Evaluation Warning: The document was created with Spire.Doc for Python.

**Heat Live（ 4.8.4版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | Heat Live |
| 版本 | 4.8.4 |
| 包名 | com.google.heatlive |
| 域名线索 | 13条 |
| URL线索 | 15条 |
| APP图标 |  |
| 分析日期 | 2025年8月2日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | heat-live-v4.8.4.apk |
| 文件大小 | 18.47MB |
| MD5值 | c296ec069cefefacf907af3ef2072681 |
| SHA1值 | 637f38e84bdfe3237029e3c9430969cce84ed55b |
| SHA256值 | 3e994f88ba604639a712ba31a082366d8746d368de3e25e25a09f1193124b577 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Heat Live |
| 包名 | com.google.heatlive |
| 主活动Activity | com.huishine.traveler.page.SplashActivity |
| 安卓版本名称 | 4.8.4 |
| 安卓版本 | 484 |

## **4. 线索情况**

### **4.1 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 |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| objectbox.io | IP: 85.13.163.69  所属国家: Germany  地区: Thuringen  城市: Friedersdorf |
| 159.65.141.228 | IP: 159.65.141.228  所属国家: Singapore  地区: Singapore  城市: Singapore |
| dns.google | IP: 8.8.8.8  所属国家: United States of America  地区: California  城市: Mountain View |
| pro.ip-api.com | IP: 18.162.49.53  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| dashif.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| acrarium.tv1633.com | 没有服务器地理信息. |
| ns.adobe.com | 没有服务器地理信息. |
| 1.1.1.1 | IP: 1.1.1.1  所属国家: United States of America  地区: California  城市: San Jose |
| api.fubo.tv | IP: 151.101.90.110  所属国家: United States of America  地区: California  城市: San Francisco |
| docs.objectbox.io | IP: 172.64.147.209  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://pro.ip-api.com/json/?key=26pQNlE2x9UwB66&fields=status,country,countryCode,region,regionName,city,district,zip,lat,lon,timezone,currentTime,org,as,query,isp | com/huishine/traveler/page/j.java |
| https://dns.google/dns-query | com/huishine/traveler/player/e.java |
| http://159.65.141.228:8081/report | com/huishine/traveler/report/CrashApplication$onCreate$1.java |
| https://acrarium.tv1633.com/report | com/huishine/traveler/report/CrashApplication$onCreate$2.java |
| https://pro.ip-api.com/json/?key=26pQNlE2x9UwB66&fields=status,country,countryCode,region,regionName,city,district,zip,lat,lon,timezone,currentTime,org,as,query,isp | com/huishine/traveler/common/NetworkReceiver.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| http://static | h2/a.java |
| http://dashif.org/guidelines/trickmode | m1/d.java |
| http://dashif.org/guidelines/last-segment-number | m1/d.java |
| https://docs.objectbox.io/android/app-bundle-and-split-apk | x2/c.java |
| http://ns.adobe.com/xap/1.0/ | s0/a.java |
| http://integerinvalidkey | lib/armeabi-v7a/libgojni.so |
| https://1.1.1.1/dns-query?name=https://api.fubo.tv/v3/locationin | lib/armeabi-v7a/libgooglejni.so |
| https://api.fubo.tv/vapi/asset/v1indefinite | lib/armeabi-v7a/libgooglejni.so |
| https://api.fubo.tv/epg/filters/v2illegal | lib/armeabi-v7a/libgooglejni.so |
| http://127.0.0.1:12854/ | lib/armeabi-v7a/libjson.so |
| https://objectbox.io/sync/ | lib/armeabi-v7a/libobjectbox-jni.so |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222 | t0/d.java |

## **5. 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=60, ST=Malaysia, L=Kuala Lumpur, O=IPTV4K, OU=dev team, CN=dev 签名算法: rsassa\_pkcs1v15 有效期自: 2020-03-25 04:26:27+00:00 有效期至: 2045-03-19 04:26:27+00:00 发行人: C=60, ST=Malaysia, L=Kuala Lumpur, O=IPTV4K, OU=dev team, CN=dev 序列号: 0x210d3b1a 哈希算法: sha256 md5值: 20da148f4a0ee47db2a7b22ee12f8c4d sha1值: 9bf507749c4d15326f68200b5e6983ff22a71b9b sha256值: cb4e4c877a0247dfa23e926cb369a7f4901208a722e215bc24493848ac32e020 sha512值: fa2bcc836b81bb6a4b7167764f6e6e9eb637cc3668f36a6d03de86ef7e448b13cf7233fe376c0c5c37449d5510549d7b65de11a392f8d0b4e192d57e35ad2416 公钥算法: rsa 密钥长度: 2048 指纹: dd138843bd9ba5dfcf25c24c1d3ba2ed01d44bc376b3f975b75d7a1798c39d5b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "menu\_lock\_authentication\_failed" : "Authentication failed" |
| "menu\_lock\_please\_enter\_password" : "Please enter password" |
| "menu\_lock\_please\_set\_password" : "Please set password" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**