南明离火
移动应用检测平台

ANDROID 静态分析报告

金蛇 • v1.01088

分析日期: 2025-08-27 11:43:49

应用概览

文件名称:	金蛇.apk
文件大小:	16.0MB
应用名称:	金蛇
软件包名:	cn.chinapost.jdpt.pda.yy
主活动:	com.hzgd.ems.activity.StartActivity
版本号:	1.01088
最小SDK:	21
目标SDK:	29
加固信息:	360加固
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	dc6bcff6a1151928657740290c54dab3
SHA1:	c03f7d0fb96292ff61c6633dba82efb8d239de9a
SHA256:	3b795d5017a3f0c4de36ee81fc92a0da254ffc8ac885ed38467be823d9302801

分析结果严重性分布

高危	中危	信息	安全	关注
3	11	1	2	0

四大组件导出状态统计

Activity组件：37个，其中export的有： 0个
Service组件：2个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-16 01:01:14+00:00
有效期至: 2049-03-10 01:01:14+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x394237f
哈希算法: sha256
证书MD5: 71b63bc054d05532ffd7914179695679
证书SHA1: 4722c00cef464625bea6cb70787f8ecbe9517f04
证书SHA256: c2ce6a69dfa5acb2d47543f1a89c2d6117f9f6836b716849fb2727369fcbe1cf
证书SHA512:
19d053a49bc08a4715686be24e58ced1fd53ce9d7d667a2f41a043345012e62ad62de4629b72e0a2b463c915f051f0315a5ab132daee0590afbe2877512cc3b7

公钥算法: rsa
密钥长度: 2048
指纹: 819a0b997ef396209f799ca0be0286e415520cb5dd0f458fa2f7e860f5cc3d03
共检测到 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	允许应用程序查看所有网络的状态。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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。
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_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
android.permission.ACCEPT_HANDOVER	危险	使呼叫应用程序能够继续在另一个应用程序中启动的呼叫	允许呼叫应用程序继续在另一个应用程序中发起的呼叫。例如，一个视频通话应用程序希望在用户的移动网络上继续语音通话。
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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ_PHONE_STATE授予的功能的一个子集，但对即时应用程序公开。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片
android.permission.WRITE_EXTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。

网络通信安全风险分析

序号	范围	严重级别	描述

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: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130002]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。

代码安全漏洞检测

高危: **3** | 警告: **7** | 信息: **1** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MST G-STORAGE-14	升级会员：解锁高级权限
2	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MST G-CODE-2	升级会员：解锁高级权限
3	应用程序记录日志信息,不应记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MST G-STORAGE-3	升级会员：解锁高级权限
4	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	安全	OWASP MASVS: MST G-NETWORK-4	升级会员：解锁高级权限

5	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	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
6	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
7	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 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
10	如果一个应用程序使用WebView.loadDataWithBaseURL()方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
11	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

12	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
13	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00044	查询该包的activity上次被使用的时间	信息收集 反射	升级会员：解锁高级权限
00045	查询当前运行的应用程序名称	信息收集 反射	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限

00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 信息收集	升级会员：解锁高级权限
00054	从文件安装其他 APK	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.CALL_PHONE android.permission.CAMERA android.permission.ACCEPT_HANDOVER android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS android.permission.PROCESS_OUTGOING_CALLS
其它常用权限	9/46	android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO

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
js.taety.cn	安全	是	**IP**地址: 221.229.203.169 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
tdy.spb.gov.cn	安全	是	**IP**地址: 43.254.119.21 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图
pl.mmlwo.cn	安全	是	**IP**地址: 45.125.45.249 国家: 中国 地区: 中国山东 城市: 济南 纬度: 36.651216 经度: 117.12 查看: 高德地图

