MOBSF

ANDROID STATIC ANALYSIS REPORT

1Tigrow (1.345)

File Name:	Tigrow! by Kid Security_merged.apk
Package Name:	kz.sirius.siriuschat
Scan Date:	Aug. 17, 2024, 9:29 p.m.

App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	13	2	1	1

FILE INFORMATION

File Name: Tigrow! by Kid Security_merged.apk
Size: 25.43MB
MD5: 128d16ba50e568b42819c2664e997f72
SHA1: 194fb813ce366c64ef653f540fe859fb3dff5746
SHA256: bec1ed06de1e62cb4fd0dcf3ec7e4bd10c84ae522157cb1319469e4eb3dce408

APP INFORMATION

App Name: 1Tigrow
Package Name: kz.sirius.siriuschat
Main Activity: kz.sirius.siriuschat.view.activity.MainActivity
Target SDK: 33
Min SDK: 25
Max SDK:
Android Version Name: 1.345
Android Version Code: 347

APP COMPONENTS

Activities: 13
Services: 13
Receivers: 15
Providers: 4
Exported Activities: 1
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=KZ, ST=Unknown, L=Astana, O=ҒҒ <atZhan>, OU=Ayapov, CN=Talgat
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-01-27 18:26:52+00:00
Valid To: 2044-06-14 18:26:52+00:00
Issuer: C=KZ, ST=Unknown, L=Astana, O=ҒҒ <atZhan>, OU=Ayapov, CN=Talgat
Serial Number: 0x7fc814e9
Hash Algorithm: sha256

