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

**iBox（ 1.2.05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 | iBox |
| 版本 | 1.2.05 |
| 包名 | com.box.art |
| 域名线索 | 4条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年6月11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 | ibox.apk |
| 文件大小 | 118.94MB |
| MD5值 | 480b025ab1ee54eac5834ceb896e276d |
| SHA1值 | 5f62b24c2f1e5089d4a8a2359b40c96f8383bb6f |
| SHA256值 | 4ecb43e36361dd639178cb3e0bd34606e1361516982f33184bfab34887366140 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | iBox |
| 包名 | com.box.art |
| 主活动Activity | com.ibox.nft.app.IBoxLauncherActivity |
| 安卓版本名称 | 1.2.05 |
| 安卓版本 | 10205 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.mob.com | IP: 45.120.103.158 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| ib-unity3d.ibox.art | IP: 220.181.135.138 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jsdelivr.com | IP: 216.24.57.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>.  | Mogua Engine V1  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>  | Mogua Engine V1  |
| https://www.mob.com  | Mogua Engine V1  |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If  | Mogua Engine V1  |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>  | Mogua Engine V1  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/catalog\_2022.10.28.08.03.21.hash  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/defaultlocalgroup\_assets\_all\_f10a3fc5a769fafa6b600d18e5ea83ce.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/defaultlocalgroup\_unitybuiltinshaders\_0a85111bda5a9d20b55620ce58201d92.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/gamedata\_assets\_all.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/modelbgs\_assets\_assets/project/hangxiaotian/hangxiaotian\_beijing.png.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/modelbgs\_assets\_assets/project/taoyi/background.png.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/models\_assets\_assets/project/hangxiaotian/hangxiaotian.prefab.bundle  | Mogua Engine V2  |
| https://ib-unity3d.ibox.art/ibox/3d/Android/models\_assets\_assets/project/taoyi/taoyi.prefab.bundle  | Mogua Engine V2  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | Mogua Engine V2  |
| https://github.com/apvarun/toastify-js  | Mogua Engine V2  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **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=86, ST=BeiJing, L=BeiJing, O=NFTBOX PTE.LTD., OU=Alpha R&D, CN=iBox 签名算法: rsassa\_pkcs1v15 有效期自: 2021-06-21 06:42:51+00:00 有效期至: 2046-06-15 06:42:51+00:00 发行人: C=86, ST=BeiJing, L=BeiJing, O=NFTBOX PTE.LTD., OU=Alpha R&D, CN=iBox 序列号: 0xb50495c 哈希算法: sha256 md5值: 7bdcca79ae6e50d35bec9790b4a18b83 sha1值: aecaf059315da24e5a14276710db1f6855ca5f2e sha256值: 5edab1254ace429cf20816d13c33e646b02035af6ae9d8f28cdcae191c601d35 sha512值: 7d79392125977c708f910d9ed317e0d94f726bfc750b8148bd4d3fbed718a4a871587ec69d99585e84a8fc2bcb9c5eb938d2614312d525cb5654c99b0484788f 公钥算法: rsa 密钥长度: 2048 指纹: 34e4034b217f3b820786289a20a697fd52a45ab39b05fd6dbbe8a4fdc66d1ecf**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyC1Kf6Lk0Fz7P41u5LKM7elVXP3xNh3rcY"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyC1Kf6Lk0Fz7P41u5LKM7elVXP3xNh3rcY"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobdemo\_authorize\_dialog\_title" : "服务授权"  |
| "private\_group" : "Discussion Group"  |
| "qd\_base\_wx\_key\_api" : "wxf5d97e23aa62841f"  |
| "qd\_base\_wx\_secret\_api" : "ef3d23d44571c4a04d9763cefede7c0f"  |
| "qd\_base\_wx\_secret\_dev" : "ef3d23d44571c4a04d9763cefede7c0f"  |
| "qd\_base\_wx\_secret\_qa" : "ef3d23d44571c4a04d9763cefede7c0f"  |
| "qd\_base\_ym\_channel\_api" : "channel"  |
| "qd\_base\_ym\_key\_api" : "5e5246677ba7e954e9f6a613"  |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供"  |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."  |
| "mobdemo\_authorize\_dialog\_title" : "service authority"  |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile"  |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "mobcommon\_authorize\_dialog\_accept" : "同意"  |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝"  |
| "mobcommon\_authorize\_dialog\_title" : "服务授权"  |
| "private\_group" : "讨论组"  |

## **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.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.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\_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.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 |
| 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.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.WRITE\_SYNC\_SETTINGS | 正常 | 写入同步设置 | 允许应用程序修改同步设置,例如是否为联系人启用同步 |
| android.permission.READ\_SYNC\_SETTINGS | 正常 | 读取同步设置 | 允许应用程序读取同步设置,例如是否为联系人启用同步 |
| 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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.ACCESS\_COARSE\_UPDATES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INSTALL\_SHORTCUT | 正常 |  | 允许应用程序在启动器中安装快捷方式 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| android.permission.FORCE\_BACK | 合法 | 强制申请关闭 | 允许应用程序强制关闭前台的任何活动并返回。普通应用程序永远不需要 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.REQUEST\_COMPANION\_USE\_DATA\_IN\_BACKGROUND | 正常 |  | 允许配套应用在后台使用数据。 |
| android.permission.REQUEST\_COMPANION\_RUN\_IN\_BACKGROUND | 正常 |  | 允许配套应用在后台运行。 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_DOWNLOAD\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_DOCUMENTS | 合法 |  | 允许应用程序管理对文档的访问,通常作为文档选择器的一部分 |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SENDTO | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.HIGH\_SAMPLING\_RATE\_SENSORS | 正常 | 访问更高采样率的传感器数据 | 允许应用访问采样率大于 200 Hz 的传感器数据 |
| 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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| getui.permission.GetuiService.com.ibox.nft | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.PACKAGE\_USAGE\_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| android.permission.LOCAL\_MAC\_ADDRESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_APN\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| com.box.art.permission.TMF\_SHARK | 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.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 |
| getui.permission.GetuiService.com.box.art | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.ibox.nft.app.IBoxLauncherActivity | **Schemes**: ibox://, sac92460c0://, **Hosts:** ibox.art, debugmode, heatmap, visualized, **Ports:** 80, **Paths:** /splash,  |
| com.ibox.nft.app.activity.IBoxSchemeActivity | **Schemes**: iboxscheme://, **Hosts:** com.ibox.push, **Paths:** /detail,  |
| com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity | **Schemes**: 您项目的 scheme://,  |
| cn.sharesdk.loopshare.LoopShareActivity | **Schemes**: ssdk34cefcd1ae6be://, **Hosts:** cn.sharesdk.loop,  |

**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。**