NCSC under the MOND
Innovation and Training Division
support@ims.nksc.lt

2021-08-23

Assessment of cybersecurity of mobile devices supporting 5G technology sold in Lithuania

ANALYSIS OF PRODUCTS MADE BY *Huawei*, *Xiaomi* and *OnePlus*

Introduction

To ensure the use of secure software and hardware in the country, the National Cyber Security Centre (NCSC) under the Ministry of National Defence carried out a cyber security assessment of mobile devices supporting 5G technology sold in Lithuania by Chinese manufacturers. This analysis presents the results of the assessment of smartphones manufactured by Huawei, Xiaomi and OnePlus.

Huawei, Xiaomi and OnePlus are Chinese IT and consumer electronics manufacturers with an international presence[1] and a strong presence in the European market[2]. In 2020, these manufacturers introduced to the Lithuanian market smartphones supporting fifth-generation (5G) mobile technology. The security assessment was carried out for widely available Huawei P40 5G[3], Xiaomi Mi 10T 5G[4] and OnePlus 8T 5G[5] mobile devices. Images of the devices examined in the assessment are shown in Figure 1.

Huawei P40 5G *Xiaomi Mi 10T 5G* *OnePlus 8T 5G*

Figure 1: The devices examined in the assessment. Front and rear panel views

[1] CNET. "Huawei, OnePlus and beyond: China's biggest smartphone brands you should know about". *https://www.cnet.com/news/huawei-oneplus-china-biggest-smartphone-brands-you-should-know-about-lenovo-meizu-xiaomi-oppo-vivo/*

[2] Counterpoint. European Smartphone Market Down 14 % YoY in 2020; Xiaomi Gains While Huawei and Samsung Lose. *https://www.counterpointresearch.com/european-smartphone-market-2020/*

[3] Huawei. Technical parameters of Huawei P40 5G. *https://consumer.huawei.com/en/phones/p40-pro/specs/*

[4] Xiaomi. Technical parameters of Xiaomi Mi 10T 5G. *https://www.mi.com/global/mi-10t-pro/specs/*

[5] OnePlus. Technical parameters of OnePlus 8T 5G. *https://www.oneplus.com/lt/8t/specs*

Despite these brands being well-known, in the 2017-2021 period the corporations faced security challenges for the equipment being developed; according to the CVE database (Common Vulnerabilities and Exposures), 9 vulnerabilities[6] related to the risk of personal data leaking were identified for Xiaomi's production (8 of these vulnerabilities could be realised by remote means), 144 vulnerabilities[7] were identified for Huawei's products during this period (28 vulnerabilities were identified in 2020; 23 in the first half of 2021), most of which were related to disruption of device functionality, and one vulnerability was identified in 2020 allowing an attacker to use third-party software to send SMS text from a mobile device when the mobile device was locked.[8]

Various sources assess that these manufacturers have a leading position[9,10] in the mobile device market, and their wide assortment of products, their development of new technologies and their noticeable growth in Lithuania undoubtedly make them an appropriate object for cyber security research.

Conclusions of the study

Decomposition analysis performed on mobile devices manufactured by Huawei, Xiaomi and OnePlus identified 10 instances of increased cybersecurity risk. This cybersecurity assessment analyses 4 cybersecurity risks related to the general security of factory-installed applications in the devices, threats of leakage of personal data, and restrictions on freedom of expression. It is planned to describe in detail the other cybersecurity risks identified in this comprehensive study, and to present the assessment of such risks by the end of 2021. This analysis examines issues related to the security of personal data.

The analysis showed that the process of installing mobile applications on Huawei devices is characterised by cybersecurity uncertainties. For the installation of mobile applications on Huawei phones, a manufacturer-based infrastructure is used, which consists of the official electronic application store AppGallery and peripheral application distribution platforms.

When the user intents to install the mobile application on a Huawei device, a search for the mobile application is performed in the AppGallery store; when the application is found, it is downloaded and installed on the mobile device. However, if the application is not found in the official store, the user is automatically directed to peripheral application distribution platforms, from which the mobile application is downloaded to the mobile device for installation. It is worth noting that most of the application distribution platforms are located in countries not covered by the General Data Protection Regulation, which creates a corresponding risk of leakage of user metadata. The study found that a portion of the mobile applications contained on the application distribution platforms are imitations of the original applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on the mobile phone, thereby jeopardising the security of the device and the data contained in it.

Data security risks have also been identified in the Xiaomi device; factory-installed system applications send statistical data on the activity of certain applications installed on the device to servers of the Chinese cloud service provider Tencent, located in Singapore, the USA, the

[6] CVE database. Publicly announced vulnerabilities in Xiaomi products. *https://www.cvedetails.com/vulnerability-list/vendor_id-19038/MI.html*

[7] CVE database. Publicly announced vulnerabilities in Huawei products. *https://www.cvedetails.com/vendor/5979/Huawei.html*

[8] CVE database. Publicly announced vulnerabilities in OnePlus products. *https://www.cvedetails.com/vendor/16036/Oneplus.html*

[9] BusinessChief. *https://businesschief.asia/technology/chinese-smartphone-brand-xiaomi-beats-apple-europe-sales*

[10] Fortune. *https://fortune.com/2020/11/25/xiaomi-third-quarter-results-largest-western-europe/*

Netherlands, Germany and India.

It was found that the original browser of the device, Mi Browser, uses two data collection modules: Google Analytics and Sensor Data. The Google Analytics module installed on the device allows the browsing and search history to be read, to send this data to analytics servers which Xiaomi accesses and the data of which Xiaomi uses[11]. This functionality is activated by registering the mobile phone into the Xiaomi User Experience marketing programme. By default, this is automatically done during the phone's first activation or when reset to factory settings.

The Sensor Data module used in the device has been found to collect statistical information on 61 parameters (time of activation of application, language used, etc.) about the activity of applications used. The collected statistics are sent via an encrypted channel to Xiaomi servers in Singapore, which is not covered by the General Data Protection Regulation. According to international sources, clear cases of unauthorised collection of user data by Xiaomi have been identified[12,13]. Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

It has also been established that when a user chooses to use Xiaomi cloud services, the user's mobile phone number is registered on servers located in Singapore. This is done by the device sending an encrypted SMS message to a special phone number. After receiving the SMS message, the server synchronises it with the Xiaomi server in Singapore, from which the phone downloads a confirmation via mobile internet, allowing the user to connect to the Xiaomi cloud service. It has been established that the registration of a telephone number is carried out regardless of whether the user chooses to be authenticated by phone number or by e-mail address. It is important to note that the encrypted and sent SMS message and its addressee are not visible to the user.

The automated sending of messages and the software functionality of their concealment pose potential threats to the security of the device and personal data; in this way, without the user's knowledge, device data can be collected and transmitted to remote servers.

The Xiaomi Cloud service is designed to store and synchronise the data stored on the device (data stored in the contact book, call history, SMS messages, photos, notes, Wi-Fi settings and browsing history, etc.) on remote servers. Using this service, user data is sent to servers located in Singapore.

Xiaomi system applications (Security, MiBrowser, Cleaner, MIUI Package Installer and Themes) have been found to regularly download the manufacturer's updated configuration file MiAdBlacklistConfig from a server located in Singapore. This file contains a list composed of the titles, names and other information of various religious and political groups and social movements (at the time the analysis was performed, 449 records were identified in the MiAdBlacklistConfig file). Analysis of the Xiaomi application code showed that the applications have implemented software classes for filtering the target multimedia displayed on the device according to the downloaded MiAdBlacklistConfig list.

This allows a Xiaomi device to perform an analysis of the target multimedia content entering a phone: to search for keywords based on the MiAdBlacklist list received from the server. When it is determined that such content contains keywords from the list, the device blocks this content. It is thought that this functionality can pose potential threats to the free availability of information.

NCSC recommends that users take an interest in the software and hardware used, and responsibly evaluate the proposed functionality of the equipment.

---

11 Xiaomi. Privacy Policy. *https://privacy.mi.com/all/en_IN/*

12 Forbes information. *https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/*

13 Android Authority information. *https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/*

Details of the research

The main software characteristics of the mobile devices included in the analysis are listed in Table 1, indicating the operating system (OS) basis, the manufacturer's modification of the operating system basis, the version of the operating system kernel and the dates of security updates.

Table 1. Main software characteristics of mobile devices included in the analysis

Name of device	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
Factory-installed OS basis	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Manufacturer's modification of factory-installed OS basis	EMUI 10.1.0	MIUI Global 12.0.10 (QJDEUXM)	Oxygen OS 11.0.5.6.KB05BA
Latest available OS basis	Android 10	Android 11	Android 11
Manufacturer's modification of the latest available OS basis	EMUI 11.0.0.151 (C432E5R5P3)	MIUI Global 12.0.2.0 (RJSEUXM)	Oxygen OS 11.0.8.13.KB05AA
Latest available OS release date	2020-12-24	2021-05-25	2021-04-08
OS kernel version	4.14.116	4.19.81-pref-gef23740	4.19.110-pref+
Initial security update package level	2020-04-01	2020-09-01	2020-10-01
Date of most recent security update	2021-06-01[14]	2021-03-01[15]	2021-04-01[16]
Number of security updates	9	3	4

All mobile devices examined are based on the Android operating system; Huawei P40 and Xiaomi Mi 10T use system version 10, while OnePlus 8T uses what is currently the latest system version, 11. It is worth noting that by default the standard Android 11 operating system has wider access control capabilities,[17] enabling the user to better control the access of applications to data stored on the device.

Android operating system security updates are updates to the components of the operating system, designed to correct software vulnerabilities that threaten the security of the device or the data stored on it. These updates are focused on software vulnerabilities allowing remote code execution, elevation of privilege, information disclosure (information leakage), denial of service and other types of attacks. Each of these security updates fixes between 20 and 60 security vulnerabilities listed in the CVE database. It is worth noting that the harmfulness of vulnerabilities ranged between 5.4 and 10.0 points (out of a possible 10 points).

For this reason, it is important for mobile device users to install these updates regularly. These Android operating system security updates are released periodically, every 1-3 months. Xiaomi has committed to delivering these updates to its devices for 2 years[18], and OnePlus has made such a commitment for a period of 3 years[19]. Huawei's commitments to supply updates of the operating

[14] Huawei information. *https://consumer.huawei.com/en/support/bulletin/*

[15] Adimorah blog information. *https://adimorahblog.com/new-stable-update-for-the-mi-10t-and-mi-10t-pro/*

[16] OnePlus information. https://www.oneplus.com/global/support/softwareupgrade/details?code=PM1605596915581

[17] Android Authority information. C. Scott Brown, *The best Android 11 features you need to know https://www.androidauthority.com/android-11-features-1085228/*

[18] Xiaomi information. *https://www.mi.com/global/service/support/security-update.html*

[19] OnePlus information. *https://forums.oneplus.com/threads/oneplus-software-maintenance-schedule.862347/*

system or operating system security updates were not found. It is worth noting that the maker of the Android operating system, Google, releases security updates for unmodified versions of the Android Open Source Project. For this reason, operating system updates and operating system security updates are available earliest for devices manufactured by Google.

On the other hand, device manufacturers such as Huawei, Xiaomi, OnePlus and others have to adapt the operating system updates or operating system security updates to the manufacturer's modifications of the operating system basis, so such updates are only available later for these manufacturers' mobile devices. It is particularly important to emphasise that the latest security updates are available only for the Huawei P40 mobile device. The analysis found that the latest security update for the Xiaomi Mi 10T was 3 months old, and the latest security update for the OnePlus 8T mobile device was 2 months old.

The NCSC notes that, in accordance with the above information, timely security updates for existing devices are essential.

1. Huawei's official store AppGallery directs users to third-party e-shops in which the applications are malicious or virus-infected

The analysis showed that the process of installing mobile applications on Huawei devices is characterised by cybersecurity uncertainties. For the installation of mobile applications on Huawei phones, a manufacturer-based infrastructure is used, which consists of the official electronic application store AppGallery and peripheral application distribution platforms (APKMonk, APKPure, Aptoide, etc.). A diagram of the Huawei e-shop is shown in Figure 1.

