NKSC prie KAM
Inovacijų ir mokymo skyrius
support@ims.nksc.lt

2021 – 08 – 23

Lietuvoje tiekiamų 5G ryšio technologiją palaikančių mobiliųjų įrenginių kibernetinio saugumo vertinimas

GAMINTOJŲ „Huawei“, „Xiaomi“ ir „OnePlus“ PRODUKCIJOS ANALIZĖ

Įžanga

Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos siekdamas užtikrinti saugios programinės ir aparatinės įrangų naudojimą šalies viduje, atliko įvairių gamintojų Lietuvoje tiekiamų 5G ryšio technologiją palaikančių mobiliųjų įrenginių kibernetinio saugumo vertinimą. Šioje analizėje pateikti gamintojų „Huawei“, „Xiaomi“ ir „OnePlus“ išmaniųjų mobiliųjų telefonų vertinimo rezultatai.

„Huawei“, „Xiaomi“ ir „OnePlus“ – Kinijos informacinių technologijų ir plataus vartojimo elektronikos gamybos bendrovės, veiklą vykdančios tarptautiniu mastu[1] ir užimančios stiprias pozicijas Europos rinkoje[2]. 2020 m. šie gamintojai Lietuvos rinkai pristatė penktos kartos 5G mobiliojo ryšio technologiją palaikančius išmaniuosius mobiliuosius telefonus. Saugumo vertinimas buvo atliktas plačiai prieinamiems „Huawei P40 5G“[3], „Xiaomi Mi 10T 5G“[4] ir „OnePlus 8T 5G“[5] mobiliesiems įrenginiams. Tyrime nagrinėtų įrenginių vaizdai patekti 1 paveiksle.

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

1 pav. Tyrime nagrinėti įrenginiai. Priekinės ir galinės panelių vaizdai

[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. „Huawei P40 5G“ techniniai parametrai. *https://consumer.huawei.com/en/phones/p40-pro/specs/*

[4] Xiaomi. „Xiaomi Mi 10T 5G“ techniniai parametrai. *https://www.mi.com/global/mi-10t-pro/specs/*

[5] OnePlus. „OnePlus 8T 5G“ techniniai parametrai. *https://www.oneplus.com/lt/8t/specs*

Nepaisant šių prekinių ženklų žinomumo, korporacijos 2017 – 2021 metų laikotarpyje susidūrė su kuriamos įrangos saugumo iššūkiais – remiantis pažeidžiamumų duomenų bazių (angl. Common Vulnerabilities and Exposures – CVE) informacija, „Xiaomi“ produkcijoje fiksuoti 9 pažeidžiamumai[6] susiję su asmens duomenų nutekinimo rizikomis (8 iš šių pažeidžiamumų gali būti realizuoti nuotoliniu būdu), „Huawei“ produkcijoje per šį laikotarpį fiksuoti 144 pažeidžiamumai[7] (2020 m. buvo fiksuoti 28 pažeidžiamumai, 2021 m. I pusmetį – 23) kurių dauguma buvo susijusi su įrenginių funkcionalumo trikdymu, „OnePlus“ 2020 m. buvo fiksuotas 1-nas pažeidžiamumas[8] leidęs atakuotojui panaudojus trečiųjų šalių programinę įrangą iš mobilaus įrenginio siųsti SMS žinutes, kai mobilusis įrenginys yra užrakintas.

Įvairų šaltinių vertinama, kad šie gamintojai užima lyderiaujančias pozicijas[9,10] mobiliųjų įrenginių rinkoje, jų platus asortimentas, plėtojamos naujos technologijos ir pastebimas augimas Lietuvoje yra neabejotinas kibernetinio saugumo tyrimų objektas.

Tyrimo išvados

Atlikus gamintojų „Huawei“, „Xiaomi“ ir „OnePlus“ mobiliųjų įrenginių dekompozicijos tyrimus buvo nustatyta 10 kibernetinio saugumo rizikas didinančių faktų. Šiame kibernetinio saugumo vertinime analizuojamos nustatytos 4 kibernetinio saugumo rizikos, susijusios su bendruoju įrenginiuose gamykliškai įdiegtų aplikacijų saugumu, asmens duomenų nutekėjimo grėsmėmis, ir žodžio laisvės ribojimais. Numatyta neaptartas kibernetinio saugumo rizikas detalizuoti kitose šio kompleksinio tyrimo dalyse ir jų vertinimą pateikti iki 2021 m. pabaigos. Šiame tyrime nagrinėjamos su asmens duomenų saugumu susijusios problemos.

Atlikus analizę nustatyta, kad Huawei įrenginiuose naudojama mobiliųjų aplikacijų diegimo procedūra pasižymi kibernetinio saugumo neapibrėžtumais. Mob. aplikacijų diegimui Huawei telefonuose yra naudojama gamintojo parengta infrastruktūra, kurią sudaro oficiali elektroninė aplikacijų parduotuvė „AppGallery“ ir periferinės aplikacijų talpyklos.

Vartotojui diegiant mob. aplikaciją Huawei įrenginyje, jos yra ieškoma „AppGallery“ parduotuvėje, aplikaciją radus, ji yra parsiunčiama ir įdiegiama į mob. įrenginį. Tačiau aplikacijos neradus oficialioje parduotuvėje, vartotojas automatiniu būdu yra nukreipiamas į periferines aplikacijų talpyklas, iš kurių mob. aplikacija atsiunčiama į mob. įrenginį diegimui. Verta pažymėti, kad dauguma aplikacijų talpyklų yra šalyse, kuriose netaikomas Bendrasis duomenų apsaugos reglamentas, dėl to kyla gretutinės vartotojų metaduomenų nutekėjimo rizikos. Atliktame tyrime buvo nustatyta, kad dalis talpyklose esančių mob. aplikacijų yra originalių aplikacijų padirbiniai, turintys kenkėjišką funkcionalumą ar užkrėsti virusais – vartotojas tokias aplikacijas gali atsisiųsti ir įsidiegti į mob. telefoną, taip sukeliant grėsmę įrenginio ir jame esančių duomenų saugumui.

Duomenų saugumo rizikos nustatytos ir Xiaomi įrenginyje – gamykliškai įdiegtos sisteminės aplikacijos siunčia statistinius tam tikrų įrenginyje įdiegtų aplikacijų veiklos duomenis į Kinijos debesijos paslaugų teikėjo Tencent serverius, kurie išsidėstę Singapūre, JAV, Nyderlanduose, Vokietijoje ir Indijoje.

---

[6] CVE duomenų bazė. Viešai skelbiami „Xiaomi“ produkcijos pažeidžiamumai. *https://www.cvedetails.com/vulnerability-list/vendor_id-19038/MI.html*

[7] CVE duomenų bazė. Viešai skelbiami „Huawei“ produkcijos pažeidžiamumai. *https://www.cvedetails.com/vendor/5979/Huawei.html*

[8] CVE duomenų bazė. Viešai skelbiami „OnePlus“ produkcijos pažeidžiamumai. *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/*

Buvo nustatyta, kad originali įrenginio naršyklė „Mi Browser“ naudoja du duomenų rinkimo modulius: „Google Analytics“ ir „Sensor Data“. Įrenginyje įdiegtas „Google Analytics“ modulis leidžia perskaityti naršymo ir paieškos istoriją, siųsti šiuos duomenis į analitikos serverius, prie kurių prieina ir duomenis naudoja „Xiaomi“[11]. Šis funkcionalumas yra aktyvuojamas mob. telefoną priregistravus į „Xiaomi User Experience“ rinkodaros programą. Pagal nutylėjimą, tai automatiškai yra atliekama telefono pirmojo įjungimo arba gamyklinių parametrų atstatymo metu.

Nustatyta, kad įrenginyje naudojamas „Sensor Data“ modulis renka 61-o parametro (aplikacijos įjungimo laikas, naudojama kalba ir kt.) statistinę informaciją apie naudojamų aplikacijų veiklą. Surinkti statistiniai duomenys šifruotu kanalu siunčiami į Xiaomi serverius Singapūre, kuriame nėra taikomas Bendrasis duomenų apsaugos reglamentas. Tarptautinių šaltinių teigimu, buvo nustatyti aiškūs Xiaomi neautorizuotų vartotojų duomenų rinkimo atvejai[12,13]. Galima teigti, kad potencialiai perteklinis analitinių duomenų rinkimas ir naudojimas kelia grėsmes asmens duomenų privatumui.

Taip pat nustatyta, kad vartotojui pasirinkus naudoti Xiaomi debesijos paslaugas, yra vykdoma vartotojo mob. telefono numerio registracija Singapūre esančiuose serveriuose. Tai atliekama įrenginiui į specialų telefono numerį išsiuntus šifruotą SMS žinutę. Tarnybinė stotis, gavusi SMS žinutę, ją sinchronizuoja su Xiaomi serveriu Singapūre, iš kurio telefonas mob. interneto ryšiu atsisiunčia patvirtinimą, leidžiantį vartotojui jungtis prie Xiaomi debesijos paslaugos. Nustatyta, kad telefono numerio registravimas yra vykdomas, nepriklausomai, kaip vartotojas pasirenka būti autentifikuotas – pagal telefono numerį ar el. pašto adresą. Svarbu pažymėti, kad išsiųsta šifruota SMS žinutė ir jos adresatas vartotojui nėra matomas.

Automatizuotas žinučių siuntimas ir jų slėpimo programinis funkcionalumas kelia potencialias grėsmes įrenginio ir asmens duomenų saugumui – šiuo būdu, vartotojui nežinant, gali būti renkami ir perduodami įrenginio duomenys į nutolusius serverius.

„Xiaomi Cloud“ debesijos paslauga yra skirta įrenginyje saugomų duomenų (kontaktų knygoje išsaugotų duomenų, skambučių istorijos, SMS žinučių, nuotraukų, užrašų, Wi-Fi nustatymų ir naršymo istorijos ir kt.) talpinimui bei sinchronizavimui nutolusiuose serveriuose – naudojantis šia paslauga, vartotojų duomenys siunčiami į tarnybines stotis, esančias Singapūre.

Nustatyta, kad Xiaomi sisteminės aplikacijos (Security, MiBrowser, Cleaner, MIUI Package Installer ir Themes) iš Singapūre esančio serverio reguliariai atsisiunčia gamintojo atnaujinamą konfigūracinę rinkmeną „MiAdBlacklistConfig“. Šioje rinkmenoje saugomas sąrašas, kurį sudaro įvairių religinių ir politinių grupių bei visuomeninių judėjimų pavadinimai, vardai ir kita informacija (tyrimo metu „MiAdBlacklistConfig“ rinkmenoje buvo fiksuoti 449 įrašai). Atlikus Xiaomi aplikacijų kodo analizę, buvo nustatyta, kad aplikacijose yra realizuotos programinės klasės, skirtos įrenginyje atvaizduojamos tikslinės multimedijos filtravimui pagal atsisiųstą *„MiAdBlacklistConfig“* sąrašą.

Tai leidžia Xiaomi įrenginiui vykdyti į telefoną įeinančio tikslinės multimedijos turinio analizę – ieško reikšminių žodžių pagal iš serverio gautą *„MiAdBlacklist“* sąrašą. Užfiksavus, kad turinyje yra ieškomų reikšminių žodžių, įrenginys šį turinį blokuoja. Manoma, kad šis funkcionalumas gali kelti potencialias grėsmes laisvam informacijos prieinamumui.

NKSC prie KAM rekomenduoja vartotojus domėtis naudojama programine ir aparatine įrangomis, atsakingai vertinti siūlomą įrangos funkcionalumą.

[11] Xiaomi. Privatumo politika. *https://privacy.mi.com/all/en_IN/*
[12] Forbes informacija. *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 informacija. *https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/*

Platesni tyrimų rezultatai

Tyrime dalyvavusių mobiliųjų įrenginių pagrindinės programinės charakteristikos, pažymint operacinės sistemos (OS) pagrindą, operacinės sistemos pagrindo gamintojo modifikaciją, operacinės sistemos branduolio versiją ir saugos atnaujinimų datas pateiktos 1 lentelėje.

1 lentelė. Tyrime dalyvavusių mobiliųjų įrenginių pagrindinės programinės charakteristikos

Įrenginio pavadinimas	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
Gamykliškai įdiegtos OS pagrindas	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Gamykliškai įdiegtos OS pagrindo gamintojo modifikacija	EMUI 10.1.0	MIUI Global 12.0.10 (QJDEUXM)	Oxygen OS 11.0.5.6.KB05BA
Naujausios galimos OS pagrindas	Android 10	Android 11	Android 11
Naujausios galimos OS pagrindo gamintojo modifikacija	EMUI 11.0.0.151 (C432E5R5P3)	MIUI Global 12.0.2.0 (RJSEUXM)	Oxygen OS 11.0.8.13.KB05AA
Naujausios galimos OS išleidimo data	2020-12-24	2021-05-25	2021-04-08
OS branduolio versija	4.14.116	4.19.81-pref-gef23740	4.19.110-pref+
Pradinis saugos atnaujinimų paketo lygmuo	2020-04-01	2020-09-01	2020-10-01
Naujausio saugos atnaujinimo data	2021-06-01[14]	2021-03-01[15]	2021-04-01[16]
Saugos atnaujinimu sk.	9	3	4

Visi nagrinėti mob. įrenginiai veikia Android operacinės sistemos pagrindu, Huawei P40 ir Xiaomi Mi 10T naudoja 10 sisteminę versiją, OnePlus 8T – šiuo metu naujausią, 11-ą. Verta pažymėti, kad pagal nutylėjimą standartinė Android 11 operacinė sistema pasižymi platesnėmis prieigos kontrolės galimybėmis[17], įgalinančiomis vartotoją labiau kontroliuoti aplikacijų prieigą prie įrenginyje saugomų duomenų.

