MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

123招聘网 1.0.0.APK

APP名称:	123招聘网
包名:	m.bz123zpw.com
域名线索:	47条
URL线索:	66条
邮箱线索:	4条
分析日期:	2022年2月2日 17:02

文件信息

文件名: 123zhaopin.apk
文件大小: 8.76MB
MD5值: 6835d73c385d9e2f60b13e1b4ba73450
SHA1值: 2faea193f0af4577437bbd05d25907911eebf8f6
SHA256值: a40deb9ff5e061215ff27d0dfa05213c93766580abd0f86697b7ac4b1d4426f1

APP 信息

App名称: 123招聘网
包名: m.bz123zpw.com
主活动**Activity:** com.kingkr.webapp.activity.MainActivity
安卓版本名称: 1.0.0
安卓版本: 9

域名线索

域名	是否危险域名	服务器信息
pingma.qq.com	good	**IP:** 119.45.78.184 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
datax.baidu.com	good	IP: 111.206.210.170 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
aip.baidubce.com	good	IP: 111.206.210.12 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
ofloc.map.baidu.com	good	IP: 111.206.209.193 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
check.shareinstall.com.cn	good	IP: 124.71.238.62 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

域名	是否危险域名	服务器信息
rqd.uu.qq.com	good	IP: 182.254.88.184 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
xml.org	good	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246 查看地图: Google Map
loc.map.baidu.com	good	IP: 111.206.209.175 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
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

域名	是否危险域名	服务器信息
cfg.imtt.qq.com	good	IP: 121.51.158.70 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
iploc.market.alicloudapi.com	good	IP: 119.23.169.39 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
daup.map.baidu.com	good	IP: 153.3.236.86 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
mqqad.html5.qq.com	good	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

域名	是否危险域名	服务器信息
openrcv.baidu.com	good	IP: 111.206.209.112 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
www.appbsl.com	good	IP: 106.53.119.251 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
mta.qq.com	good	IP: 111.161.14.94 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
port.appbsl.net	good	IP: 120.27.130.213 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
www.appk6.com	good	IP: 116.62.66.31 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
statlog.shareinstall.com.cn	good	IP: 114.116.251.190 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
ue.indoorloc.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
api.map.baidu.com	good	IP: 111.206.209.166 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
debugtbs.qq.com	good	IP: 175.27.9.46 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
maps.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
api.weibo.com	good	IP: 180.149.153.83 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
dxp.baidu.com	good	IP: 110.242.68.94 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
hmma.baidu.com	good	IP: 110.242.68.196 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
com.thoughtworks.xstream	good	没有服务器地理信息.
adblocker.appbsl.net	good	没有服务器地理信息.
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map

域名	是否危险域名	服务器信息
pv.sohu.com	good	IP: 211.159.191.96 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
verify.baidubce.com	good	IP: 112.80.255.237 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
debugx5.qq.com	good	IP: 175.27.9.46 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
itsdata.map.baidu.com	good	IP: 111.206.209.180 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
yun-hl.3g.qq.com	good	IP: 175.27.0.142 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
wup.imtt.qq.com	good	IP: 182.254.56.113 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
interface.shareinstall.com.cn	good	IP: 106.75.20.108 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
soft.tbs.imtt.qq.com	good	IP: 121.51.175.105 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

域名	是否危险域名	服务器信息
log.tbs.qq.com	good	IP: 109.244.244.32 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
www.qq.com	good	IP: 175.27.8.138 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
mdc.html5.qq.com	good	IP: 175.27.9.46 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
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

域名	是否危险域名	服务器信息
pms.mb.qq.com	good	IP: 121.51.158.70 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
wx.tenpay.com	good	IP: 182.254.88.166 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
android.bugly.qq.com	good	IP: 109.244.244.137 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
config.shareinstall.com.cn	good	IP: 124.71.238.62 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

域名	是否危险域名	服务器信息
my.wlwx.com	good	IP: 120.24.95.120 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

