MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

放大镜 222.22.38.APK

APP名称:	放大镜
包名:	com.polaris.magnifier
域名线索:	11条
URL线索:	10条
邮箱线索:	3条
分析日期:	2022年1月28日 22:02

文件信息

文件名: fangdajing9098.apk
文件大小: 7.66MB
MD5值: 217fa574d14d004812b1f89969505c08
SHA1值: 0aea6e3bf30e5482c47db12bc6bd2e11e04944f8
SHA256值: 0b26d47d38e0ac48b4c5d4863ad5fb3f610a0a6f445c369ac242604d76cf9733

APP 信息

App名称: 放大镜
包名: com.polaris.magnifier
主活动**Activity:** com.polaris.magnifier.MySplashNewActivity
安卓版本名称: 222.22.38
安卓版本: 2222238

域名线索

域名	是否危险域名	服务器信息
mon.snssdk.com	good	**IP:** 182.254.59.213 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
plugin-patch-api.bytedance.com	good	**IP:** 36.99.32.251 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.samsungapps.com	good	**IP:** 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map
cpu.baidu.com	good	**IP:** 112.80.248.129 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.chengzijianzhan.com	good	**IP:** 27.128.221.195 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
sf6-ttcdn-tos.pstatp.com	good	**IP:** 42.81.247.46 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
i.snssdk.com	good	**IP:** 123.246.197.149 **所属国家:** China **地区:** Liaoning **城市:** Fushun **纬度:** 41.855831 **经度:** 123.923332 **查看地图:** Google Map
www.toutiaopage.com	good	**IP:** 124.238.243.100 **所属国家:** China **地区:** Hebei **城市:** Langfang **纬度:** 39.509720 **经度:** 116.694717 **查看地图:** Google Map
apps.oceanengine.com	good	**IP:** 36.99.228.223 **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
imgcache.qq.com	good	**IP:** 121.51.172.229 **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
sdk.e.qq.com	good	**IP:** 58.250.137.37 **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

URL线索

URL信息	Url所在文件
https://mon.snssdk.com/monitor/appmonitor/v2/settings	com/bytedance/pangle/helper/d.java
https://mon.snssdk.com/monitor/collect/	com/bytedance/pangle/helper/d.java
https://plugin-patch-api.bytedance.com/api/plugin/config/v2/	com/bytedance/pangle/download/e.java
http://sdk.e.qq.com/activate	com/qq/e/comm/b/a.java
http://sdk.e.qq.com/launch	com/qq/e/comm/b/a.java
https://imgcache.qq.com/gdt/cdn/adn/uniondoc/ylh_sdk_privacy_statement.html	com/polaris/magnifier/PrivacyActivity.java
https://cpu.baidu.com/1022/eff0ce37?scid=42192	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1001/eff0ce37?scid=42193	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1002/eff0ce37?scid=42194	com/polaris/magnifier/cpu/a/b.java

URL信息	Url所在文件
https://cpu.baidu.com/1021/eff0ce37?scid=42195	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1024/eff0ce37?scid=42196	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1080/eff0ce37?scid=42197	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1033/eff0ce37?scid=42198	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1025/eff0ce37?scid=42199	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1009/eff0ce37?scid=42200	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1006/eff0ce37?scid=42201	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1008/eff0ce37?scid=42202	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1034/eff0ce37?scid=42203	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1043/eff0ce37?scid=42204	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1042/eff0ce37?scid=42205	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1065/eff0ce37?scid=42206	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1013/eff0ce37?scid=42207	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1035/eff0ce37?scid=42208	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1040/eff0ce37?scid=42209	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1055/eff0ce37?scid=42210	com/polaris/magnifier/cpu/a/b.java

URL信息	Url所在文件
https://cpu.baidu.com/1007/eff0ce37?scid=42211	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1005/eff0ce37?scid=42212	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1089/eff0ce37?scid=82306	com/polaris/magnifier/cpu/a/b.java
https://cpu.baidu.com/1093/eff0ce37?scid=82307	com/polaris/magnifier/cpu/a/b.java
www.chengzijianzhan.com	com/ss/android/downloadlib/addownload/compliance/b.java
www.toutiaopage.com/tetris/page	com/ss/android/downloadlib/addownload/compliance/b.java
https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/b.java
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
https://www.samsungapps.com/appquery/appDetail.as?appId=	com/ss/android/downloadlib/g/h.java
https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java

邮箱线索

邮箱地址	所在文件
answer626@163.com	com/polaris/magnifier/FeedbackActivity.java
yizhi_tech@163.com	com/polaris/magnifier/PrivacyActivity.java

邮箱地址	所在文件
您可以通过yizhi_tech@163.com联系我们 您随时可以通过yizhi_tech@163.com联系我们	com/polaris/magnifier/UserClauseActivity.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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_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.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。
com.polaris.magnifier.openadsdk.permission.TT_PANGOLIN	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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=Shanghai, L=Shanghai, O=Liu Miao, OU=PolarisTech, CN=Liu Miao
Signature Algorithm: rsassa_pkcs1v15

Valid From: 2017-04-03 14:53:59+00:00
Valid To: 2117-03-10 14:53:59+00:00
Issuer: C=86, ST=Shanghai, L=Shanghai, O=Liu Miao, OU=PolarisTech, CN=Liu Miao
Serial Number: 0x6a289e28
Hash Algorithm: sha256
md5: 0eada6cd63f57763ff8fe20eb6dfdbe0
sha1: 43ae3c24ec866a1244424a908c6bb03eb003a436
sha256: d5ed79c3fc9c79fea946e57e83729caac9bdb230082c20a454a88bb714d374f2
sha512: 73a0ef08ae953b01b3601401738a9e42f1e20357a1d4f6c0aa185101e636b3cc3934cff950444bbfb5c33d73e467cebeab2130e4d30e327a16170ed3e10d9d85
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 1fa60df7237866e74e570923741a82cf61b760ece06a313d1e0067d9e92e1fcb

Exodus威胁情报

名称	分类	URL链接
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/1d7842c4752cfad2ae1855d9ce1d687a!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
SIM operator check
network operator name check
subscriber ID check
network interface name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!assets/yaq3_0.sec</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/gdt_plugin/gdtadv2.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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
</table>

<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.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
