NCSC при отделе
инноваций и обучения MOND
support@ims.nksc.lt

2021-08-23

Оценка кибербезопасности мобильных устройств, поддерживающих технологию 5G, проданных в Литве

АНАЛИЗ ПРОДУКЦИИ, ПРОИЗВОДИМОЙ *Huawei*, *Xiaomi* а также *OnePlus*

Вступление

Чтобы обеспечить использование безопасного программного и аппаратного обеспечения в стране, Национальный центр кибербезопасности (NCSC) при Министерстве национальной обороны провел оценку кибербезопасности мобильных устройств, поддерживающих технологию 5G, продаваемых в Литве китайскими производителями. В данном анализе представлены результаты оценки смартфонов производства Huawei, Xiaomi и OnePlus.

Huawei, Xiaomi и OnePlus - китайские производители ИТ и бытовой электроники с международным присутствием.[1] и сильное присутствие на европейском рынке[2]. В 2020 году эти производители представили на литовском рынке смартфоны с поддержкой мобильных технологий пятого поколения (5G). Оценка безопасности проводилась для широко доступного Huawei P40 5G.[3], Xiaomi Mi 10T 5G[4] и OnePlus 8T 5G[5] мобильные устройства. Изображения устройств, исследованных в ходе оценки, показаны на рисунке 1.

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

Рисунок 1: Устройства, проверенные в оценке. Виды передней и задней панели

---

1 CNET. «Huawei, OnePlus и другие: крупнейшие китайские бренды смартфонов, о которых вам следует знать». *https://www.cnet.com/news/huawei-oneplus-china-biggest-smartphone-brands-you-should-know-about-lenovomeizu-xiaomi-oppo-vivo/*

2 Контрапункт. Европейский рынок смартфонов упал на 14% г / г в 2020 г .; Xiaomi выигрывает, а Huawei и Samsung проигрывают.*https://www.counterpointresearch.com/european-smartphone-market-2020/*

3 Huawei. Технические параметры Huawei P40 5G.*https://consumer.huawei.com/en/phones/p40pro/specs/*

4 Xiaomi. Технические параметры Xiaomi Mi 10T 5G.*https://www.mi.com/global/mi-10t-pro/specs/*

5 OnePlus. Технические параметры OnePlus 8T 5G.*https://www.oneplus.com/lt/8t/specs*

Несмотря на известность этих брендов, в период с 2017 по 21 год корпорации столкнулись с проблемами безопасности разрабатываемого оборудования; согласно базе CVE (Common Vulnerabilities and Exposures), 9 уязвимостей[6] связанных с риском утечки персональных данных для продукции Xiaomi (8 из этих уязвимостей могут быть реализованы удаленно), 144 уязвимости[7] были выявлены для продуктов Huawei в течение этого периода (28 уязвимостей было выявлено в 2020 году; 23 - в первой половине 2021 года), большинство из которых были связаны с нарушением функциональности устройства, а одна уязвимость была выявлена в 2020 году, позволяя злоумышленнику использовать третьи - программное обеспечение party для отправки текста SMS с мобильного устройства, когда мобильное устройство было заблокировано.[8]

По оценкам различных источников, эти производители занимают лидирующие позиции.[9,10] на рынке мобильных устройств, широкий ассортимент продуктов, развитие новых технологий и заметный рост в Литве, несомненно, делают их подходящим объектом для исследований в области кибербезопасности.

Выводы исследования

Анализ разложения, выполненный на мобильных устройствах производства Huawei, Xiaomi и OnePlus, выявил 10 случаев повышенного риска кибербезопасности. Эта оценка кибербезопасности анализирует 4 риска кибербезопасности, связанных с общей безопасностью заводских приложений на устройствах, угрозами утечки личных данных и ограничениями свободы выражения мнений. Планируется подробно описать другие риски кибербезопасности, выявленные в этом комплексном исследовании, и представить оценку таких рисков к концу 2021 года. В этом анализе рассматриваются вопросы, связанные с безопасностью персональных данных.

Анализ показал, что процесс установки мобильных приложений на устройства Huawei характеризуется неопределенностью кибербезопасности. Для установки мобильных приложений на телефоны Huawei используется производственная инфраструктура, которая состоит из официального магазина электронных приложений AppGallery и платформ распространения периферийных приложений.

Когда пользователь намеревается установить мобильное приложение на устройство Huawei, поиск мобильного приложения выполняется в магазине AppGallery; когда приложение найдено, оно загружается и устанавливается на мобильное устройство. Однако, если приложение не найдено в официальном магазине, пользователь автоматически перенаправляется на платформы распространения периферийных приложений, с которых мобильное приложение загружается на мобильное устройство для установки. Стоит отметить, что большинство платформ распространения приложений расположены в странах, не подпадающих под действие Общего регламента защиты данных, что создает соответствующий риск утечки метаданных пользователей. Исследование показало, что часть мобильных приложений, содержащихся на платформах распространения приложений, является имитацией оригинальных приложений, с вредоносным функционалом или заражением вирусами; такие приложения могут быть загружены и установлены пользователем на мобильный телефон, тем самым ставя под угрозу безопасность устройства и содержащихся в нем данных.

Риски безопасности данных также были выявлены в устройстве Xiaomi; установленные на заводе системные приложения отправляют статистические данные об активности определенных приложений, установленных на устройстве, на серверы китайского поставщика облачных услуг Tencent, расположенного в Сингапуре, США,

---

[6] CVE база данных. Публично объявил уязвимости в Xiaomi продукты. *https://www.cvedetails.com/vulnerability-list/vendor_id-19038/MI.html*

[7] База данных CVE. Публично объявленные уязвимости в Huawei продукты. *https://www.cvedetails.com/vendor/5979/Huawei.html*

[8] База данных CVE. Публично объявлено уязвимости в OnePlus продукты. *https://www.cvedetails.com/vendor/16036/Oneplus.html*

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

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

Нидерланды, Германия и Индия.

Выяснилось, что оригинальный браузер устройства Mi Browser использует два модуля сбора данных: Google Analytics и Sensor Data. Модуль Google Analytics, установленный на устройстве, позволяет читать историю просмотров и поиска, отправлять эти данные на аналитические серверы, к которым имеет доступ Xiaomi, и данные, которые использует Xiaomi.[11]. Эта функция активируется путем регистрации мобильного телефона в маркетинговой программе Xiaomi User Experience. По умолчанию это происходит автоматически при первой активации телефона или при сбросе к заводским настройкам.

Было обнаружено, что модуль Sensor Data, используемый в устройстве, собирает статистическую информацию по 61 параметру (время активации приложения, используемый язык и т. Д.) Об активности используемых приложений. Собранная статистика отправляется по зашифрованному каналу на серверы Xiaomi в Сингапуре, что не регулируется Общими правилами защиты данных. По данным международных источников, выявлены явные случаи несанкционированного сбора пользовательских данных компанией Xiaomi.[12,13]. Можно сказать, что потенциально чрезмерный сбор и использование аналитических данных представляет угрозу конфиденциальности личных данных.

Также было установлено, что когда пользователь решает использовать облачные сервисы Xiaomi, номер мобильного телефона пользователя регистрируется на серверах, расположенных в Сингапуре. Для этого устройство отправляет зашифрованное SMS-сообщение на специальный номер телефона. После получения SMS-сообщения сервер синхронизирует его с сервером Xiaomi в Сингапуре, с которого телефон загружает подтверждение через мобильный Интернет, позволяя пользователю подключиться к облачному сервису Xiaomi. Установлено, что регистрация телефонного номера осуществляется независимо от того, выбирает ли пользователь аутентификацию по номеру телефона или по адресу электронной почты. Важно отметить, что зашифрованное и отправленное SMS-сообщение и его адресат не видны пользователю.

Автоматическая отправка сообщений и программная функциональность их сокрытия создают потенциальные угрозы безопасности устройства и личных данных; Таким образом, без ведома пользователя данные устройства могут быть собраны и переданы на удаленные серверы.

Сервис Xiaomi Cloud предназначен для хранения и синхронизации данных, хранящихся на устройстве (данные, хранящиеся в книге контактов, история звонков, SMS-сообщения, фотографии, заметки, настройки Wi-Fi и история просмотров и т. Д.) На удаленных серверах. Используя этот сервис, пользовательские данные отправляются на серверы, расположенные в Сингапуре.

Было обнаружено, что системные приложения Xiaomi (Security, MiBrowser, Cleaner, MIUI Package Installer и Themes) регулярно загружают обновленный файл конфигурации производителя MiAdBlacklistConfig с сервера, расположенного в Сингапуре. Этот файл содержит список, состоящий из названий, имен и другой информации о различных религиозных и политических группах и социальных движениях (на момент проведения анализа в файле MiAdBlacklistConfig было обнаружено 449 записей). Анализ кода приложения Xiaomi показал, что в приложениях реализованы программные классы для фильтрации целевого мультимедиа, отображаемого на устройстве, в соответствии с загруженным списком MiAdBlacklistConfig.

Это позволяет устройству Xiaomi выполнять анализ целевого мультимедийного контента, поступающего в телефон: искать ключевые слова на основе списка MiAdBlacklist, полученного с сервера. Когда определено, что такое содержимое содержит ключевые слова из списка, устройство блокирует это содержимое. Считается, что эта функция может представлять потенциальную угрозу свободному доступу к информации.

NCSC рекомендует пользователям проявлять интерес к используемому программному и аппаратному обеспечению и ответственно оценивать предлагаемые функциональные возможности оборудования.

---

11 Xiaomi. Политика конфиденциальности.*https://privacy.mi.com/all/en_IN/*

12 Информация Forbes. *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 Информация об Android Authority. *https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444 /*

Детали исследования

Основные программные характеристики мобильных устройств, включенных в анализ, приведены в таблице. 1, с указанием основы операционной системы (ОС), модификации основы операционной системы производителем, версии ядра операционной системы и дат обновлений безопасности.

Таблица 1. Основные программные характеристики мобильных устройств, включенных в анализ.

