Translated from Lithuanian to English - www.onlinedoctranslator.com

NKSC to KAM
Innovation and Training Division
support@ims.nksc.lt

2021 - 08 - 23

Cyber security of mobile devices supporting 5G communication technology supplied in Lithuania evaluation

PRODUCT ANALYSIS BY Huawei, Xiaomi and OnePlus

Introduction

In order to ensure the safe use of software and hardware within the country, the National Cyber Security Center (NKSC) under the Ministry of National Defense performed a cyber security assessment of mobile devices supporting 5G communication technology supplied by various manufacturers in Lithuania. This analysis presents the evaluation results of Huawei, Xiaomi and OnePlus smartphones.

Huawei, Xiaomi and OnePlus, China's international IT and consumer electronics companies[1] and having a strong position in the European market[2]. 2020 These manufacturers introduced fifth-generation 5G mobile smartphones to the Lithuanian market. A safety assessment has been performed for the widely available Huawei P40 5G[3], Xiaomi Mi 10T 5G[4] and OnePlus 8T 5G[5] for mobile devices. The images of the devices examined in the study are shown in Figure 1.



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

Fig. 1 The equipment examined in the study. 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-lenovomeizu-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. Huawei P40 5G Specifications*https://consumer.huawei.com/en/phones/p40-pro/specs/*
4 Xiaomi. Xiaomi Mi 10T 5G Specifications*https://www.mi.com/global/mi-10t-pro/specs/*
5 OnePlus. OnePlus 8T 5G specifications.*https://www.oneplus.com/lt/8t/specs*

Despite the awareness of these brands, corporations faced security challenges in the equipment they developed between 2017 and 2021, with 9 vulnerabilities identified in Xiaomi's products based on Common Vulnerabilities and Exposures (CVEs).[6] related to the risks of personal data leakage (8 of these vulnerabilities can be realized remotely), 144 vulnerabilities were recorded in Huawei's products during this period[7] (28 vulnerabilities were recorded in 2020, 23 in the first half of 2021), most of which were related to device malfunctions, OnePlus in 2020. Vulnerability 1 was fixed[8] allowing an attacker to send SMS messages from a mobile device using third-party software when the mobile device is locked.

These manufacturers are considered to be in a leading position by various sources[9,10] In the market of mobile devices, their wide range, development of new technologies and noticeable growth in Lithuania is an undoubted object of cyber security research.

Findings of the study

Decomposition studies of Huawei, Xiaomi and OnePlus mobile devices have identified 10 cyber security risks. This cyber security assessment analyzes 4 identified cyber security risks related to the overall security of applications pre-installed on devices, threats to personal data leakage, and restrictions on freedom of expression. It is planned to detail the uncovered cyber security risks in other parts of this complex study and to present their assessment by 2021. end. This study addresses issues related to the security of personal data.

The analysis revealed that the mobile application deployment procedure used in Huawei devices is characterized by cyber security uncertainties. Mob. Huawei's applications use a manufacturer-developed infrastructure, which includes the official AppGallery and the peripheral application cache.

When installing a mob. application on the Huawei device, they are searched in the AppGallery, when the application is found, it is downloaded and installed on the mob. device. However, if the application is not found in the official store, the user is automatically redirected to the peripheral application cache, from which the mob. the application is sent to the mob. device for installation. It is worth noting that most application repositories are located in countries not covered by the General Data Protection Regulation, which poses a concomitant risk of leakage of user metadata. The study found that some of the mobs in the tanks. applications are counterfeits of original applications that have malicious functionality or are infected with viruses - the user can download and install such applications on the mob. phone

Data security risks also identified on the Xiaomi device - Factory-installed system applications send statistics on the performance of certain applications installed on the device to the servers of the Chinese cloud service provider Tencent, located in Singapore, USA, the Netherlands, Germany and India.

---

[6] CVE data base. In public published Xiaomi production vulnerabilities. *https://www.cvedetails.com/vulnerability-list/vendor_id-19038/MI.html*

[7] CVE database. Huawei publicly available production vulnerabilities. *https://www.cvedetails.com/vendor/5979/Huawei.html*

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

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

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

The original device browser, Mi Browser, was found to use two data collection modules: Google Analytics and Sensor Data. The built-in Google Analytics module allows you to read your browsing and search history, send this data to analytics servers that Xiaomi accesses and uses[11]. This functionality is activated by the mob. phone by registering with the Xiaomi User Experience Marketing Program. By default, this is done automatically when the phone is switched on for the first time or when the factory settings are restored.

It has been established that the Sensor Data module used in the device collects statistical information of parameter 61 (application activation time, language used, etc.) about the activity of the used applications. The collected statistics are sent via encrypted channel to Xiaomi servers in Singapore, which is not covered by the General Data Protection Regulation. According to international sources, clear cases of Xiaomi unauthorized user data collection have been identified[12.13]. It can be argued that the potentially excessive collection and use of analytical data poses a threat to the privacy of personal data.

It has also been found that when a user chooses to use Xiaomi cloud services, the user's mob is executed. phone number registration on servers in Singapore. This is done by sending an encrypted SMS message to the device's special phone number. Upon receiving the SMS, the server synchronizes it with the Xiaomi server in Singapore, from which the phone mob. Internet connection downloads a confirmation that allows the user to connect to the Xiaomi cloud service. It is established that the registration of a telephone number is performed regardless of how the user chooses to be authenticated - by telephone number or e-mail. email address. It is important to note that an encrypted SMS message has been sent and its contact is not visible to the user.

Automated messaging and cryptographic functionality poses potential threats to the security of the device and personal data, allowing device data to be collected and transmitted to remote servers without the user's knowledge.

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

Xiaomi system applications (Security, MiBrowser, Cleaner, MIUI Package Installer and Themes) have been found to regularly download the manufacturer's updated MiAdBlacklistConfig configuration file from a server in Singapore. This file contains a list of the names, names and other information of various religious and political groups and social movements (449 entries were recorded in the MiAdBlacklistConfig file during the investigation). After the analysis of Xiaomi application code, it was found that the applications contain software classes for filtering the target multimedia displayed on the device according to the downloaded "*MiAdBlacklistConfig* " list.

This allows the Xiaomi device to analyze the target multimedia content entering the phone - looking for keywords based on the information received from the server. *"MiAdBlacklist* list. When it detects that the content contains search terms, the device blocks that content. It is considered that this functionality may pose potential threats to the free availability of information.

NKSC at the Ministry of National Defense 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-overchinese-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/*

Wider research results

The key software characteristics of the mobile devices involved in the study, noting the operating system (OS) framework, operating system framework manufacturer modification, operating system kernel version, and security update dates, are presented in Table 1.

Table 1. The main software characteristics of the mobile devices involved in the study

Device name	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
The basis of the factory-installed OS	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Pre-installed OS based manufacturer's modification	EMUI 10.1.0	MIUI Global 12.0.10 (QJDEUXM)	Oxygen OS 11.0.5.6.KB05BA
The basis of the latest available OS	Android 10	Android 11	Android 11
Latest available OS based manufacturer's modification	EMUI 11.0.0.151 (C432E5R5P3)	MIUI Global 12.0.2.0 (RJSEUXM)	Oxygen OS 11.0.8.13.KB05AA
Latest available OS release data	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 last security update	2021-06-01[14]	2021-03-01[15]	2021-04-01[16]
Security update no.	9	3	4

All examined mob. devices run on the Android operating system, Huawei P40 and Xiaomi Mi 10T use system version 10, OnePlus 8T - currently the latest, 11. It is worth noting that, by default, the standard Android 11 operating system has more access control options[17], enabling the user to have more control over the access of applications to the data stored on the device.

Android operating system security updates are updates to operating system components designed to fix software vulnerabilities that compromise the security of a device or the data stored on it. These updates address software vulnerabilities that allow remote code execution. *Remote code execution*), the raising of privileges *Elevation of privilege*), information disclosure and leakage *Information disclosure*), service disruption *Denial of service*) and other types of attacks. Each of these security updates fixes between 20 and 60 security vulnerabilities noted in the CVE database. It is worth noting that the vulnerability of the vulnerabilities ranged from 5.4 to 10.0 points (out of 10 possible).

For this reason, the mob is important. device users to install these updates regularly. These security updates for the Android operating system are released periodically, every 1-3 months. Xiaomi is committed to supplying these upgrades to its facilities for 2 years[18]and OnePlus for 3 years[19]. About Huawei's commitment to providing operating system or security updates

[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/*

no data found. It is worth noting that the manufacturer of the Android operating system *Google* allows security updates for unmodified versions of the Android operating system *Android Open Source Project*). For this reason, updates to the operating system and its security are available at the earliest *Google* manufacturer's equipment.

Meanwhile, equipment manufacturers like Huawei, Xiaomi, OnePlus and others. operating system or its security updates have to be adapted to the modifications made by the OS-based manufacturer, therefore the mob of these manufacturers. for devices, these updates are available later. It is especially important to emphasize that the latest security updates are only available for mob. for the Huawei P40. The study found that the latest security updates for mob. the Xiaomi Mi 10T was 3 months old, and the mob. for the OnePlus 8T, 2 months ago.

The NKSC notes that, in line with the above, timely security updates of existing facilities are essential.

1. The official Huawei app store, AppGallery, redirects to third-party emails. stores where the applications are malicious or infected with viruses

The analysis revealed that the mobile application deployment procedure used in Huawei devices is characterized by cyber security uncertainties. Mob. Huawei phones use the infrastructure developed by the manufacturer, which consists of the official AppGallery and the peripheral application cache (Apkmonk,*APKPure, Aptoide* etc.). The scheme of the Huawei e-shop is shown in Figure 1.

