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

**CZ File Manager（ 15.4.4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 | CZ File Manager |
| 版本 | 15.4.4 |
| 包名 | com.chaozhuo.filemanager |
| 域名线索 | 19条 |
| URL线索 | 13条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | 超卓文管.apk |
| 文件大小 | 8.59MB |
| MD5值 | 337f8864e940058d119572be19b111b9 |
| SHA1值 | 2f1e1391ff2fe924bf73ae4c20e9c43f366b4f6f |
| SHA256值 | 7bac368c7ba8a21b394d23c1a4e5d3e0bfd482c2a292e163265e2f0e70063191 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | CZ File Manager |
| 包名 | com.chaozhuo.filemanager |
| 主活动Activity | com.chaozhuo.filemanager.activities.SplashActivity |
| 安卓版本名称 | 15.4.4 |
| 安卓版本 | 154400 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| files.phoenixos.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.chaozhuo.net | IP: 54.179.117.50 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| bbs.phoenixstudio.org | IP: 69.16.230.165 所属国家: United States of America 地区: Michigan 城市: Lansing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| api.chaozhuo.org | 没有服务器地理信息.  |
| sdk.wukongtv.com | 没有服务器地理信息.  |
| goo.gl | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| api.phenixos.com.local | 没有服务器地理信息.  |
| www.bitcandies.com | IP: 91.195.240.13 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Koeln  |
| googleads.g.doubleclick.net | IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing  |
| commons.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| cdn.phoenixstudio.org | IP: 69.16.230.165 所属国家: United States of America 地区: Michigan 城市: Lansing  |
| c-t.yunpan.360.cn | IP: 101.199.254.53 所属国家: China 地区: Beijing 城市: Beijing  |
| os.chaozhuo.net | IP: 54.179.117.50 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.phoenixstudio.org | IP: 69.16.230.165 所属国家: United States of America 地区: Michigan 城市: Lansing  |
| www.phoenixos.com | IP: 45.155.220.52 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| api.phenixos.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://api.chaozhuo.org  | com/chaozhuo/filemanager/FileManagerApplication.java  |
| http://api.phenixos.com  | com/chaozhuo/filemanager/FileManagerApplication.java  |
| https://c-t.yunpan.360.cn/upgradeannounce.html  | com/chaozhuo/filemanager/dialogs/DialogCloudStopTips.java  |
| https://play.google.com/store/apps/details?id=com.chaozhuo.gameassistant&referrer=utm\_source%3DCZFileManager  | com/chaozhuo/filemanager/dialogs/r.java  |
| http://127.0.0.1:23456/smb/  | com/chaozhuo/filemanager/j/c.java  |
| https://play.google.com/store/apps/details?id=com.chaozhuo.gameassistant&referrer=utm\_source%3DCZFileManager  | com/chaozhuo/filemanager/fragments/c.java  |
| http://bbs.phoenixstudio.org/  | com/chaozhuo/aboutpage/activities/AboutPageActivity.java  |
| http://www.phoenixos.com/help/faq  | com/chaozhuo/feedbacklib/b/b.java  |
| http://www.phoenixos.com/help/faq/arm  | com/chaozhuo/feedbacklib/b/b.java  |
| http://api.chaozhuo.net  | com/chaozhuo/feedbacklib/b/b.java  |
| http://api.phenixos.com  | com/chaozhuo/feedbacklib/b/b.java  |
| http://os.chaozhuo.net/feedback/page/1  | com/chaozhuo/feedbacklib/b/b.java  |
| http://www.phoenixos.com/feedback/page/1  | com/chaozhuo/feedbacklib/b/b.java  |
| http://sdk.wukongtv.com/yaokong/tv/wkyaokongTV\_sdk.apk?from=%s&model=%s&product=%s  | com/wukongtv/sdk/impl/b.java  |
| http://bbs.phoenixstudio.org/  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/  | 摸瓜V1引擎  |
