MoGua

LBH 1.6.15.APK 分析报告

APP名称: LBH

包名:	com.weilaiapplbh
域名线索:	12条
URL线索:	3条
邮箱线索:	0条
分析日期:	2025年1月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 6323c9e2daae0.apk
文件大小: 52.26MB
MD5值: acb9b1a0b4aecff8570e7f2be4ca2635
SHA1值: d863f907f796b14ac6132acebf3d0b05f750364f
SHA256值: cbbb11f23984dfee6cb78610a749cc2543142b6b6a8eac4154186361e120b26b

APP 信息

App名称: LBH
包名: com.weilaiapplbh
主活动Activity: com.netease.nim.main.main.activity.WelcomeActivity
安卓版本名称: 1.6.15
安卓版本: 150

域名线索

域名	服务器信息
metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.asia	没有服务器地理信息.
grs.dbankcloud.cn	**IP**: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

store.hispace.hicloud.com	**IP**: 49.4.38.106 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics1.data.hicloud.com	**IP**: 114.115.188.152 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
nim-sdk.firebaseio.com	**IP**: 34.120.160.131 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.eu	没有服务器地理信息.
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
	IP: 49.4.35.16 **所属国家**: China

appgallery.cloud.huawei.com	**地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
grs.dbankcloud.com	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
play.google.com	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
https://nim-sdk.firebaseio.com	Mogua Engine V1
https://play.google.com/store	Mogua Engine V1
https://appgallery.cloud.huawei.com/app/	Mogua Engine V1
https://play.google.com/store/apps/details?id=	Mogua Engine V1
https://appgallery.cloud.huawei.com	Mogua Engine V1
https://store.hispace.hicloud.com/hwmarket/api/	Mogua Engine V1

https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2

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=sign.keyyuingstore, ST=sign.keyyuingstore, L=sign.keyyuingstore, O=sign.keyyuingstore, OU=sign.keyyuingstore, CN=sign.keyyuingstore
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-15 10:05:54+00:00
有效期至: 2025-06-10 10:05:54+00:00

发行人: C=sign.keyyuingstore, ST=sign.keyyuingstore, L=sign.keyyuingstore, O=sign.keyyuingstore, OU=sign.keyyuingstore, CN=sign.keyyuingstore
序列号: 0x7efd560c
哈希算法: sha256
md5值: 57e13f55f700bf3f66a888a9a11c102a
sha1值: 2acc894cd8beda2dea9b2f43e1e9176282f7610c
sha256值: 2a879ca1e066f1413a4ab1ca9d9020cacbca29e26e74993f68b1dbbf34ed8a16
sha512值: cb3f62283fc4e814d9fddc831077272bf573a2d719896ed1858cf6f461f103b11cb928547dbb48782069f5ad8abdf33f02f22b68c15a1b27085f35f52fa51a26
公钥算法: rsa
密钥长度: 1024
指纹: 5c863b45029bba4fdfe6292a469d8bacfca5aef23d9a267c35b59fca7c79f28c

🔑 硬编码敏感信息

可能的敏感信息
"accept_session" : "接受"
"agian_pwd" : "请再一次输入密码"
"cancel_private_chat" : "暂禁止私聊！"
"cloud_session_list" : "云端会话列表"
"end_session_tip_content" : "退出后，你将不再接收白板演示的消息内容"
"end_session_tip_head" : "退出白板演示"
"firebase_database_url" : "https://nim-sdk.firebaseio.com"
"forget_pwd" : "重置支付密码"
"google_api_key" : "AIzaSyCL6S3DSVG3nTZjDr4UwKZQMB8NwL3Lgog"
"google_crash_reporting_api_key" : "AIzaSyCL6S3DSVG3nTZjDr4UwKZQMB8NwL3Lgog"

"input_password" : "请输入密码，6~20位字母或者数字"
"input_pwd" : "请输入支付密码"
"jrmf_w_get_pwd_title" : "找回支付密码"
"jrmf_w_no_authen" : "未实名认证"
"jrmf_w_pwd_not_same" : "两次密码输入不一致"
"jrmf_w_set_pwd_suc" : "支付密码设置成功"
"main_tab_session" : "会话"
"no_more_session" : "没有更多会话了"
"no_remmeber_pwd" : "取消记住密码！"
"nrtc_setting_other_device_default_rotation_key" : "nrtc_setting_other_device_default_rotation_key"
"nrtc_setting_other_device_rotation_fixed_offset_key" : "nrtc_setting_other_device_rotation_fixed_offset_key"
"nrtc_setting_other_server_record_audio_key" : "nrtc_setting_other_server_record_audio_key"
"nrtc_setting_other_server_record_video_key" : "nrtc_setting_other_server_record_video_key"
"nrtc_setting_vie_crop_ratio_key" : "nrtc_setting_vie_crop_ratio_key"
"nrtc_setting_vie_default_front_camera_key" : "nrtc_setting_vie_default_front_camera_key"
"nrtc_setting_vie_fps_reported_key" : "nrtc_setting_vie_fps_reported_key"
"nrtc_setting_vie_hw_decoder_key" : "nrtc_setting_vie_hw_decoder_key"

