ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	E-CHALLAN-RTO.apk
Full analysis:	https://app.any.run/tasks/1983260a-354c-465d-8105-28a0e13ebe9f
Verdict:	Malicious activity
Analysis date:	October 29, 2025 at 10:42:22
OS:	Android 14
Tags:	websocket
MIME:	application/zip
File info:	Zip archive data, at least v2.0 to extract, compression method=[0xffffeb5f]
MD5:	753876B01B6895C68EA4728422F0FC34
SHA1:	48C3E982ECADC113082CCD848E64B1243E80B8B6
SHA256:	888F6F88A85117E50A8D3C44E67A90132A514451474D67F832C58A3F6DB9BCB5
SSDEEP:	98304:2W2flg9ykjlNJB5Q+pTALgiC8RE6KpDfuFjkQDbSTeAZ00Vk2QMrJ4rsKOLPLUcF:cL9DxXQYKzmEi20VcwzMJ3rpcVYH1w

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- android (14)
- android.cuttlefish.overlay (14)
- android.cuttlefish.phone.overlay (14)
- android.ext.services (2019-09)
- android.ext.shared (1)
- com.android.adservices.api (14)
- com.android.apps.tag (1.1)
- com.android.backupconfirm (14)
- com.android.bips (14)
- com.android.bluetoothmidiservice (14)
- com.android.bookmarkprovider (14)
- com.android.calendar (14)
- com.android.calllogbackup (14)
- com.android.camera2 (2.0.002)
- com.android.cameraextensions (14)
- com.android.captiveportallogin (14)
- com.android.carrierconfig (1.0.0)
- com.android.carrierdefaultapp (14)
- com.android.cellbroadcastreceiver (R-initial)
- com.android.cellbroadcastreceiver.module (R-initial)
- com.android.cellbroadcastservice (R-initial)
- com.android.certinstaller (14)
- com.android.companiondevicemanager (14)
- com.android.compos.payload (14)
- com.android.connectivity.resources (S-initial)
- com.android.connectivity.resources.cuttlefish.overlay (14)
- com.android.contacts (1.7.34)
- com.android.credentialmanager (14)
- com.android.cts.ctsshim (14-10093150)
- com.android.cts.priv.ctsshim (14-10093150)
- com.android.deskclock (14)
- com.android.devicelockcontroller (14)
- com.android.dialer (23.0)
- com.android.documentsui (14)
- com.android.dreams.basic (14)
- com.android.dreams.phototable (14)
- com.android.dynsystem (14)

