MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

葫芦侠3楼 3.5.0.22.APK

APP名称:	葫芦侠3楼
包名:	com.huati
域名线索:	65条
URL线索:	66条
邮箱线索:	2条
分析日期:	2022年2月4日 11:13

文件信息

文件名: hlxsl.apk

文件大小: 9.02MB
MD5值: e9a8d9f4c1bb34da145f074d56510122
SHA1值: 39f6f0aa9aae5da781bb3a75fe36ef0cc0f25c86
SHA256值: be3a51141724ed8a7da8858a21601b74053dee04d81be28d46dd7690d05a923a

APP 信息

App名称: 葫芦侠3楼
包名: com.huati
主活动**Activity:** com.huluxia.ui.base.BBSAppStart
安卓版本名称: 3.5.0.22
安卓版本: 20141232

域名线索

域名	是否危险域名	服务器信息
yunpan.cn	good	**IP:** 36.110.213.149 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
ptlogin2.weiyun.com	good	**IP:** 109.244.244.141 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
tools.huluxia.net	good	**IP:** 42.81.61.107 **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
wap.huluxia.com	good	**IP:** 103.254.188.41 **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
v.qq.com	good	**IP:** 36.102.219.23 **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
cdn.u1.huluxia.com	good	**IP:** 42.81.245.1 **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

域名	是否危险域名	服务器信息
cgi.connect.qq.com	good	**IP:** 183.2.144.36 **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
search.huluxia.net	good	**IP:** 103.254.188.50 **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
appsupport.qq.com	good	**IP:** 183.2.144.86 **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
wspeed.qq.com	good	没有服务器地理信息.
s.p.qq.com	good	**IP:** 14.215.158.27 **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
test.tools.huluxia.net	good	没有服务器地理信息.
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
v.huluxia.com	good	**IP:** 183.129.249.120 **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
testmobile.qq.com	good	没有服务器地理信息.
dl.vmall.com	good	没有服务器地理信息.
sapi.skyhookwireless.com	good	**IP:** 52.76.182.201 **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
www.baidu.com	good	**IP:** 110.242.68.4 **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
xmlpull.org	good	**IP:** 74.50.61.58 **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
www.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map
goo.gl	good	**IP:** 142.251.43.14 **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
bb.huluxia.com	good	**IP:** 42.81.144.96 **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
appact.qzone.qq.com	good	**IP:** 121.51.179.156 **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
tieba.baidu.com	good	**IP:** 111.206.209.45 **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

域名	是否危险域名	服务器信息
img0.bdstatic.com	good	**IP:** 221.204.49.35 **所属国家:** China **地区:** Shanxi **城市:** Taiyuan **纬度:** 37.869438 **经度:** 112.560280 **查看地图:** Google Map
pingmid.qq.com	good	**IP:** 121.51.23.33 **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
reg.huluxia.net	good	**IP:** 42.81.245.1 **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
hlx.iweju.com	good	**IP:** 120.132.37.251 **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

域名	是否危险域名	服务器信息
stat.huluxia.com	good	**IP:** 42.81.144.96 **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
www.myapp.com	good	**IP:** 182.254.63.77 **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
test.bbs.huluxia.net	good	没有服务器地理信息.
query.hicloud.com	good	**IP:** 49.4.32.196 **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
cgi.qplus.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
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
www.huluxia.com	good	**IP:** 129.204.12.158 **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
version.check.huluxia.com	good	**IP:** 134.175.40.11 **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
v.youku.com	good	**IP:** 106.11.43.183 **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
oc.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
testupdate.hicloud.com	good	没有服务器地理信息.
www.winimage.com	good	**IP:** 198.50.170.91 **所属国家:** Canada **地区:** Quebec **城市:** Beauharnois **纬度:** 45.316780 **经度:** -73.865898 **查看地图:** Google Map
alog.umeng.co	good	没有服务器地理信息.
test.openmobile.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
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
share.weiyun.com	good	**IP:** 121.51.46.48 **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
skyhookwireless.com	good	**IP:** 96.45.82.232 **所属国家:** United States of America **地区:** Virginia **城市:** Reston **纬度:** 38.938862 **经度:** -77.346191 **查看地图:** Google Map
qzs.qq.com	good	**IP:** 182.254.54.167 **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
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
webpresence.qq.com	good	**IP:** 182.254.56.83 **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
upload.huluxia.net	good	**IP:** 129.204.46.114 **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
floor.huluxia.com	good	**IP:** 103.254.191.80 **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:** 106.11.86.76 **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
10.237.12.17	good	**IP:** 10.237.12.17 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.365078 **经度:** -71.104523 **查看地图:** Google Map
cdn2.huluxia.com	good	**IP:** 101.254.240.150 **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
openmobile.qq.com	good	**IP:** 113.96.208.233 **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
wifi.huluxia.net	good	**IP:** 61.160.249.33 **所属国家:** China **地区:** Jiangsu **城市:** Changzhou **纬度:** 31.783331 **经度:** 119.966667 **查看地图:** Google Map
bb.huluxia.net	good	**IP:** 183.129.249.120 **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
pan.baidu.com	good	**IP:** 110.242.69.43 **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
my.tv.sohu.com	good	**IP:** 211.159.191.76 **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
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
server.chat.huluxia.com	good	没有服务器地理信息.
log.umsns.com	good	**IP:** 59.82.31.210 **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
180.149.144.31	good	**IP:** 180.149.144.31 **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
lba.baidu.com	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
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://mta.qq.com/mta/api/ctr_feedback/add_feedback	com/tencent/stat/f.java
http://mta.qq.com/mta/api/ctr_feedback/get_feedback	com/tencent/stat/f.java
http://mta.qq.com/mta/api/ctr_feedback/reply_feedback	com/tencent/stat/f.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	com/tencent/stat/common/StatConstants.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/common/StatConstants.java
http://pingmid.qq.com:80/	com/tencent/mid/util/Util.java
http://cgi.qplus.com/report/report	com/tencent/jsutil/ReportUtils.java

