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

**Earn money（ 1.3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 | Earn money |
| 版本 | 1.3 |
| 包名 | com.EarnMoneyGetoffonThisApp |
| 域名线索 | 16条 |
| URL线索 | 11条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | Paytm Free Wallet Recharge.\_1.3\_APKPure.apk |
| 文件大小 | 3.09MB |
| MD5值 | db8bb750a8954ec8cbfa89112dad5fd3 |
| SHA1值 | 3c830d1aed6317c12a1227fae1ccbba272d5d6a8 |
| SHA256值 | 5220a1c52c31ed802eff44164a44b37057c621281785d3dda06ff11d99ae1a18 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Earn money |
| 包名 | com.EarnMoneyGetoffonThisApp |
| 主活动Activity | com.EarnMoneyGetoffonThisApp.splash |
| 安卓版本名称 | 1.3 |
| 安卓版本 | 4 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| connectivitycheck.gstatic.com | IP: 203.208.39.194 所属国家: China 地区: Beijing 城市: Beijing  |
| dts.startappservice.com | IP: 151.101.91.52 所属国家: United States of America 地区: California 城市: San Francisco  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| googleads.g.doubleclick.net | IP: 114.250.69.38 所属国家: China 地区: Beijing 城市: Beijing  |
| d1byvlfiet2h9q.cloudfront.net | IP: 18.245.78.35 所属国家: United States of America 地区: Washington 城市: Seattle  |
| sdk-exchange.startappservice.com | IP: 129.150.35.183 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.dummy.com | IP: 199.59.243.228 所属国家: United States of America 地区: Florida 城市: Tampa  |
| cs1112.wpc.rhocdn.net | 没有服务器地理信息.  |
| oke-ash-ms-weight-lb.startappelb.com | IP: 158.101.105.86 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| sdk-exchange.startappelb.com | IP: 129.150.35.183 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| info.static.startappservice.com | IP: 151.101.91.52 所属国家: United States of America 地区: California 城市: San Francisco  |
| edgedl.me.gvt1.com | IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View  |
| goo.gl | IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| images.startappservice.com | IP: 151.101.91.52 所属国家: United States of America 地区: California 城市: San Francisco  |
| init.startappexchange.com | IP: 168.138.169.206 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.startappexchange.com | IP: 129.150.35.183 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.startappexchange.com/tracking/adImpression  | com/startapp/android/publish/d.java  |
| http://d1byvlfiet2h9q.cloudfront.net/InApp/resources/adInformationDialog3.html  | com/startapp/android/publish/adinformation/AdInformationConfig.java  |
| http://www.startappexchange.com/tracking/adClick  | com/startapp/android/publish/model/MetaData.java  |
| http://init.startappexchange.com/1.4/  | com/startapp/android/publish/model/MetaData.java  |
| http://www.startappexchange.com/1.4/  | com/startapp/android/publish/model/MetaData.java  |
| http://www.startappexchange.com/tracking/infoEvent  | com/startapp/android/publish/d/a.java  |
| http://play.google.com  | com/startapp/android/publish/h/v.java  |
| https://play.google.com  | com/startapp/android/publish/h/v.java  |
| http://www.startappexchange.com  | com/startapp/android/publish/h/v.java  |
| http://www.dummy.com  | com/startapp/android/publish/nativead/NativeAdDetails.java  |
| http://play.google.com  | com/startapp/android/publish/c/c.java  |
| https://play.google.com  | com/startapp/android/publish/c/c.java  |
| https://play.google.com/store/apps/details?id=com.EarnMoneyGetoffonThisApp  | com/EarnMoneyGetoffonThisApp/RateUs.java  |
| https://play.google.com/store/apps/details?id=com.EarnMoneyGetoffonThisApp  | com/EarnMoneyGetoffonThisApp/Recharge.java  |
| http://goo.gl/forms/Wc3d5xDerw  | com/EarnMoneyGetoffonThisApp/Recharge.java  |
| https://play.google.com/store/apps/details?id=com.EarnMoneyGetoffonThisApp  | com/EarnMoneyGetoffonThisApp/AddsDrawer.java  |
| googleads.g.doubleclick.net  | 摸瓜V3引擎  |
| oke-ash-ms-weight-lb.startappelb.com  | 摸瓜V3引擎  |
| http://www.startappexchange.com  | 摸瓜V3引擎  |
| http://www.dummy.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| android.googleapis.com  | 摸瓜V3引擎  |
| dts.startappservice.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto&&android.support.v4.widget.DrawerLayout  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto00android.support.v7.widget.ActionBarOverlayLayout  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto//android.support.design.widget.CoordinatorLayout  | 摸瓜V3引擎  |
| images.startappservice.com  | 摸瓜V3引擎  |
| init.startappexchange.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android00android.support.v7.widget.FitWindowsLinearLayout  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid\_app\_interstitial.js  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html  | 摸瓜V3引擎  |
| www.startappexchange.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android66android.support.design.internal.NavigationMenuItemView  | 摸瓜V3引擎  |
| cs1112.wpc.rhocdn.net  | 摸瓜V3引擎  |
| sdk-exchange.startappelb.com  | 摸瓜V3引擎  |
| info.static.startappservice.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android00android.support.v7.widget.FitWindowsLinearLayout((androi  | 摸瓜V3引擎  |
| http://d1byvlfiet2h9q.cloudfront.net/InApp/resources/adInformationDialog3.html  | 摸瓜V3引擎  |
| connectivitycheck.gstatic.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto((android.support.v7.widget.ActionMenuView  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| update.googleapis.com  | 摸瓜V3引擎  |
| sdk-exchange.startappservice.com  | 摸瓜V3引擎  |
| http://goo.gl/forms/Wc3d5xDerw  | 摸瓜V3引擎  |
| edgedl.me.gvt1.com  | 摸瓜V3引擎  |
| gmscompliance-pa.googleapis.com  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid\_app\_banner.js  | 摸瓜V3引擎  |

### **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: False v3 签名: False 找到 1 个唯一证书 主题: CN=earn moneys 签名算法: rsassa\_pkcs1v15 有效期自: 2017-06-08 03:55:47+00:00 有效期至: 2062-05-28 03:55:47+00:00 发行人: CN=earn moneys 序列号: 0x117cf168 哈希算法: sha256 md5值: f5839a3a10b12995decc23bd53b2b428 sha1值: 395e5e72136747b1220a8e6cf4f561cab70e5e2a sha256值: a6815d46a1f103a9dba7fe754efe42805e7060771ac10b83e123ea1db9ecacf6 sha512值: f8a83ad89ae0646ed9521020b9c9c00af39ffcbccff45437d1f194540b25e6600bb8852a80bb31e103a5dce133ac96cfb88b06538fcd63163af5943e25803521**

## **6. 硬编码敏感信息**

## **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 |

## **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。**