MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Kilonotes Lite 1.1.3.5.APK

APP名称: Kilonotes Lite

包名: com.topstack.kilonotes

域名线索: 21条

URL线索: 17条

邮箱线索: 0条

分析日期: 2022年2月2日 22:11

📦 文件信息

文件名: qbbjliteb562886.apk
文件大小: 7.02MB
MD5值: c88beefaf3e2a0cde037359e79283dde
SHA1值: 7eda7d685a4f28d4d884f5dc01406168fb7f2aaa
SHA256值: a06f6f1287c043ccf65baa8dae06c8ad343ac6e3879f9c4c711da5b55b4bd905

ℹ APP 信息

App名称: Kilonotes Lite
包名: com.topstack.kilonotes
主活动Activity: net.gsantner.markor.activity.MainActivity
安卓版本名称: 1.1.3.5
安卓版本: 13

🔍 域名线索

域名	是否危险域名	服务器信息
xml.org	good	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 查看地图: Google Map

域名	是否危险域名	服务器信息
www.youtube.com	good	**IP:** 69.63.187.12 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
f-droid.org	good	**IP:** 149.202.95.241 所属国家: France 地区: Hauts-de-France 城市: Roubaix 纬度: 50.694210 经度: 3.174560 查看地图: Google Map
matrix.to	good	**IP:** 172.67.166.203 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
developer.android.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

域名	是否危险域名	服务器信息
play.google.com	good	**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 查看地图: Google Map
files.freemusicarchive.org	good	**IP:** 104.26.10.182 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
crowdin.com	good	**IP:** 76.223.3.83 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
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map

域名	是否危险域名	服务器信息
apache.org	good	**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 查看地图: Google Map
creativecommons.org	good	**IP:** 104.20.150.16 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
hastebin.com	good	**IP:** 104.21.18.231 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
github.githubassets.com	good	**IP:** 185.199.108.154 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708 查看地图: Google Map

域名	是否危险域名	服务器信息
www.freemusicarchive.org	good	**IP:** 104.26.10.182 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
peertube.mastodon.host	good	**IP:** 64.13.192.74 所属国家: United States of America 地区: California 城市: Culver City 纬度: 34.017185 经度: -118.392830 查看地图: Google Map
duckduckgo.com	good	**IP:** 157.240.16.50 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
katex.org	good	**IP:** 178.128.126.116 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

域名	是否危险域名	服务器信息
www.top-stack.com	good	**IP:** 42.81.144.208 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
open.tube	good	**IP:** 31.41.154.68 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264170 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
gsantner.net	good	**IP:** 35.185.44.232 所属国家: United States of America 地区: South Carolina 城市: North Charleston 纬度: 32.888561 经度: -80.007507 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://xml.org/sax/features/namespaces	com/github/mertakdut/Reader.java
http://xml.org/sax/features/validation	com/github/mertakdut/Reader.java
http://apache.org/xml/features/nonvalidating/load-dtd-grammar	com/github/mertakdut/Reader.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	com/github/mertakdut/Reader.java
https://github.githubassets.com/images/icons/emoji/	com/vladsch/flexmark/ext/emoji/internal/EmojiReference.java
https://github.githubassets.com/images/icons/emoji/	com/vladsch/flexmark/ext/emoji/internal/EmojiResolvedShortcut.java
https://github.githubassets.com/images/icons/emoji/	com/vladsch/flexmark/ext/emoji/internal/EmojiShortcuts.java
https://play.google.com/store/apps/	net/gsantner/opoc/util/ActivityUtils.java
https://hastebin.com	net/gsantner/opoc/util/ShareUtil.java
https://www.example.com	net/gsantner/opoc/util/ShareUtil.java
https://duckduckgo.com/)	net/gsantner/markor/ui/NewFileDialog.java
https://katex.org/docs/supported.html)	net/gsantner/markor/ui/NewFileDialog.java
https://github.com/waylonflinn/markdown-it-katex/blob/master/README.md).	net/gsantner/markor/ui/NewFileDialog.java
https://gsantner.net/assets/blog/img/markor/markor-v1-7-showcase-3.jpg)	net/gsantner/markor/ui/NewFileDialog.java

