MoGua

鳄鱼小顽皮爱洗澡 1.18.8.APK 分析报告

APP名称: 鳄鱼小顽皮爱洗澡

包名:	com.zls.xy.eyxwpaxz.lk.cc
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年1月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 鳄鱼洗澡.apk
文件大小: 87.88MB
MD5值: af9a78ee994d7e5e4c1b314b4e39a03f
SHA1值: faca2196fcb5a21342c108ba4084a4257bc5c843
SHA256值: 2b0f3624b7bf7430c5840d934f8cf321492b71bcc5ef5d07f4b86e78664335a2

APP 信息

App名称: 鳄鱼小顽皮爱洗澡
包名: com.zls.xy.eyxwpaxz.lk.cc
主活动Activity: com.mobbanana.SplashActivity
安卓版本名称: 1.18.8
安卓版本: 58

域名线索

URL线索

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=bj, ST=bj, L=bj, O=bj, OU=bj, CN=databin

签名算法: rsassa_pkcs1v15
有效期自: 2013-08-17 07:54:10+00:00
有效期至: 3012-12-18 07:54:10+00:00
发行人: C=bj, ST=bj, L=bj, O=bj, OU=bj, CN=databin
序列号: 0x7b9f3894
哈希算法: sha256
md5值: fc007c2e2c0a43cd1f5f3a561cdca088
sha1值: 3645af60f8302526d376405c596596158379c7c2
sha256值: ab3d97a5314945ef85306fcb3ba4b271c5fbadcd1ce2e6ce199611e2e6e96271
sha512值: 20440f4ed6f255d3588ee6257f69b56119dcc8e47ff286a98d21277ef1484edd8ea7c418809e3150c30bbd5e905092a4898f5d207e5feec16fe26e3cac41f82c
公钥算法: rsa
密钥长度: 2048
指纹: 21f1157ed2d6ae30adf613ec88d592140e3976f41656f86e68e09ca068a7d387

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.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.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
com.zls.xy.eyxwpaxz.lk.cc.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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.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。
com.zls.xy.eyxwpaxz.lk.cc.permission.KW_SDK_BROADCAST	未知	Unknown permission	Unknown permission from android reference
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.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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.disney.WMW.WMWActivity	Schemes: wheresmywater://, Hosts: *,
com.bytedance.applog.util.SimulateLaunchActivity	Schemes: rangersapplog.abcdefgh12345678://, Hosts: rangersapplog, Paths: /picker,