



MoGua

SPOTLED 1.9.4.APK 分析报告



APP名称:

SPOTLED

包名:	com.led.spotled
域名线索:	14条
URL线索:	21条
邮箱线索:	0条
分析日期:	2025年5月6日
分析平台:	摸瓜APK反编译平台

文件名: 4_base.apk
文件大小: 15.57MB
MD5值: 51a6da421fc844ac6718f395933a7ae2
SHA1值: baceacd5cf07b115303e72197b0bb05bc24ca364
SHA256值: 3008ca52e467aa75293a420a840b081a361aed9481d49b4a4057a7e6552dcbf3

i APP 信息

App名称: SPOTLED
包名: com.led.spotled
主活动Activity: com.led.spotled.activity.MainActivity
安卓版本名称: 1.9.4
安卓版本: 61

🔍 域名线索

域名	服务器信息
oss-cn-.aliyuncs.comor	没有服务器地理信息.
mta.oa.com	IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
pingma.qq.com	IP: 116.147.19.64 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

oss.aliyuncs.com	IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mta.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
image.cnamedomain.com	没有服务器地理信息.
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.189 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
led.spotled.xyz	IP: 47.104.29.90 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
	IP: 20.205.243.166 所属国家: Singapore

github.com	地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
203.107.1.1	IP: 203.107.1.1 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
open.weixin.qq.com	IP: 140.207.58.67 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
schemas.android.com	没有服务器地理信息.
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

URL线索

URL信息	Url所在文件
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java

http://image.cnamedomain.com/!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://203.107.1.1/181345/d?host=	com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com/!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://led.spotled.xyz/customer/101	com/led/spotled/Constants.java
https://led.spotled.xyz/	com/led/spotled/Constants.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java

邮箱线索

手机线索

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=ch, ST=cd, L=sichuan, O=company, OU=company, CN=kryl

签名算法: rsassa_pkcs1v15

有效期自: 2019-08-28 07:17:45+00:00

有效期至: 2052-08-19 07:17:45+00:00

发行人: C=ch, ST=cd, L=sichuan, O=company, OU=company, CN=kryl

序列号: 0x1c949e6c
哈希算法: sha256
md5值: c6e49b8e47644cd52973c6a1ed0818f5
sha1值: 6f707330f4c08662b1473da9ccaa6fa3a5672aed
sha256值: 67b3dd7f0fcd1b1b9f62dff7614cb0f01da4c1b25f0924d15cf071447bd14dc
sha512值: 2ba091f085623fbe05aad02d2338b446e7e4f2559d81d3fa20251b12295040562fbc4601f9fcd3071934a96971d2295c847d60afdcd231736b738f14c8bffeeb
公钥算法: rsa
密钥长度: 2048
指纹: 0ebf0e0d247f8adfe7a4a4bed22d519754c4d8953782abcbeebd060a206f1a

硬编码敏感信息

可能的敏感信息
"edit_password" : "Change the password"
"forget_password" : "Forgot password"
"google_api_key" : "AlzaSyDiCqdXoK1bETcm2gH5RDIKHwmqQ98YaT4"
"google_crash_reporting_api_key" : "AlzaSyDiCqdXoK1bETcm2gH5RDIKHwmqQ98YaT4"
"inconsistent_password" : "Inconsistent passwords"
"reset_password" : "To reset your password"
"edit_password" : "修改密码"
"forget_password" : "忘记密码"
"inconsistent_password" : "两次密码输入不一致"
"reset_password" : "重置密码"
"edit_password" : "Alterar senha"

edit_password : Alterar senha
"forget_password" : "Esquecer-se da sua senha?"
"inconsistent_password" : "As senhas introduzidas duas vezes não são correspondes"
"reset_password" : "Redefinir a senha"
"edit_password" : "修改密碼"
"forget_password" : "忘記密碼"
"inconsistent_password" : "兩次密碼輸入不一致"
"reset_password" : "重置密碼"
"edit_password" : "Ändern des Kennworts"
"forget_password" : "Passwort vergessen"
"inconsistent_password" : "Zwei Passworteingaben sind inkonsistent"
"reset_password" : "Zurücksetzen des Kennworts"
"edit_password" : "เปลี่ยนรหัสผ่าน"
"forget_password" : "ลืมรหัสผ่าน"
"inconsistent_password" : "การป้อนรหัสผ่านสองครั้งไม่สอดคล้องกัน"
"reset_password" : "รีเซ็ตรหัสผ่าน"
"edit_password" : "パスワード変更"
"forget_password" : "パスワードを忘れた"

"inconsistent_password" : "二回のパスワードが不一致"
"reset_password" : "パスワードリセット"
"edit_password" : "Changer le mot de passe"
"forget_password" : "Mot de passe oublié"
"inconsistent_password" : "Deux entrées de mot de passe sont incohérentes"
"reset_password" : "Réinitialisation du mot de passe"
"edit_password" : "비밀번호 수정하기"
"forget_password" : "비밀번호 잊어버렸습니다"
"inconsistent_password" : "두 번의 비밀번호 입력이 일치하지 않습니다"
"reset_password" : "비밀번호 리셋"
"edit_password" : "Cambiar contraseña"
"forget_password" : "He olvidado la contraseña"
"inconsistent_password" : "Las contraseñas no coinciden"
"reset_password" : "Restablecer contraseña"
"edit_password" : "Change the password"
"forget_password" : "Forgot password"
"inconsistent_password" : "Inconsistent passwords"
"reset_password" : "To reset your password"

"edit_password" : "Cambiare la password"
"forget_password" : "Hai dimenticato la tua password?"
"inconsistent_password" : "Due voci di password non corrispondono"
"reset_password" : "Ripristina la password"
"edit_password" : "Измени пароль"
"forget_password" : "Забыли пароль"
"inconsistent_password" : "Две записи пароля несовместимы"
"reset_password" : "Заново установить пароль"

 加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

 第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

☰ 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.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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADVERTISE	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
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_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.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

com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.led.spotled.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。