URL信息	Url所在文件
https://www.youtube.com/watch?v=RJREFH7Lmm8)	net/gsantner/markor/ui/NewFileDialog.java
https://www.youtube.com/embed/RJREFH7Lmm8'	net/gsantner/markor/ui/NewFileDialog.java
https://open.tube/videos/watch/8116312a-dbbd-43a3-9260-9ea6367c72fc)	net/gsantner/markor/ui/NewFileDialog.java
https://peertube.mastodon.host/download/videos/8116312a-dbbd-43a3-9260-9ea6367c72fc-480.mp4'	net/gsantner/markor/ui/NewFileDialog.java
https://www.freemusicarchive.org/music/Guifrog/Xia_Yu)	net/gsantner/markor/ui/NewFileDialog.java
https://files.freemusicarchive.org/storage-freemusicarchive-org/music/ccCommunity/Guifrog/Xia_Yu/Guifrog_-_Xia_Yu.mp3'	net/gsantner/markor/ui/NewFileDialog.java
https://gsantner.net/project/markor?source=markdownref)	net/gsantner/markor/ui/NewFileDialog.java
https://gsantner.net)	net/gsantner/markor/ui/NewFileDialog.java
https://creativecommons.org/publicdomain/zero/1.0/legalcode)	net/gsantner/markor/ui/NewFileDialog.java
https://github.com/gsantner/markor	net/gsantner/markor/ui/NewFileDialog.java
https://gsantner.net/project/markor?source=markdownref	net/gsantner/markor/ui/NewFileDialog.java
https://gsantner.net	net/gsantner/markor/ui/NewFileDialog.java
https://creativecommons.org/publicdomain/zero/1.0/legalcode	net/gsantner/markor/ui/NewFileDialog.java
https://developer.android.com/reference/java/text/SimpleDateFormat#date-and-time-patterns	net/gsantner/markor/format/general/DatetimeFormatDialog.java

URL信息	Url所在文件
http://www.top-stack.com/page/Note_Privacy_Policy_zhCN.html	net/gsantner/markor/activity/MainActivity.java
http://www.top-stack.com/page/Note_Terms_of_use_zhCN.html	net/gsantner/markor/activity/MainActivity.java
https://gsantner.net/project/	net/gsantner/markor/activity/DocumentEditFragment.java
https://github.com/gsantner/markor/issues	Android String Resource
https://matrix.to/#/#markor:matrix.org	Android String Resource
https://github.com/gsantner/markor/blob/master/README.md#contributions	Android String Resource
https://gsantner.net/page/supportme.html?project=markor&source=inapp_supdon	Android String Resource
https://github.com/gsantner/markor	Android String Resource
https://crowdin.com/project/markor/invite	Android String Resource
https://gsantner.net/index.html?source=inapp_license_official_project_source)	Android String Resource
https://github.com/gsantner/markor)	Android String Resource
https://f-droid.org/repository/browse/?fdid=net.gsantner.markor)	Android String Resource
https://play.google.com/store/apps/details?id=net.gsantner.markor)	Android String Resource
http://www.top-stack.com/page/Note_Privacy_Policy_HW_zhCN.html	Android String Resource
https://github.com/gsantner/markor/issues/197	Android String Resource

URL信息	Url所在文件
http://www.top-stack.com/page/Note_Terms_of_use_HW_zhCN.html	Android String Resource

☰ 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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.INSTALL_SHORTCUT	正常		允许应用程序在启动器中安装快捷方式
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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