Название устройства	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
Основа ОС, установленная на заводе	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Модификация производителя установленная на заводе основа	EMUI 10.1.0	MIUI Global 12.0.10 (QJDEUXM)	Кислородная ОС 11.0.5.6.KB05BA
ОС Последняя доступная ОС	Android 10	Android 11	Android 11
Модификация производителя последняя доступная ОС	EMUI 11.0.0.151 (C432E5R5P3)	MIUI Глобальный 12.0.2.0 (RJSEUXM)	Кислородная ОС 11.0.8.13.KB05AA
Последняя доступная дата выпуска ОС	2020-12-24	2021-05-25	2021-04-08
Версия ядра ОС	4.14.116	4.19.81-pref-gef23740	4.19.110-преф +
Исходный уровень пакета обновления безопасности	2020-04-01	2020-09-01	2020-10-01
Дата последнего обновления безопасности	2021-06-01[14]	2021-03-01[15]	2021-04-01[16]
Количество обновлений безопасности	9	3	4

Все исследованные мобильные устройства основаны на операционной системе Android; Huawei P40 и Xiaomi Mi 10T используют версию системы 10, в то время как OnePlus 8T использует последнюю в настоящее время версию системы, 11. Стоит отметить, что по умолчанию стандартная операционная система Android 11 имеет более широкие возможности контроля доступа,[17] позволяя пользователю лучше контролировать доступ приложений к данным, хранящимся на устройстве.

Обновления безопасности операционной системы Android - это обновления компонентов операционной системы, предназначенные для исправления уязвимостей программного обеспечения, которые угрожают безопасности устройства или данных, хранящихся на нем. Эти обновления ориентированы на уязвимости программного обеспечения, позволяющие удаленное выполнение кода, повышение привилегий, раскрытие информации (утечка информации), отказ в обслуживании и другие типы атак. Каждое из этих обновлений безопасности устраняет от 20 до 60 уязвимостей, перечисленных в базе данных CVE. Стоит отметить, что вредоносность уязвимостей колеблется от 5,4 до 10,0 баллов (из возможных 10 баллов).

По этой причине пользователям мобильных устройств важно регулярно устанавливать эти обновления. Эти обновления безопасности для операционной системы Android выпускаются периодически, каждые 1–3 месяца. Xiaomi обязуется доставлять эти обновления на свои устройства в течение 2 лет.[18], и OnePlus взяла на себя такое обязательство сроком на 3 года.[19]. Обязательства Huawei по предоставлению обновлений операционной

14 Информация о Huawei. *https://consumer.huawei.com/en/support/bulletin/*

15 Информация в блоге Adimorah. *https://adimorahblog.com/new-stable-update-for-the-mi-10t-and-mi-10t-pro /*

16 Информация о OnePlus. https://www.oneplus.com/global/support/softwareupgrade/details?code=PM1605596915581

17 Информация об Android Authority. К. Скотт Браун,*Лучшие функции Android 11, которые вам нужно знать https://www.androidauthority.com/android-11-features-1085228/*

18 Информация о Xiaomi. *https://www.mi.com/global/service/support/security-update.html*

19 Информация о OnePlus. *https://forums.oneplus.com/threads/oneplus-software-maintenanceschedule.862347/*

обновления безопасности системы или операционной системы не обнаружены. Стоит отметить, что производитель операционной системы Android, компания Google, выпускает обновления безопасности для неизмененных версий Android Open Source Project. По этой причине обновления операционной системы и обновления безопасности операционной системы доступны раньше всех для устройств, произведенных Google.

С другой стороны, производители устройств, такие как Huawei, Xiaomi, OnePlus и другие, должны адаптировать обновления операционной системы или обновления безопасности операционной системы к модификациям производителя операционной системы, поэтому такие обновления доступны только позже для мобильных устройств этих производителей. устройств. Особенно важно подчеркнуть, что последние обновления безопасности доступны только для мобильного устройства Huawei P40. Анализ показал, что последнее обновление безопасности для Xiaomi Mi 10T было выпущено 3 месяца назад, а последнее обновление безопасности для мобильного устройства OnePlus 8T - 2 месяца назад.

NCSC отмечает, что, в соответствии с приведенной выше информацией, необходимы своевременные обновления безопасности для существующих устройств.

1. Официальный магазин Huawei AppGallery направляет пользователей в сторонние интернет-магазины, в которых приложения вредоносны или заражены вирусом

Анализ показал, что процесс установки мобильных приложений на устройства Huawei характеризуется неопределенностью кибербезопасности. Для установки мобильных приложений на телефоны Huawei используется инфраструктура производителя, которая состоит из официального магазина электронных приложений AppGallery и платформ распространения периферийных приложений (APKMonk, APKPure, Aptoide и др.). Схема интернет-магазина Huawei представлена на рисунке 1.

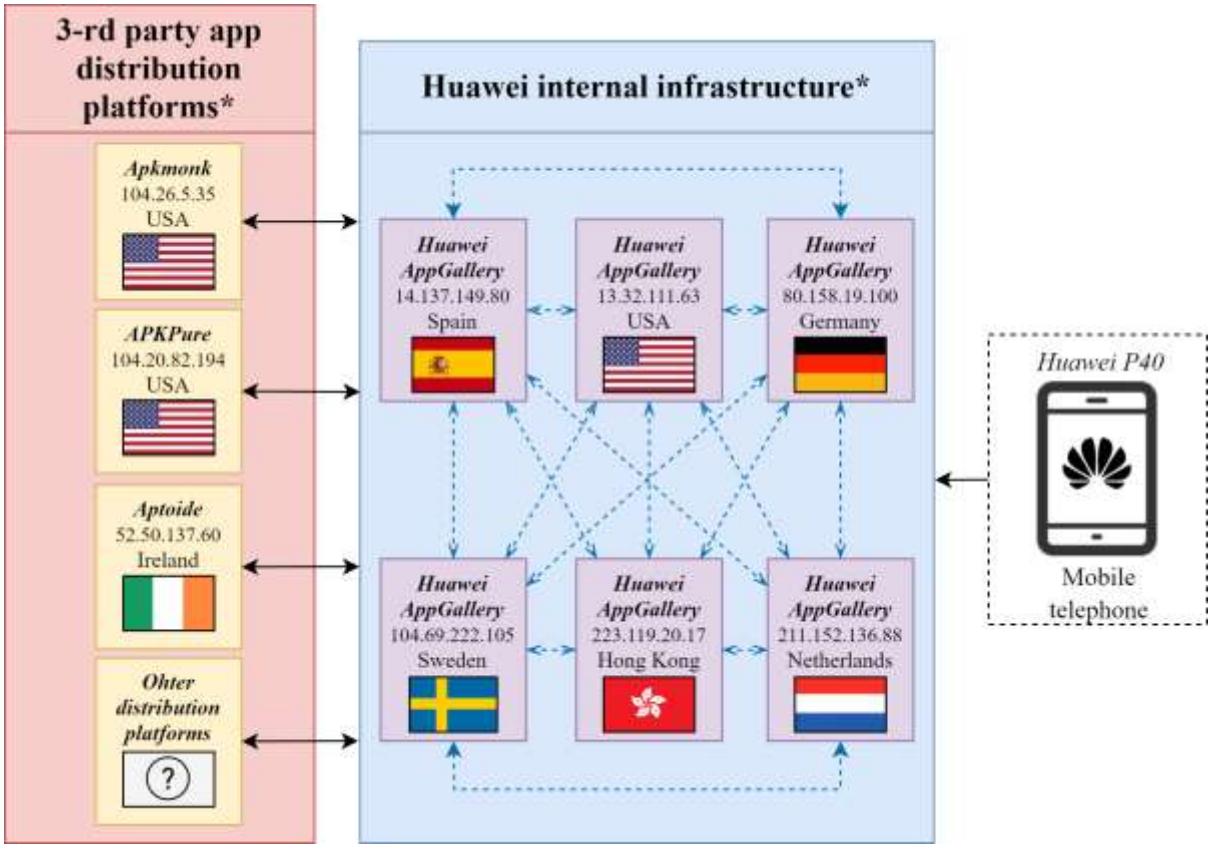


Рисунок 1: Схема интернет-магазина мобильных приложений Huawei

Инфраструктура электронного магазина мобильных приложений Huawei состоит из двух блоков: внутренней инфраструктуры Huawei AppGallery и сторонних платформ распространения приложений. Собственная инфраструктура Huawei AppGallery должна быть расположена в Испании, США, Германии, Швеции, Нидерландах, Гонконге и Таиланде. Эта инфраструктура интегрирована со сторонними платформами распространения, три из которых наиболее известные работают в США, Ирландии и Нидерландах. По разным данным[20], Инфраструктура распространения мобильных приложений Huawei в настоящее время включает 6-8 сторонних платформ распространения. Информация об инфраструктуре распространения мобильных приложений Huawei представлена в таблице 2.

Таблица 2. Информация об инфраструктуре распространения мобильных приложений Huawei с указанием параметров для внутренней галереи приложений Huawei и трех наиболее известных интегрированных внешних раздаватьплатформы ution

Линия Нет.:	Инфраструктура	Адрес:	айпи адрес	Состояние
1	Внутренний Huawei AppGallery	appdl-1-drcn.dbankcdn.com.c.cdnhwc1.com	223.119.20.17	Гонконг
2		pay7.hicloud.com	14.137.149.80	Испания
3		appdl-11-dre.dbankcdn.com appdl-11-	13.32.111.63	США
4		drcn.dbankcdn.com appdl-2-	65.9.52.144	США
5		drcn.dbankcdn.com.cdn.dnsv1.com	211.152.136.88	Нидерланды
6		uc3.hispace.hicloud.com sdkserver-	23.14.13.247	Швеция
7		dre.op.hicloud.com HWID-	104.69.222.105	Швеция
8		dre.platform.hicloud.com appdl-12-	104.69.222.145	Швеция
9		drcn.dbankcdn.com.akamaised.net appdl-12-	184.31.15.17	Швеция
10		dre.dbankcdn.com.akamaised. net appdl-1-	184.31.15.51	Швеция
11		dre.dbankcdn.com.c.cdnhwc1.com appdl-1-	119.46.76.15	Таиланд
12		dre.dbankcdn.com.c.cdnhwc1.com	119.46.76.17	Таиланд
13		appstore.huawei.com	80.158.2.135	Германия
14		metrics2.data.hicloud.com	80.158.2.190	Германия
15		www.hicloud.com	80.158.19.100	Германия
16		query.hicloud.com	80.158.19.121	Германия
17		grs.dbankcloud.com	80.158.20.103	Германия
18		Jos.hicloud.com	80.158.23.247	Германия
19		iap.hicloud.com	80.158.40.92	Германия
20		appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	101.33.11.29	Германия
21 год		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	101.33.11.45	Германия
22		appdl-4-drcn.dbankcdn.com	163.171.128.127	Германия
23		appdl-4-drcn.dbankcdn.com	163.171.128.129	Германия
24	Внешняя платформа APKMonk	www.apkmonk.com	104.26.4.35	США
25	Внешняя платформа APKPure	download.apkpure.com	104.20.83.194	США
26 год	Внешняя платформа Aptoide	en.aptoide.com	34.249.219.183	Ирландия
27		ws75.aptoide.com	34.254.115.204	Ирландия
28 год		ws75.aptoide.com	52.17.222.230	Ирландия
29		en.aptoide.com	52.50.137.60	Ирландия
30		rakam-api.aptoide.com	52.209.136.146	Ирландия
31 год		pnp.aptoide.com	54.194.247.193	Ирландия
32		en.aptoide.com	54,220,86,7	Ирландия
33		ws75.aptoide.com	54.229.235.132	Ирландия
34		CDN-mobile.aptoide.com	172.67.29.206	США
35 год		pool.apk.aptoide.com	5.79.110.134	Нидерланды
36		apkins.aptoide.com	95.211.168.137	Нидерланды
37		apkins.aptoide.com	95.211.223.52	Нидерланды