- com.android.egg (1.0)
- com.android.emergency (14)
- com.android.ext.adservices.api (14)
- com.android.externalstorage (14)
- com.android.federatedcompute.services (T-initial)
- com.android.gallery3d (1.1.40030)
- com.android.google.gce.gceservice (14)
- com.android.health.connect.backuprestore (14)
- com.android.healthconnect.controller (14)
- com.android.hotspot2.osulogin (14)
- com.android.htmlviewer (14)
- com.android.imsserviceentitlement (14)
- com.android.inputdevices (14)
- com.android.inputmethod.latin (14)
- com.android.intentresolver (2021-11)
- com.android.internal.display.cutout.emulation.corner (1.0)
- com.android.internal.display.cutout.emulation.double (1.0)
- com.android.internal.display.cutout.emulation.hole (1.0)
- com.android.internal.display.cutout.emulation.tall (1.0)
- com.android.internal.display.cutout.emulation.waterfall (1.0)
- com.android.internal.systemui.navbar.gestural (1.0)
- com.android.internal.systemui.navbar.gestural_extra_wide_back (1.0)
- com.android.internal.systemui.navbar.gestural_narrow_back (1.0)
- com.android.internal.systemui.navbar.gestural_wide_back (1.0)
- com.android.internal.systemui.navbar.threebutton (1.0)
- com.android.internal.systemui.navbar.transparent (1.0)
- com.android.keychain (14)
- com.android.launcher3 (14)
- com.android.localtransport (14)
- com.android.location.fused (14)
- com.android.managedprovisioning (14)
- com.android.messaging (1.0.001)
- com.android.microdroid.empty_payload (14)
- com.android.mms.service (14)
- com.android.modulemetadata (14)
- com.android.mtp (14)
- com.android.music (14)
- com.android.musicfx (1.4)
- com.android.nearby.halfsheet (14)
- com.android.networkstack (T-next)
- com.android.networkstack.tethering (14)
- com.android.networkstack.tethering.cuttlefishoverlay (1.0)
- com.android.nfc (14)
- com.android.ondevicepersonalization.services (T-initial)
- com.android.ons (14)
- com.android.packageinstaller (14)
- com.android.pacprocessor (14)
- com.android.permissioncontroller (33 system image)
- com.android.phone (14)
- com.android.printservice.recommendation (1.3.0)
- com.android.printspooler (14)
- com.android.providers.blockednumber (14)
- com.android.providers.calendar (14)
- com.android.providers.contacts (14)
- com.android.providers.downloads (14)
- com.android.providers.downloads.ui (14)
- com.android.providers.media (14)
- com.android.providers.media.module (14)
- com.android.providers.partnerbookmarks (14)
- com.android.providers.settings (14)
- com.android.providers.settings.cuttlefish.overlay (14)
- com.android.providers.telephony (14)
- com.android.providers.userdictionary (14)
- com.android.provision (14)
- com.android.proxyhandler (14)
- com.android.quicksearchbox (14)
- com.android.rkpdapp (14)

- com.android.role.notes.enabled (1.0)
- com.android.safetycenter.resources (33 system image)
- com.android.sdksandbox (T-initial)
- com.android.se (14)
- com.android.server.telecom (14)
- com.android.settings (14)
- com.android.settings.intelligence (14)
- com.android.sharedstoragebackup (14)
- com.android.shell (14)
- com.android.simappdialog (14)
- com.android.soundpicker (14)
- com.android.statementservice (1.0)
- com.android.stk (14)
- com.android.storagemanager (14)
- com.android.systemui (14)
- com.android.systemui.accessibility.accessibilitymenu (14)
- com.android.telephony.qns (14)
- com.android.theme.font.notoserifsource (1.0)
- com.android.traceur (1.0)
- com.android.uwb.resources (T-initial)
- com.android.virtualmachine.res (14)
- com.android.vpndialogs (14)
- com.android.wallpaper.livepicker (14)
- com.android.wallpaperbackup (14)
- com.android.wallpapercropper (14)
- com.android.wallpaperpicker (1.0)
- com.android.webview (137.0.7122.0)
- com.android.wifi.dialog (14)
- com.android.wifi.resources (R-initial)
- com.android.wifi.resources.cf (1.0)
- com.google.android.telephony.satellite (14)
- org.chromium.chrome (137.0.7122.0)

Behavior activities

MALICIOUS

Initiates background APK installation
- app_process64 (PID: 4020)

SUSPICIOUS

Uses encryption API functions
- app_process64 (PID: 4020)

Accesses system-level resources
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Creates a WakeLock to manage power state
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Establishing a connection
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Collects data about the device's environment (JVM version)
- app_process64 (PID: 4020)

Updates data in the storage of application settings (SharedPreferences)
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Checks exemption from battery optimization
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)
- app_process64 (PID: 4434)

Checks if the device's lock screen is showing
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Accesses memory information
- app_process64 (PID: 4020)

Retrieves a list of running services
- app_process64 (PID: 4020)

Retrieves Android OS build information
- app_process64 (PID: 4020)

Acquires a wake lock to keep the device awake

INFO

Dynamically loads a class in Java
- app_process64 (PID: 4020)

Dynamically inspects or modifies classes, methods, and fields at runtime
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Returns elapsed time since boot
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Retrieves data from storage of application settings (SharedPreferences)
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Detects device power status
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Dynamically registers broadcast event listeners
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Handles throwable exceptions in the app
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Creates and writes local files
- app_process64 (PID: 4020)