✿ 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates

Subject: C=86, ST=Anhui, L=Hefei, O=01, OU=01, CN=Top Stack
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-04-20 09:50:09+00:00
Valid To: 2071-04-08 09:50:09+00:00
Issuer: C=86, ST=Anhui, L=Hefei, O=01, OU=01, CN=Top Stack
Serial Number: 0x49abc21e
Hash Algorithm: sha256
md5: baf541fb211f1926f7647355b8d9c576
sha1: baeea3aede0286a414e2a804905275ecdd12a1b3
sha256: f33f11c8065d7206e97eb5ca32870b40eef402d21e75c7d366f0a3023c13e8d7
sha512: ce2ba8fa9238daed4a98a58043dd84eedadc40ebcd7d71706cbc391eb1173bab149688980f0d7d07426fb22bb3126201b9e0c0229be3a6650bf252dc06ba2fe8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6de8c27e019c546df41aba7d946d3769f83f6b0d7f7c846e307a99571f06f821

🔑 硬编码敏感信息

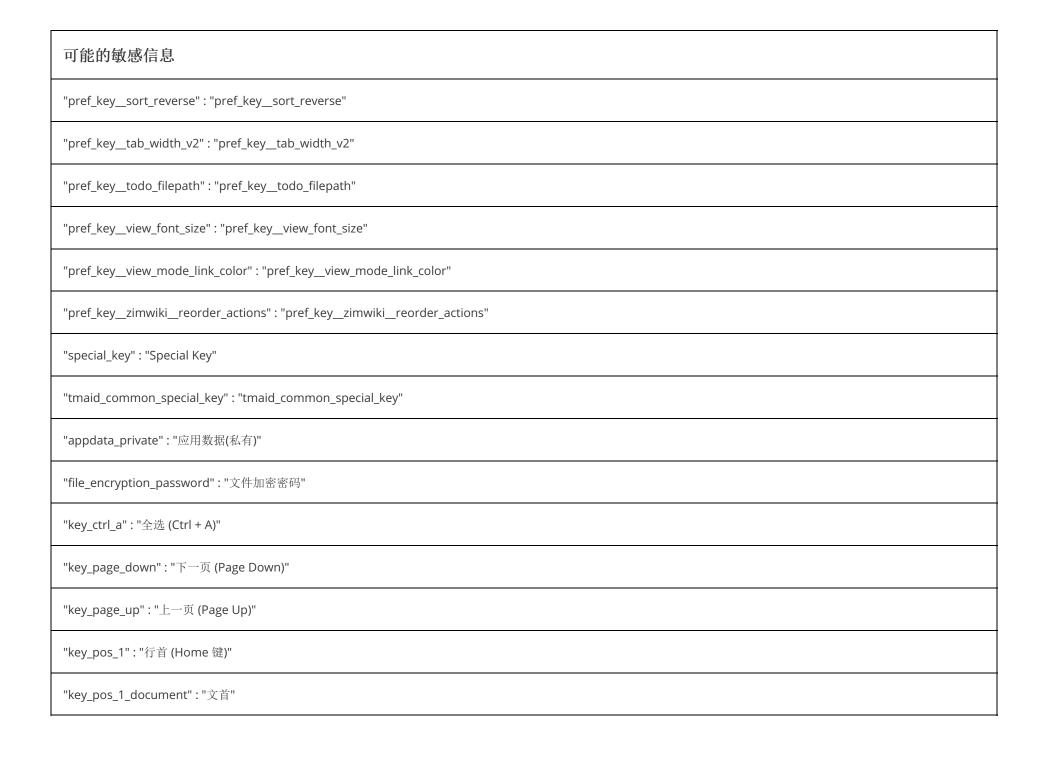| 可能的敏感信息 |
| --- |
| "appdata_private" : "AppData (private)" |
| "file_encryption_password" : "File encryption password" |
| "key_ctrl_a" : "Select all (Ctrl+A)" |
| "key_page_down" : "Page Down (Page Down)" |
| "key_page_up" : "Page Up (Page Up)" |
| "key_pos_1" : "Line Start (Pos Home)" |
| "key_pos_1_document" : "Document Start" |

