MoGua

浪鲸下载器 1.0.1.APK 分析报告

APP名称:	浪鲸下载器

包名:	com.langjing.downloader
域名线索:	10条
URL线索:	5条
邮箱线索:	2条
分析日期:	2025年7月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 12.21MB
MD5值: 444ce3b63ddae41c6767e051abfefe99
SHA1值: e91d2de9446b6ee537346fe2bade45c75670c946
SHA256值: d21d6dfd2892bb19fd7163824349d33e8f14eabca1638ca2abd405f4eadbc3ff

APP 信息

App名称: 浪鲸下载器
包名: com.langjing.downloader
主活动Activity: com.e4a.runtime.android.StartActivity
安卓版本名称: 1.0.1
安卓版本: 2

域名线索

域名	服务器信息
gdl.lixian.vip.xunlei.com	**IP**: 127.0.0.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
schemas.xmlsoap.org	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
127.0.0.1	**IP**: 127.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
www.btspread.com	**IP**: 104.244.46.244 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
xmlconf.rcv.sandai.net	**IP**: 101.133.169.157 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
torcache.net	**IP**: 185.53.177.11 **所属国家**: Germany **地区**: Bayern **城市**: Munich **纬度**: 48.137428 **经度**: 11.575490
c.appjiagu.com	**IP**: 123.125.81.24 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

shortvideo.xl	没有服务器地理信息.
d1.lengziyuan.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
c.appjiagu.com	摸瓜V3引擎
http://www.openssl.org/support/faq.html	lib/armeabi/libcrypto.so
http://www.openssl.org/support/faq.html	lib/armeabi/libksyplayer.so
http://%s	lib/armeabi/libksyplayer.so
http://xmlconf.rcv.sandai.net/?appid=	lib/armeabi/libxl_stat.so
http://shortvideo.xl/	lib/armeabi/libxl_thunder_sdk.so
http://gdl.lixian.vip.xunlei.com/	lib/armeabi/libxl_thunder_sdk.so
http://127.0.0.1:%d/%s	lib/armeabi/libxl_thunder_sdk.so
http://[fe80:	lib/armeabi/libxl_thunder_sdk.so
http://schemas.xmlsoap.org/soap/envelope/	lib/armeabi/libxl_thunder_sdk.so
http://schemas.xmlsoap.org/soap/encoding/	lib/armeabi/libxl_thunder_sdk.so
https://torcache.net/	lib/armeabi/libxl_thunder_sdk.so

http://www.btspread.com/	lib/armeabi/libxl_thunder_sdk.so
http://d1.lengziyuan.com/?infohash=	lib/armeabi/libxl_thunder_sdk.so
http://i	lib/armeabi/libxl_thunder_sdk.so
http://gdl.lixian.vip.xunlei.com/download	lib/armeabi/libxl_thunder_sdk.so
http://www.openssl.org/support/faq.html	lib/armeabi/libxl_thunder_sdk.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi/libksyplayer.so
download@qq.com	lib/armeabi/libxl_thunder_sdk.so

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=CN, ST=JiangXi, L=NanChang, O=E4A, OU=E4A, CN=Siyu
签名算法: rsassa_pkcs1v15
有效期自: 2020-07-18 10:05:32+00:00
有效期至: 2102-09-07 10:05:32+00:00

发行人: C=CN, ST=JiangXi, L=NanChang, O=E4A, OU=E4A, CN=Siyu
序列号: 0xd68f41a
哈希算法: sha1
md5值: 8c2567978e1a8faf87d38fee6c97fb4f
sha1值: d6de0f10b8c246d87924bbc9dbda98b188fba2a2
sha256值: a640eefee356b9b41f3178cfb890f56831cb94dcee63f75e6297d4d31582384c
sha512值: b016a180f4490c68ab1cd9afdb0627d92a512eb4dbe30e6663a8bf2ad7d537ff909ffc90e1f3ff22108d84db43b927a407a42422d32c8b856c5bb1e602423229

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	类型	详细情况

	险		
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
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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。
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.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.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.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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference

android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.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_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.e4a.runtime.android.mainActivity	Schemes: http://, https://, ftp://, thunder://, ed2k://, content://, file://, magnet://, Hosts: *, Mime Types: text/plain, image/*, audio/*, video/*, application/*, torrent/*, application/x-bittorrent, application/mp4, */rmvb, */avi, */mkv, */*,

com.e4a.runtime.android.mainActivity	Path Prefixes: :, Path Patterns: .*torrent, .*exe.*, .*apk.*, .*torrent.*, .*avi.*, .*mov.*, .*asf.*, .*wmv.*, .*mp4.*, .*3gp.*, .*mkv.*, .*flv.*, .*f4v.*, .*rmvb.*, .*rm.*, .*asx.*, .*mpg.*, .*mpeg.*, .*m4v.*, .*wma.*, .*mp3.*, .*wav.*, .*acc.*, .*ape.*, .*7z.*, .*rar.*, .*zip.*, .*EXE.*, .*APK.*, .*TORRENT.*, .*AVI.*, .*MOV.*, .*ASF.*, .*WMV.*, .*MP4.*, .*3GP.*, .*MKV.*, .*FLV.*, .*F4V.*, .*RMVB.*, .*RM.*, .*ASX.*, .*MPG.*, .*MPEG.*, .*M4V.*, .*WMA.*, .*MP3.*, .*WAV.*, .*ACC.*, .*APE.*, .*7Z.*, .*RAR.*, .*ZIP.*, .*mov, .*f4v, .*xv,

---