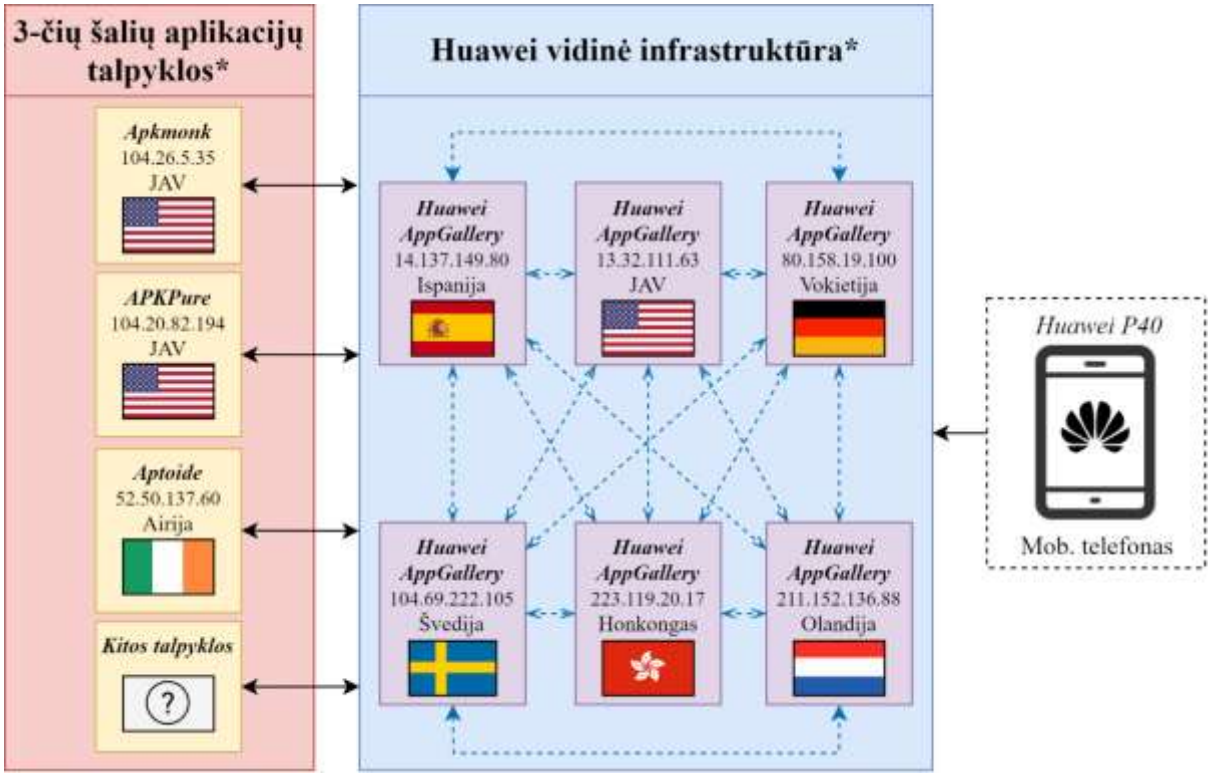


Fig. 1 "Huawei Electronic Mobile App Store Scheme

The infrastructure of the Huawei e-mobile application store consists of two blocks - the internal infrastructure Huawei AppGallery and third-party repositories. Founded to own “Huawei

AppGallery's infrastructure is located in Spain, the United States, Germany, Sweden, the Netherlands, Hong Kong and Thailand. This infrastructure is integrated with third-party repositories, three of which are most widely known to operate in the US, Ireland and the Netherlands. Different assessments of sources[20], Huawei 's mobile application distribution infrastructure currently includes 6 to 8 third - party repositories. Table 2 provides information on Huawei's mobile application distribution infrastructure.

Table 2. Information on Huawei's mobile application distribution infrastructure, including internal "Huawei AppGallery and the three best-known integrated external cache settings

Eil. No.	Infrastructure	Address	IP address	State
1	Inner 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 appdl-11-	13.32.111.63	USA
4		drcn.dbankcdn.com appdl-2-	65.9.52.144	USA
5		drcn.dbankcdn.com.cdn.dnsv1.com	211.152.136.88	The Netherlands
6		uc3.hispace.hicloud.com sdkserver-	23.14.13.247	Sweden
7		dre.op.hicloud.com hwid-	104.69.222.105	Sweden
8		dre.platform.hicloud.com appdl-12-	104.69.222.145	Sweden
9		drcn.dbankcdn.com.akamaized.net appdl-12-	184.31.15.17	Sweden
10		dre.dbankcdn.com.akamaized. net appdl-1-	184.31.15.51	Sweden
11		dre.dbankcdn.com.c.cdnhwc1.com appdl-1-	119.46.76.15	Thailand
12		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 storage APKMonk	www.apkmonk.com	104.26.4.35	USA
25	External storage ApkPure	download.apkpure.com	104.20.83.194	USA
26	External storage 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	USA
35		pool.apk.aptoide.com	5,779,110,134	The Netherlands
36		apkins.aptoide.com	95,211,168,137	The Netherlands
37		apkins.aptoide.com	95,211,223.52	The Netherlands

When installing a mob. application on the Huawei device, they are searched in the AppGallery, when the application is found, it is downloaded and installed on the mob. device. Figure 2 shows the installation scheme of mobile applications using the Huawei AppGallery platform.

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

When you enter the name of the application you are looking for in the search box in the Huawei AppGallery application, a list of search results is displayed. The Petal Search section appears in the search results window. When selected, the user is provided with a list of applications accessible through third-party application repositories (1). When the user selects an application from this section, a warning message (2) is displayed. The warning message states that further action will be taken outside the Huawei AppGallery.

When the user closes the alert window, a web browser is opened on the device, and the user is redirected to the 3rd party application cache website. When the user selects the application installation file download option (3) on the website, it is downloaded and saved in the device's internal memory (4, 5). When the device completes the procedure of downloading the application installation file, the application installation is started.

Since in this case the application installation is initiated by the device's web browser, the user is presented with an information window (6) requesting permission for the web browser to initiate the application installation procedure. After the user gives permission, the application installation window is displayed (7), which requires user input to begin the installation. When the user confirms the installation of the application again, the application is installed (8, 9) and the icon of the newly installed application is added to the main window (10).

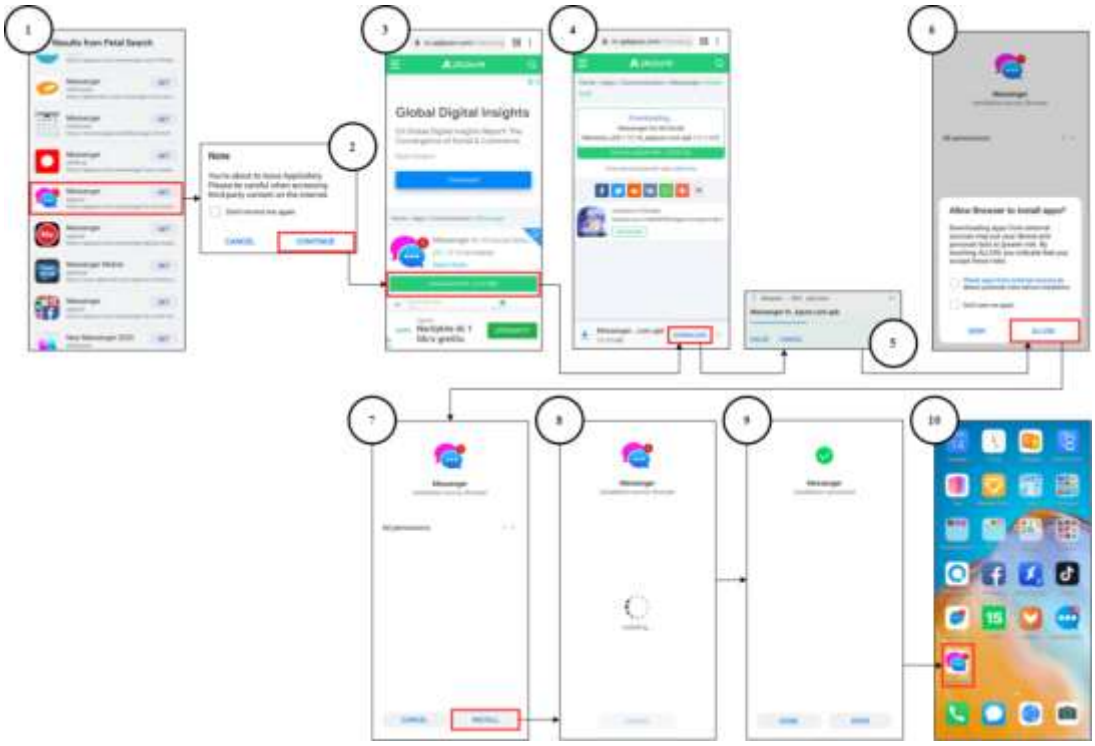


Fig. 2 Mobile application deployment scheme using Huawei AppGallery platform

If the application you are looking for is not available in the Huawei AppGallery, the user is automatically redirected to the peripheral caches of third-party applications, from which the mob. the application is sent to the phone for installation.

The study found that some of the mobs in the tanks. applications are counterfeits of original applications that have malicious functionality or are infected with viruses - the user

applications can be downloaded and installed on mob. phone, thereby compromising the security of the device and the data on it.

A schematic diagram of the implementation of Huawei applications, using third-party repositories, is presented in Figure 3.

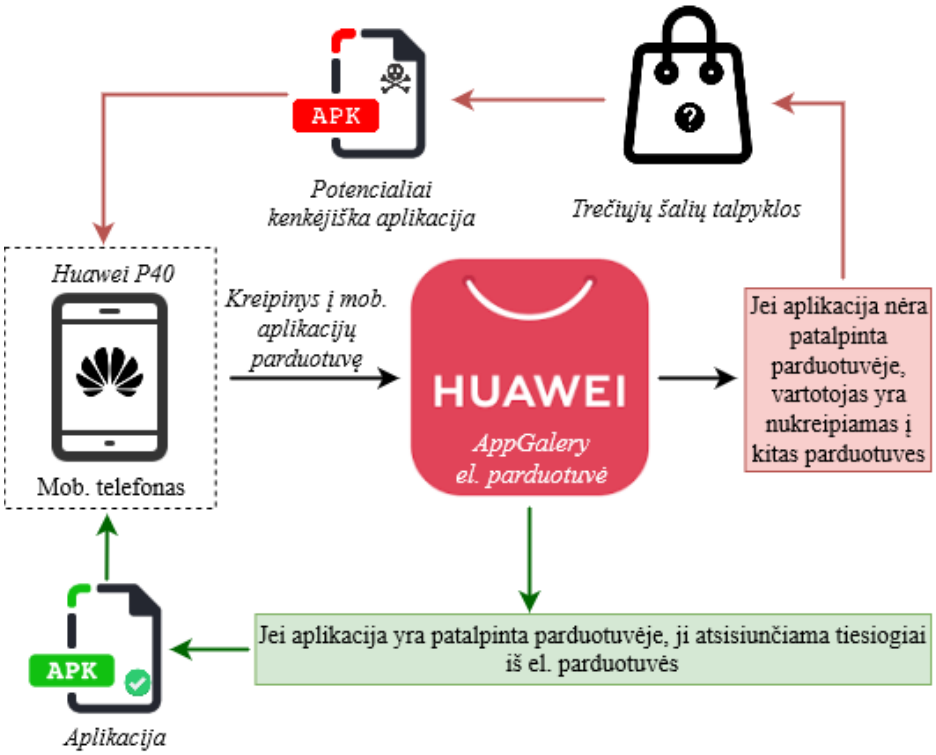


Fig. 3 Schematic diagram of Huawei application deployment, including third-party storage

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 sending an application from a mob in a BDAR country. may refer to third countries in which this Regulation does not apply. This poses a concomitant risk of user metadata leakage.

