Native 库安全加固检测

| 序号 | 动态库 | NX(堆栈禁止执行) | IE | STACK CANARY (栈保护) | RELRO | RP<br>ATH<br>(指定SO搜索路径) | R<br>UN<br>P<br>A<br>T<br>H<br>(指定SO搜索路径) | FORTIFY(常用函数加强检查) | SY<br>M<br>B<br>O<br>L<br>S<br>T<br>R<br>I<br>P<br>P<br>E<br>D(裁剪符号表) |
|----|-----|------------|----|--------------------|-------|-------------------------|-------------------------------------------|-------------------|-----------------------------------------------------------------------|
|----|-----|------------|----|--------------------|-------|-------------------------|-------------------------------------------|-------------------|-----------------------------------------------------------------------|



|   |                        |                                                                                                |                                                                                                                |                                                                                                                                                     |                                                                         |                                                                                                |                                                                                                                                                                          |                                                                                                                             |
|---|------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 1 | arm64-v8a/libsgcore.so | <div>True</div> <div>info</div> <div>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</div> | <div>True</div> <div>info</div> <div>这个二进制文件在栈上添加了一个栈哨兵值，以便它不会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</div> | <div>Full RELRO</div> <div>info</div> <div>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。</div> | <div>No</div> <div>ne</div> <div>info</div> <div>二进制文件没有设置运行时搜索路径</div> | <div>N</div> <div>o</div> <div>n</div> <div>e</div> <div>info</div> <div>二进制文件没有设置 RPATH</div> | <div>False</div> <div>warning</div> <div>二进制文件没有任何加固函数。加固函数提供了针对 libc 的常见不安全函数（如 strcpy, gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/FIutter 库不适用</div> | <div>Fal</div> <div>se</div> <div>wa</div> <div>rni</div> <div>ng</div> <div>符</div> <div>号</div> <div>可</div> <div>用</div> |
|---|------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|

敏感权限滥用分析

| 类型       | 匹配   | 权限                                                                                                                                                                                                      |
|----------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 恶意软件常用权限 | 4/30 | android.permission.WAKE_LOCK<br>android.permission.READ_PHONE_STATE<br>android.permission.REQUEST_INSTALL_PACKAGES<br>android.permission.VIBRATE                                                        |
| 其它常用权限   | 5/46 | android.permission.ACCESS_NETWORK_STATE<br>android.permission.INTERNET<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.READ_EXTERNAL_STORAGE |

常用: 已知恶意软件广泛滥用的权限

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

| 域名               | 状态 | 中国境内 | 位置信息                                                                                                                                                                         |
|------------------|----|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| xingjishidai.top | 安全 | 是    | <div>IP地址: 47.107.188.232</div> <div>国家: 中国</div> <div>地区: 广东</div> <div>城市: 深圳</div> <div>纬度: 22.545673</div> <div>经度: 114.068108</div> <div>查看: <a href="#">高德地图</a></div> |

|                                                  |    |   |                                                                                                                                                                     |
|--------------------------------------------------|----|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| speedtest01.hn165.com.prod.hosts.ooklaserver.net | 安全 | 是 | <b>IP地址:</b> 220.202.152.178<br><b>国家:</b> 中国<br><b>地区:</b> 湖南<br><b>城市:</b> 吉首<br><b>纬度:</b> 28.316669<br><b>经度:</b> 109.716667<br><b>查看:</b> <a href="#">高德地图</a> |
| apps.oceanengine.com                             | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 苏州<br><b>纬度:</b> 31.311365<br><b>经度:</b> 120.617691<br><b>查看:</b> <a href="#">高德地图</a>  |
| dict.youdao.com                                  | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 贵州<br><b>城市:</b> 遵义<br><b>纬度:</b> 27.686441<br><b>经度:</b> 106.907135<br><b>查看:</b> <a href="#">高德地图</a>  |
| app.starkos.cn                                   | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 深圳<br><b>纬度:</b> 22.545673<br><b>经度:</b> 114.068108<br><b>查看:</b> <a href="#">高德地图</a>  |
| f1987f2136.imdo.co                               | 安全 | 否 | No Geolocation information available.                                                                                                                               |
| aip.baidubce.com                                 | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 苏州<br><b>纬度:</b> 31.311365<br><b>经度:</b> 120.617691<br><b>查看:</b> <a href="#">高德地图</a>  |
| www.chengzijianzhan.com                          | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 苏州<br><b>纬度:</b> 31.311365<br><b>经度:</b> 120.617691<br><b>查看:</b> <a href="#">高德地图</a>  |
| apis.juhe.cn                                     | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 杭州<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583<br><b>查看:</b> <a href="#">高德地图</a>  |

