MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

LOVE NEWS

Love News 9.8.0.APK

APP名称:	Love News
包名:	lovenews.azca
域名线索:	41条
URL线索:	87条
邮箱线索:	0条
分析日期:	2022年1月28日 23:05

文件信息

文件名: lovenews527839.apk
文件大小: 8.59MB

MD5值: dd63098652df30e331066eb381da3730
SHA1值: 0d58c50eec9cdbdb5863037b73a8dc4e4f7ca0e5
SHA256值: c5d7e9f2aea14dc5eda9807fa417e8aae3419e93cee28214fafa5aeaf8a672ce

APP 信息

App名称: Love News
包名: lovenews.azca
主活动**Activity:** lovenews.azca.preinicio
安卓版本名称: 9.8.0
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
daneden.me	good	**IP:** 76.76.21.98 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223 查看地图: Google Map
www.paypal.com	good	**IP:** 151.101.129.21 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map

域名	是否危险域名	服务器信息
imp.startappservice.com	good	**IP:** 188.42.120.84 **所属国家:** Luxembourg **地区:** Luxembourg **城市:** Luxembourg **纬度:** 49.611671 **经度:** 6.130000 **查看地图:** Google Map
api.appnxt.net	good	**IP:** 13.232.70.145 **所属国家:** India **地区:** Maharashtra **城市:** Mumbai **纬度:** 19.014410 **经度:** 72.847939 **查看地图:** Google Map
graph.facebook.com	good	**IP:** 104.244.46.244 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.773968 **经度:** -122.410446 **查看地图:** Google Map
video.e-droid.net	good	**IP:** 84.17.44.181 **所属国家:** United States of America **地区:** California **城市:** Los Angeles **纬度:** 34.052231 **经度:** -118.243683 **查看地图:** Google Map

域名	是否危险域名	服务器信息
admin.appnext.com	good	**IP:** 52.5.42.24 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map
d1byvlfiet2h9q.cloudfront.net	good	**IP:** 99.84.142.138 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
global.appnext.com	good	**IP:** 13.213.173.146 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
d2to8y50b3n6dq.cloudfront.net	good	**IP:** 13.32.50.108 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map

域名	是否危险域名	服务器信息
info.startappservice.com	good	**IP:** 152.195.62.69 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.034081 **经度:** -77.488503 **查看地图:** Google Map
support.startapp.com	good	**IP:** 217.65.36.172 **所属国家:** United States of America **地区:** New Jersey **城市:** Clifton **纬度:** 40.858429 **经度:** -74.163757 **查看地图:** Google Map
www.com.startapp.com	good	没有服务器地理信息.
geoip.api.p3insight.de	good	**IP:** 54.77.149.100 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.343990 **经度:** -6.267190 **查看地图:** Google Map
imgs1.e-droid.net	good	**IP:** 212.102.46.9 **所属国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.606209 **经度:** -122.332069 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.fqtag.com	good	**IP:** 35.190.72.161 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看地图:** Google Map
api-project-751842291101.firebaseio.com	good	**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 **查看地图:** Google Map
www.example.com	good	**IP:** 93.184.216.34 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map
www.appnext.com	good	**IP:** 18.234.79.235 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.google.com	good	**IP:** 173.231.12.107 **所属国家:** United States of America **地区:** Utah **城市:** Ogden **纬度:** 41.276379 **经度:** -111.987442 **查看地图:** Google Map
geoip.api.c0nnectthed0ts.com	good	**IP:** 54.77.149.100 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.343990 **经度:** -6.267190 **查看地图:** Google Map
wd.adcolony.com	good	**IP:** 54.243.105.143 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map
adc3-launch-staging.adcolony.com	good	**IP:** 34.193.213.110 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map

域名	是否危险域名	服务器信息
opensource.org	good	**IP:** 159.65.34.8 **所属国家:** United States of America **地区:** New Jersey **城市:** Clifton **纬度:** 40.858429 **经度:** -74.163757 **查看地图:** Google Map
apk.e-droid.net	good	**IP:** 195.181.175.46 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
play.google.com	good	**IP:** 172.217.160.110 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
wallkit.instal.com	good	**IP:** 130.211.39.79 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看地图:** Google Map

