



にち 9.6.6.APK 分析報告



APP名称:

にち

包名:	com.zucbgc.bdwbdg
域名线索:	54条
URL线索:	52条
邮箱线索:	3条
分析日期:	2025年8月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: hyGf.apk
文件大小: 66.81MB
MD5值: 381983d517232d3501716e4dd033fd1c

SHA1值: 97bd991c2f7bf76e9c823ee494e54aa6aef613f1
SHA256值: b13a42101428e110ff501845519319b3bd4320b178b0a7c6725ee01a0e2b51f4

i APP 信息

App名称: にち
包名: com.zucbgc.bdwbdbg
主活动Activity: org.telegram.ui.LaunchActivity
安卓版本名称: 9.6.6
安卓版本: 25061801

🔍 域名线索

域名	服务器信息
1.15.89.53	IP: 1.15.89.53 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
othstr.beacon.qq.com	IP: 140.206.162.29 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
27.151.172.32	IP: 27.151.172.32 所属国家: China 地区: Fujian 城市: Quanzhou 纬度: 24.913891 经度: 118.585831
	IP: 95.213.253.92

coub.com	所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264200
szcp.mxdx.net	IP: 27.155.98.155 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390 经度: 119.306107
play.google.com	IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig 纬度: 52.266121 经度: 10.526730
ss3.4sqi.net	IP: 151.101.90.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
otheve.beacon.qq.com	IP: 113.56.189.125 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
maps.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 13.115.13.148

api.stripe.com	所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
www.example.com	IP: 23.197.49.24 所属国家: Japan 地区: Osaka 城市: Ibaraki 纬度: 34.816425 经度: 135.568909
messenger.telegram.org	IP: 31.13.88.26 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
xinstall.top	IP: 124.163.194.237 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
tun-cos-1258344701.file.myqcloud.com	IP: 221.204.20.91 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
	IP: 195.15.222.169

www.slf4j.org	所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180931 经度: 6.138709
tgb-playground.smart-glocal.com	IP: 99.83.179.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
test.snowflake.qq.com	IP: 221.198.69.15 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
bit.909321.xyz	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
console.cloud.tencent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
	IP: 31.13.94.49

youtube.com	所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
htrace.wetvinfo.com	IP: 60.28.215.54 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.instagram.com	IP: 47.88.58.234 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
gips2.baidu.com	IP: 123.117.132.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
snowflake.qq.com	IP: 116.130.220.65 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
1.15.81.219	IP: 1.15.81.219 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 199.59.148.96

www.google.com	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
telegram.org	IP: 130.211.15.150 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
fragment.com	IP: 104.22.72.137 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
xmlpull.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
h.trace.qq.com	IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
youtube.googleapis.com	IP: 142.251.215.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

101.42.6.119	IP: 101.42.6.119 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
likeinstall.cn	IP: 121.199.65.132 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
usher.ttvnw.net	IP: 18.155.68.102 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
1.117.189.122	IP: 1.117.189.122 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tgb.smart-glocal.com	IP: 99.83.179.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
api.map.baidu.com	IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

www.aparat.com	IP: 185.147.178.12 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
1.58.219.129	IP: 1.58.219.129 所属国家: China 地区: Heilongjiang 城市: Harbin 纬度: 45.750000 经度: 126.650002
stripe.com	IP: 54.64.207.232 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
www.youtube.com	IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
instagram.com	IP: 67.15.100.252 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
api.twitch.tv	IP: 31.13.95.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249

player.vimeo.com	IP: 31.13.94.37 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
attheme.org	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
maps.googleapis	没有服务器地理信息.
astat.bugly.qcloud.com	IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
android.bugly.qq.com	IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
1.30.8.153	IP: 1.30.8.153 所属国家: China 地区: Nei Mongol 城市: Baotou 纬度: 40.651909 经度: 109.822922
schema.org	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View

	纬度: 37.405991 经度: -122.078514
res.openinstall.com	IP: 47.121.128.49 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
twitter.com	IP: 108.160.165.53 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