URL信息	Url所在文件
http://cgi.connect.qq.com/qqconnectutil/sdk	com/tencent/jsutil/ReportUtils.java
http://s.p.qq.com/pub/check_bizup	com/tencent/jsutil/JsConfig.java
http://s.p.qq.com/pub/check_bizup?qver=	com/tencent/connect/a/b.java
http://qzs.qq.com/open/mobile/rate/sdk_rate.html?	com/tencent/open/SocialApiIml.java
http://appact.qzone.qq.com/appstore_activity_task_pcpush_sdk	com/tencent/open/TaskGuide.java
http://wspeed.qq.com/w.cgi	com/tencent/open/cgireport/ReportManager.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/sdkutil/ServerSetting.java
https://openmobile.qq.com/	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/sdkutil/ServerSetting.java
http://wspeed.qq.com/w.cgi	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/sdkutil/ServerSetting.java
http://qzs.qq.com/open/mobile/not_support.html?	com/tencent/sdkutil/ServerSetting.java
https://test.openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/sdkutil/ServerSetting.java

URL信息	Url所在文件
http://testmobile.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/sdkutil/ServerSetting.java
http://testmobile.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/sdkutil/ServerSetting.java
https://test.openmobile.qq.com/	com/tencent/sdkutil/ServerSetting.java
http://testmobile.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/sdkutil/ServerSetting.java
http://testmobile.qq.com/open/mobile/request/sdk_request.html?	com/tencent/sdkutil/ServerSetting.java
http://test.openmobile.qq.com	com/tencent/sdkutil/ServerSetting.java
http://www.myapp.com/forward/a/45592?g_f=990935	com/tencent/tauth/Tencent.java
http://webpresence.qq.com/getonline?Type=1&	com/tencent/tauth/Tencent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/tauth/Tencent.java
https://openmobile.qq.com/	com/tencent/tauth/Constants.java
https://openmobile.qq.com/weiyun/download_music	com/tencent/tauth/DownloadFileFromWeiyun.java
https://openmobile.qq.com/weiyun/download_photo	com/tencent/tauth/DownloadFileFromWeiyun.java
https://openmobile.qq.com/weiyun/get_photo_thumb	com/tencent/tauth/DownloadFileFromWeiyun.java
https://openmobile.qq.com/weiyun/download_video	com/tencent/tauth/DownloadFileFromWeiyun.java
http://lba.baidu.com/	com/baidu/location/BDLocation.java
https://sapi.skyhookwireless.com/wps2/location	com/baidu/location/b/k.java

URL信息	Url所在文件
http://loc.map.baidu.com/tcu.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/wloc	com/baidu/location/b/k.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/b/k.java
http://loc.map.baidu.com/statloc	com/baidu/location/b/o.java
http://180.149.144.31:8091/offline_loc	com/baidu/location/c/d.java
http://loc.map.baidu.com/offline_loc	com/baidu/location/c/d.java
http://%s/%s	com/baidu/location/c/a.java
http://loc.map.baidu.com/cc.php	com/baidu/location/e/i.java
http://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/e/i.java
http://skyhookwireless.com/wps/2005	com/baidu/location/g/b.java
http://testupdate.hicloud.com:8180/plugintest/v2/CheckEx.action	com/huawei/deviceCloud/microKernel/config/UpdateConstant.java
http://query.hicloud.com/HwCloudSDK/v2/CheckEx.action	com/huawei/deviceCloud/microKernel/config/UpdateConstant.java

