



MoGua

Exness 3.57.6-china-release.APK 分析报告



APP名称:

Exness

包名:

com.exness.android.pa

域名线索:	89条
URL线索:	97条
邮箱线索:	6条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: exness-app.apk

文件大小: 86.9MB

MD5值: 6ea3b43f42da1e884af3699c1f2b5aac

SHA1值: 1c60c9b3f2a059adf0b3657df53287cb3b8426cc

SHA256值: 72cf5716447a77f0cf711ac31e354c3a93801df321269323beeb0e6ab7a0fd80

APP 信息

App名称: Exness
包名: com.exness.android.pa
主活动Activity: com.exness.features.entry.impl.presentation.EntryActivity
安卓版本名称: 3.57.6-china-release
安卓版本: 2001135

🔍 域名线索

域名	服务器信息
api.pushy.me	IP: 52.205.199.157 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
spia.s	没有服务器地理信息.
bit.ly	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
api.lab.amplitude.com	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
www.docs.developers.amplitude.com	IP: 66.33.60.130 所属国家: Canada 地区: Ontario 城市: Etobicoke 纬度: 43.623768 经度: -79.559723
	IP: 127.0.0.1 所属国家: -

exness.com	地区: - 城市: - 纬度: 0.000000 经度: 0.000000
sentry2.exness.io	IP: 107.154.196.67 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
stage.app.igodigital.com	IP: 34.237.254.57 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
sconversions.s	没有服务器地理信息.
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
api.eu.amplitude.com	IP: 18.158.38.155 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
firebase-settings.crashlytics.com	IP: 114.250.65.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
svalidate.s	没有服务器地理信息.
	IP: 93.46.8.90

accounts.google.com	所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
static.exmobi.mobi	IP: 13.35.37.76 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei 纬度: 25.038172 经度: 121.563599
firebase.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
console.firebase.google.com	IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
smonitorsdk.s	没有服务器地理信息.
jsonip.com	IP: 34.160.111.145 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
simpression.s	没有服务器地理信息.
metatraderweb.app	IP: 78.140.180.90 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980

scdn-ssettings.s	没有服务器地理信息.
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
api2.lab.amplitude.com	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
ssdk-services.s	没有服务器地理信息.
social-trading.exness.com	IP: 31.13.112.9 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
schemas.android.com	没有服务器地理信息.
sonelink.s	没有服务器地理信息.
slaunches.s	没有服务器地理信息.
goo.gl	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
api.ipify.org	IP: 104.26.13.205 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
my.exness.com	IP: 199.59.148.202 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
goo.gle	IP: 67.199.248.12 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
my.ex-markets.pro	IP: 188.164.248.11 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
static.exmobi.asia	IP: 188.164.248.11 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
api.domain	没有服务器地理信息.
scdn-stestsettings.s	没有服务器地理信息.
my.exnessaffiliates.com	IP: 107.154.196.37 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
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
www.google.com	IP: 199.16.158.12 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
firebaseinstallations.googleapis.com	IP: 142.250.217.74 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
pp.exxesspp.com	IP: 107.154.196.37 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
api.myip.com	IP: 157.240.17.36 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
app.igodigital.com	IP: 35.168.70.169 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
api-bdc.net	IP: 76.223.87.32 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842

svalidate-and-log.s	没有服务器地理信息.
my.exaffiliate.com	IP: 188.164.248.66 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
ap.api.fpjs.io	IP: 3.33.219.3 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
developer.android.com	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
mct9813hhqdnlxcbr0tkgn9rhhm.device.marketingcloudapis.com	IP: 13.111.18.59 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.788464 经度: -122.394608
developer.apple.com	IP: 17.253.85.205 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aomedia.org	IP: 199.59.148.20 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
app-measurement.com	IP: 114.250.64.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.fpjs.io	IP: 76.223.60.10 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
md.domain	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
download.mqI5.com	IP: 27.111.161.152 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.seeip.org	IP: 23.128.64.156 所属国家: United States of America 地区: Oregon 城市: Clackamas 纬度: 45.415646 经度: -122.524277
sattr.s	没有服务器地理信息.
sregister.s	没有服务器地理信息.
	IP: 59.24.3.174

google.com	所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
sinapps.s	没有服务器地理信息.
issuetracker.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
eu.api.fpjs.io	IP: 99.83.255.25 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
sdlSDK.s	没有服务器地理信息.
www.googleadservices.com	IP: 114.250.63.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
appassets.androidplatform.net	没有服务器地理信息.
md.eccalls.mobi	IP: 188.164.248.34 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
input.frontrics.site	IP: 52.77.161.232 所属国家: Singapore 地区: Singapore 城市: Singapore