URL线索

URL信息	Url所在文件
https://likeinstall.cn	com/shubao/xinstall/a/e/c.java
https://xinstall.top	com/shubao/xinstall/a/e/c.java
https://stripe.com/docs/stripe.js.	com/stripe/android/Stripe.java
https://stripe.com/docs/stripe.js	com/stripe/android/Stripe.java
https://api.stripe.com	com/stripe/android/net/StripeApiHandler.java
https://stripe.com/api	com/stripe/android/net/StripeApiHandler.java
https://twitter.com/stripestatus,	com/stripe/android/net/StripeApiHandler.java
https://otheve.beacon.qq.com/analytics/v2_upload	com/tencent/beacon/base/net/b/b.java

https://othstr.beacon.qq.com/analytics/v2_upload	com/tencent/beacon/base/net/b/b.java
https://htrace.wetvinfo.com/kv	com/tencent/beacon/a/b/c.java
https://h.trace.qq.com/kv	com/tencent/beacon/a/b/c.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://xmlpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlSlimBuilder.java
http://xmlpull.org/v1/doc/features.html	com/tencent/qcloud/qcloudxml/core/QCloudXml.java
https://tun-cos-1258344701.file.myqcloud.com/fp.js	com/tencent/qimei/s/c.java
https://tun-cos-1258344701.file.myqcloud.com/my.html	com/tencent/qimei/s/c.java
https://tun-cos-1258344701.file.myqcloud.com/fp.js	com/tencent/qimei/s/a.java
https://test.snowflake.qq.com/ola	com/tencent/qimei/e/a.java
https://snowflake.qq.com/ola	com/tencent/qimei/e/a.java
https://res.openinstall.com/%s.dnc	io/openinstall/sdk/j.java
https://api.map.baidu.com/staticimage/v2	org/telegram/messenger/BuildVars.java
http://gips2.baidu.com/it/u=195724436,3554684702&fm=3028&app=3028&f=JPEG&fmt=auto?w=1280&h=960	org/telegram/messenger/BuildVars.java
https://t.me/proxy?	org/telegram/messenger/SharedConfig.java

https://t.me/socks?	org/telegram/messenger/SharedConfig.java
https://play.google.com/store/account/subscriptions?sku=%s&package=%s	org/telegram/messenger/BillingController.java
https://telegram.org/dl	org/telegram/messenger/ContactsController.java
https://static-maps	org/telegram/messenger/ImageLoader.java
https://maps.googleapis	org/telegram/messenger/ImageLoader.java
https://t.me/+PublicChat	org/telegram/messenger/MessageObject.java
https://instagram.com/	org/telegram/messenger/MessageObject.java
https://www.instagram.com/explore/tags/	org/telegram/messenger/MessageObject.java
https://twitter.com/	org/telegram/messenger/MessageObject.java
https://twitter.com/hashtag/	org/telegram/messenger/MessageObject.java
http://www.example.com	org/telegram/messenger/support/customtabsclient/shared/CustomTabsHelper.java
http://t.me/	org/telegram/messenger/browser/Browser.java
https://t.me/	org/telegram/messenger/browser/Browser.java
https://)?t\\.me/iv\\??(/.*	org/telegram/messenger/browser/Browser.java
https://)?telegram\\.org/(blog	org/telegram/messenger/browser/Browser.java
https://)?fragment\\.com(/.*	org/telegram/messenger/browser/Browser.java
http://www.google.com	org/telegram/messenger/browser/Browser.java
https://fragment.com/username/	org/telegram/ui/ChangeUsernameActivity.java
https://fragment.com	org/telegram/ui/ChangeUsernameActivity.java

