

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 诚博彩票 V2.0.8.APK

APP名称: 诚博彩票

包名: com.tg9.cbcp

域名线索: 43条

URL线索: 90条

邮箱线索: 4条

分析日期: 2022年1月19日 11:12

文件名: 18155146.apk 文件大小: 30.24MB

MD5值: b47608e7b0160463b3007fcdb20db25b

SHA1值: 81607f745084300bae9679b9dfc12c0b17dffd1d

SHA256值: ad0cfafd5e92320ef7b20d1b02658889193c267b52a67bd0710381da1f7d2055

i APP 信息

App名称: 诚博彩票 包名: com.tg9.cbcp

主活动**Activity:** com.cp99.tz01.lottery.ui.activity.SplashActivity

安卓版本名称: V2.0.8

安卓版本: 120

0 域名线索

域名	是否危险域名	服务器信息
metrics.data.hicloud.com	good	IP: 49.4.18.4 所属国家: China 地区: Beijing 城市: Beijing 结度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
cstaticdun.126.net	good	IP: 103.254.188.71 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
restapi.amap.com	good	IP: 106.11.43.113 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
xmlpull.org	good	IP: 74.50.62.60 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
ouplog.umeng.com	good	IP: 47.74.172.6 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map

域名	是否危险域名	服务器信息
ulogs.umengcloud.com	good	IP: 106.11.86.78 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
store.hispace.hicloud.com	good	IP: 49.4.44.164 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
nav.cn.ronghub.com	good	IP: 140.143.50.86 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
resolver.msg.xiaomi.net	good	IP: 183.84.5.221 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

域名	是否危险域名	服务器信息
cc.map.qq.com	good	IP: 182.254.57.47 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
alogus.umeng.com	good	IP: 106.11.43.229 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
upload.ffmpeg.org	good	IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.853409 经度: 2.348800 查看地图: Google Map
www.jivesoftware.com	good	IP: 35.238.7.255 所属国家: United States of America 地区: lowa 城市: Council Bluffs 纬度: 41.261940 经度: -95.860832 查看地图: Google Map

域名	是否危险域名	服务器信息
support.rongcloud.cn	good	IP: 150.138.213.79 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
stats.cn.ronghub.com	good	IP: 117.50.12.93 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
analytics.map.qq.com	good	IP: 182.254.63.54 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
52.83.240.50	good	IP: 52.83.240.50 所属国家: China 地区: Ningxia 城市: Zhongwei 纬度: 37.509998 经度: 105.180000 查看地图: Google Map

域名	是否危险域名	服务器信息
ue.indoorloc.map.qq.com	good	IP: 182.254.50.54 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
www.baidu.com	good	IP: 110.242.68.5 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
metrics1.data.hicloud.com	good	IP: 118.194.33.17 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
feedback.cn.ronghub.com	good	IP: 106.75.12.130 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

域名	是否危险域名	服务器信息
ccc.sys.miui.com	good	IP: 120.133.33.125 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
nstool.netease.com	good	IP: 42.186.241.14 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
cmnsguider.yunos.com	good	IP: 203.119.169.69 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
a.vmall.com	good	IP: 49.4.39.87 所属国家: China 地区: Beijing 城市: Beijing 绿度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
register.xmpush.global.xiaomi.com	good	IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
nav2-cn.ronghub.com	good	IP: 82.157.74.142 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
developer.umeng.com	good	IP: 59.82.31.95 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
schemas.android.com	good	没有服务器地理信息.
github.com	good	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 查看地图: Google Map

域名	是否危险域名	服务器信息
metok.sys.miui.com	good	IP: 124.251.100.14 所属国家: China 地区: Beijing 城市: Beijing 结度: 39.907501 经度: 116.397232 查看地图: Google Map
yun-hl.3g.qq.com	good	IP: 109.244.212.210 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
ru.register.xmpush.global.xiaomi.com	good	IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752220 经度: 37.615559 查看地图: Google Map
cbcp-api23sd.tgcloud2.com	good	没有服务器地理信息.
plbslog.umeng.com	good	IP: 59.82.43.171 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

域名	是否危险域名	服务器信息
ac.dun.163yun.com	good	IP: 59.111.19.16 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
api.xmpush.xiaomi.com	good	IP: 117.48.116.220 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
alogsus.umeng.com	good	IP: 106.11.43.142 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
play.google.com	good	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map