md5: 8ce28f3e7d1a87355d20b635e0aa6330
sha1: 78aa45bb52a5d0bd6eeadbab4334c1eef56f7bfa
sha256: 7507f451fb25e20ab388dfc682343b9c80291c2e8779981fcd2ba412550e7fc1
sha512: e946a4574ca011de5c907f2dc81dbf4cf38afaf69ec971e7ed281ff57df5e3e89691c921cd8939fa4f4851ec1a572fc3eb948138c9ed1b46f085639639d71390
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 83bcc95b0479c689d0b8171b189b102a4f1bb65fc23a49b942e49a9b7a8f226b
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.RECEIVE_BOOT_COMPLETE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
kz.sirius.siriuschat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check SIM operator check FINDINGS: Compiler — r8 without marker (suspicious)
classes2.dex	FINDINGS: Anti Debug Code — Debug.isDebuggerConnected() check FINDINGS: Anti-VM Code — Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check FINDINGS: Compiler — r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.1-7.1.2, [minSdk=25]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.canhub.cropper.CropImageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (kz.sirius.siriuschat.applimits.AppInstallReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	kz/sirius/siriuschat/applimits/AppDBHelper.java kz/sirius/siriuschat/readnotifications/MessageSentDBHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/canhub/cropper/BitmapUtils.java com/canhub/cropper/CropImageActivity.java com/canhub/cropper/utils/GetUriForFileKt.java com/datadog/android/core/internal/data/upload/CurlInterceptor.java com/datadog/android/ndk/internal/NdkCrashLog.java com/datadog/android/rum/DdRumContentProvider.java kz/sirius/siriuschat/push/UniListenerService.java kz/sirius/siriuschat/retrofit/services/AddParentRepository.java kz/sirius/siriuschat/retrofit/services/AddParentServiceImpl.java kz/sirius/siriuschat/retrofit/services/ApiServiceImpl.java kz/sirius/siriuschat/retrofit/services/LimitRepository.java kz/sirius/siriuschat/retrofit/services/LimitServiceImpl.java kz/sirius/siriuschat/retrofit/services/Repository.java kz/sirius/siriuschat/retrofit/services/TrackerRepository.java kz/sirius/siriuschat/retrofit/services/TrackeriServiceImpl.java kz/sirius/siriuschat/view/activity/ParentAttentionActivity.java kz/sirius/siriuschat/view/fragment/ChatFragment.java kz/sirius/siriuschat/view/fragment/DreamerHistoryFragment.java kz/sirius/siriuschat/wiretapping/Wiretapping.java pub/devrel/easypermissions/EasyPermissions.java pub/devrel/easypermissions/helper/ActivityPermissionHelper.java pub/devrel/easypermissions/helper/BaseSupportPermissionsHelper.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/datadog/android/api/net/RequestFactory.java com/datadog/android/core/SdkInternalLogger.java com/datadog/android/core/internal/metrics/BatchMetricsDispatcher.java com/datadog/android/log/internal/LogsFeature.java com/datadog/android/rum/internal/FeaturesContextResolver.java com/datadog/android/rum/internal/RumFeature.java com/datadog/android/rum/internal/domain/event/RumEventMeta.java com/datadog/android/rum/internal/domain/scope/ExternalResourceTimingsKt.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/android/rum/internal/domain/scope/RumSessionScope.java com/datadog/android/telemetry/internal/TelemetryEventHandler.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java kz/sirius/siriuschat/retrofit/request/NewChatMessage.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	kz/sirius/siriuschat/retrofit/services/AddParentServiceImpl.java kz/sirius/siriuschat/retrofit/services/ApiServiceImpl.java kz/sirius/siriuschat/retrofit/services/LimitServiceImpl.java kz/sirius/siriuschat/retrofit/services/TrackeriServiceImpl.java
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/lyft/kronos/AndroidClockFactory.java kz/sirius/siriuschat/service/PostProvisioningHelper.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/canhub/cropper/BitmapUtils.java kz/sirius/siriuschat/util/Utils.java kz/sirius/siriuschat/util/UtilsPerms.java
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	kz/sirius/siriuschat/util/Utils.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/canhub/cropper/BitmapUtils.java com/canhub/cropper/CropImageActivity.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.
2	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/24	android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	9/45	android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_WIFI_STATE, android.permission.CALL_PHONE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, android.permission.PACKAGE_USAGE_STATS, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dev-sirius.kidsecurity.tech	ok	**IP:** 67.207.72.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
dev-svc.kidsecurity.tech	ok	**IP:** 67.207.72.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
dev-debug.kidsecurity.tech	ok	**IP:** 67.207.72.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
rest.kidsecurity.tech	ok	**IP:** 138.68.115.229 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
dev-gw.kidsecurity.tech	ok	**IP:** 206.81.26.59 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomediacodec.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
gw.gps-watch.kz	ok	**IP:** 185.5.248.2 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
svc.kidsecurity.tech	ok	**IP:** 138.68.115.229 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.webrtc.org	ok	**IP:** 172.217.16.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sirius.kidsecurity.tech	ok	**IP:** 157.230.16.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dev-rest.kidsecurity.tech	ok	**IP:** 67.207.72.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
rest.gps-watch.kz	ok	**IP:** 185.5.248.2 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
debug.gps-watch.kz	ok	**IP:** 185.5.248.2 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
yadi.sk	ok	**IP:** 87.250.250.50 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
child-packet.gps-watch.kz	ok	**IP:** 185.5.248.2 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
debug.kidsecurity.tech	ok	**IP:** 157.245.25.153 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
kidsecurity.net	ok	**IP:** 51.83.226.243 **Country:** Poland **Region:** Mazowieckie **City:** Warsaw **Latitude:** 52.229771 **Longitude:** 21.011780 **View:** Google Map
eng.kidsecurity.net	ok	**IP:** 51.83.226.243 **Country:** Poland **Region:** Mazowieckie **City:** Warsaw **Latitude:** 52.229771 **Longitude:** 21.011780 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
child-packet.kidsecurity.tech	ok	**IP:** 138.68.115.229 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sirius.gps-watch.kz	ok	**IP:** 158.160.77.112 **Country:** Venezuela (Bolivarian Republic of) **Region:** Carabobo **City:** Valencia **Latitude:** 10.162020 **Longitude:** -68.007652 **View:** Google Map
kz-sirius-child.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
dev-child-packet.kidsecurity.tech	ok	**IP:** 67.207.72.53 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
svc.gps-watch.kz	ok	**IP:** 185.5.248.2 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
gw.kidsecurity.tech	ok	**IP:** 167.99.251.182 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://kz-sirius-child.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
652958122426@fcm.googleapis	kz/sirius/siriuschat/push/SiriusMessagingListenerService.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://kz-sirius-child.firebaseio.com"
"google_api_key" : "AIzaSyCz3wxbvA5_EnvfSDk8Qe4JMbALehBq3KE"
"google_crash_reporting_api_key" : "AIzaSyCz3wxbvA5_EnvfSDk8Qe4JMbALehBq3KE"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
5181942b9ebc31ce68dacb56c16fd79f
470fa2b4ae81cd56ecbcda9735803434cec591fa

POSSIBLE SECRETS
bc2d7e71bd39bc49870b6681312f526b4
ae2044fb577e65ee8bb576ca48a2f06e
110fe81d-63db-4913-bbab-9e0fc79a0713
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

PLAYSTORE INFORMATION

Title: Tigrow! by Kid Security

Score: 3.292683 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** kz.sirius.siriuschat