http://1.30.8.153:8088/images/yeastar.ico	org/telegram/ui/JMTFastShotManager.java
http://1.15.81.219:8088/static/common/images/icon-play.png	org/telegram/ui/JMTFastShotManager.java
http://1.58.219.129:8088/source?get=Vesn%20Data.gif	org/telegram/ui/JMTFastShotManager.java
http://27.151.172.32:8088/dist/OEM/GOCLOUD/favicon.ico	org/telegram/ui/JMTFastShotManager.java
http://szcp.mxdx.net:8088/cache/suzhiceping_exe/n3/res/_A406AAA462DF6EEC06E61D67.png	org/telegram/ui/JMTFastShotManager.java
http://bit.909321.xyz:8088/static/img/icons/favicon-32x32.png	org/telegram/ui/JMTFastShotManager.java
http://1.15.89.53:8088/Content/img/login-input-icon.png	org/telegram/ui/JMTFastShotManager.java
http://1.117.189.122:8088/TruckMng/Content/Images/dsico.ico	org/telegram/ui/JMTFastShotManager.java
http://console.cloud.tencent.com:9999	org/telegram/ui/JMTFastShotManager.java
https://t.me/	org/telegram/ui/PremiumPreviewFragment.java
https://t.me/\$	org/telegram/ui/PremiumPreviewFragment.java
https://fragment.com/username/	org/telegram/ui/ChannelCreateActivity.java
https://fragment.com/username/	org/telegram/ui/ChatEditTypeActivity.java
https://ss3.4sqi.net/img/categories_v2/	org/telegram/ui/LocationActivity.java
http://maps.google.com/maps	org/telegram/ui/LocationActivity.java
https://t.me/+%s	org/telegram/ui/PrivacyControlActivity.java
https://tgb-playground.smart-glocal.com/cds/v1/tokenize/card	org/telegram/ui/PaymentFormActivity.java
https://tgb.smart-glocal.com/cds/v1/tokenize/card	org/telegram/ui/PaymentFormActivity.java

https://t.me/BotFather	org/telegram/ui/ChatEditActivity.java
https://t.me/BotFather?start=	org/telegram/ui/ChatEditActivity.java
https://telegram.org/embed	org/telegram/ui/ArticleViewer.java
https://telegram.org/deactivate?phone=	org/telegram/ui/PassportActivity.java
https://t.me/	org/telegram/ui/PhotoViewer.java
https://t.me/	org/telegram/ui/LaunchActivity.java
http://schema.org/CompletedActionStatus	org/telegram/ui/LaunchActivity.java
http://schema.org/FailedActionStatus	org/telegram/ui/LaunchActivity.java
https://fragment.com	org/telegram/ui/ProfileActivity.java
https://t.me/proxy?	org/telegram/ui/ProxySettingsActivity.java
https://t.me/socks?	org/telegram/ui/ProxySettingsActivity.java
https://telegram.org	org/telegram/ui/ThemePreviewActivity.java
https://t.me/	org/telegram/ui/ChatActivity.java
https://)?t.me/([0-9a-zA-Z_]+)/([0-9]+)/?([0-9]+)?	org/telegram/ui/ChatActivity.java
https://)?t.me/([0-9a-zA-Z_]+)\\?(voicechat+)	org/telegram/ui/ChatActivity.java
https://)?t.me/c/([0-9]+)/([0-9]+)/?([0-9]+)?	org/telegram/ui/ChatActivity.java
https://t.me/	org/telegram/ui/ManageLinksActivity.java
https://t.me/+	org/telegram/ui/ManageLinksActivity.java

https://t.me/joinchat/	org/telegram/ui/ManageLinksActivity.java
https://t.me/	org/telegram/ui/Components/URLSpanNoUnderline.java
https://messenger.telegram.org/	org/telegram/ui/Components/EmbedBottomSheet.java
https://www.youtube.com/iframe_api\	org/telegram/ui/Components/EmbedBottomSheet.java
https://youtube.com	org/telegram/ui/Components/EmbedBottomSheet.java
https://t.me/	org/telegram/ui/Components/BotWebViewContainer.java
https://www.youtube.com/youtupei/v1/player?key=	org/telegram/ui/Components/PhotoViewerWebView.java
https://www.youtube.com/watch?v=	org/telegram/ui/Components/PhotoViewerWebView.java
https://messenger.telegram.org/	org/telegram/ui/Components/PhotoViewerWebView.java
https://youtube.com	org/telegram/ui/Components/PhotoViewerWebView.java
https://www.youtube.com	org/telegram/ui/Components/WebPlayerView.java
https://www.youtube.com/embed/	org/telegram/ui/Components/WebPlayerView.java
https://youtube.googleapis.com/v/	org/telegram/ui/Components/WebPlayerView.java
https://www.youtube.com/get_video_info?	org/telegram/ui/Components/WebPlayerView.java
https://player.vimeo.com/video/%s/config	org/telegram/ui/Components/WebPlayerView.java
http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s	org/telegram/ui/Components/WebPlayerView.java
https://api.twitch.tv/kraken/streams/%s?stream_type=all	org/telegram/ui/Components/WebPlayerView.java
https://api.twitch.tv/api/channels/%s/access_token	org/telegram/ui/Components/WebPlayerView.java
https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	org/telegram/ui/Components/WebPlayerView.java

