MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

海棠线上文学城 1.0.13.APK

APP名称:	海棠线上文学城
包名:	com.leyian.akk
域名线索:	13条
URL线索:	2条
邮箱线索:	0条
分析日期:	2022年2月4日 11:13

文件信息

文件名: haitang.apk

文件大小: 17.85MB
MD5值: 3cf7ee888ccd88c9ab054f2c0e4fb739
SHA1值: 771582574a40c2009f2ba24a56cbe1a23cf166fa
SHA256值: 21d481604dd67dfde5244320b0bc5bae3050d66ded4919977cb8da0f906a0614

APP 信息

App名称: 海棠线上文学城
包名: com.leyian.akk
主活动**Activity:** com.hcd.fantasyhouse.ui.welcome.WelcomeActivity
安卓版本名称: 1.0.13
安卓版本: 14

域名线索

域名	是否危险域名	服务器信息
alanskycn.gitee.io	good	**IP:** 212.64.62.183 **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
t.me	good	**IP:** 149.154.167.99 **所属国家:** United Kingdom of Great Britain and Northern Ireland **地区:** England **城市:** Lowestoft **纬度:** 52.475201 **经度:** 1.751590 **查看地图:** Google Map

域名	是否危险域名	服务器信息
play.google.com	good	**IP:** 172.217.160.110 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
m.so.com	good	**IP:** 101.198.191.56 **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
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
gedoor.github.io	good	**IP:** 185.199.108.153 **所属国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.baidu.com	good	**IP:** 110.242.68.3 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map
store.hispace.hicloud.com	good	**IP:** 49.4.18.123 **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
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
api.github.com	good	**IP:** 20.205.243.168 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.coolapk.com	good	**IP:** 121.51.175.120 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
www.sogou.com	good	**IP:** 211.159.235.175 **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
m.sm.cn	good	**IP:** 59.82.31.200 **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
https://play.google.com/store/apps/details?id=io.legado.play.release	Android String Resource
https://www.baidu.com/s?wd=%1$s	Android String Resource

URL信息	Url所在文件
https://github.com/gedoor/legado/graphs/contributors	Android String Resource
https://gedoor.github.io/MyBookshelf/disclaimer.html	Android String Resource
https://m.so.com/index.php?q=%1$s	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://gedoor.github.io/MyBookshelf/	Android String Resource
http://%1$s:%2$d	Android String Resource
https://api.github.com/repos/gedoor/legado/releases/latest	Android String Resource
https://github.com/gedoor/legado/releases/latest	Android String Resource
https://m.sm.cn/s?q=%1$s	Android String Resource
https://www.sogou.com/web?query=%1$s	Android String Resource
https://alanskycn.gitee.io/teachme/	Android String Resource
https://t.me/yueduguanfang	Android String Resource
https://github.com/gedoor/legado	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
https://www.coolapk.com/apk/256030	Android String Resource

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.MANAGE_DOCUMENTS	合法		允许应用程序管理对文档的访问,通常作为文档选择器的一部分
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.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_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
com.vivo.notification.permission.BADGE_ICON	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.leyian.akk.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.leyian.akk.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.leyian.akk.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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
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
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
com.leyian.akk.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.leyian.akk.permission.KW_SDK_BROADCAST	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates

Subject: C=86, ST=guangdong, L=shenzhen, O=nanshan, CN=akaka
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-21 02:03:25+00:00
Valid To: 2046-06-15 02:03:25+00:00
Issuer: C=86, ST=guangdong, L=shenzhen, O=nanshan, CN=akaka
Serial Number: 0x2ea66b07
Hash Algorithm: sha256
md5: fd815903b7027f5997fc0e733f31e44d
sha1: d27ef2fff14a7805ef12863200209da75d9ecd0f
sha256: 5325b7bfa72f809eddbc8c672f294e14372c081a42adc0d3fd336966db75a0a6
sha512: e9303fd82cc87fe7179865a0052d72537d256fb25311ccb7563b50e1ec60382cb6a4b9a8276d6dd6c9dbce652a1c17ba1aaa3b88e15841a5d2b673705d1789c1
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: dcdfa8022edd008182d550b9454a70841e211910fc1fa90afb866b26080a13d8

硬编码敏感信息

可能的敏感信息
"custom_page_key" : "Set page-turning buttons"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"latest_release_api" : "https://api.github.com/repos/gedoor/legado/releases/latest"
"next_page_key" : "Page down button"
"page_key_set_help" : "将焦点放到输入框按下物理按键会自动录入键值,多个按键会自动用英文逗号隔开."
"prev_page_key" : "Page up button"
"r_author" : "作者规则(author)"

可能的敏感信息
"search_book_key" : "Search book name/author"
"volume_key_page" : "Volume keys to turn page"
"volume_key_page_on_play" : "Volume keys to turn page when reading"
"custom_page_key" : "自定义翻页按键"
"next_page_key" : "下一页按键"
"page_key_set_help" : "将焦点放到输入框按下物理按键会自动录入键值,多个按键会自动用英文逗号隔开."
"prev_page_key" : "上一页按键"
"r_author" : "作者规则(author)"
"search_book_key" : "搜索书名、作者"
"volume_key_page" : "音量键翻页"
"volume_key_page_on_play" : "朗读时音量键翻页"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.hcd.fantasyhouse.ui.association.ImportBookSourceActivity	Schemes: yuedu://, Hosts: booksource,

活动(ACTIVITY)	通信(INTENT)
com.hcd.fantasyhouse.ui.association.ImportRssSourceActivity	Schemes: yuedu://, Hosts: rsssource,
com.hcd.fantasyhouse.ui.association.ImportReplaceRuleActivity	Schemes: yuedu://, Hosts: replace,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Jiagu
assets/gdt_plugin/gdtadv2.jar!assets/yaq3_0.sec	壳列表 / 详细情况 反虚拟机 / Build.MODEL check 编译器 / dexlib 2.x

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
classes.dex	壳列表 | 详细情况 编译器 | dexlib 2.x