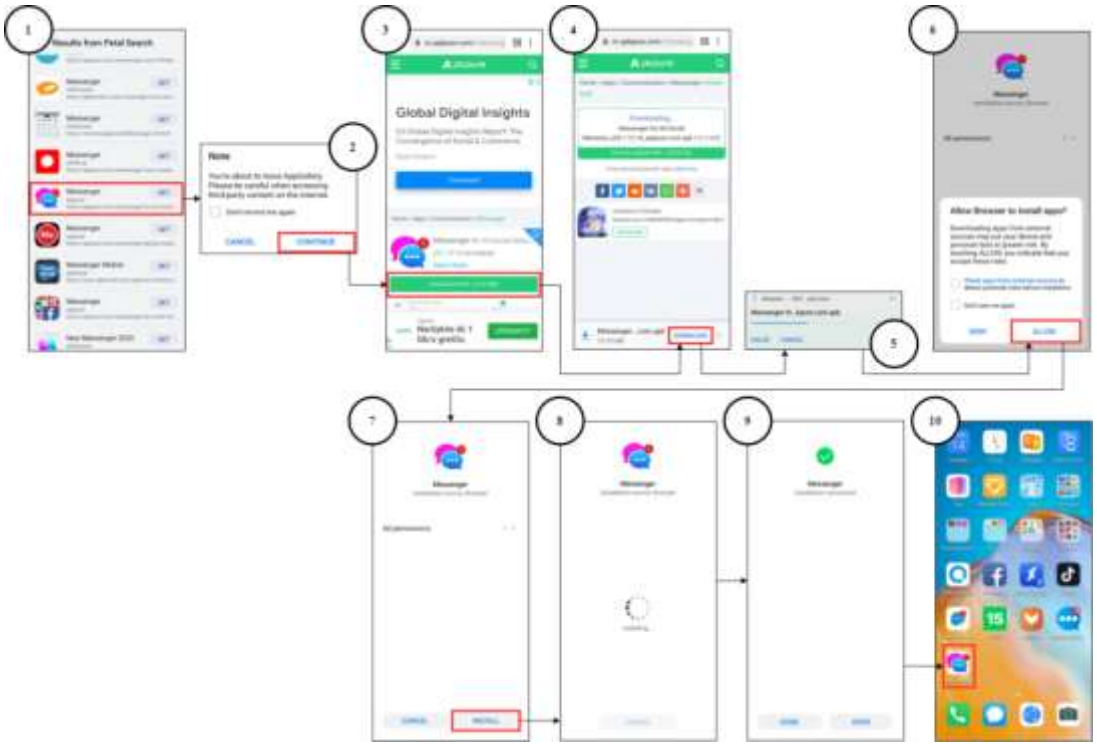
20 Информация XDA-Developers. *https://www.xda-developers.com/petal-search-download-apps-huawei-честь-смартфоны-hms /*

Когда пользователь устанавливает мобильное приложение на устройство Huawei, поиск мобильного приложения выполняется в магазине AppGallery; когда приложение найдено, оно загружается и устанавливается на мобильное устройство. Схема установки мобильного приложения с использованием платформы Huawei AppGallery представлена на рисунке 2.

Когда имя приложения вводится в поле поиска приложения Huawei AppGallery, создается список результатов поиска. Окно результатов поиска содержит раздел «Поиск лепестков». Когда выбран Petal Search, пользователю отображается список приложений, доступных через сторонние платформы распространения приложений (1). Когда пользователь выбирает приложение из этого раздела, отображается предупреждающее сообщение (2). Предупреждающее сообщение указывает, что дальнейшие действия будут происходить за пределами приложения Huawei AppGallery.

Когда пользователь закрывает окно с предупреждением, на устройстве открывается веб-браузер, пользователь перенаправляется на платформу распространения сторонних приложений. Если пользователь выбирает вариант загрузки установочного файла приложения (3) на платформе, файл загружается и сохраняется во внутренней памяти устройства (4, 5). Когда устройство завершит процесс загрузки установочного файла приложения, начнется установка приложения.

Поскольку в этом случае установка приложения инициируется веб-браузером устройства, пользователю отображается информационное окно (6) с запросом авторизации для запуска процедуры установки приложения с помощью веб-браузера. После того, как пользователь дал разрешение, отображается окно установки приложения (7), в котором снова запрашивается ввод данных для начала установки. После того, как пользователь подтвердит установку приложения, приложение будет установлено (8, 9), а в главное окно (10) добавляется значок для вновь установленного приложения.



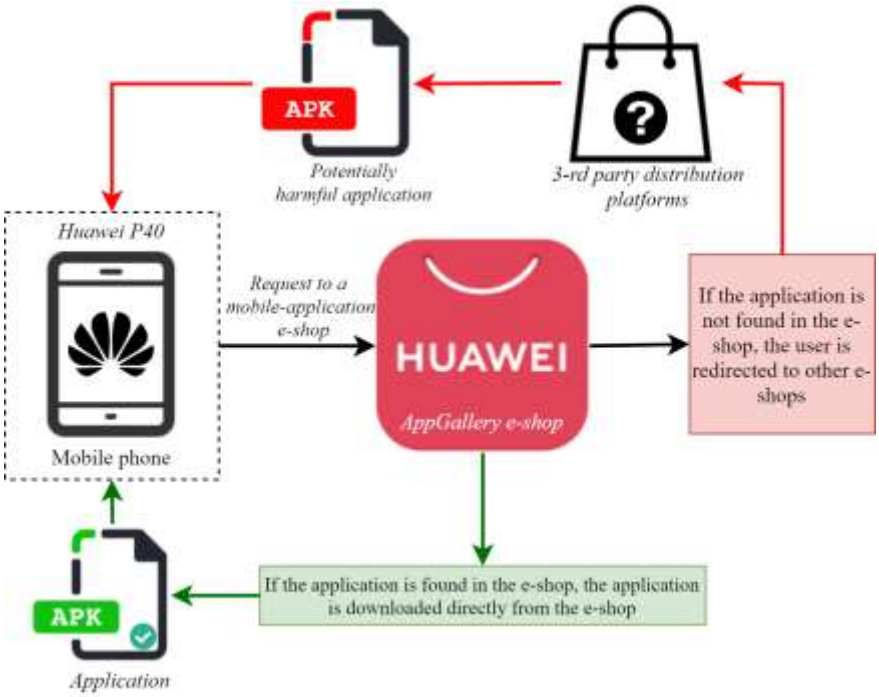
Фигура 2: Схема установки мобильного приложения с помощью платформы Huawei AppGallery

Если искомое приложение недоступно в магазине Huawei AppGallery, пользователь

автоматически перенаправляется на периферийные сторонние платформы распространения приложений, с которых мобильное приложение загружается в телефон для установки.

Анализ показал, что часть мобильных приложений, доступных на таких платформах распространения, являются подделками подлинных приложений с вредоносной функциональностью или заражением вирусами; такие приложения могут быть загружены и установлены пользователем на мобильный телефон, тем самым ставя под угрозу безопасность устройства и содержащихся в нем данных.

Принципиальная схема установки приложения Huawei, включая сторонние платформы распространения для их установки, показана на рисунке 3.



Фигура 3: Принципиальная схема установки приложения Huawei, в том числе стороннего платформы распространения

Стоит отметить, что часть инфраструктуры распространения приложений, используемой Huawei, находится в странах, на которые не распространяется Общий регламент защиты данных. Важно отметить, что мобильное устройство, загружающее приложение из электронного магазина мобильных приложений, расположенного в стране, на которую распространяется GDPR, может выполнять запросы в третьи страны, не подпадающие под действие Регламента. Это создает соответствующий риск утечки метаданных пользователя.

В ходе анализа был изучен интернет-магазин AppGallery, работающий в инфраструктуре Huawei, и три наиболее известные интегрированные сторонние платформы распространения: APKMonk, Aptoide и APKPure. Стоит отметить, что информацию о разработчиках APKMonk и APKPure в свободно доступных источниках найти не удалось. Согласно Aptoide[21 год], головной офис дистрибьюторской платформы зарегистрирован в Португалии (Лиссабон), а филиалы компании работают в Китае (Шэньчжэнь) и Сингапуре.

В ходе анализа отслеживался трафик по мере загрузки приложений из источников, используемых в инфраструктуре Huawei. В ходе исследования поиск приложений производился в интернет-магазине Huawei AppGallery без изменения последовательности загрузки приложений, изначально установленной производителями; приложения были загружены непосредственно из исходного интернет-магазина и со сторонних платформ распространения приложений, предоставленных AppGallery.

При регистрации количества подключений было обнаружено, что при загрузке приложения из оригинального интернет-магазина AppGallery были выявлены запросы на 38 адресов, а в

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

корпус APKMonk, 56 адресов. Наибольшее количество запросов было выявлено для Aptoide и APKPure; соответственно 74 и 73 адреса.

Информация, иллюстрирующая запросы мобильных устройств Huawei во время процедур загрузки приложений, показана на рисунке 4.