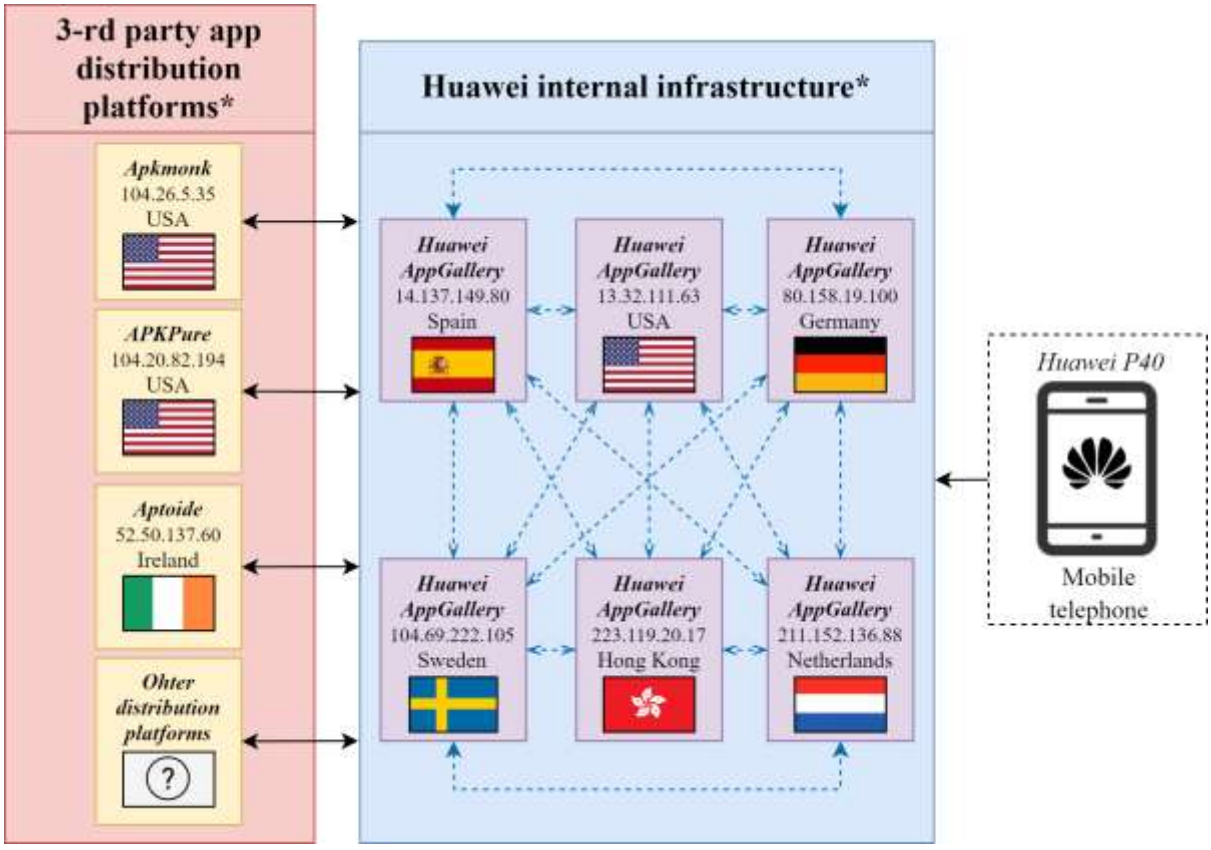

Figure 1: Diagram of Huawei's mobile-application e-shop

Huawei's mobile-application e-shop infrastructure consists of two blocks: the internal Huawei AppGallery infrastructure and third-party application distribution platforms. Its own Huawei AppGallery infrastructure has been determined to be located in Spain, the USA, Germany, Sweden, the Netherlands, Hong Kong and Thailand. This infrastructure is integrated with third-party distribution platforms, of which the three best-known operate in the USA, Ireland and the Netherlands. According to various sources[20], Huawei's mobile-application distribution infrastructure currently includes 6-8 third-party distribution platforms. Information about Huawei's mobile-application distribution infrastructure is presented in Table 2.

Table 2. Information about the Huawei mobile-application distribution infrastructure, indicating the parameters for the internal Huawei AppGallery and the three best-known integrated external distribution platforms

Line No.:	Infrastructure	Address:	IP address	State
1	Internal Huawei AppGallery	appdl-1-drcn.dbankcdn.com.c.cdnhwc1.com	223.119.20.17	Hong Kong
2		pay7.hicloud.com	14.137.149.80	Spain
3		appdl-11-dre.dbankcdn.com	13.32.111.63	the USA
4		appdl-11-drcn.dbankcdn.com	65.9.52.144	the USA
5		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	211.152.136.88	the Netherlands
6		uc3.hispace.hicloud.com	23.14.13.247	Sweden
7		sdkserver-dre.op.hicloud.com	104.69.222.105	Sweden
8		HWID-dre.platform.hicloud.com	104.69.222.145	Sweden
9		appdl-12-drcn.dbankcdn.com.akamaised.net	184.31.15.17	Sweden
10		appdl-12-dre.dbankcdn.com.akamaised.net	184.31.15.51	Sweden
11		appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	119.46.76.15	Thailand
12		appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	119.46.76.17	Thailand
13		appstore.huawei.com	80.158.2.135	Germany
14		metrics2.data.hicloud.com	80.158.2.190	Germany
15		www.hicloud.com	80.158.19.100	Germany
16		query.hicloud.com	80.158.19.121	Germany
17		grs.dbankcloud.com	80.158.20.103	Germany
18		Jos.hicloud.com	80.158.23.247	Germany
19		iap.hicloud.com	80.158.40.92	Germany
20		appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	101.33.11.29	Germany
21		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	101.33.11.45	Germany
22		appdl-4-drcn.dbankcdn.com	163.171.128.127	Germany
23		appdl-4-drcn.dbankcdn.com	163.171.128.129	Germany
24	External platform APKMonk	www.apkmonk.com	104.26.4.35	the USA
25	External platform APKPure	download.apkpure.com	104.20.83.194	the USA
26	External platform Aptoide	en.aptoide.com	34.249.219.183	Ireland
27		ws75.aptoide.com	34.254.115.204	Ireland
28		ws75.aptoide.com	52.17.222.230	Ireland
29		en.aptoide.com	52.50.137.60	Ireland
30		rakam-api.aptoide.com	52.209.136.146	Ireland
31		pnp.aptoide.com	54.194.247.193	Ireland
32		en.aptoide.com	54.220.86.7	Ireland
33		ws75.aptoide.com	54.229.235.132	Ireland
34		CDN-mobile.aptoide.com	172.67.29.206	the USA
35		pool.apk.aptoide.com	5.79.110.134	the Netherlands
36		apkins.aptoide.com	95.211.168.137	the Netherlands
37		apkins.aptoide.com	95.211.223.52	the Netherlands

[20] XDA-Developers information. *https://www.xda-developers.com/petal-search-download-apps-huawei-honor-smartphones-hms/*

When the user installs a mobile application on a Huawei device, a search for the mobile application is performed in the AppGallery store; when the application is found, it is downloaded and installed on the mobile device. The mobile-application installation scheme using the Huawei AppGallery platform is presented in Figure 2.

When the name of an application is entered in the search box of the Huawei AppGallery application, a list of search results is generated. The search results window contains the Petal Search section. When the Petal Search is selected, the user is shown a list of applications accessible through third-party application distribution platforms (1). When a user selects an application from this section, a warning message (2) is displayed. The warning message indicates that further actions will occur outside the Huawei AppGallery application.

When the user closes the warning window, the web browser is opened on the device, the user is redirected to the third-party application distribution platform. If the user selects the application-installation file download option (3) on the platform, the file is downloaded and saved in the device's internal memory (4, 5). Once the device completes the process of downloading the application-installation file, the installation of the application starts.

Since in this case the installation of the application is initiated by the web browser of the device, the user is shown an information window (6) requesting authorisation to initiate the application installation procedure using the web browser. Once the user has given permission, an application-installation window (7) is shown, which again requests user input to start the installation. Once the user has reconfirmed the application-installation, the application is installed (8, 9) and an icon for the newly-installed application is added to the main window (10).

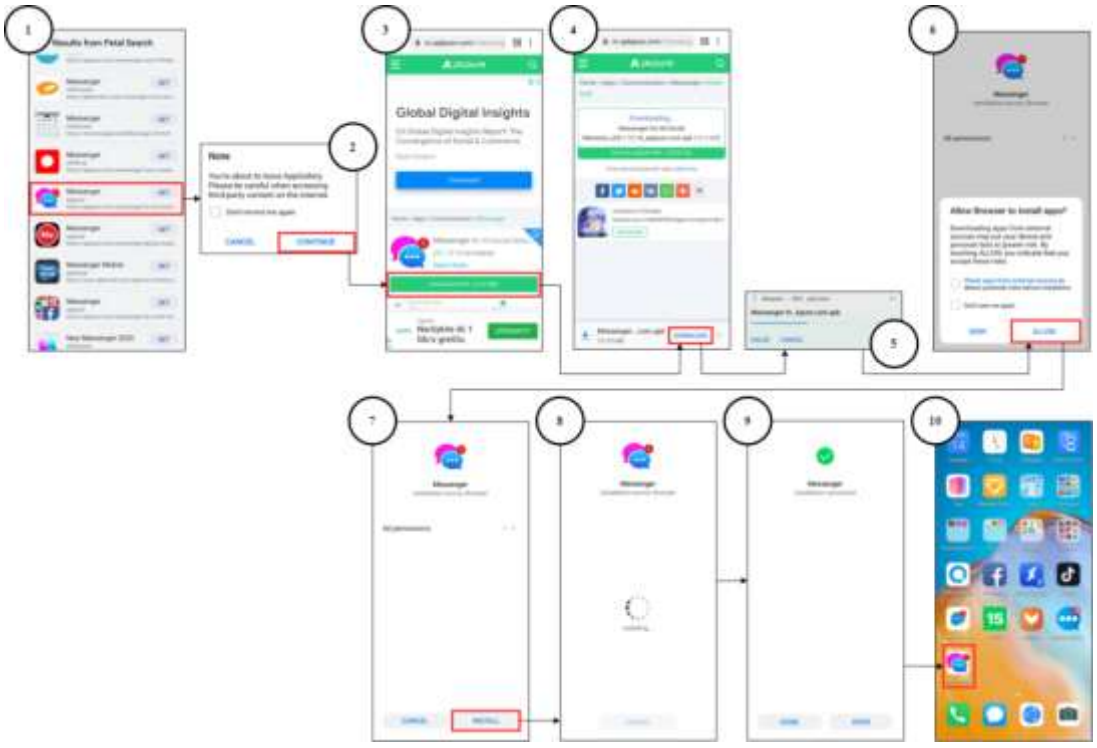

Figure 2: Mobile application installation scheme using the Huawei AppGallery platform

If the application being searched for is not available in the Huawei AppGallery store, the user is

automatically redirected to peripheral third-party application distribution platforms, from which the mobile application is downloaded to the phone for installation.

The analysis found that a portion of the mobile applications available at such distribution platforms are fakes of the authentic applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on a mobile phone, thereby jeopardising the security of the device and the data contained in it.

A schematic diagram of the installation of a Huawei application, including third-party distribution platforms for their installation, is shown in Figure 3.

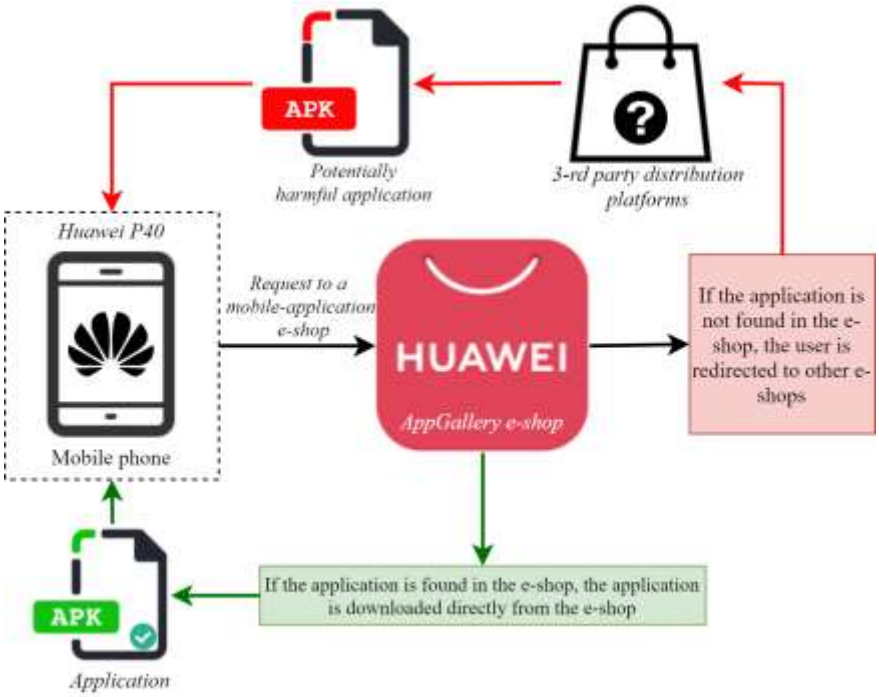

Figure 3: Schematic diagram for the installation of a Huawei application, including third-party distribution platforms

It is worth noting that part of the application-distribution infrastructure used by Huawei is located in countries not covered by the General Data Protection Regulation. It is important to note that a mobile device downloading an application from a mobile-application e-shop located in a country covered by the GDPR can execute requests to third countries not covered by the Regulation. This creates a corresponding risk of leakage of user metadata.