Gets the display metrics associated with the device's screen
- app_process64 (PID: 4020)
- app_process64 (PID: 4434)

Loads a native library into the application
- app_process64 (PID: 4020)

Gets file name without full path

- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Launches a new activity
- app_process64 (PID: 4020)
- app_process64 (PID: 4434)

Abuses foreground service for persistence
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Connects to unusual port
- app_process64 (PID: 4020)
- app_process64 (PID: 4366)

Monitors and intercepts incoming messages
- app_process64 (PID: 4020)

Retrieves installed applications on device
- app_process64 (PID: 4434)

- app_process64 (PID: 4020)

Verifies whether the device is connected to the internet
- app_process64 (PID: 4434)

Verifies presence of SIM card
- app_process64 (PID: 4434)

Retrieves the value of a secure system setting
- app_process64 (PID: 4434)

Malware configuration

No Malware configuration.

Static information

TRiD

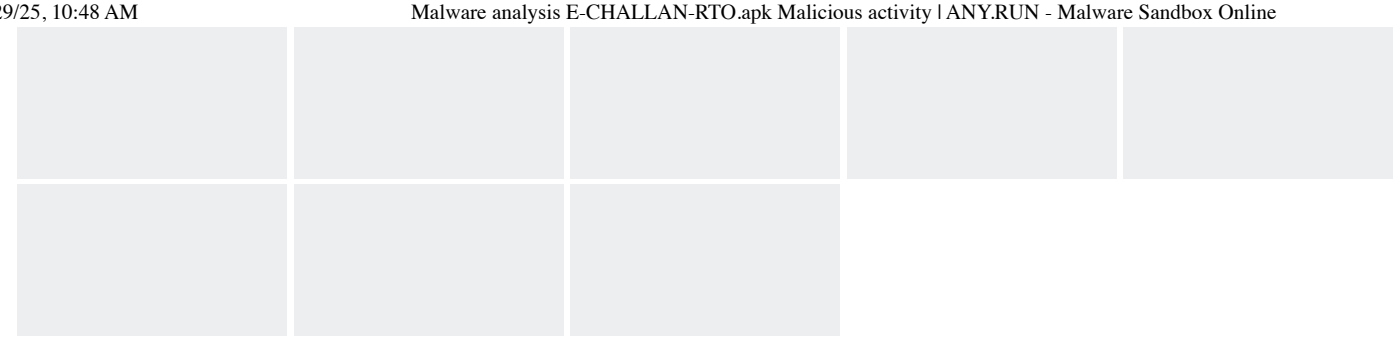
.zip | ZIP compressed archive (100)

EXIF

ZIP

ZipRequiredVersion:	20
ZipBitFlag:	0x0001
ZipCompression:	Unknown (60255)
ZipModifyDate:	2025:10:24 11:13:42
ZipCRC:	0x2335ba4a
ZipCompressedSize:	-
ZipUncompressedSize:	219724
ZipFileName:	resources.arsc

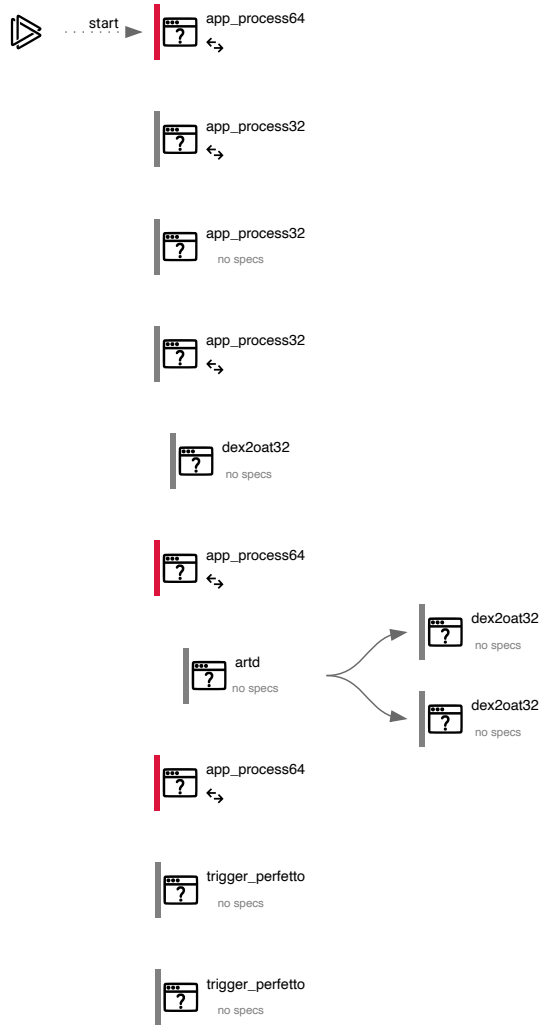
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
141	12	3	0

