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

**HEALTH²（ 3.37.0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 | HEALTH² |
| 版本 | 3.37.0 |
| 包名 | tv.i999 |
| 域名线索 | 27条 |
| URL线索 | 31条 |
| APP图标 |  |
| 分析日期 | 2025年6月1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 | dh829\_jjkk.apk |
| 文件大小 | 29.82MB |
| MD5值 | d6038cf071b7bec90061993bff455e9d |
| SHA1值 | d1ad2c15387d31f7e32524dc545f8d6efeab14d3 |
| SHA256值 | 9bb305d62d40925f54d574277880bea2e6a1d4d2d6fd84f3d5f117ad745487de |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | HEALTH² |
| 包名 | tv.i999 |
| 主活动Activity | tv.i999.MVVM.Activity.LandingActivity.TestLandingActivity |
| 安卓版本名称 | 3.37.0 |
| 安卓版本 | 127 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| data.flurry.com | IP: 98.136.147.16 所属国家: United States of America 地区: New York 城市: New York City  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| d1vcfwitp2um8b.cloudfront.net | IP: 65.9.37.137 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| sdk.open.lbs.igexin.com | IP: 121.52.255.89 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dev-avnight-cpi.appdev.icu | IP: 139.162.98.177 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| jkjk-1318371851.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.181 所属国家: China 地区: Fujian 城市: Fuzhou  |
| www.sec.co.kr | IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| night9.oss-cn-hongkong.aliyuncs.com | IP: 47.79.64.211 所属国家: United States of America 地区: California 城市: San Mateo  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.xmlsoap.org | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| proton.flurry.com | 没有服务器地理信息.  |
| d.gt.igexin.com | 没有服务器地理信息.  |
| sdk.open.phone.igexin.com | IP: 101.68.218.171 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| s-gt.getui.com | IP: 124.160.155.57 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| sdk.open.amp.igexin.com | IP: 124.160.124.197 所属国家: China 地区: Zhejiang 城市: Wenzhou  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| bitdash-a.akamaihd.net | IP: 2.19.126.159 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| storage.googleapis.com | IP: 142.250.217.123 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| i.imgur.com | IP: 52.175.9.80 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| jkjk-1309454273.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.181 所属国家: China 地区: Fujian 城市: Fuzhou  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| c-hzgt2.getui.com | IP: 124.160.155.57 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| sdk.open.inc2.igexin.com | 没有服务器地理信息.  |
| app-jjkk-45621.firebaseio.com | IP: 34.120.206.254 所属国家: United States of America 地区: Missouri 城市: Kansas City  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/i.java  |
| http://%s:%d/%s  | com/danikula/videocache/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/k.java  |
| http://%s:%d/%s  | com/danikula/videocache/g.java  |
| https://data.flurry.com/pcr.do  | com/flurry/sdk/A.java  |
| https://data.flurry.com/aap.do  | com/flurry/sdk/K.java  |
| http://data.flurry.com/aap.do  | com/flurry/sdk/K.java  |
| https://proton.flurry.com/sdk/v1/config  | com/flurry/sdk/C0651s.java  |
| http://sdk.open.phone.igexin.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://c-hzgt2.getui.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://s-gt.getui.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://d.gt.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.amp.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.lbs.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.inc2.igexin.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://bi.  | com/igexin/push/config/p.java  |
| http://config.  | com/igexin/push/config/p.java  |
| http://stat.  | com/igexin/push/config/p.java  |
| http://log.  | com/igexin/push/config/p.java  |
| http://amp.  | com/igexin/push/config/p.java  |
| http://lbs.  | com/igexin/push/config/p.java  |
| http://inc.  | com/igexin/push/config/p.java  |
| http://purl.org/dc/elements/1.1/\  | com/ngs/videocast/Screening/j.java  |
| http://xml.org/sax/features/external-general-entities  | com/ngs/videocast/Screening/n/a.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/ngs/videocast/Screening/n/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | g/a/f.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  |
| http://schemas.xmlsoap.org/soap/envelope/  | org/fourthline/cling/transport/c/p.java  |
| http://schemas.xmlsoap.org/soap/encoding/  | org/fourthline/cling/transport/c/p.java  |
| http://www.sec.co.kr/dlna  | org/fourthline/cling/binding/xml/g.java  |
| http://xml.org/sax/features/external-general-entities  | org/seamless/xml/b.java  |
| http://xml.org/sax/features/external-parameter-entities  | org/seamless/xml/b.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/seamless/xml/b.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| https://bitdash-a.akamaihd.net/content/sintel/hls/video/  | tv/i999/MVVM/Activity/DownloadActivity/u.java  |
| https://i.imgur.com/YBIWSdQ.png  | tv/i999/MVVM/Bean/IOnlyFansActor.java  |
| https://i.imgur.com/YBIWSdQ.png  | tv/i999/MVVM/Bean/AvVideoBean.java  |
| https://i.imgur.com/8nPDtvG.jpeg  | tv/i999/MVVM/Bean/AvVideoBean.java  |
| https://i.imgur.com/8nPDtvG.jpeg  | tv/i999/MVVM/Bean/Comic/IComicData.java  |
| https://i.imgur.com/flwncYr.jpeg  | tv/i999/MVVM/Bean/PhotoModel/IPhotoModel.java  |
| https://i.imgur.com/pqggrK0.jpeg  | tv/i999/MVVM/Bean/Photo/PhotoDataBean.java  |
| https://i.imgur.com/DoXLf7v.jpeg  | tv/i999/MVVM/Bean/Youtube/IYoutuberData.java  |
| https://i.imgur.com/DoXLf7v.jpeg  | tv/i999/MVVM/Bean/Youtube/IYoutubeVideoData.java  |
| https://i.imgur.com/87gFf3V.jpeg  | tv/i999/MVVM/Bean/Actor/ActorResultBean.java  |
| https://i.imgur.com/cDUQah7.png  | tv/i999/MVVM/Bean/LiveStream/NewLiveStreamBean.java  |
| https://dev-avnight-cpi.appdev.icu/API/  | tv/i999/MVVM/API/F0.java  |
| https://jkjk-1309454273.cos.ap-guangzhou.myqcloud.com/short\_host.jsonb  | tv/i999/MVVM/API/ApiServiceManagerKt.java  |
| https://jkjk-1318371851.cos.ap-guangzhou.myqcloud.com/short\_host.jsonb  | tv/i999/MVVM/API/ApiServiceManagerKt.java  |
| https://storage.googleapis.com/jkjkjk/short\_host.jsonb  | tv/i999/MVVM/API/ApiServiceManagerKt.java  |
| https://d1vcfwitp2um8b.cloudfront.net/api/short\_host.jsonb  | tv/i999/MVVM/API/ApiServiceManagerKt.java  |
| https://night9.oss-cn-hongkong.aliyuncs.com/api/short\_host.json/  | tv/i999/MVVM/API/ApiServiceManagerKt.java  |
| https://i.imgur.com/YBIWSdQ.png  | tv/i999/MVVM/Model/FruitPieItemData.java  |
| https://app-jjkk-45621.firebaseio.com  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/i.java  |
| o@netstream.failed  | lib/x86\_64/librtmp-jni.so  |