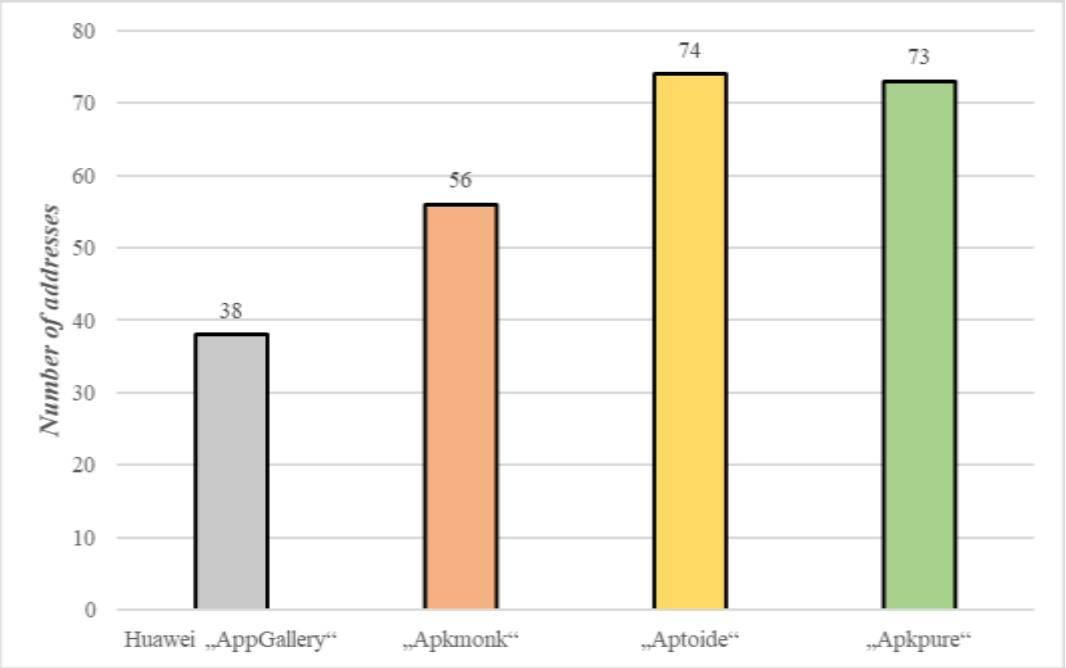
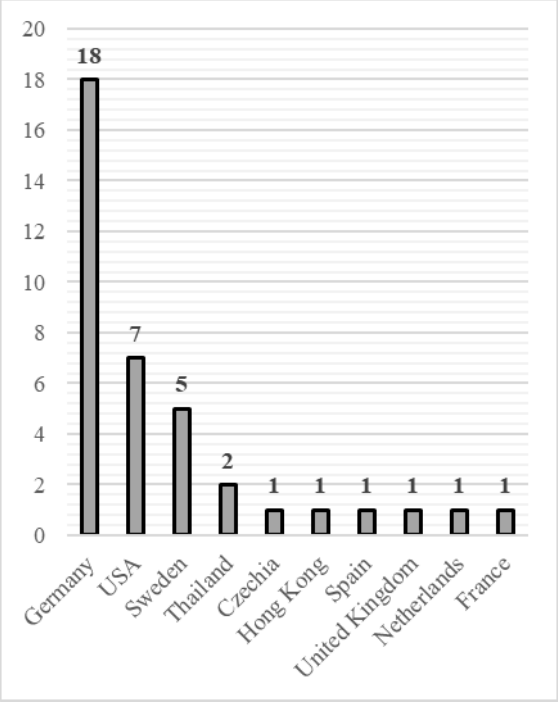


Рисунок 4: Количество запросов мобильного устройства Huawei во время процедуры загрузки приложения

Более подробная информация о странах, в которые были направлены запросы, и количестве таких запросов представлена на рисунках с 5 по 7.



Фигура 5: Запрос Huawei AppGallery

Информация

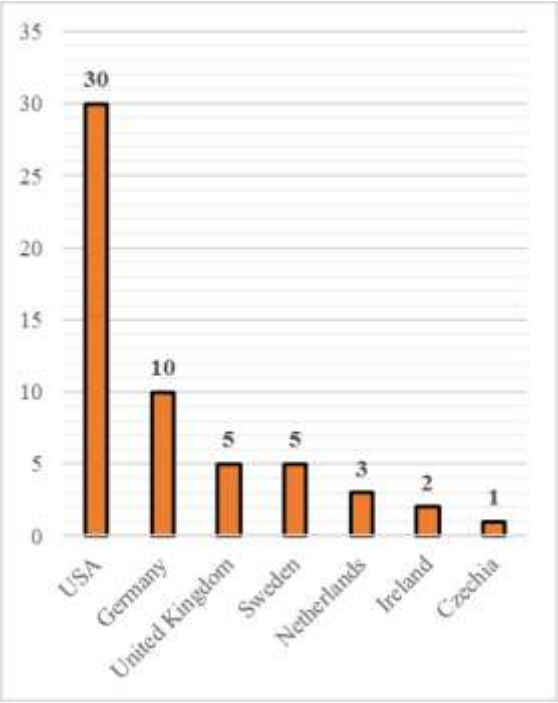
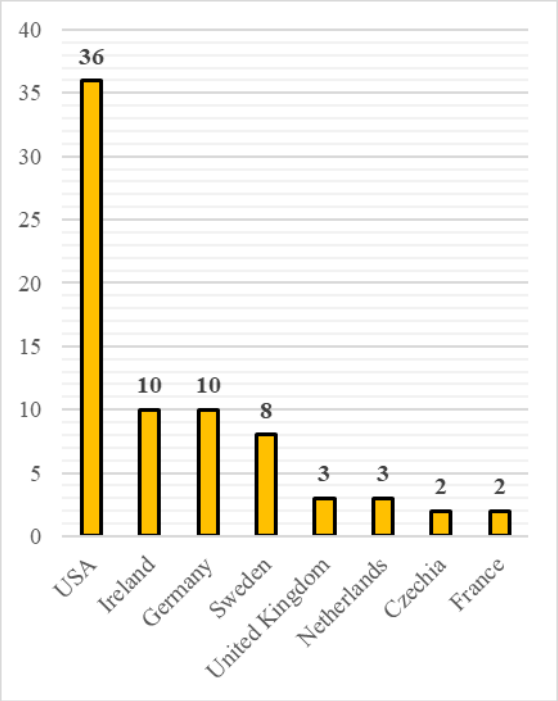


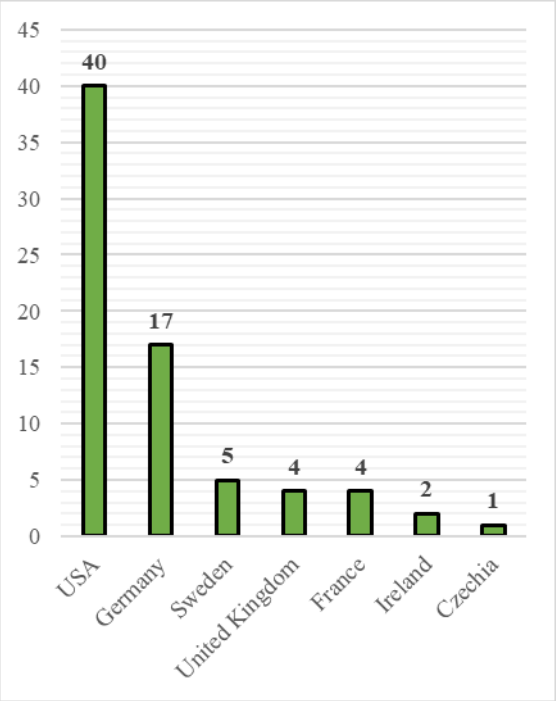
Рисунок 6: Платформа распространения APKMonk

запросить информацию



Фигура 7: Платформа распространения Aptoide

запросить информацию



Фигура 8: Платформа распространения APKPure

запросить информацию

Более подробная аналитическая информация с конкретными IP-адресами и странами представлена в таблице 3.

Стол 3. Более подробная аналитическая информация с конкретными IP-адресами и странами.

Линия Нет.:	Галерея приложений Huawei		APKMonk		Aptoide		APKPure	
	Адрес	Состояние	Адрес	Состояние	Адрес	Состояние	Адрес	Состояние
1	apkrep.ns1.ff.avast.com	Чехия	34.250.145.50	Ирландия	iwinmobi.com	Ирландия	apkrep.ns1.ff.avast.com	Чехия
2	приложение-1-drcn.dbankcdn.com.c.cdnhwc1.com	Гонконг	52.209.136.146	Ирландия	en.aptoide.com	Ирландия	sync.crwdcntrl.сеть	Ирландия
3	pay7.hicloud.ком	Испания	5.62.53.15	Чехия	ws75.aptoide.com	Ирландия	52.209.246.140	Ирландия
4	8.8.8.8	США	appimg3.dbankcdn.com	США	ws75.aptoide.com	Ирландия	13.32.111.63	США
5	appdl-11-dre.dbankcdn.ком	США	13.33.242.107	США	webservices.aptwords.net	Ирландия	feeds.apyhi.com	США
6	13.33.242.98	США	аукцион.. unity3d.com	США	en.aptoide.com	Ирландия	34,98,67,61	США
7	13.107.213.44	США	odr.mookie1.com	США	ракам-api.aptoide.com	Ирландия	34.236.65.196	США
8	52.177.138.113	США	аукцион.. unity3d.com	США	pnp.aptoide.com	Ирландия	rtb.openx.net	США
9	appdl-11-drcn.dbankcdn.com	США	аукцион.. unity3d.com	США	en.aptoide.com	Ирландия	35.244.159.8	США
10	152.199.21.230	США	EU-u.openx.net	США	ws75.aptoide.com	Ирландия	35.244.174.68	США
11	5.62.36.56	Великобритания	id.rlcdn.com	США	apkrep.ns1.ff.avast.com	Чехия	65.9.52.144	США
12	приложение-2-drcn.dbankcd	В Нидерланды	52.85.48.221	США	5.62.53.117	Чехия	download.apkpure.com	США

