MoGua

两新国补 1.0.0.APK 分析报告

APP名称:	两新国补

包名:	com.ansiag.lxgbapp1
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 两新国补.apk
文件大小: 5.52MB
MD5值: d3b09f04c867d197dc383c895ad0eb49
SHA1值: 92e09d53f4390af8302e4056147fa0b4a0cd5756
SHA256值: 16637d724dbe3ab4e96d96e3944a8b804e05d940db55d654260b76e70c7eccbd

APP 信息

App名称: 两新国补
包名: com.ansiag.lxgbapp1
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	服务器信息
1.12.12.12	**IP**: 1.12.12.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.baidu.com	**IP**: 110.242.70.57 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
dns.alidns.com	**IP**: 223.5.5.5 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
https://dns.alidns.com/dns-query	m3/r.java
https://1.12.12.12/dns-query	m3/r.java
https://www.baidu.com/favicon.ico?\	l3/h1.java

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: False
找到 1 个唯一证书
主题: C=CN, O=COM, OU=IT, CN=VVWM
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-09 03:10:11+00:00
有效期至: 2125-05-16 03:10:11+00:00
发行人: C=CN, O=COM, OU=IT, CN=VVWM

序列号: 0x7672bdcf
哈希算法: sha256
md5值: 2b6409c5c99da4ff8c5411759ee22697
sha1值: bf6b70de2e9b52e314aa3b1390a738d7a0053f37
sha256值: ab5d0b693c14e4bb9f21a9e2ea2c9dd6b04097016c282923eee7d3c7211ca796
sha512值: 627d4f6c2562d38ab8008fe802c6e965a81947a6d3fdbf899de6a77d519052958e26d24cfcd02d8d484b52cbf1c219f8602c523c8775fbe5a43671b93398982e
公钥算法: rsa
密钥长度: 2048
指纹: f1d56f64c08b45674d6760c1895317e738b6a044fd5b6a8257bba61f15700669

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	类型	详细情况

	危险		
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。
com.ansiag.lxgbapp1.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
com.ansiag.lxgbapp1.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp459778://,