可能的敏感信息
"key_pos_end" : "Line End (Pos End)"
"key_pos_end_document" : "Document End"
"key_tab" : "Tabulator"
"key_value" : "Key - Value"
"perf_key_policy_private_rule" : "perf_key_policy_private_rule"
"perf_key_policy_user_rule" : "perf_key_policy_user_rule"
"policy_private" : "Privacy Policy"
"policy_user" : "Terms Of Use"
"pref_key__app_start_tab_v2" : "pref_key__app_start_tab_v2"
"pref_key__app_theme" : "pref_key__app_theme"
"pref_key__default_encryption_password" : "pref_key__default_encryption_password"
"pref_key__default_encryption_password_set_once" : "pref_key__default_encryption_password_set_once"
"pref_key__editor_basic_color_scheme__bg_dark" : "pref_key__editor_basic_color_scheme__bg_dark"
"pref_key__editor_basic_color_scheme__bg_light" : "pref_key__editor_basic_color_scheme__bg_light"
"pref_key__editor_basic_color_scheme__fg_dark" : "pref_key__editor_basic_color_scheme__fg_dark"

可能的敏感信息
"pref_key__editor_basic_color_scheme__fg_light" : "pref_key__editor_basic_color_scheme__fg_light"
"pref_key__editor_basic_color_scheme_amoled" : "pref_key__editor_basic_color_scheme_amoled"
"pref_key__editor_basic_color_scheme_blackorwhite" : "pref_key__editor_basic_color_scheme_blackorwhite"
"pref_key__editor_basic_color_scheme_greenscale" : "pref_key__editor_basic_color_scheme_greenscale"
"pref_key__editor_basic_color_scheme_gruvbox" : "pref_key__editor_basic_color_scheme_gruvbox"
"pref_key__editor_basic_color_scheme_markor" : "pref_key__editor_basic_color_scheme_markor"
"pref_key__editor_basic_color_scheme_nord" : "pref_key__editor_basic_color_scheme_nord"
"pref_key__editor_basic_color_scheme_sepia" : "pref_key__editor_basic_color_scheme_sepia"
"pref_key__editor_basic_color_scheme_solarized" : "pref_key__editor_basic_color_scheme_solarized"
"pref_key__editor_disable_spelling_red_underline" : "pref_key__editor_disable_spelling_red_underline"
"pref_key__editor_enable_line_breaking" : "pref_key__editor_enable_line_breaking"
"pref_key__editor_font_size" : "pref_key__editor_font_size"
"pref_key__editor_line_spacing" : "pref_key__editor_line_spacing"
"pref_key__editor_markdown_bigger_headings_2" : "pref_key__editor_markdown_bigger_headings_2"
"pref_key__editor_start_editing_in_center" : "pref_key__editor_start_editing_in_center"

可能的敏感信息
"pref_key__editor_start_editing_on_bottom" : "pref_key__editor_start_editing_on_bottom"
"pref_key__editor_unordered_list_character" : "pref_key__editor_unordered_list_character"
"pref_key__editor_zimwiki_bigger_headings" : "pref_key__editor_zimwiki_bigger_headings"
"pref_key__favourite_files" : "pref_key__favourite_files"
"pref_key__file_description_format" : "pref_key__file_description_format"
"pref_key__font_family" : "pref_key__font_family"
"pref_key__inject_to_body" : "pref_key__inject_to_body"
"pref_key__inject_to_head" : "pref_key__inject_to_head"
"pref_key__is_debug_log_enabled" : "pref_key__is_debug_log_enabled"
"pref_key__is_editor_statusbar_hidden" : "pref_key__is_editor_statusbar_hidden"
"pref_key__is_enable_experimental_features" : "pref_key__is_enable_experimental_features"
"pref_key__is_highlighting_activated" : "pref_key__is_highlighting_activated"
"pref_key__is_highlighting_for_hexcolor_activated" : "pref_key__is_highlighting_for_hexcolor_activated"
"pref_key__is_keep_screen_on" : "pref_key__keep_screen_on"
"pref_key__is_launcher_for_special_files_enabled" : "pref_key__is_launcher_for_special_files_enabled"