	纬度: 1.289987 经度: 103.850281
sapp.s	没有服务器地理信息.
salesforce-marketingcloud.github.io	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
javax.xml.xmlconstants	没有服务器地理信息.
www.exness.com	IP: 103.252.114.61 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.exnessaffiliates.com	IP: 107.154.196.37 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
sgcdsdk.s	没有服务器地理信息.
10.0.2.2	IP: 10.0.2.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
api2.amplitude.com	IP: 52.40.67.33 所属国家: United States of America 地区: Oregon 城市: Boardman 纬度: 45.839859 经度: -119.700577

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
pp.eksnecc.com	IP: 188.164.248.42 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
pay.ibex.exchange	IP: 107.154.196.37 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.532440 经度: -122.248833
sadrevenue.s	没有服务器地理信息.
privacy-sandbox.appsflyersdk.com	IP: 13.35.49.83 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
get.exness.help	IP: 104.18.248.37 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
download.feedder.com	IP: 188.164.248.72 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980

premier.exness.com	IP: 108.160.165.212 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
sviap.s	没有服务器地理信息.
sars.s	没有服务器地理信息.
g.co	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

URL线索

URL信息	Url所在文件
https://firebase.google.com/support/guides/disable-analytics	C3/RunnableC0301e.java
https://api.domain_placeholder/api/	Am/C0176x.java
https://github.com/google/gson/blob/main/Troubleshooting.md	DL/O.java
https://github.com/google/gson/blob/main/Troubleshooting.md	DL/A.java
https://issuetracker.google.com/issues/297974033	I/V.java
https://issuetracker.google.com/issues/300280216	I/V.java
http://schemas.android.com/apk/res/android	B1/b.java
http://10.0.2.2:8969/stream	A3/h.java
https://github.com/google/gson/blob/main/Troubleshooting.md	IL/a.java

https://www.google.com	D4/c.java
https://www.docs.developers.amplitude.com/data/sdks/android-kotlin/	B2/f.java
https://api.lab.amplitude.com/	O4/g.java
https://api.fpjs.io	YH/f.java
https://eu.api.fpjs.io	YH/f.java
https://ap.api.fpjs.io	YH/f.java
https://goo.gle/compose-feedback	Z/AbstractC1973q.java
http://ns.adobe.com/xap/1.0/	V2/a.java
https://privacy-sandbox.appsflyersdk.com/api/trigger	com/appsflyer/internal/AFj1kSDK.java
http://salesforce-marketingcloud.github.io/MarketingCloudSDK-Android	com/salesforce/marketingcloud/MarketingCloudConfig.java
https://app.igodigital.com/api/v1/collect/process_batch	com/salesforce/marketingcloud/MarketingCloudConfig.java
https://stage.app.igodigital.com/api/v1/collect/qa/qa1s1/process_batch	com/salesforce/marketingcloud/analytics/piwama/i.java
https://stage.app.igodigital.com/api/v1/collect/qa/qa3s1/process_batch	com/salesforce/marketingcloud/analytics/piwama/i.java
https://app.igodigital.com/api/v1/collect/process_batch	com/salesforce/marketingcloud/analytics/piwama/i.java
https://appassets.androidplatform.net/assets/tradingplatform/index.html	com/exness/features/terminal/impl/presentation/chart/web/views/WebChartFragment.java
https://metatraderweb.app/trade/?m=1&version=5&servers=	com/exness/features/terminal/impl/presentation/mt5web/MT5WebTerminalFragment.java
https://play.google.com	com/exness/features/socialtrading/impl/presentation/views/d.java
https://get.exness.help/hc/en-us/articles/360011550959-The-Impact-of-Leverage-on-Stop-Out	com/exness/features/stopout/presentation/summary/help/views/widgets/StopOutSummaryHelpView.java
https://get.exness.help/hc/en-us/articles/360011050319?tab=tab3	com/exness/features/stopout/presentation/summary/help/views/widgets/StopOutSummaryHelpView.java

