MoGua

华,泰资本 1.0.4.APK 分析报告

APP名称: 华,泰资本

包名:	x237.x232.x39.x103
域名线索:	4条
URL线索:	3条
邮箱线索:	0条
分析日期:	2024年9月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app (1).apk
文件大小: 3.36MB
MD5值: 9ed5f2a7b93144687a3e5ecebf80eb82
SHA1值: d870e1c009c114e48884261757089925d597d397
SHA256值: f6ce4d9c7c5d8cbef066f38f0338e5032c581387a53eacb0751bdcd5efc374f9

APP 信息

App名称: 华,泰资本
包名: x237.x232.x39.x103
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 1.0.4
安卓版本: 104

域名线索

域名	服务器信息
www.baidu.com	**IP**: 110.242.68.4 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
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
schemas.android.com	没有服务器地理信息.
	IP: 223.6.6.6

dns.alidns.com	IP: 223.6.6.6 **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	com/lt/plugin/d0.java
https://1.12.12.12/dns-query	com/lt/plugin/d0.java
https://www.baidu.com/favicon.ico?\	com/lt/app/views/o0.java
http://schemas.android.com/apk/res/android	f/g/d/f/k.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=DBEV
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-29 07:00:42+00:00
有效期至: 2124-04-05 07:00:42+00:00
发行人: C=CN, O=COM, OU=IT, CN=DBEV
序列号: 0x6491d77a
哈希算法: sha256
md5值: 54b2fd1471a8f807eebd9e0b26f7491c
sha1值: a68ffe6464643e9c278956b00b13a7285b210ab9
sha256值: 557aeff2aa6cd7f73c87e6cd03609a2d0ca8b16194a4a3d379d3741448949823
sha512值: 610698b1d7565844d87000287bf6c7d80774f59e32c915884c4c443a70543f25eb8244aabec1d3c55052ad125b3fc1585b48fc7cdc377807e5075c678d5522ba
公钥算法: rsa
密钥长度: 2048
指纹: 326e3dd592647820f9ba12a897afda8c31da429fa6b7438714520504673d36d6

🔑 硬编码敏感信息

可能的敏感信息
"http_auth" : "HTTP Authentication"
"http_auth_p" : "Password"
"http_auth_u" : "User Name"
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""
"p_rcpush_xmAppKey" : ""
"p_weibo_appkey" : ""

p_weibo_appkey" :
"http_auth" : "HTTP 身份驗證"
"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"
"http_auth" : "HTTP 身份驗證"
"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"
"http_auth" : "HTTP 身份验证"
"http_auth_p" : "密码"
"http_auth_u" : "用户名"

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**

登陆搜瓜网站后查看		

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.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。
x237.x232.x39.x103.permission.YM_APP	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
android.permission.READ_MEDIA_IMAGES	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.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp411664://,
