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

**Virtual Hosts（ 2.1.1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 | Virtual Hosts |
| 版本 | 2.1.1 |
| 包名 | com.github.xfalcon.vhosts |
| 域名线索 | 12条 |
| URL线索 | 12条 |
| APP图标 |  |
| 分析日期 | 2024年12月22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 | virtualhostsv2.1.1.apk |
| 文件大小 | 1.46MB |
| MD5值 | e594b09713b34da8409ad578d3463253 |
| SHA1值 | aecede7e52bfffce4162d40d0df8054815b527f2 |
| SHA256值 | 0c60700b31cd498098f2ad56c4c0956c5a77b9aab0f53c3eb4e2f60c56435a23 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Virtual Hosts |
| 包名 | com.github.xfalcon.vhosts |
| 主活动Activity | com.github.xfalcon.vhosts.VhostsActivity |
| 安卓版本名称 | 2.1.1 |
| 安卓版本 | 38 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.googleadservices.com | IP: 220.181.174.166 所属国家: China 地区: Beijing 城市: Beijing  |
| firebase.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.paypal.com | IP: 151.101.109.21 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 64.13.192.74 所属国家: United States of America 地区: California 城市: Culver City  |
| play.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| app-measurement.com | IP: 220.181.174.97 所属国家: China 地区: Beijing 城市: Beijing  |
| google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| goo.gl | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.android.com | 没有服务器地理信息.  |
| pagead2.googlesyndication.com | IP: 220.181.174.166 所属国家: China 地区: Beijing 城市: Beijing  |
| raw.githubusercontent.com | IP: 185.199.110.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api-5874083157835505386-758464.firebaseio.com | IP: 34.120.160.131 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 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | a/a/k/u.java  |
| https://raw.githubusercontent.com/x-falcon/tools/master/w.png  | com/github/xfalcon/vhosts/DonationActivity.java  |
| https://play.google.com/store/apps/details?id=com.github.xfalcon.vhosts  | com/github/xfalcon/vhosts/DonationActivity.java  |
| https://raw.githubusercontent.com/x-falcon/tools/master/a.png  | com/github/xfalcon/vhosts/DonationActivity.java  |
| https://www.paypal.com/cgi-bin/webscr?cmd=\_donations&business=X2SCFSHBXUMUC&lc=GB&item\_name=Donate&no\_note=0&currency\_code=USD&bn=PP%2dDonationsBF%3abtn\_donateCC\_LG%2egif%3aNonHostedGuest  | com/github/xfalcon/vhosts/DonationActivity.java  |
| https://google.com/search?  | b/c/a/a/f/b/f7.java  |
| https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s  | b/c/a/a/f/b/m6.java  |
| https://app-measurement.com/a  | b/c/a/a/f/b/p.java  |
| https://firebase.google.com/support/guides/disable-analytics  | b/c/a/a/f/b/u3.java  |
| https://www.google.com  | b/c/a/a/f/b/w9.java  |
| https://goo.gl/NAOOOI.  | b/c/a/a/f/b/w9.java  |
| https://goo.gl/NAOOOI  | b/c/a/a/f/b/w9.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | b/c/a/a/a/a/b.java  |
| https://app-measurement.com/a  | b/c/a/a/e/c/ba.java  |
| https://goo.gl/J1sWQy  | b/c/a/a/e/c/g.java  |
| https://firebase.google.com/support/privacy/init-options.  | b/c/b/k/c.java  |
| https://api-5874083157835505386-758464.firebaseio.com  | Mogua Engine V1  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | b/c/a/a/b/w.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15552000000  | b/c/a/a/f/b/k6.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: CN=xfalcon 签名算法: rsassa\_pkcs1v15 有效期自: 2017-04-24 07:03:22+00:00 有效期至: 2042-04-18 07:03:22+00:00 发行人: CN=xfalcon 序列号: 0x7920d0e4 哈希算法: sha256 md5值: d23b5a3fc686327f96ab04f1991a7bf8 sha1值: c525527086eac5df5b753ae9fd043b5a19928c69 sha256值: 6aab9878ce6a17d8975de52280f67ca7828b88489c3421d4f6b7c7c1d5d2ceba sha512值: 18f72d012f5f47385001d3e6886478979673c7f29abc4d65ae65f6ca89f5a2f62a173f84a5747a9f18492870b9b40303d6ac54f0bf63798a02e9b24149ba1c36 公钥算法: rsa 密钥长度: 2048 指纹: 9eac1ebc71d4741c437c40828e6bfe793d3b0906f1a1f83280c2f45122bf56d5**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "bitcoin" : "Donate with Bitcoin"  |
| "firebase\_database\_url" : "https://api-5874083157835505386-758464.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyAkDG6T5t2EtA6oXquofFoT5FTWQLoMe88"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAkDG6T5t2EtA6oXquofFoT5FTWQLoMe88"  |
| "tip\_bitcoin" : "bitcoin address has copy to the clipboard"  |
| "bitcoin" : "比特币捐赠"  |
| "tip\_bitcoin" : "比特币地址已经复制到剪切板"  |
| "bitcoin" : "Đóng góp bằng Bitcoin"  |
| "tip\_bitcoin" : "Địa chỉ bitcoin có bản sao vào bộ nhớ tạm"  |
| "bitcoin" : "比特幣捐贈"  |
| "tip\_bitcoin" : "比特幣地址已經複製到剪切板"  |

## **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.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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**