MoGua

# APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

小雁收银
YOUNG GEESE CASHIER

小雁收银 1.0.3.APK

| | |
|---|---|
| APP名称: | 小雁收银 |
| 包名: | com.dcits.myapplication |
| 域名线索: | 0条 |
| URL线索: | 0条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2022年2月3日 12:44 |

## 文件信息

文件名: xiaoyanshouyin513260.apk
文件大小: 4.73MB
**MD5值:** eaa6586b843a13aef68b22b7b13f04f9
**SHA1值:** 09ca3bac424b23b03c1dbd95b8d7189723e7e1c2
**SHA256值:** 1ca3ff51cd24a7c59e2df5527c9ff802800f6e5efc390fbf89c5c52836e0ee0e

# APP 信息

**App名称:** 小雁收银
包名: com.dcits.myapplication
主活动**Activity:** com.dcits.myapplication.ui.main.MainWebView
安卓版本名称: 1.0.3
安卓版本: 3

# 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.dcits.myapplication.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.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_BACKGROUND_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.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.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_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 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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 |

# 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=新疆, L=哈密市, O=哈密市商业银行, OU=哈密市商业银行, CN=哈密市商业银行
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-17 02:19:24+00:00
Valid To: 2046-12-11 02:19:24+00:00
Issuer: C=86, ST=新疆, L=哈密市, O=哈密市商业银行, OU=哈密市商业银行, CN=哈密市商业银行
Serial Number: 0x5c8ccf52

Hash Algorithm: sha256
md5: 5a0462a1f8b8844d5734d9e5dca09922
sha1: 5b17af1d51459df4276bee3e86b93d136dacbbc9
sha256: 48eec14b5350be02bbc21fd9bb9c02de952d3445e2b5d741e334c29086e88b46
sha512: e87f9ea0f634cf53782ae925ed9b007391e7034b25277ee9b76c031db298276cbb6621a6cf8c8a1505492b4dd2d0c984454eae3b966a6c36640a987b16c78522
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 25011606e39c736eba2bdd11e66777be9343d02c49205488933e6e46ae7f931b

# 加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>Ijiami</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/libijm-emulator.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>UPX (unknown, modified)</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libijm-emulator.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>UPX (unknown, modified)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/libijmDataEncryption.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>UPX (unknown, modified)</td></tr>
</table>
</td></tr>
<tr><td>assets/ijm_lib/armeabi/libexecmain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>UPX (unknown, modified)</td></tr>
</table>
</td></tr>
<tr><td>assets/ijm_lib/armeabi/libexec.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>UPX (unknown, modified)</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

---