The study looked at the original AppGallery email running on Huawei's infrastructure. store and three selected most widely known integrated third-party repositories - APKMonk, Aptoide, Apkpure. It is worth noting that information about the developers of APKMonk and Apkpure could not be found in freely available sources. Based on Aptoide information[21], is headquartered in Portugal (Lisbon) and has branches in China (Shenzhen) and Singapore.

During the study, traffic capture was performed by sending applications from sources used in Huawei's infrastructure. During the investigation, applications were searched on Huawei's AppGallery email. in the store, without changing the original application delivery order provided by the manufacturers - the applications were sent directly from the original store and third-party application repositories provided by AppGallery.

By recording the number of connections, it was found that at the time of sending the application, references to 38 addresses were set from the original AppGallery store, in the case of APKMonk - to 56 addresses. The highest number of referrals was recorded in the cases of Aptoide and Apkpure, to addresses 74 and 73, respectively.

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

Information illustrating the Huawei mob. device prompts during application download procedures are shown in Figure 4.

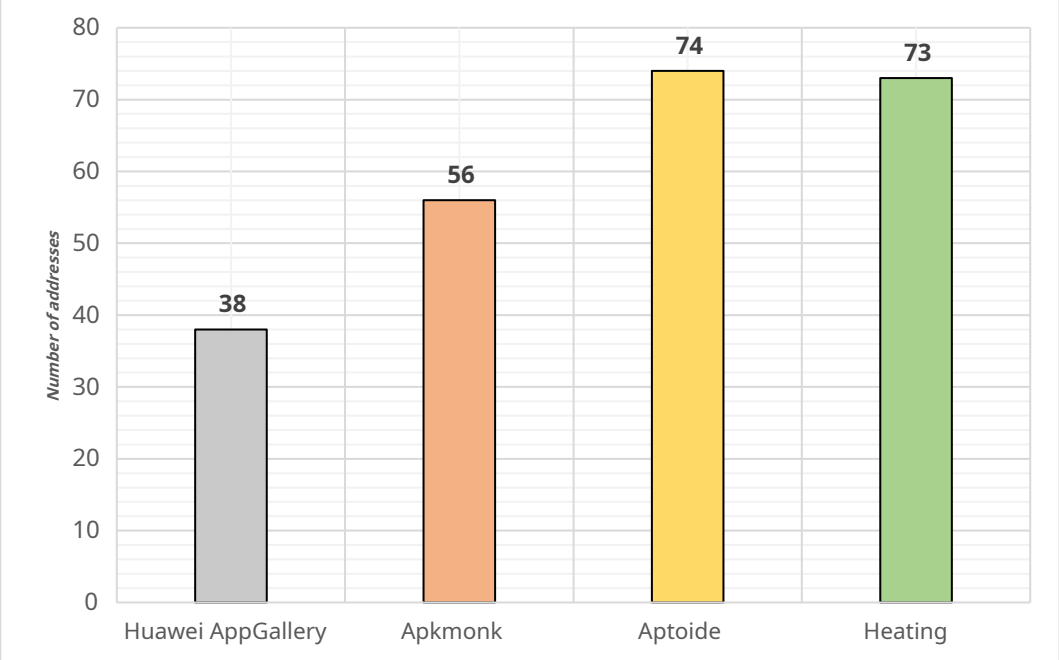


Fig. 4 "Huawei "mob. the number of device requests during application download procedures

More detailed information describing the countries of appeal and their number is provided in Figures 5 - 7.

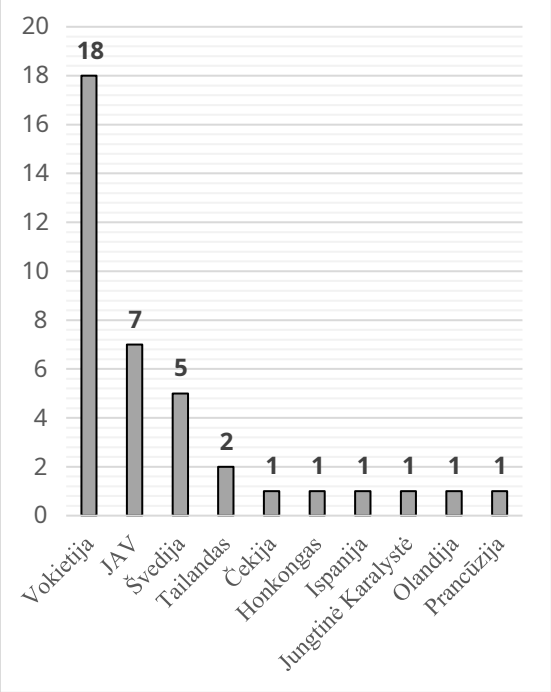


Fig. 5 "Huawei AppGallery information

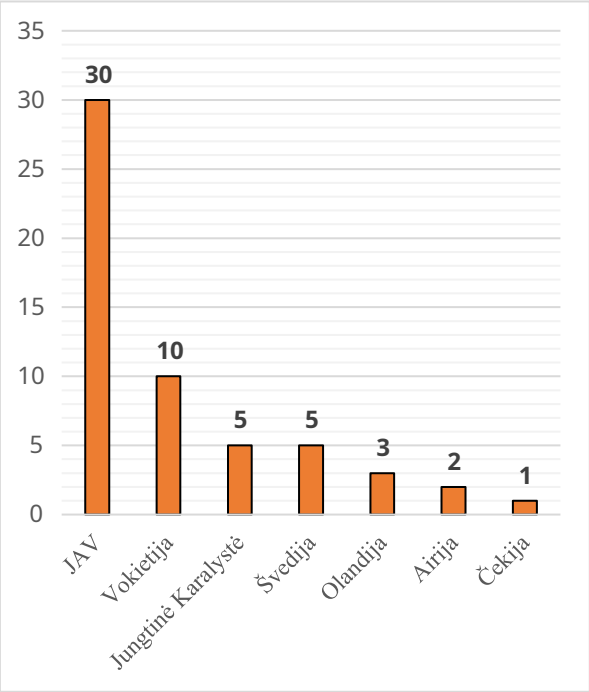


Fig. 6 Cache ApkMonk Referrals information

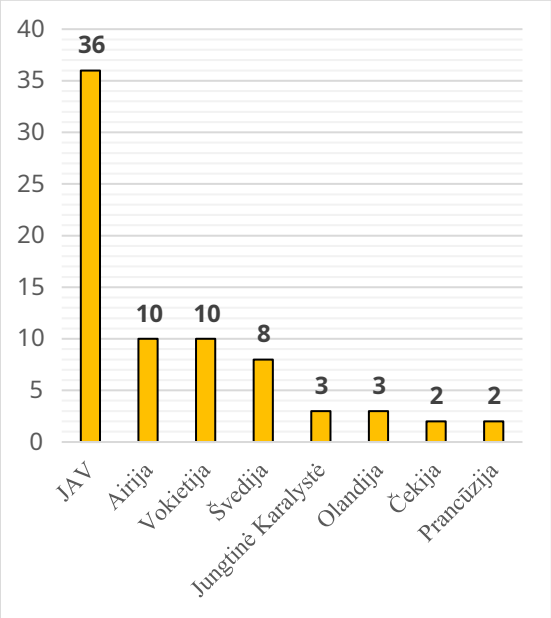


Fig. 7 Cache Aptoide Referrals information

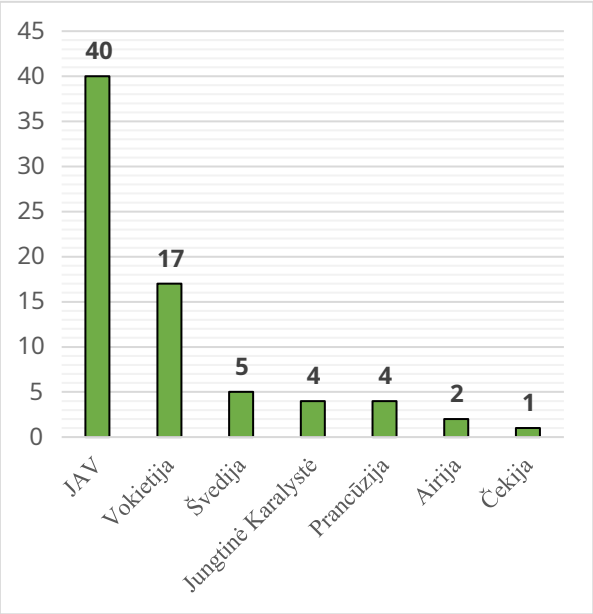


Fig. 8 Cache Apkpure Referrals information

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

3 lentele. More detailed analytical information indicating specific IP addresses and countries

