MoGua

HF UFO 1.2.5.APK 分析报告

APP名称: HF UFO

包名:	com.hfufo.rxdrone
域名线索:	5条
URL线索:	5条
邮箱线索:	1条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: HF UFO_1.2.5_Apkpure.apk
文件大小: 71.39MB
MD5值: 3a2ec8927debeaf18454684197644d8d
SHA1值: c79db28bcb987ec2ab5ef5ada40650258f311cc7
SHA256值: 29967f0b95412a9c5e50dadb8a075ff88e3e2930941ddf8e7c5bfca08bbd547f

APP 信息

App名称: HF UFO
包名: com.hfufo.rxdrone
主活动Activity: com.hfufo.rxdrone.MainActivity
安卓版本名称: 1.2.5
安卓版本: 25

域名线索

域名	服务器信息
www.baidu.com	**IP**: 110.242.68.4 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
dev.zhthinkjoy.com	没有服务器地理信息.
www.mob.com	**IP**: 45.113.201.237 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600

schemas.android.com	没有服务器地理信息.
www.google.com	**IP**: 104.244.43.136 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446

URL线索

URL**信息**	Url**所在文件**
http://%s:%d/	com/jieli/lib/stream/tools/ParseHelper.java
http://dev.zhthinkjoy.com:8082/platform-api/service	com/thinkjoy/zhthinkjoygesturedetectlib/ZHThinkjoyGesture.java
https://www.google.com/search?q=download++MP3+music&oq=download++MP3+music	com/videooperate/activity/MusicLibraryActivity.java
https://www.baidu.com/s?wd=download%20%20MP3%20music&oq=download%2520MP%2526lt%253B%2520music	com/videooperate/activity/MusicLibraryActivity.java
http://schemas.android.com/apk/res/android	com/videooperate/view/SegmentTabLayout.java
http://www.mob.com	Mogua Engine V1

邮箱线索

邮箱地址	**所在文件**
wifi@baidu.com	com/fh/hdutil/IConstant.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-05-15 09:58:44+00:00
有效期至: 2048-05-15 09:58:44+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xf769229998aef3219b54d59094019aebab280340
哈希算法: sha256
md5值: e08c77cb374af50d12913ed0cf7227fc
sha1值: 8b8cfc51e17d328ebe9ce6abc7f2a598f0f04063
sha256值: c2fe6c1f9edd044dd8c221f3833d37a3b42fe67bfd5d9ab17adcb8ace1271b75
sha512值: b641fdcf29dd7079f4d2fbd7590b02bd585cdf48cd43aa963fafacb49d4a991e6e565b9ae3ed11cc75f2cbd8744e9e1ca472d4fd30aca77a4989deb4a6331da5
公钥算法: rsa
密钥长度: 4096
指纹: 2a0d31f432267dad53eb9a8a6089f26120ef83ea569069bdbe8ca4d95e1e58d3

硬编码敏感信息

可能的敏感信息
"input_pwd" : "Input password"
"pwd" : "Password:"
"pwd_diff" : "The two passwords do not match!"
"pwd_length_tipes" : "Password length is greater than or equal to a minimum of 5 characters"
"pwd_level_0" : "Password Level: Very weak"
"pwd_level_1" : "Password Level: Weak"
"pwd_level_3" : "Password Level: Medium"
"pwd_level_4" : "Password Level: Strong"
"pwd_level_5" : "Password Level: Very strong"
"pwd_modification" : "Password modification"
"pwd_setting" : "seting..."
"pwd_setting_failed" : "Password set failed!"
"pwd_setting_success" : "Password set success!"
"save_pwd" : "save"
"setting_pwd" : "Password set"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

"input_pwd" : "Passwort eingeben"
"pwd" : "Kennwort:"
"pwd_diff" : "The two passwords do not match!"
"pwd_length_tipes" : "Password length is greater than or equal to a minimum of 5 characters"
"pwd_level_0" : "Password Level: Very weak"
"pwd_level_1" : "Password Level: Weak"
"pwd_level_3" : "Password Level: Medium"
"pwd_level_4" : "Password Level: Strong"
"pwd_level_5" : "Password Level: Very strong"
"pwd_modification" : "Password modification"
"pwd_setting" : "seting..."
"pwd_setting_failed" : "Password set failed!"
"pwd_setting_success" : "Password set success!"
"save_pwd" : "Speichern"
"setting_pwd" : "Passwort-Satz"
"input_pwd" : "Input password"
"pwd" : "Password:"

"pwd_diff" : "The two passwords do not match!"

"pwd_length_tipes" : "Password length is greater than or equal to a minimum of 5 characters"

"pwd_level_0" : "Password Level: Very weak"

"pwd_level_1" : "Password Level: Weak"

"pwd_level_3" : "Password Level: Medium"

"pwd_level_4" : "Password Level: Strong"

"pwd_level_5" : "Password Level: Very strong"

"pwd_modification" : "Password modification"

"pwd_setting" : "seting..."

"pwd_setting_failed" : "Password set failed!"

"pwd_setting_success" : "Password set success!"

"save_pwd" : "save"

"setting_pwd" : "Password set"

"ssdk_instapaper_pwd" : "密码"

"ssdk_weibo_oauth_regiseter" : "应用授权"

"input_pwd" : "Input password"

"pwd" : "Password:"

"pwd_diff" : "The two passwords do not match!"

"pwd_length_tipes" : "Password length is greater than or equal to a minimum of 5 characters"
"pwd_level_0" : "Password Level: Very weak"
"pwd_level_1" : "Password Level: Weak"
"pwd_level_3" : "Password Level: Medium"
"pwd_level_4" : "Password Level: Strong"
"pwd_level_5" : "Password Level: Very strong"
"pwd_modification" : "Password modification"
"pwd_setting" : "seting..."
"pwd_setting_failed" : "Password set failed!"
"pwd_setting_success" : "Password set success!"
"save_pwd" : "save"
"setting_pwd" : "Password set"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"input_pwd" : "Input password"
"pwd" : "Password:"
"pwd_diff" : "The two passwords do not match!"

"pwd_length_tipes" : "Password length is greater than or equal to a minimum of 5 characters"
"pwd_level_0" : "Password Level: Very weak"
"pwd_level_1" : "Password Level: Weak"
"pwd_level_3" : "Password Level: Medium"
"pwd_level_4" : "Password Level: Strong"
"pwd_level_5" : "Password Level: Very strong"
"pwd_modification" : "Password modification"
"pwd_setting" : "seting..."
"pwd_setting_failed" : "Password set failed!"
"pwd_setting_success" : "Password set success!"
"save_pwd" : "save"
"setting_pwd" : "Password set"

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.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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.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
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位

		提供程序命令	置源的操作
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

应用内通信