The analysis examined the AppGallery e-shop operating in the Huawei infrastructure and three of the best-known integrated third-party distribution platforms, APKMonk, Aptoide and APKPure. It is worth noting that information on APKMonk and APKPure developers could not be found in freely-available sources. According to Aptoide[21], the headquarters of the distribution platform is registered in Portugal (Lisbon), and the company's branches operate in China (Shenzhen) and Singapore.

The analysis monitored traffic as applications were downloaded from sources used in the Huawei infrastructure. During the research, applications were searched for in the Huawei AppGallery e-shop, without changing the sequence for download of applications as originally set by the manufacturers; the applications were downloaded directly from the original e-shop and from the third-party application distribution platforms provided by AppGallery.

When recording the number of connections, it was found that during the downloading of an application from the original AppGallery e-shop, requests to 38 addresses were identified, and in the

[21] Aptoide information. *https://en.aptoide.com/company/about-us*

case of APKMonk, 56 addresses. The highest number of requests was identified for Aptoide and APKPure; respectively, 74 and 73 addresses.

Information illustrating Huawei mobile device requests during application download procedures is shown in Figure 4.

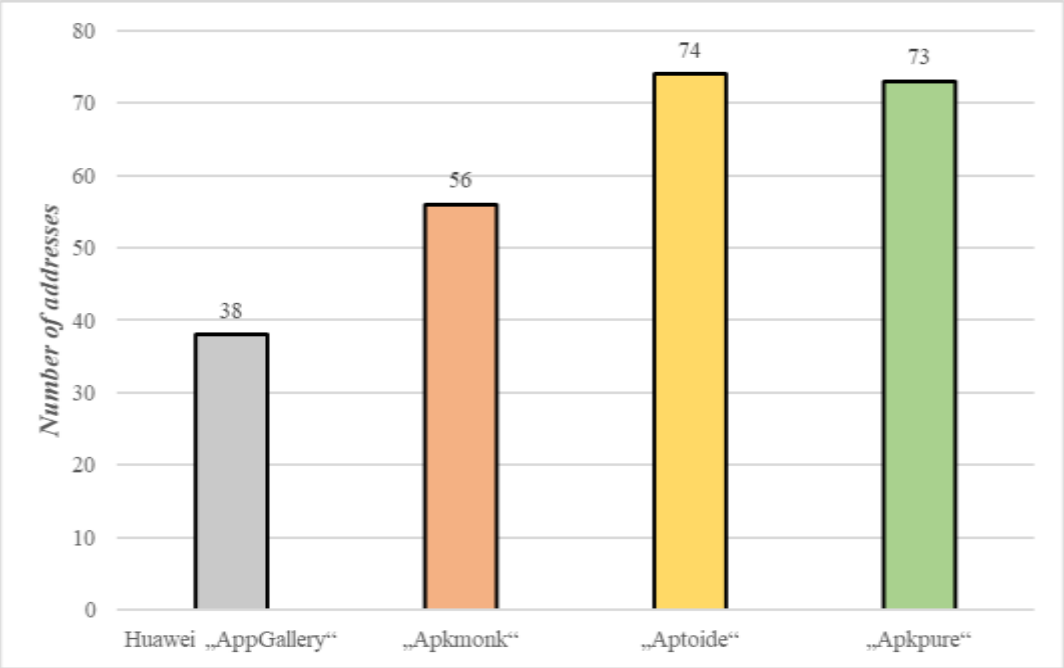

Figure 4: Number of Huawei mobile device requests during application download procedures

More detailed information on the countries to which the requests were directed and the number of such requests is given in Figures 5 through 7.

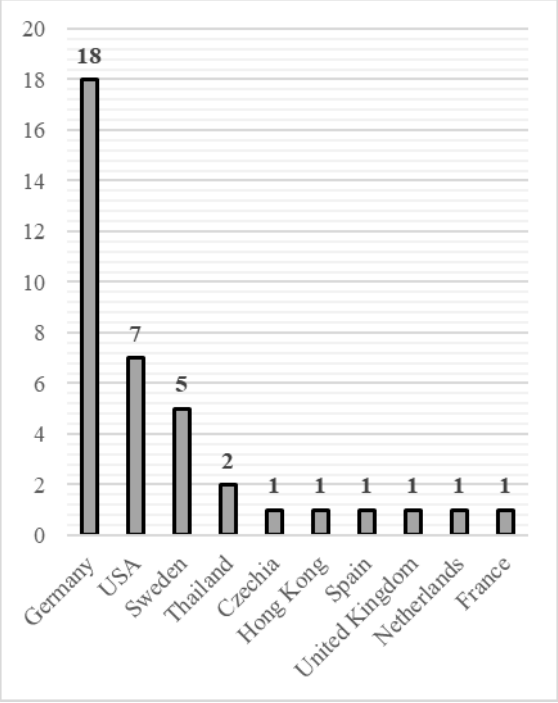

Figure 5: Huawei AppGallery request information

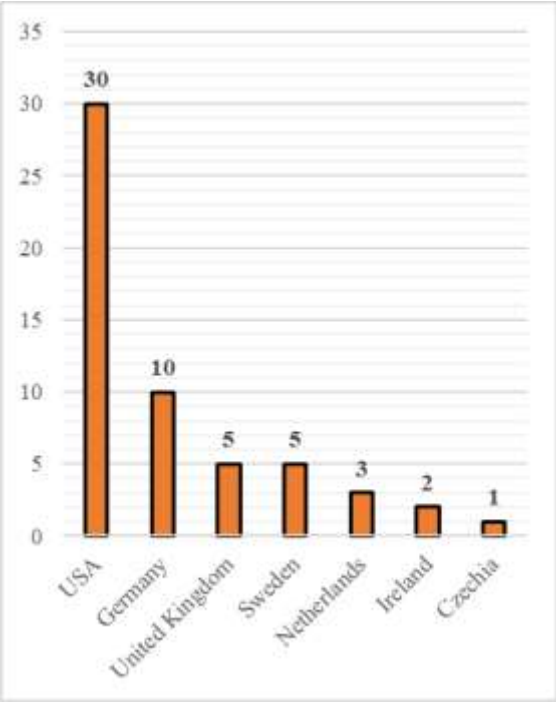

Figure 6: Distribution platform APKMonk request information

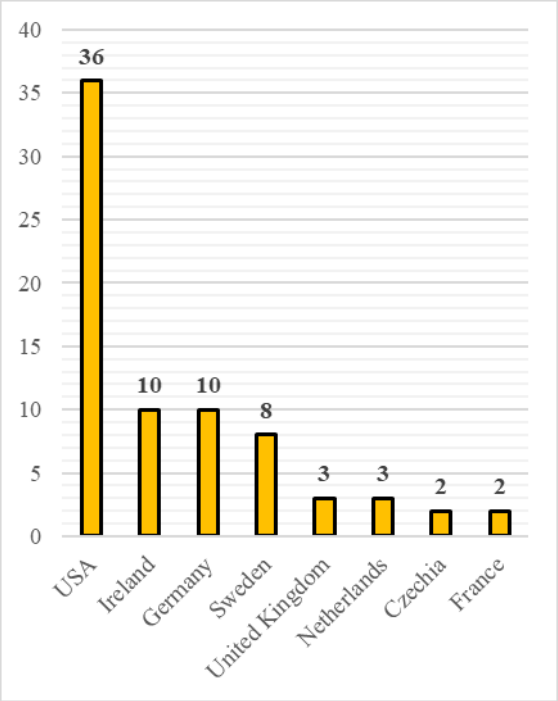

Figure 7: Distribution platform Aptoide request information

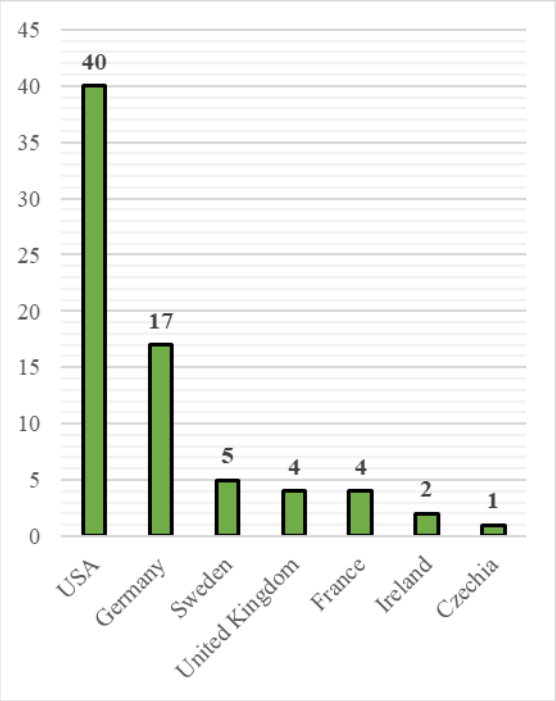

Figure 8: Distribution platform APKPure request information

More detailed analytical information with specific IP addresses and countries is provided in Table 3.

Table 3. More detailed analytical information with specific IP addresses and countries

Line No.:	Huawei AppGallery		APKMonk		Aptoide		APKPure	
	Address	State	Address	State	Address	State	Address	State
1	apkrep.ns1.ff.avast.com	Czechia	34.250.145.50	Ireland	i.w.inmobi.com	Ireland	apkrep.ns1.ff.avast.com	Czechia
2	appdl-1-drcn.dbankcdn.com.c.cdnhwc1.com	Hong Kong	52.209.136.146	Ireland	en.aptoide.com	Ireland	sync.crwdcntrl.net	Ireland
3	pay7.hicloud.com	Spain	5.62.53.15	Czechia	ws75.aptoide.com	Ireland	52.209.246.140	Ireland
4	8.8.8.8	the USA	appimg3.dbankcdn.com	the USA	ws75.aptoide.com	Ireland	13.32.111.63	the USA
5	appdl-11-dre.dbankcdn.com	the USA	13.33.242.107	the USA	webservices.aptwords.net	Ireland	feeds.apyhi.com	the USA
6	13.33.242.98	the USA	auction.unityads.unity3d.com	the USA	en.aptoide.com	Ireland	34.98.67.61	the USA
7	13.107.213.44	the USA	odr.mookie1.com	the USA	rakam-api.aptoide.com	Ireland	34.236.65.196	the USA
8	52.177.138.113	the USA	auction.unityads.unity3d.com	the USA	pnp.aptoide.com	Ireland	rtb.openx.net	the USA
9	appdl-11-drcn.dbankcdn.com	the USA	auction.unityads.unity3d.com	the USA	en.aptoide.com	Ireland	35.244.159.8	the USA
10	152.199.21.230	the USA	EU-u.openx.net	the USA	ws75.aptoide.com	Ireland	35.244.174.68	the USA
11	5.62.36.56	the UK	id.rlcdn.com	the USA	apkrep.ns1.ff.avast.com	Czechia	65.9.52.144	the USA
12	appdl-2-drcn.dbankcd	the Netherlands	52.85.48.221	the USA	5.62.53.117	Czechia	download.apkpure.com	the USA