域名	是否危险域名	服务器信息
fr.register.xmpush.global.xiaomi.com	good	IP: 18.198.9.84 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.115520 经度: 8.684170 查看地图: Google Map
ulogs.umeng.com	good	IP: 59.82.29.246 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
lark.alipay.com	good	IP: 103.52.199.80 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
up-hl.3g.qq.com	good	IP: 109.244.209.172 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



URL信息	Url所在文件
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://lark.alipay.com/yj131525/byt0wl/ufnf3i#A10200	com/umeng/commonsdk/statistics/internal/c.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://developer.umeng.com/docs/66632/detail/70018?um_channel=sdk	com/umeng/analytics/b.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/a.java
https://cstaticdun.126.net/api/v2/mobile.v2.10.1.html	com/netease/nis/captcha/CaptchaConfiguration.java
https://ac.dun.163yun.com/v2/collect?	com/netease/mobsec/rjsb/i.java

URL信息	Url所在文件
http://nstool.netease.com/info.js	com/netease/mobsec/rjsb/i.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
https://store.hispace.hicloud.com/hwmarket/api/	com/huawei/updatesdk/service/a/e.java
http://a.vmall.com/app/	com/huawei/hms/update/e/k.java
https://metrics1.data.hicloud.com:6447	com/huawei/hms/api/HuaweiApiClient.java
https://play.google.com/store/apps/details?id=	com/huawei/hms/support/api/push/a/a.java
http://a.vmall.com/	com/huawei/hms/support/api/push/a/a.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/x1.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/x1.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/x1.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/l0.java
www.baidu.com:80	com/xiaomi/push/service/m.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/c.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/v0.java

URL信息	Url所在文件
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/v0.java
https://cbcp-api23sd.tgcloud2.com:5869	com/cp99/tz01/lottery/ui/activity/personalCenter/setting/c.java
https://cbcp-api23sd.tgcloud2.com:5869	com/cp99/tz01/lottery/ui/fragment/homePage/j.java
http://support.rongcloud.cn/kb/Mjc2	com/cp99/tz01/lottery/ui/fragment/chat/k0.java
https://cbcp-api23sd.tgcloud2.com:5869	com/cp99/tz01/lottery/e/h.java
http://schemas.android.com/apk/res/android	com/cp99/tz01/lottery/widget/FixedSlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/cp99/tz01/lottery/widget/FixCommonTabLayout.java
https://up-hl.3g.qq.com/upreport	c/t/m/g/at.java
https://analytics.map.qq.com/?wf4	c/t/m/g/cs.java
https://ue.indoorloc.map.qq.com/	c/t/m/g/ek.java
https://cc.map.qq.com/?get_c3	c/t/m/g/cz.java
https://yun-hl.3g.qq.com/halleycloud	c/t/m/g/cd.java
https://ue.indoorloc.map.qq.com/?wl	c/t/m/g/eh.java
https://analytics.map.qq.com/?sf	c/t/m/g/cu.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	f/q/h/i.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#process-namespaces	f/q/h/q/a.java
http://www.jivesoftware.com/xmlns/xmpp/properties	f/q/h/o/d.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	f/q/h/p/c.java
http://%1\$s/gslb/?ver=4.0	f/q/e/f.java
https://metok.sys.miui.com	f/q/d/d.java
http://ccc.sys.miui.com	f/q/d/a/f.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	f/q/g/e.java
https://metrics.data.hicloud.com:6447	f/h/a/f/c/b/n.java
https://)	f/h/a/f/c/b/h.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://restapi.amap.com/v3/staticmap?location=	io/rong/imkit/plugin/location/AMapLocationActivity.java
http://restapi.amap.com/v3/staticmap?location=	io/rong/imkit/plugin/location/AMapLocationActivity2D.java
http://support.rongcloud.cn/kb/NzA1	io/rong/imkit/plugin/image/PictureSelectorActivity.java