域名	是否危险域名	服务器信息
awsdus.api.p3insight.de	good	**IP:** 52.17.41.235 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.343990 **经度:** -6.267190 **查看地图:** Google Map
video-upload.e-droid.net	good	**IP:** 141.95.3.196 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
cdn.appnext.com	good	**IP:** 13.225.159.114 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
apis.appnxt.net	good	**IP:** 3.6.212.185 **所属国家:** India **地区:** Maharashtra **城市:** Mumbai **纬度:** 19.014410 **经度:** 72.847939 **查看地图:** Google Map

域名	是否危险域名	服务器信息
adc3-launch.adcolony.com	good	**IP:** 18.211.99.64 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map
docs.google.com	good	**IP:** 128.242.240.20 **所属国家:** United States of America **地区:** California **城市:** Milpitas **纬度:** 37.428268 **经度:** -121.906616 **查看地图:** Google Map
adsmetadata.startappservice.com	good	**IP:** 188.42.123.140 **所属国家:** Luxembourg **地区:** Luxembourg **城市:** Luxembourg **纬度:** 49.611671 **经度:** 6.130000 **查看地图:** Google Map
www.appcreator24.com	good	**IP:** 82.165.61.18 **所属国家:** Germany **地区:** Nordrhein-Westfalen **城市:** Strang **纬度:** 51.968700 **经度:** 8.753360 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.youtube.com	good	**IP:** 172.217.163.46 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
join-app.net	good	**IP:** 82.165.61.18 **所属国家:** Germany **地区:** Nordrhein-Westfalen **城市:** Strang **纬度:** 51.968700 **经度:** 8.753360 **查看地图:** Google Map
infoevent.startappservice.com	good	**IP:** 188.42.123.140 **所属国家:** Luxembourg **地区:** Luxembourg **城市:** Luxembourg **纬度:** 49.611671 **经度:** 6.130000 **查看地图:** Google Map
req.startappservice.com	good	**IP:** 188.42.120.108 **所属国家:** Luxembourg **地区:** Luxembourg **城市:** Luxembourg **纬度:** 49.611671 **经度:** 6.130000 **查看地图:** Google Map

域名	是否危险域名	服务器信息
ul.api.c0nnectthed0ts.com	good	**IP:** 52.30.102.165 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.343990 **经度:** -6.267190 **查看地图:** Google Map
lh6.ggpht.com	good	**IP:** 172.217.160.97 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://adc3-launch.adcolony.com/v4/launch	com/adcolony/sdk/ai.java
https://wd.adcolony.com/logs	com/adcolony/sdk/ax.java
https://adc3-launch-staging.adcolony.com/v4/launch	com/adcolony/sdk/f.java
http://global.appnext.com	com/appnext/a.java
http://cdn.appnext.com/tools	com/appnext/a.java

URL信息	Url所在文件
http://cdn.appnext.com/tools/sdk/interstitial/v75	com/appnext/a.java
http://global.appnext.com	com/appnext/banners/b.java
http://global.appnext.com	com/appnext/banners/f.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3	com/appnext/banners/f.java
https://admin.appnext.com/AdminService.asmx/checkA?z=	com/appnext/banners/BannerAd.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3/result.min.js	com/appnext/banners/BannerActivity.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/banners/BannerActivity.java
https://admin.appnext.com/tp12.aspx	com/appnext/banners/BannerActivity.java
https://cdn.appnext.com/tools/sdk/config/2.4.0/result_banner/	com/appnext/banners/BannerActivity.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3/banner.min.js	com/appnext/banners/g.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3/result.min.js	com/appnext/banners/g.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/banners/g.java
https://global.appnext.com/offerwallapi.aspx	com/appnext/banners/g.java
https://admin.appnext.com/tp12.aspx	com/appnext/banners/g.java
https://admin.appnext.com/gpi.aspx	com/appnext/banners/g.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/banners/c.java