https://get.exness.help/hc/en-us/articles/6173903134620-Exness-Market-Protection-Tools	com/exness/features/stopout/presentation/summary/help/views/widgets/StopOutSummaryHelpView.java
https://get.exness.help/hc/en-us/articles/4402645127186-What-can-cause-my-orders-to-close-automatically	com/exness/features/stopout/presentation/summary/help/views/widgets/StopOutSummaryHelpView.java
https://firebase.google.com/support/privacy/init-options	cL/C2664d.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	cM/C2675d.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	cM/f.java
http://ns.adobe.com/xap/1.0/\u0000	e2/C3149g.java
https://api	dc/i.java
https://00356e20a84a42a1ac4658f4328a6221@sentry2.exness.io/43	io/sentry/b2.java
https://github.com/google/gson/blob/main/Troubleshooting.md	io/sentry/internal/debugmeta/c.java
https://app-measurement.com/a	IJ/AbstractC4896y.java
https://goo.gl/NAOOOI	IJ/Z0.java
https://goo.gl/NAOOOI	IJ/Z0.java
https://google.com/search?	IJ/RunnableC4880p0.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=	IJ/RunnableC4872l0.java
https://api.pushy.me	me/pushy/sdk/config/PushyAPIConfig.java
http://javax.xml.XMLConstants/feature/secure-processing	me/pushy/sdk/lib/jackson/databind/ext/DOMDeserializer.java
https://bit.ly/3GfZoys	me/pushy/sdk/util/PushyPermissionVerification.java
https://bit.ly/2O3fHEX	me/pushy/sdk/services/PushyJobService.java
https://issuetracker.google.com/issues/new?component=413106	x3/J0.java

http://xml.org/sax/features/external-general-entities	y5/H0.java
http://xml.org/sax/features/external-parameter-entities	y5/H0.java
http://xml.org/sax/properties/lexical-handler	y5/H0.java
http://xmlpull.org/v1/doc/features.html	y5/H0.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	x2/z.java
https://accounts.google.com/o/oauth2/revoke?token=	ll/c.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	v2/t.java
http://g.co/dev/packagevisibility .	v2/y.java
https://get.exness.help/hc/en-us/articles/360009664679-Price-Gap-Protection	NG/a.java
https://get.exness.help/hc/en-us/articles/360011050319?tab=tab3	NG/a.java
https://get.exness.help/hc/en-us/articles/360011676519-Stop-Levels	NG/a.java
https://api.domain_placeholder/api/	Gj/C0665b.java
https://github.com/google/gson/blob/main/Troubleshooting.md	HL/a.java
https://api.domain_placeholder/api/	gp/C3760i.java
https://download.mql5.com/cdn/web/metaquotes.software.corp/mt4/metatrader4.apk	mx/C5188e.java
https://download.mql5.com/cdn/web/metaquotes.software.corp/mt5/metatrader5.apk	mx/C5188e.java
https://api.domain_placeholder/api/	td/C6299b.java
https://static.exmobi.mobi/pins.json	lc/C4925f.java
https://static.exmobi.asia/pins.json	lc/C4925f.java

