MoGua

Destek AI 1.8.28.APK 分析报告

APP名称: Destek AI

包名:	com.hengxin.hengxinAi
域名线索:	9条
URL线索:	8条
邮箱线索:	1条
分析日期:	2024年10月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app.apk
文件大小: 11.14MB
MD5值: 53d026557cdda9e7f76e4483ad27933b
SHA1值: cb5b78c72a2b83acb881060be5e184ea45721ee7
SHA256值: e80bc75846cc48b1e8b3c486778b37447337a488d4d5c83053c81b39ff280bec

APP 信息

App名称: Destek AI
包名: com.hengxin.hengxinAi
主活动Activity: com.hengxin.hengxinAi.MainActivity
安卓版本名称: 1.8.28
安卓版本: 2096

域名线索

域名	服务器信息
www.google.com	**IP**: 31.13.106.4 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
developer.android.com	**IP**: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
app.mi.com	**IP**: 123.125.102.202 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.jsdelivr.com	**IP**: 172.67.208.113 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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
a.app.qq.com	**IP**: 60.28.219.32 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ns.adobe.com	没有服务器地理信息.
play.google.com	**IP**: 8.7.198.46 **所属国家**: United States of America **地区**: Louisiana **城市**: Monroe **纬度**: 32.548328 **经度**: -92.045235

URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	h/a/c/d/e.java
https://play.google.com/store/apps/details?id=	com/example/r_upgrade/common/j/a.java
http://www.google.com	com/example/r_upgrade/common/j/a.java
https://a.app.qq.com/o/simple.jsp?pkgname=	com/example/r_upgrade/common/j/b.java
https://app.mi.com/details?id=	com/example/r_upgrade/common/j/c.java
https://app.mi.com	com/example/r_upgrade/common/j/c.java
http://ns.adobe.com/xap/1.0/\u0000	e/d/a/a.java
http://undefined/	j/b/g/d.java
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2023-07-14 02:08:40+00:00
有效期至: 2123-06-20 02:08:40+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x8e0eb44
哈希算法: sha256
md5值: c92109bc4f896e8423bf35c016ec661e
sha1值: e4e3488a0c89cb7efe38effc1b4ebbeae8e4781d
sha256值: df751ac06850bb246c9eef4df0a482b85c1dbf99e2a0099cfb0f57945870c11f
sha512值: 226a1e3d36ddb3cad66b11534e927801afcb65c632d55f5f9af7cedf4a5740daa4b3499f12316378da0e32ceb4d37785abc8f5978b6eccefb772d9210ede6bb1
公钥算法: rsa
密钥长度: 2048
指纹: 2536a3fc01f39ea280bb82e605c1f996028cdf69140c93eb5db4c62938585ff3

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.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_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。
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序

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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

应用内通信
