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

**Debot（ 2.3.10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 | Debot |
| 版本 | 2.3.10 |
| 包名 | io.diting.app.android |
| 域名线索 | 32条 |
| URL线索 | 38条 |
| APP图标 |  |
| 分析日期 | 2025年9月13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 | debot-native.apk |
| 文件大小 | 29.55MB |
| MD5值 | a39b16c1d14d27d1a3a443013ef8cd6d |
| SHA1值 | fb36a09d89ac1374ff9c8d44fdf24ccacd557c17 |
| SHA256值 | 8e54f15dcc17b09393ed15e0292b2e99c83de1c10eb453294836134c3e6fd81d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Debot |
| 包名 | io.diting.app.android |
| 主活动Activity | io.diting.app.android.MainActivity |
| 安卓版本名称 | 2.3.10 |
| 安卓版本 | 17 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| stat.api.tpns.tencent.com | IP: 42.194.154.20  所属国家: China  地区: Beijing  城市: Beijing |
| code.google.com | IP: 142.250.73.142  所属国家: United States of America  地区: California  城市: Mountain View |
| alogus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| aspect-upush.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cs.android.com | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| resolve.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| issuetracker.google.com | IP: 142.250.73.142  所属国家: United States of America  地区: California  城市: Mountain View |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| developer.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| developer.android.com | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39  所属国家: China  地区: Beijing  城市: Beijing |
| ucc.umeng.com | IP: 203.119.169.9  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| dev.to | IP: 151.101.194.217  所属国家: United States of America  地区: California  城市: San Francisco |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| errnewlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gist.github.com | IP: 8.7.198.45  所属国家: United States of America  地区: Louisiana  城市: Monroe |
| cnlogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| api.tpns.tencent.com | IP: 101.72.227.61  所属国家: China  地区: Hebei  城市: Langfang |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| log.tpns.tencent.com | IP: 163.177.1.125  所属国家: China  地区: Guangdong  城市: Guangzhou |
| errnewlogos.umeng.com | IP: 47.246.110.18  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Jiangsu  城市: Nanjing |
| docs.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| alogsus.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| android.googlesource.com | IP: 173.194.202.82  所属国家: United States of America  地区: California  城市: Mountain View |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/d/c.java |
| https://issuetracker.google.com/issues/139738913 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/af7dcdf35a37d7a7dbaad7d9869c1c91bce2272b | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/9b5257c9c99c4cb541d8e8e78fb04f008b1a9091 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/893d6fe48d37f71e683f722457bea646994a10 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/b3a9bc038d3a218b1dbdf7b5668e3d6c12be5e | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=171190 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/pyricau/4df64341cc978a7de414 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=171830 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=172542 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=172659 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/andaag/b05ab66ed0f06167d6e0 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173689 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173788 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173789 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/27db46850b708070452c0ce49daf5f79503fbde6 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/7a96f3c917e0001ee739b65da37b2fadec7d7765 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=152173 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/jankovd/891d96f476f7a9ce24e2 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=188551 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://android.googlesource.com/platform/frameworks/base/+/5b734f2430e9f26c769d6af8ea5645e390fcf5af%5E%21/ | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=198852 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/e0bef71662d81caaaa0d7214fb0bef5d39996a69 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://android.googlesource.com/platform/frameworks/base/+/193520e3dff5248ddcf8435203bf99d2ba667219%5E%21/core/java/android/view/accessibility/AccessibilityNodeInfo.java | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/aosp-mirror/platform\_frameworks\_base/commit/86b326012813f09d8f1de7d6d26c986a909d | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://issuetracker.google.com/issues/112792715 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1210 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://issuetracker.google.com/issues/129250419 