Android operacinės sistemos saugos atnaujinimai – operacinės sistemos komponentų naujiniai, skirti ištaisyti programines spragas, kurios kelia grėsmę įrenginio ar jame saugomų duomenų saugumui. Šie atnaujinimai yra orientuoti į programines spragas, leidžiančias vykdyti nuotilinio kodo vykdymo (angl. *Remote code execution*), privilegijų kėlimo (angl. *Elevation of privilege*), informacijos atskleidimo ir nutekinimo (angl. *Information disclosure*), paslaugų trikdymo (angl. *Denial of service*) ir kitų tipų atakas. Kiekvienas šių saugumo naujinių ištaiso tarp 20 ir 60 CVE duomenų bazėje pažymėtų saugumo spragų. Verta pastebėti, kad pažeidžiamumų žalingumas svyravo 5,4 – 10,0 balų (iš 10 galimų) intervale.

Dėl šios priežasties yra svarbu mob. įrenginių vartotojams šiuos atnaujinimus diegti reguliariai. Šie Android operacinės sistemos saugos atnaujinimai yra išleidžiami periodiškai – kas 1–3 mėnesius. Xiaomi yra įsipareigojusi šiuos atnaujinimus savo įrenginiams tiekti 2-us metus[18], o OnePlus – 3-us metus[19]. Apie Huawei įsipareigojimus operacinės sistemos ar jos saugumo atnaujinimų tiekimui

[14] Huawei informacija. *https://consumer.huawei.com/en/support/bulletin/*
[15] Adimorah blog informacija. *https://adimorahblog.com/new-stable-update-for-the-mi-10t-and-mi-10t-pro/*
[16] OnePlus informacija. https://www.oneplus.com/global/support/softwareupgrade/details?code=PM1605596915581
[17] Android authority informacija. C. Scott Brown, „The best Android 11 features you need to know“ *https://www.androidauthority.com/android-11-features-1085228/*
[18] Xiaomi informacija. *https://www.mi.com/global/service/support/security-update.html*
[19] OnePlus informacija. *https://forums.oneplus.com/threads/oneplus-software-maintenance-schedule.862347/*

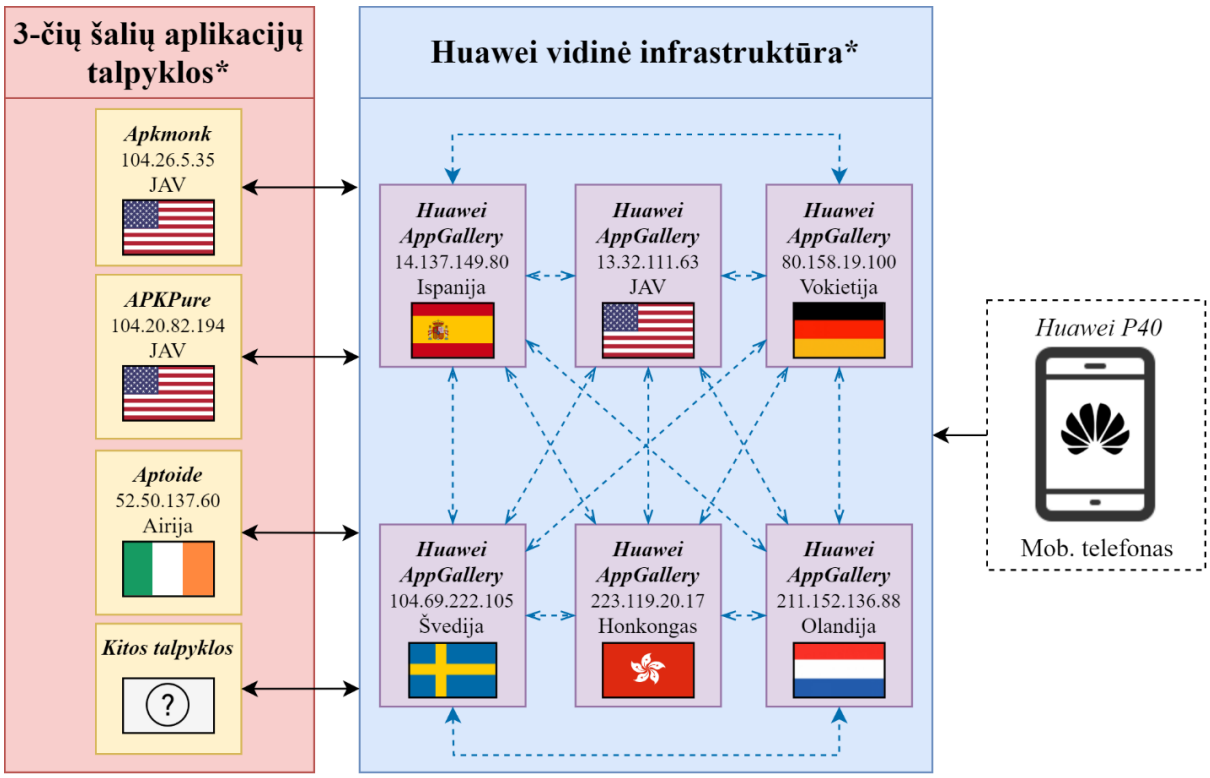
duomenų nebuvo rasta. Verta pabrėžti, kad Android operacinės sistemos gamintojas *Google* saugos atnaujinimus leidžia nemodifikuotoms Android operacinės sistemos versijoms (angl. *Android Open Source Project*). Dėl šios priežasties operacinės sistemos ir jos saugos atnaujinimai anksčiausiai yra prieinami *Google* gamintojo įrenginiams.

Tuo tarpu, įrenginių gamintojams kaip Huawei, Xiaomi, OnePlus ir kt. operacinės sistemos ar jos saugos atnaujinimus tenka derinti prie OS pagrindo gamintojo atliktų modifikacijų, todėl šių gamintojų mob. įrenginiams minėtieji atnaujinimai yra prieinami vėliau. Ypatingai svarbu pabrėžti tai, kad naujausi saugos atnaujinimai yra pasiekiami tik mob. įrenginiui Huawei P40. Tyrimo metu fiksuota, kad naujausi saugumo atnaujinimai, skirti mob. įrenginiui Xiaomi Mi 10T buvo 3-jų mėnesių senumo, o mob. įrenginiui OnePlus 8T – 2-jų mėnesių senumo.

NKSC pažymi, kad sutinkamai su aukščiau išdėstyta informacija, itin svarbu laiku atlikti turimų įrenginių saugumo atnaujinimus.

1. Oficiali „Huawei“ aplikacijų parduotuvė „AppGallery“ nukreipia į trečiųjų šalių el. parduotuves, kuriose esančios aplikacijos yra kenkėjiškos ar užkrėstos virusais

Atlikus analizę nustatyta, kad Huawei įrenginiuose naudojama mobiliųjų aplikacijų diegimo procedūra pasižymi kibernetinio saugumo neapibrėžtumais. Mob. aplikacijų diegimui Huawei telefonuose yra naudojama gamintojo parengta infrastruktūra, kurią sudaro oficiali elektroninė aplikacijų parduotuvė „AppGallery“ ir periferinės aplikacijų talpyklos (Apkmonk, *APKPure, Aptoide* ir kt.). Huawei elektroninės parduotuvės schema pateikta 1 paveiksle.



1 pav. „Huawei“ elektroninės mobiliųjų aplikacijų parduotuvės schema

„Huawei“ elektroninės mobiliųjų aplikacijos parduotuvės infrastruktūra sudaryta iš dviejų blokų – vidinės infrastruktūros „Huawei AppGallery“ ir trečiųjų šalių talpyklų. Nustatyta, kad nuosava „Huawei

AppGallery“ infrastruktūra yra išdėstyta Ispanijoje, JAV, Vokietijoje, Švedijoje, Olandijoje, Honkonge ir Tailande. Ši infrastruktūra yra integruota su trečiųjų šalių talpyklomis, iš kurių trys plačiausiai žinomos funkcionuoja JAV, Airijoje ir Olandijoje. Įvairiu šaltinių vertinimu[20], šiuo metu „Huawei“ mobiliųjų aplikacijų platinimo infrastruktūros sudėtyje yra fiksuotos 6 – 8 trečiųjų šalių talpyklos. „Huawei“ mobiliųjų aplikacijų platinimo infrastruktūrą nusakanti informacija pateikta 2 lentelėje.

2 lentelė. „Huawei“ mobiliųjų aplikacijų platinimo infrastruktūros informacija, nurodant vidinės „Huawei AppGallery“ ir trijų žinomiausių integruotų išorinių talpyklų parametrus

Eil. Nr.	Infrastruktūra	Adresas	IP adresas	Valstybė
1	Vidinė Huawei „AppGallery“	appdl-1-drcn.dbankcdn.com.c.cdnhwc1.com	223.119.20.17	Honkongas
2		pay7.hicloud.com	14.137.149.80	Ispanija
3		appdl-11-dre.dbankcdn.com	13.32.111.63	JAV
4		appdl-11-drcn.dbankcdn.com	65.9.52.144	JAV
5		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	211.152.136.88	Olandija
6		uc3.hispace.hicloud.com	23.14.13.247	Švedija
7		sdkserver-dre.op.hicloud.com	104.69.222.105	Švedija
8		hwid-dre.platform.hicloud.com	104.69.222.145	Švedija
9		appdl-12-drcn.dbankcdn.com.akamaized.net	184.31.15.17	Švedija
10		appdl-12-dre.dbankcdn.com.akamaized.net	184.31.15.51	Švedija
11		appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	119.46.76.15	Tailandas
12		appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	119.46.76.17	Tailandas
13		appstore.huawei.com	80.158.2.135	Vokietija
14		metrics2.data.hicloud.com	80.158.2.190	Vokietija
15		www.hicloud.com	80.158.19.100	Vokietija
16		query.hicloud.com	80.158.19.121	Vokietija
17		grs.dbankcloud.com	80.158.20.103	Vokietija
18		jos.hicloud.com	80.158.23.247	Vokietija
19		iap.hicloud.com	80.158.40.92	Vokietija
20		appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	101.33.11.29	Vokietija
21		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	101.33.11.45	Vokietija
22		appdl-4-drcn.dbankcdn.com	163.171.128.127	Vokietija
23		appdl-4-drcn.dbankcdn.com	163.171.128.129	Vokietija
24	Išorinė talpykla APKMonk	www.apkmonk.com	104.26.4.35	JAV
25	Išorinė talpykla ApkPure	download.apkpure.com	104.20.83.194	JAV
26	Išorinė talpykla Aptoide	en.aptoide.com	34.249.219.183	Airija
27		ws75.aptoide.com	34.254.115.204	Airija
28		ws75.aptoide.com	52.17.222.230	Airija
29		en.aptoide.com	52.50.137.60	Airija
30		rakam-api.aptoide.com	52.209.136.146	Airija
31		pnp.aptoide.com	54.194.247.193	Airija
32		en.aptoide.com	54.220.86.7	Airija
33		ws75.aptoide.com	54.229.235.132	Airija
34		cdn-mobile.aptoide.com	172.67.29.206	JAV
35		pool.apk.aptoide.com	5.79.110.134	Olandija
36		apkins.aptoide.com	95.211.168.137	Olandija
37		apkins.aptoide.com	95.211.223.52	Olandija

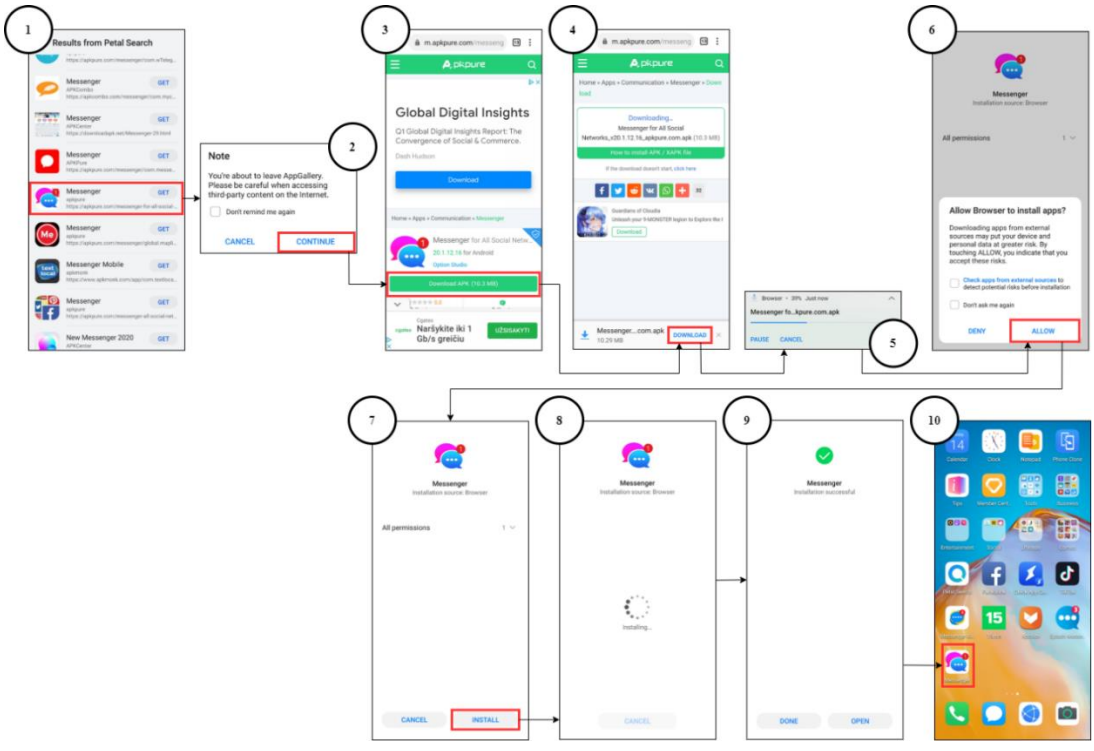
Vartotojui diegiant mob. aplikaciją Huawei įrenginyje, jos yra ieškoma „AppGallery“ parduotuvėje, aplikaciją radus, ji yra parsiunčiama ir įdiegiama į mob. įrenginį. Mobiliųjų aplikacijų diegimo schema naudojant Huawei „AppGallery“ platformą pateikta 2 paveiksle.