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
4020	com.zmh.wkjwqvogg	/system/bin/app_process64		app_process64
Information				

User: root Integrity Level: UNKNOWN
Exit code: 0

4102	com.android.webview:webview_service	/system/bin/app_process32	↪	app_process32

Information
User: root Integrity Level: UNKNOWN
Exit code: 0

4103	webview_zygote	/system/bin/app_process32	–	app_process32

Information
User: webview_zygote Integrity Level: UNKNOWN
Exit code: 0

4153	com.android.webview:webview_apk	/system/bin/app_process32	↪	app_process32

Information
User: root Integrity Level: UNKNOWN
Exit code: 0

4351	/apex/com.android.art/bin/dex2oat32 --zip-fd=6 --zip-location=/data/app/~~D8kxTHVAyaKps24y3uhavA==/com.qcec.yjupvn-oxyl_i2aMZ9Vn8G0jCjTUw==/base.apk --oat-fd=7 --oat-location=/data/app/~~D8kxTHVAyaKps24y3uhavA==/com.qcec.yjupvn-oxyl_i2aMZ9Vn8G0jCjTUw==/oat/arm64/base.odex --output-vdex-fd=8 --swap-fd=9 --class-loader-context-fds=10 --class-loader-context=PCL[]{PCL[/system/framework/android.test.base.jar]} --classpath-dir=/data/app/~~D8kxTHVAyaKps24y3uhavA==/com.qcec.yjupvn-oxyl_i2aMZ9Vn8G0jCjTUw== --instruction-set=arm64 --instruction-set-features=default --instruction-set-variant=cortex-a53 --compiler-filter=verify --compilation-reason=install --compact-dex-level=none --max-image-block-size=524288 --resolve-startup-const-strings=true --generate-mini-debug-info --runtime-arg -Xtarget-sdk-version:28 --runtime-arg -Xhidden-api-policy:enabled --runtime-arg -Xms64m --runtime-arg -Xmx512m --comments=app-version-name:1.0,app-version-code:1,art-version:340090000	/apex/com.android.art/bin/dex2oat32	–	artd

Information
User: artd Integrity Level: UNKNOWN
Exit code: 0

4366	com.qcec.yjupvn	/system/bin/app_process64	↪	app_process64

Information
User: root Integrity Level: UNKNOWN
Exit code: 0

4423	/apex/com.android.art/bin/artd	/apex/com.android.art/bin/artd	–	init

Information
User: artd Integrity Level: UNKNOWN
Exit code: 0

4426	/apex/com.android.art/bin/dex2oat32 --zip-fd=6 --zip-location=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-rVE0r_L_Mw==/base.apk --oat-fd=7 --oat-location=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-rVE0r_L_Mw==/oat/arm64/base.odex --output-vdex-fd=8 --swap-fd=9 --class-loader-context=PCL[] --classpath-dir=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-rVE0r_L_Mw== --instruction-set=arm64 --instruction-set-features=default --instruction-set-variant=cortex-a53 --compiler-filter=verify --compilation-reason=install --compact-dex-level=none --max-image-block-size=524288 --resolve-startup-const-strings=true --generate-mini-debug-info --runtime-arg -Xtarget-sdk-version:36 --runtime-arg -Xhidden-api-policy:enabled --runtime-arg -Xms64m --runtime-arg -Xmx512m --comments=app-version-name:1.0,app-version-code:1,art-version:340090000	/apex/com.android.art/bin/dex2oat32	–	artd