URL信息	Url所在文件
https://global.appnext.com/offerwallapi.aspx	com/appnext/banners/c.java
https://admin.appnext.com/tp12.aspx	com/appnext/banners/c.java
https://admin.appnext.com/gpi.aspx	com/appnext/banners/c.java
http://cdn.appnext.com/tools/sdk/confign/banner/banner_config.txt	com/appnext/banners/d.java
http://cdn.appnext.com/tools/services/4.7.2/config.json	com/appnext/base/b/d.java
http://cdn.appnext.com/tools/services/4.7.2/plist.json	com/appnext/base/b/d.java
http://cdn.appnext.com/tools/services/4.7.2/config.json?packageId=	com/appnext/base/operations/imp/cdm.java
http://cdn.appnext.com/tools/sdk/confign/nativeads_new/native_ads_config.json	com/appnext/nativeads/b.java
https://admin.appnext.com/AdminService.asmx/checkA?z=	com/appnext/nativeads/NativeAdObject.java
http://global.appnext.com	com/appnext/nativeads/c.java
https://www.fqtag.com/pixel.cgi?org=TkBXEI5C3FBIr4zXwnmK&p=	com/appnext/nativeads/NativeAd.java
http://global.appnext.com	com/appnext/nativeads/a.java
http://global.appnext.com	com/appnext/ads/fullscreen/b.java
http://cdn.appnext.com/tools/sdk/confign/rewarded/rewarded_config.txt	com/appnext/ads/fullscreen/f.java
https://www.fqtag.com/pixel.cgi?org=TkBXEI5C3FBIr4zXwnmK&p=	com/appnext/ads/fullscreen/FullscreenActivity.java
https://admin.appnext.com/adminService.asmx/SetRewards	com/appnext/ads/fullscreen/FullscreenActivity.java

URL信息	Url所在文件
https://admin.appnext.com/AdminService.asmx/checkA?z=	com/appnext/ads/fullscreen/Video.java
http://cdn.appnext.com/tools/sdk/confign/fullscreen/fullscreen_config.txt	com/appnext/ads/fullscreen/c.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/ads/interstitial/b.java
https://admin.appnext.com/tp12.aspx	com/appnext/ads/interstitial/b.java
https://cdn.appnext.com/tools/sdk/config/2.4.0/result_banner/	com/appnext/ads/interstitial/b.java
http://cdn.appnext.com/tools/sdk/interstitial/v75/result.min.js	com/appnext/ads/interstitial/InterstitialActivity.java
https://www.fqtag.com/pixel.cgi?org=TkBXEI5C3FBIr4zXwnmK&p=	com/appnext/ads/interstitial/InterstitialActivity.java
http://cdn.appnext.com/tools/sdk/interstitial/v75/script.min.js	com/appnext/ads/interstitial/Interstitial.java
https://admin.appnext.com/AdminService.asmx/checkA?z=	com/appnext/ads/interstitial/Interstitial.java
http://www.appnext.com/myid.html	com/appnext/ads/interstitial/Interstitial.java
http://cdn.appnext.com/tools/sdk/confign/interstitial/interstitial_config.txt	com/appnext/ads/interstitial/c.java
http://global.appnext.com	com/appnext/ads/interstitial/a.java
https://admin.appnext.com/AdminService.asmx/SetOpenV1	com/appnext/core/AdsService.java
https://cdn.appnext.com/tools/sdk/adchoices/adchoices_big.png	com/appnext/core/k.java
https://admin.appnext.com/tp12.aspx?tid=%s&vid=%s&osid=%s&auid=%s&session_id=%s&pid=%s&ref=%s&ads_type=%s&bid=%s&cid=%s	com/appnext/core/f.java
https://global.appnext.com/stp.aspx	com/appnext/core/f.java

