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

**春秋航空（ 8.0.5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 | 春秋航空 |
| 版本 | 8.0.5 |
| 包名 | com.china3s.android |
| 域名线索 | 26条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年7月4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 | 春秋航空.apk |
| 文件大小 | 60.77MB |
| MD5值 | 25bdeb0305571d824c7d778e1a75d8f4 |
| SHA1值 | 6f09b0f7c084366a9f03ea8f27ee2d66b5c81b0d |
| SHA256值 | 7120018d81c494b410570a95ac3067a42aab2fae06fca9010b19cf866f73d4dc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 春秋航空 |
| 包名 | com.china3s.android |
| 主活动Activity | com.china3s.android.home.view.Main |
| 安卓版本名称 | 8.0.5 |
| 安卓版本 | 8050 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| openmp.llvm.org | IP: 54.67.122.174 所属国家: United States of America 地区: California 城市: San Jose  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| bugs.llvm.org | IP: 54.67.122.174 所属国家: United States of America 地区: California 城市: San Jose  |
| m.zzx.cnklog.com | IP: 124.64.196.23 所属国家: China 地区: Beijing 城市: Beijing  |
| daily.m.zzx9.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| grs.dbankcloud.asia | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| ms.zzx9.cn | IP: 124.64.196.27 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| auth.wosms.cn | IP: 124.64.196.28 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| 192.168.62.1 | IP: 192.168.62.1 所属国家: - 地区: - 城市: -  |
| grs.dbankcloud.cn | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| android.googlesource.com | IP: 173.194.203.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| msv6.wosms.cn | IP: 123.125.99.31 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 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://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://openmp.llvm.org/  | 摸瓜V3引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html  | 摸瓜V3引擎  |
| http://192.168.62.1:58001  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://msv6.wosms.cn  | 摸瓜V3引擎  |
| https://daily.m.zzx9.cn  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android//tv\_name  | 摸瓜V3引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V3引擎  |
| https://m.zzx.cnklog.com  | 摸瓜V3引擎  |
| https://bugs.llvm.org/.  | 摸瓜V3引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html/var/run/egd-pool/dev/egd-pool/etc/egd-pool/etc/entropy/dev/r  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/androidzztv\_receive\_name\_des  | 摸瓜V3引擎  |
| https://ms.zzx9.cn  | 摸瓜V3引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V3引擎  |
| https://auth.wosms.cn  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/clang  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14442730474  | 摸瓜V1引擎  |

## **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=86, ST=Shanghai, L=Shanghai, O=Spring, OU=Spring, CN=Spring 签名算法: rsassa\_pkcs1v15 有效期自: 2010-06-18 05:05:50+00:00 有效期至: 2035-06-12 05:05:50+00:00 发行人: C=86, ST=Shanghai, L=Shanghai, O=Spring, OU=Spring, CN=Spring 序列号: 0x4c1afeae 哈希算法: sha1 md5值: 92172a9b3326e0158074c3eb3f8489b1 sha1值: 3ef570cd544e1fc6159bed8997d4f348b35fa8fd sha256值: 2afd8c542e9631146d02a62859261da81f6d5137858ee7b3f37e3ee2ed93a658 sha512值: dac0553d47e2a43364018bb4e9392f4e5672bfa89d629d1a3e67be598138a0abc5f9edbbc2877ea956efc0cb6f942d827a8a7644ba036f396e679ddcd7f59587 公钥算法: rsa 密钥长度: 1024 指纹: dc4e3283674e58d21e7d22843bb21d5ebe87a5de6ac23aa7de327835bb1c6d1b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "UserRegister\_java\_plzputcorrect\_password" : "请按要求填写密码"  |
| "bugly\_key" : "900015348"  |
