



MoGua

UU电玩 12.APK 分析报告



APP名称:

UU电玩

| | |
|--------|----------------------------|
| 包名: | com.xinyule.xyl |
| 域名线索: | 2条 |
| URL线索: | 2条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2024年10月18日 |
| 分析平台: | 摸瓜APK反编译平台 |

文件名: ase1005_2.apk

文件大小: 67.78MB

MD5值: 2898e1397ea24b220725c2726b77f6db

SHA1值: 61b8a14c3239985675ec029ddd7d2f6501963295

SHA256值: 2e023852cb8ea275488af8cc56787dbc240d318dc26fa8ee322d6d4e64838be2

i APP 信息

App名称: UU电玩

包名: com.xinyule.xyl

主活动Activity: org.cocos2dx.lua.AppActivity

安卓版本名称: 12

安卓版本: 6

🔍 域名线索

| 域名 | 服务器信息 |
|---------------|--|
| example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904 |
| www.apple.com | IP: 221.194.154.187 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 |

🌐 URL线索

| URL信息 | Url所在文件 |
|--|--|
| http://example.com/ | cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd | lib/armeabi/libcocos2dlua.so |

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: CN=xinyule

签名算法: rsassa_pkcs1v15

有效期自: 2020-06-10 09:05:41+00:00

有效期至: 3018-10-12 09:05:41+00:00

发行人: CN=xinyule

序列号: 0x5a7ef2c6

哈希算法: sha256

md5值: aa79330ac44017ec9f1f678f8c3e9cf7

sha1值: 3639436f164932083584a7925850dbafa11fd554

sha256值: 543dd48b26c57104e0ed40ea27bef8aafb23180ecf5d6eb5e91e8dad3d78b47c

sha512值: 93b765b30750214d870f915580a333ff48b7f52fd9609bca9f712cb125a6f07a803721a29a4348cd9f40382090e81742d6290998b696de1827702879b40344f2

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.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_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_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.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.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.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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |

应用内通信

| 活动(ACTIVITY) | 通信(INTENT) |
|------------------------------|---------------------|
| org.cocos2dx.lua.AppActivity | Schemes: aaaaaa://, |

报告由 [摸瓜APK反编译平台](#) 自动生成,并非包含所有检测结果,有疑问请联系管理员。