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

Huawei „AppGallery“ aplikacijoje paieškos laukelyje įvedus ieškomos aplikacijos pavadinimą, yra pateikiamas paieškos rezultatų sąrašas. Paieškos rezultatų lange yra pateikta skiltis „Petal Search“. Ją pasirinkus, vartotojui yra pateikiamas aplikacijų, pasiekiamų per trečiųjų šalių aplikacijų talpyklas, sąrašas (1). Vartotojui pasirinkus aplikaciją iš šios skilties, yra atvaizduojamas perspėjamasis pranešimas (2). Perspėjamajame pranešime yra nurodoma, kad tolimesni veiksmai bus vykdomi ne Huawei „AppGallery“ aplikacijoje.

Vartotojui uždarius perspėjamąjį langą, yra įrenginyje atidaroma interneto naršyklė, vartotojas yra nukreipiamas į 3-čiųjų šalių aplikacijų talpyklos tinklapį. Tinklapyje vartotojui pasirinkus aplikacijos diegiamosios rinkmenos atsisiuntimo parinktį (3), ši yra atsiunčiama ir išsaugoma įrenginio vidinėje atmintyje (4, 5). Įrenginiui pabaigus aplikacijos diegiamosios rinkmenos atsiuntimo procedūrą, yra pradedamas aplikacijos diegimas.

Kadangi šiuo atveju aplikacijos diegimą inicijuoja įrenginio interneto naršyklė, vartotojui yra pateikiamas informacinis langas (6), kuriame yra prašoma suteikti leidimą, interneto naršyklei inicijuoti aplikacijos diegimo procedūrą. Vartotojui davus leidimą, yra pateikiamas aplikacijos diegimo langas (7), kuriame yra reikalaujama pakartotinės vartotojo įvesties diegimui pradėti. Vartotojui pakartotinai patvirtinus aplikacijos diegimą, aplikacija yra sudiegiama (8, 9) ir naujai įdiegtos aplikacijos ikona yra pridedama į pagrindinį langą (10).



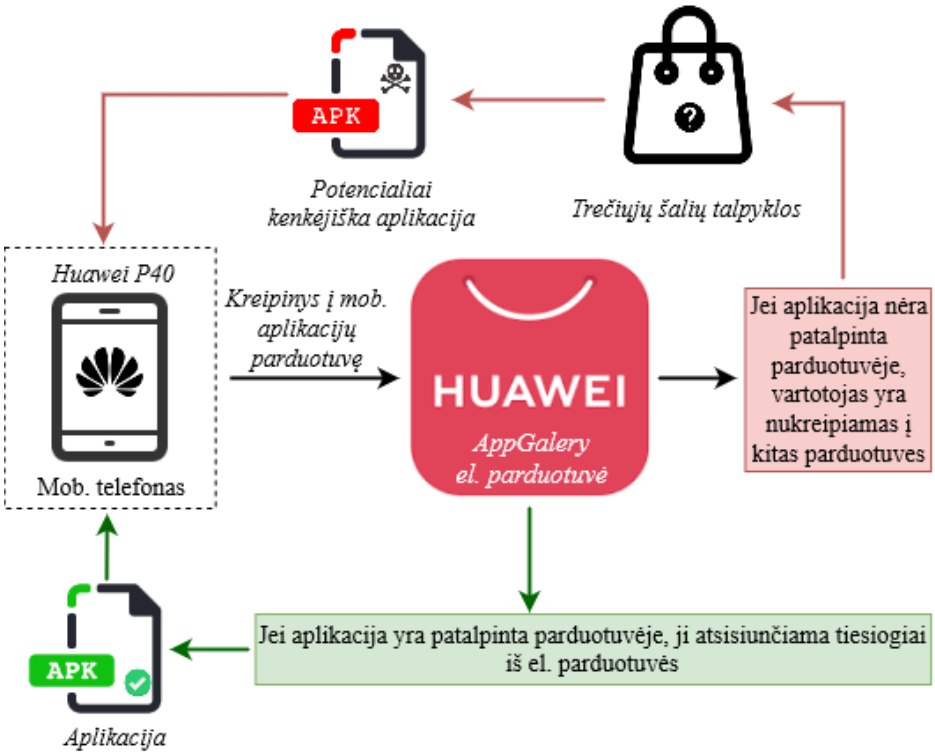
2 pav. Mobiliųjų aplikacijų diegimo schema naudojant Huawei „AppGallery“ platformą

Jeigu ieškomos aplikacijos Huawei „AppGallery“ parduotuvėje nėra, vartotojas automatiniu būdu yra nukreipiamas į periferines trečiųjų šalių aplikacijų talpyklas, iš kurių mob. aplikacija atsiunčiama į telefoną diegimui.

Atliktame tyrime buvo nustatyta, kad dalis talpyklose esančių mob. aplikacijų yra originalių aplikacijų padirbiniai, turintys kenkėjišką funkcionalumą ar užkrėsti virusais – vartotojas tokias

aplikacijas gali atsisiųsti ir įsidiegti į mob. telefoną, taip sukeliant grėsmę įrenginio ir jame esančių duomenų saugumui.

Huawei aplikacijų diegimo principinė schema, jų diegimui panaudojant ir trečiųjų šalių talpyklas, pateikta 3 paveiksle.



3 pav. Principinė Huawei aplikacijų diegimo schema, panaudojant ir trečiųjų šalių talpyklas

Verta pažymėti, kad dalis „Huawei“ naudojamos aplikacijų platinimo infrastruktūros yra šalyse, kuriose netaikomas Bendrasis duomenų apsaugos reglamentas. Svarbu pažymėti, kad mobilusis įrenginys, siunčiantis aplikaciją iš BDAR šalyje esančios mob. parduotuvės, gali vykdyti kreipinius į trečiąsias šalis, kuriose šis reglamentas negalioje. Dėl to kyla gretutinės vartotojų metaduomenų nutekėjimo rizikos.

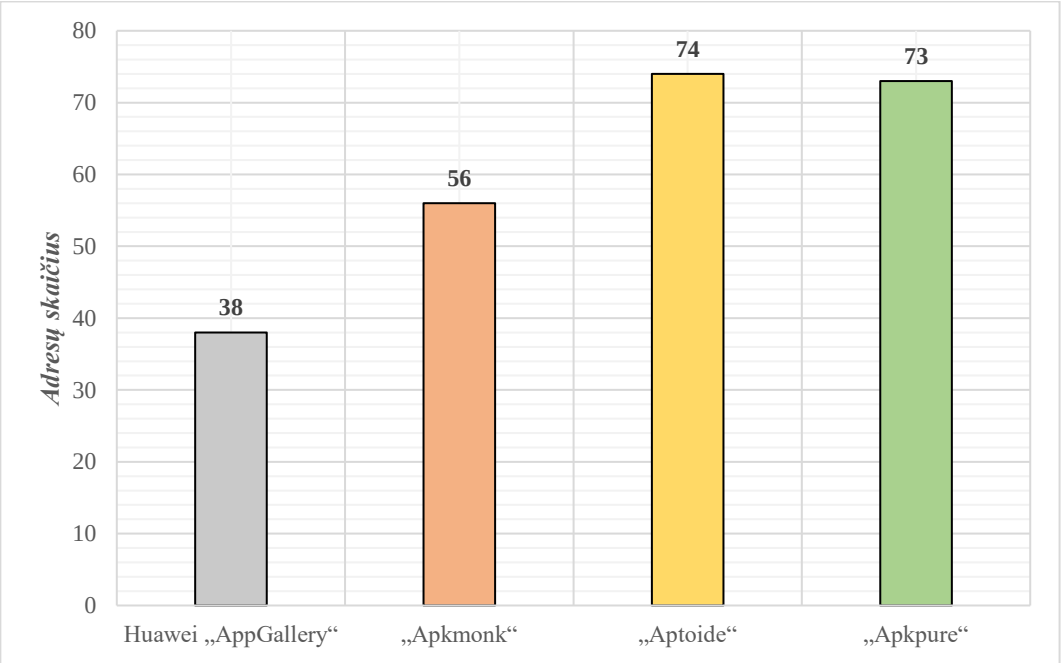
Tyrimo metu buvo nagrinėta „Huawei“ infrastruktūroje veikianti originali „AppGallery“ el. parduotuvė ir trys pasirinktos plačiausiai žinomos integruotos trečiųjų šalių talpyklos – „APKMonk“, „Aptoide“, „Apkpure“. Verta pažymėti, kad informacijos apie „APKMonk“ ir „Apkpure“ vystytojus laisvai prieinamose šaltiniuose rasti nepavyko. Remiantis „Aptoide“ informacija[21], šios talpyklos būstinė yra registruota Portugalijoje (Lisabona), įmonės filialai veiklą vykdo Kinijoje (Šendzenas) ir Singapūre.

Tyrimo metu buvo atliktas srauto fiksavimas, aplikacijas siunčiantis Huawei infrastruktūroje naudojamų šaltinių. Tyrimo metu aplikacijos buvo ieškotos Huawei „AppGallery“ el. parduotuvėje, nekeičiant originaliai gamintojų numatytos aplikacijų siuntimosi sekos – aplikacijos buvo siunčiamos tiesiogiai iš originalios parduotuvės ir „AppGallery“ pateiktų trečiųjų šalių aplikacijų talpyklų.

Fiksuojant sujungimų skaičių nustatyta, kad aplikacijos siuntimo metu iš originalios „AppGallery“ parduotuvės buvo nustatyti kreipiniai į 38 adresus, „APKMonk“ atveju – kreipiniai į 56 adresus. Daugiausia kreipinių buvo fiksuota „Aptoide“ ir „Apkpure“ atvejais – atitinkamai į 74 ir 73 adresus.

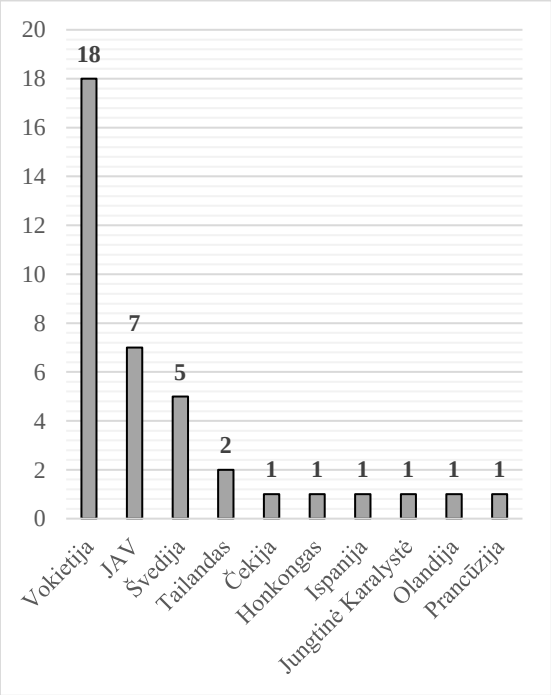
[21] Aptoide informacija. *https://en.aptoide.com/company/about-us*

Informacija, iliustruojanti „Huawei“ mob. įrenginių kreipinius, vykdant aplikacijos atsisiuntimo procedūras, pateikta 4 paveiksle.

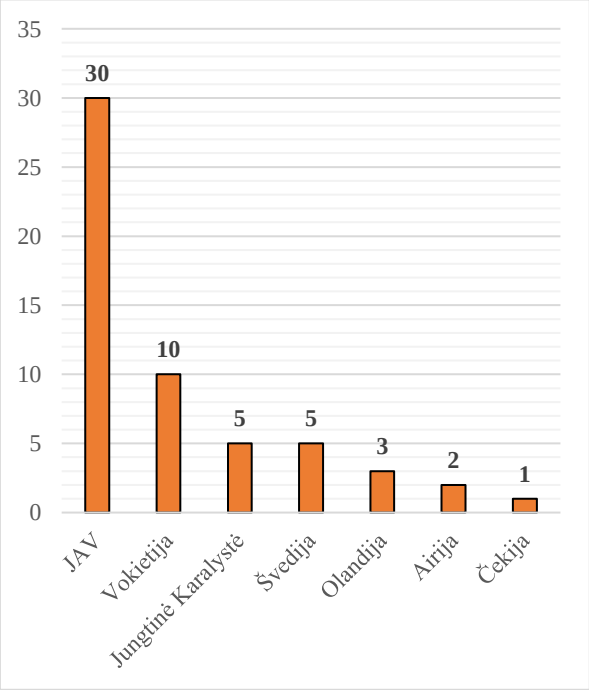


4 pav. „Huawei“ mob. įrenginių kreipinių skaičius, vykdant aplikacijos atsisiuntimo procedūras

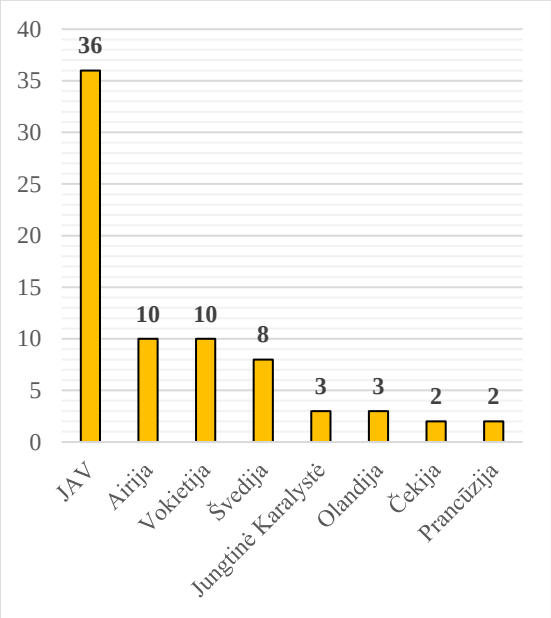
Detalesnė informacija, nusakanti kreipinių šalis ir jų kiekį, pateikta 5 – 7 paveiksluose.