| "check\_pwd\_fail" : "密码必须为6-16位字符，且由英文字母和数字组成"  |
| "check\_pwd\_null" : "密码不能为空"  |
| "check\_pwdok\_null" : "确认密码不能为空"  |
| "comment\_user" : "用户点评"  |
| "fission\_auth\_content" : "实名认证后，即可领取银卡会员"  |
| "fission\_auth\_repeat" : "抱歉，您的认证因系统异常没有完成，所以领取银卡失败。如需帮助请致电95524。"  |
| "green\_authenticate" : "绿翼认证"  |
| "green\_integral\_password" : "密码"  |
| "gt\_one\_login\_auth\_btn" : "一键登录"  |
| "hot\_Certificate" : "热门"  |
| "id\_settings\_pwd" : "设置登录密码"  |
| "id\_userpassword" : "密码"  |
| "integral\_apply\_green\_set\_password" : "设置交易密码"  |
| "login\_pwdsetting\_notify" : "注册成功了，初始登录密码已发送到您的手机，您也可以设置自己喜欢的登录密码"  |
| "retry\_authenticate" : "重新认证"  |
| "secretKey" : "spring20140530airlines!)"  |
| "security\_public\_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"  |
| "set\_password" : "设置密码"  |
| "set\_pwd\_success" : "密码设置成功"  |
| "str\_abnormal\_flight\_certificate" : "异常航班证明"  |
| "str\_auth\_face\_authentication" : "扫脸认证"  |
| "str\_auth\_face\_authentication\_right\_now" : "立即扫脸认证"  |
| "str\_auth\_face\_introducation" : "扫脸认证介绍方便快捷"  |
| "str\_auth\_ly\_member\_can\_refund\_account" : "认证为绿翼会员后，才能退款到乘机人账户"  |
| "str\_auth\_real\_name" : "实名认证"  |
| "str\_auth\_spring\_face\_authentication" : "春秋扫脸认证"  |
| "str\_auth\_success" : "认证成功"  |
| "str\_auth\_success\_can\_pick\_seat" : "认证后可选座"  |
| "str\_auth\_v6912" : "认证"  |
| "str\_authenticat\_problem" : "认证遇到问题？您可以："  |
| "str\_authenticat\_problem\_tip" : "查看常见问题 上传手持证件照片进行认证"  |
| "str\_authentication\_again" : "重新实名认证"  |
| "str\_authentication\_success" : "实名认证更新成功，已享受最新权益"  |
| "str\_birth\_certificate" : "出生证明"  |
| "str\_calculate\_other\_user" : "切换会员账号、重新登录"  |
| "str\_cancel\_authentication" : "取消实名认证"  |
| "str\_check\_authentication\_account\_notice" : "账号认证“处理中”，会员等级已发生变化，您可重新登录后，通过【我的】下的实名认证引导完成后续认证，也可继续等待当前账号处理结果。"  |
| "str\_check\_authentication\_account\_notice\_one" : "账号认证正在处理中，预计等待3分钟； 为了您的账号安全，“处理中”期间，建议您不要有下单等操作。"  |
| "str\_check\_authentication\_account\_notice\_two" : "\*若您当前需先离开，后续通过【我的-账号设置-查看认证结果】再次进入，给您带来的不便深感歉意。"  |
| "str\_check\_authentication\_account\_online\_warm" : "\*若您的账号较长时间仍无法处理结果，您可联系在线客服进行处理。"  |
| "str\_check\_authentication\_account\_warm" : "账号认证“处理中”，为了您的账号安全，“处理中”期间，建议您不要有下单等操作。"  |
| "str\_check\_authentication\_go\_account" : "【我的-账号设置-查看认证结果】"  |
| "str\_check\_authentication\_goto\_account" : "前往【账号设置】"  |
| "str\_check\_authentication\_login" : "重新登录"  |
| "str\_check\_authentication\_result" : "查看认证结果"  |
| "str\_check\_authentication\_wait" : "继续等待"  |
| "str\_choose\_seat\_auth\_login" : "实名认证登录成为绿翼会员，满足条件的乘机人可免费选择带有xx的标识座位。"  |
| "str\_choose\_seat\_auth\_only" : "实名认证为绿翼会员，满足条件的乘机人可免费选择带有xx标识的座位。"  |
| "str\_close\_account\_need\_safe\_auth" : "申请账号注销需进行安全验证"  |
| "str\_face\_authentication\_failed" : "您的信息未通过身份认证,请重新输入"  |
| "str\_flight\_qr\_code\_certificate" : "二维码凭证"  |
