MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

LOL充值助手 1.0.APK

APP名称:	LOL充值助手
包名:	com.jshare6.lolrycz
域名线索:	10条
URL线索:	7条
邮箱线索:	0条
分析日期:	2022年1月28日 23:05

文件信息

文件名: lolczzs27596.apk
文件大小: 1.65MB
MD5值: 6a53eff6bae13948cc55da7bca2bc6ed
SHA1值: 48818f0b25d139b93360ddbad2a30706870efd50
SHA256值: 28eb2297930fee819f15b37cee82eb20031d564f0267b9aa7a9e15038e141a6b

APP 信息

App名称: LOL充值助手
包名: com.jshare6.lolrycz
主活动**Activity:** com.e4a.runtime.android.StartActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
bbs.e4asoft.com	good	**IP:** 119.3.32.105 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map

域名	是否危险域名	服务器信息
www.123cha.com	good	IP: 121.36.230.208 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
log.umsns.com	good	IP: 59.82.31.92 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
alog.umeng.com	good	IP: 59.82.31.151 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
oc.umeng.com	good	IP: 203.119.128.55 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
alog.umeng.co	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
bbs.e4asoft.compath	good	没有服务器地理信息.
api.fanyi.baidu.com	good	**IP:** 112.80.255.4 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779 查看地图: Google Map
www.baidu.com	good	**IP:** 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
oc.umeng.co	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://oc.umeng.com/check_config_update	com/umeng/analytics/a.java

URL信息	Url所在文件
http://oc.umeng.co/check_config_update	com/umeng/analytics/a.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://log.umsns.com/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://bbs.e4asoft.com/openapi_unsafe.php	com/e4a/runtime/MySQL.java
http://www.123cha.com/	com/e4a/runtime/C0057.java
http://bbs.e4asoft.com;path=/	com/e4a/runtime/C0057.java
http://api.fanyi.baidu.com/api/trans/vip/translate?q=	com/e4a/runtime/C0057.java
http://www.baidu.com/search?q=	com/e4a/runtime/components/impl/android/p013/WebViewPresenterImpl.java

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.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_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference

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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=中国, ST=TzRcVxptq, L=VvLcKcfv, O=RaLxNss, OU=UfDjLq, CN=BrUcM
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-12 06:54:02+00:00
Valid To: 2031-10-10 06:54:02+00:00
Issuer: C=中国, ST=TzRcVxptq, L=VvLcKcfv, O=RaLxNss, OU=UfDjLq, CN=BrUcM
Serial Number: 0x37e8899b
Hash Algorithm: sha256
md5: 40443c24ac708cbd70c4663bc1ea4494
sha1: 70bca8d0bbbf488aad64b7d35e3e344753debe1c

sha256: c0790b7bc193fc0a314c338fdedb479581bfe384fdbc10556c601bd5032eb444
sha512: c20cd3d66e0c9d9ad951a3d1309079881753ffe5d35ee7ae6ff45404e8a07f975593ae4cabaa669a1dd2e26e012801ced92aa0fd007a573d9b98b0bc6ccaf668

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check network operator name check 编译器: r8 模糊器: unreadable field names unreadable method names

---