https://api.domain_placeholder/api/	L5/b.java
https://api.domain_placeholder/api/	ub/C6445b.java
https://api.domain_placeholder/api/	wr/b.java
https://api.domain_placeholder/api/	AE/d.java
https://api.domain_placeholder/tex-logs/	AE/d.java
https://api.domain_placeholder/api/	Uc/C1638d.java
https://firebaseinstallations.googleapis.com/v1/	eL/c.java
https://console.firebase.google.com/project/	gq/m.java
https://api.domain_placeholder/tex-api/	KF/b.java
https://get.exness.help/hc/en-us/articles/360011050319?tab=tab3	AA/a.java
https://get.exness.help/hc/en-us/articles/360011550959-The-Impact-of-Leverage-on-Stop-Out	AA/a.java
https://get.exness.help/hc/en-us/articles/6173903134620-Exness-Market-Protection-Tools	AA/a.java
https://get.exness.help/hc/en-us/articles/4402645127186-What-can-cause-my-orders-to-close-automatically	AA/a.java
https://www.exness.com	sd/C6036d.java
https://get.exness.help/hc/en-us/articles/4402341895570	sd/C6036d.java
https://get.exness.help/hc/en-us/articles/4405523320594	sd/C6036d.java
https://get.exness.help/hc/	sd/C6036d.java
https://premier.exness.com/	sd/C6036d.java
https://md.eccalls.mobi/accounts/reset-password-card	sd/C6036d.java

https://md.eccalls.mobi/kyc/	sd/C6036d.java
https://md.eccalls.mobi/mfp/kyc-status-widget/frame/	sd/C6036d.java
https://md.eccalls.mobi/myaccount/	sd/C6036d.java
https://pp.exnesspp.com	sd/C6036d.java
https://pp.eksnecc.com	sd/C6036d.java
https://www.exnessaffiliates.com/?source=exness	sd/C6036d.java
https://my.exnessaffiliates.com/?lang=	sd/C6036d.java
https://my.exaffiliate.com/?lang=	sd/C6036d.java
https://metatraderweb.app/trade/?m=1	sd/C6036d.java
https://social-trading.exness.com	sd/C6036d.java
https://my.exness.com	sd/C6036d.java
https://my.ex-markets.pro	sd/C6036d.java
https://md.eccalls.mobi/mfp/host/	sd/C6036d.java
https://mct9813hhqdnlxcbr0tkgn9rhhm.device.marketingcloudapis.com/	sd/C6036d.java
https://api.eu.amplitude.com/2/httpapi	zb/c.java
https://api2.amplitude.com/2/httpapi	zb/c.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/	mB/g.java
https://api.domain_placeholder/api/	AD/d.java
https://api.domain_placeholder/tex-api/	AD/d.java
https://md.domain_placeholder/mfp/host/	Mb/d.java

https://md.	Mb/d.java
https://api.domain_placeholder/api/	Wa/C1783b.java
https://api.domain_placeholder/mobile-ws2/	Wa/C1783b.java
https://api.domain_placeholder/	Wa/C1783b.java
https://api.domain_placeholder/tex-api/	Wa/C1783b.java
https://api.domain_placeholder/tex-logs/	Wa/C1783b.java
https://md.domain_placeholder/kyc/	vd/C6653a.java
https://md.domain_placeholder/mfp/kyc-status-widget/frame/	vd/C6653a.java
https://pay.ibex.exchange/	vd/C6653a.java
https://md.domain_placeholder/mfp/host/	vd/C6653a.java
https://api.ipify.org	nc/C5293c.java
https://api.myip.com	nc/C5293c.java
https://api.seeip.org	nc/C5293c.java
https://api-bdc.net/data/client-ip	nc/C5293c.java
https://jsonip.com/	nc/C5293c.java
https://api.domain_placeholder/api/	v7/C6541b1.java
https://play.google.com/store/apps/details?id=	ua/C6443d.java
https://api.domain_placeholder/	Bb/e.java
https://download.feedder.com/apk/exness-app.apk	UD/f.java
https://download.feedder.com/apk/exness.apk	UD/f.java