uyz.mmlwo.cn	安全	是	**IP地址:** 45.125.45.249 国家: 中国 地区: 中国山东 城市: 济南 纬度: 36.651216 经度: 117.12 查看: 高德地图
b23.tv	安全	是	**IP地址:** 61.147.236.104 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/OnlineRechargeFragment.java
• 211.156.195.12	com/hzgd/zylt/pickupClient.java
• https://211.156.197.65/dln-app/dln/tdqdcxbydzonepointthree/list • https://uyz.mmlwo.cn/ • https://211.156.197.65/dln-app/dln/bktdfkbydzonepointthree/list • https://211.156.197.65/dln-app/dln/ygpbddxxcx/list	com/hzgd/ems/activity/CheckBkActivity.java
• http://tdy.spb.gov.cn/mobile/login • http://tdy.spb.gov.cn/mobile/updatedakarecord • https://uyz.mmlwo.cn/ • http://tdy.spb.gov.cn/mobile/loaddkrecord	com/hzgd/ems/activity/CheckPfActivity.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/pickup-app/p/pda/basedownload/getnewwarninfoname	com/hzgd/ems/activity/AllocateActivity.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/MainActivity.java
• https://211.156.197.65/pdalogin/p/common/logingpyusrface • https://uyz.mmlwo.cn/ • https://211.156.197.65/pdalogin/p/common/loginbyusrsms • https://jinshe-oss-cn-beijing.aliyuncs.com/app.json • https://211.156.197.65/pdalogin/p/common/notokenaccesssendauthcodebyusr	com/hzgd/ems/activity/LoginActivity.java
• http://undefined/	org/jsoup/helper/HttpConnection.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/OnlineRechargeFragment1.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/adt-app/p/clockinforfieldnew/findbykeypointquery • https://211.156.197.65/adt-app/p/clockinforfieldnew/signin	com/hzgd/ems/activity/CheckHbActivity.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/OnlineRechargeTiaoFragment.java

• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasetroadsegone/queryunfinishone • https://211.156.197.65/delivery-app/p/pdasetroadsegone/makereceiveonemixed • https://211.156.197.65/delivery-app/p/pdasetroadsegone/findwaybillnoinfoone • https://211.156.197.65/pcs-app/p/deliverofficecheck/getcountreclist	com/hzgd/ems/activity/ScanCodeBzActivity.java
• https://uyz.mmlwo.cn/ • https://jinshe8.oss-cn-beijing.aliyuncs.com/app.json	com/hzgd/ems/activity/LogoActivity.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasetroadsegmanager/makereceiveonemixed • https://211.156.197.65/pcs-app/p/deliverofficecheck/getcountreclist • https://211.156.197.65/delivery-app/p/pdasetroadsegmanager/findwaybillnoinfoone • https://211.156.197.65/delivery-app/p/pdasetroadsegmanager/queryschedulinginfo	com/hzgd/ems/activity/ScanCodeNqActivity.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/OnlineRechargeTiaoFragment1.java
• 223.5.5.5	com/aaron/baselib/utils/NetworkUtils.java
• 169.254.169.254	com/hzgd/ems/utils/ProxyDetector.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/pdalogin/p/common/changesubstitutionorg	com/hzgd/ems/fragment/MyFragment.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/activity/EditPasswordActivity.java
• https://211.156.197.65/delivery-app/p/delivery/nondeliveryrec/querynondeliveryrec • https://211.156.195.23/delivery-web/a/delivery/returnwork/acceptdelivertask • https://211.156.197.65/delivery-app/p/delivery/pdataskquery/findpdasignwaybillnew.do • https://211.156.195.23/delivery-web/a/delivery/returnwork/querydelivertask • https://211.156.197.65/delivery-app/p/delivery/pdasignwaybillreturned/completeconfirmbatch • https://211.156.195.23/portal/a • https://211.156.197.65/delivery-app/p/delivery/receiptwaybillbatch/updatedlvstate • https://211.156.197.65/delivery-app/p/delivery/cloudcall/newlandfile • https://211.156.195.23 • https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/batchalldeliver • https://211.156.195.23/cas/login • https://211.156.197.65/delivery-app/p/delivery/pdataskquery/findpdasignwaybillinfonew.do • https://211.156.197.65/delivery-app/p/delivery/cloudcall/updatephone • https://211.156.197.65/delivery-app/p/delivery/pdanondeliverybatch/updateallnondeliverybatch • https://211.156.195.23/delivery-web/a/delivery/receiverecode/querydata? • 211.156.195.23 • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/singledeliver • https://211.156.197.65 • https://211.156.197.65/delivery-app/p/delivery/cloudcall/querywaybill • 180.139.97.29	com/hzgd/ems/fragment/HomeFragment1.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/pickup-app/p/pdabasedownload/getnewallinfoname	com/hzgd/ems/activity/DouDouLtActivity.java