	n.com.cdn.dnsv1.com							
13	www.petalsearch.com	France	52.154.69.245	the USA	wv.inner-active.mobi	the USA	104.26.4.35	the USA
14	uc3.hispace.hicloud.com	Sweden	65.9.53.128	the USA	wv.inner-active.mobi	the USA	partner.googleadservices.com	the USA
15	sdkserver-dre.op.hicloud.com	Sweden	104.21.35.78	the USA	8.8.8.8	the USA	pagead2.googlesyndication.com	the USA
16	HWID-dre.platform.hicloud.com	Sweden	www.apkmonk.com	the USA	test.quantcast.mgr.consensu.org	the USA	142.250.74.100	the USA
17	appdl-12-drcn.dbankcdn.com.akamaised.net	Sweden	104.197.172.31	the USA	quantcast.mgr.consensu.org	the USA	s0.2mdn.net	the USA
18	appdl-12-dre.dbankcdn.com.akamaised.net	Sweden	partner.googleadservices.com	the USA	auction.unityads.unity3d.com	the USA	firebaseremoteconfig.googleapis.com	the USA
19	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Thailand	142.250.74.35	the USA	Publisher-config.unityads.unity3d.com	the USA	app-measurement.com	the USA
20	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Thailand	adservice.google.com	the USA	www.datadoghq-browser-agent.com	the USA	adservice.google.com	the USA
21	appstore.huawei.com	Germany	142.250.74.100	the USA	sdktm.w.inmobi.com	the USA	Firebase-settings.crashlytics.com	the USA
22	80.158.2.189	Germany	142.250.74.102	the USA	rules.quantcount.com	the USA	142.250.74.136	the USA
23	metrics2.data.hicloud.com	Germany	142.250.74.129	the USA	104.21.35.78	the USA	142.250.74.142	the USA
24	80.158.16.161	Germany	142.250.74.130	the USA	config.inmobi.com	the USA	Sync-tm.everesttech.net	the USA
25	www.hicloud.com	Germany	um.simpli.fi	the USA	142.250.74.2	the USA	152.199.21.230	the USA
26	query.hicloud.com	Germany	172.67.29.206	the USA	www.googletagmanager.com	the USA	172.67.68.182	the USA
27	grs.dbankcloud.com	Germany	tpc.googlesyndication.com	the USA	partner.googleadservices.com	the USA	172.217.20.33	the USA
28	80.158.20.104	Germany	googleads4.g.doubleclick.net	the USA	connectivitycheck.gstatic.com	the USA	googleads.g.doubleclick.net	the USA
29	Jos.hicloud.com	Germany	www.gstatic.com	the USA	firebaseinstallations.googleapis.com	the USA	172.217.20.35	the USA
30	iap.hicloud.com	Germany	172.217.21.161	the USA	cdn.ampproject.org	the USA	tpc.googlesyndication.com	the USA
31	80.158.54.98	Germany	ade.googlesyndication.com	the USA	adservice.google.com	the USA	172.217.21.130	the USA
32	appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	Germany	cm.g.doubleclick.net	the USA	www.google.com	the USA	www.gstatic.com	the USA
33	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	Germany	192.48.236.3	the USA	pagead-googlehosted.l.google.com	the USA	ade.googlesyndication.com	the USA
34	160.44.194.86	Germany	Pixel-sync.sitescout.com	the UK	142.250.74.130	the USA	www.google.com	the USA
35	160.44.199.4	Germany	openx2-match.dotomi.com	the UK	Firebase-settings.crashlytics.com	the USA	172.217.21.166	the USA
36	160.44.207.213	Germany	91.228.74.189	the UK	softonic.map.fastly.net	the USA	172.217.21.170	the USA
37	appdl-4-drcn.dbankcdn.com	Germany	image6.pubmatic.com	the UK	api.facebook.com	the USA	172.217.22.162	the USA

38	appdl-4-drcn.dbankcdn.com	Germany	188.125.94.206	the UK	connect.facebook.net	the USA	raw.githubusercontent.com	the USA
39			81.171.20.104	the Netherlands	www.facebook.com	the USA	216.58.207.206	the USA
40			95.211.137.160	the Netherlands	CDN-mobile.aptoide.com	the USA	www.gstatic.com	the USA
41			ib.adnxs.com	the Netherlands	tpc.googlesyndication.com	the USA	firebaseinstallations.googleapis.com	the USA
42			store3.hispace.hicloud.com	Sweden	fonts.gstatic.com	the USA	cm.g.doubleclick.net	the USA
43			104.73.93.58	Sweden	pagead-googlehosted.l.google.com	the USA	216.58.211.130	the USA
44			tls.adobe.com	Sweden	adservice.google.com	the USA	ad.turn.com	the UK
45			sdkserver-dre.op.hicloud.com	Sweden	fonts.googleapis.com	the USA	185.29.135.233	the UK
46			sdkserver-dre.op.hicloud.com.edgekey.net	Sweden	ads.mopub.com	the USA	185.64.190.78	the UK
47			j.mrpdata.net	Germany	ads.mopub.com	the USA	212.82.100.176	the UK
48			23.193.116.193	Germany	app-measurement.com	the USA	51.75.146.159	France
49			metrics2.data.hicloud.com	Germany	pixel.quantserve.com	the UK	pixel.onaudience.com	France
50			platform.hicloud.com	Germany	185.64.190.78	the UK	D-08.winudf.com	France
51			grs.dbankcloud.com	Germany	data.flurry.com	the UK	green.erne.co	France
52			appgallery.cloud.huawei.com	Germany	pool.apk.aptoide.com	the Netherlands	dsum-sec.casalemedia.com	Sweden
53			JFS-dre.jos.hicloud.com	Germany	apkins.aptoide.com	the Netherlands	store3.hispace.hicloud.com	Sweden
54			80.158.34.57	Germany	apkins.aptoide.com	the Netherlands	sdkserver-dre.op.hicloud.com.edgekey.net	Sweden
55			160.44.199.4	Germany	id5-sync.com	France	HWID-dre.platform.hicloud.com	Sweden
56			160.44.202.175	Germany	51.255.81.18	France	sdkserver-dre.op.hicloud.com	Sweden
57					2.18.33.213	Sweden	3.66.135.160	Germany
58					z.moatads.com	Sweden	tracking.justpremium.com	Germany
59					store3.hispace.hicloud.com	Sweden	49.51.130.46	Germany
60					d.applovin.com	Sweden	pixel.rubiconproject.net.akadns.net	Germany
61					sdkserver-dre.op.hicloud.com	Sweden	80.158.2.189	Germany
62					sdkserver-dre.op.hicloud.com.edgekey.net	Sweden	metrics2.data.hicloud.com	Germany
63					cdn2.inner-active.mobi	Sweden	OAuth-login-dre.platform.dbankcloud.com	Germany
64					webview.unityads.unity3d.com	Sweden	80.158.19.69	Germany
65					api.vungle.com	Germany	80.158.19.100	Germany

66			ads.api.vungle.com	Germany	80.158.19.121	Germany
67			metrics2.data.hicloud.com	Germany	80.158.20.104	Germany
68			OAuth-login-dre.platform.dbankcloud.com	Germany	JFS-dre.jos.hicloud.com	Germany
69			JFS-dre.jos.hicloud.com	Germany	80.158.34.57	Germany
70			cloud.hicloud.com	Germany	grs.dbankcloud.com	Germany
71			80.158.40.21	Germany	80.158.44.234	Germany
72			appdlssl.hicloud.com	Germany	101.33.11.48	Germany
73			160.44.199.4	Germany	160.44.199.4	Germany
74			connectivitycheck.platform.hicloud.com	Germany		

The analysis found that when downloading an application from the Huawei infrastructure, a redirection to third-party application distribution platforms was carried out, from which applications with potentially malicious code were downloaded. A summary of the security analysis of mobile applications downloaded by a Huawei device from the Huawei infrastructure is presented in Table 4. The security analysis was performed with the well-known file analysis tool VirusTotal[22].

Table 4. Summary of downloaded mobile applications after inspection using VirusTotal

Line No.:	Application name	Identifier	Application version	VirusTotal result
1	Social Media	com.social.messenger.allinoneapps	14	*Malicious software:* A.gray.andrsca.f
2	Web Machinist Mobile Pro Tapping	com.webmachinist.cncmachinisttappingcalculator	1.0	*Virus:* Trojan.Trojan.Banker.AndroidOS.Agent.ed
3	Messenger All in One	comm.essagechat.listing	28.0	*Malicious software:* Adware/Loead for Android.fyben.a

The research analysed three mobile applications downloaded from Huawei mobile application distribution infrastructure servers. According to VirusTotal scanning data, it was determined by one antivirus system that potentially malicious software, A.gray.andrsca.f, was installed in the Social Media application. After examining another mobile application, Web Machinist Mobile Pro Tapping, downloaded from Huawei infrastructure servers, one VirusTotal antivirus system identified a potential virus, Trojan.Trojan.Banker.AndroidOS.Agent.ed. This virus can carry out[23] theft of data for connection to banking systems. In the third application that was analysed, Messenger All in One, two antivirus systems found that the application uses potentially malicious software, the packages Adware/Loead and Android.fyben.a.

This raises serious concerns about the security of the device, as not all third-party application distribution platforms perform verification of uploaded applications.

This infrastructure security vulnerability can be exploited by obtaining original (authentic) applications from the Google Play Store, decompiling the application and then applying the necessary modifications to the content of the decompiled application by adding malicious code. The application code with malicious content is then recompiled, packaged and signed with a new private key. The modified application is uploaded to the above-mentioned third-party application distribution

[22] VirusTotal information. *https://www.virustotal.com/gui/*

[23] Clavister information. *https://www.clavister.com/advisories/antivirus/view/?id=544073*

platforms. An associative diagram of this process[24] is given in Figure 9.

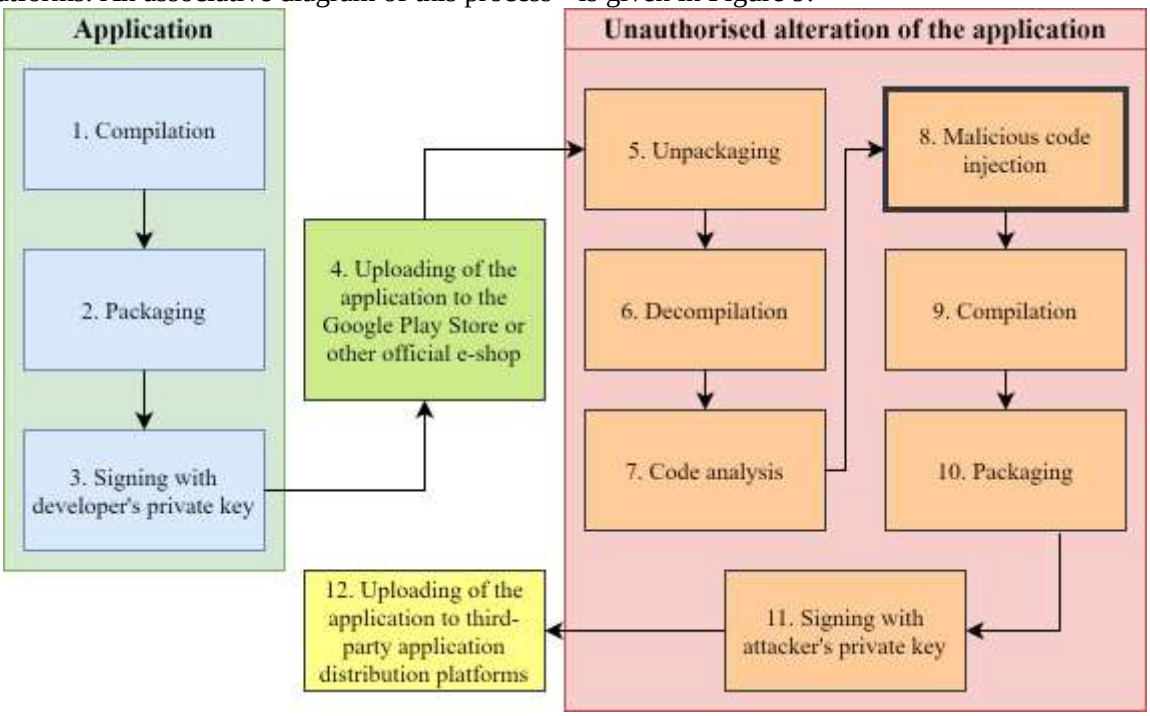

Figure 9: Associative diagram of malicious code insertion into a mobile application

An application developer compiles the code during application development and thus forms a functioning application. This application is packaged in the installation file and signed with the application developer's private key. The signed installation file for the application can be uploaded to application stores such as Google Play Store.

An attacker, like all users of application stores (except for relevant regional restrictions) can download this application; once received from official sources, it is unpacked and decompiled into the application code. This allows an attacker to perform analysis of the application, to determine the viability of the installation site of the malicious code and the installation technology to be used, and to insert malicious code into the application. After completion of malicious code insertion procedures, the application code is recompiled and packaged into an installation file, which is signed with the attacker's private key. The generated malicious application installation file is uploaded to third-party application distribution platforms, where not all uploaded applications are checked.

Virus-containing e-shops have been found to be a serious problem for these stores[25]. A user who installs a virus-infected application may suffer from the collection or leaking of data stored in the device or an associated cloud service, or from damage to the mobile device.

