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

**隆基CRM（ 1.3.5.2022122801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 | 隆基CRM |
| 版本 | 1.3.5.2022122801 |
| 包名 | cn.com.longi.sfa |
| 域名线索 | 34条 |
| URL线索 | 117条 |
| APP图标 |  |
| 分析日期 | 2025年7月22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 | 110\_4b53394ad1cffad64ea17357167fb7de.apk |
| 文件大小 | 8.75MB |
| MD5值 | 66ca6b68b68be8d4c9990f59e6de203b |
| SHA1值 | 0c63017ac70c3e59d6b43655a822bb3418ea37b7 |
| SHA256值 | 15dfa44df5c78b80a458b992bee9b17004123cfbcc113ed4670d6e5d887f37f4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 隆基CRM |
| 包名 | cn.com.longi.sfa |
| 主活动Activity | cn.com.rektec.xrm.app.WelcomeActivity |
| 安卓版本名称 | 1.3.5.2022122801 |
| 安卓版本 | 29 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| h.trace.qq.com | IP: 109.244.244.241 所属国家: China 地区: Beijing 城市: Beijing  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| debugx5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| debugtbs.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| soft.tbs.imtt.qq.com | IP: 121.51.175.60 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| log.tbs.qq.com | IP: 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| crmmobile.longi.com | IP: 124.114.178.18 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| jivesoftware.org | IP: 216.146.46.11 所属国家: United States of America 地区: New Hampshire 城市: Manchester  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| etherx.jabber.org | IP: 208.68.163.210 所属国家: United States of America 地区: Iowa 城市: Monticello  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| mdc.html5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| bcr2.intsig.net | IP: 106.75.218.19 所属国家: China 地区: Shanghai 城市: Shanghai  |
| android.bugly.qq.com | IP: 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| crm.rektec.com.cn | 没有服务器地理信息.  |
| cfg.imtt.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| ofloc.map.baidu.com | IP: 111.206.209.193 所属国家: China 地区: Beijing 城市: Beijing  |
| www.igniterealtime.org | IP: 52.58.216.59 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| jabber.org | IP: 208.68.163.216 所属国家: United States of America 地区: Iowa 城市: Monticello  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| upload-z2.qiniup.com | IP: 220.181.135.136 所属国家: China 地区: Beijing 城市: Beijing  |
| ce3e75d5.jpush.cn | IP: 120.233.50.35 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| sdkapi-smartop.jiguang.cn | 没有服务器地理信息.  |
| daup.map.baidu.com | IP: 124.237.208.108 所属国家: China 地区: Hebei 城市: Baoding  |
| jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| api.map.baidu.com | IP: 111.206.209.166 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jivesoftware.org | IP: 216.146.46.11 所属国家: United States of America 地区: New Hampshire 城市: Manchester  |
| pms.mb.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://xmlpull.org/v1/doc/features.html  | org/jivesoftware/smack/PacketReader.java  |
| http://jabber.org/protocol/compress  | org/jivesoftware/smack/PacketReader.java  |
| http://etherx.jabber.org/streams\  | org/jivesoftware/smack/PacketWriter.java  |
| http://jabber.org/protocol/httpbind  | org/jivesoftware/smack/BOSHConnection.java  |
| http://jabber.org/protocol/compress'>  | org/jivesoftware/smack/XMPPConnection.java  |
| http://xmlpull.org/v1/doc/features.html  | org/jivesoftware/smack/BOSHPacketReader.java  |
| http://xmlpull.org/v1/doc/features.html  | org/jivesoftware/smack/SmackConfiguration.java  |
| http://xmlpull.org/v1/doc/features.html  | org/jivesoftware/smack/provider/ProviderManager.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties  | org/jivesoftware/smack/util/PacketParserUtils.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | org/jivesoftware/smack/packet/Packet.java  |
| http://jabber.org/protocol/disco  | org/jivesoftware/smackx/ServiceDiscoveryManager.java  |
| http://jabber.org/protocol/chatstates  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/xhtml-im  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/offline  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://www.jivesoftware.org/protocol/sharedgroup  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/address  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/si  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/ConfigureProviderManager.java  |
| http://jabber.org/protocol/xhtml-im  | org/jivesoftware/smackx/XHTMLManager.java  |
| http://jabber.org/protocol/chatstates  | org/jivesoftware/smackx/ChatStateManager.java  |
| http://jabber.org/protocol/offline  | org/jivesoftware/smackx/OfflineMessageManager.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/PEPManager.java  |
| http://jabber.org/protocol/address  | org/jivesoftware/smackx/MultipleRecipientManager.java  |
| http://jabber.org/protocol/si/profile/file-transfer  | org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java  |
| http://jabber.org/protocol/si  | org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java  |
| http://jabber.org/protocol/ibb  | org/jivesoftware/smackx/bytestreams/ibb/InBandBytestreamManager.java  |
| http://jabber.org/protocol/bytestreams  | org/jivesoftware/smackx/bytestreams/socks5/Socks5BytestreamManager.java  |
| http://jabber.org/protocol/bytestreams\  | org/jivesoftware/smackx/bytestreams/socks5/packet/Bytestream.java  |
| http://www.igniterealtime.org/projects/smack  | org/jivesoftware/smackx/entitycaps/EntityCapsManager.java  |
| http://jabber.org/protocol/caps  | org/jivesoftware/smackx/entitycaps/EntityCapsManager.java  |
| http://jabber.org/protocol/caps\  | org/jivesoftware/smackx/entitycaps/packet/CapsExtension.java  |