Information
User: artd Integrity Level: UNKNOWN
Exit code: 256

4428	/apex/com.android.art/bin/dex2oat32 --zip-fd=6 --zip-location=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-rVE0r_L_Mw==/split_basiccomponent.config.dex.apk --oat-fd=7 --oat-location=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-	/apex/com.android.art/bin/dex2oat32	–	artd

rVE0r_L_Mw==/oat/arm64/split_basiccomponent.config.dex.odex --output-vdex-fd=8 --swap-fd=9 --class-loader-context-fds=10 --class-loader-context=PCL[base.apk] --classpath-dir=/data/app/~~hsMjbxXpW9YE097-RGfb0g==/businessapp.customer-OIyIPLQ4bPw-rVE0r_L_Mw== --instruction-set=arm64 --instruction-set-features=default --instruction-set-variant=cortex-a53 --compiler-filter=verify --compilation-reason=install --compact-dex-level=none --max-image-block-size=524288 --resolve-startup-const-strings=true --generate-mini-debug-info --runtime-arg -Xtarget-sdk-version:36 --runtime-arg -Xhidden-api-policy:enabled --runtime-arg -Xms64m --runtime-arg -Xmx512m --comments=app-version-name:1.0,app-version-code:1,art-version:340090000

Information

User: artd Integrity Level: UNKNOWN

Exit code: 0

4434	businessapp.customer	/system/bin/app_process64	↔	app_process64

Information

User: root Integrity Level: UNKNOWN

Exit code: 0

4707	/system/bin/trigger_perfetto com.android.telemetry.interaction-jank-monitor-39	/system/bin/trigger_perfetto	–	app_process64

Information

User: u0_a82 Integrity Level: UNKNOWN

Exit code: 0

4776	/system/bin/trigger_perfetto com.android.telemetry.interaction-jank-monitor-9	/system/bin/trigger_perfetto	–	app_process64

Information

User: u0_a79 Integrity Level: UNKNOWN

Exit code: 0

Registry activity

Total events	Read events	Write events	Delete events
0	0	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	63	177	0

Dropped files

PID	Process	Filename	Type
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/g9mxbcgv MD5: – SHA256: –	compressed
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/reporter.xml MD5: – SHA256: –	xml
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/app_logs.txt MD5: – SHA256: –	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MTozODkyNzY5Mzc3Mjc6YW5kcm9pZDo1ZDIzMDJlODFlNzk1Mjg1OGQwYmNh.xml MD5: – SHA256: –	xml
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/AppSettings.xml MD5: – SHA256: –	xml
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/com.google.firebase.messaging.xml	xml

		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/images		compressed
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/ic_google_play		image
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/CZ		compressed
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/installer		image
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/img_everyone		image
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/rating		image
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/last-exit-info		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/arm64-v8a		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/WebViewChromiumPrefs.xml		xml
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Web Data-journal		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Shared Dictionary/cache/index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Shared Dictionary/cache/index-dir/temp-index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/WebView/Default/HTTP Cache/Code Cache/wasm/index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/WebView/Default/HTTP Cache/Code Cache/js/index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/WebView/Default/HTTP Cache/Code Cache/wasm/index-dir/temp-index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/WebView/Default/HTTP Cache/Code Cache/js/index-dir/temp-index		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Local Storage/leveldb/MANIFEST-000001		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/DIPS-journal		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Local Storage/leveldb/000001.dbtmp		text
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Local Storage/leveldb/CURRENT		text
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/Local Storage/leveldb/000002.dbtmp		text
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/WebView/font_unique_name_table.pb		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/battery.xml		xml
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/metadata/MANIFEST-000001		binary
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/metadata/000001.dbtmp		text
		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/metadata/CURRENT		text
		MD5: —	SHA256: —	

