



ANDROID 静态分析报告



🔗 老司机软件库 • v1.8.0

分析日期: 2025-04-26 00:00:15

i应用概览

文件名称:	老司机软件库 v1.8.0.apk
文件大小:	3.97MB
应用名称:	老司机软件库
软件包名:	com.app.lsjcnzml
主活动:	com.app.lsjcnzml.FirstActivity
版本号:	1.8.0
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	1/432
杀软检测:	2 个杀毒软件报毒
MD5:	58ce1131ad11cc76830fcb7ae90c456e
SHA1:	1292420b92bd1e5df389c3ff3e6e211bf8bfbcd1
SHA256:	cced0ec67da08af6a4dc7831941c1ecea3a7300f92ac9bba9790ac3308bf2bf2

分析结果严重性

🚨 高危	🔥 中危	📄 信息	✓ 安全	🔍 关注
4	13	2	1	0

四大组件信息

Activity组件: 8个, 其中export的有: 0个
Service组件: 0个, 其中export的有: 0个
Receiver组件: 0个, 其中export的有: 0个
Provider组件: 4个, 其中export的有: 0个

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: CN=xiao, OU=xiao, O=xiao, L=xiao, ST=xiao, C=xiao
签名算法: rsassa_pkcs1v15
有效期自: 2023-03-09 09:44:13+00:00
有效期至: 2048-03-02 09:44:13+00:00
发行人: CN=xiao, OU=xiao, O=xiao, L=xiao, ST=xiao, C=xiao
序列号: 0x1
哈希算法: sha256
证书MD5: 480bcd4839b7c9ece3fa59244fc37839
证书SHA1: 478ed5aa5c9e4a8110b47e815669975b1df0db38
证书SHA256: 607031ee4575a0f88561357b943a32ed31d65d3b5572e0745b33baa33de86223
证书SHA512:
0d2ced03e88e4e50186e25815e65a4e3749350a524c09bad94860d2b54721696d69bd5ae2a630f3dc5969085a6254dbea483f719410ac099886df6ae3e051533

公钥算法: rsa
密钥长度: 2048
指纹: 540713211c7a9e3f6c2b23033066954c1adb61d7d62782cc6038f6f8c466dbd2
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android 11 新增权限，读取本地文件，如简历，聊天图片。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11 引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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。

网络通信安全

序号	范围	严重级别	描述
----	----	------	----

证书安全分析

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	应用程序使用代码签名证书进行签名

Q MANIFEST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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序数据可以被备份 [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。

</> 安全漏洞检测

高危: 4 | 警告: 9 | 信息: 2 | 安全: 1 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	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
2	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
3	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
4	应用程序使用不安全的随机数生成器	警告	CWE: CWE-538: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MST G-CRYPTO-6	升级会员: 解锁高级权限
5	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。	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') OWASP Top 10: M7: Client Code Quality	升级会员: 解锁高级权限
6	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MST G-STORAGE-10	升级会员: 解锁高级权限
7	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: MST G-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	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
10	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-2	升级会员: 解锁高级权限
11	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员: 解锁高级权限
12	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意义处理不恰当（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
13	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员: 解锁高级权限
14	不安全的WebView实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员: 解锁高级权限

15	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
16	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00054	从文件安装其他APK	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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	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
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
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
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
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
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
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
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
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
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

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
00162	创建 InetAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WiFi信息	WiFi 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	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
00192	获取短信收件箱中的消息	短信	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
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	1/100	android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE

常用: 已知恶意软件经常滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
aria.laoyuyu.me	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
https://openrcv.baidu.com/1010/bplus.gif	p090/C1906.java
1.9.2.6	com/arialyy/aria/http/upload/HttpUThreadTaskAdapter.java
https://github.com/arialyy/aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Options.java
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
- https://hmma.baidu.com/auto.gif - https://hmma.baidu.com/app.gif	p090/RunnableC2021.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://dxp.baidu.com/upgrade?	p090/C1947.java
10.0.0.200 10.0.0.172	p090/C1944.java

第三方SDK

SDK名称	开发者	描述信息
libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现对各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
AgentWeb	Jackson	AgentWeb 是一个基于的 Android WebView，极度容易使用以及功能强大的库，提供了 Android WebView 系列的问题解决方案，并且轻量和极度灵活。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。