| "str\_free\_auth\_ly\_or\_buy\_year\_card" : "免费实名认证成为绿翼会员或购买“座位优享卡”产品并绑定，立即选择心仪座位！"  |
| "str\_go\_to\_set\_password" : "下一步，设置密码"  |
| "str\_green\_member\_authentication\_again" : "重新认证"  |
| "str\_green\_member\_authentication\_bind" : "绑定信息"  |
| "str\_green\_member\_authentication\_cancel\_status" : "取消实名认证后状态"  |
| "str\_green\_member\_authentication\_cancel\_success" : "已取消实名认证"  |
| "str\_green\_member\_authentication\_fail" : "重新认证失败"  |
| "str\_green\_member\_authentication\_other\_way" : "您也可以选择其他认证方式再次认证："  |
| "str\_green\_member\_authentication\_protocol" : "我已阅读并确认以上信息"  |
| "str\_green\_member\_authentication\_status" : "重新认证后状态"  |
| "str\_green\_member\_authentication\_submit" : "重新认证提交中"  |
| "str\_green\_member\_authentication\_success" : "重新认证成功"  |
| "str\_green\_member\_authentication\_suggest" : "建议您登录上述账号后，再重新认证。"  |
| "str\_green\_member\_authentication\_warm" : "网络不给力，请重新尝试"  |
| "str\_green\_member\_cancel\_authentication\_fail" : "取消实名认证失败"  |
| "str\_has\_no\_insure\_invoice\_order\_auth\_try\_latter" : "您暂时没有可开具电子发票的保险订单, 可实名认证快速匹配订单。"  |
| "str\_input\_login\_password" : "请输入登录密码"  |
| "str\_integral\_modify\_password" : "修改交易密码"  |
| "str\_integral\_modify\_trading\_password" : "修改交易密码"  |
| "str\_integral\_reset\_trading\_password" : "重置交易密码"  |
| "str\_integral\_six\_digit\_trading\_password" : "6位数字交易密码"  |
| "str\_integral\_though\_email\_reset\_trading\_password" : "通过邮件验证码重置交易密码："  |
| "str\_login\_check\_password" : "请检查您的密码是否为6-16位英文和数字组合"  |
| "str\_mailing\_leader\_des\_key" : "点击此处"  |
| "str\_mine\_qy\_user" : "企业用户"  |
| "str\_need\_alipay\_or\_wx\_auth\_login" : "很抱歉，一键登录失败，您可以通过微信、支付宝账号实名认证登录后，和当前账号关联。"  |
| "str\_pay\_before\_one\_phone\_auth" : "请完成安全验证"  |
| "str\_please\_auth\_account" : "请验证账号"  |
| "str\_please\_auth\_befor\_query\_flight" : "查询航班,请先授权"  |
| "str\_please\_set\_login\_password" : "请设置登录密码"  |
| "str\_plz\_input\_password" : "请输入密码"  |
| "str\_private\_traffic\_tip1" : "扫描二维码入群"  |
| "str\_private\_traffic\_tip2" : "分享至微信加入群聊"  |
| "str\_private\_traffic\_tip3" : "春秋航空服务微信交流群"  |
| "str\_private\_traffic\_tip4" : "该功能暂未开放，敬请期待！"  |
| "str\_retrieve\_password" : "找回密码"  |
| "str\_set\_login\_password" : "请设置密码"  |
| "str\_share\_power\_copy\_password" : "复制口令"  |
| "str\_travel\_high\_speed\_auth" : "极速认证"  |
| "tingyun\_app\_key" : "e60267b079474ed88ff201709070a355"  |
| "tingyun\_app\_scheme\_key" : "tingyun.102005"  |
| "weibosdk\_demo\_toast\_auth\_canceled" : "取消授权"  |
| "weibosdk\_demo\_toast\_auth\_failed" : "授权失败"  |
| "UserRegister\_java\_plzputcorrect\_password" : "必要なパスワードを記入してください"  |
| "check\_pwd\_fail" : "6～16桁の英数字"  |
| "check\_pwd\_null" : "パスワードを入力してください"  |
| "check\_pwdok\_null" : "パスワードをもう一度入力してください"  |
| "comment\_user" : "レビュー"  |
| "green\_authenticate" : "スプリングパス認証"  |
| "green\_integral\_password" : "パスワード"  |
| "hot\_Certificate" : "人気"  |
| "id\_settings\_pwd" : "パスワードを設定してください"  |
| "id\_userpassword" : "パスワード"  |
| "login\_pwdsetting\_notify" : "新規登録完了しました。初回登録用のパスワードはご利用の携帯に送信しました。登録後にパスワードの変更は可能です。"  |
| "retry\_authenticate" : "もう一度認証を行う"  |
| "set\_password" : "パスワード設定"  |
| "set\_pwd\_success" : "パスワードを設定しました"  |
| "str\_abnormal\_flight\_certificate" : "欠航・遅延証明書"  |