The analysis found that a portion of the mobile applications available in the application distribution platforms are fakes of original (authentic) applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on a mobile phone, thereby jeopardising the security of the device and the data contained in it.

[24] Springer info. Repackaging Attack on Android Banking Applications and Its Countermeasures. *https://link.springer.com/article/10.1007/s11277-013-1258-x*

[25] P. Kotzias et al. How Did That Get In My Phone? Unwanted App Distribution on Android Devices. *https://arxiv.org/pdf/2010.10088.pdf*

2. Devices designed and manufactured in China access servers in third countries. This allows for the collection and aggregation of user metadata, and based on such data to monitor users

Analysis of decompiled software and data flows showed that Mi Browser uses two data collection modules: Google Analytics and Sensors Data. Sensors Data is a platform of Chinese origin, in functionality close to Google Analytics. According to the Sensors Data company,[26] it has more than 1,500 customers, including some of the largest corporations in the People's Republic of China, such as China Telecom, Baidu, CYTS, Sichuan Airlines, etc.

Google Analytics is an analytics platform for programmers or administrators to access information allowing them to evaluate the use of applications in the iOS, Android or web environments[27]. Google Analytics automatically generates an event log allowing evaluation of the performance of an application. It is worth noting that developers have the technical ability to select the parameters to be analysed, and to set the depth of the analysis of such parameters.

It was found that this module can collect data about user browsing, clicks, etc., and send information for possible analysis to Google servers. It should be noted that these modules are activated at the time of initial switching-on of the device, upon consent to participate in the Xiaomi User Experience programme.

Having decompiled the Xiaomi device's factory-installed system applications, it was found that the functionality of these analytics applications was installed and operated in the standard internet browser of the Xiaomi phone, Mi Browser. Table 5 shows a fragment of Mi Browser code, denoting the Google Analytics functionality.

Table 5. Fragment of Mi Browser code, denoting the Google Analytics functionality

```
public static void reportAsync(String str, Map<String, Object> map) {
 if if (!TextUtils.isEmpty(str) &AMP;& !BrowserSettings.getInstance.isNotAllowCollectData) {
BrowserReportUtils.stripUrlIfNecessary(map);
BackgroundThread.postOnIOThread(new Runnable(str, map)
 {public final/* synthetic */ String f$0;
 public final /* synthetic */ Map f$1;
 {
 this.f$0 = r1;
 this.f$1 = r2;
 }
 Public final void run {
 FirebaseReportHelper.report(this.f$0, this.f$1);
 }
});
 }
}
```

In the code fragment displayed in the table, the function for sending data to the Firebase analytics platform on Google servers is implemented. Table 6 shows a fragment of Sensors Data code installed in the Mi Browser application. In the code fragment, the function that launches Sensors Data functionality in the Mi Browser application is presented.

Table 6. Fragment of Sensors Data startup code in the Mi Browser application

[26] Sensors Data information. *https://www.sensorsdata.cn/about/aboutus-en.html*
[27] Google Firebase information. *https://firebase.google.com/docs/analytics/get-started*

```
public static void initSensorsDataAPI(final Context context) {
 if (context!= null) {
 Context applicationContext = context.getApplicationContext;
 TRY {
 SensorsDataAPI.startWithConfigOptions(applicationContext, new
SAConfigOptions(SA_SERVER_URL).setAutoTrackEventType(3).enableLog(permissionUtil.isBuildDebu
g(applicationContext).enableTrackScreenOrientation(false));
 SensorsDataAPI.sharedInstance.identify(AnonymousID.get application(Context));
 setFlushNetworkPolicy(PrivacyAgreement.getInstance.isApproved);
 SensorsDataAPI.sharedInstance.setSessionIntervalTime(10000);
 registerSuperProperties(applicationContext);
 SensorsDataAPI.sharedInstance.unregisterSuperProperty(C4683v.f6510ae);
 SensorsDataAPI.sharedInstance.unregisterSuperProperty(uuid);
 logout;
 SensorsDataAPI.sharedInstance.enableEncrypt(true);
 SensorsDataAPI.sharedInstance.persistentSecretKey(new SensorsDataEncrypt. PersistentSecretKey{
 public void saveSecretKey.SecreteKeysecreteKey {} public

 SensorsDataEncrypt.SecreteKeyloadSecretKey { return
 new SensorsDataEncrypt.SecreteKeycontext.getString(R.string.ABCDEF), 1);
 }
});
 } catch (Exception unused) {
}
}
}
```

The Sensors Data module used in the device has been found to collect statistical information about 61 parameters of the operation of applications used (time of activation of the application, language used, etc.). A list of data collected by Sensors Data is given in Table 7.

Table 7. List of 61 parameters collected by Sensors Data

No.:	Parameter	Commentary
1	log_miaccount	Is the user logged in
2	Autocomplete_switch	Is automatic text completion enabled
3	No_track_switch	Is the Do Not Track function enabled
4	bookmark_sync	Whether bookmark synchronisation with the cloud is enabled
5	history_sync	Whether synchronisation of browsing history with the cloud is enabled
6	feature_report_switch	Is the user participating in the Xiaomi User Experience programme
7	clear_history_switch	Whether history is deleted when the application is closed
8	personal_service_switch	Whether programme recommendations are enabled
9	enhanced_incognito_switch	Whether the browser is running in Enhanced Incognito mode
10	system_out_of_ads	Whether the Limit Ad Tracking function is activated. Using this feature, advertisers do not have access to the device identifier

11	swipe_up	What function is registered for the swipe-up motion
12	current_default_search_engine	Current search engine used
13	language	Language set in the system
14	language_browser	Language setting in the browser
15	icon_reddot_status	—
16	user_newsfeed	Is the news stream disabled
17	user_download_videos	—
18	user_night_mode	Whether the browser uses night mode
19	dark_mode	Whether the system uses night mode
20	user_data_save_mode	Whether data-saving functionality is activated in the browser
21	user_incognito_mode	Is Incognito Mode enabled
22	user_desktop_mode	Browser's user-agent
23	user_checkbox_4G	Is browser updating via 4G allowed
24	user_push_agree	Whether browser notifications are activated
25	user_facebook_notification	Whether Facebook messages have been activated in the browser
26	user_youtube_signin	Whether the user is logged in to YouTube
27	user_click_interest	Shows how many times the user clicked on cards in the browser (news, YouTube recommendations, etc.)
28	user_login	Whether the user is logged in to Mi Account
29	adblock_switch	Is the ad-blocking function activated
30	adblock_show_notification	Is Adblock enabled
31	first_enter_newsfeed_way	Is the news stream window enabled for the first time
32	Fandst_appstart_source	—
33	first_appstart_third_party	—
34	Miu_personalised	Whether personalised advertising is activated
35	personalised_services	Whether personalised content recommendations have been activated
36	browser_ads	—
37	protection_type	—
38	app_boot_third_party	—
39	app_boot	Start-up time of the programme
40	feed_default_channel	—
41	experience_improve	Is Xiaomi User Experience activated
42	platform	Platform. Always Android
43	Miu_version	MIUI version
44	log_miaccount	Whether the user is logged in to the Mi account
45	MUI_region	Mi region
46	EID	—
47	apk_name	Application APK name
48	browser_install_referrer	—
49	Autocomplete_switch	Is AutoComplete in the search window activated
50	No_track_switch	Is the Do Not Track function enabled
51	bookmark_sync	Is synchronisation of bookmarks with the Mi server activated
52	history_sync	Is synchronisation of browsing history with the Mi server activated

53	feature_report_switch	Whether the user participates in the Xiaomi User Experience programme
54	clear_history_switch	Whether browsing history is deleted when the application is closed
55	personal_service_switch	Whether the functionality of user recommendations is enabled: personalised YouTube clips, etc.
56	enhanced_incognito_switch	Is Incognito enabled
57	user_tab_news	Has the user enabled the news tab
58	user_tab_games	Has the user enabled the games tab
59	search_optimization_switch	Constant, always equal to 1
60	cookie_status	Provides data about user cookie settings
61	subscription	Indicates whether a VPN is used and, if so, its identifier

During the analysis, full decoding and decryption of Xiaomi encrypted messages was carried out. Xiaomi's phone has been found to send Sensors Data data in a Base64 dataset, which is additionally encoded using the *urlencode* algorithm. An example of a fragment of encoded data sent is given in Table 8.

Table 8. Fragment of data sent by a Xiaomi phone

zzvhrYfjw6d%2FA8RXtmQLWd2RTDyUWp5DBsFc55eI9yBbDROnrH12GSpq8SRDUtyJ8PquOrUqpsID
g6qvSg%2FksVvDG3gcl6SWzk9uL4hWhOCpEw%2B%2BzMBq0KCtqdOkn4kljhDgt
CfdRixfrJe8PHTjr8x1cK5xMHHlSL0MK%2FWu3utqKnuhf1UQGi64uYDCp%2FeEZ1MdakDE%2BLXsF
4wZKGiftO64 %2B8liP1NvxVl%2BsgTutVEbroI%2FWJUJkz9MfZyvL6OAPG6z9rRbJ354mUo6
%2BOMwZdN%2BAuWSzRz8IKITU6HwNZGMB0xmPDB8tSTM7ehnya%2FyAiHPqOIXD7lYzrvupBJT
rZLCXLQzbTgIxtZG65KvV7yfgiwMhCxY%2Bkg0t3d0LXljOOrQqFfsqdJW%2B6LnWvE6lKdm7
%2BCPydhautVIgiMSZDi94iH%2FuYL%2B2dkmLxSjQFQh51FSBA%2BygRzfCItmL87KjjgT0t3
%2BmtvO%2Bs93lH72rC6ai0Y5kdIIdSuIg6A%2BomC73JYOeHygMR0jmjCjM5 %2FiUANqsH
XPfeoaGBn8F%2FV1vik03CPbetK3yzfwLn9ZpmkmzO64Ic%2BEsRNTgNk7jc0mKZrsisWs4IPO1e

Table 9 shows the decrypted content of data sent by Xiaomi's phone to Sensors Data servers located in Singapore. Data sent for analysis: application version, application name, current region, device manufacturer, etc.

Table 9. Content sent by a Xiaomi phone to Sensors Data servers in Singapore

{
"_track_id": 1687170607,
for Time: 1623852507838,
for 'type': track,
for 'distinct_id': '7d03ab71-91b1-47ca-8f56-0ce2d77f6c86',
for Lib: {
For $Lib: Android,
For $lib_version: "4.0.3-pre",
For $app_version: '12.4.1-g',
For $lib_method: 'code',
"$lib_detail": "com.android.browser.BrowserActivity#####"
},
for Event: "$AppStart",
for Properties: {
For $Lib: Android,
"$os_version": '10',

For $lib_version: “4.0.3-pre”,
For $Model: ‘M2007J3SY’,
‘$s’: Android,
“$screen_width”: 1080,
For $screen_height: 2400,
For $Manufacturer: ‘Xiaomi’,
For $app_version: ‘12.4.1-g’,
for Platform: AndroidApp,
for ‘miui_version’: ‘V12.0.18.0.QJDEUXM’,
“log_miaccount”: 0,
‘miui_region’: “LT”,
for EID: “channel_en_youtube-web”,
“apk_name”: “com.mi.globalbrowser”,
“browser_install_referrer”: Google-play,
“autocomplete_switch”: 1,
“no_track_switch”: ‘2’,
bookmark_sync: 1,
for ‘history_sync’: 1,
‘feature_report_switch’: 1,
“clear_data_switch”: 0,
“personal_service_switch”: 1,
“enhanced_incognito_switch”: 0,
‘hashtag_follow_count’: 0,
‘hashtag_follow_list’: “”,
“account_follow_count”: 0,
“account_follow_list”: “”,
“feed_default_channel”: “”,
For $WiFi: True,
For $network_type: WIFI,
“$resume_from_background”: True,
“$is_first_time”: false,
“$screen_name”: “com.android.browser.BrowserActivity”,
For $title: ‘Mi Browser’,
“$is_first_day”: True
}
}

Sensors Data data was found to be sent to the address *https://sa.api.intl.miui.com*. Table 10 provides information that characterises the analytical data transmitted over the network to servers located in Singapore.

Table 10. Characteristics of data sent by Sensors Data

Line No.:	IP address	Data sent, *B*	Data received, *B*	Total data, *B*	State
1	47.241.109.186	11789	0	11789	Singapore
2	161.117.9.4	4318		4318	
3	161.117.84.89	13386		13386	
4	161.117.189.14	1230		1230	
5	161.117.230.146	5294		5294	

The collected statistics are sent through an encrypted channel to Xiaomi servers in Singapore, which is a country not covered by the General Data Protection Regulation. Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

Figure 10 shows the Sensors Data data encryption mechanism that was recreated during the

analysis, used to establish the data link between the device and the servers located in Singapore.

