南明离火
移动应用检测平台

ANDROID 静态分析报告

AVATrade • v1.0

分析日期: 2024-07-05 19:54:48

应用概览

文件名称:	avatrade.apk
文件大小:	1.61MB
应用名称:	AVATrade
软件包名:	com.example.zjyjqk.zjyjqk
主活动:	com.example.zjyjqk.zjyjqk.MainActivity
版本号:	1.0
最小SDK:	25
目标SDK:	25
加固信息:	未加壳
应用程序安全分数:	38/100 (高风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	8c302d0b09dba40794ea2ca6c6c10d3a
SHA1:	f17fd48a9222d394418d7234e83c0f9027c1ed7b
SHA256:	c97c03efa103b3488e3186e9d242f6b9b45b29031419fbfc3883554e5d2cfae0

分析结果严重性分布

高危	中危	信息	安全	关注
3	1	0	1	0

四大组件导出状态统计

Activity组件：1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：0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: False
v3 签名: False
v4 签名: False
主题: C=21, ST=, L=H6yvEBB06N, O=pOc6YW50VR, OU=L85RRiyIiP, CN=tkYoOoCNBQ
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-16 09:45:12+00:00
有效期至: 2024-08-14 09:45:12+00:00
发行人: C=21, ST=, L=H6yvEBB06N, O=pOc6YW50VR, OU=L85RRiyIiP, CN=tkYoOoCNBQ
序列号: 0x123953fef29d4611
哈希算法: sha256
证书MD5: 59dbe54a12aedd0e41dd0df4d9ac6f46
证书SHA1: 4f5567a04d7f373d3fea9931686b74c46018d608
证书SHA256: ada27ef8225f098da90145d837fd33ab33666d08d4361df61a41720193222135
证书SHA512:
5689c6c5c2d91143feabf094fd38aa317838059fe6325c55f62fa3d47b4ac9cb7c137d72ec3c61163d350be1e79651cd97ba37c0b3bf20ee0f84fe04b85fa3e

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.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.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_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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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。
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。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.android.launcher2.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.android.launcher3.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.yulong.android.launcherL.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.bbk.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.qiku.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	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.zte.mifavor.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。

com.lenovo.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.google.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.yulong.android.launcher3.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
org.adw.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.qihoo360.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.lge.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
net.qihoo.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
org.adwfreak.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
org.adw.launcher_donut.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.launcher3.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.fede.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.nd.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.yulong.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.ztemt.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
cn.nubia.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.gionee.amisystem.permission.READ_SHORTCUT	未知	未知权限	来自 android 引用的未知权限。
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。

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: **1** | 警告: **0** | 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
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **1** | 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 Android 7.1-7.1.2, [minSdk=25]	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	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	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。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	启用了调试配置。生产版本不能是可调试的	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
2	不安全的Web视图实现。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

3	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: MSTG-STORAGE-14	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	13/30	android.permission.GET_TASKS android.permission.READ_CONTACTS android.permission.VIBRATE android.permission.WRITE_CONTACTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.GET_ACCOUNTS android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WRITE_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

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。

URL 链接安全分析

URL信息	源码文件
• https://bomkfdrew-8g0uywyka225nd9f-1320561696.ap-shanghai.app.tcloudbase.com/xiaobo.com.html	自研引擎-A

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

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。