| "str\_auth\_face\_authentication" : "顔認証"  |
| "str\_auth\_face\_authentication\_right\_now" : "すぐに顔認証を行う"  |
| "str\_auth\_face\_introducation" : "便利でスピーディな顔認証のご紹介"  |
| "str\_auth\_spring\_face\_authentication" : "春秋顔認証"  |
| "str\_auth\_v6912" : "認証"  |
| "str\_authenticat\_problem" : "認証に問題が発生しました？"  |
| "str\_authenticat\_problem\_tip" : "よくある質問を見る 証明書を手に持つ画像をアップロードして認証"  |
| "str\_birth\_certificate" : "出生証明書"  |
| "str\_face\_authentication\_failed" : "お客様の情報は身元認証をパスしていません。もう一度入力してください。"  |
| "str\_flight\_qr\_code\_certificate" : "QRコード"  |
| "str\_go\_to\_set\_password" : "次に、パスワードを設定"  |
| "str\_input\_login\_password" : "登録パスワードを入力"  |
| "str\_integral\_modify\_password" : "決済パスワード変更"  |
| "str\_integral\_reset\_trading\_password" : "決済パスワードを再設定"  |
| "str\_integral\_six\_digit\_trading\_password" : "決済パスワード（数字6桁）"  |
| "str\_integral\_though\_email\_reset\_trading\_password" : "予備のメールアドレスでパスワードを変更する:"  |
| "str\_login\_check\_password" : "パスワードが6文字以上16文字以内、英文字と数字の組み合わせであるかどうかを確認"  |
| "str\_pay\_before\_one\_phone\_auth" : "セキュリティ検証を完了してください"  |
| "str\_please\_auth\_befor\_query\_flight" : "フライトを検索する前に、授権を行ってください"  |
| "str\_please\_set\_login\_password" : "登録パスワードを設定"  |
| "str\_plz\_input\_password" : "パスワードを入力"  |
| "str\_retrieve\_password" : "パスワードの再設定"  |
| "str\_set\_login\_password" : "パスワードを設定"  |
| "weibosdk\_demo\_toast\_auth\_canceled" : "認証を解除する"  |
| "weibosdk\_demo\_toast\_auth\_failed" : "承認に失敗しました"  |
| "UserRegister\_java\_plzputcorrect\_password" : "please fill out the required password"  |
| "check\_pwd\_fail" : "Password must be 6-16 characters and consist of English letters and numbers"  |
| "check\_pwd\_null" : "Password can’t be empty"  |
| "check\_pwdok\_null" : "Confirm password can’t be empty"  |
| "comment\_user" : "Comments"  |
| "green\_authenticate" : "SpringPass certification"  |
| "green\_integral\_password" : "Password"  |
| "gt\_one\_login\_auth\_btn" : "one-click login"  |
| "hot\_Certificate" : "Hot"  |
| "id\_settings\_pwd" : "Setting password"  |
| "id\_userpassword" : "Password"  |
| "login\_pwdsetting\_notify" : "Registration complete, the initial password has been sent to your phone, and you can set your own login password"  |
| "retry\_authenticate" : "Try again"  |
| "set\_password" : "Set password"  |
| "set\_pwd\_success" : "Password has been set successfully"  |
| "str\_abnormal\_flight\_certificate" : "Abnormal flight certificate"  |
| "str\_auth\_face\_authentication" : "Face Authentication"  |
| "str\_auth\_face\_authentication\_right\_now" : "Start Now"  |
| "str\_auth\_face\_introducation" : "Introduction: Fast & Convenient"  |
| "str\_auth\_spring\_face\_authentication" : "Spring Airlines Face Authentication"  |
| "str\_auth\_v6912" : "Authentication"  |
| "str\_authenticat\_problem" : "Any problem with the certification? You can:"  |
| "str\_authenticat\_problem\_tip" : "View FAQ Upload photos of passengers hand-held documents to certificate"  |
| "str\_birth\_certificate" : "Birth certificate"  |
| "str\_face\_authentication\_failed" : "You authentication is failed, please enter again"  |
| "str\_flight\_qr\_code\_certificate" : "QR code"  |
| "str\_go\_to\_set\_password" : "Next, set a password"  |
