MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

IM兼职 1.0.1.APK

APP名称:	IM兼职
包名:	com.imisingmlm.apps
域名线索:	13条
URL线索:	10条
邮箱线索:	0条

分析日期: 2022年2月2日 20:18

文件信息

文件名: imjianzhi.apk
文件大小: 8.87MB
MD5值: 0e55977915d93b6e991a1576ae0d3302
SHA1值: 9d9af3a03a20ec05afbd69f6d194b0ffe4b47286
SHA256值: afb8fac8c0a9e938dc9e2590fdb6c6a96bb21092a99052a21318da2fa7c1eff1

APP 信息

App名称: IM兼职
包名: com.imisingmlm.apps
主活动Activity: com.imisingmlm.apps.UI.Splash.SplashActivity
安卓版本名称: 1.0.1
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
img-u-3.51miz.com	good	**IP:** 1.180.29.28 **所属国家:** China **地区:** Nei Mongol **城市:** Baotou **纬度:** 40.652222 **经度:** 109.822220 **查看地图:** Google Map

域名	是否危险域名	服务器信息
timgsa.baidu.com	good	**IP:** 218.68.136.48 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
images.669pic.com	good	**IP:** 36.102.212.72 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
photo.16pic.com	good	**IP:** 122.114.37.12 **所属国家:** China **地区:** Henan **城市:** Zhengzhou **纬度:** 34.757778 **经度:** 113.648613 **查看地图:** Google Map
ss0.bdstatic.com	good	**IP:** 101.72.203.32 **所属国家:** China **地区:** Hebei **城市:** Tangshan **纬度:** 39.633331 **经度:** 118.183327 **查看地图:** Google Map
cdn.doumistatic.com	good	**IP:** 103.18.208.227 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
img.tianyancha.com	good	**IP:** 42.81.249.131 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
core.zuolin.com	good	**IP:** 47.111.45.211 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

域名	是否危险域名	服务器信息
ss1.bdstatic.com	good	**IP:** 101.72.203.32 **所属国家:** China **地区:** Hebei **城市:** Tangshan **纬度:** 39.633331 **经度:** 118.183327 **查看地图:** Google Map
dog.hotbuybuy.com	good	**IP:** 27.221.68.165 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **查看地图:** Google Map
img5.tianyancha.com	good	**IP:** 111.206.76.41 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
mp.weixin.qq.com	good	**IP:** 175.24.209.30 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
ss3.bdstatic.com	good	**IP:** 101.72.203.32 **所属国家:** China **地区:** Hebei **城市:** Tangshan **纬度:** 39.633331 **经度:** 118.183327 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://dog.hotbuybuy.com/api/dog/list/1/0	com/imisingmlm/apps/UI
https://core.zuolin.com/ecommerce/user/?lang=zh-CN&appId=976218#/pages/micro-mall/index?lang=zh-CN&martId=1	com/imisingmlm/apps/UI
http://dog.hotbuybuy.com/api/dog/list/1/0	com/imisingmlm/apps/UI
https://ss1.bdstatic.com/70cFvXSh_Q1YnxGkpoWK1HF6hhy/it/u=3923190736,3586353517&fm=26&gp=0.jpg	com/imisingmlm/apps/UI