本报告由南明离火移动安全分析平台生成

• http://tdy.spb.gov.cn/ • https://uyz.mmlwo.cn/ • http://211.156.201.20:8012/ • https://211.156.197.65/ • https://pl.mmlwo.cn/api?appid=10001 • https://211.156.195.23/ • https://js.taety.cn/ • https://pl.mmlwo.cn	com/hzgd/ems/manager/AppManager.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasetroadsegone/queryunfinishone • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/batchalldeliver • https://211.156.197.65/delivery-app/p/pdasetroadsegone/makereceiveonemixed • https://211.156.197.65/delivery-app/p/delivery/cloudcall/newcallandfile • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/querycyzbybranchandseq • https://211.156.197.65/delivery-app/p/pdasetroadsegone/findwaybillnoinfoone • https://211.156.197.65/delivery-app/p/delivery/cloudcall/querywaybill • https://211.156.197.65/pcs-app/p/deliverofficecheck/getcountreclist	com/hzgd/ems/fragment/ScanCodeFragment.java
• 211.156.197.65	com/aaron/baselib/client/ClientTokenZ1.java
• https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/singledeliver	com/hzgd/ems/activity/SignForActivity$getQueryallwaybillInfoQi5$1$onResponse$1.java
• http://tdy.spb.gov.cn/mobile/login • http://tdy.spb.gov.cn/mobile/updatedakarecord • https://uyz.mmlwo.cn/ • http://tdy.spb.gov.cn/mobile/loaddkrecord	com/hzgd/ems/fragment/CheckPfFragment1.java
• https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/singledeliver	com/hzgd/ems/fragment/HomeFragment1$getQueryallwaybillInfoQi5$1$onResponse$1.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/activity/RegisterActivity.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/adt-app/p/clockinforfieldnew/signin	com/hzgd/ems/fragment/CheckFragment1.java
• https://211.156.197.65	com/hzgd/ems/utils/NewRc4ApiTokenUtill.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/batchalldeliver • https://211.156.197.65/delivery-app/p/delivery/pdasignwaybillreturned/completeconfirmbatch • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/singledeliver • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/querycyzbybranchandseq	com/hzgd/ems/activity/SignForActivity.java
• https://b23.tv/2vcdiz	com/hzgd/ems/activity/AboutActivity.java
• 211.156.197.65	com/aaron/baselib/client/ClientLoginToken.java

• 211.156.197.65	com/aaron/baselib/client/ClientTokenLngLat.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/CardPasswordRechargeFragment.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/activity/ResetPwdActivity.java
• https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/queryallwaybillinfo	com/hzgd/ems/fragment/HomeFragment1$getBatchallDeliverKuaiQi5$1$onResponse$1.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/fragment/GongNengFragment.java
• https://211.156.197.65/pdalogin/p/common/loginbyusrface • https://uyz.mmlwo.cn/	com/hzgd/ems/activity/ZrVipActivity.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/pdalogin/p/common/changesubstitutionorg • https://211.156.197.65/pdalogin/p/common/putorginfo • https://211.156.197.65/pcs-tc-app/p/traceinfo/query	com/hzgd/ems/fragment/TrajectoryQueryFragment.java
• https://211.156.195.23/cas/jdptcaptcha.jpg	com/hzgd/ems/dialog/VerificationImageDialog.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/delivery/pdanondeliverybatch/queryalldeliverinfo	com/hzgd/ems/activity/WeiTuoTouEditActivity.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/activity/HandoverActivity.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/delivery/pdanewfeedbackquery/querytask	com/hzgd/ems/activity/ComprehensiveQueryActivity.java
• http://tdy.spb.gov.cn/mobile/login • http://tdy.spb.gov.cn/mobile/updatedakarecord • https://uyz.mmlwo.cn/ • http://tdy.spb.gov.cn/mobile/loaddkrecord	com/hzgd/ems/fragment/CheckPfFragment.java
• https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/queryallwaybillinfo	com/hzgd/ems/activity/SignForActivity$getBatchallDeliverKuaiQi5$1$onResponse$1.java
• https://uyz.mmlwo.cn/ • https://211.156.197.65/delivery-app/p/pdasetroadsegone/queryunfinishone • https://211.156.197.65/delivery-app/p/pdasetroadsegone/makereceiveonemixed • 211.156.197.65 • https://211.156.197.65/delivery-app/p/pdasignwaybillfeedback/querycyzbybranchandseq • https://211.156.197.65/delivery-app/p/pdasetroadsegone/findwaybillnoinfoone • https://211.156.197.65/pcs-app/p/deliverofficecheck/getcountreclist	com/hzgd/ems/activity/ScanCodeActivity.java
• https://uyz.mmlwo.cn/	com/hzgd/ems/activity/AliPay1Activity.java