Eil. No.	*Huawei* "AppGallery		ApkMonk		Aptoide		Heating	
	Address	State	Address	State	Address	State	Address	State
1	apkrep.ns1.ff.avast.com	Czech Republic	34.250.145.50	Ireland	iwinmobi.com	Ireland	apkrep.ns1.ff.avast.com	Czech Republic
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	Czech Republic	ws75.aptoide.com	Ireland	52,209,246,140	Ireland
4	8.8.8.8	USA	appimg3.dbankcdn.com	USA	ws75.aptoide.com	Ireland	13.32.111.63	USA
5	appdl-11-dre.dbankcdn.com	USA	13.33.242.107	USA	webservices.aptwords.net	Ireland	feeds.apyhi.com	USA
6	13.33.242.98	USA	auction.unityads.unity3d.com	USA	en.aptoide.com	Ireland	34.98.67.61	USA
7	13.107.213.44	USA	odr.mookie1.com	USA	rakam-api.aptoide.com	Ireland	34,236.65.196	USA
8	52,177,138.113	USA	auction.unityads.unity3d.com	USA	pnp.aptoide.com	Ireland	rtb.openx.net	USA
9	appdl-11-drcn.dbankcdn.com	USA	auction.unityads.unity3d.com	USA	en.aptoide.com	Ireland	35,244,159.8	USA
10	152.199.21.230	USA	eu-u.openx.net	USA	ws75.aptoide.com	Ireland	35,244,174.68	USA
11	5.62.36.56	United Kingdom	id.rlcdn.com	USA	apkrep.ns1.ff.avast.com	Czech Republic	65.9.52.144	USA
12	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	The Netherlands	52.85.48.221	USA	5.62.53.117	Czech Republic	download.apkpure.com	USA
13	www.petalsearch.com	France	52,154.69,245	USA	wv.inner-active.mobi	USA	104.26.4.35	USA

14	uc3.hispace.hicloud.com	Sweden	65.9.53.128	USA	wv.inner-active.mobi	USA	partner.googleadservices.com	USA
15	sdkserver-dre.op.hicloud.com	Sweden	104.21.35.78	USA	8.8.8.8	USA	pagead2.googlesyndication.com	USA
16	hwid-dre.platform.hicloud.com	Sweden	www.apkmonk.com	USA	test.quantcast.mgr.consensu.org	USA	142,250.74,100	USA
17	appdl-12-drcn.dbankcdn.com.akamaized.net	Sweden	104,197,172.31	USA	quantcast.mgr.consensu.org	USA	s0.2mdn.net	USA
18	appdl-12-dre.dbankcdn.com.akamaized.net	Sweden	partner.googleadservices.com	USA	auction.unityads.unity3d.com	USA	firebaseremoteconfig.googleapis.com	USA
19	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Thailand	142.250.74.35	USA	publisher-config.unityads.unity3d.com	USA	app measurement.com	USA
20	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Thailand	adservice.google.com	USA	www.datadoghq-browser-agent.com	USA	adservice.google.com	USA
21	appstore.huawei.com	Germany	142,250.74,100	USA	sdktm.w.inmobi.com	USA	firebase-settings.crashlytics.com	USA
22	80.158.2.189	Germany	142.250.74.102	USA	rules.quantcount.com	USA	142,250.74,136	USA
23	metrics2.data.hicloud.com	Germany	142.250.74.129	USA	104.21.35.78	USA	142,250.74,142	USA
24	80.158.16.161	Germany	142,250.74,130	USA	config.inmobi.com	USA	sync-tm.everesttech.net	USA
25	www.hicloud.com	Germany	um.simpli.fi	USA	142.250.74.2	USA	152.1992.21.230	USA
26	query.hicloud.com	Germany	172.67.29.206	USA	www.googletagmanager.com	USA	172.67.68.182	USA
27	grs.dbankcloud.com	Germany	tpc.googlesyndication.com	USA	partner.googleadservices.com	USA	172.217.20.33	USA
28	80.158.20.104	Germany	googleads4.g.doubleclick.net	USA	connectivitycheck.gstatic.com	USA	googleads.g.doubleclick.net	USA
29	jos.hicloud.com	Germany	www.gstatic.com	USA	firebaseinstallations.googleapis.com	USA	172.217.20.35	USA
30	iap.hicloud.com	Germany	172.217.21.161	USA	cdn.ampproject.org	USA	tpc.googlesyndication.com	USA
31	80.158.54.98	Germany	ade.googlesyndication.com	USA	adservice.google.com	USA	172.217.21.130	USA
32	appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	Germany	cm.g.doubleclick.net	USA	www.google.com	USA	www.gstatic.com	USA
33	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	Germany	192.48.236.3	USA	pagead googlehosted.lgoogle.com	USA	ade.googlesyndication.com	USA
34	160.44.194.86	Germany	pixel sync.sitescout.com	United Kingdom	142,250.74,130	USA	www.google.com	USA
35	160.44.199.4	Germany	openx2-match.dotomi.com	United Kingdom	firebase-settings.crashlytics.com	USA	172.217.21.166	USA
36	160.44.207.213	Germany	91,228.74.189	United Kingdom	softonic.map.fastly.net	USA	172.217.21.170	USA
37	appdl-4-drcn.dbankcdn.com	Germany	image6.pubmatic.com	United Kingdom	api.facebook.com	USA	172.217.22.162	USA
38	appdl-4-drcn.dbankcdn.com	Germany	188.125.94.206	United Kingdom	connect.facebook.net	USA	raw.githubusercontent.com	USA

39		81.171.20.104	The Netherlands	www.facebook.com	USA	216.58.207.206	USA
40		95,211,137,160	The Netherlands	cdn-mobile.aptoide.com	USA	www.gstatic.com	USA
41		ib.adnxs.com	The Netherlands	tpc.googlesyndication.com	USA	firebaseinstallations.googleapis.com	USA
42		store3.hispace.hicloud.com	Sweden	fonts.gstatic.com	USA	cm.g.doubleclick.net	USA
43		104.73.93.58	Sweden	pagead googlehosted.lgoogle.com	USA	216.58.211.130	USA
44		tls.adobe.com	Sweden	adservice.google.com	USA	ad.turn.com	United Kingdom
45		sdkserver-dre.op.hicloud.com	Sweden	fonts.googleapis.com	USA	185.29.135.233	United Kingdom
46		sdkserver-dre.op.hicloud.com.edgekey.net	Sweden	ads.mopub.com	USA	185.64.190.78	United Kingdom
47		j.mrpdata.net	Germany	ads.mopub.com	USA	212.82.100.176	United Kingdom
48		23,193,116,193	Germany	app measurement.com	USA	51.75.146.159	France
49		metrics2.data.hicloud.com	Germany	pixel.quantserve.com	United Kingdom	pixel.onaudience.com	France
50		platform.hicloud.com	Germany	185.64.190.78	United Kingdom	d-08.winudf.com	France
51		grs.dbankcloud.com	Germany	data.flurry.com	United Kingdom	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	3,666,135,160	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 investigation found that sending the application from Huawei's infrastructure redirected to third-party application repositories from which applications containing potentially malicious code were downloaded. Table 4 provides a summary of the security analysis of mobile applications downloaded to your Huawei device from Huawei's infrastructure. Security analysis was performed with the well-known file analysis tool VirusTotal[22].

4 lentele. Downloaded mob. Summary of applications after scanning with VirusTotal

Eil. No.	Applications name	Identifier	Applications version	VirusTotal score
1	Social Media	com.social.messenger.allinoneapps	14	*Malware equipment:* 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	*Malware equipment:* Adware / Loead Android.fyben.a

The study analyzed three mobile applications sent from Huawei's mobile application distribution infrastructure servers. According to a scan by VirusTotal, one antivirus system in the Social Media application found that the application contained potentially malicious software, A.gray.andrsca.f. After examining another mob. The Web Machinist Mobile Pro Tapping app, downloaded from Huawei's infrastructure servers, contained a potential virus, Trojan.Trojan.Banker.AndroidOS.Agent.ed, from one VirusTotal antivirus. This virus can carry[23] data theft of connections to banking systems. In the third application, Messenger All in One, two antivirus systems detected that the gadget was using potentially malicious software, such as the Adware / Loead and Android.fyben.a packages.

This is a major security concern for the device, as not all third-party application repositories perform checks on uploaded applications.

This infrastructure security vulnerability can be exploited by receiving original applications from *Google* Play Store after decomposing the application and making the necessary modifications to the content of the application decomposition by adding malicious code. The application code with malicious content is then compiled, packaged and signed with a new private key. The resulting modified application is uploaded to said third party application repositories. This process

22 VirusTotal information. *https://www.virustotal.com/gui/*
23 Clavister information. *https://www.clavister.com/advisories/antivirus/view/?id=544073*

associative scheme[24] presented in Figure 9.

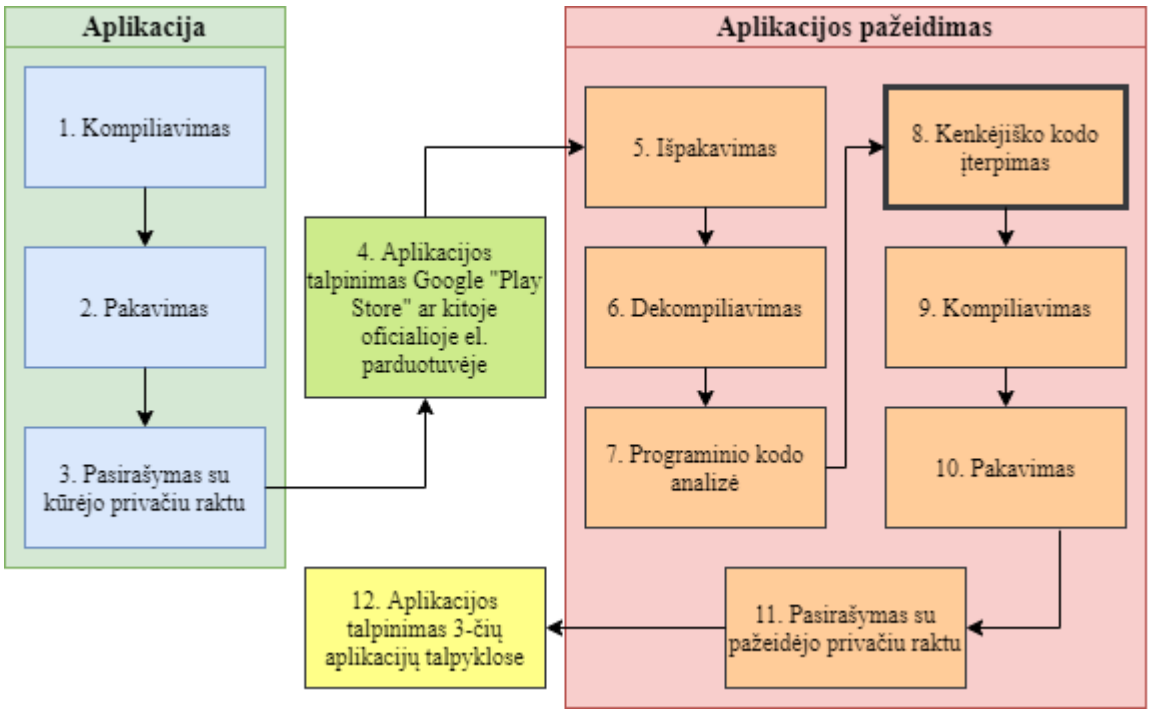


Fig. 9 Associative malware insertion into mob. application scheme

During application development, the application developer compiles the program code and thus forms a functioning application. This application is packaged in an installation file and signed with the application developer's private key. The signed installation file can be hosted in application stores, such as *Google* "Play Store.