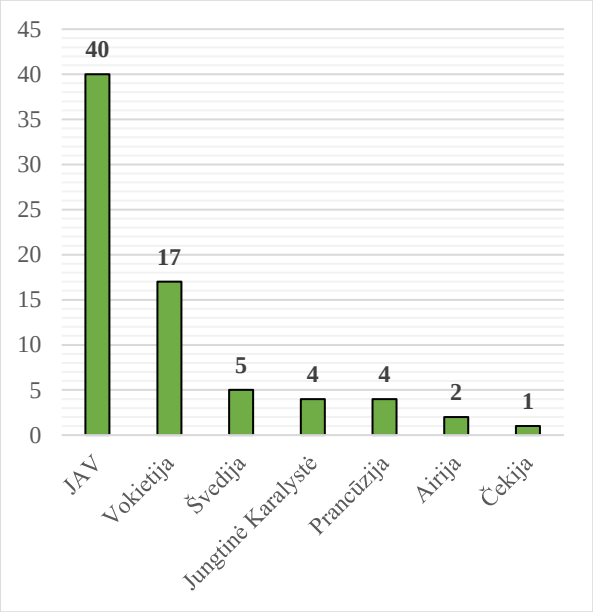
5 pav. „Huawei AppGallery“ kreipinių informacija



6 pav. Talpyklos „ApkMonk“ kreipinių informacija



7 pav. Talpyklos „Aptoide“ kreipinių informacija



8 pav. Talpyklos „Apkpure“ kreipinių informacija

Detalesnė analitinė informacija, nurodanti konkrečius IP adresus ir šalis, pateikta 3 lentelėje.

3 lentelė. Detalesnė analitinė informacija, nurodanti konkrečius IP adresus ir šalis

Eil. Nr.	*Huawei* „AppGallery“		„ApkMonk“		„Aptoide“		„Apkpure“	
	Adresas	Valstybė	Adresas	Valstybė	Adresas	Valstybė	Adresas	Valstybė
1	apkrep.ns1.ff.avast.com	Čekija	34.250.145.50	Airija	i.w.inmobi.com	Airija	apkrep.ns1.ff.avast.com	Čekija
2	appdl-1-drcn.dbankcdn.com.c.cdnhwc1.com	Honkongas	52.209.136.146	Airija	en.aptoide.com	Airija	sync.crwdcntrl.net	Airija
3	pay7.hicloud.com	Ispanija	5.62.53.15	Čekija	ws75.aptoide.com	Airija	52.209.246.140	Airija
4	8.8.8.8	JAV	appimg3.dbankcdn.com	JAV	ws75.aptoide.com	Airija	13.32.111.63	JAV
5	appdl-11-dre.dbankcdn.com	JAV	13.33.242.107	JAV	webservices.aptwords.net	Airija	feeds.apyhi.com	JAV
6	13.33.242.98	JAV	auction.unityads.unity3d.com	JAV	en.aptoide.com	Airija	34.98.67.61	JAV
7	13.107.213.44	JAV	odr.mookie1.com	JAV	rakam-api.aptoide.com	Airija	34.236.65.196	JAV
8	52.177.138.113	JAV	auction.unityads.unity3d.com	JAV	pnp.aptoide.com	Airija	rtb.openx.net	JAV
9	appdl-11-drcn.dbankcdn.com	JAV	auction.unityads.unity3d.com	JAV	en.aptoide.com	Airija	35.244.159.8	JAV
10	152.199.21.230	JAV	eu-u.openx.net	JAV	ws75.aptoide.com	Airija	35.244.174.68	JAV
11	5.62.36.56	Jungtinė Karalystė	id.rlcdn.com	JAV	apkrep.ns1.ff.avast.com	Čekija	65.9.52.144	JAV
12	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	Olandija	52.85.48.221	JAV	5.62.53.117	Čekija	download.apkpure.com	JAV
13	www.petalsearch.com	Prancūzija	52.154.69.245	JAV	wv.inner-active.mobi	JAV	104.26.4.35	JAV

14	uc3.hispace.hicloud.com	Švedija	65.9.53.128	JAV	wv.inner-active.mobi	JAV	partner.googleadservices.com	JAV
15	sdkserver-dre.op.hicloud.com	Švedija	104.21.35.78	JAV	8.8.8.8	JAV	pagead2.googlesyndication.com	JAV
16	hwid-dre.platform.hicloud.com	Švedija	www.apkmonk.com	JAV	test.quantcast.mgr.consensu.org	JAV	142.250.74.100	JAV
17	appdl-12-drcn.dbankcdn.com.akamaized.net	Švedija	104.197.172.31	JAV	quantcast.mgr.consensu.org	JAV	s0.2mdn.net	JAV
18	appdl-12-dre.dbankcdn.com.akamaized.net	Švedija	partner.googleadservices.com	JAV	auction.unityads.unity3d.com	JAV	firebaseremoteconfig.googleapis.com	JAV
19	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Tailandas	142.250.74.35	JAV	publisher-config.unityads.unity3d.com	JAV	app-measurement.com	JAV
20	appdl-1-dre.dbankcdn.com.c.cdnhwc1.com	Tailandas	adservice.google.com	JAV	www.datadoghq-browser-agent.com	JAV	adservice.google.com	JAV
21	appstore.huawei.com	Vokietija	142.250.74.100	JAV	sdktm.w.inmobi.com	JAV	firebase-settings.crashlytics.com	JAV
22	80.158.2.189	Vokietija	142.250.74.102	JAV	rules.quantcount.com	JAV	142.250.74.136	JAV
23	metrics2.data.hicloud.com	Vokietija	142.250.74.129	JAV	104.21.35.78	JAV	142.250.74.142	JAV
24	80.158.16.161	Vokietija	142.250.74.130	JAV	config.inmobi.com	JAV	sync-tm.everesttech.net	JAV
25	www.hicloud.com	Vokietija	um.simpli.fi	JAV	142.250.74.2	JAV	152.199.21.230	JAV
26	query.hicloud.com	Vokietija	172.67.29.206	JAV	www.googletagmanager.com	JAV	172.67.68.182	JAV
27	grs.dbankcloud.com	Vokietija	tpc.googlesyndication.com	JAV	partner.googleadservices.com	JAV	172.217.20.33	JAV
28	80.158.20.104	Vokietija	googleads4.g.doubleclick.net	JAV	connectivitycheck.gstatic.com	JAV	googleads.g.doubleclick.net	JAV
29	jos.hicloud.com	Vokietija	www.gstatic.com	JAV	firebaseinstallations.googleapis.com	JAV	172.217.20.35	JAV
30	iap.hicloud.com	Vokietija	172.217.21.161	JAV	cdn.ampproject.org	JAV	tpc.googlesyndication.com	JAV
31	80.158.54.98	Vokietija	ade.googlesyndication.com	JAV	adservice.google.com	JAV	172.217.21.130	JAV
32	appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	Vokietija	cm.g.doubleclick.net	JAV	www.google.com	JAV	www.gstatic.com	JAV
33	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	Vokietija	192.48.236.3	JAV	pagead-googlehosted.l.google.com	JAV	ade.googlesyndication.com	JAV
34	160.44.194.86	Vokietija	pixel-sync.sitescout.com	Jungtinė Karalystė	142.250.74.130	JAV	www.google.com	JAV
35	160.44.199.4	Vokietija	openx2-match.dotomi.com	Jungtinė Karalystė	firebase-settings.crashlytics.com	JAV	172.217.21.166	JAV
36	160.44.207.213	Vokietija	91.228.74.189	Jungtinė Karalystė	softonic.map.fastly.net	JAV	172.217.21.170	JAV
37	appdl-4-drcn.dbankcdn.com	Vokietija	image6.pubmatic.com	Jungtinė Karalystė	api.facebook.com	JAV	172.217.22.162	JAV
38	appdl-4-drcn.dbankcdn.com	Vokietija	188.125.94.206	Jungtinė Karalystė	connect.facebook.net	JAV	raw.githubusercontent.com	JAV

39		81.171.20.104	Olandija	www.facebook.com	JAV	216.58.207.206	JAV
40		95.211.137.160	Olandija	cdn-mobile.aptoide.com	JAV	www.gstatic.com	JAV
41		ib.adnxs.com	Olandija	tpc.googlesyndication.com	JAV	firebaseinstallations.googleapis.com	JAV
42		store3.hispace.hicloud.com	Švedija	fonts.gstatic.com	JAV	cm.g.doubleclick.net	JAV
43		104.73.93.58	Švedija	pagead-googlehosted.l.google.com	JAV	216.58.211.130	JAV
44		tls.adobe.com	Švedija	adservice.google.com	JAV	ad.turn.com	Jungtinė Karalystė
45		sdkserver-dre.op.hicloud.com	Švedija	fonts.googleapis.com	JAV	185.29.135.233	Jungtinė Karalystė
46		sdkserver-dre.op.hicloud.com.edgekey.net	Švedija	ads.mopub.com	JAV	185.64.190.78	Jungtinė Karalystė
47		j.mrpdata.net	Vokietija	ads.mopub.com	JAV	212.82.100.176	Jungtinė Karalystė
48		23.193.116.193	Vokietija	app-measurement.com	JAV	51.75.146.159	Prancūzija
49		metrics2.data.hicloud.com	Vokietija	pixel.quantserve.com	Jungtinė Karalystė	pixel.onaudience.com	Prancūzija
50		platform.hicloud.com	Vokietija	185.64.190.78	Jungtinė Karalystė	d-08.winudf.com	Prancūzija
51		grs.dbankcloud.com	Vokietija	data.flurry.com	Jungtinė Karalystė	green.erne.co	Prancūzija
52		appgallery.cloud.huawei.com	Vokietija	pool.apk.aptoide.com	Olandija	dsum-sec.casalemedia.com	Švedija
53		jfs-dre.jos.hicloud.com	Vokietija	apkins.aptoide.com	Olandija	store3.hispace.hicloud.com	Švedija
54		80.158.34.57	Vokietija	apkins.aptoide.com	Olandija	sdkserver-dre.op.hicloud.com.edgekey.net	Švedija
55		160.44.199.4	Vokietija	id5-sync.com	Prancūzija	hwid-dre.platform.hicloud.com	Švedija
56		160.44.202.175	Vokietija	51.255.81.18	Prancūzija	sdkserver-dre.op.hicloud.com	Švedija
57				2.18.33.213	Švedija	3.66.135.160	Vokietija
58				z.moatads.com	Švedija	tracking.justpremium.com	Vokietija
59				store3.hispace.hicloud.com	Švedija	49.51.130.46	Vokietija
60				d.applovin.com	Švedija	pixel.rubiconproject.net.akadns.net	Vokietija
61				sdkserver-dre.op.hicloud.com	Švedija	80.158.2.189	Vokietija
62				sdkserver-dre.op.hicloud.com.edgekey.net	Švedija	metrics2.data.hicloud.com	Vokietija
63				cdn2.inner-active.mobi	Švedija	oauth-login-dre.platform.dbankcloud.com	Vokietija
64				webview.unityads.unity3d.com	Švedija	80.158.19.69	Vokietija
65				api.vungle.com	Vokietija	80.158.19.100	Vokietija
66				ads.api.vungle.com	Vokietija	80.158.19.121	Vokietija
67				metrics2.data.hicloud.com	Vokietija	80.158.20.104	Vokietija

68			oauth-login-dre.platform.dbankcloud.com	Vokietija	jfs-dre.jos.hicloud.com	Vokietija
69			jfs-dre.jos.hicloud.com	Vokietija	80.158.34.57	Vokietija
70			cloud.hicloud.com	Vokietija	grs.dbankcloud.com	Vokietija
71			80.158.40.21	Vokietija	80.158.44.234	Vokietija
72			appdlssl.hicloud.com	Vokietija	101.33.11.48	Vokietija
73			160.44.199.4	Vokietija	160.44.199.4	Vokietija
74			connectivitycheck.platform.hicloud.com	Vokietija		

Tyrimo metu nustatyta, kad siunčiantis aplikaciją iš „Huawei“ infrastruktūros, buvo įvykdytas nukreipimas į trečiųjų šalių aplikacijų talpyklas, iš kurių buvo atsisiųstos aplikacijos, galimai turinčios kenkėjiško programinio kodo. Mobiliųjų aplikacijų, atsisiųstų „Huawei“ įrenginiu iš „Huawei“ infrastruktūros saugumo analizės suvestinė pateikta 4 lentelėje. Saugumo analizė buvo atlikta plačiai žinomu rinkmenų analizės įrankiu „VirusTotal“[22].