|                          |    |   |                                                                                                                                                                          |
|--------------------------|----|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| i.snssdk.com             | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 苏州<br><b>纬度:</b> 31.311365<br><b>经度:</b> 120.617691<br><b>查看:</b> <a href="#">高德地图</a>       |
| japi.juhe.cn             | 安全 | 是 | <b>IP地址:</b> 203.107.54.210<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 杭州<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583<br><b>查看:</b> <a href="#">高德地图</a>       |
| www.toutiaopage.com      | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 台州<br><b>纬度:</b> 32.492168<br><b>经度:</b> 119.910767<br><b>查看:</b> <a href="#">高德地图</a>       |
| byteapi.starkos.cn       | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 深圳<br><b>纬度:</b> 22.545673<br><b>经度:</b> 114.068108<br><b>查看:</b> <a href="#">高德地图</a>       |
| sf6-ttcdn-tos.pstatp.com | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 台州<br><b>纬度:</b> 28.666668<br><b>经度:</b> 121.349998<br><b>查看:</b> <a href="#">高德地图</a>       |
| biteapi.starkos.cn       | 安全 | 是 | <b>IP地址:</b> 47.107.188.232<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 深圳<br><b>纬度:</b> 22.545673<br><b>经度:</b> 114.068108<br><b>查看:</b> <a href="#">高德地图</a>       |
| www.samsungapps.com      | 安全 | 否 | <b>IP地址:</b> 54.229.93.185<br><b>国家:</b> 爱尔兰<br><b>地区:</b> 都柏林<br><b>城市:</b> 都柏林<br><b>纬度:</b> 53.344151<br><b>经度:</b> -6.267249<br><b>查看:</b> <a href="#">Google 地图</a> |
| v.juhe.cn                | 安全 | 是 | <b>IP地址:</b> 203.107.54.210<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 杭州<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583<br><b>查看:</b> <a href="#">高德地图</a>       |

|                    |    |   |                                                                                                                                                                    |
|--------------------|----|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service.starkos.cn | 安全 | 是 | <b>IP地址:</b> 203.107.54.210<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 深圳<br><b>纬度:</b> 22.545673<br><b>经度:</b> 114.068108<br><b>查看:</b> <a href="#">高德地图</a> |
| web.juhe.cn        | 安全 | 是 | <b>IP地址:</b> 203.107.54.210<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 杭州<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161588<br><b>查看:</b> <a href="#">高德地图</a> |