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

38	приложение-4-drcn.dbankcdn.com	Германия	188.125.94.206	Великобритания	connect.facebook.net	США	raw.githubusercontent.com	США
39			81.171.20.104	в Нидерланды	www.facebook.ком	США	216.58.207.206	США
40			95.211.137.160	в Нидерланды	CDN-mobile.aptoide.ком	США	www.gstatic.com	США
41 год			ib.adnxs.com	в Нидерланды	tpc.googlesyndication.com	США	firebaseinstallations.googleapis.ком	США
42			store3.hispace.hicloud.com	Швеция	fonts.gstatic.com	США	cm.g.doubleclick.net	США
43 год			104,73,93,58	Швеция	pagead-googlehosted.lgoogle.com	США	216.58.211.130	США
44 год			tls.adobe.com	Швеция	adservice.google.com	США	ad.turn.com	Великобритания
45			sdkserver-dre.op.hicloud.com	Швеция	fonts.googleapis.ком	США	185.29.135.233	Великобритания
46			sdkserver-dre.op.hicloud.com.edgekey.net	Швеция	ads.mopub.com	США	185.64.190.78	Великобритания
47			j.mrpdata.net	Германия	ads.mopub.com	США	212.82.100.176	Великобритания
48			23.193.116.193	Германия	приложение-Measurement.com	США	51.75.146.159	Франция
49			metrics2.data.hicloud.com	Германия	pixel.quantserve.ком	Великобритания	pixel.onaudience.com	Франция
50			platform.hicloud.com	Германия	185.64.190.78	Великобритания	D-08.winudf.com	Франция
51			grs.dbankcloud.ком	Германия	data.flurry.com	Великобритания	green.erne.co	Франция
52			appgallery.cloud.huawei.com	Германия	pool.apk.aptoide.com	в Netherlands	dsum-sec.casalemedia.ком	Швеция
53			JFS-dre.jos.hicloud.ком	Германия	apkins.aptoide.com	в Netherlands	store3.hispace.hicloud.com	Швеция
54			80.158.34.57	Германия	apkins.aptoide.com	в Netherlands	sdkserver-dre.op.hicloud.com.edgekey.net	Швеция
55			160.44.199.4	Германия	id5-sync.com	Франция	HWID-dre.platform.hicгромкий.com	Швеция
56			160.44.202.175	Германия	51.255.81.18	Франция	sdkserver-dre.op.hicloud.com	Швеция
57 год					2.18.33.213	Швеция	3.66.135.160	Германия
58					z.moatads.com	Швеция	tracking.justpremium.com	Германия
59					store3.hispace.hicloud.com	Швеция	49.51.130.46	Германия
60					d.applovin.com	Швеция	pixel.rubiconproject.net.akadns. сеть	Германия
61					sdkserver-dre.op.hicloud.com	Швеция	80.158.2.189	Германия
62					sdkserver-dre.op.hicloud.com.edgekey.net	Швеция	metrics2.data.hicloud.com	Германия
63					cdn2.inner-active.mobi	Швеция	OAuth-логин-dre.platform.dbankcloud.com	Германия
64					webview.unityads.unity3d.com	Швеция	80.158.19.69	Германия
65					api.vungle.com	Германия	80.158.19.100	Германия

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

Анализ показал, что при загрузке приложения из инфраструктуры Huawei осуществлялось перенаправление на сторонние платформы распространения приложений, с которых загружались приложения с потенциально вредоносным кодом. Сводка анализа безопасности мобильных приложений, загружаемых устройством Huawei из инфраструктуры Huawei, представлена в таблице 4. Анализ безопасности проводился с помощью известного инструмента анализа файлов VirusTotal.[22].

Стол 4. Сводка загруженных мобильных приложений после проверки с помощью VirusTotal.

Линия Нет.:	заявка имя	Идентификатор	заявка версия	Результат VirusTotal
1	Социальные медиа	com.social.messenger.allinoneapps	14	*Вредоносное ПО:* A.gray.andrsca.f
2	Веб-машинист Mobile Pro Нажатие	com.webmachinist.cncmachi калькулятор	1.0	*Вирус:* Trojan.Trojan.Banker.AndroidOS.Agent.ed
3	Посланник Все в одном	comm.essagechat.listing	28,0	*Вредоносное ПО:* Рекламное ПО / нагрузка для Android.fyben.a

В ходе исследования были проанализированы три мобильных приложения, загруженных с серверов инфраструктуры распространения мобильных приложений Huawei. Согласно данным сканирования VirusTotal, одна антивирусная система определила, что потенциально вредоносное ПО A.gray.andrsca.f было установлено в приложении Social Media. После изучения другого мобильного приложения Web Machinist Mobile Pro Tapping, загруженного с серверов инфраструктуры Huawei, одна антивирусная система VirusTotal выявила потенциальный вирус - Trojan.Trojan.Banker.AndroidOS.Agent.ed. Этот вирус может выполнять[23] кража данных для подключения к банковским системам. В третьем проанализированном приложении, Messenger All in One, две антивирусные системы обнаружили, что приложение использует потенциально вредоносное программное обеспечение, пакеты Adware / Loead и Android.fyben.a.

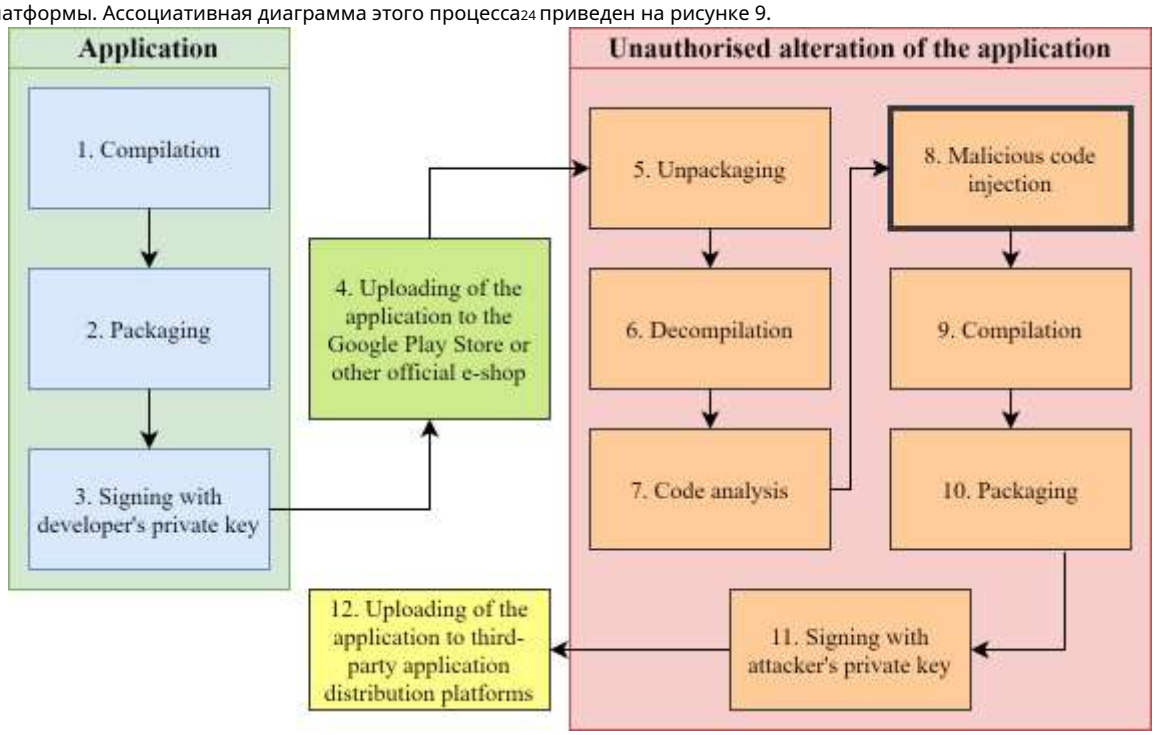
Это вызывает серьезные опасения по поводу безопасности устройства, поскольку не все сторонние платформы распространения приложений выполняют проверку загруженных приложений.

Этой уязвимостью безопасности инфраструктуры можно воспользоваться путем получения оригинальных (аутентичных) приложений из Google Play Store, декомпиляции приложения и последующего внесения необходимых изменений в содержимое декомпилированного приложения путем добавления вредоносного кода. Затем код приложения с вредоносным содержимым перекомпилируется, упаковывается и подписывается новым закрытым ключом. Модифицированное приложение загружается в вышеупомянутый дистрибутив стороннего приложения.

22 Информация о VirusTotal. *https://www.virustotal.com/gui/*

23 Информация о клавистере. *https://www.clavister.com/advisories/antivirus/view/?id=544073*

платформы. Ассоциативная диаграмма этого процесса[24] приведен на рисунке 9.



Фигура 9: Ассоциативная диаграмма внедрения вредоносного кода в мобильное приложение

Разработчик приложения компилирует код во время разработки приложения и, таким образом, формирует работающее приложение. Это приложение упаковано в установочный файл и подписано закрытым ключом разработчика приложения. Подписанный установочный файл приложения можно загрузить в магазины приложений, такие как Google Play Store.

Злоумышленник, как и все пользователи магазинов приложений (за исключением соответствующих региональных ограничений), может скачать это приложение; после получения из официальных источников он распаковывается и декомпилируется в код приложения. Это позволяет злоумышленнику выполнить анализ приложения, определить жизнеспособность места установки вредоносного кода и используемую технологию установки, а также вставить вредоносный код в приложение. После завершения процедур вставки вредоносного кода код приложения перекомпилируется и упаковывается в установочный файл, подписанный закрытым ключом злоумышленника. Созданный установочный файл вредоносного приложения загружается на сторонние платформы распространения приложений, где проверяются не все загруженные приложения.

Было обнаружено, что интернет-магазины, содержащие вирусы, представляют собой серьезную проблему для этих магазинов.[25] Пользователь кто устанавливает зараженное вирусом приложение, может пострадать от сбора или утечки данных, хранящихся на устройстве или связанной с ним облачной службе, или от повреждения мобильного устройства.

Анализ показал, что часть мобильных приложений, доступных на платформах распространения приложений, являются подделками оригинальных (аутентичных) приложений с вредоносными функциями или зараженными вирусами; такие приложения могут быть загружены и установлены пользователем на мобильный телефон, тем самым ставя под угрозу безопасность устройства и содержащихся в нем данных.

[24] Информация о Springer. Атака переупаковки на банковские приложения Android и меры противодействия. *https://link.springer.com/article/10.1007/s11277-013-1258-x*

[25] P. Kotzias et al. Как это попало в мой телефон? Нежелательное распространение приложений на устройствах Android. *https://arxiv.org/pdf/2010.10088.pdf*

2. Устройства, разработанные и произведенные в Китае, имеют доступ к серверам в третьих странах. Этот позволяет собирать и агрегировать пользовательские метаданные и на основе этих данных отслеживать пользователей

Анализ декомпилированного ПО и потоков данных показал, что Mi Browser использует два модуля сбора данных: Google Analytics и Sensors Data. Sensors Data - это платформа китайского происхождения, по функциональности близкая к Google Analytics. По данным компании Sensors Data,[26 год] у него больше чем 1500 клиентов, включая некоторые из крупнейших корпораций Китайской Народной Республики, такие как China Telecom, Baidu, CYTS, Sichuan Airlines и т. Д.