4 lentelė. Atsisiųstų mob. aplikacijų suvestinė atlikus patikrą įrankiu „VirusTotal“

Eil. Nr.	Aplikacijos pavadinimas	Identifikatorius	Aplikacijos versija	VirusTotal rezultatas
1	Social Media	com.social.messenger.allinoneapps	14	*Kenkėjiška programinė įranga:* A.gray.andrsca.f
2	Web Machinist Mobile Pro Tapping	com.webmachinist.cncmachinisttappingcalculator	1.0	*Virusas:* Trojan.Trojan.Banker.AndroidOS.Agent.ed
3	Messenger All in One	comm.essagechat.listing	28.0	*Kenkėjiška programinė įranga:* Adware/Loead Android.fyben.a

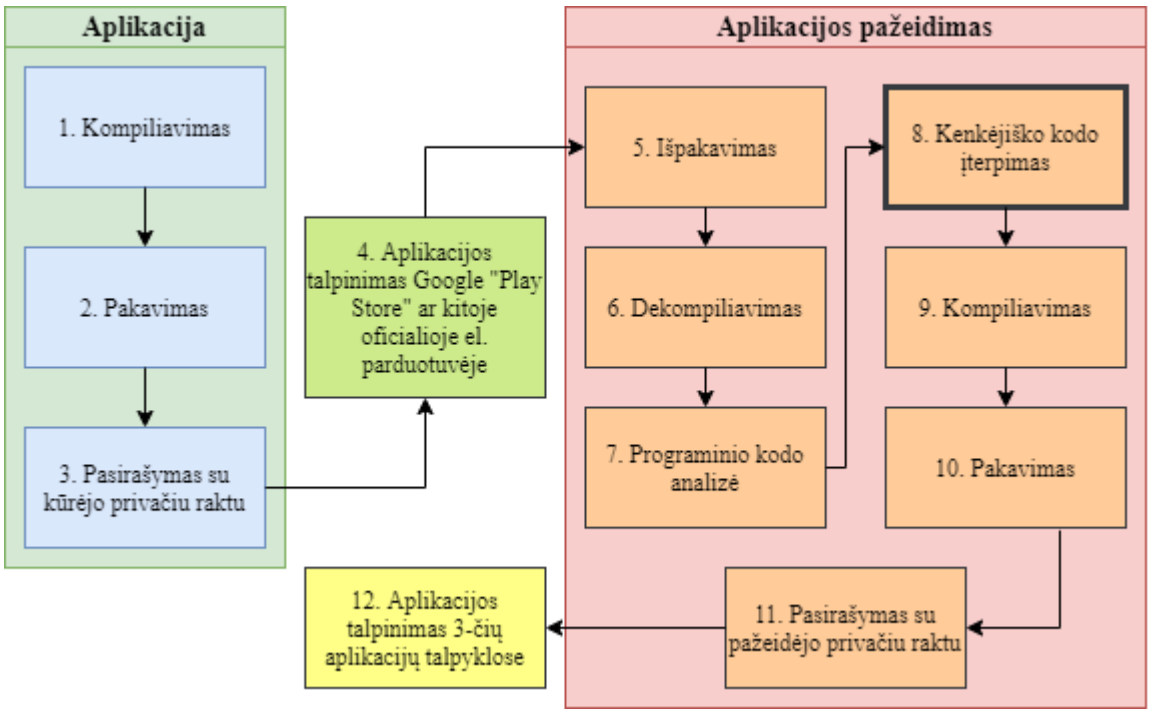
Atliekant tyrimą, buvo analizuotos trys mobiliosios aplikacijos, atsiųstos iš „Huawei“ mobiliųjų aplikacijų platinimo infrastruktūros serverių. „VirusTotal“ skenavimo duomenimis, „Social Media“ aplikacijoje vienos antivirusinės sistemos buvo nustatyta, kad aplikacijoje įdiegta galimai kenkėjiška programinė įranga „A.gray.andrsca.f“. Išnagrinėjus kitą mob. programėlę „Web Machinist Mobile Pro Tapping“, atsisiųstą iš „Huawei“ infrastruktūros serverių, vieno „VirusTotal“ antiviruso buvo fiksuotas potencialus virusas „Trojan.Trojan.Banker.AndroidOS.Agent.ed“. Šis virusas gali vykdyti[23] prisijungimų prie bankinių sistemų duomenų vagystes. Trečioje nagrinėtoje aplikacijoje „Messenger All in One“ dvi antivirusinės sistemos nustatė, kad programėlė naudoja potencialiai kenkėjišką programinę įrangą – paketus „Adware/Loead“ ir „Android.fyben.a“.

Tai kelia didelį susirūpinimą įrenginio saugumu, kadangi ne visos trečiųjų šalių aplikacijų talpyklos vykdo įkeliamų aplikacijų patikrą.

Ši infrastruktūros saugumo spraga gali būti išnaudojama gavus originalias aplikacijas iš *Google* „Play Store“, įvykdžius aplikacijos dekompoziciją ir reikiamas modifikacijas aplikacijos dekompozicijos turinyje, pridedant kenkėjišką kodą. Aplikacijos programinis kodas su kenkėjišku turiniu tuomet yra sukompiliuojamas, supakuojamas ir pasirašomas su nauju privačiu raktu. Gauta modifikuota aplikacija yra įkeliama į minėtąsias trečiųjų šalių aplikacijų talpyklas. Šio proceso

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

asociatyvi schema[24] pateikta 9 paveiksle.



9 pav. Asociatyvi kenkėjiško kodo įterpimo į mob. aplikaciją schema

Aplikacijos kūrėjas aplikacijos kūrimo metu sukompiliuoja programinį kodą ir taip suformuoja funkcionuojančią aplikaciją. Ši aplikacija yra supakuojama į diegiamąją rinkmeną ir pasirašoma aplikacijos kūrėjo privačiu raktu. Pasirašyta diegiamoji aplikacijos rinkmena gali būti talpinama į aplikacijos parduotuves, tokias kaip *Google* „Play Store“.

Pažeidėjas, kaip ir visi aplikacijų parduotuvių vartotojai (išskyrus atitinkamus regionų ribojimus) gali šią aplikaciją parsisiųsti – aplikaciją gavus iš oficialių šaltinių, ji yra išpakuojama ir dekompiliuojama į aplikacijos programinį kodą. Tai leidžia pažeidėjui atlikti jo analizę, nustatyti kenkėjiško kodo diegimo vietos ir naudotinos diegimo technologijos perspektyvumą, į aplikaciją įdiegti kenkėjišką kodą. Įvykdžius kenkėjiško programinio kodo įterpimo procedūras, aplikacijos programinis kodas yra sukompiliuojamas ir supakuojamas į diegiamąją rinkmeną, kuri yra pasirašoma pažeidėjo privačiu raktu. Sugeneruota kenkėjiškos aplikacijos diegiamoji rinkmena yra talpinama į trečiųjų šalių aplikacijų talpyklas, kuriose ne visais atvejais vykdoma talpinamų aplikacijų patikra.

Nustatyta, kad virusų turinčios el. parduotuvės yra rimta ir šių parduotuvių vystytojams aktuali problema[25]. Vartotojas, įsidiegęs virusuotą aplikaciją, gali nukentėti dėl įrenginyje ar susietoje debesijos paslaugoje saugomų duomenų rinkimo, nutekėjimo ar mob. įrenginio sugadinimo.

Atliktame tyrime buvo nustatyta, kad dalis talpyklose esančių mob. aplikacijų yra originalių aplikacijų padirbiniai, turintys kenkėjišką funkcionalumą ar užkrėsti virusais – vartotojas tokias aplikacijas gali atsisiųsti ir įsidiegti į mob. telefoną, taip sukeliant grėsmę įrenginio ir jame esančių duomenų saugumui.

[24] Springer informacija. 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. Kinijoje suprojektuoti ir pagaminti įrenginiai kreipiasi į serverius trečiose šalyse. Tai leidžia rinkti ir agreguoti vartotojų metaduomenis, jais remiantis vykdyti vartotojų stebėseną

Programinės dekompozicijos ir duomenų srautų analizė parodė, kad naršyklė „Mi Browser“ naudoja du duomenų rinkimo modulius: „Google Analytics“ ir „Sensors Data“. „Sensors Data“ yra kiniškos kilmės, funkcionalumu artima platforma „Google Analytics“. Įmonės „Sensors Data“ teigimu[26], ji turi daugiau nei 1500 klientų, tarp jų – didžiausios Kinijos Liaudies Respublikos korporacijos „China Telecom“, „Baidu“, „CYTS“, „Sichuan Airlines“ ir kt.

„Google Analytics“ yra analitikos platforma, skirta programų autoriams ar jas administruojantiems subjektams gauti informaciją, leidžiančią vertinti vartotojų naudojimąsi sukurtomis aplikacijomis iOS, Android ar web aplinkose[27]. „Google Analytics“ automatiškai sugeneruoja įvykių žurnalą, leidžiantį įvertinti aplikacijos veikimo charakteristikas. Verta pažymėti, kad programos kūrėjas turi technines galimybes pasirinkti analizuojamus parametrus, nustatyti jų analizės gylį.

Buvo nustatyta, kad šis modulis gali rinkti duomenis apie vartotojo naršymą, mygtukų paspaudimus ir kt., siųsti informaciją galimai analizei į Google serverius. Reikia pažymėti, kad šie moduliai yra aktyvuojami įrenginio pradinio įjungimo metu sutikus dalyvauti „Xiaomi User Experience“ programoje.

Atlikus „Xiaomi“ įrenginio gamykliškai sukomponuotų sisteminių aplikacijų dekompoziciją, buvo nustatyta, kad šių analitikos programų funkcionalumas buvo įdiegtas ir veikė standartinėje „Xiaomi“ telefono internetinėje naršyklėje „Mi Browser“. 5 lentelėje pateiktas „Mi Browser“ aplikacijos kodo fragmentas, pažymintis „Google Analytics“ funkcionalumą.

5 lentelė. „Mi Browser“ naršyklės programinio kodo fragmentas, pažyminitis „Google Analytics“ funkcionalumą

```
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);
      }
    });
  }
}
```

Lentelėje pateiktame kodo fragmente realizuota duomenų išsiuntimo funkcija į „Google“ serveriuose esančią analitikos platformą „Firebase“. 6 lentelėje pateiktas „SensorData“ kodo fragmentas, įdiegtas „Mi Browser“ aplikacijoje. Kodo fragmente pateikta funkcija, „Mi Browser“ aplikacijoje paleidžianti „Sensors Data“ funkcionalumą.

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

6 lentelė. „Sensors Data“ paleidimo kodo fragmetnas „Mi Browser“ aplikacijoje

```
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("uuid");
         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) {
      }
   }
}
```

Nustatyta, kad įrenginyje naudojamas „Sensors Data“ modulis renka 61-o parametro (aplikacijos įjungimo laikas, naudojama kalba ir kt.) statistinę informaciją apie naudojamų aplikacijų veiklą. „Sensors Data“ renkamų duomenų sąrašas pateiktas 7 lentelėje.

7 lentelė. „Sensors Data“ renkamo 61-o parametro sąrašas

Nr.	Parametras	Komentaras
1	log_miaccount	Ar vartotojas prisijungęs
2	autocomplete_switch	Ar įjungtas automatinio teksto užbaigimo funkcija
3	no_track_switch	Ar įjungta „Do Not Track“ funkcija
4	bookmark_sync	Ar įjungta „bookmark“ sinchronizacija su debesija
5	history_sync	Ar įjungta naršymo istorijos sinchronizacija su debesija
6	feature_report_switch	Ar vartotojas dalyvauja „Xiaomi User Experience“ programoje
7	clear_history_switch	Ar istorija pašalinama išjungus aplikacija
8	personal_service_switch	Ar įjungtos programų rekomendacijos
9	enhanced_incognito_switch	Ar naršyklė veikia „Enhanced Incognito“ rėžime
10	system_out_of_ads	Ar aktyvuota „Limit Ad Tracking“ funkcija. Ši funkcija, reklamos teikėjams yra neprieinamas įrenginio identifikatorius
11	swipe_up	Kokia funkcija užregistruota „swipe up“ veiksmui
12	current_default_search_engine	Dabartinis naudojamas paieškos variklis
13	language	Sistemoje nustatyta kalba

14	language_browser	Naršykles parametruose nustatyta kalba
15	icon_reddot_status	-
16	user_newsfeed	Ar naujienų srautas yra išjungtas
17	user_download_videos	-
18	user_night_mode	Ar naršyklėje naudojamas naktinis rėžimas
19	dark_mode	Ar sistemoje naudojamas naktinis režimas
20	user_data_save_mode	Ar aktyvuotas duomenų taupymo funkcionalumas naršyklėje
21	user_incognito_mode	Ar įjungtas „incognito“ rėžimas
22	user_desktop_mode	Naršykles „user-agent“
23	user_checkbox_4G	Ar leidžiama atlikti naršykles atnaujinimus per 4G
24	user_push_agree	Ar aktyvuoti naršyklėje pranešimai
25	user_facebook_notification	Ar aktyvuoti naršyklėje Facebook pranešimai
26	user_youtube_signin	Ar vartotojas prisijungęs prie „YouTube“
27	user_click_interest	Rodo, kiek kartų vartotojas paspaudė ant naršyklėje esančių kortelių (naujienos, „YouTube“ rekomendacijos ir kt)
28	user_login	Ar vartotojas prisijungęs prie „Mi Account“
29	adblock_switch	Ar aktyvuota reklamų blokavimo funkcija
30	adblock_show_notification	Ar įjungtas „Adblock“
31	first_enter_newsfeed_way	Ar pirma kartą įjungtas naujienų srauto langas
32	first_appstart_source	-
33	first_appstart_third_party	-
34	miui_personalised	Ar aktyvuotos suasmenintos reklamos
35	personalised_services	Ar aktyvuotos suasmenintos turinio rekomendacijos
36	browser_ads	-
37	protection_type	-
38	app_boot_third_party	-
39	app_boot	Programos įjungimo laikas
40	feed_default_channel	-
41	experience_improve	Ar aktyvuota „Xiaomi User Experience“ funkcija
42	platform	Platforma. Visuomet „Android“
43	miui_version	MIUI versija
44	log_miaccount	Ar vartotojas prisijungęs prie Mi paskyros
45	miui_region	Mi regionas
46	eid	-
47	apk_name	Aplikacijos APK pavadinimas
48	browser_install_referrer	-
49	autocomplete_switch	Ar aktyvuotas „autocomplete“ paieškos lange
50	no_track_switch	Ar įjungta „Do Not Track“ funkcija
51	bookmark_sync	Ar aktyvuota „bookmarks“ sinchronizacija su Mi serveriu
52	history_sync	Ar aktyvuota naršymo istorijos sinchronizacija su Mi serveriu
53	feature_report_switch	Ar vartotojas dalyvauja „Xiaomi User Experience“ programoje
54	clear_history_switch	Ar naršymo istorija pašalinama išjungus aplikaciją
55	personal_service_switch	Ar įjungta vartotojo rekomendacijų funkcionalumas – personalzuoti „YouTube“ klipai ir kt.
56	enhanced_incognito_switch	Ar įjungtas „incognito“

57	user_tab_news	Ar vartotojas įjungė naujienų langą
58	user_tab_games	Ar vartotojas įjungė žaidimų langą
59	search_optimization_switch	Konstanta, visuomet lygi 1
60	cookie_status	Pateikia duomenis apie vartotojo sausainių nustatymus
61	subscription	Nurodo ar naudojamas VPN ir jei taip, jo identifikatorių.