URL 链接安全分析

| URL信息                                                                                                                                                                                           | 源码文件                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>https://www.pangle.cn/privacy/partner</li><li>https://www.tencent.com/zh-cn/privacy-policy.html</li><li>https://u.kuaishou.com/home/detail/1290</li></ul> | 自研引擎-A                                                                         |
| <ul style="list-style-type: none"><li>https://aip.baidubce.com/rest/2.0/ocr/</li></ul>                                                                                                          | k/a/c/mj.java                                                                  |
| <ul style="list-style-type: none"><li>https://aip.baidubce.com/rest/2.0/image-classify/</li></ul>                                                                                               | k/a/c/c/e.java                                                                 |
| <ul style="list-style-type: none"><li>192.168.43.1</li></ul>                                                                                                                                    | stark/common/basic/utis/WiFiUtil.java                                          |
| <ul style="list-style-type: none"><li>https://f1987f2136.imdo.co/v1/</li><li>https://app.starkos.cn/v1/</li></ul>                                                                               | stark/common/basic/appserver/AppServerConst.java                               |
| <ul style="list-style-type: none"><li>http://vop.baidu.com/</li></ul>                                                                                                                           | k/a/c/c/p.java                                                                 |
| <ul style="list-style-type: none"><li>https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetrissite/personal-privacy-page.html</li></ul>                                                                   | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| <ul style="list-style-type: none"><li>https://speedtest01.hn165.com/prod.hosts.ooklaserver.net/8080/download?size=25000000</li></ul>                                                            | stark/common/basic/utis/NetSpeedTestUtil.java                                  |
| <ul style="list-style-type: none"><li>https://github.com/lingochamp/filedownloader/wiki/filedownloader.properties</li></ul>                                                                     | com/kwai/filedownloader/services/a.java                                        |
| <ul style="list-style-type: none"><li>https://apis.juhe.cn</li></ul>                                                                                                                            | k/a/c/d/a.java                                                                 |
| <ul style="list-style-type: none"><li>www.tetrispage.com/tetris/page</li><li>https://apps.oceanengine.com/customer/api/app/pkg_info?</li><li>www.chengzijianzhan.com</li></ul>                  | com/ss/android/downloadlib/addownload/compliance/b.java                        |
| <ul style="list-style-type: none"><li>https://aip.baidubce.com/rest/2.0/image-classify/</li></ul>                                                                                               | k/a/c/c/a.java                                                                 |
| <ul style="list-style-type: none"><li>https://i.snsdtk.com/</li></ul>                                                                                                                           | com/ss/android/downloadad/api/constant/AdBaseConstants.java                    |
| <ul style="list-style-type: none"><li>https://lite2api.starkos.cn</li></ul>                                                                                                                     | stark/common/api/StkResApiService.java                                         |
| <ul style="list-style-type: none"><li>https://aip.baidubce.com/</li></ul>                                                                                                                       | k/a/g/a/a/b.java                                                               |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| <ul style="list-style-type: none"> <li>https://www.samsungapps.com/appquery/appdetail.as?appid=</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | com/ss/android/downloadlib/g/h.java               |
| <ul style="list-style-type: none"> <li>http://xingjishidai.top/a/terms/1cfb2b74e95f98c664d21ffd06dae455</li> <li>http://xingjishidai.top/a/privacy/1cfb2b74e95f98c664d21ffd06dae455</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | flc/ast/App.java                                  |
| <ul style="list-style-type: none"> <li>http://dict.youdao.com/dictvoice?audio=</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | stark/common/basic/sound/DictSpeaker.java         |
| <ul style="list-style-type: none"> <li>http://apis.juhe.cn/fapig/birthdaybook/query</li> <li>http://japi.juhe.cn/charconvert/change.from</li> <li>http://web.juhe.cn/constellation/getall</li> <li>http://apis.juhe.cn/birtheight/query</li> <li>http://v.juhe.cn/toutiao/content</li> <li>http://apis.juhe.cn/ip/ipnewv3</li> <li>http://apis.juhe.cn/fapig/birthdayflower/query</li> <li>http://apis.juhe.cn/simpleweather/life</li> <li>http://apis.juhe.cn/simpleweather/query</li> <li>http://v.juhe.cn/toutiao/index</li> <li>http://apis.juhe.cn/mobile/get</li> <li>http://v.juhe.cn/laohuangli/h</li> <li>http://v.juhe.cn/dream/category</li> <li>http://v.juhe.cn/joke/content/text.php</li> <li>http://apis.juhe.cn/fapig/stature/query</li> <li>http://v.juhe.cn/laohuangli/d</li> <li>http://apis.juhe.cn/simpleweather/citylist</li> <li>http://v.juhe.cn/dream/query</li> </ul> | k/a/c/d/e.java                                    |
| <ul style="list-style-type: none"> <li>https://service.starkos.cn/</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | stark/common/core/appconfig/AppConfigManager.java |
| <ul style="list-style-type: none"> <li>https://fanyi-api.baidu.com/api/</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | k/a/g/a/b/b.java                                  |
| <ul style="list-style-type: none"> <li>https://service.starkos.cn</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | stark/common/basic/retrofit/BaseApi.java          |
| <ul style="list-style-type: none"> <li>https://service.starkos.cn/a/feedback/addfeedbacksecure</li> <li>https://byteapi.starkos.cn</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | stark/common/api/StkApiService.java               |