### **4.4 手机号线索**

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

## **5. 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: O=AvNight, OU=IT, CN=Eric Lin 签名算法: rsassa\_pkcs1v15 有效期自: 2016-05-06 02:54:23+00:00 有效期至: 2041-04-30 02:54:23+00:00 发行人: O=AvNight, OU=IT, CN=Eric Lin 序列号: 0x633954be 哈希算法: sha256 md5值: ae49c75d9549826f5b7adfb259649fcb sha1值: 7302bcc88f1adb1b280497f8b83627f720c59474 sha256值: 4d16c34c491c9e6ca60524f7c139f74127d9cc8b70258380a40f274ea562ea78 sha512值: 15d82146fc34a20ef65ef43518807548f188cf55defe2932f0e684cc74abd258098c7008f923ff548fb1da2f6f529b1317982d3fcf4b6828c2444527f828b811 公钥算法: rsa 密钥长度: 2048 指纹: f8128e85d6b21bfbdbbcb784f3d7be801f82df0129d340ff82e93a317cbed2ea**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_forget\_password" : "忘记密码"  |
| "account\_reset\_password" : "重新设定密码"  |
| "do\_you\_forget\_password" : "忘记密码了？"  |
| "fileProvider\_authorities" : "jjkk\_number\_one"  |
| "firebase\_database\_url" : "https://app-jjkk-45621.firebaseio.com"  |
| "forget\_password" : "忘记密码"  |
| "go\_to\_forget\_password" : "去找回密码"  |
| "google\_api\_key" : "AIzaSyAYeEix0Dy2qcOlJLBj2uipIFdMtKLNsiI"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAYeEix0Dy2qcOlJLBj2uipIFdMtKLNsiI"  |
| "input\_password" : "输入密码"  |
| "key\_in\_password" : "输入密码"  |
| "oops\_cant\_reset\_password" : "Oops! 这个月修改密码次数用完啦"  |
| "password" : "密码"  |
| "please\_input\_password" : "请输入密码"  |
| "send\_email\_to\_reset\_password" : "验证码已寄到此邮箱 请重新设定密码"  |
| "send\_phone\_to\_reset\_password" : "验证码已寄到此手机号码 请重新设定密码"  |
| "setting\_password" : "设定密码"  |
| "your\_password" : "你的密码"  |

## **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.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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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.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.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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| getui.permission.GetuiService.tv.i999 | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| tv.i999.MVVM.Activity.LandingActivity.TestLandingActivity | **Schemes**: bg8://, http://, https://, **Hosts:** bg8,  |

**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。**