MoGua

DailyTask 2.0.0.APK 分析报告

APP名称:	DailyTask

包名:	com.alibaba.android.komcuz
域名线索:	11条
URL线索:	20条
邮箱线索:	0条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: DT_20241231_2.0.0.apk
文件大小: 9.03MB
MD5值: 26db666b20a6b651c6ebd50ee4c25c2b
SHA1值: a44556fe9db2bc434a51bc45556d337ca6496237
SHA256值: d41d3ece94c60442cfe18e69a1fdfeb8c322023150a924845db8d0fa72a0b502

APP 信息

App名称: DailyTask
包名: com.alibaba.android.komcuz
主活动Activity: com.pengxh.daily.app.ui.MainActivity
安卓版本名称: 2.0.0
安卓版本: 2000

域名线索

域名	服务器信息
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.eclipse.org	**IP**: 198.41.30.198 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
greenrobot.org	**IP**: 85.13.163.69 **所属国家**: Germany **地区**: Thuringen

	城市: Friedersdorf **纬度**: 50.604919 **经度**: 11.035770
wiki.eclipse.org	**IP**: 198.41.30.195 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
tools.ietf.org	**IP**: 104.16.44.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
astat.bugly.cros.wr.pvp.net	**IP**: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
	IP: 119.28.121.133

astat.bugly.qcloud.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
netty.io	**IP**: 172.67.130.186 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://tools.ietf.org/html/rfc7540	io/netty/handler/codec/http2/HttpConversionUtil.java

https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
http://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java
http://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
http://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
https://github.com/AndroidCoderPeng/DailyTask/issues/27\	摸瓜V2引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=北京市, L=海淀区, OU=Casic, CN=Peng
签名算法: dsa
有效期自: 2024-12-24 01:54:15+00:00
有效期至: 2034-12-22 01:54:15+00:00
发行人: C=CN, ST=北京市, L=海淀区, OU=Casic, CN=Peng
序列号: 0x3bb638e5
哈希算法: sha256
md5值: 8e71a97c43cad1d52e18be08ab00bf9c
sha1值: 8ed587e727893fb3b9d3b3dac6562220c12f0d75
sha256值: 084a3aad1b82bf4f09099c9f23bbc569275b6e5fa2748bcd63f4747469a61a4b
sha512值: 9ef144c4cd72dd1b98e57f0a3c7c1eb248bdd8a1cc3b60d11f7f1e3a96e6635ae77923275c277550219301d14191d6c7603fbc6d9a08e1150da3807a52e4418f
公钥算法: dsa
密钥长度: 2048
指纹: dad3d4b158313176877312de569b6b0656dd58205f10e993254fecfd16d5e354

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.POST_NOTIFICATIONS	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

com.alibaba.android.komcuz.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信