MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

法大大
FADADA

法大大 5.1.20.APK

APP名称:	法大大
包名:	com.fadada
域名线索:	2条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年2月2日 19:45

文件信息

文件名: fadada369694.apk
文件大小: 12.06MB
MD5值: 319f2e0d9e8dc8027f16a2b0d7cdc9c7
SHA1值: 0e1ae658f60e7e04ec82049bb0f75bc418eeb657
SHA256值: 3d781b2006f07b495d5b7c327997d97addc2c406d499ec164890ab671275109f

APP 信息

App名称: 法大大
包名: com.fadada
主活动**Activity:** com.fadada.android.ui.SplashActivity
安卓版本名称: 5.1.20
安卓版本: 50120

域名线索

域名	是否危险域名	服务器信息
www.fadada.com	good	**IP:** 116.211.155.251 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
www.fadada.com进行操作	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://www.fadada.com进行操作	Android String Resource
https://www.fadada.com/充值后再发起签署	Android String Resource
https://www.fadada.com	Android String Resource
https://www.fadada.com/	Android String Resource
www.fadada.com	Android String Resource

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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

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
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True

Found 1 unique certificates
Subject: C=86, ST=GuangDong, L=SZ, O=CN, OU=CN, CN=Fadada
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-04-16 04:35:41+00:00
Valid To: 2115-03-23 04:35:41+00:00
Issuer: C=86, ST=GuangDong, L=SZ, O=CN, OU=CN, CN=Fadada
Serial Number: 0x5846c527
Hash Algorithm: sha256
md5: 9dd2dde2fb4c0c5c0aea28a677ac11e7
sha1: 8684cca9563337f3d5b563f7b28ac4b91770cada
sha256: 9933e0af77300b3c4fb01bed89a82e4fd5e68da81344f22751ec1e1df6857ee6
sha512: 042ec89299953be8afd9d0efe8bb6f3cd936e8c87cb8d6e82b1d7b7f555340d19c07501eb4710f2070e43cd50035b0b2ab248edd4d03bb889c0ee2051b1fa601
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b9f8c38b894a5f33a4cb817078a081aa11d369d1dea8fd8ecab315cf9def35cf

硬编码敏感信息

可能的敏感信息
"ca_certificate" : "CA证书"
"company_authenticate_guide" : "请进行企业实名认证"
"company_authenticate_guide_content" : "企业实名认证将获得具有法律效应企业电子印章，可用于签署企业级电子文书处理用途"
"fingerprint_password" : "指纹密码"
"identity_authentication_center" : "身份认证中心"
"login_password" : "登录密码"
"modify_login_password" : "修改登录密码"

可能的敏感信息
"no_authorization_sign_tips" : "您没有授权可使用的企业签章 请联系管理员授权"
"personal_real_name_authentication_prompt" : "身份认证成功后将赋予电子签名法律效力，可用于各种电子签约处理用途"
"real_name_authentication_ca_certificate" : "实名认证CA证书"
"set_password" : "设置密码"
"setting_login_password" : "设置登录密码"
"type_of_certificate" : "证件类型"
"unauthenticated_user" : "未认证用户"
"view_certificate" : "查看证书"
"wbcf_user_auth_protocol_name" : "《个人信息处理授权书》"

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>SecNeo.A
Bangcle (SecShell)</td></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libturingmfa.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>