URL信息	Url所在文件
https://ss3.bdstatic.com/70cFv8Sh_Q1YnxGkpoWK1HF6hhy/it/u=2650478385,2821614220&fm=26&gp=0.jpg	com/imisingmlm/apps/UI
https://ss0.bdstatic.com/70cFvHSh_Q1YnxGkpoWK1HF6hhy/it/u=3948653472,3667149970&fm=26&gp=0.jpg	com/imisingmlm/apps/UI
https://ss1.bdstatic.com/70cFvXSh_Q1YnxGkpoWK1HF6hhy/it/u=1343410676,405819035&fm=26&gp=0.jpg	com/imisingmlm/apps/UI
https://ss0.bdstatic.com/70cFuHSh_Q1YnxGkpoWK1HF6hhy/it/u=1840552500,1968568&fm=26&gp=0.jpg	com/imisingmlm/apps/UI
https://images.669pic.com/element_psd/88/68/85/82/950ad532da294cfdbd121a980f1c2594.jpg	com/imisingmlm/apps/UI
https://img-u-3.51miz.com/Templet/00/16/52/82/165282_ff342da9439b96238f9c04f756321115.jpg	com/imisingmlm/apps/UI
https://photo.16pic.com/00/88/19/16pic_8819709_b.jpg	com/imisingmlm/apps/UI
http://dog.hotbuybuy.com/api/dog/list/1/0	com/imisingmlm/apps/UI
https://mp.weixin.qq.com/s/qltDyNdnEcmxk9FTD72fLQ?sc=an_vivo&parent=isApp&versionNumber=2.1.1	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/224,01ddeba9725375f7.png	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/203,01ddeb72309fe2af.png	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/215,01ddeb5f1b55a71c.png	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074914491&di=a7a1931c53ab6cbbc247a53ff5eb9b91&imgtype=0&src=http%3A%2F%2Fimg3.imgtn.bdimg.com%2Fit%2Fu%3D3946008273%2C1846012299%26fm%3D214%26gp%3D0.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074951142&di=738e74b873c711c0b6310901988ebfeb&imgtype=0&src=http%3A%2F%2Fimg1.wanguan.com%2Fimg%2F001%2F1%2F1507%2F1555af4dec84716.png	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913957&di=ad0b79ffdf1d37a02759a58b822a0575&imgtype=0&src=http%3A%2F%2Fa.img.youboy.com%2Fcoimg%2F2010%2F2%2F3%2Fg3_2271146.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=b3608aebe0e90c6e1e8ea49eef921853&imgtype=0&src=http%3A%2F%2Fimg011.hc360.cn%2Fg3%2FM05%2F8A%2F78%2FwKhQvFK0Bi6EIS33AAAAADcLN0g442.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=c5461595b9330238aaa24dfc9d3686e5&imgtype=0&src=http%3A%2F%2Fdpic.tiankong.com%2Fln%2Fi9%2FQJ6379153906.jpg%3Fx-oss-process%3Dstyle%2Fshow	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=9bbdd5f21e5c5900aaee7df33b145b04&imgtype=0&src=http%3A%2F%2Fmpic.tiankong.com%2Fd02%2Fc6a%2Fd02c6af0587ecebfdd2ad43a5ee52132%2F640.jpg%40%2521670w	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=e63515de4495130abe32181b941f3424&imgtype=0&src=http%3A%2F%2Fdpic.tiankong.com%2Ftz%2Fsa%2FQJ6990922167.jpg%3Fx-oss-process%3Dstyle%2Fshow	com/imisingmlm/apps/UI
https://img.tianyancha.com/tmp/19051710/958188891013/edit_company503992.png@!fill_200x200	com/imisingmlm/apps/UI
https://img5.tianyancha.com/logo/lll/e1b941681af34d681682132623a44d19.png@!f_200x200	com/imisingmlm/apps/UI
https://img5.tianyancha.com/logo/lll/715a10081596006e8c0f2c99d932e666.png@!f_200x200	com/imisingmlm/apps/UI
https://images.669pic.com/element_psd/88/68/85/82/950ad532da294cfdbd121a980f1c2594.jpg	com/imisingmlm/apps/UI