• 211.156.197.65	com/aaron/baselib/client/ClientToken.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
360 加固	360	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。
HMS Scan Kit	Huawei	统一扫码服务（Scan Kit）提供便捷的条形码和二维码扫描、解析、生成能力，帮助您快速构建应用内的扫码功能。得益于华为在计算机视觉领域能力的积累，Scan Kit 可以实现远距离码或小型码的检测和自动放大，同时针对常见复杂扫码场景（如反光、暗光、污损、模糊、柱面）做了针对性识别优化，提升扫码成功率与用户体验。Scan Kit 支持 Android 和 iOS 系统集成。其中，Android 系统集成 Scan Kit 后支持横屏扫码能力。
AndroidUtilCode	Blankj	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。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
Jetpack Lifecycle	Google	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	Android	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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS ML Kit	Huawei	机器学习服务（ML Kit）提供机器学习套件，为开发者使用机器学习能力开发各类应用，提供优质体验。得益于华为长期技术积累，ML Kit 为开发者提供简单易用、服务多样、技术领先的机器学习能力，助力开发者更快更好地开发各类 AI 应用。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

敏感凭证泄露检测

可能的密钥
百度地图的=> "com.baidu.lbsapi.API_KEY" : "HswkNS4bJCYkAXbFTCWN6dkrwnXA3FCQ"
cEdnSUd7WecrX4rHhzYLueGuj8H6c7RRbSbrJ6

00395369676e61747572657c736464467465694854587856736d51367c4d5154545f313338353535303733303030333633305f42656c46466e5455001c666f4b346f706142767252757166745675793330664265716d31593d827e000100164a4450545f504b505f53454e445441534b544f50444100001a4a4450545f504b505f435553544f4d45525441534b544f5044410000194a4450545f504b505f53454e445f504f53545f544f5f5044410000114a4450545f444c565f5044415f544f444f0000134a4450545f43574d5f5041434b5f4f524445520032ab0300124a4450545f4d44535f4845415254424541540002
qrcklmDoExthWJiHAp1sVYKU3RFMQw8IGfPO92bvLNj
108b0100044d51545404c0005a00264749445f303032404040
3LtMSEBZqDukovDZ4HGCff8wosvlowf6IFJ3U7LFBIeHfiHBKiFuAV8
ob36GQFv968nE1UBXxNekA9pIHBcvcl0ZWfwFhk
Fwb5BtLRveCWbx7FkXarl1zVOdwDvbDTl7gv
ysHMLgnC6wVqkomIKsi6C9TcGd4d6XQBjeJgdgccvDcD
T2wm9GlUDn3X0wnHHXkE8cqAT6PcE0g0ide6beP9
6c062f94fd6f732b2b1085312b4952bdb892fc67
22698c92494385f5ee37bb62f7c502c1
pFltCfTXtA4AwgVUnwbBMBWBfIJiLDi02ev30V
6e53fc0dc562406d238beaef705abfb5
kyOF2FmQvpPY9LkqiCV0T32vhJet0n93ti2PBoFILxvChjzdOgSG9M0flH78Vm696Q4mHo7VMt

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隐患。