MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

小心窝 1.0.1.APK

APP名称:	小心窝
包名:	com.zhacai.clone
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年1月29日 00:17

文件信息

文件名: xiaoxinwo.apk
文件大小: 1.7MB
MD5值: 68a9199e476058ac1ae5fce5f7bba7f7
SHA1值: 40cb045dd1a96c56b8384c4ad42a951c2afec99c
SHA256值: 13916ffbc9f0edac31ba217db48af4705df916b61207b1264a7d25ba908daa9a

APP 信息

App名称: 小心窝
包名: com.zhacai.clone
主活动**Activity:** com.androlua.Welcome
安卓版本名称: 1.0.1
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
pic.sogou.com	good	**IP:** 49.7.21.42 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://pic.sogou.com/pic/ris_searchList.jsp?statref=home&v=5&keyword=	com/androlua/MyWebView.java

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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

签名证书

APK is signed
v1 signature: True
v2 signature: False

v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.androlua.Main	Schemes: file://, Hosts: *, Path Patterns: .*fas,

加壳分析

文件列表	分析结果
classes.dex	壳列表 | 详细情况 编译器 | dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes10.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes11.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes12.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes2.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes3.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes4.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes5.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes6.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr><tr><td>模糊器</td><td>unreadable method names</td></tr></table></td></tr>
<tr><td>classes7.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes8.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