"nrtc_setting_vie_hw_encoder_key" : "nrtc_setting_vie_hw_encoder_key"
"nrtc_setting_vie_max_bitrate_key" : "nrtc_setting_vie_max_bitrate_key"
"nrtc_setting_vie_quality_key" : "nrtc_setting_vie_quality_key"
"nrtc_setting_vie_rotation_key" : "nrtc_setting_vie_rotation_key"
"nrtc_setting_voe_audio_aec_key" : "nrtc_setting_voe_audio_aec_key"
"nrtc_setting_voe_audio_ns_key" : "nrtc_setting_voe_audio_ns_key"
"nrtc_setting_voe_call_proximity_key" : "nrtc_setting_voe_call_proximity_key"
"nrtc_setting_voe_high_quality_key" : "nrtc_setting_voe_high_quality_key"
"private_chat" : "是否允许用户私聊"
"private_config_note" : " 1.私有化配置的将在app重启后生效，请注销登陆并杀掉进程。 2.如果要切换到环境，关闭或打开开关退出登陆杀掉进程即可。 "
"pwd_agian_fail" : "两次密码输入不一样，请检查！"
"pwd_not_same" : "两次密码输入不一致，请重新输入"
"pwd_too_easy" : "密码太简单,请重新输入！"
"receive_session" : "对方发起白板演示"
"reject_session" : "拒绝"
"remember_pwd" : "记住密码"
"remmeber_pwd" : "记住密码！"
"res_pwd_succ" : "重置密码成功"

"session_end_record" : "白板演示已结束"

"setting_private_config" : "私有化配置"

"start_session" : "正在邀请对方，请稍后"

"start_session_record" : "我发起了白板演示"

"target_has_end_session" : "对方结束白板演示"

"team_authentication" : "身份验证"

"team_invitee_authentication" : "被邀请人身份验证"

"team_invitee_need_authen" : "需要验证"

"team_invitee_not_need_authen" : "不需要验证"

"team_need_authentication" : "需要身份验证"

"updata_pwd" : "修改密码"

"view_cloud_session" : "查看云端会话"

"ysf_dialog_close_session" : "确认退出对话？ "

"ysf_menu_close_session" : "退出"

"ysf_work_sheet_auth" : "填写信息"

"ysf_work_sheet_session_change" : "工单已过期"

"agian_pwd" : "Vui lòng nhập lại mật khẩu"

"cancel_private_chat" : "Cấm nói chuyện riêng！"

"cloud_session_list" : "Trình đầu cuốiComment"

"forget_pwd" : "重置支付密码"

"input_password" : "Hãy nhập mật khẩu, 6~20 letters or numbers"

"input_pwd" : "请输入支付密码"

"jrmf_w_get_pwd_title" : "找回支付密码"

"jrmf_w_no_authen" : "未实名认证"

"jrmf_w_pwd_not_same" : "两次密码输入不一致"

"jrmf_w_set_pwd_suc" : "支付密码设置成功"

"main_tab_session" : "Tin nhắn"

"no_more_session" : "Không còn gì cả"

"no_remmeber_pwd" : "Không ghi nhớ mật khẩu！"

"private_chat" : "Cho phép người dùng chat riêng"

"private_config_note" : " 1.Cấu hình dành riêng sẽ có tác dụng sau khi ứng dụng được khởi chạy lại. Vui lòng ngắt kết nối và tắt tiến trình. 2.Nếu bạn muốn chuyển sang môi trường, tắt hay bật công tắc để thoát ra bằng cách đăng nhập và tắt quá trình. "

"pwd_agian_fail" : "Hai mật khẩu không giống nhau, vui lòng kiểm tra！"

"pwd_not_same" : "两次密码输入不一致，请重新输入"

"pwd_too_easy" : "Mật khẩu quá đơn giản, vui lòng nhập lại！"

"remember_pwd" : "Nhớ mật khẩu"