| http://xmlpull.org/v1/doc/features.html  | org/jivesoftware/smackx/entitycaps/cache/SimpleDirectoryPersistentCache.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/pubsub/packet/PubSubNamespace.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/muc/Occupant.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/muc/PacketMultiplexListener.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/muc/DeafOccupantInterceptor.java  |
| http://jivesoftware.org/protocol/muc  | org/jivesoftware/smackx/muc/DeafOccupantInterceptor.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/muc/MultiUserChat.java  |
| http://jabber.org/protocol/commands  | org/jivesoftware/smackx/commands/AdHocCommandManager.java  |
| http://jabber.org/protocol/disco  | org/jivesoftware/smackx/packet/DiscoverInfo.java  |
| http://jabber.org/protocol/commands\  | org/jivesoftware/smackx/packet/AdHocCommandData.java  |
| http://jabber.org/protocol/commands  | org/jivesoftware/smackx/packet/AdHocCommandData.java  |
| http://jabber.org/protocol/nick  | org/jivesoftware/smackx/packet/Nick.java  |
| http://jabber.org/protocol/address  | org/jivesoftware/smackx/packet/MultipleAddresses.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/packet/PEPEvent.java  |
| http://jabber.org/protocol/xhtml-im  | org/jivesoftware/smackx/packet/XHTMLExtension.java  |
| http://www.jivesoftware.org/protocol/sharedgroup\  | org/jivesoftware/smackx/packet/SharedGroupsInfo.java  |
| http://jabber.org/protocol/offline  | org/jivesoftware/smackx/packet/OfflineMessageInfo.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/packet/PEPItem.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/packet/MUCInitialPresence.java  |
| http://jabber.org/protocol/shim  | org/jivesoftware/smackx/packet/HeadersExtension.java  |
| http://jabber.org/protocol/si\  | org/jivesoftware/smackx/packet/StreamInitiation.java  |
| http://jabber.org/protocol/si/profile/file-transfer\  | org/jivesoftware/smackx/packet/StreamInitiation.java  |
| http://jabber.org/protocol/si/profile/file-transfer  | org/jivesoftware/smackx/packet/StreamInitiation.java  |
| http://jabber.org/protocol/feature-neg  | org/jivesoftware/smackx/packet/StreamInitiation.java  |
| http://jabber.org/protocol/feature-neg\  | org/jivesoftware/smackx/packet/StreamInitiation.java  |
| http://jabber.org/protocol/offline\  | org/jivesoftware/smackx/packet/OfflineMessageRequest.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/packet/MUCAdmin.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/packet/MUCUser.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/packet/MUCOwner.java  |
| http://jabber.org/protocol/chatstates  | org/jivesoftware/smackx/packet/ChatStateExtension.java  |
| http://jabber.org/protocol/pubsub  | org/jivesoftware/smackx/packet/PEPPubSub.java  |
| http://jabber.org/protocol/disco  | org/jivesoftware/smackx/packet/DiscoverItems.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/MetaData.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/user/Workgroup.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/workgroup/user/Workgroup.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/user/Workgroup.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/user/Workgroup.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/agent/Offer.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/agent/AgentRoster.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/agent/AgentSession.java  |
| http://jabber.org/protocol/muc  | org/jivesoftware/smackx/workgroup/agent/AgentSession.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/agent/AgentSession.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/agent/OfferConfirmation.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/agent/OfferConfirmation.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/util/MetaDataUtils.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/util/MetaDataUtils.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/GenericSettings.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/OfflineSettings.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/ChatSettings.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/WorkgroupProperties.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/SearchSettings.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/settings/SoundSettings.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/Transcript.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/TranscriptSearch.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/OfferRevokeProvider.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/AgentWorkgroups.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/AgentStatusRequest.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/AgentStatusRequest.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/Transcripts.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/OfferRequestProvider.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/OfferRequestProvider.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/OfferRequestProvider.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/MonitorPacket.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/OccupantsInfo.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/RoomTransfer.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/RoomTransfer.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/QueueDetails.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/QueueUpdate.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/QueueUpdate.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/AgentStatus.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/AgentStatus.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/SessionID.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/AgentInfo.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/QueueOverview.java  |
