MoGua

五福彩票 9.9.9.APK 分析报告

APP名称: 五福彩票

包名:	com.hsmse0206.hsmsey
域名线索:	37条
URL线索:	35条
邮箱线索:	0条
分析日期:	2024年9月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 0byqjib16b0957.apk
文件大小: 42.84MB
MD5值: 4b6e87d0be6215ef8dce31ceaef06e04
SHA1值: f1c9422ef15edd3a9a77c793676c1fc794c3ba15
SHA256值: b8e8bfbf09d398773eb6bdab948bff11d02c342c03a16713ac556ba7931ac75c

APP 信息

App名称: 五福彩票
包名: com.hsmse0206.hsmsey
主活动Activity: com.fb.zh758.MainActivity
安卓版本名称: 9.9.9
安卓版本: 1

域名线索

域名	服务器信息
alogsus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
hydra.alibaba.com	**IP**: 203.119.144.20 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw.stable.alipay.net	没有服务器地理信息.
	IP: 109.244.244.137

android.bugly.qq.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
h.trace.qq.com	IP: 109.244.244.241 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mcgw.alipay.com	IP: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
plus.google.com	IP: 31.13.96.193 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.343990 **经度**: -6.267190
mobilegw.alipaydev.com	IP: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
h5.m.taobao.com	IP: 111.225.210.166 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717

mobilegw.aaa.alipay.net	没有服务器地理信息.
mclient.alipay.com	**IP**: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
loggw-exsdk.alipay.com	**IP**: 110.76.6.71 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
astat.bugly.qcloud.com	**IP**: 150.109.27.253 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
cmnsguider.yunos.com	**IP**: 203.119.145.40 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
tsis.jpush.cn	**IP**: 121.36.81.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000

ulogs.umengcloud.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
monitor.geetest.com	**IP**: 47.95.165.133 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
ulogs.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
bjuser.jpush.cn	**IP**: 122.9.9.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
m.alipay.com	**IP**: 203.209.245.74 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
developer.umeng.com	**IP**: 59.82.29.163 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou

	纬度: 30.293650 **经度**: 120.161423
ouplog.umeng.com	IP: 47.246.110.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
codepush.azurewebsites.net	IP: 199.16.156.38 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.facebook.com	IP: 157.240.7.8 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
xmlpull.org	IP: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
github.com	IP: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
	IP: 183.232.25.153 **所属国家**: China

ce3e75d5.jpush.cn	**地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
wappaygw.alipay.com	IP: 124.239.239.236 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
alogus.umeng.com	IP: 223.109.148.177 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
static.geetest.com	IP: 220.181.158.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
pinterest.com	IP: 202.160.128.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
182.92.20.189	IP: 182.92.20.189 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423

plbslog.umeng.com	**IP**: 36.156.202.78 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw.alipay.com	**IP**: 203.209.250.2 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
astat.bugly.cros.wr.pvp.net	**IP**: 170.106.135.32 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
twitter.com	**IP**: 74.86.226.234 **所属国家**: United States of America **地区**: Texas **城市**: Dallas **纬度**: 32.939491 **经度**: -96.838730

URL线索

URL信息	Url所在文件
https://pinterest.com/pin/create/button/?url=	cl/json/f/h.java
https://twitter.com/intent/tweet?text=	cl/json/f/n.java

https://plus.google.com/share?url=	cl/json/f/e.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/f/b.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/f/c.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ae/b.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/af/d.java
https://tsis.jpush.cn	cn/jiguang/ak/i.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java

http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/e.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
https://codepush.azurewebsites.net/	com/microsoft/codepush/react/a.java
http://developer.umeng.com/docs/66650/cate/66650	b/l/a/g/g.java
https://ulogs.umeng.com/unify_logs	b/l/b/k/c.java
https://alogus.umeng.com/unify_logs	b/l/b/k/c.java
https://alogsus.umeng.com/unify_logs	b/l/b/k/c.java
https://ulogs.umengcloud.com/unify_logs	b/l/b/k/c.java
https://cmnsguider.yunos.com:443/genDeviceToken	b/l/b/k/h/u.java
https://plbslog.umeng.com	b/l/b/j/b.java
https://ouplog.umeng.com	b/l/b/j/b.java
https://developer.umeng.com/docs/66632/detail/	b/l/b/e/g.java

https://mcgw.alipay.com/sdklog.do	b/a/b/f/f/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	b/a/b/f/f/d.java
https://mobilegw.alipay.com/mgw.htm	b/a/b/a/a.java
https://mobilegw.alipaydev.com/mgw.htm	b/a/b/j/k.java
http://m.alipay.com/?action=h5quit	b/a/b/j/l.java
https://h5.m.taobao.com/mlapp/olist.html	b/a/b/b/a.java
https://h.trace.qq.com/kv	b/j/a/d/e.java
https://astat.bugly.qcloud.com/rqd/async	b/j/a/d/d.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	b/j/a/d/d.java
https://android.bugly.qq.com/rqd/async	b/j/a/c/c/b/a.java
https://monitor.geetest.com/monitor/send	b/e/a/s1.java
https://static.geetest.com/static/appweb/app3-index.html	b/e/a/s2/a/d.java

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=xxx.com, OU=dev, O=vihoo, L=SZ, ST=GD, C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2022-12-02 03:52:21+00:00
有效期至: 2077-09-04 03:52:21+00:00
发行人: CN=xxx.com, OU=dev, O=vihoo, L=SZ, ST=GD, C=CN
序列号: 0x3d21080c
哈希算法: sha256
md5值: 1a7c8da36370fdac977d839d11667d06
sha1值: 5fbd62881999d77805e02f8681bc1f3ef7c9c965
sha256值: 8274b973859946d4e25165e10439ad7e6756cbc27c7c071aceca4c473d0d5315
sha512值: 7fcf668b13cde74df3aa318629ea226a8c28371078e23056bf81e2425f4df9ab1a8b851f8246c294468e82be0b9aa8243c6b7af51ff99616e35759f9e57b2248

硬编码敏感信息

可能的敏感信息
"UMENG_KEY" : "616e7da0e0f9bb492b33a15c"
"reactNativeCodePush_androidDeploymentKey" : ""

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.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.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.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.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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
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
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
com.hsmse0206.hsmsey.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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
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.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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.fb.zh758.MainActivity	Schemes: zonghepingtai://,
com.alipay.sdk.app.AlipayResultActivity	Schemes: newzonghepingtai://,

---