The infringer, like all users of the application stores (except for the relevant regional restrictions), can download this application - upon receipt of the application from official sources, it is unpacked and decompiled into the application software code. This allows the infringer to perform its analysis, determine the viability of the malicious code installation site and the installation technology to be used, and install malicious code in the application. After the malware insertion procedures are completed, the application software code is compiled and packaged into an installation file that is signed by the infringer's private key. The generated malicious application installation file is hosted in third-party application repositories, which do not always check the hosted applications.

It has been found that e-mails containing viruses stores is a serious problem that is relevant to the developers of these stores[25]. A user who installs a viral application may suffer from data collection, leakage, or mob on the device or the associated cloud service. device damage.

The study found that some of the mobs in the tanks. applications are counterfeits of original applications that have malicious functionality or are infected with viruses - the user can download such applications and install them on the mob. phone, thereby compromising the security of the device and the data on it.

[24] Springer information. Repackaging Attack is an 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 turn to servers in third countries. This allows the collection and aggregation of user metadata based on which to monitor users

Software decomposition and traffic analysis showed that Mi Browser uses two data collection modules: Google Analytics and Sensors Data. Sensors Data is a Chinese-based, functional Google Analytics platform. According to Sensors Data[26], it has more than 1,500 customers, including China Telecom, Baidu, CYTS, Sichuan Airlines and others, the largest corporations in the People's Republic of China.

Google Analytics is an analytics platform for application authors or their administrators to obtain information that allows them to evaluate user usage of built applications in iOS, Android, or web environments.[27]. Google Analytics automatically generates an event log that allows you to evaluate the performance of the application. It is worth noting that the program developer has the technical ability to select the parameters to be analyzed, to determine the depth of their analysis.

It has been found that this module can collect data about user browsing, button presses etc., send information for possible analysis to Google servers. It should be noted that these modules are activated during the initial power-up of the device by agreeing to participate in the "Xiaomi User Experience program.

After decomposing the Xiaomi device's factory-built system applications, it was found that the functionality of these analytics programs was installed and running on the standard Xiaomi phone's Mi Browser. Table 5 shows a snippet of Mi Browser application code that identifies Google Analytics functionality.

Table 5. A snippet of code from the Mi Browser browser that identifies the functionality of Google Analytics

```
public static void reportAsync(String str, Map <String, Object> map) {
    if (! TextUtils.isEmpty (str) &&!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);
            }
        });
    }
}
```

The code snippet in the table implements the function of sending data to the analytics platform Firebase on Google servers. Table 6 shows the SensorData code snippet installed in the Mi Browser application. The code snippet contains a feature that launches the Sensors Data functionality in the Mi Browser application.

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

Table 6. A fragment of the Sensors Data launch code in the Mi Browser application

```
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.isBuildDebug(app
licationContext)). enableTrackScreenOrientation (false));
         SensorsDataAPI.sharedInstance() .identify (AnonymousID.get(applicationContext));
         setFlushNetworkPolicy(PrivacyAgreement.getInstance() .isApproved ());
         SensorsDataAPI.sharedInstance() .setSessionIntervalTime (10000);
         registerSuperProperties(applicationContext);
         SensorsDataAPI.sharedInstance() .unregisterSuperProperty (C4683v.f6510ae);
         SensorsDataAPI.sharedInstance() .unregisterSuperProperty ("new");
         logout();
         SensorsDataAPI.sharedInstance() .enableEncrypt (true);
         SensorsDataAPI.sharedInstance() .persistentSecretKey (new SensorsDataEncrypt.PersistentSecretKey() {
            public void saveSecretKey(SensorsDataEncrypt.SecreteKey secreteKey) {}

            public SensorsDataEncrypt.SecreteKey loadSecretKey() {
               return new SensorsDataEncrypt.SecreteKey (context.getString (R.string.abcdef), 1);
            }
         });
      } catch (Exception unused) {}

   }
}
```

It has been established that the Sensors Data module used in the device collects statistical information about the activity of the used applications for parameter 61 (application activation time, language used, etc.). See Table 7 for a list of data collected by Sensors Data.

7 tabe. List of parameter 61 to be collected by Sensors Data

No.	Parameters	Comment
1	log_miaccount	Is the user logged in
2	autocomplete_switch	Whether the AutoComplete feature is turned on
3	no_track_switch	Whether the Do Not Track function is on
4	bookmark_sync	Is bookmark sync with cloud turned on Is
5	history_sync	browsing sync with cloud turned on
6	feature_report_switch	Is the user participating in the “Xiaomi User Experience program
7	clear_history_switch	Whether to delete history when the app is turned
8	personal_service_switch	off Is app recommendations turned on
9	enhanced_incognito_switch	Whether the browser is running in Enhanced Incognito mode
10	system_out_of_ads	Whether Limit Ad Tracking is activated. This feature the device is not available to advertisers identifier
11	swipe_up	What function is registered for the swipe up action
12	current_default_search_engine	The current search engine used
13	language	The language set in the system

14	language_browser	The language set in the browser settings
15	icon_reddot_status	-
16	user_newsfeed	Whether the news feed is off
17	user_download_videos	-
18	user_night_mode	Does the browser use night mode
19	dark_mode	Does the system use night mode
20	user_data_save_mode	Is the data saving functionality activated in the browser
21	user_incognito_mode	Whether incognito mode is turned on
22	user_desktop_mode	User-agent browsers
23	user_checkbox_4G	Is it possible to perform browser updates via 4G
24	user_push_agree	Have activated browser notifications
25	user_facebook_notification	Can activate Facebook notifications in the browser
26	user_youtube_signin	Is the user signed in to YouTube
27	user_click_interest	Shows how many times the user clicked on the ones in the browser cards (news, YouTube recommendations, etc.)
28	user_login	Is the user logged in to Mi Account Is
29	adblock_switch	the ad blocking function activated?
30	adblock_show_notification	Is Adblock enabled
31	first_enter_newsfeed_way	Is the news feed window turned on for the first time
32	first_appstart_source	-
33	first_appstart_third_party	-
34	miui_personalised	Are personalized ads activated
35	personalized_services	Have personalized content recommendations activated
36	browser_ads	-
37	protection_type	-
38	app_boot_third_party	-
39	app_boot	Program activation time
40	feed_default_channel	-
41	experience_improve	Whether the Xiaomi User Experience feature is activated
42	platform	Platform. Always on Android
43	miui_version	MIUI version
44	log_miaccount	Is the user logged in to the Mi account
45	miui_region	Mi region
46	eid	-
47	apk_name	The name of the application APK
48	browser_install_referrer	-
49	autocomplete_switch	Is autocomplete activated in the search box
50	no_track_switch	Whether the Do Not Track function is on
51	bookmark_sync	Is bookmark synchronization with the Mi server enabled?
52	history_sync	Is your browsing history synced to Mi server
53	feature_report_switch	Is the user participating in the “Xiaomi User Experience program
54	clear_history_switch	Whether to clear the browsing history when the app is turned
55	personal_service_switch	off Is the user recommendations functionality enabled - personalized YouTube clips, etc.
56	enhanced_incognito_switch	Is incognito enabled

57	user_tab_news	Has the user enabled the news window
58	user_tab_games	Has the user enabled the games window
59	search_optimization_switch	Constant, always equal to 1
60	cookie_status	Provides data about the user's cookie settings Specifies
61	subscription	whether a VPN is used and, if so, its identifier.

The study performed a complete decoding and decryption of Xiaomi's encrypted messages. The Xiaomi phone is set to send Sensors Data data to a Base64-encoded data set, which is additionally encoded using *urlencode* algorithm. An example of a fragment of encoded data to be sent is given in Table 8.

Table 8. A snippet of data sent by a Xiaomi phone

zzvhrYfjw6d% 2FA8RXtmQLWd2RTDyUWp5DBsFc55eI9yBbDROnrH12GSpq8SRDUtymJ8PquOrUqpsI
Dg6qsvSg% 2FksVvDG3gcl6SWzk9uL4hWhOCpEw% 2B% 2BzMBq0KCtqdOkn4kljhDgtCfdRixfrJe8PHTjr
8x1cK5xMHHlSL0MK% 2FWu3utqKnuhf1UQGi64uYDCp% 2FeEZ1MdakDE% 2BLXsF4wZKGiftO64% 2
B8liP1NvxVl% 2BsgTutVEbroI% 2FWJUJkz9MfZyvL6OAPG6z9rRbJ354mUo6% 2BOMwZdN% 2BAuWSz
Rz8IKqITU6HwNZGMB0xmPDB8tSTM7ehnya% 2FyAiHPqOIXD7lYzrvupBJTrZLCXLQzbTgIxtZGL65
KvV7yfgiwMhCxY% 2Bkg0t3d0LXljOOrQqFfsqdJW% 2B6LnWvE6lKdm7% 2BCPydhautVIgiMSZDi94iH%
2FuYL% 2B2dkmYSLxSjQFQh51FSBA% 2BygRzfCItmL87KjFjgT0t3% 2BmtvO% 2Bs93lH72rC6ai0Y5k
dIIdSuIg6A% 2BomC73JYOeHygMR0jmjCjM5% 2FiUANqsHXPfeoaGBn8F% 2FV1vik03CPbetK3yzfwLn
9ZpmkmzO64Ic% 2BEsRNTgNk7jc0mKZrsisWs4IPO1e

Table 9 shows the decoded content of the data sent by the Xiaomi phone to the Sensors Data content in Singapore. Data sent for analysis - application version, application name, current region, device manufacturer, etc.