URL信息	Url所在文件
http://stat.huluxia.com/downstat/install/begin	com/huluxia/f.java
http://stat.huluxia.com/downstat/install/complete	com/huluxia/f.java
http://stat.huluxia.com/downstat/error	com/huluxia/f.java
http://stat.huluxia.com/stat/gamedown	com/huluxia/f.java
http://stat.huluxia.com/stat/service/event	com/huluxia/f.java
http://stat.huluxia.com/downstat/down/begin	com/huluxia/f.java
http://stat.huluxia.com/downstat/down/complete	com/huluxia/f.java
http://pan.baidu.com/	com/huluxia/module/GameInfo.java
http://dl.vmall.com/	com/huluxia/module/GameInfo.java
http://yunpan.cn/	com/huluxia/module/GameInfo.java
http://v.youku.com/	com/huluxia/module/GameInfo.java
http://my.tv.sohu.com/	com/huluxia/module/GameInfo.java
http://v.qq.com/	com/huluxia/module/GameInfo.java
http://search.huluxia.net	com/huluxia/module/j.java
http://test.tools.huluxia.net	com/huluxia/module/j.java
http://test.bbs.huluxia.net	com/huluxia/module/j.java

URL信息	Url所在文件
http://tools.huluxia.net	com/huluxia/module/j.java
http://server.chat.huluxia.com	com/huluxia/module/j.java
http://floor.huluxia.com	com/huluxia/module/j.java
http://floor.huluxia.com/friendship/follow	com/huluxia/module/j.java
http://reg.huluxia.net/game/downloadlimitsize.txt	com/huluxia/module/j.java
http://upload.huluxia.net/upload/file	com/huluxia/module/feedback/a.java
http://img0.bdstatic.com/img/image/shouye/mntsc-11681494554.jpg	com/huluxia/module/area/detail/e.java
http://img0.bdstatic.com/img/image/shouye/mnqz-11867945883.jpg	com/huluxia/module/area/detail/e.java
http://img0.bdstatic.com/img/image/shouye/mntsc-11681494554.jpg	com/huluxia/module/area/spec/l.java
http://test.tools.huluxia.net	com/huluxia/http/base/b.java
http://tools.huluxia.net	com/huluxia/http/base/b.java
http://upload.huluxia.net	com/huluxia/http/base/b.java
http://hlx.iweju.com	com/huluxia/http/base/b.java
http://floor.huluxia.com	com/huluxia/http/base/b.java
http://test.bbs.huluxia.net	com/huluxia/http/base/a.java
http://floor.huluxia.com	com/huluxia/http/base/a.java

URL信息	Url所在文件
http://www.huluxia.com/course/search	com/huluxia/http/game/c.java
http://version.check.huluxia.com/hlx_iccgame	com/huluxia/http/other/j.java
http://version.check.huluxia.com/hlx_tool	com/huluxia/http/other/j.java
http://version.check.huluxia.com/hlx_floor	com/huluxia/http/other/j.java
http://version.check.huluxia.com/test	com/huluxia/http/other/j.java
http://v.huluxia.com/video_number.txt	com/huluxia/http/other/d.java
http://bb.huluxia.net/h5game/	com/huluxia/ui/home/DiscoveryLayout.java
http://v.huluxia.com	com/huluxia/ui/home/DiscoveryLayout.java
http://bb.huluxia.com/bbs/jifen.html	com/huluxia/ui/profile/ProfileScoreActivity.java
http://bb.huluxia.com/bbs/hulu.html	com/huluxia/ui/profile/ProfileScoreActivity.java
http://reg.huluxia.net/game/2015/10/23/baidu.html	com/huluxia/ui/game/NetPanNewActivity.java
http://reg.huluxia.net/game/2015/10/23/qihoo.html	com/huluxia/ui/game/NetPanNewActivity.java
http://reg.huluxia.net/game/2015/10/23/weiyun.html	com/huluxia/ui/game/NetPanNewActivity.java
http://share.weiyun.com/	com/huluxia/ui/game/NetPanNewActivity.java
http://ptlogin2.weiyun.com/jump?	com/huluxia/ui/game/NetPanNewActivity.java
http://tieba.baidu.com/p/3219122263	com/huluxia/widget/Constants.java

