MoGua

360借条 1.10.68.APK 分析报告

APP名称: 360借条

包名:	com.qihoo.loan
域名线索:	21条
URL线索:	7条
邮箱线索:	0条
分析日期:	2025年9月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: QiHooLoan-oppo-release-1.10.68-701.apk
文件大小: 66.96MB
MD5值: 2f5e40578444aa7c7641ad8487e3b264
SHA1值: 68d4e3413935806e36023d6ff8b0db05d35c9d12
SHA256值: 8f91d86fe5989e819d7cdf0393f9007623fe48f6fe7de90a57f7799583db3002

APP 信息

App名称: 360借条
包名: com.qihoo.loan
主活动Activity: com.qihoo.loan.LunchActivity
安卓版本名称: 1.10.68
安卓版本: 701

域名线索

域名	服务器信息
grs.dbankcloud.eu	没有服务器地理信息.
connectivitycheck.platform.dbankcloud.com	**IP**: 218.68.58.28 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
grs.platform.dbankcloud.ru	没有服务器地理信息.
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

data-drcn.push.dbankcloud.com	**IP**: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics-dra.dt.dbankcloud.cn	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metrics1-drcn.dt.dbankcloud.cn	**IP**: 218.12.91.83 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
huashan-datahub-drcn.emui.dbankcloud.com	**IP**: 49.4.36.71 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
connectivitycheck.cbg-app.huawei.com.cn	**IP**: 49.4.45.202 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast'

	城市: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
metrics-dre.dt.dbankcloud.cn	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
render.alipay.com	**IP**: 101.28.133.85 **所属国家**: China **地区**: Hebei **城市**: Handan **纬度**: 36.600559 **经度**: 114.467781
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.cn	**IP**: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.asia	**IP**: 119.8.176.197 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
httpdns.huaweicloud.com	**IP**: 159.138.112.7 **所属国家**: Chile **地区**: Region Metropolitana de Santiago **城市**: Santiago **纬度**: -33.426498 **经度**: -70.566521
grs.dbankcloud.com	**IP**: 113.201.107.54 **所属国家**: China **地区**: Shaanxi **城市**: Baoji **纬度**: 34.353611

	经度: 107.375275

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html	Mogua Engine V1
https://httpdns.huaweicloud.com	Mogua Engine V1
https://metrics1-drcn.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics-dra.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics-dre.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics5.dt.dbankcloud.ru:443	Mogua Engine V2
https://huashan-datahub-drcn.emui.dbankcloud.com	Mogua Engine V2
https://connectivitycheck.cbg-app.huawei.com.cn/	Mogua Engine V2
https://connectivitycheck.platform.dbankcloud.com/	Mogua Engine V2
https://data-drcn.push.dbankcloud.com	Mogua Engine V2
https://data-dra.push.dbankcloud.com	Mogua Engine V2
https://data-dre.push.dbankcloud.com	Mogua Engine V2
https://data-drru.push.dbankcloud.com	Mogua Engine V2

https://metrics1-drcn.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.dt.dbankcloud.ru:6447	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://grs.platform.dbankcloud.ru	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2

邮箱线索

手机线索

手机号	所在文件
14534438610	Mogua Engine V2
16057009010	Mogua Engine V2
19318408234	Mogua Engine V2

18138650888	Mogua Engine V2
14534438610	Mogua Engine V2
19298225107	Mogua Engine V2

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: CN=loan
签名算法: rsassa_pkcs1v15
有效期自: 2016-04-11 07:22:03+00:00
有效期至: 2041-04-05 07:22:03+00:00
发行人: CN=loan
序列号: 0x2f72db56
哈希算法: sha256
md5值: f8837fc6c737023c70a4cf368923a6da
sha1值: 3a4582d530171a42137b7a2816935c239b4afdf9
sha256值: 7129f2e6e961ff2fd06cf34443998ae02ffcbe7dc2ebc3681ac7141d60c44870
sha512值: d4862c9c71e66cb7770a10f3861d04e2ca50003eb1de7fdd1890853e124f3b2d097555668ac5bc9f500b213a1a4856e744baf33bc6015b64ae1c264f026a6e51
公钥算法: rsa
密钥长度: 2048
指纹: 840f6159cddbe0355c1ff6617566d4791126e48e871b03ad9002e2c2b9524622

硬编码敏感信息

可能的敏感信息
"loan_event_id_pwd_dialog" : "9003601"

"loan_pwd_verify_forget_face" : "忘记交易密码，可通过刷脸完成借款申请，完成借款后可在APP→我的→账号设置→账户安全管理→重置交易密码，进行交易密码修改。"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.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.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_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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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。
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。

com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
com.qihoo.loan.permission.LDSDK_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.qihoo.loan.permission.QDAS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.android.permission.GET_INSTALLED_APPS	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
com.qihoo.loan.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.qihoo.loan.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

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
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.qihoo.loan.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.qihoo.loan.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.qihoo.loan.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.qihoo.loan.LunchActivity	Schemes: qihooloan://, https://, Hosts: 360.cn, app.xjietiao.com, jrurl.cn,

com.qihoo.loan.SchemeLauncherActivity	Schemes: qihoopanda://,
com.alipay.sdk.app.AlipayResultActivity	Schemes: qihooloan_alipay://,
com.tencent.tauth.AuthActivity	Schemes: tencent1105862642://,

---