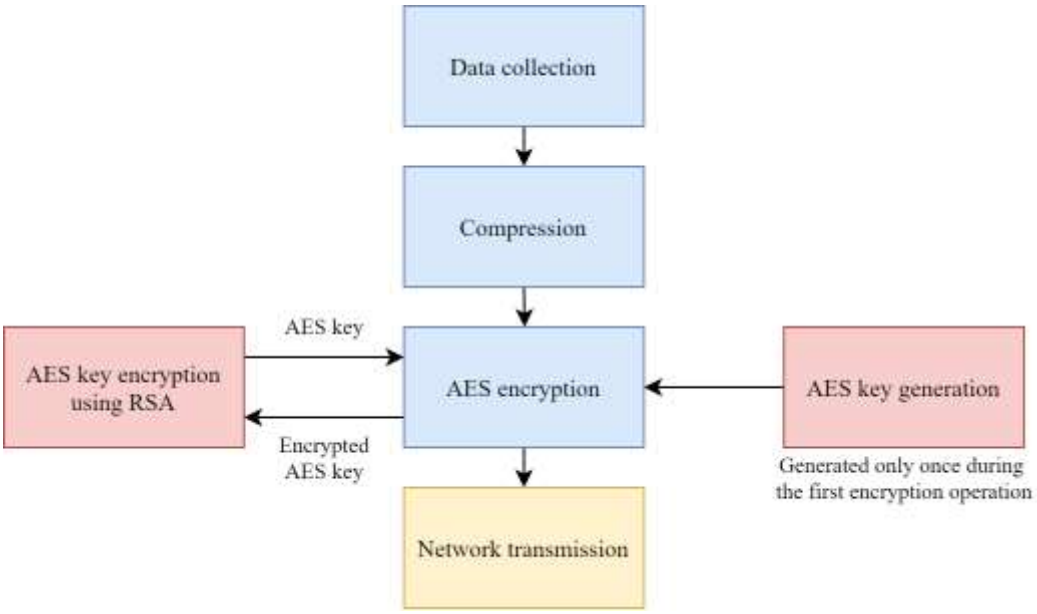

Figure 10: Data encryption mechanism used by Xiaomi

The encrypted dataset is generated by calling Sensors Data software installed in the Mi Browser: *registerSuperProperties* and *registerDynamicSuperProperties*. These functions are responsible for data collection and preparation of the JSON object. When the dataset is to be sent, it is first converted into a byte expression and archived using the *gzip* algorithm.

This is done to reduce the amount of data sent. The result is encrypted using the AES128-CBC algorithm. A key is generated using the device's pseudorandom number generator. After that, the key used in the AES encryption is encrypted by the RSA algorithm, using a public key downloaded from Xiaomi servers. The resulting dataset is packaged into a JSON object and sent to servers in Singapore.

The application calls the functions *registerSuperProperties* and *registerDynamicSuperProperties*. These functions are responsible for collecting data and preparing JSON objects. It can be said that the Sensors Data encryption mechanism ensures a relatively high level of data security when transmitting such data to the analytics servers located in Singapore.

The Google Analytics module installed on the device allows the Mi Browser browsing history, search results and other parameters of application activity to be read, and to send this data to the analytics servers. Data is sent via an encrypted TLS channel using Protobuf encoding. Decoding data without a Protobuf configuration file is impossible or difficult, but certain data can be discerned in the encrypted stream: the internet address opened in MI Browser, data entered in the search field or an action performed by the user (e.g., a click on the search field).

This data can be accessed and used by the application developer, Xiaomi.[28] An encoded fragment of data sent to Google Analytics servers is presented in Table 11.

[28] Xiaomi information. *https://privacy.mi.com/all/en_US/*

Table 11. Encoded fragment of outgoing data sent by a Xiaomi device to Google Analytics servers

event_network r:LT|285
_oapp _scBrowserActivity _siçÈ¾å°òT

“urlr
:LT| https://nksc.lt/¢þ¦¡/ ý Âicon _oapp op

r:LT|wifi_ifremind r

:LT|remind languager
:LT|en
is_system_languager
:LT|1sourcer:LT|search_icon _oapp op

r:LT|show_scBrowserActivity _siçÈ¾å°òTweb_translate_op²

“ýæ/ñ®ý/event_network

r:
LT|wifienter_wayr:LT|searchBar_website _oapp _scBrowserActivity _siçÈ¾å°òT imp_search_page Îæýæ/ý
event_network r

:LT|323
_oapp _scBrowserActivity _siçÈ¾å°òT urlr: LT| https://kam.lt

Table 12 presents information characterising the analytical data transmitted by the Xiaomi device through the network to Google Analytics servers.

Table 12. Characteristics of data sent to Google Analytics servers

Line No.:	IP address	Data sent, *B*	Data received, *B*	Total data, *B*	State
1	142.250.74.110	2545	0	2545	the USA
2	172.217.16.14	1282		1282	
3	216.58.207.206	12699		12699	

Based on the findings, it can be said that Xiaomi collects a relatively large amount of information about the processes running on the device, the behaviour of installed software packages, the actions performed by users and the configuration parameters of applications. Two analytics systems, Sensors Data and Google Analytics, are used to implement this process. An overview of sources found that Xiaomi devices collect a wider range of data compared to other manufacturers of

mobile devices[29, 30, 31].

Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

3. The functionality implemented on a Xiaomi device can limit the free availability of information

It has been established that during the initialisation of the system applications factory-installed on a Xiaomi Mi 10T device, these applications contact a server in Singapore at the address globalapi.ad.xiaomi.com (IP address 47.241.69.153) and download the JSON file MiAdBlacklistConfig, and save this file in the metadata catalogues of the applications. A list of applications for which the MiAdBlacklistConfig file was found in metadata catalogues is presented in Table 13.

Table 13. List of mobile applications using the MiAdBlacklistConfig file

Line No.:	Application name	Application identifier	Device
1	Security	*com.miui.securitycenter*	Xiaomi Mi 10T
2	Mi Browser	*com.mi.globalbrowser*	
3	Downloads	*com.android.providers.downloads.ui*	
4	Music	*com.miui.player*	
5	Themes	*com.android.thememanager*	
6	MIUI Package Installer	*com.miui.global.packageinstaller*	
7	Cleaner	*com.miui.cleanmaster*	

Once the applications have downloaded the file, the download date is recorded in order to facilitate periodically updating the list. The scheme for downloading the MiAdBlacklistConfig file is shown in Figure 11.

29 Apple Privacy Policy. *https://www.apple.com/legal/privacy/en-ww/*

30 Douglas J. Leith. Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google. *https://www.scss.tcd.ie/doug.leith/apple_google.pdf*

31 Xiaomi Privacy Policy. *https://privacy.mi.com/all/en_IN/*

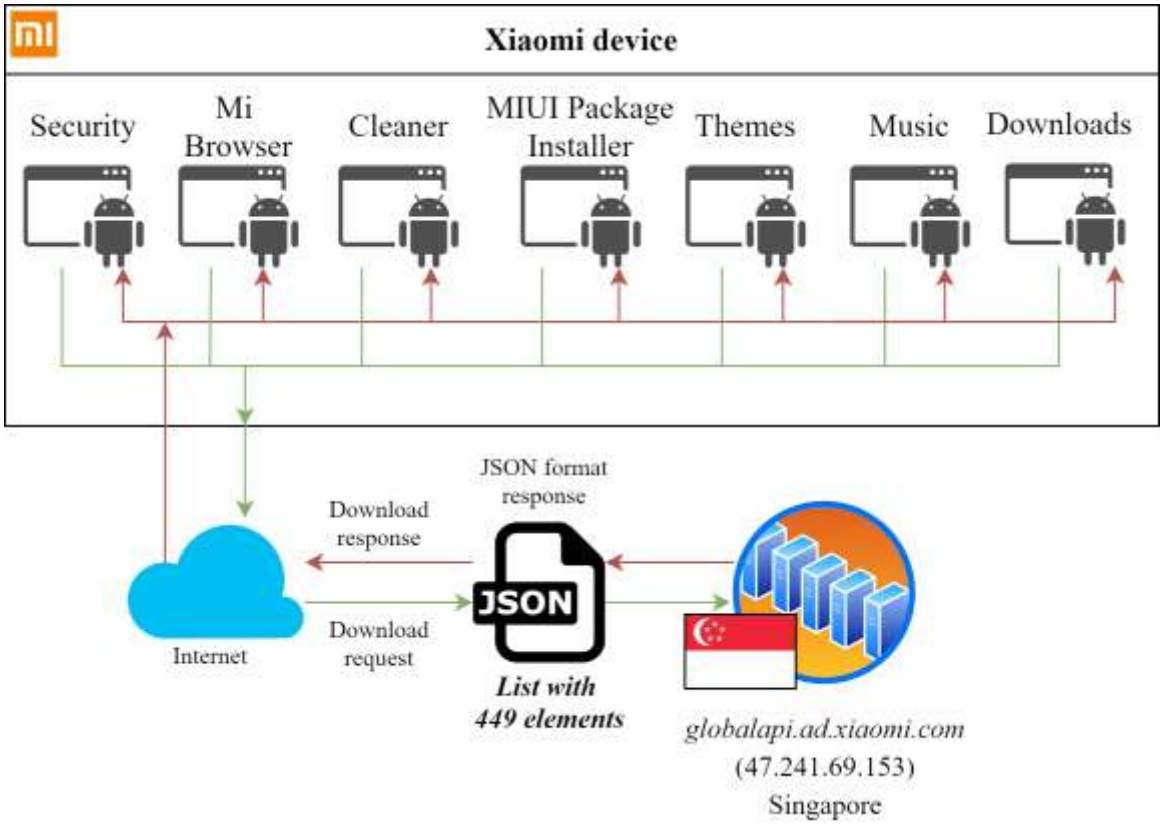

Figure 11. MiAdBlacklistConfig download scheme

This file contains a list composed of the titles, names and other information of various religious and political groups and social movements (at the time of the analysis, the MiAdBlacklistConfig file contained 449 elements). A fragment of the MiAdBlacklistConfig file is shown in Table 14.

Table 14. Fragment of the MiAdBlacklistConfig file

Line No.:	Original	Approximate translation
1	"宗教虔信者阵线",	“Front of religious believers”,
...		
22	"西藏自由",	“Free Tibet”,
...		
60	"蒙古独立",	“Independence of Mongolia”,
61	"89民运",	“89 Democracy Movement”,
62	"基督灵恩布道团",	“Christian charismatic mission”,
...		
145	"伊斯兰联盟",	“Islamic League”,
...		
201	"民运",	“Democratic Movement”,
202	"妇女委员会",	“Women’s Committee”,
203	"伊斯兰马格里布基地组织",	“Al-Qaida in the Islamic Maghreb”,
204	"人民报",	“People’s daily newspaper”,
205	"巴勒斯坦解放组织",	“The Organisation for the Liberation of Palestine”,

	...	
313	"台独万岁",	“Long live Taiwan’s independence”,
	...	
369	"美国之音",	“The Voice of America”,
	...	
420	"89运动",	“89 Movement”,
	...	
449	"夏米斯丁艾合麦提·阿布都米吉提"	“Xia Misteen Ahemet Abu Dumijiti”

Analysis of the Xiaomi application code showed that the applications have implemented software classes for filtering the target multimedia displayed on the device based on the downloaded list in the MiAdBlacklistConfig file. A fragment of this code is shown in Table 16.

Table 16. A fragment of content filtering code used in a Xiaomi device

```
public boolean mo76794a(INativeAd iNativeAd, C8380a Avar) {
 if (iNativeAd == null) {
 return true;
 }
 Long currentTimeMillis = System.currentTimeMillis;
 for (String str: new HashSet(this.f11160b))
 {if (iNativeAd.getAdTitle!= null &AMP;&m12161a (iNativeAd.getAdTitle, str)
) {MLog.m6439d(MiAdBlacklistConfig, Ads: “ + iNativeAd.getAdTitle + “is blocked by title word: “ + Art);
 IF (Avar!= null) {
aVar. f11165a= Art;
 }
 this.f11161c = Art;
 return true;
 } other if (iNativeAd.getAdBody!= null &AMP; &m12161a (iNativeAd.getAdBody, str))
 {MLog.m6439d(MiAdBlacklistConfig),Ads: [” + iNativeAd.getAdBody + “] is blocked by desc word: “ +
Art);
 IF (Avar!= null) {
aVar. f11165a= Art;
 }
 this.f11161c = Art;
 return true;
 }
 MLog.m6443i
 (MiAdBlacklistConfig, isAdsBlocked—> totalTime=” + (System.currentTimeMillis – currentTimeMillis)+
“&threadId=” + Thread.currentThread.getId);
 return false;
}
```

After analysing the Mi Browser, it was found that the application performs the download functionality of the MiAdBlacklistConfig file, but does not filter the content according to the list in the MiAdBlacklistConfig file. Based on the Xiaomi code, this functionality has been deactivated in “the European Union region”. The event registration content generated by the Mi Browser is presented in Table 17.

