MoGua

HC蓝牙助手 1.5.0.APK 分析报告

APP名称:	HC蓝牙助手

包名:	com.hc.mixthebluetooth
域名线索:	5条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: HC蓝牙助手v1.5.0(兼容到Android13).apk
文件大小: 3.64MB
MD5值: 28155fa6402d416a462b984545747828
SHA1值: dfc7e903503cfef1c8321f193cd4c517ea4966fc
SHA256值: 931fb6b9332b0681ac251aa69e1d100fb0e94542bb912553b6389430fc44ea29

APP 信息

App名称: HC蓝牙助手
包名: com.hc.mixthebluetooth
主活动Activity: com.hc.mixthebluetooth.activity.MainActivity
安卓版本名称: 1.5.0
安卓版本: 1

域名线索

域名	服务器信息
xml.org	**IP**: 104.239.142.8 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
pan.baidu.com	**IP**: 110.242.69.176 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.hc01.com	**IP**: 61.48.83.205 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL**信息**	Url**所在文件**
http://)?([\\w-]+\\.)+[\\w-]+(:\\d+)*(/[\\w-	cn/hutool/core/lang/PatternPool.java
http://xml.apache.org/xslt	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/disallow-doctype-decl	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-general-entities	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-parameter-entities	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java

http://www.hc01.com/download	com/hc/mixthebluetooth/activity/HIDActivity.java
https://pan.baidu.com/s/1oO97-wgyiQh8P9DHHFNt8A	com/hc/mixthebluetooth/activity/HIDActivity.java
http://www.hc01.com/download	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java

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=CN, ST=GD, L=GZ, O=HC, OU=HC, CN=Lgx
签名算法: rsassa_pkcs1v15
有效期自: 2019-07-05 02:38:26+00:00
有效期至: 2044-06-28 02:38:26+00:00
发行人: C=CN, ST=GD, L=GZ, O=HC, OU=HC, CN=Lgx
序列号: 0x162a921c
哈希算法: sha256
md5值: 85dd932f745e6b0f9dc2633098cbe2d0
sha1值: ffb256d2db459bddbca8f4349a82a3975f8fe403
sha256值: 7edc0315ba2d5359c0dd73f01f04edce6d09632c05ab14060efb4c1fde93cfce
sha512值: 148cda5457f684efbb16e2e7279286a86dff4330dd6fb5f170ac0d338baa7ad3939080e7b946be45632c2446a8eb958f8dc56a64602089e93985d824ed035f47

公钥算法: rsa
密钥长度: 2048
指纹: c51a4c4cb6714a442d2a0a33a9da3f46dd724e2853fad803f600572a4d55634e

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
			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

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference
android.Manifest.permission#BLUETOOTH	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 **摸瓜APK反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。