https://md.eccalls.mobi/static/calendar/android/	wc/AbstractC6886a.java
https://github.com/google/gson/blob/main/Troubleshooting.md	FL/c.java
https://api2.lab.amplitude.com	Ya/c.java
https://api2.lab.amplitude.com	Ya/C1914a.java
https://exness.com	EE/c.java
https://download.feedder.com/apk/version.txt	QD/a.java
https://api.domain_placeholder/llc/sse/connection/uni_sse	fs/b.java
https://md.eccalls.mobi/static/currency/android/	z7/C7426a.java
https://md.eccalls.mobi/static/calendar/android/	kB/AbstractC4549a.java
https://api.domain_placeholder/tex-api/	wE/C6754b.java
https://aomedia.org/emsg/ID3	Y2/a.java
https://developer.apple.com/streaming/emsg-id3	Y2/a.java
https://get.exness.help/hc/en-us/articles/360011550959-The-Impact-of-Leverage-on-Stop-Out	Bu/a.java
https://get.exness.help/hc/en-us/articles/360011050319?tab=tab3	Bu/a.java
https://get.exness.help/hc/en-us/articles/6173903134620-Exness-Market-Protection-Tools	Bu/a.java
https://get.exness.help/hc/en-us/articles/4402645127186-What-can-cause-my-orders-to-close-automatically	Bu/a.java
https://api.domain_placeholder/mobile-ws2/	ja/d.java
https://api.domain_placeholder/	B7/d.java
https://api.domain_placeholder/api/	B7/a.java

https://api.domain_placeholder/tex-api/	B7/c.java
https://api.domain_placeholder/api/	B7/b.java
https://input.frontrics.site/	hb/C3853a.java
https://download.feedder.com/apk/exness-app.apk	Mf/C1187b.java
https://download.feedder.com/apk/exness.apk	Mf/C1187b.java
https://api.domain_placeholder/	jm/C4440a.java
https://00356e20a84a42a1ac4658f4328a6221@sentry2.exness.io/43	id/C4017a.java
https://api2.lab.amplitude.com	al/C2347a.java

 邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	Kl/m.java
support@exness.com	com/exness/main/impl/presentation/main/view/AccountDeletionDialog.java
42a1ac4658f4328a6221@sentry2.exness	io/sentry/b2.java
support@exness.com	Ao/a.java
support@exness.com	Bu/a.java
42a1ac4658f4328a6221@sentry2.exness	id/C4017a.java

 手机线索

手机号	所在文件
16222222222	C/C0290x.java
15552000000	lj/C4889u0.java
17179869184	y5/H0.java
17179869184	y5/x0.java

🌸 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=CY, L=Limassol, O=Exness, OU=MD, CN=Dmitrii Shustov
签名算法: rsassa_pkcs1v15
有效期自: 2017-04-13 08:58:24+00:00
有效期至: 2042-04-07 08:58:24+00:00
发行人: C=CY, L=Limassol, O=Exness, OU=MD, CN=Dmitrii Shustov
序列号: 0x7e6f5553
哈希算法: sha256
md5值: b4c7f902afefb79f8537b9657318ba20
sha1值: f6beb3846e8707851f7a9aae1e21e0fb0e2f232a
sha256值: e6d13cb570b9e15437090db3d181e8f86a9b581b74f76e2e21b271e2653583ef
sha512值: 73f8a325f2887243aeea57c3647832d0fb25975caf91fdef286637092533c56e0795546e2725cc16ab8b37d82cbfdca799b0a9268d17944c4113f0fbbf5866af
公钥算法: rsa
密钥长度: 2048
指纹: cda72ef92a4115e24ba64ce9a09414e0af9eaeb4e01252f193a1f1f61758b888

🔑 硬编码敏感信息

🌀 加壳分析

加壳类型	所属文件
------	------

登录摸瓜网站后查看	
-----------	--

第三方插件

名称	分类	URL链接
登录摸瓜网站后查看		

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
	正常	防止手机休眠	允许应用程序防止手机进入睡眠状态

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.POST_NOTIFICATIONS	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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
com.android.vending.CHECK_LICENSE	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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	未知	Unknown permission	Unknown permission from android reference
com.samsung.android.mapsagent.permission.READ_APP_INFO	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	Unknown permission	Unknown permission from android reference

com.exness.permission.MESSAGING.com.exness.android.pa	未知	Unknown permission	Unknown permission from android reference
com.exness.android.pa.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.exness.features.entry.impl.presentation.EntryActivity	Schemes: https://, exness://, Hosts: exness.onelink.me, exness.sng.link, pa,
com.exness.features.entry.impl.presentation.PremierEntryActivity	Schemes: https://, exness://, Hosts: exness.onelink.me, pa,