URL信息	Url所在文件
http://support.rongcloud.cn/kb/Mjc2	io/rong/imkit/widget/adapter/MessageListAdapter.java
http://nav.cn.ronghub.com/navipush.json	io/rong/push/common/PushConst.java
http://%s/%s	io/rong/push/core/PushNaviClient.java
http://52.83.240.50/upload	io/rong/common/fwlog/LogEntity.java
https://stats.cn.ronghub.com/active.json	io/rong/imlib/RongIMClient.java
http://%s/active.json	io/rong/imlib/RongIMClient.java
http://%s	io/rong/imlib/httpdns/HttpDnsClient.java
https://nav2-cn.ronghub.com/navi.xml	io/rong/imlib/navigation/NavigationClient.java
http://nav2-cn.ronghub.com/navi.xml	io/rong/imlib/navigation/NavigationClient.java
https://nav.cn.ronghub.com/navi.xml	io/rong/imlib/navigation/NavigationClient.java
http://%s/navi.xml	io/rong/imlib/navigation/NavigationClient.java
http://nav.cn.ronghub.com/navi.xml	io/rong/imlib/navigation/NavigationClient.java
http://%s/%s	io/rong/imlib/navigation/NavigationClient.java
https://feedback.cn.ronghub.com	io/rong/imlib/navigation/NavigationCacheHelper.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	g/a/t.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	g/a/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	g/a/f.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	g/a/m.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	g/a/j.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	g/a/a0/f.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	g/a/a0/d.java
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
ftp://upload.ffmpeg.org/incoming/	lib/x86/libijkplayer.so
ftp://upload.ffmpeg.org/incoming/	lib/armeabi/libijkplayer.so

✓邮箱线索

邮箱地址	所在文件
xxxx@xxxx.com	com/huawei/hms/support/api/push/a/d/a.java
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi/libijkplayer.so

畫此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.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.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_FORMAT_FILESYSTEMS	危险	格式化外部存储器	允许应用程序格式化可移动存储
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.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。

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
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.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.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.hardware.sensor.accelerometer	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频 设置	允许应用程序修改全局音频设置,例如音量和路由
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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECEIVE_USER_PRESENT	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。
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上 显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上 显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.action.UPDATE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上 显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上 显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_APP_BADGE	正常	显示应用程序 通知	允许应用程序显示应用程序图标徽章
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上 显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上 显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上 显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上 显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上 显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上 显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
com.tg9.cbcp.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	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.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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒



APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates

Subject: O=tg9

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2018-12-10 08:14:12+00:00 Valid To: 2043-12-04 08:14:12+00:00

Issuer: O=tg9

Serial Number: 0x54704b86 Hash Algorithm: sha256

md5: cba4775a8ea279ef23a17d573a4e4d3e

sha1: b2f0e9c90ee5a772f296306fe414e5fd553e1689

sha256: 7276f37da7be779ed3290c4477eb9df70bfccaff1ff55f4d1f830d881ffb3983

sha512: ab908e3ccb75f69356534ffa39de38d55d9165e235ff65ed78537dcf7ed7625cfe141cc06946b3dd21c94af3972dc60653ff48309de18954f4dec89e1714a8f5

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 78ef8818fd56f24fea2500597a80685bd08fd2cf36e626c678ef97c25e6fe762

在 Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
WeChat Location		https://reports.exodus-privacy.eu.org/trackers/76

₽ 硬编码敏感信息

可能的敏感信息

"agent_add_user": "新增会员"