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

{
"_track_id": 1687170607,
"time": 1623852507838,
"type": "track",
"distinct_id": "7d03ab71-91b1-47ca-8f56-0ce2d77f6c86",
"lib": {
"$ lib": "Android"
"$ lib_version": "4.0.3-pre", "$
app_version": "12.4.1-g", "$
lib_method": "code",
"$ lib_detail": "com.android.browser.BrowserActivity ######"
},
"event": "$ AppStart",
"properties": {
"$ lib": "Android"
"$ os_version": "10",
"$ lib_version": "4.0.3-pre",
"$ model": "M2007J3SY",
"$ os": "Android",
"$ screen_width": 1080
"$ screen_height": 2400, "$
manufacturer": "Xiaomi", "$
app_version": "12.4.1-g",
"platform": "AndroidApp",

```
    "miui_version": "V12.0.18.0.QJDEUXM",
    "log_miaccount": 0,
    "miui_region": "LT",
    "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,
    "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": "",
    "$ wifi": true,
    "$ network_type": "WIFI", "$
    resume_from_background": true, "$
    is_first_time": false,
    "$ screen_name": "com.android.browser.BrowserActivity", "$
    title": "Mi Browser",
    "$ is_first_day": true
  }
}
```


It has been determined that Sensors Data data is being sent to an Internet address *https://sa.api.intl.miui.com*. Table 10 presents the information characterizing the network transmissions analytical data to servers in Singapore.

Table 10. Characteristics of the data sent by Sensors Data

Eil. No.	IP address	Sent data *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 via encrypted channel to Xiaomi servers in Singapore, which is not covered by the General Data Protection Regulation. It can be argued that the potentially excessive collection and use of analytical data poses a threat to the privacy of personal data.

Figure 10 shows the Sensors Data data encryption mechanism used in the research to establish a data connection between the device and servers in Singapore.

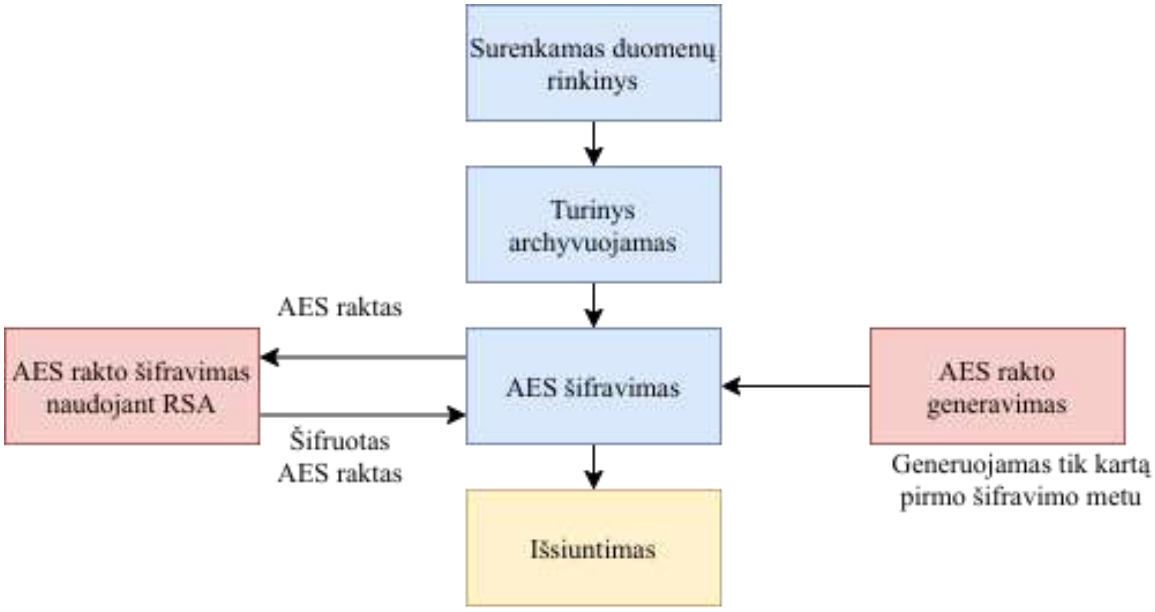


Fig. 10 "Xiaomi uses a data encryption mechanism

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

This is done to reduce the amount of data sent. The obtained result is encrypted with AES128-CBC algorithm. The key is generated using the device's pseudo-random number generator. The key used in the AES encryption is then encrypted using the RSA algorithm using a public key downloaded from the Xiaomi servers. The resulting set is packaged into a JSON object and sent to servers in Singapore.

Application, invites features *registerSuperProperties* and *registerDynamicSuperProperties*. These functions are responsible for data collection and preparation of JSON objects. It can be argued that the encryption mechanism used by Sensors Data ensures a relatively high level of data security when transmitting it to analytics servers located in Singapore.

The Google Analytics module installed on the device allows you to read the browsing history of Mi Browser, search results and other application performance parameters, send this data to analytics servers. Data is sent over an encrypted TLS channel using Protobuf encoding. Decoding data without a Protobuf configuration file is impossible or difficult to implement, but some data can be seen in the encoded stream: a web address opened in Mi Browser, data entered in a search box, or a user action (such as a click on a search box).

This data can be accessed and used by Xiaomi application developer[28]. Encrypted outgoing The snippet of data that is sent to Google Analytics servers is shown in Table 11.

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

Table 11. An encrypted snippet of data sent by the Xiaomi device to Google Analytics servers

```
event_network r: LT | wifi
durationr: LT | 285
_oapp
_scBrowserActivity
_siçÈ¾å ° òT "
urlr: LT |https://nksc.lt/¢þ¦¡/ ý¦¡ / ¯

event_network r: LT | wifi
if_remind
r: LT | remind
languager: LT | en
is_system_languager: LT | 1
sourcer: LT | search_icon
_oapp
op r: LT | show
_scBrowserActivity
_siçÈ¾å ° òTweb_translate_op² »ý¦¡ / ñ®ý¦¡ /

event_network r: LT | wifi enter_wayr:
LT | searchBar_website _oapp

_scBrowserActivity
_siçÈ¾å ° òTimp_search_pageÌæý¦¡ / Æ½ü¦¡ / ú

event_network r: LT | wifi
durationr: LT | 323
_oapp
_scBrowserActivity
_siçÈ¾å ° òT
urlr: LT |https: //kam.ltæ¬þ¦¡/ ¢ þ¦¡ /
```

Table 12 presents the information that characterizes the analytical data transmitted by the Xiaomi network to Google Analytics servers.

Table 12. Characteristics of the data sent to Google Analytics

Eil. No.	IP address	Sent data *B*	Data received *B*	Total data *B*	State
1	142,250.74,110	2545	0	2545	USA
2	172.217.16.14	1282		1282	
3	216.58.207.206	12699		12699	

Based on the findings, Xiaomi collects a relatively large amount of information about the processes running on the device, the behavior of installed software packages, user actions performed, and application configuration parameters. Two analytical systems are used to implement this process - Sensors Data and Google Analytics. A review of the sources found that Xiaomi devices collect a wider range of data compared to other mobs. facilities

manufacturers[29,30,31].

It can be argued that the potentially excessive collection and use of analytical data poses a threat to the privacy of personal data.

3. The Xiaomi device implements functionality that can limit the free flow of information availability

It was found that during the initialization of the system applications pre-installed on the Xiaomi Mi 10T, these applications contact the server in Singapore at Globalapi.ad.xiaomi.com (IP address 47.241.69.153) and downloads the JSON file MiAdBlacklistConfig, saves this file in the application metadata directories. See Table 13 for a list of applications for which a MiAdBlacklistConfig file was found in the metadata directories. Table 13. Mob. A list of applications that use the MiAdBlacklistConfig file

Eil. No.	Applications 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*	

When applications download a file, the download date is fixed in order to update the list periodically. The download scheme for 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/*

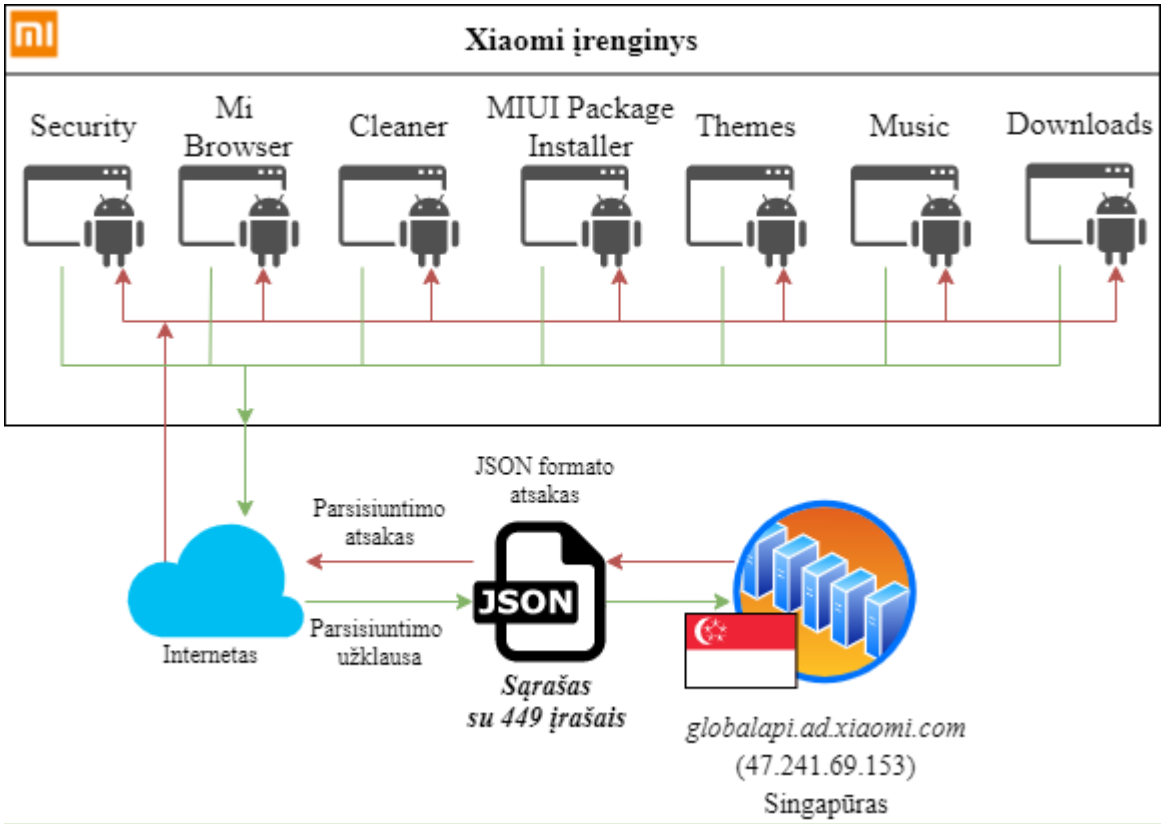


Fig. 11 MiAdBlacklistConfig file download scheme

This file contains a list of names, names and other information of various religious and political groups and social movements (during the investigation).
449 entries were recorded in the MiAdBlacklistConfig file). Files
The MiAdBlacklistConfig snippet is shown in Table 14.