URL信息	Url所在文件
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/core/f.java
http://www.appnext.com/myid.html	com/appnext/core/f.java
https://admin.appnext.com/tools/navtac.html?bid=	com/appnext/core/e.java
https://play.google.com/store/apps/	com/appnext/core/e.java
https://admin.appnext.com/AdminService.asmx/	com/appnext/core/e.java
https://admin.appnext.com/AdminService.asmx/SetRL?guid=	com/appnext/core/q.java
http://www.appnext.com/myid.html	com/appnext/core/q.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3	com/appnext/core/i.java
http://cdn.appnext.com/tools/sdk/langs/2.4.4	com/appnext/core/i.java
http://cdn.appnext.com/tools/sdk/confign	com/appnext/core/i.java
http://apis.appnxt.net:443	com/appnext/core/i.java
https://api.appnxt.net	com/appnext/core/i.java
http://cdn.appnext.com/tools/services/4.7.2	com/appnext/core/i.java
http://cdn.appnext.com/tools/sdk/confign	com/appnext/core/p.java
https://admin.appnext.com/AdminService.asmx/bns	com/appnext/core/d.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/core/result/b.java

URL信息	Url所在文件
https://admin.appnext.com/tp12.aspx	com/appnext/core/result/b.java
https://cdn.appnext.com/tools/sdk/config/2.4.0/result_banner/	com/appnext/core/result/b.java
http://cdn.appnext.com/tools/sdk/banner/2.4.3/result.min.js	com/appnext/core/result/ResultPageActivity.java
https://www.appnext.com/privacy_policy/index.html?z=	com/appnext/core/result/ResultPageActivity.java
https://admin.appnext.com/tp12.aspx	com/appnext/core/result/ResultPageActivity.java
https://cdn.appnext.com/tools/sdk/config/2.4.0/result_banner/	com/appnext/core/result/ResultPageActivity.java
http://cdn.appnext.com/tools/sdk/langs/2.4.4/langs.json	com/appnext/core/a/b.java
https://support.startapp.com/hc/en-us/articles/360002411114	com/startapp/sdk/adsbase/k.java
http://www.example.com	com/startapp/sdk/adsbase/k.java
https://imp.startappservice.com/tracking/adImpression	com/startapp/sdk/adsbase/AdsConstants.java
http://play.google.com	com/startapp/sdk/adsbase/a.java
https://play.google.com	com/startapp/sdk/adsbase/a.java
https://infoevent.startappservice.com/tracking/infoEvent	com/startapp/sdk/adsbase/infoevents/AnalyticsConfig.java
https://d1byvlfiet2h9q.cloudfront.net/InApp/resources/adInformationDialog3.html	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java
https://www.com.startapp.com/policy/sdk-policy/	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java
https://info.startappservice.com/InApp/resources/info_l.png	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java

URL信息	Url所在文件
https://adsmetadata.startappservice.com/1.5/	com/startapp/sdk/adsbase/remoteconfig/MetaData.java
https://req.startappservice.com/1.5/	com/startapp/sdk/adsbase/remoteconfig/MetaData.java
https://daneden.me/animate	com/startapp/sdk/ads/splash/SplashHtml.java
https://opensource.org/licenses/MIT	com/startapp/sdk/ads/splash/SplashHtml.java
https://lh6.ggpht.com/Vo9wbFH89BbDbWFhUezQZOGPKmfkJSAtIbVWk3QxPbvJwcR8I79EVuI0aB41a-je7x-6=w200	com/startapp/sdk/ads/splash/SplashHtml.java
https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/sdk/insight/NetworkTestsMetaData.java
https://geoip.api.p3insight.de/geoip/	com/startapp/sdk/insight/NetworkTestsMetaData.java
https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/networkTest/a.java
https://geoip.api.c0nnectthed0ts.com/geoip/	com/startapp/networkTest/a.java
https://awsdus.api.p3insight.de/isupload/upload_check_lumen.php	com/startapp/networkTest/a.java
https://ul.api.c0nnectthed0ts.com/ul/v3/	com/startapp/networkTest/a.java
https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/networkTest/startapp/NetworkTester.java
https://geoip.api.c0nnectthed0ts.com/geoip/	com/startapp/networkTest/startapp/NetworkTester.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t.java
https://imgs1.e-droid.net/srv/imgs/ususgal/	lovenews/azca/t.java
https://imgs1.e-droid.net/srv/imgs/videos_pro/v	lovenews/azca/t.java