| "str\_input\_login\_password" : "Please enter your password"  |
| "str\_integral\_modify\_password" : "Modify transaction password"  |
| "str\_integral\_reset\_trading\_password" : "Reset the transaction password"  |
| "str\_integral\_six\_digit\_trading\_password" : "6 characters transaction password"  |
| "str\_integral\_though\_email\_reset\_trading\_password" : "Reset your transaction password via email verification code:"  |
| "str\_login\_check\_password" : "Please check if your password is 6-16 character English and number combination"  |
| "str\_pay\_before\_one\_phone\_auth" : "Please complete security verification"  |
| "str\_please\_auth\_befor\_query\_flight" : "Please authorize before flight query"  |
| "str\_please\_set\_login\_password" : "Please set login password"  |
| "str\_plz\_input\_password" : "Please enter your password"  |
| "str\_retrieve\_password" : "Retrieve Password"  |
| "str\_set\_login\_password" : "Please set a password"  |
| "weibosdk\_demo\_toast\_auth\_canceled" : "deauthorize"  |
| "weibosdk\_demo\_toast\_auth\_failed" : "Authorization failed"  |
| "UserRegister\_java\_plzputcorrect\_password" : "请按要求填写密码"  |
| "check\_pwd\_fail" : "密码必须为6-16位字符，且由英文字母和数字组成"  |
| "check\_pwd\_null" : "密码不能为空"  |
| "check\_pwdok\_null" : "确认密码不能为空"  |
| "comment\_user" : "用户点评"  |
| "green\_authenticate" : "绿翼认证"  |
| "green\_integral\_password" : "密码"  |
| "hot\_Certificate" : "热门"  |
| "id\_settings\_pwd" : "设置登录密码"  |
| "id\_userpassword" : "密码"  |
| "login\_pwdsetting\_notify" : "注册成功了，初始登录密码已发送到您的手机，您也可以设置自己喜欢的登录密码"  |
| "retry\_authenticate" : "重新认证"  |
| "set\_password" : "设置密码"  |
| "set\_pwd\_success" : "密码设置成功"  |
| "str\_abnormal\_flight\_certificate" : "异常航班证明"  |
| "str\_auth\_face\_authentication" : "扫脸认证"  |
| "str\_auth\_face\_authentication\_right\_now" : "立即扫脸认证"  |
| "str\_auth\_face\_introducation" : "扫脸认证介绍方便快捷"  |
| "str\_auth\_spring\_face\_authentication" : "春秋扫脸认证"  |
| "str\_auth\_v6912" : "认证"  |
| "str\_authenticat\_problem" : "认证遇到问题？您可以："  |
| "str\_authenticat\_problem\_tip" : "查看常见问题 上传手持证件照片进行认证"  |
| "str\_birth\_certificate" : "出生证明"  |
| "str\_face\_authentication\_failed" : "您的信息未通过身份认证,请重新输入"  |
| "str\_flight\_qr\_code\_certificate" : "二维码凭证"  |
| "str\_go\_to\_set\_password" : "下一步，设置密码"  |
| "str\_input\_login\_password" : "请输入登录密码"  |
| "str\_integral\_modify\_password" : "修改交易密码"  |
| "str\_integral\_reset\_trading\_password" : "重置交易密码"  |
| "str\_integral\_six\_digit\_trading\_password" : "6位数字交易密码"  |
| "str\_integral\_though\_email\_reset\_trading\_password" : "通过邮件验证码重置交易密码："  |
| "str\_login\_check\_password" : "请检查您的密码是否为6-16位英文和数字组合"  |
| "str\_pay\_before\_one\_phone\_auth" : "请完成安全验证"  |
| "str\_please\_auth\_befor\_query\_flight" : "查询航班,请先授权"  |
| "str\_please\_set\_login\_password" : "请设置登录密码"  |
| "str\_plz\_input\_password" : "请输入密码"  |
| "str\_retrieve\_password" : "找回密码"  |
| "str\_set\_login\_password" : "请设置密码"  |
| "weibosdk\_demo\_toast\_auth\_canceled" : "取消授权"  |
| "weibosdk\_demo\_toast\_auth\_failed" : "授权失败"  |
| "UserRegister\_java\_plzputcorrect\_password" : "請按要求填寫密碼"  |
| "check\_pwd\_fail" : "密碼必須為6-16位字符，且由英文字母和數字組成"  |
| "check\_pwd\_null" : "密碼不能為空"  |