URL信息	Url所在文件
https://img-u-3.51miz.com/Templet/00/16/52/82/165282_ff342da9439b96238f9c04f756321115.jpg	com/imisingmlm/apps/UI
https://photo.16pic.com/00/88/19/16pic_8819709_b.jpg	com/imisingmlm/apps/UI
https://core.zuolin.com/ecommerce/user/?lang=zh-CN&appId=976218#/pages/micro-mall/index?lang=zh-CN&martId=1	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074914491&di=a7a1931c53ab6cbbc247a53ff5eb9b91&imgtype=0&src=http%3A%2F%2Fimg3.imgtn.bdimg.com%2Fit%2Fu%3D3946008273%2C1846012299%26fm%3D214%26gp%3D0.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074951142&di=738e74b873c711c0b6310901988ebfeb&imgtype=0&src=http%3A%2F%2Fimg1.wanguan.com%2Fimg%2F001%2F1%2F1507%2F1555af4dec84716.png	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913957&di=ad0b79ffdf1d37a02759a58b822a0575&imgtype=0&src=http%3A%2F%2Fa.img.youboy.com%2Fcoimg%2F2010%2F2%2F3%2Fg3_2271146.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=b3608aebe0e90c6e1e8ea49eef921853&imgtype=0&src=http%3A%2F%2Fimg011.hc360.cn%2Fg3%2FM05%2F8A%2F78%2FwKhQvFK0Bi6EIS33AAAADcLN0g442.jpg	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=c5461595b9330238aaa24dfc9d3686e5&imgtype=0&src=http%3A%2F%2Fdpic.tiankong.com%2Fln%2Fi9%2FQJ6379153906.jpg%3Fx-oss-process%3Dstyle%2Fshow	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=9bbdd5f21e5c5900aaee7df33b145b04&imgtype=0&src=http%3A%2F%2Fmpic.tiankong.com%2Fd02%2Fc6a%2Fd02c6af0587ecebfdd2ad43a5ee52132%2F640.jpg%40%2521670w	com/imisingmlm/apps/UI
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1600074913955&di=e63515de4495130abe32181b941f3424&imgtype=0&src=http%3A%2F%2Fdpic.tiankong.com%2Ftz%2Fsa%2FQJ6990922167.jpg%3Fx-oss-process%3Dstyle%2Fshow	com/imisingmlm/apps/UI
https://img.tianyancha.com/tmp/19051710/958188891013/edit_company503992.png@!fill_200x200	com/imisingmlm/apps/UI
https://img5.tianyancha.com/logo/lll/e1b941681af34d681682132623a44d19.png@!f_200x200	com/imisingmlm/apps/UI
https://img5.tianyancha.com/logo/lll/715a10081596006e8c0f2c99d932e666.png@!f_200x200	com/imisingmlm/apps/UI
http://dog.hotbuybuy.com/api/dog/list/1/0	com/imisingmlm/apps/UI
https://mp.weixin.qq.com/s/qltDyNdnEcmxk9FTD72fLQ?sc=an_vivo&parent=isApp&versionNumber=2.1.1	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/224,01ddeba9725375f7.png	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/203,01ddeb72309fe2af.png	com/imisingmlm/apps/UI
https://cdn.doumistatic.com/215,01ddeb5f1b55a71c.png	com/imisingmlm/apps/UI
http://dog.hotbuybuy.com/api/dog/list/1/0	com/imisingmlm/apps/UI

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

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.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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=imjianzhi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-09-03 03:47:46+00:00
Valid To: 2046-08-28 03:47:46+00:00
Issuer: CN=imjianzhi
Serial Number: 0x2954d3c5
Hash Algorithm: sha256
md5: 3436b17980b6d7b4dc85d7a92c1e244d
sha1: 501fa8da5071ced89edb53c0e63db813e33ae78d
sha256: fe8eddaa6a33e027e0f8729355953d68b0397e801f306d26b24085e36fc90c1a
sha512: 887706ec534af70f55e7c75420683946cb828162917c96ca95032c5d64415f9e3f6a35b3fc9cf2652c559321b46103174f5702b80f3c7db131c28e1f00f9724f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 04014f072bd8df90fd7c305d215c3d7061ce31dd1f242f981896d49fb48b8c6b

硬编码敏感信息

可能的敏感信息
"blend_pwd" : "請輸入英數混合至少8位數的密碼"
"forget_password" : "忘记密码"
"forget_pwd_code" : "验证码"
"forget_pwd_input_code" : "请填写您的验证码"
"forget_pwd_title" : "请输入注册所填写的 E-mail，我们将寄出验证码给您"
"input_password" : "密码为8-20英数字组合"
"password" : "密码"
"pls_input_password" : "请填写您的密码"

可能的敏感信息
"rebuild_pwd" : "重設密碼"

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机 / Build.FINGERPRINT check 编译器 / unknown (please file detection issue!)