URL信息	Url所在文件
https://imgs1.e-droid.net/android-app-creator/game/promo	lovenews/azca/t.java
https://imgs1.e-droid.net/srv/imgs/videos_busc/v	lovenews/azca/t.java
https://video.e-droid.net/files_pro/v	lovenews/azca/t.java
http://jugar/	lovenews/azca/profile.java
https://jugar/	lovenews/azca/profile.java
https://video.e-droid.net/files_pro/v	lovenews/azca/profile.java
https://imgs1.e-droid.net/srv/imgs/ususgal/	lovenews/azca/profile.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/profile.java
https://imgs1.e-droid.net/srv/imgs/videos_pro/v	lovenews/azca/profile.java
http://join-app.net/a1013702/	lovenews/azca/chat_perfil.java
https://play.google.com/store/apps/details?id=	lovenews/azca/chat_perfil.java
http://play.google.com/store/apps/details?id=	lovenews/azca/chat_perfil.java
https://www.appcreator24.com/app	lovenews/azca/chat_perfil.java
http://www.appcreator24.com/app	lovenews/azca/chat_perfil.java
https://graph.facebook.com/	lovenews/azca/chat_perfil.java
https://imgs1.e-droid.net/srv/imgs/fondos_submenu/	lovenews/azca/t_submenu.java

URL信息	Url所在文件
http://wallkit.instal.com	lovenews/azca/t_url.java
https://wallkit.instal.com	lovenews/azca/t_url.java
https://moregames	lovenews/azca/t_url.java
https://quiz_tableclasif	lovenews/azca/t_url.java
http://perfilajeno/	lovenews/azca/t_url.java
https://perfilajeno/	lovenews/azca/t_url.java
http://perfilpropio/?desdeforo	lovenews/azca/t_url.java
https://perfilpropio/?desdeforo	lovenews/azca/t_url.java
https://closethis	lovenews/azca/t_url.java
http://tel:	lovenews/azca/t_url.java
http://mailto:	lovenews/azca/t_url.java
http://smsto:	lovenews/azca/t_url.java
http://action_	lovenews/azca/t_url.java
http://go:	lovenews/azca/t_url.java
http://goid:	lovenews/azca/t_url.java
https://www.youtube.com/watch?v=	lovenews/azca/t_url.java

URL信息	Url所在文件
http://www.appcreator24.com/open	lovenews/azca/t_url.java
https://www.appcreator24.com/open	lovenews/azca/t_url.java
https://docs.google.com/viewer?embedded=true&url=	lovenews/azca/t_url.java
https://imgs1.e-droid.net/srv/imgs/ususgal/	lovenews/azca/s.java
https://imgs1.e-droid.net/srv/imgs/videos_pro/v	lovenews/azca/s.java
https://imgs1.e-droid.net/android-app-creator/game/promo	lovenews/azca/s.java
https://imgs1.e-droid.net/srv/imgs/videos_busc/v	lovenews/azca/s.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/s.java
http://tel:	lovenews/azca/t_html.java
http://mailto:	lovenews/azca/t_html.java
http://smsto:	lovenews/azca/t_html.java
http://action_	lovenews/azca/t_html.java
http://go:	lovenews/azca/t_html.java
https://www.youtube.com/watch?v=	lovenews/azca/t_html.java
http://www.appcreator24.com/open	lovenews/azca/t_html.java
https://www.appcreator24.com/open	lovenews/azca/t_html.java

URL信息	Url所在文件
https://docs.google.com/viewer?embedded=true&url=	lovenews/azca/t_html.java
https://imgs1.e-droid.net/srv/imgs/gen/1013702_slider.png?v=	lovenews/azca/s_cargar_sliderheader.java
https://video-upload.e-droid.net/upload.php	lovenews/azca/t_chat.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_chat.java
https://imgs1.e-droid.net/srv/imgs/frases/f	lovenews/azca/t_chat.java
https://imgs1.e-droid.net/srv/imgs/videos/v	lovenews/azca/t_chat.java
https://video.e-droid.net/files/v	lovenews/azca/t_chat.java
https://imgs1.e-droid.net/srv/imgs/chat/	lovenews/azca/t_chat.java
https://imgs1.e-droid.net/srv/imgs/cards/	lovenews/azca/t_card.java
https://imgs1.e-droid.net/srv/imgs/gal/	lovenews/azca/t_gal.java
https://imgs1.e-droid.net/srv/imgs/seccs/	lovenews/azca/t_gal.java
https://imgs1.e-droid.net/android-app-creator/icos_secc/	lovenews/azca/t_gal.java
https://imgs1.e-droid.net/srv/imgs/fondos_menu/fm1013702.png?v=	lovenews/azca/t_menugrid.java
www.appcreator24.com/open1013702/	lovenews/azca/config.java
http://action_	lovenews/azca/config.java
http://tel:	lovenews/azca/config.java