Tyrimo metu buvo atliktas pilnas „Xiaomi“ užšifruotų pranešimų dekodavimas ir dešifravimas. Nustatyta, kad „Xiaomi“ telefonas siunčia „Sensors Data“ duomenis Base64 algoritmu užkoduotą duomenų rinkinį, kuris papildomai yra užkoduotas naudojant *urlencode* algoritmą. Siunčiamų užkoduotų duomenų fragmento pavyzdys pateiktas 8 lentelėje.

8 lentelė. „Xiaomi“ telefono siunčiamų duomenų fragmentas

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

9 lentelėje pateikiamas dešifruotas „Xiaomi“ telefono siunčiamų duomenų turinys Singapūre esantiems „Sensors Data“ turinys. Analizei siunčiami duomenys – aplikacijos versija, aplikacijos pavadinimas, esamas regionas, įrenginio gamintojas ir kt.

9 lentelė. „Xiaomi“ telefono siunčiamas turinys į „Sensors Data“ serverius Singapūre


```
{
  "_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
  }
}
```

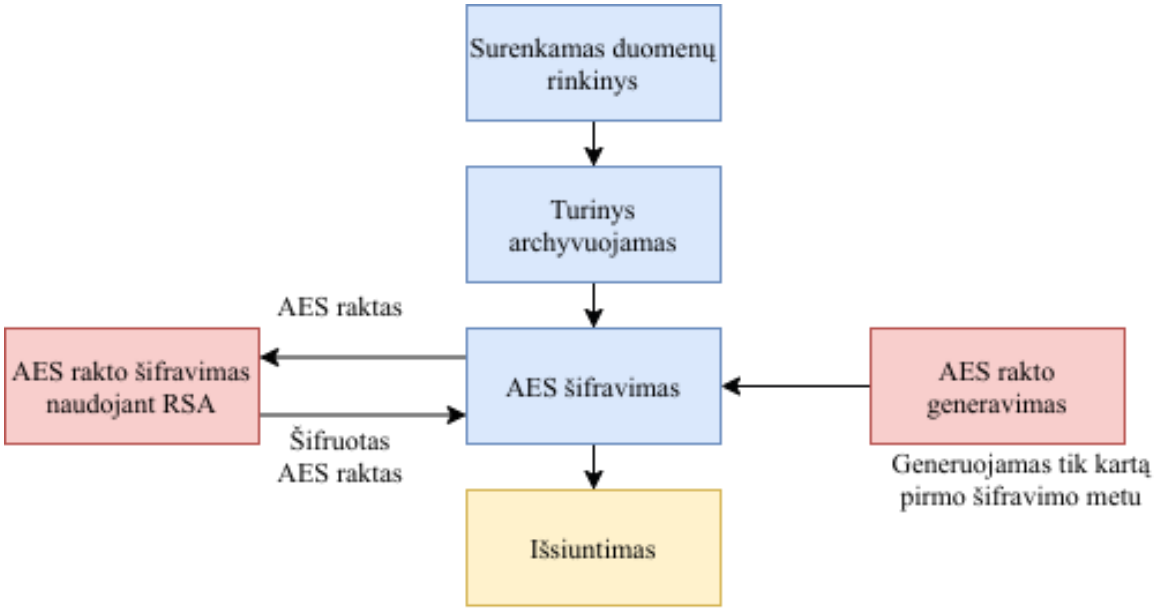

Buvo nustatyta, kad „Sensors Data“ duomenys yra siunčiami internetiniu adresu *https://sa.api.intl.miui.com*. 10 lentelėje pateikta informacija, charakterizuojanti tinklu perduodamus analitinius duomenis į Singapūre esančius serverius.

10 lentelė. „Sensors Data“ siunčiamų duomenų charakteristikos

Eil. Nr.	IP adresas	Išsiųsti duomenys, *B*	Gauti duomenys, *B*	Viso duomenų, *B*	Valstybė
1	47.241.109.186	11789	0	11789	Singapūras
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	

Surinkti statistiniai duomenys šifruotu kanalu yra siunčiami į „Xiaomi“ serverius Singapūre, kuriame nėra taikomas Bendrasis duomenų apsaugos reglamentas. Galima teigti, kad potencialiai perteklinis analitinių duomenų rinkimas ir naudojimas kelia grėsmes asmens duomenų privatumui.

10 paveiksle pateiktas tyrimų metu atkurtas „Sensors Data“ duomenų šifravimo mechanizmas, naudojamas mezgant duomenų perdavimo ryšį tarp įrenginio ir Singapūre esančių serverių.



10 pav. „Xiaomi“ naudojamas duomenų šifravimo mechanizmas

Šifruotų duomenų rinkinys yra sugeneruojamas kviečiant „Mi Browser“ įdiegtas programines „Sensors Data“ funkcijas: *registerSuperProperties* ir *registerDynamicSuperProperties*. Šios funkcijos yra atsakingos už duomenų surinkimą ir JSON objekto paruošimą. Kai duomenų rinkinys turi būti išsiųstas, pirmiausia, jis yra paverčiamas į baitinę išraišką ir archyvuojamas naudojant *gzip* algoritmu.

Tai yra daroma siekiant sumažinti išsiųstų duomenų kiekį. Gautas rezultatas yra šifruojamas AES128-CBC algoritmu. Raktas yra sugeneruojamas naudojant įrenginio pseudoatsitiktinių skaičių generatorių. Po to, AES šifravime naudotas raktas yra užšifruojamas RSA algoritmu, naudojant iš „Xiaomi“ serverių parsisiųstą viešąjį raktą. Gautas rinkinys yra supakuojamas į JSON objektą ir išsiunčiamas į serverius Singapūre.

Aplikacija, kviečia funkcijas *registerSuperProperties* ir *registerDynamicSuperProperties*. Šios funkcijos yra atsakingos už duomenų surinkimą ir JSON objektų paruošimą. Galima teigti, kad naudojamas „Sensors Data“ šifravimo mechanizmas užtikrina santykinai aukštą duomenų saugumo lygį juos perduodant į analitikos serverius esančius Singapūre.

Įrenginyje įdiegtas „Google Analytics“ modulis leidžia perskaityti „Mi Browser“ naršymo istoriją, paieškos rezultatus ir kitus aplikacijos veiklos parametrus, siųsti šiuos duomenis į analitikos serverius. Duomenys yra siunčiami šifruotu TLS kanalu naudojant Protobuf koduotę. Duomenų dekodavimas, neturint Protobuf konfigūracinio failo yra neįmanomas arba sunkiai realizuotinas, tačiau užkoduotame sraute galima įžvelgti tam tikrus duomenis: „Mi Browser“ naršyklėje atidarytas internetinis adresas, paieškos lauke vesti duomenys ar vartotojo atliktas veiksmas (pvz., paspaudimas ant paieškos lauko).

Prie šių duomenų prieiti ir juos naudoti gali aplikacijos kūrėjas „Xiaomi“[28]. Užkoduotas siunčiamų duomenų fragmentas, kuris siunčiamas į „Google Analytics“ serverius, pateiktas 11 lentelėje.

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

11 lentelė. Užkoduotas siunčiamų duomenų fragmentas, „Xiaomi“ įrenginio siunčiamas į „Google Analytics“ serverius

```
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¦¡/
```

12 lentelėje pateikta informacija, charakterizuojanti tinklu „Xiaomi“ įrenginio perduodamus analitinius duomenis į „Google Analytics“ serverius.

12 lentelė. „Google Analytics“ siunčiamų duomenų charakteristikos

Eil. Nr.	IP adresas	Išsiųsti duomenys, *B*	Gauti duomenys, *B*	Viso duomenų, *B*	Valstybė
1	142.250.74.110	2545	0	2545	JAV
2	172.217.16.14	1282		1282	
3	216.58.207.206	12699		12699	

Remiantis nustatytais faktais, galima teigti, kad „Xiaomi“ renka santykinai didelį kiekį informacijos apie įrenginyje veikiančius procesus, įdiegtų programinių paketų elgseną, atliktus vartotojų veiksmus ir aplikacijų konfigūracinius parametrus. Šiam procesui įgyvendinti naudojamos dvi analitikos sistemos – „Sensors Data“ ir „Google Analytics“. Atlikus šaltinių apžvalgą, buvo nustatyta, kad Xiaomi įrenginiai renka platesnį duomenų spektrą lyginant su kitais mob. įrenginių

gamintojais[29,30,31].

Galima teigti, kad potencialiai perteklinis analitinių duomenų rinkimas ir naudojimas kelia grėsmes asmens duomenų privatumui.

3. „Xiaomi“ įrenginyje realizuotas funkcionalumas galintis riboti laisvą informacijos prieinamumą

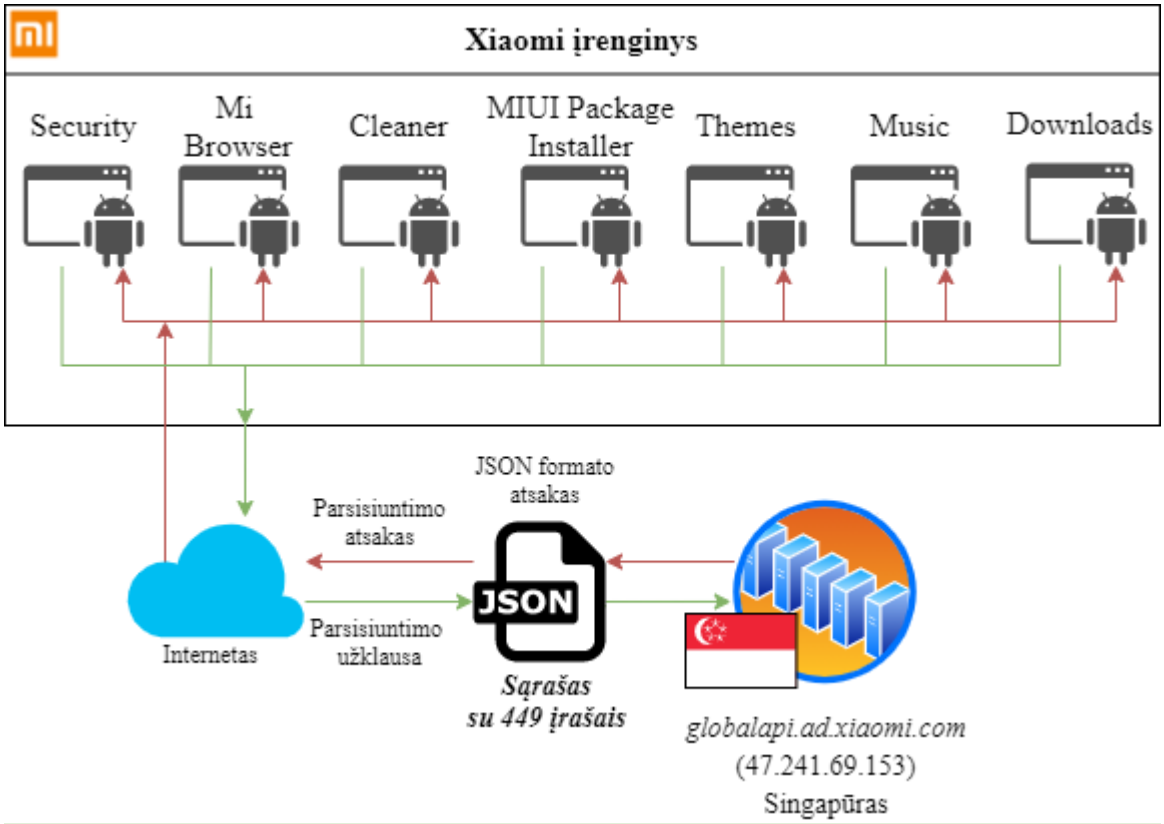
Nustatyta, kad „Xiaomi Mi 10T“ įrenginyje gamykliškai įdiegtų sisteminių aplikacijų inicializacijos metu, šios aplikacijos kreipiasi į Singapūre esantį serverį adresu „globalapi.ad.xiaomi.com“ (IP adresas – 47.241.69.153) ir atsisiunčia JSON formato failą „MiAdBlacklistConfig“, išsaugo šį failą aplikacijų metaduomenų kataloguose. Aplikacijų, kurių metaduomenų kataloguose buvo rastas „MiAdBlacklistConfig“ failas, sąrašas pateikiamas 13 lentelėje.

