MoGua

AdLocus_BV-Video 1.0.APK 分析报告

BV-Video

APP名称:	AdLocus_BV-Video

包名:	com.example.adlocus_bv_video
域名线索:	5条
URL线索:	5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_BV-Video.apk
文件大小: 1.05MB
MD5值: 79f6775d0488887f248739e69f808a7f
SHA1值: 3f4aba1462f42399619b007629d659d4be6acb47
SHA256值: 3177eb76921aee1bacae4ea6f55658e1e1e719b78fdaa077cbc658f590b601aa13

APP 信息

App名称: AdLocus_BV-Video
包名: com.example.adlocus_bv_video
主活动Activity: .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
emaico.rd.hyxencloud.com	没有服务器地理信息.
hyxen-adlocus-api.rd.hyxencloud.com	**IP**: 172.232.31.180 **所属国家**: United States of America **地区**: Illinois **城市**: Chicago **纬度**: 41.875771 **经度**: -87.620605
www.google.com.tw	**IP**: 157.240.17.35 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790

a.api.ad-locus.com	**IP**: 54.65.30.147 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
www.youtube.com	**IP**: 31.13.68.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249

URL线索

URL信息	Url所在文件
http://a.api.ad-locus.com/	com/example/adlocus_bv_video/AdLocusUtil.java
http://hyxen-adlocus-api.rd.hyxencloud.com/	com/example/adlocus_bv_video/AdLocusUtil.java
http://emaico.rd.hyxencloud.com/uiview/maggie/Adlocus_PR.jpg	com/example/adlocus_bv_video/LandingPageActivity.java
http://www.google.com.tw	com/example/adlocus_bv_video/VideoAdActivity.java
http://www.google.com.tw	com/example/adlocus_bv_video/InterstitialVideoAd.java
https://www.youtube.com/embed/I8sjF40Gb8g\	com/example/adlocus_bv_video/MainActivity.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=US, O=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2015-06-15 10:22:44+00:00
有效期至: 2045-06-07 10:22:44+00:00
发行人: C=US, O=Android, CN=Android Debug
序列号: 0x3c5d91d6
哈希算法: sha256
md5值: 0b637ff8da1fb5d501859d85721ccaf4
sha1值: 0176cb464a6a1af69d4686323f2ab41023528651
sha256值: f6311a9b790442dd20abcad86feef961bc87a7c753630da9d9cac77fe7756b30
sha512值: d87a32494eedcd27b789aa16a52cf4dca73bdc46063cdaa090c69178ad5f29487b91b55c3a419e7c83eb8a6e758d49a963ff7e0fe83248d614c42ddfb41b5640

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

应用内通信