| http://jabber.org/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/DepartQueuePacket.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/RoomInvitation.java  |
| http://jivesoftware.com/protocol/workgroup\  | org/jivesoftware/smackx/workgroup/packet/RoomInvitation.java  |
| http://jabber.org/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/WorkgroupInformation.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/packet/UserID.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/ext/history/ChatMetadata.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/ext/history/AgentChatHistory.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/ext/notes/ChatNotes.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/ext/macros/Macros.java  |
| http://jivesoftware.com/protocol/workgroup  | org/jivesoftware/smackx/workgroup/ext/forms/WorkgroupForm.java  |
| https://sdkapi-smartop.jiguang.cn  | cn/jiguang/be/c.java  |
| https://upload-z2.qiniup.com  | cn/jiguang/bf/a.java  |
| https://ce3e75d5.jpush.cn/wi/cjc4sa  | cn/jiguang/ax/c.java  |
| https://ce3e75d5.jpush.cn/wi/d8n3hj  | cn/jiguang/ax/c.java  |
| https://ce3e75d5.jpush.cn/wi/op8jdu  | cn/jiguang/s/c.java  |
| https://crmmobile.longi.com:18002/ula.html  | cn/com/rektec/xrm/app/PrivacyWebViewActivity.java  |
| https://crmmobile.longi.com:18002/privacy.html  | cn/com/rektec/xrm/app/PrivacyWebViewActivity.java  |
| http://debugx5.qq.com  | cn/com/rektec/xrm/app/LoginActivity.java  |
| http://crm.rektec.com.cn:7901/  | cn/com/rektec/xrm/setting/ChangeServerUrlDevActivity.java  |
| http://jabber.org/protocol/chatstates  | cn/com/rektec/chat/XmppConnectionManager.java  |
| http://jabber.org/protocol/muc  | cn/com/rektec/chat/XmppConnectionManager.java  |
| http://jabber.org/protocol/offline  | cn/com/rektec/chat/XmppConnectionManager.java  |
| http://jabber.org/protocol/nick+notify  | cn/com/rektec/chat/XmppConnectionManager.java  |
| http://jabber.org/protocol/muc  | cn/com/rektec/chat/RTGroupManager.java  |
| http://jabber.org/protocol/disco  | cn/com/rektec/chat/RTGroupManager.java  |
| http://bcr2.intsig.net/BCRService/BCR\_VCF2?user=eastlv@rektec.com.cn&pass=7JQAFN5JEYRJ3DTC&json=1&lang=2  | cn/com/rektec/ocr/utils/HttpUtil.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/e/g.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/cc.php  | com/baidu/location/b/e.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/e.java  |
| https://ofloc.map.baidu.com/locnu  | com/baidu/location/b/q.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/b/a.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://www.w3.org/XML/1998/namespace  | com/kenai/jbosh/Attributes.java  |
| http://www.w3.org/XML/1998/namespace  | com/kenai/jbosh/ComposableBody.java  |
| http://jabber.org/protocol/httpbind  | com/kenai/jbosh/BodyQName.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/m.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/m.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/j.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| http://crm.rektec.com.cn:7901/  | Mogua Engine V2  |
| http://crm.rektec.com.cn:7501/  | Mogua Engine V2  |
| http://crm.rektec.com.cn:9901/  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| eastlv@rektec.com  | cn/com/rektec/ocr/utils/HttpUtil.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: False 找到 1 个唯一证书 主题: ST=Jiangsu, L=Suzhou, O=RekTec, OU=RekTec, CN=RekTec 签名算法: rsassa\_pkcs1v15 有效期自: 2015-04-02 09:04:23+00:00 有效期至: 2040-03-26 09:04:23+00:00 发行人: ST=Jiangsu, L=Suzhou, O=RekTec, OU=RekTec, CN=RekTec 序列号: 0x53391390 哈希算法: sha256 md5值: 93fb92d0a72919e8ba1e49ffae6c638c sha1值: 8e56060ec41212c8ce1212d346843d833cc22c5a sha256值: b17bd70413593724151eecc3605a578c6df68fbea98165ce4f64406e6d4e558e sha512值: b438d1ef60538e3304d51961c4d1d6250c7830315c6d926e9927888b3c8da70e7064cb67d93bc465ef92056971a3a0a10dcdf35b89f42249a216132bcd34059b 公钥算法: rsa 密钥长度: 2048 指纹: 6301e1af33f768063d46b91a2d5cdb9ad7fb259199387304a9512ed680787a11**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "password" : "密码"  |
| "remember\_password" : "记住密码"  |
| "user\_name" : "账号"  |
| "password" : "Password"  |
| "remember\_password" : "Remember"  |
| "user\_name" : "Account"  |
| "password" : "密码"  |
| "remember\_password" : "记住密码"  |
| "user\_name" : "账号"  |

## **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 |
| --- | --- | --- | --- |
| cn.com.longi.sfa.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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\_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\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.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\_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.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.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\_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 |
| 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.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 |
| 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.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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。 |
| 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 |
| 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 |

## **10. 应用内通信**

**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。**