13 lentelė. Mob. aplikacijų, naudojančių „MiAdBlacklistConfig“ failą, sąrašas

Eil. Nr.	Aplikacijos pavadinimas	Aplikacijos identifikatorius	Įrenginys
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*	

Aplikacijoms atsisiuntus rinkmeną, yra fiksuojama atsisiuntimo data, siekiant sąrašą atnaujinti periodiškai. Rinkmenos „MiAdBlacklistConfig“ atsisiuntimo schema pateikta 11 paveiksle.

[29] Apple privatumo politika. *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 privatumo politika. *https://privacy.mi.com/all/en_IN/*



11 pav. Rinkmenos „MiAdBlacklistConfig“ atsisiuntimo schema

Šioje rinkmenoje saugomas sąrašas, kurį sudaro įvairių religinių ir politinių grupių bei visuomeninių judėjimų pavadinimai, vardai ir kita informacija (tyrimo metu „MiAdBlacklistConfig“ rinkmenoje buvo fiksuoti 449 įrašai). Rinkmenos „MiAdBlacklistConfig“ fragmentas pateiktas 14 lentelėje.

14 lentelė. Rinkmenos „MiAdBlacklistConfig“ fragmentas

Eil. Nr.	Originalas	Vertinys
1	"宗教虔信者阵线",	„Religinių tikinčiųjų frontas“,
...		
22	"西藏自由",	„Tibetas laisvas“,
...		
60	"蒙古独立",	„Mongolijos nepriklausomybė“,
61	"89民运",	„89 demokratijos judėjimas“,
62	"基督灵恩布道团",	„Krikščioniška charizmatiška misija“,
...		
145	"伊斯兰联盟",	„Islamo lyga“,
…		
201	"民运",	„Demokratinis judėjimas“,
202	"妇女委员会",	„Moterų komitetas“,
203	"伊斯兰马格里布基地组织",	„Al-Qaida islamo Magrebe“,
204	"人民报",	„Žmonių dienraštis“,

205	"巴勒斯坦解放组织",	„Palestinos išlaisvinimo organizacija“,
	...	
313	"台独万岁",	„Tegyvuoja Taivano nepriklausomybė“,
	...	
369	"美国之音",	„Amerikos balsas“,
	...	
420	"89运动",	„89 judėjimas“,
	...	
449	"夏米斯丁艾合麦提·阿布都米吉提"	„Xia Misteen Ahemet Abu Dumijiti“

Atlikus Xiaomi aplikacijų kodo analizę, buvo nustatyta, kad aplikacijose yra realizuotos programinės klasės, skirtos įrenginyje atvaizduojamos tikslinės multimedijos filtravimui pagal atsisiųstą rinkmenoje „MiAdBlacklistConfig“ esantį sąrašą. Šio programinio kodo fragmentas pateiktas 16 lentelėje.

16 lentelė. „Xiaomi“ įrenginyje naudojamas turinio filtravimo kodo fragmentas

```
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;
}
```

Įvykdžius aplikacijos „Mi Browser“ programinės dekompozicijos tyrimą buvo nustatyta, kad aplikacija vykdo „MiAdBlacklistConfig“ failo atsisiuntimo funkcionalumą, tačiau nevykdo turinio filtravimo pagal „MiAdBlacklistConfig“ faile pateiktą sąrašą. Remiantis „Xiaomi“ programiniu kodu, šis funkcionalumas deaktyvuotas „Europos Sąjungos regione“. Aplikacijos „Mi Browser“ generuojamas įvykių registracijos turinys yra pateiktas 17 lentelėje.

17 lentelė. Aplikacijos „Mi Browser“ generuojamas įvykių registracijos turinys

Eil.	Funkcijos	Parametras 1	Parametras 2

Nr.	pavadinimas		
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,"mElapsed":0,"mIsBid":0,"mCost":333682}

Manoma, kad šis funkcionalumas leidžia „Xiaomi“ įrenginiui vykdyti į telefoną įeinančio tikslinės multimedijos turinio analizę – ieško reikšminių žodžių pagal iš serverio gautą *„MiAdBlacklist“* sąrašą.

Užfiksavus, kad turinyje yra ieškomų reikšminių žodžių, įrenginys atlieka šio turinio filtravimą ir vartotojas jo matyti negali. Duomenų analizės principas leidžia analizuoti ne tik žodžius, parašytus hieroglifais – iš serverio reguliariai atsiunčiamas sąrašas gali būti suformuotas bet kokia kalba. Svarbu pabrėžti, kad šis funkcionalumas yra aktyvuojamas gamintojo nuotoliniu būdu. Manoma, kad tokio funkcionalumo egzistavimas gali kelti grėsmę laisvai informacijos prieigai, riboti jos pasiekiamumą. Galima teigti, kad tai yra svarbu ne tik Lietuvai, bet ir visoms šalims, naudojančioms Xiaomi įrenginius.

4. „Xiaomi“ įrenginiuose norint prisiregistruoti prie Cloud, reikia priregistruoti SIM kortelę. Siunčiamos žinutės nėra atvaizduojamos telefone. Vartotojo duomenų nutekinimo rizika

Atliktuose tyrimuose nustatyta, kad vartotojui pasirinkus naudoti „Xiaomi“ debesijos paslaugas, yra vykdoma vartotojo mob. telefono numerio registracija Singapūre esančiuose serveriuose. Tai atliekama įrenginiui į specialų telefono numerį išsiuntus šifruotą SMS žinutę. „Xiaomi“ įrenginyje vykdoma registracijos procedūra prie „Xiaomi“ debesijos paslaugų, išsiunčiant SMS žinutę, pateikta 12 paveiksle.

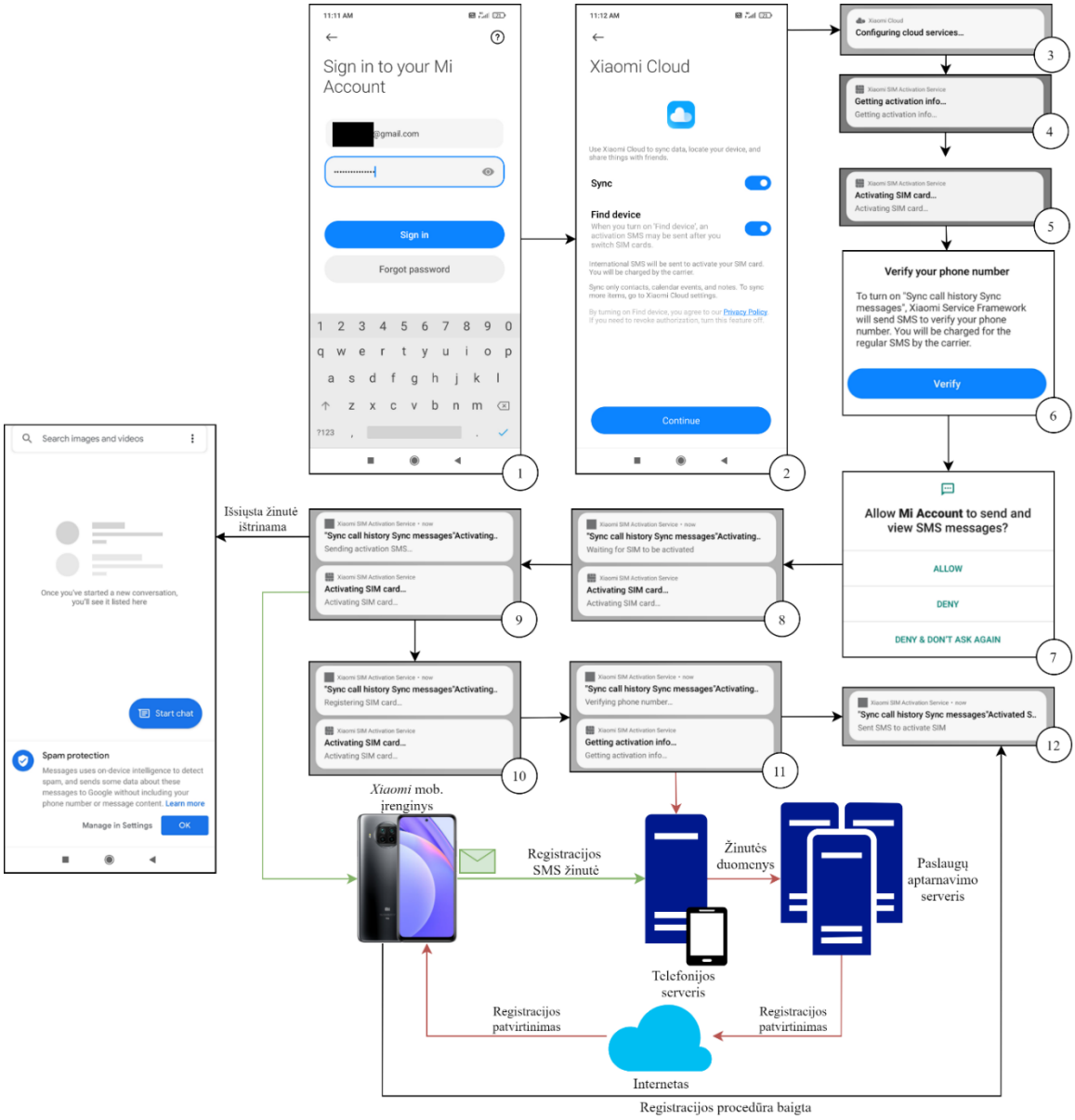
Vartotojui pirmą kartą bandant jungtis prie „Xiaomi Cloud“ paslaugos, įrenginys reikalauja prisijungti prie (1) „Xiaomi Account“ paskyros. Suvedus prisijungimo duomenis ir sėkmingai prisijungus prie paskyros, išvedamas parinkčių langas (2), kuriame galima įjungti ir išjungti pagrindines „Xiaomi Cloud“ funkcijas – duomenų sinchronizaciją ir įrenginio praradimo atveju naudojamą įrenginio geografinės vietovės nustatymą.

Pasirinkus normas funkcijas, įrenginyje, foniniame rėžime veikiantis servisas pradeda SIM kortelės duomenų rinkimo procedūras (3, 4 ir 5). Servisui pabaigus vykdyti SIM kortelės duomenų rinkimo procedūras, vartotojui yra pateikiamas informacinis langas (6), kuriame yra nurodoma, kad norint įgalinti skambučių istorijos ir pranešimų sinchronizacijos funkcionalumą, įrenginys turi išsiųsti SMS žinutę, siekiant patikrinti telefono numerį.

Taip pat informaciniame lange yra nurodoma, kad vartotojas už SMS žinutės išsiuntimą gali būti apmokestintas standartiniais mob. ryšio tiekėjo tarifais. Vartotojui uždarius informacinį langą, vartotojui yra pateikiamas operacinės sistemos langas (7), kuriame yra vartotojo klausiama, ar SIM kortelės registracijos servisui leisti automatiškai siųsti SMS žinutes. Vartotojui sutikus yra pradedama automatinė telefono numerio registracijos procedūra (8).

Įrenginys iš **bendrojo** paslaugų aptarnavimo serverio atsisiunčia procedūros konfigūracijos duomenų struktūrą, kurioje yra nurodyta serverio, su kuriuo vykdoma tolimesnė tinklo komunikacija, adresas, SMS adresato telefono numeris ir kiti parametrai. Tuomet įrenginys suformuoja SMS žinutę ir siunčia ją konfigūracijos duomenų struktūroje nurodytu telefono numeriu (9). Išsiųsta žinutė iš karto yra ištrinama iš siųstų žinučių žurnalo.