URL信息	Url所在文件
http://mailto:	lovenews/azca/config.java
http://smsto:	lovenews/azca/config.java
https://www.youtube.com/watch?v=	lovenews/azca/config.java
https://imgs1.e-droid.net/srv/imgs/gen/	lovenews/azca/t_buscchats.java
https://video.e-droid.net/files_busc/v	lovenews/azca/t_buscvideos.java
https://imgs1.e-droid.net/srv/imgs/videos_busc/v	lovenews/azca/t_buscvideos.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_buscvideos.java
http://tel:	lovenews/azca/t_detalle_fr.java
http://mailto:	lovenews/azca/t_detalle_fr.java
http://smsto:	lovenews/azca/t_detalle_fr.java
http://go:	lovenews/azca/t_detalle_fr.java
https://www.youtube.com/watch?v=	lovenews/azca/t_detalle_fr.java
https://docs.google.com/viewer?embedded=true&url=	lovenews/azca/t_detalle_fr.java
https://www.paypal.com/cgi-bin/webscr/?rm=2&cmd=_xclick&business=	lovenews/azca/t_detalle_fr.java
https://CLOSETHIS	lovenews/azca/t_detalle_fr.java
https://imgs1.e-droid.net/srv/imgs/seccs/	lovenews/azca/t_video_exoplayer.java

URL信息	Url所在文件
https://imgs1.e-droid.net/android-app-creator/icos_secc/	lovenews/azca/t_video_exoplayer.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_video_exoplayer.java
https://global.appnext.com/offerWallApi.aspx?id=	lovenews/azca/t_video_exoplayer.java
https://imgs1.e-droid.net/srv/imgs/seccs/	lovenews/azca/s_cargar_icos.java
https://imgs1.e-droid.net/android-app-creator/icos_secc/	lovenews/azca/s_cargar_icos.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/preperfil.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_buscusus.java
http://tel:	lovenews/azca/t_and.java
http://mailto:	lovenews/azca/t_and.java
http://smsto:	lovenews/azca/t_and.java
http://action_	lovenews/azca/t_and.java
http://go:	lovenews/azca/t_and.java
https://www.youtube.com/watch?v=	lovenews/azca/t_and.java
https://docs.google.com/viewer?embedded=true&url=	lovenews/azca/t_and.java
https://imgs1.e-droid.net/srv/imgs/and_items/f	lovenews/azca/t_and.java
https://imgs1.e-droid.net/srv/imgs/gen/	lovenews/azca/s_cargar_icos_gen.java

URL信息	Url所在文件
http://tel:	lovenews/azca/t_rssdetalle_fr.java
http://mailto:	lovenews/azca/t_rssdetalle_fr.java
http://smsto:	lovenews/azca/t_rssdetalle_fr.java
http://go:	lovenews/azca/t_rssdetalle_fr.java
https://www.youtube.com/watch?v=	lovenews/azca/t_rssdetalle_fr.java
https://docs.google.com/viewer?embedded=true&url=	lovenews/azca/t_rssdetalle_fr.java
https://global.appnext.com/offerWallApi.aspx?id=	lovenews/azca/t_video_pro.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_video_pro.java
https://www.google.com/maps/search/?api=1&query=	lovenews/azca/t_mapa_web.java
https://imgs1.e-droid.net/srv/imgs/ofics/f	lovenews/azca/t_oficinas.java
https://imgs1.e-droid.net/srv/imgs/gen/	lovenews/azca/t_buscchats_lista.java
https://global.appnext.com/offerWallApi.aspx?id=	lovenews/azca/t_buscvideo.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_buscvideo.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_radio.java
https://imgs1.e-droid.net/srv/imgs/radio/	lovenews/azca/t_radio.java
https://apk.e-droid.net/apk/app1013702.apk?v=	lovenews/azca/preinicio.java