4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/metadata/000002.dbtmp MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/MANIFEST-000001 MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/000001.dbtmp MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/CURRENT MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/shared_proto_db/000002.dbtmp MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/output8.mp3 MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/original_miner/src_0.apk MD5: — SHA256: —	compressed
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/oat_primary/arm64/base.4020.tmp MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752564.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/SplitApkInstallerminer.xml MD5: — SHA256: —	xml
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/profileInstalled MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752565.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/.org.chromium.Chromium.0ohDRS MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/BrowserMetrics-spare.pma.tmp MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/original_user/src_0.apk MD5: — SHA256: —	compressed
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/original_user/src_2.apk MD5: — SHA256: —	compressed
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/cache/apksigner6498692495427860266.apk MD5: — SHA256: —	compressed
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/SplitApkInstalleruser.xml MD5: — SHA256: —	xml
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752575.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/ic_lottie MD5: — SHA256: —	image
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752585.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/miner.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MTozODkyNzY5Mzc3Mjc6YW5kcm9pZDo1ZDIzMDJlODFlNzk1Mjg1OGQwYmNh.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/com.google.firebase.messaging.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/reporter.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/com.google.android.gms.appid.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/aptabase.xml	xml

		MD5: — SHA256: —	
4366	app_process64	/data/user/0/com.qcec.yjupvn/shared_prefs/fcm.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/files/output8.mp3 MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/shared_prefs/pref.xml MD5: — SHA256: —	xml
4434	app_process64	/data/data/businessapp.customer/files/datastore/FirebaseHeartBeatW0RFRkFVTFRd+MTo3NTY5NzUxODgyMjc6YW5kcm9pZDplNWM0N2ViOTI4NDdlYTAyY2ZkMTM2.preferences_pb.tmp MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/datastore/FirebaseHeartBeatW0RFRkFVTFRd+MTo3NTY5NzUxODgyMjc6YW5kcm9pZDplNWM0N2ViOTI4NDdlYTAyY2ZkMTM2.preferences_pb MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/shared_prefs/com.google.firebase.messaging.xml MD5: — SHA256: —	xml
4366	app_process64	/data/user/0/com.qcec.yjupvn/cache/oat_primary/arm64/base.4366.tmp MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752595.txt MD5: — SHA256: —	text
4434	app_process64	/data/data/businessapp.customer/files/PersistedInstallation698643943795009638 6tmp MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/PersistedInstallation.W0RFRkFVTFRd+MTo3NTY5NzUxODgyMjc6YW5kcm9pZDplNWM0N2ViOTI4NDdlYTAyY2ZkMTM2.json MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/PersistedInstallation6218975809820315254tmp MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/datastore/app-datastore.preferences_pb.tmp MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/profileinstaller_profileWrittenFor_lastUpdateTime.dat MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/files/profileInstalled MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/no_backup/androidx.work.workdb-journal MD5: — SHA256: —	binary
4434	app_process64	/data/data/businessapp.customer/no_backup/androidx.work.workdb-wal MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/oat/mQMZR.cur.prof.qiPsIC.tmp MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752605.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752615.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752625.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752635.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752645.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752655.txt MD5: — SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752665.txt MD5: — SHA256: —	text
4434	app_process64	/data/data/businessapp.customer/files/datastore/app-datastore.preferences_pb MD5: — SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752675.txt	text

		MD5: —	SHA256: —	
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/app_webview/Default/SharedStorage-journal MD5: —	SHA256: —	binary
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752685.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752695.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752705.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752715.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752725.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752735.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752745.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752755.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752765.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752775.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752785.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752795.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752806.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752816.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752826.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752836.txt MD5: —	SHA256: —	text
4020	app_process64	/data/user/0/com.zmh.wkjwqvogg/files/crash/crash_report_1761752846.txt MD5: —	SHA256: —	text