Developer Details: Kid security LLP, 8196086933510381552, Kazahstan, Astana, Abay street 18 office 306, https://kidsecurity.net, siriuskids@mail.ru,

Release Date: Apr 17, 2019 **Privacy Policy:** Privacy link

Description:

Tigrow is a companion app to Kid Security, our parent phone app. Please only download this app to a device used by your child or teen. Tigrow is the perfect locator app to track your kids' location using GPS tracker. It has been designed to ensure the well-being and safety of your children. With its powerful features and intuitive interface, Tigrow provides you with real location data about your baby, allowing you to know where your baby is, giving you peace of mind. OUR KEY FEATURES: GPS locator - see your child's location on a map and movement history for the day - online movement diary. Make sure your child stays out of dangerous places; Surround sound - listen to what's going on around your child to see if he or she is okay; Loud alert - send a loud alert to your child's phone if he or she has left it in a backpack or on silent mode and can't hear it ring. Parental controls - find out what apps he's been using at school, if he's been playing in class instead of gaining knowledge. Notifications - make sure your child is on time for school by getting alerts when they get to school, come home, and other places you've created. Battery monitoring - remind your child to charge their phone on time: you'll be notified if the battery is about to run out. Family chat - chat with your child with fun stickers and send voice messages. In case of technical problems you can always contact the 24/7 support team of ""Kid Security"" service via the support chat in the app or by e-mail support@kidsecurity.net. The application requests the following permissions: 1. On top of other applications - to block applications when time limit rules are met; 2. Accessibility - to limit the time of using the phone; 3. Access to usage data - to collect statistics about the time of application; 4. Autorun - for the constant operation of the application tracker on the child's device; 5. Device administrator - to protect against unauthorized deletion. 6. Tigrow sends a list of installed applications to our server https://rest.kidsecurity.tech and http://rest.gps-watch.kz. Our server transmits data to the parent's phone

SCAN LOGS

Timestamp	Event	Error
2024-08-17 21:29:55	Generating Hashes	OK

2024-08-17 21:29:55	Extracting APK	OK
2024-08-17 21:29:55	Unzipping	OK
2024-08-17 21:29:56	Getting Hardcoded Certificates/Keystores	OK
2024-08-17 21:29:58	Parsing AndroidManifest.xml	OK
2024-08-17 21:29:58	Parsing APK with androguard	OK
2024-08-17 21:29:58	Extracting Manifest Data	OK
2024-08-17 21:29:58	Performing Static Analysis on: 1Tigrow (kz.sirius.siriuschat)	OK
2024-08-17 21:29:58	Fetching Details from Play Store: kz.sirius.siriuschat	OK
2024-08-17 21:29:58	Manifest Analysis Started	OK
2024-08-17 21:29:58	Checking for Malware Permissions	OK
2024-08-17 21:29:58	Fetching icon path	OK
2024-08-17 21:29:58	Library Binary Analysis Started	OK
2024-08-17 21:29:58	Analyzing lib/x86_64/libjingle_peerconnection_so.so	OK
2024-08-17 21:29:59	Analyzing apktool_out/lib/x86_64/libjingle_peerconnection_so.so	OK

2024-08-17 21:29:59	Reading Code Signing Certificate	OK
2024-08-17 21:29:59	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/128d16ba50e568b42819c2664e997f72/128d16ba50e568b42819c2664e997f72.apk'])
2024-08-17 21:29:59	Running APKiD 2.1.5	OK
2024-08-17 21:30:02	Detecting Trackers	OK
2024-08-17 21:30:03	Decompiling APK to Java with jadx	OK
2024-08-17 21:30:27	Converting DEX to Smali	OK
2024-08-17 21:30:27	Code Analysis Started on - java_source	OK
2024-08-17 21:30:46	Android SAST Completed	OK
2024-08-17 21:30:46	Android API Analysis Started	OK
2024-08-17 21:30:57	Android Permission Mapping Started	OK
2024-08-17 21:31:15	Android Permission Mapping Completed	OK
2024-08-17 21:31:17	Finished Code Analysis, Email and URL Extraction	OK
2024-08-17 21:31:17	Extracting String data from APK	OK
2024-08-17 21:31:17	Extracting String data from SO	OK

2024-08-17 21:31:17	Extracting String data from Code	OK
2024-08-17 21:31:17	Extracting String values and entropies from Code	OK
2024-08-17 21:31:19	Performing Malware check on extracted domains	OK
2024-08-17 21:31:23	Saving to Database	OK

Report Generated by - MobSF v4.0.6

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.