追踪器

名称	类别	网址
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

🔑 密钥凭证

可能的密钥
百度统计的=> "BaiduMobAd_STAT_ID" : "c7f29e1d7b"
百度统计的=> "BaiduMobAd_CHANNEL" : "软件库"
5306170b121d15020a111656571b0006064e49101100131b
eb3058191c4f211f69041e64
0578465c465b551b0e4b485840474b5d180a43504e0b0b4241401435512246
5306170b121d15020a1116564a1105
b567395e603e5f7b384079156f7213615d0f51431f53450b426704
c66c044540137d4335584238
83432b6a6f3c53582e767a1f
27464e58424853541b135a505c185407
81641e694104567c0a677d07
43435f5b5c164a5f195b53595d1406475f4a4a5f5f1e12535d1d195b53595d15195551f
5b1911071d170c0b444c050f03470b58
f13770293d6f310f6c033468
fe107b07165d251c62100b6b022a7a
5303061a115740424a09544800131a1a03061a11
15595c404b505b1c11514c475d4c0c1954414b505162b405d5c
d32a4a2c2e61032a59302b51
93244f332269100a673a3a701f107138116c
df1c5938014c312e712f1e5a342d47190160122e7c
6e5a0f1d54410d0f100241dd4d0d185a4f0d181ccb010a1315521e
cb3251001c512d0f1731325652130633f01442511512e1c7d0f3361
a91b45221c422307443c0569130e6f11d27132d3f632f39773e1b78
3411190f151f04034c440d070b4f0950
ac4035597613495f001b781c
6264787c7b316d703a7c747e7a332160786d6d78783935747a3a3e7c747e7a323e727438
7c6237251732276325792b3a263f3d3f73
5957697369747a34216467776f68647237256c7f6124246d6e6f3b1a7e0d69
44081a161d5740425709495b0502

7838213a3e140d372e233834
81641e6941045553074b4e03
d3462d51400b734a344a58127d72135a7f0e
d0773a5d58256e6b0e7a6019
15595c404b505b1c11514c475d4c0c1954414b5057162e495a44
cb3251001c512e03650a1679031c7d0f3361
071247551c094547584a0455095b4a5e4b5c1b56
5b7e7b676c777c3b36766b607a6b2b3e73666c7770311279707c796f7d61737e717a667c7d61737e60687e7478
825e3161570259722d5e5b31
70303529223932757838252e342565723d2a2e3d37223468553e3c382b2627
5306170b121d15020a1116565509130f0a01
4c3f011b011c125c490c0f1f07000c1a5f4d0417094c4c0506075372166501
070d08141f040f48450518130918584d00151f0403427a1d0e10
5306170b121d15020a1116564e0f1d5d5409494d0f0a0e0f
5306170b121d15020a1116564e0f1d5d540a08100a0c575a1100110a18181d760206
d0703959640b7c7a15706b2c5a4c28784f144b4501
d36d3f426036467a15706b2c5a4c21714f144b4501
4a66584258454b05105556465e59554306145d4e5015135c9f5e0a2b4f3c58
0f0e1216115b071254161e1410594b0a120707121259511e105054161e14105854181e52
83432b6a6f3c5d782f5a6a29
3001000a0e171f1819085c4d051c46
d0703959640b7c56377e5b2a
fc175d280d40232a763721450c2958
7e251b011b060816531615051d1a160045571e0d7356561f1c1d49680c7f1b
44081a1b14574042b74e55
286d65736963787f3038717b77337f9c
5306170b121d15020a111656404248040448591b150a150001170116
3441495f454f54531c145d675b1f5300
7f717b62434a74b2706460
58574b4f4025e4b114d5d5c0b570954524957111150541408545210545d5d0f52574a
d36d3f426036467a15706b2c5a4e26744f144b4501

d0703959640b7c7a15706b2c5a4c21714f144b4501
7c1f5e50101b5d575b5a504f455659594b040c4a4a
58574b4f48025e4b114d5d5c08540954524957111150541408545210545d5d0f52574a
5306170b121d15020a1116564e0f1d5d5409495f0a0c111e
d0703959640b7c7a15706b2c5a4e26744f144b4501
70303529223932757838252e342565703d2822393e7f4720332d
d3462d51400b734a34494425567c0e476805
e8224b163e5e1c0d403d2d42122471
d36d3f426036457313705b07
93244f332269100a67391071381d6c
fc175d280d40232a76321c473b0c6c
fd3e510137623a3b673c2f5f
7e457b617b666826337675657d7a766025377e6d7336367f7c7d29086c1f7b
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
836f3d537224575a2c746e0668582e7a4a16
d3462d51400b734a34494425567c0e476a02
6324656b2b357f6d7a78622e3534377171
92394c200f6a3026790a0f65
2a747a7035652d686a63647c7820652b79
6229170d170a044a5f1a190911161a0c495b12011f5a5a1310114564007317
d0703959640b7c7a15706b2c5a4c28
913b58340847183555361d41
a3601f50673b7c5f3e4d6b715
83432b6a6f3c625c1a176d17
541f1a060161d5a07170a011b0a4a5112070d161150680f1c02
eb30581911c4f2e0b5c29195a
5306170b121d15020a11165640423d0a040e
5303061a11574042570a0215
d1593a566a257a0731b47f23
44081a1611b14042570912081a161d
786d68747f646f28256578736978382d60757f6463221a7d6e70

