MoGua

哔咔漫画 1.3.2.APK 分析报告

APP名称:	哔咔漫画

包名:	com.comics.bika
域名线索:	3条
URL线索:	3条
邮箱线索:	3条
分析日期:	2024年9月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 112222.apk
文件大小: 40.59MB
MD5值: 9b6792fcfb132845e9aef6c5d9ca5766
SHA1值: e6a6809f85ee69f0c1c38afa0fe6e28a5e504109
SHA256值: 8b83e16597ad88c1f010a15530554e0d0bb736b0db72f622db6d94b2e3dd63ce

APP 信息

App名称: 哔咔漫画
包名: com.comics.bika
主活动Activity: com.comics.bika.ui.activity.launch.SplashActivity
安卓版本名称: 1.3.2
安卓版本: 18

域名线索

域名	服务器信息
errlogos.umeng.com	**IP**: 47.246.110.18 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
errlog.umeng.com	**IP**: 223.109.148.180 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.openssl.org	**IP**: 104.71.138.221 **所属国家**: Japan **地区**: Tokyo

	城市: Tokyo **纬度**: 35.689507 **经度**: 139.691696

URL线索

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi/libijkffmpeg.so
http://www.openssl.org/support/faq.html	lib/x86/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi/libijkplayer.so
o@netstream.failed	lib/x86/librtmp-jni.so
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so

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=fj, L=xm, O=bk, OU=bk, CN=bk
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-12 02:30:21+00:00
有效期至: 2046-07-06 02:30:21+00:00
发行人: C=cn, ST=fj, L=xm, O=bk, OU=bk, CN=bk
序列号: 0x3055300f
哈希算法: sha256
md5值: 8748ca738f076f95f2e0dcf08d91cc62
sha1值: 63c17d24c3266b46fa85c371e456138d5edc6731
sha256值: ebde88045bb65451eab576de6638a9134278378c3681c57449bfe32dcf35560e
sha512值: 3695b6b69fb0413e05afefe266c3804c560af468516d56b7eae81c64dc8fad1bc09d5e5f1a1b555621b682214b9d77f749e8ab7a3ed957851d4e20893b70feb0
公钥算法: rsa
密钥长度: 2048
指纹: 7ca0abddd13ab435d3eca0b8a2cf3d5ce884c8e1ef3786d8b39853082e1bb1f5

硬编码敏感信息

可能的敏感信息
"again_sure_pwd" : "重新输入密码"
"input_pwd" : "请输入密码"
"intput_pwd" : "请输入密码"

"please_sure_pwd" : "请输入确认密码"
"set_pwd" : "设置密码"
"set_pwd_tip" : "启动青少年模式，需先设置独立密码"
"sure_pwd" : "确认密码"

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

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.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.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
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.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.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.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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.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.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
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
com.comics.bika.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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1111979765://,

---