MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

准点倒数日 3.0.2.APK

APP名称:	准点倒数日
包名:	com.bee.cdday
域名线索:	41条
URL线索:	56条
邮箱线索:	0条
分析日期:	2022年2月3日 13:15

文件信息

文件名: zddsr.apk
文件大小: 6.9MB
MD5值: 1f822b68f126e4dceb9825ddf300a3e2
SHA1值: ee891f6b1fed28645866e18f092d1834516f6325
SHA256值: dfa9284759b76c547ac5c72d2317958d7604ad6439e3260880cbed9184f2ad38

APP 信息

App名称: 准点倒数日
包名: com.bee.cdday
主活动**Activity:** com.bee.cdday.SplashActivity
安卓版本名称: 3.0.2
安卓版本: 30002

域名线索

域名	是否危险域名	服务器信息
app.qq.com	good	**IP:** 182.254.51.124 **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
api.weixin.qq.com	good	**IP:** 109.244.145.152 **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
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map
api.applink.mob.com	good	**IP:** 203.107.55.19 **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
issuetracker.google.com	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
lks.share.mob.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
www.mob.com	good	**IP:** 116.62.130.46 **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
errlog.umeng.com	good	**IP:** 106.8.130.60 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.
p.share.mob.com	good	没有服务器地理信息.
alogsus.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
developer.umeng.com	good	**IP:** 59.82.31.160 **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
service.weibo.com	good	**IP:** 49.7.40.133 **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
api.u.mob.com	good	没有服务器地理信息.
astat.bugly.cros.wr.pvp.net	good	**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 **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
android.bugly.qq.com	good	**IP:** 109.244.244.35 **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
api.utag.mob.com	good	没有服务器地理信息.
graph.qq.com	good	**IP:** 113.96.208.232 **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
open.weibo.cn	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
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
i.open.t.sina.com.cn	good	没有服务器地理信息.
ulogs.umengcloud.com	good	**IP:** 106.11.86.69 **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
qzs.qq.com	good	**IP:** 182.254.48.69 **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
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
login.sina.com.cn	good	**IP:** 49.7.36.166 **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
gwtools.redbeeai.com	good	**IP:** 101.132.188.145 **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.sdk.mob.com	good	**IP:** 203.107.55.19 **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
alogus.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
aaid.umeng.com	good	**IP:** 106.8.130.61 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
api.data.sentinel.mob.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
pslog.umeng.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
ns.adobe.com	good	没有服务器地理信息.
api.manager.sentinel.mob.com	good	没有服务器地理信息.
weibo.com	good	**IP:** 180.149.138.246 **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
feedback.redbeeai.com	good	**IP:** 47.102.147.84 **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
config.redbeeai.com	good	**IP:** 139.196.45.82 **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
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
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
api.config.sentinel.mob.com	good	没有服务器地理信息.
ulogs.umeng.com	good	**IP:** 106.11.43.144 **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://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/i/c.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/d/a.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/d/a.java
https://login.sina.com.cn/visitor/signin	com/weibo/ssosdk/WeiboSsoSdk.java
http://api.u.mob.com	com/mob/MobUser.java
http://api.utag.mob.com/bdata	com/mob/commons/utag/UserTager.java
http://api.utag.mob.com/conf	com/mob/commons/utag/TagRequester.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.java
http://api.data.sentinel.mob.com	com/mob/mobapm/core/d.java
http://api.manager.sentinel.mob.com	com/mob/mobapm/core/d.java
http://api.config.sentinel.mob.com	com/mob/mobapm/core/d.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java

URL信息	Url所在文件
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.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://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/i.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://api.weibo.com/oauth2/access_token	com/sina/weibo/sdk/b/f.java
https://service.weibo.com/share/mobilesdk_uppic.php	com/sina/weibo/sdk/b/e.java

URL信息	Url所在文件
http://i.open.t.sina.com.cn/mobilesdk/sendmessage.php	com/sina/weibo/sdk/b/d.java
https://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/WebActivity.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/web/WebActivity.java
https://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/b/d.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/auth/a.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
http://gwtools.redbeeai.com/daoshuri/html/agreeandprivate/private.html	b/b/a/e/a.java
http://gwtools.redbeeai.com/daoshuri/html/agreeandprivate/agree.html	b/b/a/e/a.java
http://schemas.android.com/apk/res-auto	b/e/a/a/k/a.java
https://config.redbeeai.com/	b/d/b/f/a.java

URL信息	Url所在文件
http://feedback.redbeeai.com	b/d/c/g/b.java
https://feedback.redbeeai.com	b/d/c/g/b.java
https://){1}	cn/sharesdk/framework/b/a.java
http://p.share.mob.com/tags/getTagList	cn/sharesdk/framework/authorize/f.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com	cn/sharesdk/tencent/qq/c.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile	cn/sharesdk/tencent/qq/a.java
http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk	cn/sharesdk/tencent/qq/a.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/photo/upload_pic	cn/sharesdk/tencent/qzone/b.java

URL信息	Url所在文件
http://api.applink.mob.com	cn/sharesdk/loopshare/utils/h.java
http://lks.share.mob.com/share/shareLog	cn/sharesdk/sina/weibo/b.java
http://weibo.com/	cn/sharesdk/sina/weibo/SinaWeibo.java
http://service.weibo.com/share/mobilesdk_uppic.php	cn/sharesdk/sina/weibo/h.java
http://service.weibo.com/share/mobilesdk.php?	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/oauth2/default.html	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/oauth2/access_token	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/users/show.json	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/friendships/create.json	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/friendships/friends/bilateral.json	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/friendships/followers.json	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/friendships/friends.json	cn/sharesdk/sina/weibo/i.java
https://api.weibo.com/2/statuses/user_timeline.json	cn/sharesdk/sina/weibo/i.java
http://lks.share.mob.com/share/genShareInfo	cn/sharesdk/sina/weibo/a.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/h.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/h.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/z.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/i0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/j.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/q.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/a.java
http://schemas.android.com/apk/res/android	a/j/c/l/i.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	a/z/y0.java
http://ns.adobe.com/xap/1.0/	a/p/a/a.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
http://www.mob.com/policy/en	Android String Resource
http://www.mob.com	Android String Resource
http://www.mob.com/policy/zh	Android String Resource

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=chif
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-24 03:03:46+00:00
Valid To: 2120-10-31 03:03:46+00:00
Issuer: CN=chif
Serial Number: 0xb0372bc
Hash Algorithm: sha256
md5: d16fee776451e070a695289af952531d
sha1: 35638a41c2c5dedcb4419e9e3032911dc27dbc40
sha256: 471f209d7c513653c69b5b3674928d4ec9757e971f826d66cd6b6ff13d730bd7
sha512: 544cf97ab91dfa616cb982c60d565154a80f6b6d84f71e4e59a38e0cac5e5cfb3fb555e509af3bda4decf6b1624c7756b5336f5b6541eb580418a69d2197ef92
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 91eab2d2985d4642cb68eaeb2ead22e1d7d280bd54ffb788c42193f348ee0f6b

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"

可能的敏感信息
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent1111682237://,
cn.sharesdk.loopshare.LoopShareActivity	Schemes: ssdk33fc2258e4b11://, Hosts: cn.sharesdk.loop,

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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