URL线索

URL信息	Url所在文件
https://statlog.shareinstall.com.cn/shareinstall_log/online	com/sh/sdk/shareinstall/helper/n.java
https://statlog.shareinstall.com.cn/shareinstall_log/install	com/sh/sdk/shareinstall/helper/k.java
https://check.shareinstall.com.cn/wwwroot	com/sh/sdk/shareinstall/helper/f.java
http://iploc.market.alicloudapi.com/v3/ip	com/sh/sdk/shareinstall/helper/g.java
https://statlog.shareinstall.com.cn/shareinstall_log/si	com/sh/sdk/shareinstall/helper/l.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/helper/c.java
http://pv.sohu.com/cityjson?ie=utf-8	com/sh/sdk/shareinstall/helper/i.java
https://statlog.shareinstall.com.cn/shareinstall_log/register	com/sh/sdk/shareinstall/helper/p.java

URL信息	Url所在文件
https://statlog.shareinstall.com.cn/sdkinfoscollection/startover	com/sh/sdk/shareinstall/helper/d.java
https://interface.shareinstall.com.cn/hike/exce	com/sh/sdk/shareinstall/helper/o.java
https://statlog.shareinstall.com.cn/shareinstall_log/active	com/sh/sdk/shareinstall/helper/a.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/c/a/b.java
http://mta.qq.com/	com/tencent/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/stat/StatServiceImpl.java
http://mta.qq.com/mta/api/ctr_feedback/add_feedback	com/tencent/stat/d.java
http://mta.qq.com/mta/api/ctr_feedback/get_feedback	com/tencent/stat/d.java
http://mta.qq.com/mta/api/ctr_feedback/reply_feedback	com/tencent/stat/d.java
http://mta.qq.com/mta/api/ctr_feedback	com/tencent/stat/common/StatConstants.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/common/StatConstants.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
www.qq.com	com/tencent/smtt/sdk/ag.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/ag.java

URL信息	Url所在文件
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/d.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/v.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/v.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/v.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/v.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/v.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/v.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/v.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/v.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/i.java
https://aip.baidubce.com/rest/2.0/ocr/v1/accurate_basic?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/idcard?	com/baidu/ocr/sdk/a.java

URL信息	Url所在文件
https://aip.baidubce.com/rest/2.0/ocr/v1/bankcard?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/vehicle_license?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/driving_license?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/license_plate?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/business_license?	com/baidu/ocr/sdk/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/receipt?	com/baidu/ocr/sdk/a.java
https://verify.baidubce.com/verify/1.0/token/sk?sdkVersion=1_4_4	com/baidu/ocr/sdk/a.java
https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1_4_4	com/baidu/ocr/sdk/a.java
https://verify.baidubce.com/verify/1.0/sdk/report	com/baidu/ocr/sdk/c/c.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/b/a/b.java
http://loc.map.baidu.com/gpsz	com/baidu/location/b/a.java
http://loc.map.baidu.com/indoorlocbuildinginfo.php	com/baidu/location/indoor/a.java
http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet	com/baidu/location/indoor/mapversion/c/a.java
http://loc.map.baidu.com/check_indoor_data_update	com/baidu/location/indoor/mapversion/a/e.java
https://loc.map.baidu.com/ios_indoorloc	com/baidu/location/indoor/mapversion/a/a.java

URL信息	Url所在文件
https://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/a/f.java
http://loc.map.baidu.com/cc.php	com/baidu/location/a/d.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/d/k.java
http://ofloc.map.baidu.com/offline_loc	com/baidu/location/d/h.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/d/g.java
http://%s/%s	com/baidu/location/d/c.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/d/c.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/wloc	com/baidu/location/g/k.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/g/k.java

URL信息	Url所在文件
https://loc.map.baidu.com/sdk.php	com/baidu/location/g/k.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/g/k.java
http://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/s.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/s.java
http://datax.baidu.com/xs.gif	com/baidu/mobstat/aa.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/aa.java
http://dxp.baidu.com/upgrade	com/baidu/mobstat/aa.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/aa.java
https://hmma.baidu.com/auto.gif	com/baidu/mobstat/Config.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://dxp.baidu.com/vizParser	com/baidu/mobstat/bg.java
https://dxp.baidu.com/autoTracker	com/baidu/mobstat/bg.java
https://dxp.baidu.com/circleConfig?	com/baidu/mobstat/bg.java
http://www.appk6.com	com/kingkr/webapp/MainApplication.java