可能的敏感信息
"pref_key__is_multi_window_enabled" : "pref_key__is_multi_window_enabled"
"pref_key__is_overview_statusbar_hidden" : "pref_key__is_overview_statusbar_hidden"
"pref_key__is_preview_first" : "pref_key__is_preview_first"
"pref_key__is_render_rtl" : "pref_key__is_render_rtl"
"pref_key__language" : "pref_key__language"
"pref_key__last_opened_directory" : "pref_key__last_opened_directory"
"pref_key__load_last_directory_at_startup" : "pref_key__load_last_directory_at_startup"
"pref_key__markdown__auto_renumber_ordered_list" : "pref_key__markdown__auto_renumber_ordered_list"
"pref_key__markdown__disable_code_block_highlight" : "pref_key__markdown__disable_code_block_highlight"
"pref_key__markdown__highlight_lineending_two_or_more_space" : "pref_key__markdown__highlight_lineending_two_or_more_space"
"pref_key__markdown__hl_delay_v2" : "pref_key__markdown__hl_delay_v2"
"pref_key__markdown__monospace_some_parts" : "pref_key__markdown__monospace_some_parts"
"pref_key__markdown__reorder_actions" : "pref_key__markdown__reorder_actions"
"pref_key__markdown_render_math" : "pref_key__markdown_render_math"
"pref_key__markdown_show_toc" : "pref_key__markdown_show_toc"

可能的敏感信息
"pref_key__more_info__settings" : "pref_key__more_info__settings"
"pref_key__navigationbar_color" : "pref_key__navigationbar_color"
"pref_key__notebook_directory" : "pref_key__notebook_directory"
"pref_key__popular_documents" : "pref_key__popular_documents"
"pref_key__quicknote_filepath" : "pref_key__quicknote_filepath"
"pref_key__recent_documents" : "pref_key__recent_documents"
"pref_key__share_into__calendar_event" : "pref_key__share_into__calendar_event"
"pref_key__share_into__clipboard" : "pref_key__share_into__clipboard"
"pref_key__share_into__existing_document" : "pref_key__share_into__existing_document"
"pref_key__share_into__open_in_browser" : "pref_key__share_into__open_in_browser"
"pref_key__share_into__quicknote" : "pref_key__share_into__quicknote"
"pref_key__share_into__reshare" : "pref_key__share_into__reshare"
"pref_key__share_into__todo" : "pref_key__share_into__todo"
"pref_key__show_dot_files" : "pref_key__show_dot_files"
"pref_key__sort_method" : "pref_key__sort_method"

可能的敏感信息
"pref_key__sort_reverse" : "pref_key__sort_reverse"
"pref_key__tab_width_v2" : "pref_key__tab_width_v2"
"pref_key__todo_filepath" : "pref_key__todo_filepath"
"pref_key__view_font_size" : "pref_key__view_font_size"
"pref_key__view_mode_link_color" : "pref_key__view_mode_link_color"
"pref_key__zimwiki__reorder_actions" : "pref_key__zimwiki__reorder_actions"
"special_key" : "Special Key"
"tmaid_common_special_key" : "tmaid_common_special_key"
"appdata_private" : "应用数据(私有)"
"file_encryption_password" : "文件加密密码"
"key_ctrl_a" : "全选 (Ctrl + A)"
"key_page_down" : "下一页 (Page Down)"
"key_page_up" : "上一页 (Page Up)"
"key_pos_1" : "行首 (Home 键)"
"key_pos_1_document" : "文首"

可能的敏感信息
"key_pos_end" : "行末 (End 键)"
"key_pos_end_document" : "文末"
"key_tab" : "制表符"
"policy_private" : "隐私条款"
"policy_user" : "用户协议"
"special_key" : "特殊按键"

加壳分析

文件列表	分析结果
classes.dex	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>编译器</td><td>r8</td></tr></table>