



MoGua

51漫画 3.01.APK 分析报告



APP名称:

51漫画

包名:	com.qnmd.a51mh.vz022p
域名线索:	14条
URL线索:	15条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ozcll1mh_1.apk

文件大小: 23.61MB

MD5值: 5254414a57b3225d926be42451cc8c98

SHA1值: 32dc7947ac26b993824b2656d58f0ec43815ba00
SHA256值: 4363dcc9f293775ce45f696e9037ebad5d55c6427caf4fa768ac806c2cecf0b1

i APP 信息

App名称: 51漫画
包名: com.qnmd.a51mh.vz022p
主活动Activity: com.jbzd.media.movecartoons.ui.splash.SplashActivity
安卓版本名称: 3.01
安卓版本: 301

🔍 域名线索

域名	服务器信息
playready.directtaps.net	IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
schemas.microsoft.com	IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 3.173.254.43

api.hfzill9tvkl01.com	所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
api.kkq5r8h53cbw8.com	IP: 3.173.254.43 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
dashif.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
schemas.android.com	没有服务器地理信息.
api.ak32jnnfh8qde.com	IP: 3.173.254.43 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
api.telegram.org	IP: 157.240.10.41 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604
api.vbsyvufjtj029c.com	IP: 3.164.121.93 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
api.z8apru15xg0sv.com	IP: 3.173.254.32 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
api.ly3ccp3g40n9a.com	IP: 3.164.121.93 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199

URL线索

URL信息	Url所在文件
https://api.telegram.org/bot6086117813:AAFwiL2Rn_qZbWa_a6DkegGeAx1glJorQzA/sendMessage	b/a/a/a/h.java
http://api.ly3ccp3g40n9a.com/mhapi/	b/a/a/a/r/i.java

http://api.vbsyvufjtj029c.com/mhapi/	b/a/a/a/r/i.java
http://api.hfzill9tvkl01.com/mhapi/	b/a/a/a/r/i.java
http://api.kkq5r8h53cbw8.com/mhapi/	b/a/a/a/r/i.java
http://api.ak32jnnfh8qde.com/mhapi/	b/a/a/a/r/i.java
http://api.z8apru15xg0sv.com/mhapi/	b/a/a/a/r/i.java
http://api.hfzill9tvkl01.com/mhapi/	b/a/a/a/r/m/c.java
https://github.com/danikula/AndroidVideoCache/issues/88.	b/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	b/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	b/f/a/i.java
http://%s:%d/%s	b/f/a/l.java
http://%s:%d/%s	b/f/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134.	b/f/a/g.java
http://dashif.org/guidelines/last-segment-number	b/j/a/a/k1/l0/k/c.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/jbzd/media/movecartoons/view/ImageTabLayout.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	g/b/a/c/b.java

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	g/b/a/c/d.java
http://xml.apache.org/xslt	d/a/a/b/a/m.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	b/f/a/i.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-27 20:00:02+00:00
有效期至: 2052-03-14 20:00:02+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
 序列号: 0x1af025ed
 哈希算法: sha256
 md5值: 2a08ebd2d353a9ca914f67fb0e8036eb
 sha1值: cd642261119703f93d2ca1d6711ed743a4176e63
 sha256值: b86776f59ed58f0b28aa4d1058de57ef56570f10ca1903cdd4b6389185511a7e
 sha512值: 7acb41abc8b1576e096e3d0c7ee5b082eac15805b3562c390eb79c5a88b633e99403cd40867ddb9c2c68d38c8ee1da3001f92afdcf0c9e9a92698cc663f470e9
 公钥算法: rsa
 密钥长度: 2048
 指纹: 4ea95d7ab9612f96ade3a818fb925ae3cba633815d40c0fc43c0b46b0dd629f3

🔑 硬编码敏感信息

可能的敏感信息
"account_certificate" : "账号凭证"
"account_credentials" : "账号凭证"
"credentials_notice_tips" : "1. 请您保存二维码凭证，以便找回您的账号 2. 请妥善保管此账号凭证，不要随意透露给任何人 3. 若此账号不慎丢失，可通过app账号安全扫取该二维码凭证账号登录"
"credentials_tips" : "请到设置—找回账号—账号凭证找回或者扫描凭证"
"merchant_credentials_tips" : "支付小贴士： 1、跳转后请及时付款，超时支付，重复扫码，修改金额均无法到账。 2、付款后没有到账，请保存好付款截图，联系在线客服处理。 3、支付通道在夜间比较忙碌，为保证您的付款体验，您可以尽量选择白天支付，晚上观看，谢谢您的理解。"
"mine_account_credentials" : "账号凭证"
"scan_credentials" : "扫描二维码"
"upload_credentials" : "从相册选择"

🛡️ 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.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.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_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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_PRIVILEGED_PHONE_STATE	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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信