Table 14. A snippet of the MiAdBlacklistConfig file

Eil. No.	Original	Rating
1	"宗教 虔信 者阵线 ",	Front of Religious Believers
	...	
22	"西藏 自由",	"Tibet is free",
	...	
60	"蒙古 独立",	"Mongolian Independence",
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-Qaeda in the Islamic Maghreb
204	"人民报 ",	People's Daily,



205	"巴勒斯坦 解放组织 ",	Palestine Liberation Organization,
	...	
313	"台独 万岁 ",	"Long live Taiwan's independence",
	...	
369	"美国之音",	The Voice of America
	...	
420	"89运动 ",	"Movement 89"
	...	
449	"夏米斯丁艾 合 麦提·阿布 都 米吉提 "	Xia Misteen Ahemet Abu Dumijiti

After Xiaomi application code analysis, was found that applications are realized software classes for filtering the target multimedia displayed on the device according to the downloaded list in the MiAdBlacklistConfig file. A snippet of this program code is given in Table 16.

Table 16. The Xiaomi device uses a snippet of content filtering code

```
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 && m12161a(iNativeAd.getAdTitle (), str)) {MLog.m6439d (
            "MiAdBlacklistConfig", "Ads:" + iNativeAd.getAdTitle () + "is blocked by title word:" + str);

            if (aVar! = null) {aVar.
                f11165a = str;
            }
            this.f11161c = str;
            return true;
        } else if (iNativeAd.getAdBody ()! = null && m12161a(iNativeAd.getAdBody (), str)) {MLog.m6439d (
            "MiAdBlacklistConfig", "Ads: [" + iNativeAd.getAdBody () + "] is blocked by desc word:" + str);

            if (aVar! = null) {aVar.
                f11165a = str;
            }
            this.f11161c = str;
            return true;
        }
    }
    MLog.m6443i ("MiAdBlacklistConfig", "isAdsBlocked-> totalTime =" + (System.currentTimeMillis () -
currentTimeMillis) + "& threadId =" + Thread.currentThread (). GetId ());
    return false;
}
```

An application's Mi Browser software decomposition study found that the application performs MiAdBlacklistConfig file download functionality, but does not perform content filtering based on the list in the MiAdBlacklistConfig file. According to the Xiaomi software code, this functionality is deactivated in the "Region of the European Union". Applications “Mi
The event logging content generated by the Browser is presented in Table 17.

Table 17. Event log content generated by Mi Browser

Eil.	Functions	Parameter 1	Parameter 2

No.	name		
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 "," mMiuiVersion ":" 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, "mIsBid ": 0}
24	i:	MIADSDK	Personalized ad is disabled in EU region, reporting is not allowed
25	i:	MIADSDK	Personalized ad is disabled in 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 "," mMiuiVersion ":" V12.0.18.0.QJDEUXM ", "mRegion": "LT", "mTriggerId": "9d1f86e3-579e-4110-b71e-065f520c1fa3 "," mInstaller ":" com.xiaomi.discover "," mIsPreInstall ": 0," mChildren ": 0," mIsBid ": 0," mCost ": 333682}

It is believed that this functionality allows the Xiaomi device to analyze the target multimedia content entering the phone - looking for keywords based on the information received from the server. *"MiAdBlacklist* list.

When content is found to contain searchable keywords, the device filters that content and the user cannot see it. The principle of data analysis allows to analyze not only the words written in hieroglyphs - the list regularly sent from the server can be formed in any language. It is important to note that this functionality is activated remotely by the manufacturer. It is believed that the existence of such functionality may threaten the free access to information, limit its availability. It can be said that this is important not only for Lithuania, but also for all countries that use Xiaomi devices.

4. On Xiaomi devices, you need to register a SIM to sign up for the Cloud card. Outgoing messages are not displayed on the phone. Risk of user data leakage

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

When a user first attempts to connect to the Xiaomi Cloud Service, the device requires that they log in to (1) the Xiaomi Account. After entering the login details and successfully logging in to the account, an options window (2) is displayed, where you can enable and disable the main features of Xiaomi Cloud, such as data synchronization and device geolocation in case of device loss.

After selecting the standard functions, the service running in the background mode on the device starts the SIM card data collection procedures (3, 4 and 5). When the service completes the SIM card data collection procedures, the user is presented with an information window (6) stating that in order to enable call history and message synchronization functionality, the device must send an SMS message to verify the phone number.

The information window also indicates that the user may be charged for standard mobs for sending an SMS message. connection provider rates. When the user closes the information window, the user is presented with an operating system window (7), which asks the user whether to allow the SIM card registration service to automatically send SMS messages. With the consumer's consent, an automatic telephone number registration procedure is initiated (8).

Device from **general** the service server downloads the procedure configuration data structure, which contains the address of the server with which further network communication takes place, the telephone number of the SMS recipient and other parameters. The device then generates an SMS message and sends it 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 saved in the internal service database (10). When an SMS message is sent, its contents are encrypted and sent to the service server whose address is specified in the configuration data structure, together with a registration confirmation request (11).

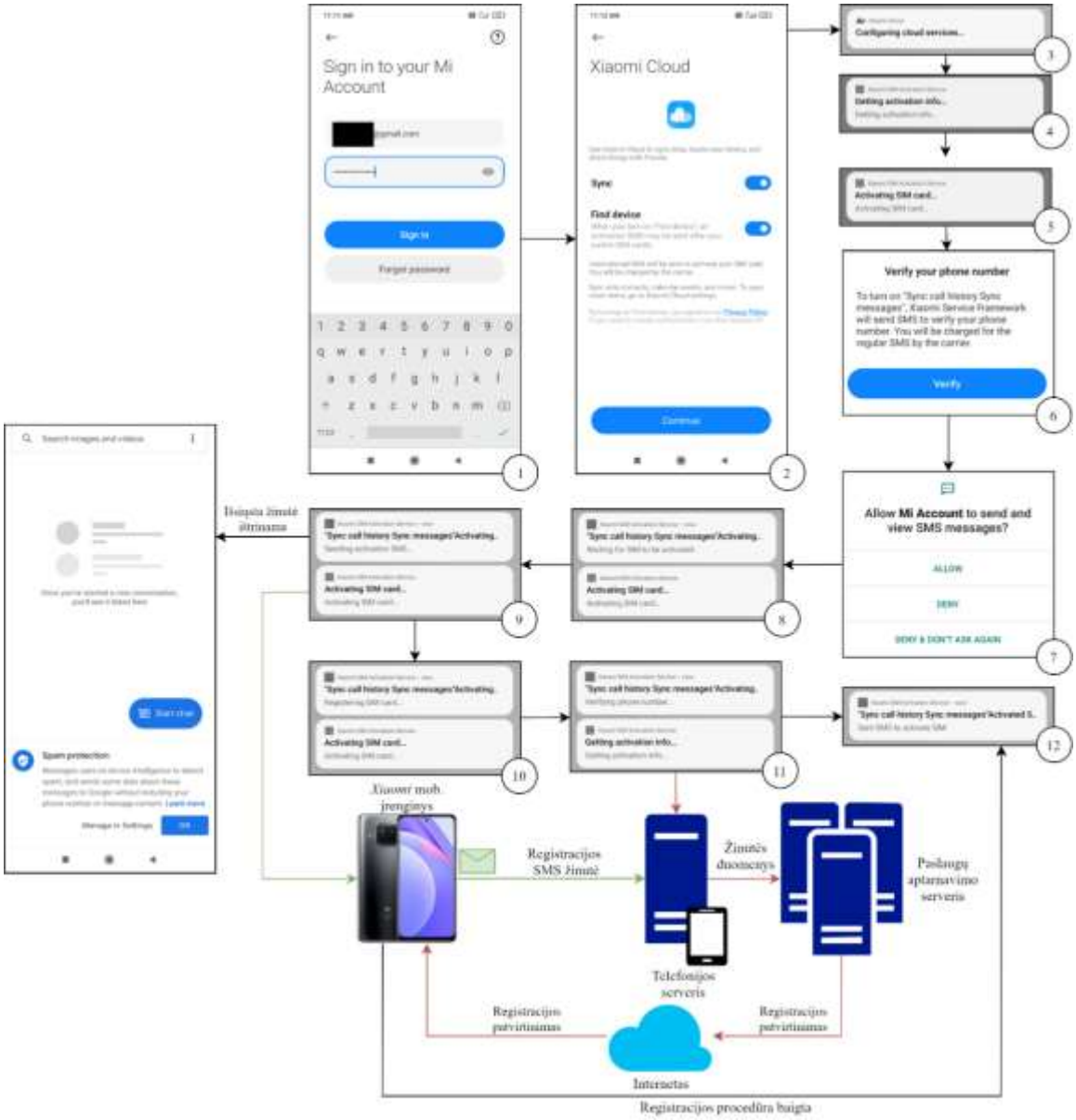


Fig. 12 The phone is undergoing a registration process with Xiaomi Cloud Services at the time of shipment SMS message

When the device sends a registration request to the service server, it receives a request response from it indicating the result of the registration (positive or negative) (12).

It is established that the registration of a telephone number is performed regardless of how the user chooses to be authenticated - by telephone number or e-mail. email address. It is important to note that an encrypted SMS message has been sent and its contact is not visible to the user. During the study, messaging was not fixed when the Xiaomi Cloud service functionality was turned off. A more detailed network flow diagram is shown in Figure 13.