URL信息	Url所在文件
https://wx.tenpay.com/	com/kingkr/webapp/browser/WebViewUtils.java
www.appbsl.com	com/kingkr/webapp/browser/WebViewUtils.java
http://maps.google.com/maps?saddr=	com/kingkr/webapp/browser/Bridge.java
https://api.weibo.com/2/users/	com/kingkr/webapp/component/WeiboComponent.java
http://my.wlwx.com:6006	com/kingkr/webapp/component/quicklogin/QuickLoginComponent.java
http://port.appbsl.net/public/adv/index/appcount	com/kingkr/webapp/e/a.java
https://adblocker.appbsl.net/index.php?g=port&m=unionadvblock&a=get	com/kingkr/webapp/service/UpdateFilterIpService.java
https://wx.tenpay.com/	com/kingkr/webapp/fragment/WebFragment.java
http://com.thoughtworks.xstream/XStreamSource/feature	com/thoughtworks/xstream/io/xml/TraxSource.java
http://com.thoughtworks.xstream/sax/property/configured-xstream	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespaces	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespace-prefixes	com/thoughtworks/xstream/io/xml/SaxWriter.java
https://cc.map.qq.com/?get_c3	c/t/m/g/da.java
https://up-hl.3g.qq.com/upreport	c/t/m/g/aq.java

URL信息	Url所在文件
https://yun-hl.3g.qq.com/halleycloud	c/t/m/g/cb.java
https://ue.indoorloc.map.qq.com/	c/t/m/g/dq.java
https://ue.indoorloc.map.qq.com/?wl	c/t/m/g/dq.java
http://analytics.map.qq.com/?sf	c/t/m/g/cr.java

邮箱线索

邮箱地址	所在文件
ctwap@mycdma.cn	com/tencent/mid/a/b.java
null@null.xml	com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi-v7a/libiconv.so
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi/libiconv.so

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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.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_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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.SET_DEBUG_APP	危险	启用应用程序调试	允许一个应用程序打开另一个应用程序的调试。恶意应用程序可以使用它来杀死其他应用程序
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.CLEAR_APP_CACHE	系统需要	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

向手机申请的权限	是否危险	类型	详细情况
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	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.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	未知	Unknown permission	Unknown permission from android reference
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	Unknown permission	Unknown permission from android reference
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: C=CN, O=123[illegible], OU=123[illegible], CN=314309
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-01-15 11:30:19+00:00
Valid To: 2118-08-09 11:30:19+00:00
Issuer: C=CN, O=123[illegible], OU=123[illegible], CN=314309
Serial Number: 0x3c3e52b0
Hash Algorithm: sha256
md5: 8d3c130dd1ae0d2ee07f2e2df3126841
sha1: daf6e525f61e00f1fb95221d6496acd77724fa4a
sha256: 32e2cacf54b66d70fb983778f84c69ca095374abba31e03efbdebb1e9c04a6f4
sha512: ada3ae7c99440ee6f78e6e353e06121b7d751ded169300d7422f6307cc1499d914f4656d9b3a9c734ecd446824908c1758b2cb8b4578e4a71a24e0508f66e4c3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 117e1b7f0987573972ee73f49157198fd37f10d7b73785d392fa7d923684062f

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
WeChat Location		https://reports.exodus-privacy.eu.org/trackers/76

硬编码敏感信息

可能的敏感信息
"QQ_AppSecret" : "_QQ_AppSecret"
"SINA_APP_KEY" : "_SINA_APP_KEY"
"WX_AppSecret" : "_WX_AppSecret"
"baid_ai_app_key" : "_baid_ai_app_key"
"baid_ai_secret_key" : "_baid_ai_secret_key"
"hw_app_key" : "_hw_app_key"
"mi_app_key" : "_mi_app_key"
"oppo_app_key" : ""
"shareinstall_appkey" : ""

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.kingkr.webapp.activity.MainActivity	Schemes: @string/wx_app_id://, @string/shareinstall_scheme://,
com.tencent.tauth.AuthActivity	Schemes: @string/tencent://,
com.kingkr.webapp.activity.HtmlOpenApp	Schemes: m.bz123zpw.com://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
device ID check
subscriber ID check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