Table 17. Event registration content generated by the Mi Browser

Line No.:	Name of function	Parameter 1	Parameter 2
1	MLog.d	MiAdBlacklistConfig	start to request url
2	MLog.d	ConfigRequestCommon	UserAgent: Dalvik/2.1.0 (Linux; U; Android 10;

			M2007J3SY MIUI/V12.0.18.0.QJDEUXM)
3	MLog.d	MiAdBlacklistConfig	handleResponse
4	MLog.d	MiAdBlacklistConfig	request retry: success reset times
5	MLog.d	MiAdBlacklistConfig	response parsed success
6	MLog.d	MiAdBlacklistConfig	updateAdConfig
7	MLog.d	MiAdBlacklistConfig	notifyAllObservers
8	I:	NativeAdManagerInternal	posid[1.306.1.3],requestAd isPreload: false
9	I:	NativeAdManagerInternal	AdSwitch expired: new query from remote
10	I:	AdSwitchUtils	AdSwitchOFF is false
...			
23	I:	AdReportTask	{“mEvent”:“LOAD_AD”,“mPositionId”:“1,306.1.3” ,“mAppId”:“10000”,“mChannelId”:“miui”,“mOperator”:“246_01”,“mClientVersion”:“100492”,“mSdkVersion”:“130200”,“mAdTime”:“1621431087190”, mModel: M2007J3SY,mGaid:“d3a32b43-6e7e-4306-82ca-0f65f1586511”,“mLanguage”:“en_US”,“mBuildSdkVersion”:“29”,“mDoNotTrack”:“false”,“mBuildType”:“stable”, muiVersion:“V12.0.18.0.QJDEUXM”,“mRegion”:“LT”,“mTriggerId”:“9d1f86e3-579e-4110-b71e-065f520c1fa3”, “mIsPreload”:“false”,“mCustomKey”:“adsCnt”,“mCustomValue”:“0”,“mInstaller”:“com.xiaomi.discover”,“mIsPreInstall”:0,mElapsed:0,mIsid:0}
24	I:	MIADSDK	Personalised ad is disabled in the EU region, reporting is not allowed
25	I:	MIADSDK	Personalised ad is disabled in the EU region, reporting is not allowed
...			
38	I:	AdReportTask	{“mEvent”:“PAGE_VIEW”,“mPositionId”:“1.306.1.3”,“mAppId”:“10000”,“mChannelId”:“miui”,“mOperator”:“246_01”,“mClientVersion”:“100492”,“mSdkVersion”:“130200”,“mAdTime”:“1621431420870” , mModel: M2007J3SY,mGaid:“d3a32b43-6e7e-4306-82ca-0f65f1586511”,“mLanguage”:“en_US”,“mBuildSdkVersion”:“29”,“mDoNotTrack”:“false”,“mBuildType”:“stable”, muiVersion:“V12.0.18.0.QJDEUXM”,mRegion:“LT”,“mTriggerId”:“9d1f86e3-579e-4110-b71e-065f520c1fa3”,mInstaller:“com.xiaomi.discover”,“mIsPreInstall”:0,“mElapsed”:0,“mIsBid”:0,“mCost”:333682}

It is believed that this functionality allows a Xiaomi device to perform an analysis of the target multimedia content entering the phone; to search for keywords based on the MiAdBlacklist list received from the server. Once the device determines that the content contains certain keywords, the device performs filtering of this content and the user cannot see it. The principle of data analysis allows analysis not only of words written in letters; the list that is regularly downloaded from the

server can be formed in any language. It is important to emphasise that this functionality is activated remotely by the manufacturer. It is believed that the existence of such functionality may jeopardise free access to information and limit its accessibility. It can be said that this is important not only for Lithuania, but also for all countries using Xiaomi devices.

4. On Xiaomi devices, to connect to the cloud, it is necessary to register a SIM card. Sent messages are not displayed on the phone. The risk of leakage of user data

Studies have shown that when a user chooses to use Xiaomi Cloud services, the user's mobile phone number is registered on servers located in Singapore. This is done by the device sending an encrypted SMS message to a special phone number. The registration procedure for Xiaomi Cloud services is performed on the Xiaomi device by sending an SMS message as shown in Figure 12.

When a user attempts to connect to the Xiaomi Cloud service for the first time, the device requests access to a (1) Xiaomi Account. After entering login data and successfully logging in to the account, a menu window (2) opens in which it is possible to enable and disable the main Xiaomi Cloud functions: data synchronisation and device geolocation in case of loss of a device.

After selecting the desired functions, the service operating in the background starts the SIM card data collection procedures (3, 4 and 5). After the service completes the SIM card data collection procedures, the user is shown an information window (6) indicating that in order to enable the functionality of call history and message synchronisation, the device must send an SMS to check the phone number.

It is also indicated in the information window that the user may be charged for sending an SMS message at the standard rates of the mobile telecommunications operator (provider). When the user closes the information window, the user is shown an operating system window (7), which asks the user whether to allow the SIM card registration service to send SMS messages automatically. With the user's consent, an automated telephone number registration procedure is launched (8).

The device downloads from the **general** server the configuration data structure for the procedure, which includes the address of the server with which further network communication is to be carried out, the phone number of the SMS addressee and other parameters. The device then generates an SMS message and sends the message to the phone number specified in the configuration data structure (9). The sent message is immediately deleted from the sent message log.

At the same time, the collected SIM card data is stored in the internal service database (10). After sending the SMS message, its content is encrypted and sent to a server, the address of which is specified in the configuration data structure, together with a query for confirmation of registration (11).

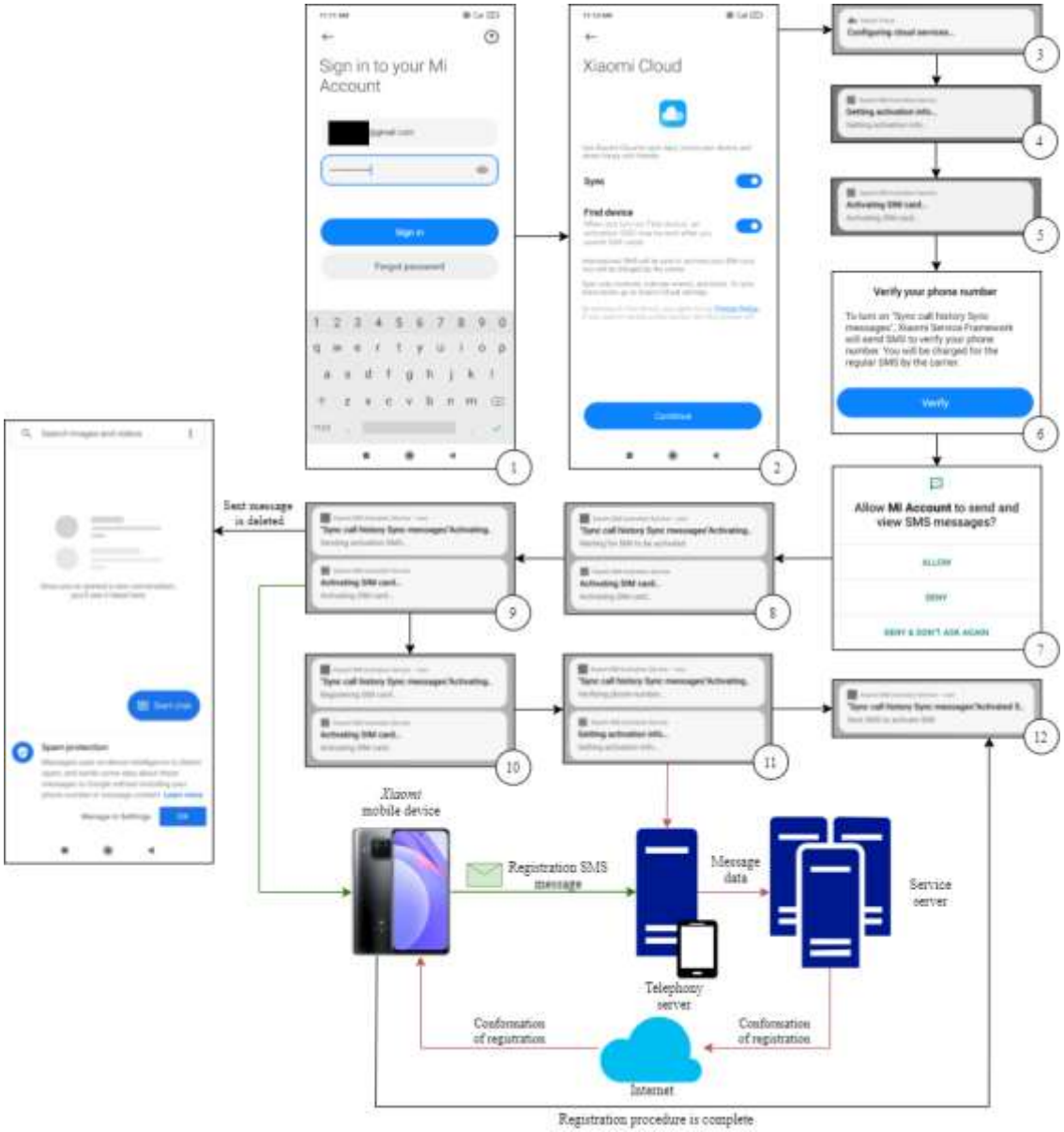

Figure 12. Registration procedure for Xiaomi Cloud services performed on a phone by sending an SMS message

After sending a registration query to the server, the device receives a response to the query, displaying a registration result (positive or negative) (12).

It has been established that the registration of a telephone number is carried out regardless of how the user chooses to be authenticated, either by phone number or by e-mail address. It is important to note that the sent encrypted SMS message and its addressee are not visible to the user. At the time of the analysis, after disabling the functionality of the Xiaomi Cloud service, the sending of messages was not observed. A more detailed network flow diagram is given in Figure 13.