Network activity

HTTP(S) requests: 2
TCP/UDP connections: 26
DNS requests: 13
Threats: 5

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1939	app_process64	GET	204	142.250.181.227:80	http://connectivitycheck.gstatic.com/generate_204	unknown	—	—	whitelisted
—	—	GET	204	172.217.18.4:80	http://www.google.com/gen_204	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation

450	mdnsd	224.0.0.251:5353	–	–	–	whitelisted
–	–	172.217.18.4:80	www.google.com	GOOGLE	US	whitelisted
–	–	142.250.181.227:80	connectivitycheck.gstatic.com	GOOGLE	US	whitelisted
–	–	172.217.18.4:443	www.google.com	GOOGLE	US	whitelisted
579	app_process64	216.239.35.0:123	time.android.com	–	–	whitelisted
1939	app_process64	142.250.181.227:80	connectivitycheck.gstatic.com	GOOGLE	US	whitelisted
1939	app_process64	172.217.18.4:443	www.google.com	GOOGLE	US	whitelisted
2943	app_process64	64.233.184.81:443	staging-remoteprovisioning.sandbox.googleapis.com	GOOGLE	US	whitelisted
4020	app_process64	147.93.153.119:8443	aptabase.fud2026.xyz	–	BE	unknown
4102	app_process32	142.250.184.227:443	clientservices.googleapis.com	GOOGLE	US	whitelisted
4153	app_process32	216.58.206.35:443	update.googleapis.com	GOOGLE	US	whitelisted
4153	app_process32	142.250.185.110:443	dl.google.com	GOOGLE	US	whitelisted
4020	app_process64	207.90.195.25:2000	timeserver.uasecurity.org	RICAWEBSERVICES	CA	malicious
4366	app_process64	147.93.153.119:8443	aptabase.fud2026.xyz	–	BE	unknown
4434	app_process64	35.190.39.113:443	business-apps-7b493-default-rtdb.firebaseio.com	GOOGLE	US	whitelisted
4434	app_process64	142.250.184.234:443	firebaseinstallations.googleapis.com	GOOGLE	US	whitelisted
4434	app_process64	35.201.97.85:443	business-apps-7b493-default-rtdb.firebaseio.com	GOOGLE	US	whitelisted

DNS requests

Domain	IP	Reputation
www.google.com	172.217.18.4	whitelisted
google.com	142.250.185.174	whitelisted
connectivitycheck.gstatic.com	142.250.181.227	whitelisted
time.android.com	216.239.35.0 216.239.35.4 216.239.35.8 216.239.35.12	whitelisted
staging-remoteprovisioning.sandbox.googleapis.com	64.233.184.81	whitelisted
aptabase.fud2026.xyz	147.93.153.119	unknown
clientservices.googleapis.com	142.250.184.227	whitelisted
update.googleapis.com	216.58.206.35	whitelisted
dl.google.com	142.250.185.110	whitelisted
timeserver.uasecurity.org	207.90.195.25	unknown
business-apps-7b493-default-rtdb.firebaseio.com	35.190.39.113 34.120.160.131 34.120.206.254 35.201.97.85	unknown
firebaseinstallations.googleapis.com	142.250.184.234 142.250.185.234 216.58.206.42 216.58.206.74 142.250.185.106 142.250.181.234 142.250.186.170 142.250.186.138 142.250.186.74 142.250.185.170 142.250.186.42 142.250.185.202	whitelisted

	142.250.74.202 142.250.184.202 142.250.185.138 142.250.186.106	
s-usc1b-nss-2141.firebaseio.com	35.201.97.85 35.190.39.113 34.120.206.254 34.120.160.131	unknown

Threats

PID	Process	Class	Message
1939	app_process64	Misc activity	ET INFO Android Device Connectivity Check
4434	app_process64	Not Suspicious Traffic	INFO [ANY.RUN] Firebase Web App Development Platform (firebaseio .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Websocket Upgrade Request
4434	app_process64	Not Suspicious Traffic	INFO [ANY.RUN] Firebase Web App Development Platform (firebaseio .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Websocket Upgrade Request

Debug output strings

No debug info