MoGua

君盛 9.APK 分析报告

APP名称:	君盛

包名:	vxxt.hxexg.eppkoispua.ecxmgfzryi
域名线索:	13条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年7月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 3.2MB
MD5值: b5e4355f796363492acd25607bab2d3c
SHA1值: c95e0f41da29c954641c4fa63c09441fece54ee9
SHA256值: a1c6f10cd39a66faeb3eb591a86d8dd65145ff3b3e48607b69bca6887d89f22d

APP 信息

App名称: 君盛
包名: vxxt.hxexg.eppkoispua.ecxmgfzryi
主活动Activity: com.k70369.webviewtest.SplashActivity
安卓版本名称: 9
安卓版本: 1

域名线索

域名	服务器信息
cn-hongkong.log.aliyuncs.com	**IP**: 47.244.67.194 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
cfg.imtt.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
tbs.imtt.qq.com	**IP**: 211.97.84.73 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
youtrack.jetbrains.com	IP: 63.33.88.220 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
mdc.html5.qq.com	IP: 125.39.196.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
goo.gle	IP: 67.199.248.12 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009
gitee.com	IP: 180.76.199.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
android.googlesource.com	IP: 108.177.98.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

pms.mb.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.bilibili.com	**IP**: 218.60.18.18 **所属国家**: China **地区**: Liaoning **城市**: Fuxin **纬度**: 42.015911 **经度**: 121.658890
log.tbs.qq.com	**IP**: 124.95.224.248 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL信息	Url所在文件
https://debugtbs.qq.com?10000	摸瓜V3引擎
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	摸瓜V3引擎
https://www.bilibili.com/video/BV1qmrfYgEDE	摸瓜V3引擎
https://log.tbs.qq.com/ajax?c=ul&v=2&k=:https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079/h	摸瓜V3引擎
https://cn-hongkong.log.aliyuncs.com	摸瓜V3引擎
https://pms.mb.qq.com/rsp2041https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	摸瓜V3引擎
https://log.tbs.qq.com/ajax?c=pu&tk=	摸瓜V3引擎
https://gitee.com/wangjingdi88767	摸瓜V3引擎
https://debugx5.qq.com	摸瓜V3引擎
https://pms.mb.qq.com/rsp204	摸瓜V3引擎
https://youtrack.jetbrains.com/issue/KT-55980	摸瓜V3引擎
https://gitee.com/annabelle74100	摸瓜V3引擎
https://cfg.imtt.qq.com/tbs?v=2&mk=	摸瓜V3引擎
https://gitee.com/wangjingdi88767#https://log.tbs.qq.com/ajax?c=dl&k=$https://log.tbs.qq.com/ajax?c=	摸瓜V3引擎
https://log.tbs.qq.com/ajax?c=dl&k=	摸瓜V3引擎
https://www.bilibili.com/video/BV1RbUGYHE8u	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎

http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://mdc.html5.qq.com/mh?channel_id=50079&u=	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://debugtbs.qq.com	摸瓜V3引擎
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	摸瓜V3引擎
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	摸瓜V3引擎
https://youtrack.jetbrains.com/issue/KT-46465	摸瓜V3引擎
https://goo.gle/compose-feedback	摸瓜V3引擎
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	摸瓜V3引擎

邮箱线索

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=(), ST=(), L=(), O=

(), OU=(), CN=()
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-27 12:20:20+00:00
有效期至: 2026-02-27 12:20:20+00:00
发行人: C=(), ST=(), L=(), O=(), OU=(), CN=()
序列号: 0x7cbd266d
哈希算法: sha256
md5值: 3b31896b63dc3ff0c04946b6fc8b41f7
sha1值: 4410463839728253c6202b367f2aa1de305da0e8
sha256值: f9e48423bd0e896f3f12a2c7a30e89ef29a8186c401a64d621c7245406179038
sha512值: 758c3dbcdda328a4de0564e3b9c00cbad7a9f9d4c91ce51c3f523a358445cf7a818db1a16f603d586d41a604912b70dda5871964c1e0db9caaecdf3daa2c3732
公钥算法: rsa
密钥长度: 1024
指纹: 64795d5430dba73fb41c6e84656929c81043f498b080c011c9431667ebdf5be3

硬编码敏感信息

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.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.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.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用
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
vxxt.hxexg.eppkoispua.ecxmgfzryi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

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.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

应用内通信