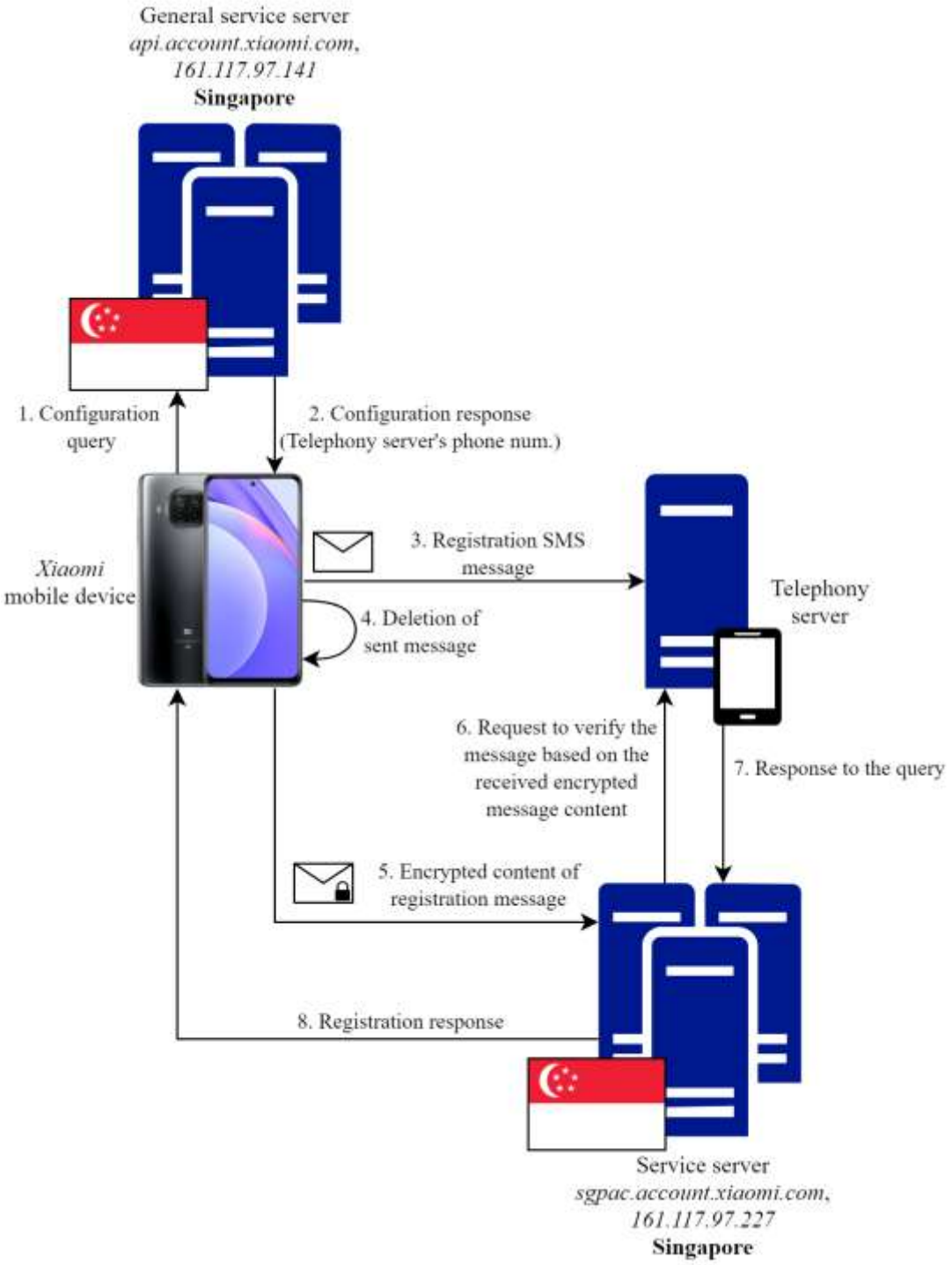

Figure 13. Registration scheme for the Xiaomi Cloud services network

Once the phone number registration process has started, the device sends a query to a general server located in Singapore (1), from which it receives a data structure as a response. This data structure includes the address of the target server for this service, the number of the telephony server and other parameters used for the registration procedure (2). The device then generates and sends an SMS message to the phone number specified in the received data structure (3). The message sent is immediately deleted from the sent message log (4). After sending the message, the device contacts the server located in Singapore and sends to the telephony server the encrypted content of the sent

message (5). The server communicates with the telephony server to which the SMS message was sent (6, 7). During the communication, the message sent by telephone is checked and the encrypted content of the message is sent by means of the mobile internet network. After successful verification of the messages, the device is given a response to the query, adding on the registration result (8).

It is important to note that if the SIM card is not installed on the device at the time of registration, the registration process is terminated and the device displays an error message.

Before the device sends the phone number registration SMS message, the device contacts the general server located in Singapore, the address of which is api.account.xiaomi.com (IP address: 161.117.97.141).

During communication, the device downloads the configuration data structure required for the registration process. This data structure includes the telephone number of the telephony server, the server address and other data. An extract of the network communication data from the device to the general server is shown in Table 18.

Table 18. Extract of configuration download network traffic

Get/pass/configuration HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; M2007J3SY MI/V12.0.18.0.QJDEUXM) APP/unknown MK/TWkgMTBU
Cookie: sdkVersion=accountsdk-2020.01.09
Host: api.account.xiaomi.com
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Wed, 05 May 2021 09:48:42 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-Alive
Content-Encoding: gzip

{“result”:“ok”,“code”:0,“date”:{“”mo“:{”460(03|05|11)“:[”“10690329119863”,“10690329119867”,“10690329119868”,“10690329119862”,“520(05|18|47)”:[“”1614813“],”708[0-9]+:[“+ 50494340090”,“425[0-9]+:[”+ 972559882264“],”255[0—
<...>
9]+:["+ 8804445652000","+ 8804445652019"],"262[0-9]+:["+ 4915735981865"],"216[0-9]+:["+ 36305555538","450[0-9]+:["15996816","246[0-9]+:[”+ 37066803015“,”206[0-9]+:[“+ 32460225522”],“226[0-9]+:[”+ 40371700668“],”440[0-9]+“:[”+ 819070094460“,”260[0-9]+:[“+ 48666068953”,“40[45][0-9]+:[”+ 918652202112“,”56161974“],”502(0|1|2[0-9])[0-9]*“:[”+ 601117225668“],”250[0-9]+:[“+ 79037672679”,“+ 447491163442”,
<...>
9]+:"sgpac.account.xiaomi.com","262[0-9]+":"sgpac.account.xiaomi.com","216[0-9]+":"sgpac.account.xiaomi.com","450[0-9]+":"sgpac.account.xiaomi.com",”246[0-9]+:"sgpac.account.xiaomi.com",”206[0-9]+:“sgpac.account.xiaomi.com”,“226[0-9]+”:“sgpac.account.xiaomi.com”,“440[0-9]+”:“sgpac.account.xiaomi.com”,“260[0-9]+”:“sgpac.account.xiaomi.com”,“40[45][0-9]+:”inac.account.xiaomi.com“,”502(0~1|2[0—
<...>

The device sends an SMS message to the phone number specified in the configuration data

structure.
During the analysis of the phone number registration service Xiaomi SIM Activation Service, it was established that the device performs the function of automatic sending of an SMS message. The addressee of the SMS message and the content of the message are shown in Figure 14.

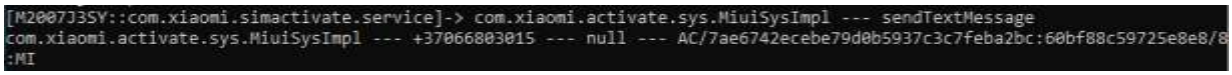

Figure 14. Content of the SMS message and process of sending

After analysing the decompiled factory-installed system service Xiaomi SIM Activation Service, it was found that the application performs the function of automatic sending of an SMS message using the external software class miui.telephony.SmsManager, which is not compiled and is archived in the service installation file.

A fragment of the code for sending the SMS message is given in Table 19.

Table 19. Fragment of the code for sending the SMS message

```
public void sendTextMessage(int i, String str2, String str3, PendingIntent pendingIntent, PendingIntent
pendingIntent2) {
try {
class<?> cls = Class.forName(miui.telephony.SmsManager));
 Object raise = cls.getDeclaredMethod(getDefault, new Class {Integer.TYPE}).invoke((Object) null, new
Object{Integer.valueOf(i)});
 CLS.getMethod(sendTextMessage, new Class{String. class,String.class,String.class, PendingIntent. class,
PendingIntent. class}.invoke(invoke, new Object{str, str2, str3, pendingIntent, pendingIntent2));
 Log.d(MiuSysImpl, "successfully send text message");
 } catch (NoSuchMethodException e) {
Log.e(MiuSysImpl), "error when send text message: NoSuchMethodException, e);
 throw new RuntimeException(e);
 } catch (IllegalAccessException e2) {
Log.e(MiuSysImpl), "error when send text message: IllegalAccessException, e2);
 throw new RuntimeException(e2);
 } catch (InvocationTargetException e3) {
Log.e(MiuSysImpl), "error when send text message: InvocationTargetException, e3);
 throw new RuntimeException(e3);
 } catch (ClassNotFoundException e4) {
Log.e(MiuSysImpl), "error when send text message: ClassNotFoundException, e4);
 throw new RuntimeException(e4);
 } catch (SecurityException e5
) {ActivateLog.m24w(MiSysImpl,sendTextMessage,e5);
 }
}
```

It is worth noting that in the above-mentioned external software class miui.telephony.SmsManager, there is an implemented functionality allowing deletion of SMS messages. The functions of sending and deleting SMS messages, and other functions implemented in the external software class miui.telephony.SmsManager, are shown in Figure 15.

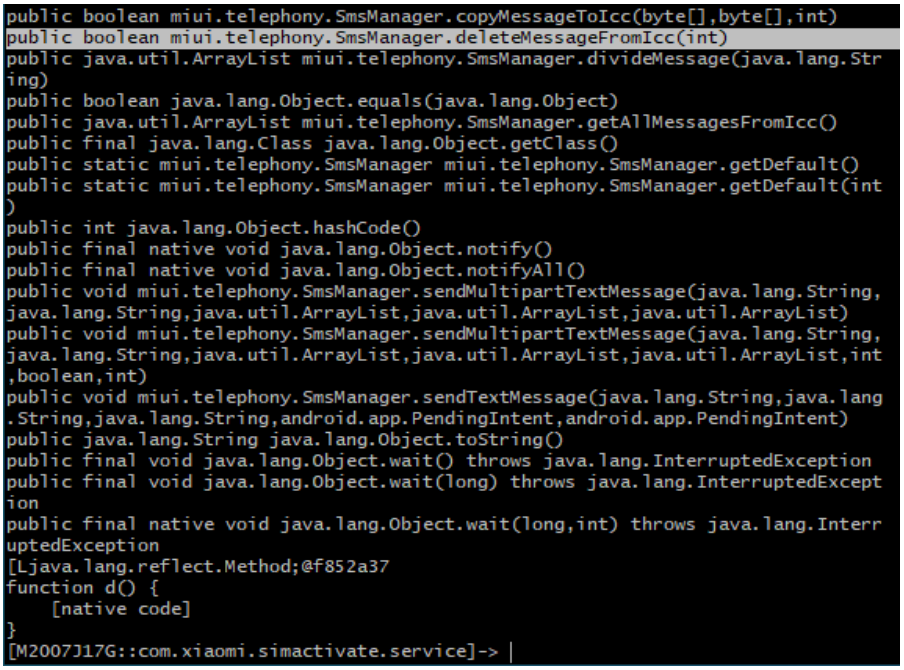

Figure 15. Functions of sending and deleting SMS messages, and other functions, implemented in the external software class miui.telephony.SmsManager

When the device sends an SMS message to the phone number specified in the configuration data structure, the device sends the encrypted content of the SMS message to the address sgpac.account.xiaomi.com (Singapore).

The server performs content verification against the received encrypted data with the SMS message data received by the telephony server and sends the activation result to the mobile device. An extract of the network traffic is given in Table 20.

Table 20. Communication with the server located in Singapore

```
Post/pass/activation/report HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; M2007J3SY MI/V12.0.18.0.QJDEUXM) APP/unknown MK/TWkgMTBU
Cookie: sdkVersion=accountsdk-2020.01.09
Host: sgpac.account.xiaomi.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 346

DevID=VqFuDPTDczp39bXc&features=CALL_LOG_SYNC++MMS_SYNC+&mnc=24601&activationMode=uplink&simId=F_9M83JIJb_VOKce&smsBodyEncrypted=fu_5ODSHBbJv5XO6wRTIUfNCEerj978hkm5RhLrK19IYsgPUeVQoXbY9Di8-B9WaMvgJeAVwudc_nYD9LWJww28gYA9A9V1kqzNCf8e1tfLftN_Y0UXpvy4cXlHISL5yiGj2sI77KFzS20PgKfocTxNcleEuLlTEjTY_38 %3D& action=vkey%3Aok%2Cverify%3A14 %2Cdone%3A14HTTP/1.1 200 OK
Date: Wed, 05 May 2021 09:50:27 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-Alive
Content-Encoding: gzip

{“result”:“ok”,“code”:0,“date”:{},“description”:“.....”}
```

During the analysis, it was established that the device communicated with servers located in

Singapore. The list of identified communications is given in Table 21.

Table 21. Information about communications with servers located in Singapore

Line No.:	Domain	Address	Data, Bytes	State	Purpose
1	api.account.xiaomi.com	161.117.97.141	9200	Singapore	**General server** *Configuration for authentication is sent from the server to the phone: SMS tel. number, server address, etc.*
2	sgpac.account.xiaomi.com	161.117.97.227	48990	Singapore	**Server** *Based on the SMS message received from the phone, a registration response is generated and sent to the phone.*

IP addresses belonging to the domains api.account.xiaomi.com and sgpac.account.xiaomi.com are registered with Alibaba.com Singapore E-Commerce Private Limited. Alibaba is an information technology company established in 1999 in the People's Republic of China. It is known that Chinese IT companies are obliged to transfer any form of information under the companies' control to the Chinese government or its intelligence agencies[32].

Automated sending of messages and its concealment by means of software pose potential threats to the security of the device and personal data; in this way, without the user's knowledge, device data can be collected and transmitted to remote servers.

[32] The Diplomat. *https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/*