URL信息	Url所在文件
http://wifi.huluxia.net/wifi/saveBatch	com/huluxia/utils/az.java
http://pan.baidu.com/api/sharedownload	com/huluxia/utils/g.java
http://pan.baidu.com/api/getcaptcha	com/huluxia/utils/g.java
http://wifi.huluxia.net/wifi/saveBatch	com/huluxia/utils/UtilsWifiDatabase.java
http://wap.huluxia.com	com/huluxia/utils/ah.java
http://cdn2.huluxia.com/avatar/1/201406/19/07ceb0ca9fcbea5f84f528b1be9535fc.png_80x80.jpeg	com/huluxia/utils/ah.java
http://pan.baidu.com/api/sharedownload	com/huluxia/utils/as.java
http://pan.baidu.com/api/getcaptcha	com/huluxia/utils/as.java
http://bb.huluxia.net/idol	com/huluxia/utils/gameplugin/a.java
http://bb.huluxia.net/tool/help/	com/huluxia/utils/gameplugin/a.java
http://reg.huluxia.net/game/2014/11/root/BoomBeachPatch.json	com/huluxia/utils/gameplugin/a.java
http://cdn.u1.huluxia.com/g1/M00/CB/04/wKgBB1XgSe-AG3mhAAALwQuN1SE568.png	com/huluxia/data/game/c.java
http://cdn.u1.huluxia.com/g1/M00/CB/04/wKgBB1XgSgaAaO7AAAATdzek9P8465.png	com/huluxia/data/game/c.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/smack/r.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/smack/i.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/smack/o.java

URL信息	Url所在文件
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/smack/packet/d.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/smack/util/c.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/smack/provider/c.java
http://www.w3.org/XML/1998/namespace	com/xiaomi/kenai/jbosh/ai.java
http://www.w3.org/XML/1998/namespace	com/xiaomi/kenai/jbosh/r.java
http://%1$s/gslb/gslb/getbucket.asp?ver=3.0	com/xiaomi/network/HostManager.java
http://%1$s/diagnoses/v1/report	com/xiaomi/network/UploadHostStatHelper.java
www.baidu.com	com/xiaomi/push/service/u.java
www.baidu.com:	com/xiaomi/push/service/u.java
http://10.237.12.17:9085/pass/register	com/xiaomi/push/service/g.java
http://goo.gl/rb6C2Y	Android String Resource
http://www.winimage.com/zLibDll	lib/x86/libInstallMod.so
http://www.winimage.com/zLibDll	lib/armeabi/libInstallMod.so

邮箱线索

邮箱地址	所在文件
eray.jiang@gmail.com	com/system/util/ay.java
n请将投诉信息发送至邮箱xiaosong@huluxia.com	com/huluxia/ui/loginAndRegister/PolicyActivity.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.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.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.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_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

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.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
com.android.launcher.permission.INSTALL_SHORTCUT	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.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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.huati	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
com.huati.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.huati.permission.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
com.huati.permission.ACCESS_DOWNLOAD_MANAGER_ADVANCED	未知	Unknown permission	Unknown permission from android reference
com.huati.permission.SEND_DOWNLOAD_COMPLETED_INTENTS	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.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.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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.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。

向手机申请的权限	是否危险	类型	详细情况
com.android.launcher.permission.READ_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.GET_TASKS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.ACCESS_COARSE_LOCATION	未知	Unknown permission	Unknown permission from android reference
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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Guangdong, L=Guangzhou, O=huluxia, OU=huluxia, CN=huluxia
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-11-29 19:49:35+00:00
Valid To: 2113-11-05 19:49:35+00:00
Issuer: C=CN, ST=Guangdong, L=Guangzhou, O=huluxia, OU=huluxia, CN=huluxia
Serial Number: 0x7dc84ba3
Hash Algorithm: sha256
md5: 345452757f4aede24c5627be65dfe64f
sha1: 49f4145d8007dc71c77d7f83bf6e722c1fae0cf4
sha256: 60d5241e149cbac47f2eb36053332934c02572f5d6f1ede8a4523e19027fac79

sha512: cd8d2b2abe694fccdf632f14892118878ccf184c362bcf6db07d6d9109911784ce3a1e739b30717128a0c7c781df247aedca7e43e0ea9ca8739417fa126bddcf

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Tencent MTA	Analytics	https://reports.exodus-privacy.eu.org/trackers/114
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"send_no_user" : "暂无文件接收者"
"deleted_key" : "%1$s deleted"
"forgetPassword" : "找回密码"
"root_kinguser" : "使用kinguser工具获取手机权限"
"send_no_user" : "Tidak ada koneksi"
"send_no_user" : "暂无文件接收者"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent100580922://,

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.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check 编译器 / dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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
SIM operator check
network operator name check
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>assets/HiAnalytics.plugin!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>network operator name check
device ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>assets/frontia_plugin/plugin-deploy.jar!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
network operator name check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>