"remember_pwd" : "Nhớ mật khẩu"
"remmeber_pwd" : "Nhớ mật khẩu！"
"res_pwd_succ" : "重置密码成功"
"setting_private_config" : "Cấu hình Privatation"
"team_authentication" : "Chính xác"
"team_invitee_authentication" : "Xác thực mời"
"team_invitee_need_authen" : "Cần miếng dán"
"team_invitee_not_need_authen" : "Không cần kiểm tra"
"team_need_authentication" : "Phải xác thực"
"updata_pwd" : "Đổi mật khẩu"
"view_cloud_session" : "Xem ảnh mây"
"agian_pwd" : "Please enter the password again"
"cancel_private_chat" : "Private chat is temporarily prohibited!"
"cloud_session_list" : "Cloud session list"
"input_password" : "Please enter password， 6~20 letters or numbers"
"main_tab_session" : "conversation"
"no_more_session" : "no more sessions"
"no_remmeber_pwd" : "Cancel remember password！"

"private_chat" : "Whether to allow users to chat privately"

"private_config_note" : " 1.The privatization configuration will take effect after the app is restarted， Please log out and log in and kill the process。 2. If you want to switch to the environment， Close or open the switch to log out and kill the process。 "

"pwd_agian_fail" : "Different passwords entered twice，Please check！"

"pwd_too_easy" : "password is too simple, please enter again！"

"remember_pwd" : "remember password"

"remmeber_pwd" : "remember password！"

"setting_private_config" : "Privatization configuration"

"team_authentication" : "Authentication"

"team_invitee_authentication" : "Invitee Authentication"

"team_invitee_need_authen" : "requires verification"

"team_invitee_not_need_authen" : "No verification required"

"team_need_authentication" : "Authentication required"

"updata_pwd" : "change Password"

"view_cloud_session" : "View cloud session"

"agian_pwd" : "Silakan masukkan kata sandi lagi"

"cancel_private_chat" : "Larang sementara obrolan pribadi！"

"cloud_session_list" : "Daftar sesi cloud"

"forget_pwd" : "重置支付密码"
"input_password" : "Silakan masukkan kata sandi，6~20 huruf atau angka"
"input_pwd" : "请输入支付密码"
"jrmf_w_get_pwd_title" : "找回支付密码"
"jrmf_w_no_authen" : "未实名认证"
"jrmf_w_pwd_not_same" : "两次密码输入不一致"
"jrmf_w_set_pwd_suc" : "支付密码设置成功"
"main_tab_session" : "percakapan"
"no_more_session" : "tidak ada sesi lagi"
"no_remmeber_pwd" : "Batalkan ingat kata sandi！"
"private_chat" : "Apakah akan mengizinkan pengguna untuk mengobrol secara pribadi"
"private_config_note" : " 1.Konfigurasi privatisasi akan berlaku setelah aplikasi dimulai ulang，Silakan logout dan login dan matikan prosesnya。 2.Jika Anda ingin beralih ke lingkungan，Tutup atau buka sakelar untuk keluar dan mematikan prosesnya。 "
"pwd_agian_fail" : "Kedua kata sandi berbeda, silakan periksa!"
"pwd_not_same" : "Kedua entri kata sandi tidak konsisten, silakan masukkan kembali"
"pwd_too_easy" : "Kata sandinya terlalu sederhana, silakan masukkan kembali！"
"remember_pwd" : "ingat kata Sandi"
"remmeber_pwd" : "Ingat kata sandinya!"

"res_pwd_succ" : "重置密码成功"
"setting_private_config" : "Konfigurasi privatisasi"
"team_authentication" : "Autentikasi"
"team_invitee_authentication" : "Otentikasi Undangan"
"team_invitee_need_authen" : "memerlukan verifikasi"
"team_invitee_not_need_authen" : "Tidak diperlukan verifikasi"
"team_need_authentication" : "Otentikasi diperlukan"
"updata_pwd" : "ganti kata sandi"
"view_cloud_session" : "Lihat sesi cloud"

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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.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.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.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_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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.weilaiapplbh.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
com.weilaiapplbh.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.weilaiapplbh.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.weilaiapplbh.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	知	permission	Unknown permission from android reference
com.weilaiapplbh.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.weilaiapplbh.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.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。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知	在 htc 手机的应用程序启动图标上显示通知计数或徽章。

		计数	
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
	正	在应用程序	

com.oppo.launcher.permission.READ_SETTINGS	常	上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.netease.nim.main.main.activity.WelcomeActivity	Schemes: easychat://,

com.netease.nim.main.main.activity.MixPushActivity	Schemes: pushscheme://, Hosts: com.huawei.codelabpush, Paths: /deeplink,
com.netease.yunxin.nertc.nertcvideocall.push.SignallingHuaweiPushActivity	Schemes: pushscheme://, Hosts: com.netease.nimlib.avsignalling.push, Paths: /huawei,

---