MoGua

AdLocus APP-Android 1.0.APK 分析报告

APP名称: AdLocus APP-Android

包名:	com.example.adlocusapp_android
域名线索:	5条
URL线索:	15条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: AdLocus_150116.apk
文件大小: 0.49MB
MD5值: af81f18b6ef9b6c029b0d81a37570ecf
SHA1值: c97e3e7a021d738dd58985cc9a63bd4cf3b3f4d2
SHA256值: 66546203c420c0b5677c3ffb243bf4d7e23f9ef432d2d2cb85dc2c5f6b16ef58

APP 信息

App名称: AdLocus APP-Android
包名: com.example.adlocusapp_android
主活动Activity: com.example.adlocusapp_android.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
api.ad-locus.com	**IP**: 35.77.139.149 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
ad-locus.com	**IP**: 18.178.225.229 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
emaico.rd.hyxencloud.com	没有服务器地理信息.
	IP: 54.64.220.126

a.api.ad-locus.com	**所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
user.ad-locus.com	**IP**: 54.64.220.126 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

URL线索

URL信息	Url所在文件
http://a.api.ad-locus.com/dev_html5/req?	com/adlocus/InterstitialAd.java
http://a.api.ad-locus.com/dev/auth	com/adlocus/n.java
http://a.api.ad-locus.com/dev_html5/req	com/adlocus/n.java
http://a.api.ad-locus.com/dev_html5/req?	com/adlocus/InterstitialVideoAd.java
http://a.api.ad-locus.com/devpush/newimp	com/adlocus/h.java
http://a.api.ad-locus.com/dev_html5/req	com/adlocus/af.java
http://user.ad-locus.com/pref/set?device_id=%s&app_key=%s	com/adlocus/PushAd.java
http://a.api.ad-locus.com/dev_html5/req	com/adlocus/t.java
http://a.api.ad-locus.com/dev_html5/req?	com/adlocus/am.java

http://a.api.ad-locus.com/	com/adlocus/e/c.java
http://a.api.ad-locus.com/devpush/req	com/adlocus/push/m.java
http://a.api.ad-locus.com/devpush/get_json_link	com/adlocus/push/aa.java
http://a.api.ad-locus.com/devpush/get_json_link\n	com/adlocus/push/aa.java
http://a.api.ad-locus.com/devpush/get_json_link	com/adlocus/push/a.java
http://a.api.ad-locus.com/devpush/get_json_link\n	com/adlocus/push/a.java
http://a.api.ad-locus.com/devpush/imp	com/adlocus/push/u.java
http://ad-locus.com	com/adlocus/push/PushService.java
http://emaico.rd.hyxencloud.com/fullad/300x250-02.gif	com/adlocus/push/PushService.java
http://api.ad-locus.com/	com/adlocus/adapters/d.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False

找到 1 个唯一证书
主题: C=TW, ST=Taiwan, L=Taipei, O=HyXen, OU=HyXen, CN=HyXen
签名算法: rsassa_pkcs1v15
有效期自: 2010-05-24 06:25:11+00:00
有效期至: 2065-02-24 06:25:11+00:00
发行人: C=TW, ST=Taiwan, L=Taipei, O=HyXen, OU=HyXen, CN=HyXen
序列号: 0x4bfa1bc7
哈希算法: sha1
md5值: b3511cca07d51c26d111cafc33cb276c
sha1值: 0c05702f061505481373d32507e55a9008181acb
sha256值: 6e2fccf1d19202a97f06ec400db4d4da3b1e54e8caa435f2231cfc924d636379
sha512值: bbfdb94ceafebfbc355ad533d85a718f4f4f52efdc46436029c0e4ac8da29f2c70693c93b0a9fb721ffa774908eabfc9453f5f5b767ebeb53e667f4f8593a159fb

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.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.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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
com.adlocus.permission.SEND	未知	Unknown permission	Unknown permission from android reference

应用内通信