MoGua

BrightChat 3.2.13.APK 分析报告

APP名称:	BrightChat
包名:	com.mycurrentmessenger

域名线索:	33条
URL线索:	45条
邮箱线索:	6条
分析日期:	2025年4月24日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: BrightChat - Secure Messaging_3.2.13_Apkpure.apk
文件大小: 68.55MB
MD5值: 33de85c58484c68ae802e7ec5b86e04c
SHA1值: 7951052e344cfcf7890c8223a9b3e5736ead71d8
SHA256值: 15f2282f743a8c2f97901476618653be61898eaabe97a8054cf771f1eeff96ba

APP 信息

App名称: BrightChat
包名: com.mycurrentmessenger
主活动Activity: com.mycurrentmessenger.ui.activities.SplashActivity
安卓版本名称: 3.2.13
安卓版本: 3002013

域名线索

域名	服务器信息
logback.qos.ch	**IP**: 159.100.250.151 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
shenxun-b9ed1.firebaseio.com	**IP**: 35.201.97.85 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
schemas.android.com	没有服务器地理信息.
aomediacodec.github.io	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 159.100.250.151 **所属国家**: Switzerland

www.slf4j.org	**地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
www.brightchat.com	IP: 104.196.141.80 **所属国家**: United States of America **地区**: South Carolina **城市**: North Charleston **纬度**: 32.888702 **经度**: -80.007584
rest.mycurrentmessenger.com	IP: 34.102.237.245 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
apache.org	IP: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
u.mycurrentmessenger.com	IP: 34.117.245.71 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
callsurvey.shenxunchat.com	IP: 35.203.179.200 **所属国家**: United States of America **地区**: Oregon **城市**: The Dalles **纬度**: 45.594784 **经度**: -121.178688
	IP: 13.224.141.70 **所属国家**: Japan

www.zetetic.net	**地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
im01.epochtimes.com	IP: 74.86.118.24 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
xml.org	IP: 104.239.240.11 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
crbug.com	IP: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
messagingtest.mycurrentmessenger.com	IP: 104.196.156.174 **所属国家**: United States of America **地区**: South Carolina **城市**: North Charleston **纬度**: 32.888702 **经度**: -80.007584
updates2.signal.org	IP: 199.59.149.201 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
	IP: 142.251.43.14 **所属国家**: United States of America

maps.google.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ns.adobe.com	没有服务器地理信息.
javax.xml.xmlconstants	没有服务器地理信息.
www.google.com	**IP**: 148.163.48.215 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.439648 **经度**: -112.026154
www.epochbase.com	**IP**: 34.107.159.216 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
www.ietf.org	**IP**: 104.16.45.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.googleapis.com	**IP**: 142.251.43.10 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991

	经度: -122.078514
sfu.webhop.me	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 **纬度**: 1.289987 **经度**: 103.850281
play.google.com	**IP**: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
support.brightchat.com	**IP**: 104.16.55.111 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
o.mycurentmessanger.com	**IP**: 66.135.16.60 **所属国家**: United States of America **地区**: New Jersey **城市**: Piscataway **纬度**: 40.540092 **经度**: -74.466194
xmlpull.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 173.194.174.82 **所属国家**: United States of America

webrtc.googlesource.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
issuetracker.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
www.webrtc.org	**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://issuetracker.google.com/issues/new?component=413107&template=1096568	a2/c.java
https://o.mycurentmessanger.com/processPost.php	a2/i.java
https://messagingtest.mycurrentmessenger.com:8080/	a8/d.java
https://rest.mycurrentmessenger.com/	a8/d.java
https://play.google.com/store/apps/details?id=com.mycurrentmessenger	ab/a.java
http://www.w3.org/TR/SVG11/feature	com/caverock/androidsvg/SVGParser.java