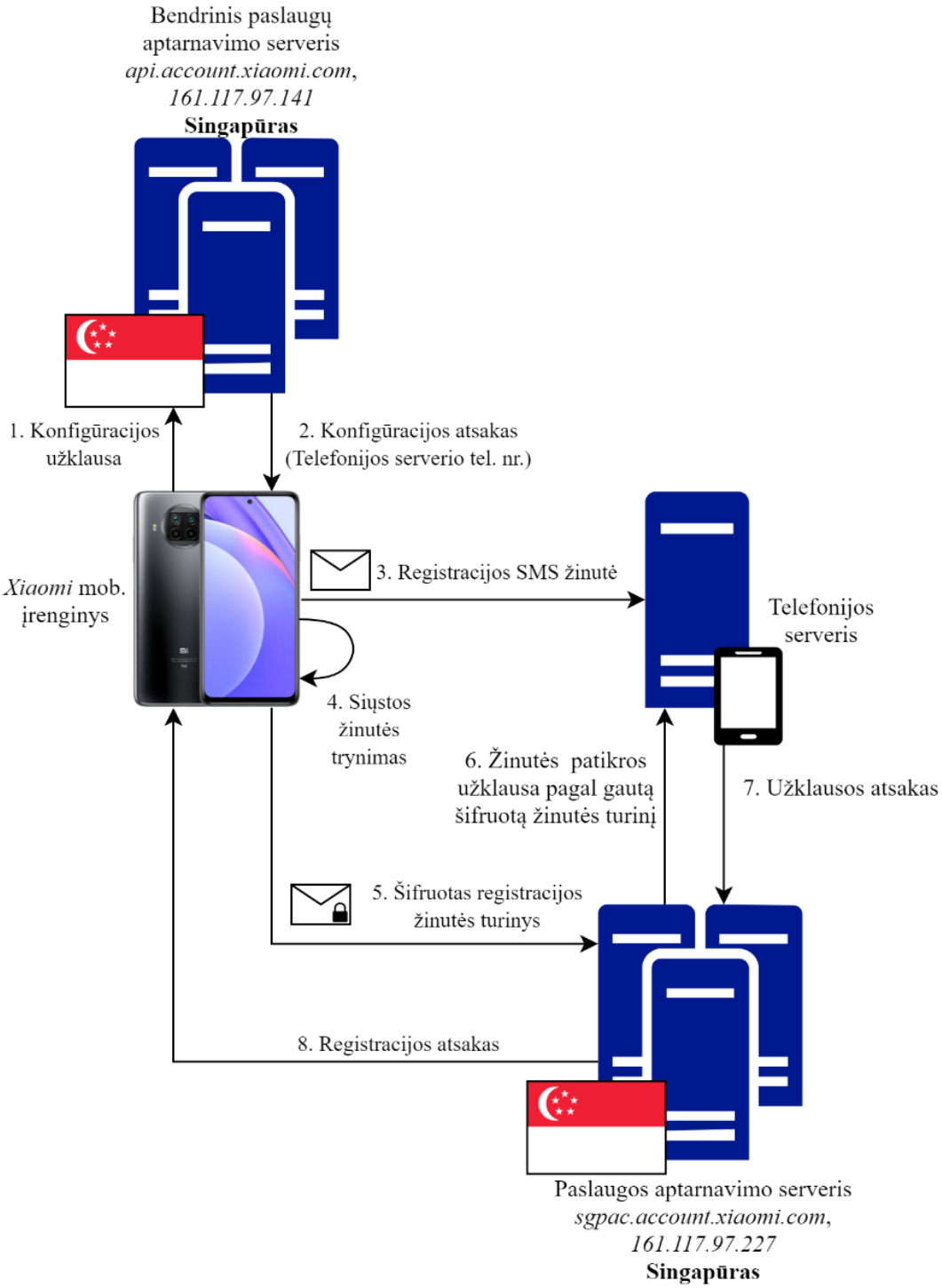
Tuo pačiu metu, surinkti SIM kortelės duomenys yra išsaugomi vidinėje serviso duomenų bazėje (10). Išsiuntus SMS žinutę, jos turinys yra užšifruojamas ir siunčiamas paslaugų aptarnavimo serveriui, kurio adresas yra nurodytas konfigūracijos duomenų struktūroje, kartu su registracijos patvirtinimo užklausa (11).



12 pav. Telefone vykdoma registracijos procedūra prie „Xiaomi“ debesijos paslaugų, išsiunčiant SMS žinutę

Įrenginys išsiuntęs registracijos užklausą paslaugų aptarnavimo serveriui, iš jo gauna užklausos atsaką, kuriame nurodytas registracijos (teigiamas arba neigiamas) rezultatas (12).

Nustatyta, kad telefono numerio registravimas yra vykdomas, nepriklausomai, kaip vartotojas pasirenka būti autentifikuotas – pagal telefono numerį ar el. pašto adresą. Svarbu pažymėti, kad išsiųsta šifruota SMS žinutė ir jos adresatas vartotojui nėra matomas. Tyrimo metu, išjungus Xiaomi Cloud paslaugos funkcionalumą, žinučių siuntimas nebuvo fiksuotas. Detalesnė tinklo srauto schema pateikta 13 paveiksle.



13 pav. Registracijos prie „Xiaomi“ debesijos paslaugų tinklo schema

Pradėjus telefono numerio registracijos procesą, įrenginys siunčia užklausą bendriniam paslaugų aptarnavimo serveriui, esančiam Singapūre (1), iš kurio kaip atsaką gauna duomenų struktūrą. Šioje duomenų struktūroje yra nurodytas tikslinio šios paslaugos aptarnavimo serverio adresas, telefonijos serverio numeris ir kiti registracijos procedūrai naudojami parametrai (2). Tuomet įrenginys suformuoja ir išsiunčia SMS žinutę gautoje duomenų struktūroje nurodytu telefono numeriu (3). Išsiųsta žinutė yra nedelsiant ištrinama iš siųstų žinučių žurnalo (4). Išsiuntus žinutę, įrenginys kreipiasi į paslaugos aptarnavimo serverį, esantį Singapūre ir siunčia telefonijos serveriui siųstos žinutės užšifruotą turinį

(5). Paslaugos aptarnavimo serveris komunikuoja su telefonijos serveriu, kuriam buvo išsiųsta SMS žinutė (6, 7). Komunikacijos metu yra tikrinama telefono ryšiu siųsta žinutė ir mobilaus interneto tinklo traktu išsiųstas šifruotas žinutės turinys. Sėkmingai įvykdžius žinučių patikrą, įrenginiui yra suformuluojamas užklausos atsakas, pridedant registracijos rezultatą (8).

Svarbu pabrėžti, kad jei registracijos metu įrenginyje SIM kortelė nėra įdiegta, registracijos procesas yra nutraukiamas ir įrenginio ekrane yra atvaizduojamas klaidos pranešimas.

Prieš įrenginiui išsiunčiant telefono numerio registracijos SMS žinutę, įrenginys kreipiasi į bendrinį paslaugų serverį, esantį Singapūre, kurio adresas – „api.acount.xiaomi.com“ (IP adresas – 161.117.97.141).

Komunikacijos metu, įrenginys parsisiunčia registracijos procesui reikalingą konfigūracijos duomenų struktūrą. Šioje duomenų struktūroje yra nurodytas telefonijos serverio telefono numeris, paslaugos aptarnavimo serverio adresas ir kiti duomenys. Įrenginio vykdytos tinklo komunikacijos su bendruoju paslaugų serveriu duomenų ištrauka pateikta 18 lentelėje.

18 lentelė. Konfigūracijos atsisiuntimo tinklo srauto ištrauka

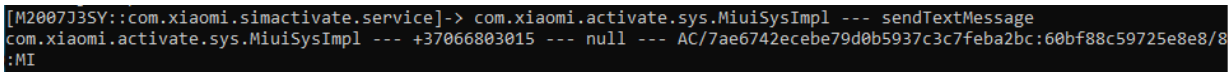
```
GET /pass/configuration HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; M2007J3SY MIUI/V12.0.18.0.QJDEUXM) APP/unknown MK/TWkgMTBU
Cookie: sdkVersion=accountsdk-2020.01.09
Host: api.account.xiaomi.com
Connection: Keep-Alive
Accept-Encoding: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

Įrenginys siunčia SMS žinutę konfigūracijos duomenų struktūroje nurodytu telefono numeriu.

Telefono numerio registracijos serviso „Xiaomi SIM Activation Service“ tyrimo metu nustatyta, kad įrenginys vykdo automatinio SMS žinutės siuntimo funkciją. SMS žinutės adresatas ir žinutės turinys pateiktas 14 paveiksle.



14 pav. SMS žinutės turinys ir siuntimo procesas

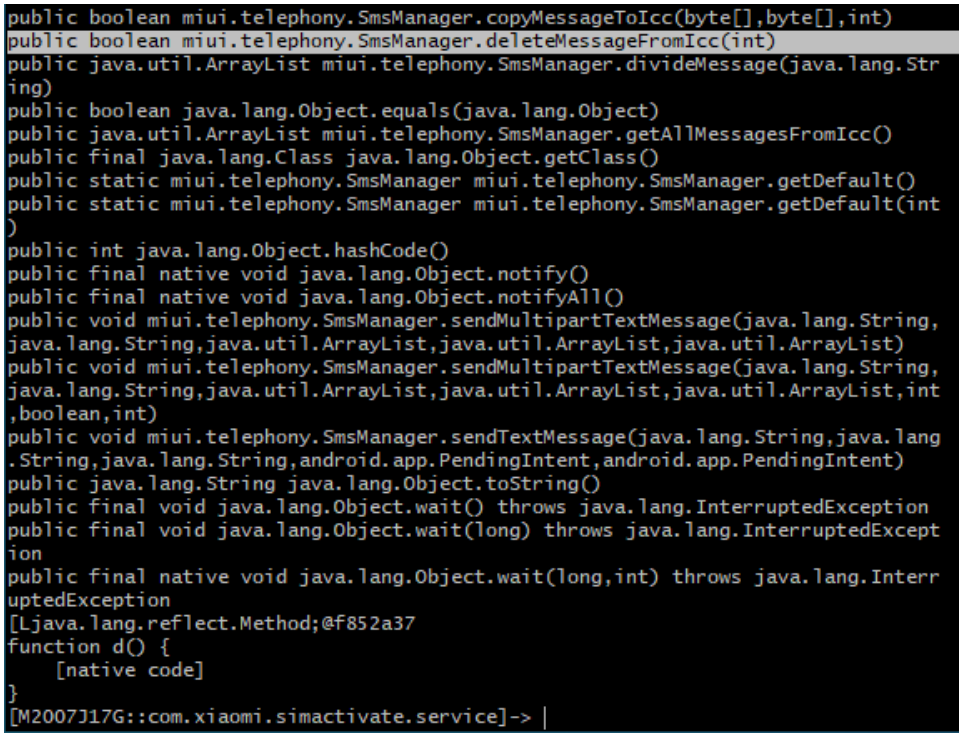
Atlikus gamykliškai įdiegto sisteminio serviso „Xiaomi SIM Activation Service“ dekompozicijos tyrimą, buvo nustatyta, kad aplikacija vykdo automatinio SMS žinutės išsiuntimo funkciją, naudojant išorinę programinę klasę „miui.telephony.SmsManager“, kuri nėra kompiliuojama ir archyvuojama į serviso diegiamąją rinkmeną.

SMS žinutės siuntimo programinio kodo fragmentas pateiktas 19 lentelėje.

19 lentelė. SMS žinutės siuntimo programinio kodo fragmentas

```
public void sendTextMessage(int i, String str, String str2, String str3, PendingIntent pendingIntent,
PendingIntent pendingIntent2) {
    try {
        Class<?> cls = Class.forName("miui.telephony.SmsManager");
        Object invoke = 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);
    }
}
```

Verta pabrėžti, kad minėtoje išorinėje programinėje klasėje „miui.telephony.SmsManager“ yra realizuojantis funkcionalumas, leidžiantis vykdyti SMS žinučių trynimo funkcijas. SMS žinučių siuntimo, trynimo ir kitos funkcijos, realizuotos išorinėje programinėje klasėje „miui.telephony.SmsManager“ yra pateiktos 15 paveiksle.



15 pav. SMS žinučių siuntimo, trynimo ir kt. funkcijos, realizuotos išorinėje programinėje klasėje „miui.telephony.SmsManager“

Įrenginiui išsiuntus SMS žinutę, konfigūracijos duomenų struktūroje nurodytu telefono numeriu, įrenginys siunčia užšifruotą SMS žinutės turinį adresu „sgpac.account.xiaomi.com“ (Singapūras).

Serveris pagal gautus šifruotus duomenis vykdo turinio patikrą su telefonijos serverio gautais SMS žinutės duomenimis ir siunčia aktyvacijos rezultatą mobiliajam įrenginiui. Tinklo srauto išrašas pateiktas 20 lentelėje.

20 lentelė. Komunikacija su paslaugos serveriu, esančiu Singapūre

```
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-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_5ODSHBbJv5XO6wRTIUfNCEerj978hkm5RhLrK19IYsgPUeVQoXbYJ9Di8-B9WaMvgJeAVwudc_nYD9LWJw28g8UO1Y_5A9V1kqzNCf8e1tfLftN_Y0UXpvy4cXlzHISL5yiGj2sI77KFzS20PgKfocTxNcleEuLlTEjTY_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":"....."}
```

Tyrimo metu fiksuota, kad įrenginys vykdė komunikacijas su serveriais, esančiais Singapūre. Fiksuotų komunikacijų sąrašas pateiktas 21 lentelėje.

21 lentelė. Komunikacijos su serveriais, esančiais Singapūre, informacija

Eil. Nr.	Domenas	Adresas	Duomenys, Baitai	Valstybė	Paskirtis
1	api.account.xiaomi.com	161.117.97.141	9200	Singapūras	**Bendrinis paslaugų serveris** *Iš serverio telefonui siunčiama konfigūracija autentifikacijai – SMS tel. Nr., paslaugos serverio adresas ir kt.*
2	sgpac.account.xiaomi.com	161.117.97.227	48990	Singapūras	**Paslaugos serveris** *Pagal iš telefono gautą SMS žinutę sugeneruojamas ir telefonui nusiunčiamas registracijos atsakas.*

Domenams „api.account.xiaomi.com“ ir „sgpac.account.xiaomi.com“ priklausantys IP adresai yra registruoti įmonėje „Alibaba.com Singapore E-Commerce Private Limited“. Bendrovė Alibaba – informacinių technologijų įmonė, 1999 m. įsteigta Kinijos Liaudies Respublikoje. Yra žinoma, kad Kinijos informacinių technologijų įmonės yra įpareigotos perduoti bet kokio pobūdžio valdomą informaciją Kinijos vyriausybei ar jos žinybinėms agentūroms[32].

Automatizuotas žinučių siuntimas ir jų slėpimo programinis funkcionalumas kelia potencialias grėsmes įrenginio ir asmens duomenų saugumui – šiuo būdu, vartotojui nežinant, gali būti renkami ir perduodami įrenginio duomenys į nutolusius serverius.

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