f13770293d6f310f7d1d2b6b2d3871252a75
d31f5801154718157a26167c22346f
d25b2e426d0852441b686d07
cb32510e227f32336c320347280173132565
6c1346541d084446594b055404445113064451554248434a5c1b57
117f415b415c521c094c4f5f47404c5a1f0d4457490c0c4546471332562541
2b202539322922656828353e243575602d3832292e6f5730233d
2b202539322922656828353e243575602d3832292e6f52392425
6b77495349545a14014447574f48445217054c5f4104044d4e4f1b3a5e2d49
dd45025b4f1d4f650c785e377663374b57088712d47f127d6a364f773a5d5825aa12d66b0e7a601965650e7143e077f14757b2e48512b695b1e564d104c491248632c5743207a5b19526b0e7a601967632c5c4e247a4b326858256e6001734f1d424c26786001734f1d40650e7949316b5a34
834126667a007878324b7b2e547335445724735e3161570250513266451a515b005a713e4c5138654d2d07e34f43307d68294e5e31615702
643135746e373826282b623b3b21
d36d3f4260364656377e5b2a
541f1a060d161d5a4e05070f140a100a161150731c1f1f16120a0a0d1c01070c1f1d011c70b0d031612
6e5a0f1d54410d0f10024c1d460d070b090d0e0a451e
2b0b352f352826687d383b2b3334382e6b7930233d78783132336f46226185
5306170b121d15020a1116564e0f1d5d540949550d160f141713
9d58385e5c137d5c3f50673b
8e365d21307b021a722d28620d02632a0f7e
58574b4f48025e4b07465f5c4a09064740464c42020b405a10055a520d111d5d5c1607465f5c4a081449564e444d5c1008545242494442475511175042585c4a02024a5e54501008545210545051024b561006454846060947594c51511608545210545d
64313574703b2734322e623b3b21
2b202539322922656828353e243575643223293c60538c3223
8078324b7b2e585e31615702
5306170b121d15020a1116564042591a150a15000117
d36d3f426036467a15706b2c5a4c26784f144b4501
5306170b121d15020a1116564e0f1d5d5409494a080f0500150811100d
553b3e222932397e73332c253f2e6e7f293832277b4e252938
fc175d280d4023a7b6f3d663937732813433d1c41
d3462d5140b6734a344972135a7f0e
207170717470787a6f322060747629206c7c7c33

805138654d2d6f7e334e5e31615702
d50a682b387704164e1c145300157d
fc175d280d40232a76320e442b24450c2958
55625c465c414f01145152425a5d51470210594a541111585b5a0e2f4b385c
e80b4138085d252d42122471
70645a405a474907125754445c5b574104165f4c5217175e5d5c08294d3e5a
69053b213b262866733635253d3a362065773e2d3376763f3c3d69482c5f3b
f02d521d2a763f37712a165d2a1c47
5303061a115740425709494d0d1b
c9305f0f396c3824783f05731b2f72
d36d3f426036467a15706b2c5a4c28
365850465c564d4a050d444e42064a19
641e203a203d337d682d2e3e26212d3b7e6c2536286d6d2427267253374420
4859677d677a743a2f6a697961666a7c392b62716f2a2a6360613514700367
0c4b696f7c6d300142646562646e60
32484943475e5651504115044c550f
6f185957171c5a505c5d574842515e5e4c030b4d4d
6e5a0f1d54410d0f10024c1d550414155d5d11070f044f1e005a1f1d54410d0f10024c1d550414155d5d11070f04401f101e0011490f1d4a
58574b4f48025e4b114d5d5c0a560954524957111150511408545210545d5d0f52574a
556d2d716d6961777f696179716d696e377e786c1f6c6d1e57213a56011a077979081f1c1f1d1b1a1f1857213a56011a6a4b247377263938391e067079094b277072234c1f18067079094b277072234c1f18067079094b277072234c1f18067079094b27707223396d6c7f0c067079094b27707524396e6f6a1957213a56011a07707908176e176e1f6c6f3e3e1d41a0e71
d0703959640b7f7313705b07
1f2d28343f242f6865253e332938786d20353f2423625a3d2e90
58574b4f48025e4b114d5d5c0a560954524957111150511408545210545d5d0f52574a58574b4f48025e4b114d5d5c0a560954524957111150511408545210545d5d0f52574a49444247550d67175042585c4a02024a5e545010085452105450510345561006454846060947594c5a5c1608545210545d
73292c303b202b6c61213c372d3c7c692431382027665e392a34
fc175d280d40232a763f3d66393773
5303061a1157550a531250561a020e
6d437d677d606e20257073637b7c70662331786b753030797a7b2f0e6a197d
071247551094547584a0455095b4a5847511c56
6f7e7b676e777c3b36766b607a6b2b3e73666c777031096e7d63
5306170b121d15020a111656480315

