MoGua

360借条 1.0.APK 分析报告

APP名称: 360借条

包名:	cdeidjdc.ejjcfcad
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年7月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: cdeidjdc.ejjcfcad.apk
文件大小: 5.67MB
MD5值: 5628e1e2d22d0c275cb1becd062179e2
SHA1值: 4f0d4a24b5271ea3a711a17cd9a70c6e759c6340
SHA256值: 6a7cfa448ed5bb9875b361f1db7ed21e008ab840951fcf62c0e15219ca31993d

APP 信息

App名称: 360借条
包名: cdeidjdc.ejjcfcad
主活动Activity: bjgbdadbebl.cgacbcceeam.bficegjjecn.cehidaefecj
安卓版本名称: 1.0
安卓版本: 1

域名线索

URL线索

邮箱线索

手机线索

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=cn, ST=aifhhecf, L=gefjgade, O=fabeefad, OU=bcaagihc, CN=hbadafjb

签名算法: rsassa_pkcs1v15
有效期自: 2024-05-03 04:44:43+00:00
有效期至: 2124-04-09 04:44:43+00:00
发行人: C=cn, ST=aifhhecf, L=gefjgade, O=fabeefad, OU=bcaagihc, CN=hbadafjb
序列号: 0x7c544f0c
哈希算法: sha256
md5值: fb0f4274d727af59dd58b5e45b0a6f0f
sha1值: 95256f266560fe977a864b9028f24969875eba57
sha256值: 08ea7769114aa9f3985dc65e4117c9009cc357c131b1f5fbd9b8de9381b3ba88
sha512值: bb874257c9d79e46dcbf3cf76412e85e2f9e2d4cf2c3948d3a4017aebed287752c6fa1c897ae14d442c706e5bbf819ba5523116d9280fd4d04291a6fff3d23fc
公钥算法: rsa
密钥长度: 1024
指纹: ba034ea4bbf8c3877e1cb707ad3e94bbdb29af67206dc17c492bb883f10d6413

硬编码敏感信息

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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.MICROPHONE	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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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.READ_SETTINGS	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
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.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.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.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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
cdeidjdc.ejjcfcad.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
cdeidjdc.ejjcfcad.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
bjgbdadbebl.cgacbcceeam.bficegjjecn.cehidaefecj	Schemes: http://, https://, about://, javascript://, inline://, tbopen://, fhbadebf://, Hosts: bjgbdadbebl.cgacbcceeam.videowallpaper, Mime Types: text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml, Path Prefixes: /index.html,