| http://%1$s:%2$d  | 摸瓜V1引擎  |
| http://www.phoenixos.com  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/browser/intro-pad  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/browser/intro  | 摸瓜V1引擎  |
| http://api.phenixos.com  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/help/fm\_faq.html  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/filemanager  | 摸瓜V1引擎  |
| http://www.phoenixos.com/  | 摸瓜V1引擎  |
| http://cdn.phoenixstudio.org/download/StardustBrowser\_pad\_arm\_1.3.apk  | 摸瓜V1引擎  |
| http://cdn.phoenixstudio.org/download/StardustBrowser\_1.2.1.apk  | 摸瓜V1引擎  |
| http://www.phoenixstudio.org/editor  | 摸瓜V1引擎  |
| http://files.phoenixos.com/img/videos.mp4  | 摸瓜V2引擎  |
| http://files.phoenixos.com/img/peripherals.mp4  | 摸瓜V2引擎  |
| http://files.phoenixos.com/img/world\_cup\_present.png  | 摸瓜V2引擎  |
| http://files.phoenixos.com/img/worldcup.mp4  | 摸瓜V2引擎  |
| http://github.com/bitcandies/upload5  | 摸瓜V2引擎  |
| http://www.bitcandies.com/  | 摸瓜V2引擎  |
| http://api.chaozhuo.org  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://goo.gl/naFqQk  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js  | 摸瓜V3引擎  |
| http://os.chaozhuo.net/feedback/page/1  | 摸瓜V3引擎  |
| http://www.phoenixos.com/help/faq  | 摸瓜V3引擎  |
| http://commons.apache.org/proper/commons-compress/limitations.html#7Z  | 摸瓜V3引擎  |
| http://goo.gl/8Rd3yj  | 摸瓜V3引擎  |
| http://sdk.wukongtv.com/yaokong/tv/wkyaokongTV\_sdk.apk?from=%s&model=%s&product=%s  | 摸瓜V3引擎  |
| http://www.bitcandies.com/  | 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  |
| http://www.phoenixos.com/feedback/page/1  | 摸瓜V3引擎  |
| http://www.phoenixos.com/help/faq/arm  | 摸瓜V3引擎  |
| http://api.phenixos.com  | 摸瓜V3引擎  |
| http://127.0.0.1:23456/smb/  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native\_ads.html  | 摸瓜V3引擎  |
| http://www.phoenixstudio.org/  | 摸瓜V3引擎  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/native\_ads.js  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://api.chaozhuo.net  | 摸瓜V3引擎  |
| api.phenixos.com.local  | 摸瓜V3引擎  |
| googleads.g.doubleclick.net  | 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  |
| http://bbs.phoenixstudio.org/  | 摸瓜V3引擎  |
| http://github.com/bitcandies/upload5  | 摸瓜V3引擎  |
| https://c-t.yunpan.360.cn/upgradeannounce.html  | 摸瓜V3引擎  |
| api.phenixos.com  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | org/c/a/d/a.java  |

## **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=Beijing Chaozhuo Technology Co. Ltd., OU=Phoenix Studio, CN=Xie ZhenYu 签名算法: rsassa\_pkcs1v15 有效期自: 2015-05-20 08:54:49+00:00 有效期至: 2040-05-13 08:54:49+00:00 发行人: C=86, ST=Beijing, L=Beijing, O=Beijing Chaozhuo Technology Co. Ltd., OU=Phoenix Studio, CN=Xie ZhenYu 序列号: 0x3004f463 哈希算法: sha256 md5值: be0dd2bc8fa3b534241f91f8b66d1c50 sha1值: 19b727b6d3eccebfb91811befc41ee8ece538af8 sha256值: 0ee714717cfa5e40c727b4fa1eb4cf6d6834c1c44f1ffebe5bbb8e2cc4fe43ce sha512值: 9e14caef44b4ef7f8b5396954e653396a3719bac52709aa85d139709ef00f5b52426575a55a3af2b4bfde4c398147e75992c1fd69e34fdd06456e3bda71997bf 公钥算法: rsa 密钥长度: 2048 指纹: 50e58015b4086c976a3f65b769df8ae234cc55c266f35dd8b352c583e47e1b29**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "password" : "Password:"  |
| "username" : "Username:"  |
| "chaozhuo\_api\_key" : "c1507240000000201"  |
| "chaozhuo\_api\_secret" : "26d945a6b3294dbca9bac4ccd75cbc05"  |
| "password" : "Adgangskode:"  |