Google Analytics - это аналитическая платформа для программистов или администраторов, позволяющая им получать доступ к информации, позволяющей им оценивать использование приложений в iOS, Android или в веб-средах.[27]. Google Analytics автоматически создает журнал событий, позволяющий оценить производительность приложения. Стоит отметить, что у разработчиков есть техническая возможность выбирать параметры для анализа и устанавливать глубину анализа таких параметров.

Было обнаружено, что этот модуль может собирать данные о просмотрах пользователей, кликах и т. Д. И отправлять информацию для возможного анализа на серверы Google. Следует отметить, что эти модули активируются во время первоначального включения устройства при согласии на участие в программе Xiaomi User Experience.

После декомпиляции системных приложений, установленных на устройстве Xiaomi, было обнаружено, что функциональность этих аналитических приложений была установлена и использовалась в стандартном интернет-браузере телефона Xiaomi Mi Browser. В таблице 5 показан фрагмент кода Mi Browser, обозначающий функциональность Google Analytics.

Таблица 5. Фрагмент кода Mi Browser, обозначающий функционал Google Analytics.

```
публичная статическая пустота reportAsync(String str, Map <String, Object> map) {
 если если (! TextUtils.isEmpty (str) & AMP; &!BrowserSettings.getInstance.isNotAllowCollectData) {
BrowserReportUtils.stripUrlIfNeeded(карта);
Фон.postOnIOThread(новый Runnable (ул., Карта)
 {общедоступный финал / * синтетический * /Нить f $ 0;
 публичный финал / * синтетический * / карта f $ 1; {


это.f0 долл. США = r1;
это.f $ 1 =
r2; }
 Публичная окончательная недействительность запустить {
FirebaseReportHelper.отчет(это.f $ 0, это.f $ 1); }

});
 }
}
```

В представленном в таблице фрагменте кода реализована функция отправки данных в аналитическую платформу Firebase на серверах Google. В таблице 6 показан фрагмент кода Sensors Data, установленного в приложении Mi Browser. Во фрагменте кода представлена функция, запускающая функционал Sensors Data в приложении Mi Browser.

Таблица 6. Фрагмент кода запуска Sensors Data в приложении Mi Browser

---

[26 год] Информация о датчиках. *https://www.sensorsdata.cn/about/aboutus-en.html*

[27] Информация о Google Firebase. *https://firebase.google.com/docs/analytics/get-started*

```
публичная статическая пустота initSensorsDataAPI(окончательный Context context) {
если (контекст! = нулевой) {Контекст applicationContext =
context.getApplicationContext;
ПЫТАТЬСЯ {
Датчики.startWithConfigOptions(applicationContext, новый
SAConfigOptions (SA_SERVER_URL) .setAutoTrackEventType (3) .enableLog (РазрешениеUtil.isBuildDebu
грамм(приложениеlicationContext) .enableTrackScreenOrientation (ложный));
Датчики.sharedInstance.идентифицировать(AnonymousID.получить заявку(Контекст));
setFlushNetworkPolicy(Соглашение о конфиденциальности.getInstance.isApproved);
Датчики.sharedInstance.setSessionIntervalTime (10000);
registerSuperProperties(applicationContext);
Датчики.sharedInstance.unregisterSuperProperty (C4683v.f6510ae);
Датчики.sharedInstance.unregisterSuperProperty (uuid);
выйти;
Датчики.sharedInstance.enableEncrypt (правда);
Датчики.sharedInstance.persistentSecretKey (новый Датчики. PersistentSecretKey{
общественная пустота saveSecretKey.SecreteKeysecretteKey {} public

Датчики.SecreteKeyloadSecretKey { возвращение
новый SensorsDataEncrypt.SecreteKeyконтекст.getString(р.нить.ABCDEF), 1);
}
});
} ловить (Исключение не используется) {}

}
}
```

Установлено, что используемый в устройстве модуль данных датчиков собирает статистическую информацию о 61 параметре работы используемых приложений (время активации приложения, используемый язык и т. Д.). Список данных, собранных Sensors Data, приведен в таблице 7.

Тспособный 7. Список из 61 параметра, собранный датчиками Data.

Нет.:	Параметр	Комментарий
1	log_miaccount	Пользователь вошел в систему
2	Autocomplete_switch	Включено ли автоматическое завершение текста?
3	No_track_switch	Включена ли функция "Не отслеживать"? Включена
4	bookmark_sync	ли синхронизация закладок с облаком? включено
5	history_sync	Есть ли синхронизация истории просмотров с облаком включен
6	feature_report_switch	Участвует ли пользователь в пользовательском интерфейсе Xiaomi? программа
7	clear_history_switch	Удаляется ли история при закрытии приложения
8	personal_service_switch	Включены ли рекомендации программы.
9	Enhanced_incognito_switch	Работает ли браузер в режиме Enhanced Incognito. Режим
10	system_out_of_ads	Активирована ли функция ограничения отслеживания рекламы. Используя эту функцию, рекламодатели не имеют доступа к устройству. идентификатор

11	swipe_up	Какая функция прописана для движения свайпом вверх
12	current_default_search_engine	Текущая используемая поисковая
13	язык	система Язык, установленный в
14	language_browser	системе Настройка языка в браузере
15	icon_reddot_status	-
16	user_newsfeed	Лента новостей отключена
17	user_download_videos	-
18	user_night_mode	Использует ли браузер ночной
19	dark_mode	режим. Использует ли система
20	user_data_save_mode	ночной режим. браузер
21 год	user_incognito_mode	Включен ли режим инкогнито
22	user_desktop_mode	Пользовательский агент браузера
23	user_checkbox_4G	Разрешено ли обновление браузера через 4G?
24	user_push_agree	Активированы ли уведомления браузера? Были ли
25	user_facebook_notification	активированы сообщения Facebook в браузер
26 год	user_youtube_signin	Авторизован ли пользователь на YouTube. Показывает,
27	user_click_interest	сколько раз пользователь нажимал на карточки в браузер (новости, рекомендации YouTube и т. д.),
28 год	Логин пользователя	вошел ли пользователь в учетную запись Mi
29	adblock_switch	Активирована ли функция блокировки рекламы?
30	adblock_show_notification	Adblock включен?
31 год	first_enter_newsfeed_way	Открывается ли окно ленты новостей впервые?
32	Fandst_appstart_source	-
33	first_appstart_third_party	-
34	Miu_personalised	Активирована ли персонализированная реклама; были ли
35 год	personalised_services	выполнены рекомендации по персонализированному содержанию. активирован
36	browser_ads	-
37	Protection_type	-
38	app_boot_third_party	-
39	app_boot	Время запуска программы
40	feed_default_channel	-
41 год	experience_improve	Активирован ли пользовательский интерфейс Xiaomi?
42	Платформа	Платформа. Всегда Android
43 год	Miu_version	Версия MIUI
44 год	log_miaccount	Выполняется ли пользовательский вход в учетную запись Mi
45	MUI_region	Ми регион
46	EID	-
47	apk_name	Имя APK приложения
48	browser_install_referrer	-
49	Autocomplete_switch	Активировано ли автозаполнение в окне поиска
50	No_track_switch	Включена ли функция "Не отслеживать"?
51	bookmark_sync	Есть синхронизация закладок с Mi сервером активирован
52	history_sync	Есть синхронизация истории просмотров с Mi сервером активирован

53	feature_report_switch	Участвует ли пользователь в пользователе Xiaomi Программа опыта
54	clear_history_switch	Удаляется ли история просмотров, когда приложение закрыто
55	personal_service_switch	Является ли функциональность рекомендаций пользователей включено: персонализированные ролики YouTube и т. д.
56	Enhanced_incognito_switch	Включен ли инкогнито
57 год	user_tab_news	Включил ли пользователь вкладку новостей?
58	user_tab_games	Включил ли пользователь вкладку игр?
59	search_optimization_switch	Постоянно, всегда равно 1 Предоставляет
60	cookie_status	данные о настройках файлов cookie пользователя.
61	подписка	Указывает, используется ли VPN, и если да, то его идентификатор

В ходе анализа была проведена полная расшифровка и расшифровка зашифрованных сообщений Xiaomi. Было обнаружено, что телефон Xiaomi отправляет данные датчиков в наборе данных Base64, который дополнительно кодируется с использованием *urlencode* алгоритм. Пример отправленного фрагмента закодированных данных приведен в таблице 8.

Таблица 8. Фрагмент данных, отправленных телефоном Xiaomi.

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

В таблице 9 показано расшифрованное содержимое данных, отправленных телефоном Xiaomi на серверы данных датчиков, расположенные в Сингапуре. Данные, отправленные на анализ: версия приложения, название приложения, текущий регион, производитель устройства и т. Д.

Таблица 9. Контент, отправляемый телефоном Xiaomi на серверы данных датчиков в Сингапуре

{
«_Track_id»: 1687170607,
для Time: 1623852507838,
для 'type': track,
для "independent_id": "7d03ab71-91b1-47ca-8f56-0ce2d77f6c86",
для Lib: {
Для $ Lib: Android,
Для $ lib_version: «4.0.3-pre»,
для $ app_version: '12 .4.1-g ',
для $ lib_method:' code ',
«$ Lib_detail»: «com.android.browser.BrowserActivity #####»},

для события: «$
AppStart», для свойств: {
Для $ Lib: Android,
«$ Os_version»: '10',

Для $ lib_version: «4.0.3-pre»,
для $ Model: «M2007J3SY», «$
s»: Android,
«$ Screen_width»: 1080,
Для $ screen_height: 2400, для $
производителя: 'Xiaomi', для $
app_version: '12 .4.1-g ', для
платформы: AndroidApp,
для miui_version: V12.0.18.0.QJDEUXM,
log_miaccount: 0,
'miui_region': «LT»,
для 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,
для '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»: «»,
Для $ WiFi: True,
Для $ network_type: WIFI, «$
resume_from_background»: True, «$
is_first_time»: false,
«$ Screen_name»: «com.android.browser.BrowserActivity»,
для $ title: «Mi Browser»,
«$ Is_first_day»: верно
}
}

Данные датчиков были отправлены на адрес *https://sa.api.intl.miui.com*. В таблице 10 представлена информация, характеризующая аналитические данные, передаваемые по сети на серверы.
расположен в Сингапуре.