http://www.w3.org/2000/svg	com/caverock/androidsvg/SVGParser.java
http://www.w3.org/1999/xlink	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-general-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-parameter-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/properties/lexical-handler	com/caverock/androidsvg/SVGParser.java
http://xmlpull.org/v1/doc/features.html	com/caverock/androidsvg/SVGParser.java
http://javax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/disallow-doctype-decl	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://schemas.android.com/apk/res/android	com/hbb20/CountryCodePicker.java
https://sfu.webhop.me	com/mycurrentmessenger/features/call/a.java
https://callsurvey.shenxunchat.com/addlog/	com/mycurrentmessenger/features/callfeedback/CallFeedbackActivity.java
https://www.google.com/maps/search/?api=1&query=	com/mycurrentmessenger/features/conversationRoom/MediaFullScreenViewActivity.java
https://maps.google.com/maps	com/mycurrentmessenger/features/conversationRoom/maps/a.java
https://www.googleapis.com/auth/drive.appdata	com/mycurrentmessenger/features/devicetransfer/ui/newdevice/TransferOrRestoreFragment.java
https://rest.mycurrentmessenger.com/rs/api/mobile/confirm	com/mycurrentmessenger/features/devicetransfer/ui/newdevice/RestoreAccountActivity.java
https://www.googleapis.com/auth/drive.appdata	com/mycurrentmessenger/features/settings/security/backups/GoogleDrive/GoogleDriveDownloadWorker.java
https://www.googleapis.com/auth/drive.appdata	com/mycurrentmessenger/features/settings/security/backups/GoogleDrive/GoogleDriveUploadWorker.java
https://rest.mycurrentmessenger.com/rs/api/mobile/confirm	com/mycurrentmessenger/ui/activities/CaptchaActivity.java

https://rest.mycurrentmessenger.com/rs/api/mobile/recaptchainit	com/mycurrentmessenger/ui/activities/CaptchaActivity.java
https://rest.mycurrentmessenger.com/rs/api/mobile/confirm	com/mycurrentmessenger/ui/activities/ActivationActivity.java
https://rest.mycurrentmessenger.com/rs/api/mobile/confirm	com/mycurrentmessenger/ui/activities/PhoneNumberActivity.java
https://www.brightchat.com/privacy	com/mycurrentmessenger/ui/activities/PolicyActivity.java
https://www.googleapis.com/auth/drive.appdata	com/mycurrentmessenger/ui/activities/StartupActivity.java
https://maps.google.com/maps	com/mycurrentmessenger/util/m1.java
https://www.google.com/maps/	com/mycurrentmessenger/util/m1.java
https://callsurvey.shenxunchat.com/	com/mycurrentmessenger/util/o0.java
https://u.mycurrentmessenger.com/imupload	com/mycurrentmessenger/util/q3.java
https://www.brightchat.com/intro	com/mycurrentmessenger/util/y3.java
https://messagingtest.mycurrentmessenger.com:8080/	com/mycurrentmessenger/util/p2.java
https://rest.mycurrentmessenger.com/	com/mycurrentmessenger/util/p2.java
https://u.mycurrentmessenger.com	com/mycurrentmessenger/util/u0.java
http://im01.epochtimes.com	com/mycurrentmessenger/util/u0.java
https://im01.epochtimes.com	com/mycurrentmessenger/util/u0.java
http://u.mycurrentmessenger.com	com/mycurrentmessenger/util/u0.java
http://ns.adobe.com/xap/1.0/\u0000	f1/a.java
https://u.mycurrentmessenger.com	g7/d0.java
https://www.epochbase.com/	g7/d0.java

https://u.mycurrentmessenger.com	g7/c3.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	hc/b.java
http://schemas.android.com/apk/res/android	k0/k.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	lc/c.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	lc/e.java
https://support.brightchat.com/hc/en-us/requests/new	o9/r.java
http://logback.qos.ch/codes.html	s3/e.java
https://updates2.signal.org	sa/b.java
http://xml.org/sax/features/validation	t3/e.java
http://xml.org/sax/features/namespaces	t3/e.java
http://www.slf4j.org/codes.html	vj/d.java
http://www.slf4j.org/codes.html	vj/c.java
https://www.googleapis.com/auth/drive.appdata	wa/y.java
https://issuetracker.google.com/issues/new?component=413106	x1/j.java
http://logback.qos.ch/codes.html	y3/f.java
http://logback.qos.ch/codes.html	yj/a.java
https://www.brightchat.com;	Mogua Engine V1
https://shenxun-b9ed1.firebaseio.com	Mogua Engine V1

