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

**Alpha（ a344ebf2-alpha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 | Alpha |
| 版本 | a344ebf2-alpha |
| 包名 | io.github.vvb2060.magisk |
| 域名线索 | 11条 |
| URL线索 | 13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 | app-release.apk |
| 文件大小 | 11.41MB |
| MD5值 | fcf146ee3c19d117cfaf8fa69905f72d |
| SHA1值 | 9502a5c4aa41683546fedefb6b1d981312c54184 |
| SHA256值 | 13a18b417ec8427c61931855a871ae1b3d9853f4d9c12d079b6add3ff3a2a9bd |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Alpha |
| 包名 | io.github.vvb2060.magisk |
| 主活动Activity | com.topjohnwu.magisk.ui.MainActivity |
| 安卓版本名称 | a344ebf2-alpha |
| 安卓版本 | 30100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.patreon.com | IP: 128.242.240.117 所属国家: United States of America 地区: Washington 城市: Redmond  |
| example.com | IP: 23.192.228.84 所属国家: United States of America 地区: California 城市: Santa Clara  |
| paypal.me | IP: 162.159.141.96 所属国家: United States of America 地区: California 城市: San Francisco  |
| dns.cloudflare.com | IP: 162.159.61.8 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  |
| twitter.com | IP: 65.49.26.99 所属国家: United States of America 地区: Missouri 城市: Saint Louis  |
| api.github.com | IP: 20.205.243.168 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| youtrack.jetbrains.com | IP: 63.33.88.220 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| commons.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| issuetracker.google.com | IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.patreon.com/topjohnwu  | defpackage/C0029Bo.java  |
| https://paypal.me/magiskdonate  | defpackage/C0029Bo.java  |
| https://github.com/sponsors/yujincheng08  | defpackage/C0029Bo.java  |
| https://twitter.com/  | defpackage/AbstractC0014Ao.java  |
| https://github.com/topjohnwu/Magisk  | defpackage/C1896zo.java  |
| https://github.com/  | defpackage/C1835yf.java  |
| http://schemas.android.com/apk/res/android  | defpackage/QL.java  |
| https://issuetracker.google.com/issues/116541301  | defpackage/AbstractC1723wM.java  |
| https://youtrack.jetbrains.com/issue/KT-55980  | defpackage/C0849iw.java  |
| https://commons.apache.org/proper/commons-compress/zip.html  | defpackage/C1881zO.java  |
| http://schemas.android.com/apk/res/android  | defpackage/G.java  |
| http://schemas.android.com/apk/res/android  | defpackage/AbstractC0729ge.java  |
| http://schemas.android.com/apk/res/android  | defpackage/YO.java  |
| https://dns.cloudflare.com/dns-query  | defpackage/C1623ub.java  |
| https://example.com/  | defpackage/C0176Ll.java  |
| https://api.github.com/  | defpackage/C0176Ll.java  |

### **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: CN=vvb2060 签名算法: rsassa\_pkcs1v15 有效期自: 1999-12-31 16:01:00+00:00 有效期至: 2099-12-06 16:01:00+00:00 发行人: CN=vvb2060 序列号: 0x17f6256c 哈希算法: sha256 md5值: b54cd9879577353554247f7d9be20b29 sha1值: 4c5d0ca0ddc3e1e88dd7edbdfdffd9708ebffbf5 sha256值: 59c23d1c00728b0284d6a46d4114618c20d354cb17dd743baa7644e541bc1e44 sha512值: ee830b8b2b48b499c43ca5f72d56a7ce1277334b3253029766ff96c4f15022bd6416718e8df67cd2bd51ca81a24cde4891b695fb9ab2fa9974128f44870c4e26 公钥算法: rsa 密钥长度: 2048 指纹: 2b3af5d39cfcfebdf94ccb1c221761f133fbd3e9268cbc04433a6d42cb0ba363**

## **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 |
| 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.HIDE\_OVERLAY\_WINDOWS | 正常 | 防止非系统覆盖窗口 | 允许应用程序防止在其上绘制非系统覆盖窗口 |
| android.permission.UPDATE\_PACKAGES\_WITHOUT\_USER\_ACTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RUN\_USER\_INITIATED\_JOBS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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**

**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。**