https://coub.com/api/v2/coubs/%s.json	org/telegram/ui/Components/WebPlayerView.java
https://t.me/	org/telegram/ui/Components/TranslateAlert2.java
https://play.google.com/store/apps/details?id=org.telegram.messenger	org/telegram/ui/Components/Premium/PremiumNotAvailableBottomSheet.java
https://telegram.org	org/telegram/ui/Cells/ThemePreviewMessagesCell.java
https://attheme.org?slug=	org/telegram/ui/ActionBar/Theme.java
https://www.google.com/resolve?name=	org/telegram/tgnet/ConnectionsManager.java
http://www.slf4j.org/codes.html	org.slf4j/LoggerFactory.java
http://console.cloud.tencent.com:9999	cos/MyCOSService.java
http://101.42.6.119:15000/api/uploadlog	cos/MyCOSService.java

 邮箱线索

邮箱地址	所在文件
support@stripe.com	com/stripe/android/net/StripeApiHandler.java
sms@telegram.org	org/telegram/ui/PassportActivity.java
sms@telegram.org	org/telegram/ui/LoginActivity.java

 手机线索

--	--

手机号	所在文件
15555215554	org/telegram/messenger/EmuDetector.java
15555215556	org/telegram/messenger/EmuDetector.java
15555215558	org/telegram/messenger/EmuDetector.java
15555215560	org/telegram/messenger/EmuDetector.java
15555215562	org/telegram/messenger/EmuDetector.java
15555215564	org/telegram/messenger/EmuDetector.java
15555215566	org/telegram/messenger/EmuDetector.java
15555215568	org/telegram/messenger/EmuDetector.java
15555215570	org/telegram/messenger/EmuDetector.java
15555215572	org/telegram/messenger/EmuDetector.java
15555215574	org/telegram/messenger/EmuDetector.java
15555215576	org/telegram/messenger/EmuDetector.java
15555215578	org/telegram/messenger/EmuDetector.java
15555215580	org/telegram/messenger/EmuDetector.java
15555215582	org/telegram/messenger/EmuDetector.java
15555215584	org/telegram/messenger/EmuDetector.java
14058229493	org/telegram/messenger/Utilities.java
16822222222	org/telegram/ui/Cells/ChatMessageCell.java

1822222222	org/telegram/ui/Cells/ChatMessageCell.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=hpl, ST=yTa, L=MTw, O=3LV, OU=s3B, CN=1kE
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-18 07:43:55+00:00
有效期至: 2052-11-03 07:43:55+00:00
发行人: C=hpl, ST=yTa, L=MTw, O=3LV, OU=s3B, CN=1kE
序列号: 0x2f2afb0358f8a7a0
哈希算法: sha256
md5值: 62e1a24c20536d46c8b41bca544ed44d
sha1值: 347f693b09c6f298cd572a958358359088f292ef
sha256值: 8ce79eb54f33c3b24a60d48ee4c60039bbbed88d55e3f92e0400a553b5712292c
sha512值: 0f11799cd8f47aef8aaf539d40985a1f34e93ae5ac51f2ea937629e8be829928592a3a728c78508483196301e9d98ecfab4a8ca62c73b92e49f751253ed094aa
公钥算法: rsa
密钥长度: 2048
指纹: 8491a0eae6c57b7b7e7ef3a9e7f9cc67f6555ae331246988433bedb282d32d30

🔑 硬编码敏感信息

🌀 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

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。