https://www.brightchat.com/privacy>Privacy	Mogua Engine V1
https://www.brightchat.com	Mogua Engine V1
https://www.zetetic.net/sqlcipher/	Mogua Engine V1
https://www.zetetic.net/sqlcipher/license/	Mogua Engine V1
https://github.com/sqlcipher/android-database-sqlcipher	Mogua Engine V1
https://github.com/vinc3m1	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1
https://www.brightchat.com/privacy>Terms	Mogua Engine V1
https://www.brightchat.com/privacy>Quy	Mogua Engine V1
https://www.brightchat.com/privacy>	Mogua Engine V1
https://crbug.com/1053756	lib/arm64-v8a/libjingle_peerconnection_so.so
https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/,	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00	lib/arm64-v8a/libjingle_peerconnection_so.so
https://aomediacodec.github.io/av1-rtp-spec/	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/arm64-v8a/libjingle_peerconnection_so.so

http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-content-type	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-timing	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/color-space	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id	lib/arm64-v8a/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrext/inband-cn	lib/arm64-v8a/libjingle_peerconnection_so.so

邮箱线索

邮箱地址	所在文件
robot@mycurrentmessenger.com groupchat@mycurrentmessenger.com	g7/g1.java
groupchat@mycurrentmessenger.com	g7/c3.java
support@brightchat.com	u9/d.java
support@brightchat.com 请联系support@brightchat.com重置密码	Mogua Engine V1
robot@mycurrentmessenger.com h3ewxi@mycurrentmessenger.com	Mogua Engine V2

appro@openssl.org	lib/arm64-v8a/libjingle_peerconnection_so.so

手机线索

手机号	所在文件
17179869184	com/caverock/androidsvg/SVGParser.java
17179869184	com/caverock/androidsvg/SVGAndroidRenderer.java
17179869184	com/caverock/androidsvg/SVG.java
17179869184	o7/b.java
15778476000	org/joda/time/chrono/GregorianChronology.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2016-05-12 06:30:04+00:00
有效期至: 2043-09-28 06:30:04+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x4a30021f
哈希算法: sha256
md5值: 1ceeccb22c405f7ff32ce81e5137c651
sha1值: b3d5b54307e0ccbcb39615220985f2d050774ee6
sha256值: 2515b2b5aea3a7ac339c6b3015ef7fb1f65cfdc7e02e39d0195690ab02de706a
sha512值: 3f8c16b4c92d534767ace2a914b3e000f8c585ffc72669c119e6cbbad33e75dc2871fc7e0be164f48dcb289c534b592768026b698e780bdc4feaed2196c78d96
公钥算法: rsa

密钥长度: 2048
指纹: c8b43486c8387276171f0a56d445e9f77209bdc3c63ccbc78afb8a29e78e0531

硬编码敏感信息

可能的敏感信息
"backup_import_wrong_password" : "Password is wrong"
"developer_options_key" : "developer_options_key"
"firebase_database_url" : "https://shenxun-b9ed1.firebaseio.com"
"google_api_key" : "AIzaSyBnP535gssMRt0Dujs9FfNEIrJh8faugpI"
"google_crash_reporting_api_key" : "AIzaSyBnP535gssMRt0Dujs9FfNEIrJh8faugpI"
"google_maps_key" : "AIzaSyDnfx9TdJexd4eSTcWrWi8mLMWgtUJgbo8"
"group_kind_upgrade_to_private_group" : "%1$s upgraded the encryption level to advanced."
"library_android_database_sqlcipher_author" : "Zetetic, LLC"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"pref_advanced_settings_key" : "advanced_settings_key"
"pref_always_online_key" : "always_online_key"
"pref_auto_lock_key" : "auto_lock_preference"