| "check\_pwdok\_null" : "確認密碼不能為空"  |
| "comment\_user" : "用戶點評"  |
| "green\_authenticate" : "綠翼認證"  |
| "green\_integral\_password" : "密碼"  |
| "hot\_Certificate" : "熱門"  |
| "id\_settings\_pwd" : "設置登錄密碼"  |
| "id\_userpassword" : "密碼"  |
| "login\_pwdsetting\_notify" : "註冊成功了，初始登錄密碼已發送到您的手機，您也可以設置自己喜歡的登錄密碼"  |
| "retry\_authenticate" : "重新認證"  |
| "set\_password" : "設置密碼"  |
| "set\_pwd\_success" : "密碼置成功"  |
| "str\_abnormal\_flight\_certificate" : "異常航班證明"  |
| "str\_auth\_face\_authentication" : "人臉識別"  |
| "str\_auth\_face\_authentication\_right\_now" : "立即進行人臉識別"  |
| "str\_auth\_face\_introducation" : "人臉識別說明方便快捷"  |
| "str\_auth\_spring\_face\_authentication" : "春秋人臉識別"  |
| "str\_auth\_v6912" : "認證"  |
| "str\_authenticat\_problem" : "認證遇到問題？您可以："  |
| "str\_authenticat\_problem\_tip" : "查看常見問題 上傳手持證件照片進行認證"  |
| "str\_birth\_certificate" : "出生證明"  |
| "str\_face\_authentication\_failed" : "未通過身份認證,請重新輸入"  |
| "str\_flight\_qr\_code\_certificate" : "二維碼憑證"  |
| "str\_go\_to\_set\_password" : "下一步，設置密碼"  |
| "str\_input\_login\_password" : "請輸入登錄密碼"  |
| "str\_integral\_modify\_password" : "修改交易密碼"  |
| "str\_integral\_reset\_trading\_password" : "重置交易密碼"  |
| "str\_integral\_six\_digit\_trading\_password" : "6位元數位交易密碼"  |
| "str\_integral\_though\_email\_reset\_trading\_password" : "通過郵件驗證碼重置交易密碼："  |
| "str\_login\_check\_password" : "請檢查您的密碼是否為6-16位英文和數字組合"  |
| "str\_pay\_before\_one\_phone\_auth" : "請完成安全驗證"  |
| "str\_please\_auth\_befor\_query\_flight" : "查詢航班,請先授權"  |
| "str\_please\_set\_login\_password" : "請設置登錄密碼"  |
| "str\_plz\_input\_password" : "請輸入密碼"  |
| "str\_retrieve\_password" : "找回密碼"  |
| "str\_set\_login\_password" : "請設置密碼"  |
| "weibosdk\_demo\_toast\_auth\_canceled" : "取消授權"  |
| "weibosdk\_demo\_toast\_auth\_failed" : "授權失敗"  |
| "gt\_one\_login\_auth\_btn" : "一鍵登錄"  |

## **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.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.WRITE\_CALENDAR | 危险 | 添加或修改日历事件并向客人发送电子邮件 | 允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件 |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| com.china3s.android.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| 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.ACCESS\_WIFI\_STATE | 正常 | 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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| com.china3s.android.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.china3s.android.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.china3s.android.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.china3s.android.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.china3s.android.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.china3s.android.home.view.Main | **Schemes**: @string/growingio\_url\_scheme://, apexdata.d5766f4d9daa8c2e://, @string/tingyun\_app\_scheme\_key://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent100737172://,  |
| com.china3s.android.pay.OrderDetailForPay | **Schemes**: alipaymsp://, **Hosts:** securitypay,  |
| com.china3s.android.message.view.LinkSetUpActivity | **Schemes**: springdeeplink://,  |

**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。**