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	lovenews/azca/preinicio.java
https://video.e-droid.net/files_pro/v	lovenews/azca/preinicio.java
www.appcreator24.com/open1013702/	lovenews/azca/preinicio.java
https://imgs1.e-droid.net/srv/imgs/gen/1013702_splash.png?v=	lovenews/azca/preinicio.java
https://imgs1.e-droid.net/srv/imgs/fonts/app1013702.ttf?v=	lovenews/azca/preinicio.java
https://imgs1.e-droid.net/srv/imgs/gen/1013702_icohome.png?v=	lovenews/azca/preinicio.java
https://imgs1.e-droid.net/srv/imgs/icos/app1013702_	lovenews/azca/preinicio.java
https://imgs1.e-droid.net/srv/imgs/seccs/	lovenews/azca/t_video.java
https://imgs1.e-droid.net/android-app-creator/icos_secc/	lovenews/azca/t_video.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/t_video.java
https://global.appnext.com/offerWallApi.aspx?id=	lovenews/azca/t_video.java
https://imgs1.e-droid.net/srv/imgs/gen/1013702_fondo.png?v=	lovenews/azca/s_cargar_fondo.java
https://imgs1.e-droid.net/srv/imgs/usus/	lovenews/azca/o.java
https://api-project-751842291101.firebaseio.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://api-project-751842291101.firebaseio.com	info App talks to a Firebase Database.

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

向手机申请的权限	是否危险	类型	详细情况
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-25 12:06:18+00:00
Valid To: 2050-04-25 12:06:18+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x2ec39f4c3c110df54ff9e0922663a7f1592b29bb
Hash Algorithm: sha256
md5: 7f6104831699b48dca9f6ffa4c157bf7
sha1: 5abab2694c2c51dfded005152df32bba45345a87
sha256: 7d81d57be9b6f6439e257a7df07fa9ccf81781096b1ec84913f3ea85e7cf3154
sha512: 3d7eb5ac13711b38a1691d2e17bf52f5b8b06fb4eab8b23a2e456071bbb2858f18a919599d6bd9eef82057c6b490e971329cfbeb4a07230ff07ed8a677bc2d3e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 8ec10e8aa9733321ce367851b679ff452c74eeee308f7864168d9765f02aa63f

Exodus威胁情报

名称	分类	URL链接
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90
Appnext		https://reports.exodus-privacy.eu.org/trackers/184
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Startapp	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/195

硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"firebase_database_url" : "https://api-project-751842291101.firebaseio.com"

可能的敏感信息
"google_api_key" : "AIzaSyCtzGwdiM8t6R6Ff6uCwEYggQECaFdCcFA"
"google_crash_reporting_api_key" : "AIzaSyCtzGwdiM8t6R6Ff6uCwEYggQECaFdCcFA"
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "تفضل بزيارة facebook.com/device وإدخال الرمز الموضح أعلاه."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device '[redacted]"
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "facebook.com/device[redacted]"

可能的敏感信息
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "[redacted] facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted] "
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]."
"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device şi introdu codul de mai sus."

可能的敏感信息
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device ■■■ ■■■■ ■■■ ■■■■ ■■■ ■■■■■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "facebook.com/device</b&gt ■■ ■■■■■■ ■■;■■■ ■■■ ■■■■■■ ■■■ ■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"

应用内通信

活动(ACTIVITY)	通信(INTENT)
lovenews.azca.preinicio	Schemes: http://, https://, Hosts: www.appcreator24.com, join-app.net, Path Prefixes: /open1013702/, /a1013702/,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.lovenews.azca,

加壳分析

文件列表	分析结果
assets/audience_network.dex	壳列表 | 详细情况 反虚拟机 | possible Build.SERIAL check 编译器 | unknown (please file detection issue!)

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>防止反汇编</td><td>illegal class name</td></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
