MoGua

AXYPlayer 1.8.136.f2867c.APK 分析报告

APP名称:	AXYPlayer

包名:	bMchzyAXciG.eqMVnOtnJP.erjKHqsrdN
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ak123.apk
文件大小: 21.12MB
MD5值: bba7078dd4a75959e81b27a1511a6f18
SHA1值: ade6472891e001918a61be80913b7b8d9576b92f
SHA256值: 9cfa87761fe4bdb0d7bd4bb8060b194789f635b4bdf60f9beeb7c04804ce0cf6

APP 信息

App名称: AXYPlayer
包名: bMchzyAXciG.eqMVnOtnJP.erjKHqsrdN
主活动Activity:
安卓版本名称: 1.8.136.f2867c
安卓版本: 1012140

域名线索

域名	服务器信息
askdbqibwdioqnwodqbqweq121e.top	**IP**: 43.198.227.200 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

URL线索

URL**信息**	Url**所在文件**
http://askdbqibwdioqnwodqbqweq121e.top/log	摸瓜V1引擎

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: True
找到 1 个唯一证书
主题: C=(IhRFKa), ST=(PMJeWPalW), L=(hWLQYiDC), O=(VauoNVhE), OU=(neoDEEFj), CN=(CmZRatd)
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-18 01:21:37+00:00
有效期至: 2075-02-06 01:21:37+00:00
发行人: C=(IhRFKa), ST=(PMJeWPalW), L=(hWLQYiDC), O=(VauoNVhE), OU=(neoDEEFj), CN=(CmZRatd)
序列号: 0xa4df797b0d9aac5a
哈希算法: sha256
md5值: a2a31a45acfbd88b91d757bf52a28e3f
sha1值: fbbe5361760cd246ed3f3fdaa6b8eeac581a7116
sha256值: 5c2674307b06aa0e09da2b2aba143085d40ebce42cca288b434fc6111362e9d5
sha512值: 8bb982ba2ffff9acf24b26cff9eb4ecae96edfc65e6dee7854dc3607faa68f233bf230a46b3be858f179d837dbc8472ccad7734397371dedbea4a063b7fa653e
公钥算法: rsa
密钥长度: 2048
指纹: 2c4f3f8d44a346339fb1d6a4075f123330912487df9164a53b91628b0960efbd

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.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.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.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.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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference
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.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference

android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.USE_EXACT_ALARM	未知	Unknown permission	Unknown permission from android reference
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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
oppo.permission.OPPO_COMPONENT_SAFE	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
		检索正在运	

android.permission.GET_TASKS	危险	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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
com.zNmEJqus.eItlRJKew.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
a.A	Schemes: player://, Hosts: start,