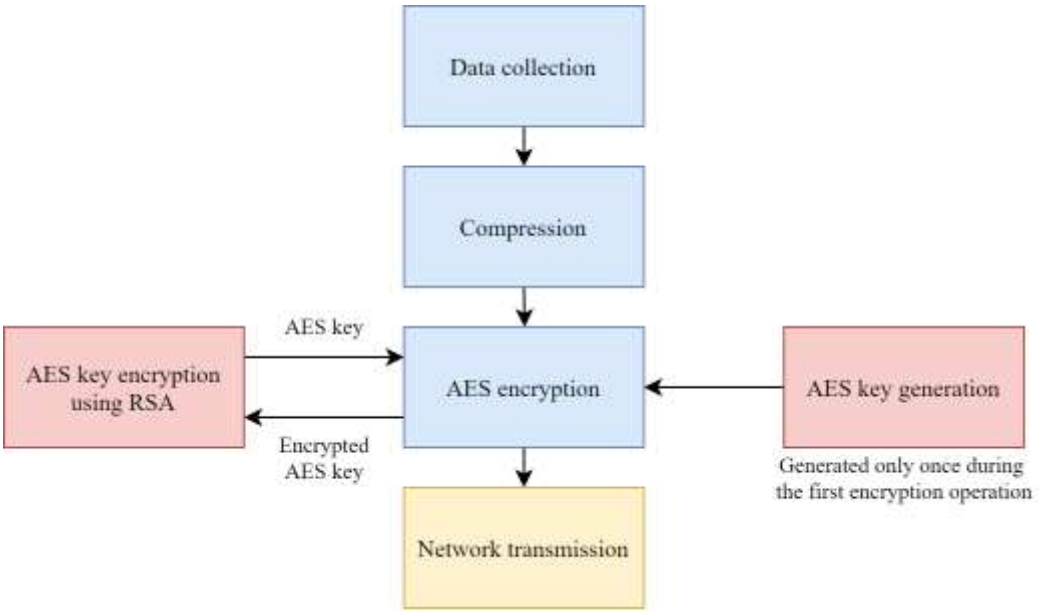
Таблица 10. Характеристики данных, отправляемых датчиками Data

Линия Нет.:	айпи адрес	Данные отправлены, *в*	Данные получены, *В*	Всего данных, *В*	Состояние
1	47.241.109.186	11789	0	11789	Сингапур
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	

Собранная статистика отправляется по зашифрованному каналу на серверы Xiaomi в Сингапуре, стране, не подпадающей под действие Общего регламента защиты данных. Можно сказать, что потенциально чрезмерный сбор и использование аналитических данных представляет угрозу конфиденциальности личных данных.

На рисунке 10 показан механизм шифрования данных датчиков, который был воссоздан во время

анализ, используемый для установления канала передачи данных между устройством и серверами, расположенными в Сингапуре.



Фигура 10: Механизм шифрования данных, используемый Xiaomi

Зашифрованный набор данных создается путем вызова программного обеспечения Sensors Data, установленного в браузере Mi: *registerSuperProperties* а также *registerDynamicSuperProperties*. Эти функции отвечают за сбор данных и подготовку объекта JSON. Когда набор данных должен быть отправлен, он сначала преобразуется в байтовое выражение и архивируется с использованием*gzip* алгоритм.

Это сделано для уменьшения количества отправляемых данных. Результат зашифрован с использованием алгоритма AES128-CBC. Ключ генерируется с помощью генератора псевдослучайных чисел устройства. После этого ключ, используемый в шифровании AES, шифруется алгоритмом RSA с использованием открытого ключа, загруженного с серверов Xiaomi. Полученный набор данных упаковывается в объект JSON и отправляется на серверы в Сингапуре.

Приложение вызывает функции *registerSuperProperties* а также *registerDynamicSuperProperties*. Эти функции отвечают за сбор данных и подготовку объектов JSON. Можно сказать, что механизм шифрования данных датчиков обеспечивает относительно высокий уровень безопасности данных при передаче таких данных на серверы аналитики, расположенные в Сингапуре.

Модуль Google Analytics, установленный на устройстве, позволяет просматривать историю просмотров в браузере Mi, считывать результаты поиска и другие параметры активности приложения и отправлять эти данные на серверы аналитики. Данные отправляются по зашифрованному каналу TLS с использованием кодирования Protobuf. Декодирование данных без файла конфигурации Protobuf невозможно или сложно, но в зашифрованном потоке можно различить определенные данные: интернет-адрес, открытый в браузере MI, данные, введенные в поле поиска, или действие, выполненное пользователем (например, щелчок по поле поиска).

Эти данные могут быть доступны и использованы разработчиком приложения Xiaomi.[28 год] Закодированный фрагмент данных, отправленных на серверы Google Analytics, представлен в таблице 11.

[28 год] Информация о Xiaomi. *https://privacy.mi.com/all/en_US/*

Таблица 11. Закодированный фрагмент исходящих данных, отправляемых устройством Xiaomi на серверы Google Analytics.

event_network r: LT | 285
_oapp _scBrowserActivity _siçÈ¾å ° òT

"Urlr"
: LT | https://nksc.lt/çþ¦¡/ ý Âicon _oapp op

r: LT | wifi_ifremind r

: LT | напомнить язык
: LT | en
is_system_languager
: LT | 1sourcer: LT | search_icon _oapp op

r: LT | show_scBrowserActivity _siçÈ¾å ° òTweb_translate_op²

«Ýæ / ñ®ý / event_network»

p:
LT | wifienter_wayr: LT | searchBar_website _oapp _scBrowserActivity _siçÈ¾å ° òT imp_search_page Îæýæ/ ü event_network p

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

В таблице 12 представлена информация, характеризующая аналитические данные, передаваемые устройством Xiaomi по сети на серверы Google Analytics.

Стол 12. Характеристики данных, отправленных на серверы Google Analytics

Линия Нет.:	айпи адрес	Данные отправлены, *B*	Данные получены, *B*	Всего данных, *B*	Состояние
1	142.250.74.110	2545	0	2545	США
2	172.217.16.14	1282		1282	
3	216.58.207.206	12699		12699	

На основании полученных данных можно сказать, что Xiaomi собирает относительно большой объем информации о процессах, запущенных на устройстве, поведении установленных пакетов программного обеспечения, действиях, выполняемых пользователями, и параметрах конфигурации приложений. Для реализации этого процесса используются две системы аналитики, Sensors Data и Google Analytics. Обзор источников показал, что устройства Xiaomi собирают более широкий спектр данных по сравнению с устройствами других производителей.

мобильные устройства[29, 30, 31].

Можно сказать, что потенциально чрезмерный сбор и использование аналитических данных представляет угрозу конфиденциальности личных данных.

3. Функциональность, реализованная на устройстве Xiaomi, может ограничивать бесплатную доступность Информация

Было установлено, что во время инициализации системных приложений, установленных на заводе на устройстве Xiaomi Mi 10T, эти приложения связываются с сервером в Сингапуре по адресу globalapi.ad.xiaomi.com (IP-адрес 47.241.69.153) и загружают JSON. файл MiAdBlacklistConfig и сохраните этот файл в каталогах метаданных приложений. Список приложений, для которых файл MiAdBlacklistConfig был найден в каталогах метаданных, представлен в таблице 13.

Стол 13. Список мобильных приложений с использованием файла MiAdBlacklistConfig.

Линия Нет.:	Имя приложения	Идентификатор приложения	Устройство
1	Безопасность	*com.miui.securitycenter*	Xiaomi Mi 10T
2	Mi Browser	*com.mi.globalbrowser*	
3	Загрузки	*com.android.providers.downloads.ui*	
4	Музыка	*com.miui.player*	
5	Темы	*com.android.thememanager*	
6	Пакет MIUI Установщик	*com.miui.global.packageinstaller*	
7	Очиститель	*com.miui.cleanmaster*	

После того, как приложения загрузили файл, дата загрузки записывается, чтобы облегчить периодическое обновление списка. Схема загрузки файла MiAdBlacklistConfig показана на рисунке 11.

29 Политика конфиденциальности Apple. *https://www.apple.com/legal/privacy/en-ww/*

30 Дуглас Дж. Лейт. Конфиденциальность мобильных телефонов: измерение данных, отправляемых iOS и Android в Apple и Google.*https://www.scss.tcd.ie/doug.leith/apple_google.pdf*

31 год Политика конфиденциальности Xiaomi. *https://privacy.mi.com/all/en_IN/*

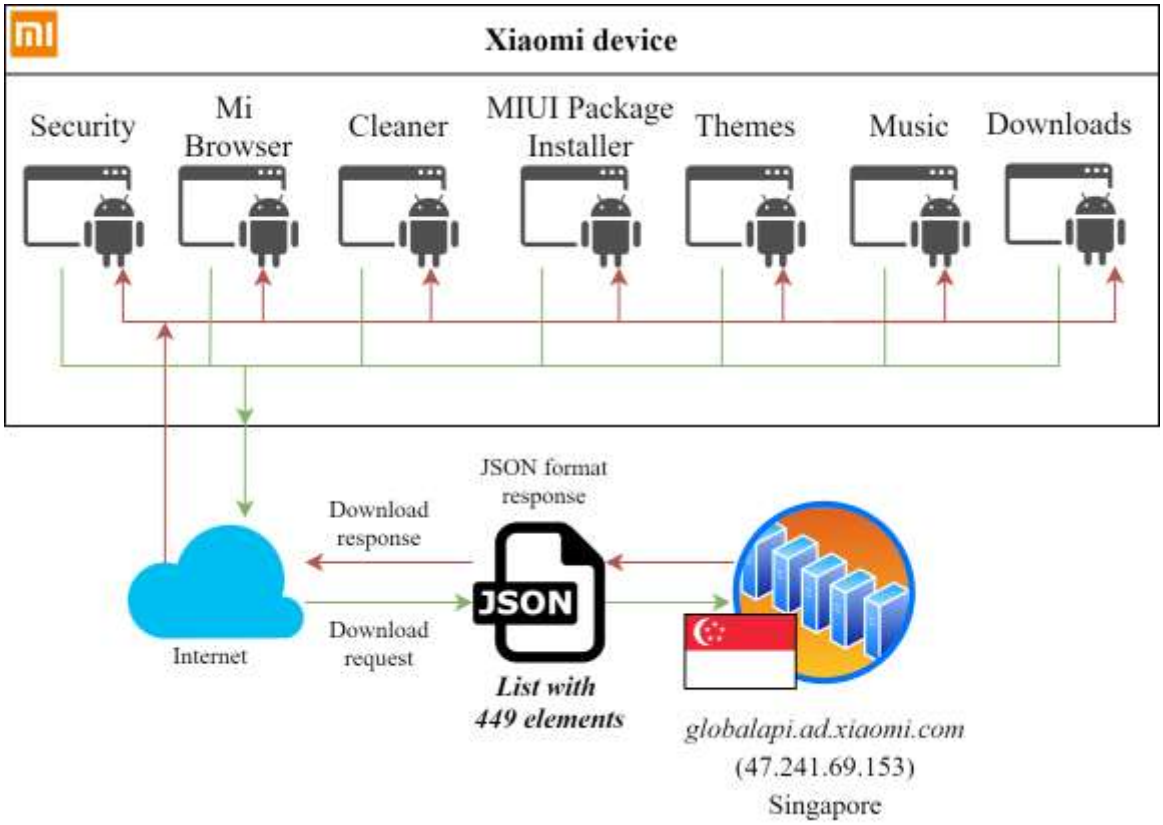


Рисунок 11. Схема загрузки MiAdBlacklistConfig

Этот файл содержит список, состоящий из названий, имен и другой информации о различных религиозных и политических группах и социальных движениях (на момент анализа файл MiAdBlacklistConfig содержал 449 элементов). Фрагмент файла MiAdBlacklistConfig показан в Таблице 14.