第三方 SDK 组件分析

| SDK名称           | 开发者                       | 描述信息                                                                                                                                    |
|-----------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Pangle SDK      | <a href="#">Bytedance</a> | 穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。                                    |
| 岳麓全景监控          | <a href="#">Alibaba</a>   | 岳麓全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。                                                                                            |
| 360 加固          | <a href="#">360</a>       | 360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。                                                             |
| 阿里聚安全           | <a href="#">Alibaba</a>   | 阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。                                                                                                            |
| 移动统计分析          | <a href="#">Umeng</a>     | U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。 |
| AndroidUtilCode | <a href="#">Blankj</a>    | AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。                                              |
| 快手广告 SDK        | <a href="#">快手</a>        | 快手信息流广告，为您和用户搭建桥梁。                                                                                                                      |

|                   |                            |                                                                                             |
|-------------------|----------------------------|---------------------------------------------------------------------------------------------|
| XPopup            | <a href="#">li-xiaojun</a> | 内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。                                                      |
| Jetpack Lifecycle | <a href="#">Google</a>     | 生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。 |
| File Provider     | <a href="#">Android</a>    | FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。  |
| OkDownload        | <a href="#">LingoChamp</a> | 可靠，灵活，高性能以及强大的下载引擎。                                                                         |

🕵️ 第三方追踪器检测

| 名称                | 类别                         | 网址                                                                                                                  |
|-------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| Pangle            | Advertisement              | <a href="https://reports.exodus-privacy.eu.org/trackers/363">https://reports.exodus-privacy.eu.org/trackers/363</a> |
| Umeng Analytics   |                            | <a href="https://reports.exodus-privacy.eu.org/trackers/119">https://reports.exodus-privacy.eu.org/trackers/119</a> |
| Yueying Crash SDK | Crash reporting, Analytics | <a href="https://reports.exodus-privacy.eu.org/trackers/448">https://reports.exodus-privacy.eu.org/trackers/448</a> |

🔑 敏感凭证泄露检测

|                                      |
|--------------------------------------|
| 可能的密钥                                |
| 258EAFa5-E914-47DA-95CA-C5AB0DC85B11 |
| 2fdd40294c8b009d2d6fcf02d4bae747     |
| 337044374e485cc574437b7e97cd3618     |
| eba8c678f96f9789fa9426108bf24b41     |
| 1cfb2b74e95f98c664d21ffd06dae455     |
| 3ec4dc9830338ffefe602a242dd4921a     |
| 41b6a88f9bae1fc113a4cf06d6c052f2     |
| 12395f0ba1c8a898201215d5018f7ab0a02  |
| b0b869441f436f60c33e3c16228ef3bc     |
| 95ca0504b60e8b7afc1f29998a6734553    |
| 00c382c0516cd56a5ec8416f35162db3     |
| de5f15f5f960c6867b9d1b0ebda34b69     |
| 616d2e1bac9567566e9b6c4c             |
| 8f981619b8290c1fb7f574c727ec4b2e     |
| 6470222e1a1ce634b06b592380c38c49     |
| 03cb6262955fe2235939d62135389324     |

|                                  |
|----------------------------------|
| 65f983964b0939bfb534ea1ab373a218 |
| 01d1f698a6c4b59fb4225f69f1bbb52e |
| 45c888972a78bbc573a938108a8376a1 |
| 5bace6a7dffe5773256b1919c07d414  |
| e9fef755e933ad52e5236380fb983c06 |

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成