



MoGua

国联尊宝 1.0.APK 分析报告



APP名称:

国联尊宝

包名: ugRjEhs.mjuhTioGkrvj9.ivUkdoYj6t

域名线索: 11条

URL线索: 9条

邮箱线索: 0条

分析日期: 2025年6月15日

分析平台: [摸瓜APK反编译平台](#)

文件名: glzbdbd_064116.apk
文件大小: 14.1MB
MD5值: f54a727032b81c19c2e3b307ddeeff6e
SHA1值: aa49628527785caa6bae802784ff8d766c94180e
SHA256值: 3dd7a21e2bd6e4d356c60bf350255b8c229868b1572513a858ef80d57be4714a

i APP 信息

App名称: 国联尊宝
包名: uGRjEhs.mjuhTioGkrvj9.ivUkdoYj6t
主活动Activity: cn.helaoliu.musicplayer.activity.LoginActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
freemarket.org	IP: 192.64.119.217 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.727291 经度: -84.425377
bndush.gz.bcebos.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
greenrobot.org	IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770
mdfgy.gz.bcebos.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
jfignj.gz.bcebos.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

freemarker.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
www.eclipse.org	IP: 198.41.30.198 所属国家: Canada 地区: Ontario 城市: Brampton 纬度: 43.702347 经度: -79.711548
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

 URL线索

URL信息	Url所在文件
https://bndush.gz.bcebos.com/Rbmszq0424.json	cn/helaoliu/musicplayer/activity/LoginActivity.java
https://jfignj.gz.bcebos.com/Rbmszq0424.json	cn/helaoliu/musicplayer/activity/LoginActivity.java
https://mdfgy.gz.bcebos.com/Rbmszq0424.json	cn/helaoliu/musicplayer/activity/LoginActivity.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://freemarker.apache.org/docs/ref_builtins.html;	freemarker/core/BuiltIn.java

http://freemarker.org/docs/ref_directive_list.html).	freemarker/core/FMParserTokenManager.java
http://freemarker.org/docs/ref_directive_alphaidx.html ;	freemarker/core/FMParserTokenManager.java
http://xml.org/sax/properties/lexical-handler	org/greenrobot/eclipse/core/internal/content/XMLRootHandler.java
http://xml.org/sax/features/validation	org/greenrobot/eclipse/core/internal/content/XMLRootHandler.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	org/greenrobot/eclipse/core/internal/content/XMLRootHandler.java
http://xml.org/sax/features/string-interning	org/greenrobot/eclipse/core/internal/registry/ExtensionsParser.java
http://xml.org/sax/features/string-interning	org/greenrobot/eclipse/core/internal/resources/ProjectDescriptionReader.java
http://www.eclipse.org/jdt/core/compiler_32_006.dtd \	org/greenrobot/eclipse/jdt/internal/compiler/batch/Main.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java

 邮箱线索

 手机线索

手机号	所在文件
17179869185	freemarker/core/FMParserTokenManager.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/ast/ASTNode.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/lookup/TagBits.java

17179869184	org/greenrobot/eclipse/jdt/internal/compiler/lookup/PackageBinding.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/lookup/SourceModuleBinding.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/lookup/SourceTypeBinding.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/lookup/MemberTypeBinding.java
17179869184	org/greenrobot/eclipse/jdt/internal/compiler/parser/ScannerHelper.java

🌸 签名证书

APK已签名

v1 签名: False

v2 签名: True

v3 签名: False

找到 1 个唯一证书

主题: C=ustobivqedtjw, ST=rsiygeqwlrvwh, L=kjhnwvqpfyksa, O=ngs1747660944747, OU=rej1747660944747, CN=TG@apkfangujiagu

签名算法: rsassa_pkcs1v15

有效期自: 2025-05-19 13:22:24+00:00

有效期至: 2075-05-07 13:22:24+00:00

发行人: C=ustobivqedtjw, ST=rsiygeqwlrvwh, L=kjhnwvqpfyksa, O=ngs1747660944747, OU=rej1747660944747, CN=TG@apkfangujiagu

序列号: 0x238c999e

哈希算法: sha1

md5值: f27eec2b682459588b8049b101752522

sha1值: 2cf6adb7020c74dc9034de56fda8c0b6630a5b45

sha256值: 5596d231fda8e2ad15f8488ce44a746dddf2ab33ab407278e57fae0a655ca90f

sha512值: 6f730dc8b31a65385ee2f06b9c879ace52d1874fc27e913dfbe42632e1e0b0dbda2983ad153c18da38836d48c57693a77cabcfdd9049cb98a5c9df88013575e3

公钥算法: rsa

密钥长度: 1024

指纹: 9b678f3f037fa8a7dc1423d6602118359ae3325d8f4f57fab8c8451df0c75713

🔑 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.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_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.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.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
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.NETWORK_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference

应用内通信