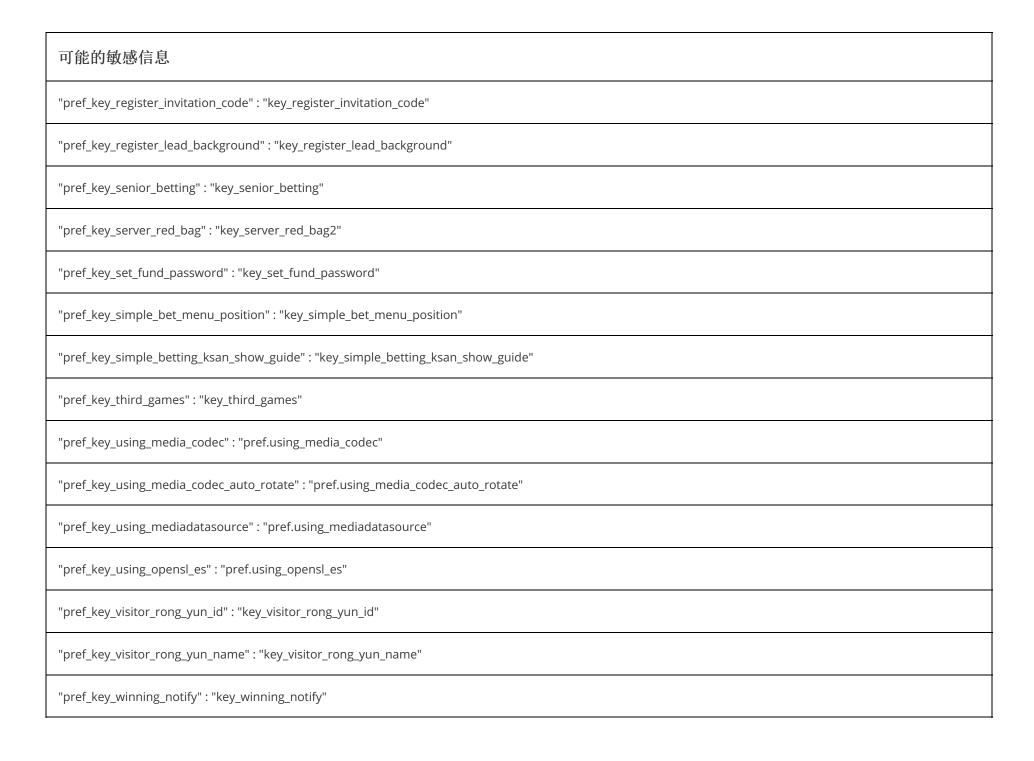




可能的敏感信息
"pref_key_bet_cancel_order" : "key_bet_cancel_order"
"pref_key_bet_slips_preset_money" : "key_bet_slips_preset_money"
"pref_key_bet_total_limit" : "key_bet_total_limit"
"pref_key_betting_help_menu_visible" : "key_betting_help_menu_visible"
"pref_key_betting_info_push" : "key_betting_info_push"
"pref_key_betting_random_show_guide" : "key_betting_random_show_guide"
"pref_key_betting_show_guide" : "key_betting_show_guide"
"pref_key_chat_room_customer_amount" : "key_chat_room_customer_amount"
"pref_key_chat_room_danmu" : "key_chat_room_danmu"
"pref_key_chat_room_global_banned" : "key_chat_room_global_banned"
"pref_key_chat_room_target_id" : "key_chat_room_target_id"
"pref_key_chat_room_top" : "key_chat_room_top"
"pref_key_config_web_site_url" : "key_config_web_site_url"
"pref_key_device_id" : "key_device_id"
"pref_key_enable_background_play" : "pref.enable_background_play"

可能的敏感信息
"pref_key_enable_no_view" : "pref.enable_no_view"
"pref_key_enable_surface_view" : "pref.enable_surface_view"
"pref_key_expand_bonus_group_status" : "key_expand_bonus_group_status"
"pref_key_forbid_chat_red_packet" : "key_forbid_chat_red_packet"
"pref_key_free_trial" : "key_free_trial"
"pref_key_free_trial_amount" : "key_free_trial_amount"
"pref_key_free_trial_set" : "key_free_trial_set"
"pref_key_game_account_auto_transform" : "key_game_account_auto_transform"
"pref_key_has_agree_jiebe" : "key_has_agree_jiebe"
"pref_key_has_agree_yuebao" : "key_has_agree_yuebao"
"pref_key_has_notice_auto_transform" : "key_has_notice_auto_transform"
"pref_key_has_set_betting" : "key_has_set_betting"
"pref_key_homepage_chat_room" : "key_homepage_chat_room"
"pref_key_homepage_show_guide" : "key_homepage_show_guide"
"pref_key_invitation_code" : "key_invitation_code"





可能的敏感信息
"pref_key_yi_dun_captcha" : "key_yi_dun_captcha"
"pref_key_yubao_balance_show" : "key_yubao_balance_show"
"private_chat" : "发送消息"
"rc_authorities_fileprovider" : ".FileProvider"
"rc_conversation_list_my_private_conversation" : "我的私人会话"
"rc_emoji_hear_no_monkey" : "不听"
"rc_emoji_see_no_monkey" : "不看"
"register_input_password": "请输入登录密码(至少6位)"
"register_input_username":"请输入用户名(须包含字母和数字)"
"setting_fund_password": "资金密码"
"setting_login_password": "登录密码"
"setting_private_chat_notify" : "私聊通知"
"token_invalid": "登录过期,请重新登录"
"token_login_on_others" : "账号在其他设备登录,请重新登录"
"username" : "用户名"

可能的敏感信息

"rc_conversation_list_my_private_conversation" : "My private conversation"

"rc_emoji_hear_no_monkey" : "Hear-No-Monkey"

"rc_emoji_see_no_monkey" : "See-No-Monkey"



活动(ACTIVITY)	通信(INTENT)
com.cp99.tz01.lottery.ui.activity.SplashActivity	Schemes: cbcplottery://, Hosts: cbcplottery,

命加壳分析

文件列表	分析结果			
classes.dex	壳列表 反虚拟机 编译器	详细情况 Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check SIM operator check subscriber ID check r8		
classes2.dex	壳列表 反虚拟机 编译器	详细情况 Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check		

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。