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://cs.android.com/android/\_/android/platform/frameworks/base/+/89608118192580ffca026b5dacafa637a556d578\nFixed | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://cs.android.com/android/\_/android/platform/frameworks/base/+/1f771846c51148b7cb6283e6dc82a216ffaa5353\nRelated | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://dev.to/pyricau/beware-packagemanager-leaks-223g | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/cypressious/91c4fb1455470d803a602838dfcd5774 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/jankovd/a210460b814c04d500eb12025902d60d | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/32 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/177 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1819 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/696 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/namespace-prefixes | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-general-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-parameter-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/string-interning | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| https://log.tpns.tencent.com/device/v4/sdk/list | com/tencent/android/tpush/common/j.java |
| https://guid. | com/tencent/tpns/baseapi/core/a.java |
| https://api.tpns.tencent.com/guid/v4/register\_device | com/tencent/tpns/baseapi/core/a.java |
| https://stat. | com/tencent/tpns/baseapi/core/a.java |
| https://stat.api.tpns.tencent.com/log/v4/statistics/push | com/tencent/tpns/baseapi/core/a.java |
| https://log. | com/tencent/tpns/baseapi/core/a.java |
| https://log.tpns.tencent.com/log/v4/statistics/push | com/tencent/tpns/baseapi/core/a.java |
| https://stat.api.tpns.tencent.com/v3/mobile/log/upload | com/tencent/tpns/baseapi/core/a.java |
| https://api.tpns.tencent.com/device/v4/account/batch\_operate | com/tencent/tpns/baseapi/core/a.java |
| https://aspect-upush.umeng.com/occa/v1/event/report | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/ext\_event | com/umeng/analytics/pro/aq.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/l.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/ar.java |
| https://resolve.umeng.com/resolve | com/umeng/analytics/pro/bt.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/119267/detail/118637 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://developer.umeng.com/docs/193624/detail/194590 | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fh.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fw.java |
| https://%1$s/gslb/?ver=5.0 | com/xiaomi/push/ch.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fx.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/ex.java |
| http://10.38.162.35:9085 | com/xiaomi/push/service/q.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/q.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/ax.java |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md | g5/c.java |
| https://github.com/Baseflow/flutter-permission-handler/issues | w2/d.java |
| https://developer.android.com/guide/topics/permissions/overview | w2/i.java |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md | h5/h.java |
| https://docs.flutter.dev/deployment/android | z2/c.java |
| https://github.com/flutter/flutter/issues/165510 | i/b.java |
| https://developer.android.com/reference/android/view/View | i/b.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0  u0013android@android.com | k1/l.java |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-14 07:31:54+00:00 有效期至: 2055-04-14 07:31:54+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0x8640ec08e0411bb27b043ddbc35b216361feade0 哈希算法: sha256 md5值: 79c6a4a1f39e2079a0cda490574c368d sha1值: 59bc9437455dba1eab7f87e005a174f728ae778c sha256值: 58e5cf102486b4bc2f9593eb69a675dcc51fb1595a669218b46caeee9fa4a8c0 sha512值: 02889c3b158e4666d95a21dfae178a4d73cce6ef2121cf88670621bae2a482d8f0c34d6da4a80ecc5ce5779876091735c54510a9bb30f2a64f4cd01e68897ba5 公钥算法: rsa 密钥长度: 4096 指纹: 745a696d7a28bdaff1064899710553d860b60b1f33cbd4757c37464661d5f42a**

## **6. 硬编码敏感信息**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_SPECIAL\_USE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| io.diting.app.android.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| io.diting.app.android.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| io.diting.app.android.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| io.diting.app.android.permission.XGPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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 |
| io.diting.app.android.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.diting.app.android.MainActivity | **Schemes**: debot://, https://, um.682d836c79267e02106ae276://,  **Hosts:** open, debot.ai,  **Path Prefixes:** /, |
| com.tencent.android.tpush.TpnsActivity | **Schemes**: tpns://,  **Hosts:** io.diting.app.android, |
| com.tencent.android.tpush.InnerTpnsActivity | **Schemes**: stpns://,  **Hosts:** io.diting.app.android, |

**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。**