72267361283d71736c7e30613a717b77757172763962
7c4f0e00404b0d070b0a001f150609091b545c1a1a
6c1346541d084446594b05540f444e42404447430c57
d922422426690b2251382359
d50a682b387704164e1c145301354b
0e4b6b626421074568736f746a
7e0647490902444e424349565c4f4040521d155353
0e456873786273301044607c
5306170b121d15020a1116564042501c00000507060c0e13
d36d3f426036467a15706b2c5a4e26
58574b4f48025e4b03011f5d4e4c1149464254064740464c42020b405a10055a520d114d5d5c1603011f5d4e4c11494642551449564e444d5c100854524249444247550c56175042585c4a02024a5e545010085452105450510345561006454846060947594c5a5c1608545210545d
5303061a115740425709494d0d0c
dc2f60313e7f3f186e06326f
d919683b0d4108164e1c1453
a3601f50673b7c720e50400d624f06665b34
5306170b121d15020a11165642040e
8e365d21307b021a722e02632a0f7e
5306170b121d15020a1116564e0f1d5d58181d010a211a3d4906151f1d11155f5b04061c160804
15595c404b505b1c11514c475d4c0c1d4b5a504b112c474b5a
553b3e222932397e73332e253f2e6e7b3622293235744c2b3826
805138654d2d6f7e334c6d18745b3e
b72e7017297716327109305c263b5a281446180a561a9c420b214d
6656687268757b35206366766e69657336246d7e6025210c6f6e3a1b7f0c68
fe3f673b0e4d22c7b112b6b
666d71757238647137757d77733a284971124647171303c7d733337757d77733b377b7d31
ad5d364a5b10697317496908416415
5306170b121d15020a11165640425d040204
2c7d7c76726b63816574203179603a
594c554e06079435a574c40
4a5c6278627f713f2a6f6c7c64636f793c2e67746a2f2f6665643011750662
cb32510e227f330173132565203059073251001c512e1c7d0f3361

d0703959640b7c7a15706b2c5a4e26
440b352f352826687d383b2b3334382e6b7930233d78783132336746225135
ad5d364a5b106973174a4309666908416415
44081a161d5749130b1d1f080a131f
4349776d776a642a3f7a796971767a6c293b72617f3a3a7370712504601377
5306170b121d15020a11165640424e0204
af42214d713e614c2c4f6438
72267361283d71736c7e30613171642633716460777d767f692e62
de2e4f111c5938014c312e712f1e5a
d049164f7d2e406d3f426036
d50a682b387704164e1c1453001565
5306170b121d15020a1116564042591b150a150001170116
44081a161d574e0f1d5d540a0215051009
5306170b121d15020a111656521c00005b5b04061c160804
2b7a72647e746f68273a454676756e35683b
d3462d51400b734a34494425567c0e47680c
75221c061c010f41541112021a1d11074250190a145151181b1a4e6f1b781c
28313428233833747939242f352464713c2923383f7e4621322c
f02d521d2a76320f7d1d2b6b
d0703959640b7c7a15706b2c5a4c21
4a505549425952151858454e54450b105cd942595e1f2740534d
1d362f34301a0339202d363a
d50a682b387704164e1c1453001773
d0483e667c147a7e717e6a20
a2752a41740a63680d79631a6652064a21f02
d50a682b387704164e1c1453001773
5d4e6f6968346364617a626262
d36d3f426036467a15706b2c5a4c21
134706084843050f030208171d0e0101135c541212
dd377e3a3a45033f56151c5938014c3d367b302e712f1e5a350476092252

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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成