| "username" : "Brugernavn:"  |
| "password" : "パスワード："  |
| "username" : "ユーザー名："  |
| "password" : "Passord:"  |
| "username" : "Brukernavn:"  |
| "password" : "Kennwort:"  |
| "username" : "Benutzername:"  |
| "password" : "Парола:"  |
| "username" : "Потребител:"  |
| "password" : "Salasana:"  |
| "username" : "Käyttäjätunnus:"  |
| "password" : "Heslo:"  |
| "username" : "Meno používateľa:"  |
| "password" : "Пароль:"  |
| "username" : "Ім'я користувача:"  |
| "password" : "Κωδικός πρόσβασης:"  |
| "username" : "Όνομα χρήστη:"  |
| "password" : "Wachtwoord:"  |
| "username" : "Gebruikersnaam:"  |
| "password" : "Hasło:"  |
| "username" : "Nazwa użytkownika:"  |
| "password" : "Geslo:"  |
| "username" : "Uporabniško ime:"  |
| "password" : "암호:"  |
| "username" : "사용자 이름:"  |
| "password" : "Parolă:"  |
| "username" : "Nume utilizator:"  |
| "password" : "كلمة المرور:"  |
| "username" : "اسم المستخدم:"  |
| "password" : "Mot de passe :"  |
| "username" : "Nom d'utilisateur :"  |
| "password" : "Lozinka:"  |
| "username" : "Korisničko ime:"  |
| "password" : "Lozinka:"  |
| "username" : "Korisničko ime:"  |
| "password" : "Lozinka:"  |
| "username" : "Korisničko ime:"  |
| "password" : "Parola:"  |
| "username" : "Kullanıcı adı:"  |
| "password" : "Heslo:"  |
| "username" : "Uživatelské jméno:"  |
| "password" : "Contraseña:"  |
| "username" : "Nombre de usuario:"  |
| "password" : "Parool:"  |
| "username" : "Kasutajanimi:"  |
| "password" : "Password:"  |
| "username" : "Nome utente:"  |
| "password" : "Slaptažodis:"  |
| "username" : "Naudotojo vardas:"  |
| "password" : "Jelszó:"  |
| "username" : "Felhasználói név:"  |
| "password" : "Пароль:"  |
| "username" : "Имя пользователя:"  |
| "password" : "Parole:"  |
| "username" : "Lietotājvārds:"  |
| "password" : "Lösenord:"  |
| "username" : "Användarnamn:"  |
| "password" : "סיסמה:"  |
| "username" : "שם משתמש:"  |
| "password" : "密碼："  |
| "username" : "使用者名稱："  |
| "password" : "密码："  |
| "username" : "用户名："  |
| "password" : "Senha:"  |
| "username" : "Nome de usuário:"  |
| "password" : "Lozinka:"  |
| "username" : "Korisničko ime:"  |
| "password" : "Palavra-passe:"  |
| "username" : "Nome de utilizador:"  |
| "password" : "密碼："  |
| "username" : "使用者名稱："  |

## **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.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.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.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.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| android.permission.ACCESS\_SUPERUSER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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 |
| 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.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.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.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.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\_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.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.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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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 |
| android.permission.BIND\_NOTIFICATION\_LISTENER\_SERVICE | 合法 |  | NotificationListenerService 必须要求,以确保只有系统可以绑定到它 |
| com.android.vending.BILLING | 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。**