"pref_call_audio_codec_key" : "audiocodec_preference"
"pref_call_audio_settings_key" : "audio_settings_key"
"pref_call_displayhud_key" : "displayhud_preference"
"pref_call_fps_key" : "fps_preference"
"pref_call_hwcodec_key" : "hwcodec_preference"
"pref_call_max_video_bitrate_key" : "maxvideobitrate_preference"
"pref_call_max_video_bitrate_value_key" : "max_video_bitrate_value_preference"
"pref_call_other_settings_key" : "call_other_settings_key"
"pref_call_resolution_key" : "resolution_preference"
"pref_call_start_audio_bitrate_key" : "startaudiobitrate_preference"
"pref_call_video_codec_key" : "videocodec_preference"
"pref_call_video_settings_key" : "video_settings_key"
"pref_dev_option_key" : "pref_dev_option"
"pref_dev_option_unread_key" : "pref_dev_option_unread"
"pref_enable_upload_encryption_log_key" : "pref_enable_upload_encryption_log_key"
"pref_enable_upload_waveform_log_key" : "pref_enable_upload_waveform_log_key"
"pref_key_realm_key" : "realm_key"
"pref_key_security_two_factor_auth" : "pref_key_security_two_factor_auth"
"pref_link_contact_key" : "pref_link_contact_key"

"pref_relay_key" : "preference_relay_key"

"pref_security_two_factor_auth_summary" : "You can reset Trustee if you have master password or by asking your current trustee to quit."

"pref_security_two_factor_auth_title" : "Two-factor Authentication"

"pref_show_unread_key" : "key_display_unread_count"

"pref_show_upload_log_key" : "show_upload_log_key"

"pref_speakerphone_key" : "speakerphone_preference"

"pref_start_audio_bitrate_value_key" : "start_audio_bitrate_value_preference"

"pref_upload_logs_key" : "upload_logs_key"

"reset_device_key" : "Reset Device Key"

"sample_author" : "— Stephanie Del Valle"

"sample_author_2" : "Dr. Robet W Malone"

"social_misc_password" : "Password"

"backup_import_wrong_password" : "Mật khẩu không đúng"

"group_kind_upgrade_to_private_group" : "%1$s đã nâng cấp độ mã hoá lên nâng cao."

"pref_security_two_factor_auth_summary" : "Bạn có thể xoá người bảo đảm nếu bạn có mật khẩu chính. Hoặc bạn có thể yêu cầu người bảo đảm thoát."

"pref_security_two_factor_auth_title" : "Xác thực hai yếu tố"

"reset_device_key" : "Đặt lại khoá thiết bị"

"social_misc_password" : "Mật khẩu"

"backup_import_wrong_password" : "비밀번호가 맞지 않아요"

"group_kind_upgrade_to_private_group" : "%1$s님이 암호화 수준을 중급으로 변경했습니다"
"pref_security_two_factor_auth_summary" : "신뢰할 수 있는 사용자를 재설정하려면 마스터 패스워드를 사용하거나 현재 신뢰할 수 있는 사용자에게 부탁해야 합니다"
"pref_security_two_factor_auth_title" : "이중 인증"
"reset_device_key" : "장치 키 재설정"
"social_misc_password" : "비밀번호"
"backup_import_wrong_password" : "密码错误！"
"group_kind_upgrade_to_private_group" : "%1$s升级群组加密级别未专家级。"
"pref_security_two_factor_auth_summary" : "设置主密码后，您可以重置Trustee；或者您也可以要求Trustee退出。"
"pref_security_two_factor_auth_title" : "两阶段认证"
"reset_device_key" : "重置设备钥匙"
"social_misc_password" : "密码"
"backup_import_wrong_password" : "密碼錯誤！"
"group_kind_upgrade_to_private_group" : "%1$s升級群組加密級別至專家級。"
"pref_security_two_factor_auth_summary" : "設置主密碼後，您可以重設Trustee，或者是要求您的Trustee 退出。"
"pref_security_two_factor_auth_title" : "兩步驟認證"
"reset_device_key" : "重設裝置金鑰"
"social_misc_password" : "密碼"

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

应用内通信