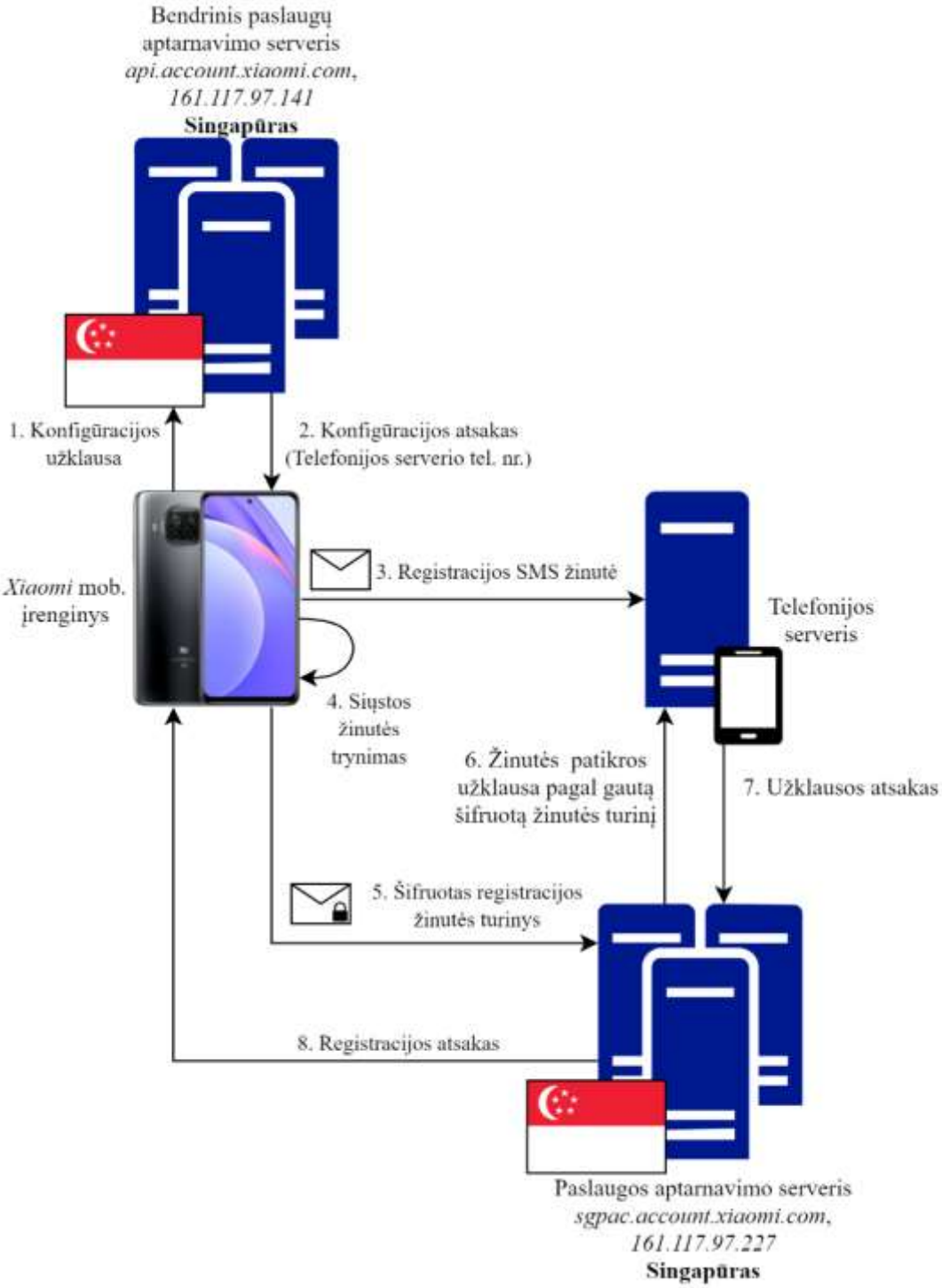


Fig. 13 Scheme of registration with Xiaomi cloud services network

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

(5). The service server communicates with the telephony server to which the SMS message was sent (6, 7). During the communication, the message sent by telephone and the encrypted message content sent via the mobile Internet network are checked. Upon successful completion of the message check, a request response is formulated for the device, appending the result of the registration (8).

It is important to note that if no SIM card is inserted in the device during registration, the registration process is aborted and an error message is displayed on the device screen.

Before the device sends a phone number registration SMS, the device contacts a shared service server in Singapore with the address "api.acount.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 contains the telephone number of the telephony server, the address of the service server and other data. An excerpt of the network communication between the device and the shared service server is provided in Table 18.

Table 18. Configuration download network traffic snippet

GET / pass / configuration HTTP / 1.1
Content-Type: application / x-www-form-urlencoded
User-Agent: Dalvik / 2.1.0 (Linux; U; Android 10; M2007J3SY MIUI / 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, "data": {"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 to the phone number specified in the configuration data structure.

An investigation by the Xiaomi SIM Activation Service of the telephone number registration service revealed that the device is performing the function of sending an automatic SMS message. The recipient of the SMS message and the content of the message are shown in Figure 14.



Fig. 14 SMS message content and sending process

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

An excerpt of the code for sending an SMS message is given in Table 19.

Table 19. A snippet of code for sending an SMS message

```
public void sendTextMessage(int i, String str, String str2, String str3, PendingIntent pendingIntent,
PendingIntent pendingIntent2) {
    try {
        Class <?> cls = Class.forName ("miui.telephony.SmsManager"); Objectinvoke = 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 ("MiuiSysImpl", "successfully send text message");
    } catch (NoSuchMethodException e) {
        Log.e ("MiuiSysImpl", "error when send text message: NoSuchMethodException", e);
        throw new RuntimeException (e); }
    catch (IllegalAccessException e2) {
        Log.e ("MiuiSysImpl", "error when send text message: IllegalAccessException", e2);
        throw new RuntimeException (e2); }
    catch (InvocationTargetException e3) {
        Log.e ("MiuiSysImpl", "error when send text message: InvocationTargetException", e3);
        throw new RuntimeException (e3); }
    catch (ClassNotFoundException e4) {
        Log.e ("MiuiSysImpl", "error when send text message: ClassNotFoundException", e4);
        throw new RuntimeException
    (e4); }catch (SecurityException e5) {
        ActivateLog.m24w ("MiuiSysImpl", "sendTextMessage", e5);
    }
}
```

It is worth noting that the above-mentioned external software class "miui.telephony.SmsManager" has a realizing functionality that allows to perform the functions of deleting SMS messages. SMS sending, deleting and other functions implemented in an external software class Miui.telephony.SmsManager is shown in Figure 15.

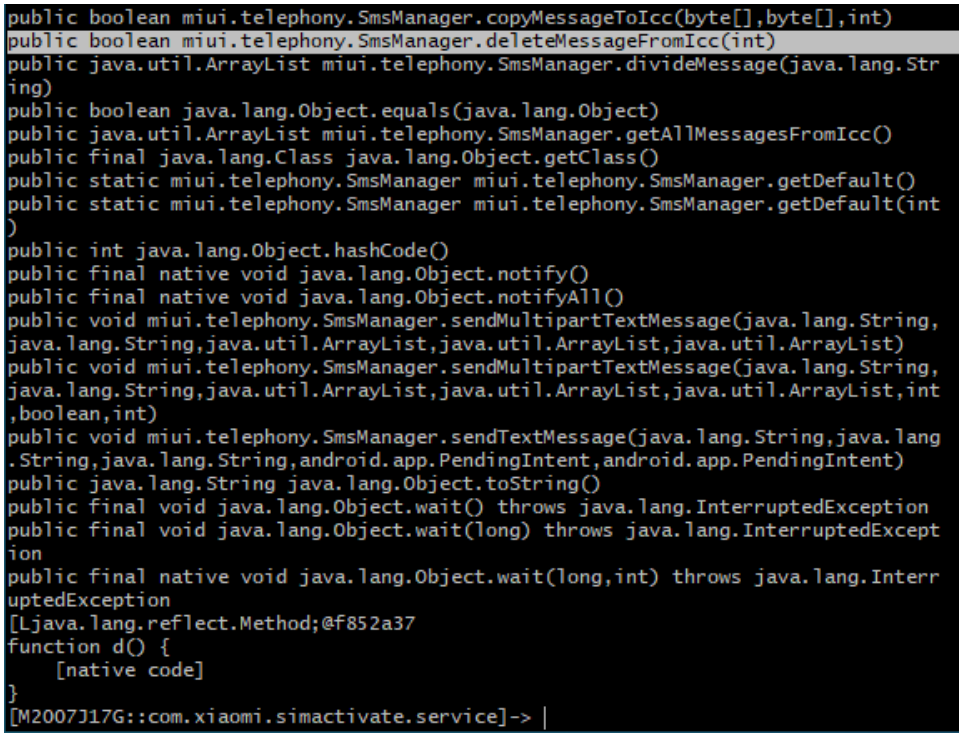


Fig. 15 Sending, deleting SMS messages, etc. functions implemented in an external software class Miui.telephony.SmsManager

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 sgpac.account.xiaomi.com (Singapore).

The server checks the content according to the received encrypted data with the SMS message data received by the telephony server and sends the activation result to the mobile device. A statement of network traffic is given in Table 20.

Table 20. Communication with the service 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 MIUI / V12.0.18.0.QJDEUXM) APP / unknown MK / TWkgMTBU
Cookie: sdkVersion = accountsdk-01.01.2015
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_5ODSHBbJv5XO6wRTIUfNCEerj978hkm5RhLrK19IYsgPUe VQoXbYJ9Di8-
B9WaMvgJeAVwudc_nYD9LWJw28g8UO1Y_5A9V1kqzNCf8e1tfLftN_Y0UXpvy4cXlzHISL5yiGj2sI77KFzS20PgK
focTxNcleEuLlTEjTY_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, "data": {}, "description": "....."}

The investigation found that the device was communicating with servers located in Singapore. A list of fixed communications is given in Table 21.

Table 21. Communication with servers located in Singapore

Eil. No.	Domain	Address	Data Baitai	State	Purpose
1	api.account.xiaomi.com	161,117.97,141	9200	Singapore	**General service server** *From server phone sent configuration for authentication - SMS tel. No, service server address, etc.*
2	sgpac.account.xiaomi.com	161,117.97,227	48990	Singapore	**Service server** *According to the SMS received from the phone message is generated and sent to the phone registration response.*

The IP addresses for the api.account.xiaomi.com and sgpac.account.xiaomi.com domains are registered with Alibaba.com Singapore E-Commerce Private Limited. Alibaba is an information technology company. established in the People's Republic of China. Chinese IT companies are known to be obliged to pass on any kind of managed information to the Chinese government or its agencies.[32].

Automated messaging and cryptographic functionality poses potential threats to the security of the device and personal data, allowing device data to be collected and transmitted to remote servers without the user's knowledge.

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