



MoGua

GC 2000 GC 2000-V01A-009.APK 分析报告



APP名称:

GC 2000

包名:	com.puyu.mobile.gc2000
域名线索:	2条
URL线索:	14条
邮箱线索:	0条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件名: GC_2000_GC_2000-V01A-009.apk

文件大小: 10.23MB

MD5值: 285e1d927ac2833cfc63ade500164123

SHA1值: 6bfe808404eb63c42f0ef614f84a4e11806071fe

SHA256值: 4a702928be381e178a75a1b092b06f4875233a89e104318c1c356e1c543da34a

i APP 信息

App名称: GC 2000

包名: com.puyu.mobile.gc2000

主活动Activity: com.puyu.mobile.gc2000.act.MainActivity

安卓版本名称: GC 2000-V01A-009

安卓版本: 29

🔍 域名线索

域名	服务器信息
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
objectbox.io	IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770

🌐 URL线索

URL信息	Url所在文件
https://objectbox.io/sync/	io/objectbox/sync/SyncBuilder.java
https://objectbox.io/sync/	io/objectbox/sync/server/SyncServerBuilder.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://objectbox.io/sync/	lib/arm64-v8a/libobjectbox-jni.so
https://objectbox.io/sync/	lib/armeabi-v7a/libobjectbox-jni.so
https://objectbox.io/sync/	lib/x86/libobjectbox-jni.so
https://objectbox.io/sync/	lib/x86_64/libobjectbox-jni.so

 邮箱线索

 手机线索

手机号	所在文件
17179869184	com/puyu/mobile/gc2000/databinding/FragHomeChannelBindingImpl.java
17179869184	com/puyu/mobile/gc2000/databinding/FragChanel2BindingImpl.java
17179869184	com/puyu/mobile/gc2000/databinding/FragChanel1BindingImpl.java
17179869184	com/puyu/mobile/gc2000/databinding/FragChanelConfigBindingImpl.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=CN, ST=Shanghai, L=Shanghai, O=Lztek, OU=TeamHD, CN=Liaokai, E=lk@lztek.cn

签名算法: rsassa_pkcs1v15

有效期自: 2018-09-06 01:20:22+00:00

有效期至: 2046-01-22 01:20:22+00:00

发行人: C=CN, ST=Shanghai, L=Shanghai, O=Lztek, OU=TeamHD, CN=Liaokai, E=lk@lztek.cn

序列号: 0x96bb23ac0c1e1a01

哈希算法: sha256

md5值: d35071d643dfb9631271ef4bf927cfae

sha1值: 5fbb393493c8c39d47adb16c1d1d8133487a1efa

sha256值: c40e70fcdf6b612ee4e3809663ea3820d52855c2ea59d49fdf560583c0af68ed

sha512值: 277bd4ed866a34c4f6e40e9cda911fdb645e46cc68fd0c92ec5aca6d8e3b5ff979af4c23d026fe666f069bebf039fdc1363cb2c06b7da3b0e630d32e55b47e06

公钥算法: rsa

密钥长度: 2048

指纹: 3e25a6ba71a4c88a381ca69d5951b144d4391a51045d006c5ccd28ae4d611cce

🔑 硬编码敏感信息

可能的敏感信息

"external_storage_has_been_authorized" : "外置存储已经授权"

"external_storage_has_been_authorized" : "External storage has been authorized"

"external_storage_has_been_authorized" : "Внешний диск авторизован"

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.REBOOT	系统需要	强制手机重启	允许应用强制手机重启

	--		
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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

应用内通信