Стол 14. Фрагмент файла MiAdBlacklistConfig.

Линия Нет.:	Оригинал	Примерный перевод
1	"宗教 虔信 者阵线 ",	«Фронт верующих»,
	...	
22	"西藏 自由",	«Свободный Тибет»,
	...	
60	"蒙古 独立",	«Независимость Монголии», «89
61	«89民运 ",	Демократическое движение»,
62	"基督 灵 恩布 道团 ",	«Христианская харизматическая миссия»,
	...	
145	"伊斯兰 联盟 ",	«Исламская лига»,
	...	
201	"民运",	«Демократическое движение»,
202	"妇女 委员会",	«Комитет женщин», г.
203	"伊斯兰马格里布 基地 组织 ",	«Аль-Каида в исламском Магрибе»,
204	"人民报 ",	«Народная ежедневная газета»,
205	"巴勒斯坦 解放组织 ",	«Организация освобождения Палестины»,

	...	
313	"台独 万岁 ",	«Да здравствует независимость Тайваня»,
	...	
369	"美国之音",	«Голос Америки»,
	...	
420	«89运动 ",	«Движение 89»,
	...	
449	"夏米斯丁艾 合 麦提·阿布 都 米吉提 "	«Ся Мистин Ахемет Абу Думиджити»

Анализ кода приложения Xiaomi показал, что в приложениях реализованы программные классы для фильтрации целевого мультимедиа, отображаемого на устройстве, на основе загруженного списка в файле MiAdBlacklistConfig. Фрагмент этого кода приведен в таблице 16.

Таблица 16. Фрагмент кода фильтрации содержимого, используемого в устройстве Xiaomi.

```
публичное логическое значение mo76794a(INativeAd iNativeAd, C8380a Avar) {
 если (iNativeAd == нулевой) {
 вернуть истину;
 }
 Длинный currentTimeMillis = System.currentTimeMillis;
 для (Нить ул.: новый HashSet (это.f11160b))
 {если (iNativeAd.getAdTitle! = нулевой &AMP;&m12161a (iNativeAd.getAdTitle, ул.)
) {MLog.m6439d (MiAdBlacklistConfig, Объявления: " + iNativeAd.getAdTitle + «Блокируется заглавным словом:« + Изобразительное искусство);
 ЕСЛИ (Авар! = нулевой) {aVar. f11165a
знак равно Изобразительное искусство;
 }
 это.f11161c знак равно Изобразительное искусство;
 вернуть истину;
 } другое, если (iNativeAd.getAdBody! = нулевой & AMP; &m12161a (iNativeAd.getAdBody, ул.)) {MLog.m6439d (
 MiAdBlacklistConfig),Объявления: [" + iNativeAd.getAdBody + "] Блокируется описанием:" +
Изобразительное искусство);
 ЕСЛИ (Авар! = нулевой) {aVar. f11165a
знак равно Изобразительное искусство;
 }
 это.f11161c знак равно Изобразительное искусство;
 вернуть истину;
 }
 MLog.m6443i
 (MiAdBlacklistConfig, isAdsBlocked—> totalTime = ” + (System.currentTimeMillis - currentTimeMillis)+
«& ThreadId =» + Thread.currentThread.getId);
 вернуть ложь;
}
```

После анализа Mi Browser было обнаружено, что приложение выполняет функцию загрузки файла MiAdBlacklistConfig, но не фильтрует контент в соответствии со списком в файле MiAdBlacklistConfig. На основании кода Xiaomi эта функция отключена в «регионе Европейского Союза». Контент регистрации событий, созданный Mi Browser, представлен в Таблице 17.

Стол 17. Контент регистрации событий, созданный Mi Browser.

Линия Нет.:	Название функция	Параметр 1	Параметр 2
1	MLog.d	MiAdBlacklistConfig	начать запрашивать 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	повторная попытка запроса: время успешного сброса
5	MLog.d	MiAdBlacklistConfig	ответ проанализирован успешно
6	MLog.d	MiAdBlacklistConfig	updateAdConfig
7	MLog.d	MiAdBlacklistConfig	notifyAllObservers
8	Я:	NativeAdManagerInternal	posid [1.306.1.3], requestAd isPreload: false Срок действия
9	Я:	NativeAdManagerInternal	AdSwitch истек: новый запрос с удаленного компьютера
10	Я:	AdSwitchUtils	AdSwitchOFF - ложь
...			
23	Я:	AdReportTask	{«MEvent»: «LOAD_AD», «mPositionId»: «1,306.1.3» , «MAppId»: «10000», «mChannelId»: «miui», «mOpera tor»: «246_01», «mClientVersion»: «100492», «mSdkV ersion»: «130200», «mAdTime»: «1621431087190» , mModel: M2007J3SY, mGaid: «d3a32b43-6e7e- 4306-82ca- 0f65f1586511 »,« mLanguage »:« en_US »,« Версия mBuildSdk »:« 29 »,« mDoNotTrack »:« false »,« mBuildTyp » e »:« стабильный », muiVersion: «V12.0.18.0.QJDEUXM», «mRegion»: «LT», «mTriggerId»: «9d1f86e3-579e-4110-b71e- 065f520c1fa3 ”, «MIsPreload»: «false», «mCustomKey»: «adsCnt», «mC ustomValue»: «0», «mInstaller»: «com.xiaomi.discover» »,« MIsPreInstall »: 0, mElapsed: 0, mIsid: 0}
24	Я:	MIADSDK	Персонализированная реклама отключена в регионе ЕС, отчетность не разрешена.
25	Я:	MIADSDK	Персонализированная реклама отключена в регионе ЕС, отчетность не разрешена
...			
38	Я:	AdReportTask	{«MEvent»: «PAGE_VIEW», «mPositionId»: «1.306.1 . 3 »,« mAppId »:« 10000 »,« mChannelId »:« miui »,« mOp erator »:« 246_01 »,« mClientVersion »:« 100492 »,« mSd kVersion »:« 130200 »,« mAdTime »:« 1621431420870 ” , mModel: M2007J3SY, mGaid: «d3a32b43-6e7e- 4306-82ca- 0f65f1586511 »,« mLanguage »:« en_US »,« Версия mBuildSdk »:« 29 »,« mDoNotTrack »:« false »,« mBuildTyp » e »:« стабильный », muiVersion: «V12.0.18.0.QJDEUXM», mRegion: «LT »,« MTriggerId »:« 9d1f86e3-579e-4110- b71e-065f520c1fa3 », mInstaller:« com.xiaomi.discover »,« m IsPreInstall »: 0,« mElapsed »: 0,« mIsBid »: 0,« mCost » : 3 33682}

Считается, что эта функция позволяет устройству Xiaomi выполнять анализ целевого мультимедийного контента, поступающего в телефон; для поиска ключевых слов на основе списка MiAdBlacklist, полученного с сервера. Как только устройство определяет, что контент содержит определенные ключевые слова, устройство выполняет фильтрацию этого контента, и пользователь не может его видеть. Принцип анализа данных позволяет анализировать не только слова, написанные буквами; список, который регулярно загружается из

сервер может быть сформирован на любом языке. Важно подчеркнуть, что данная функция активируется производителем удаленно. Считается, что наличие такой функциональности может поставить под угрозу свободный доступ к информации и ограничить ее доступность. Можно сказать, что это важно не только для Литвы, но и для всех стран, использующих устройства Xiaomi.

4. На устройствах Xiaomi для подключения к облаку необходимо зарегистрировать SIM-карту. Отправлено сообщения не отображаются на телефоне. Риск утечки пользовательских данных

Исследования показали, что когда пользователь решает использовать сервисы Xiaomi Cloud, номер мобильного телефона пользователя регистрируется на серверах, расположенных в Сингапуре. Для этого устройство отправляет зашифрованное SMS-сообщение на специальный номер телефона. Процедура регистрации для облачных сервисов Xiaomi выполняется на устройстве Xiaomi путем отправки SMS-сообщения, как показано на рисунке 12.

Когда пользователь пытается подключиться к облачной службе Xiaomi в первый раз, устройство запрашивает доступ к (1) учетной записи Xiaomi. После ввода данных для входа и успешного входа в учетную запись открывается окно меню (2), в котором можно включать и отключать основные функции Xiaomi Cloud: синхронизацию данных и геолокацию устройства в случае потери устройства.

После выбора желаемых функций служба, работающая в фоновом режиме, запускает процедуры сбора данных с SIM-карты (3, 4 и 5). После того, как сервис завершит процедуры сбора данных с SIM-карты, пользователю будет показано информационное окно (6), в котором указано, что для включения функции истории вызовов и синхронизации сообщений устройство должно отправить SMS-сообщение для проверки номера телефона.

В информационном окне также указывается, что с пользователя может взиматься плата за отправку SMS-сообщения по стандартным тарифам оператора (провайдера) мобильной связи. Когда пользователь закрывает информационное окно, ему отображается окно операционной системы (7), в котором пользователя спрашивают, разрешить ли службе регистрации SIM-карты автоматически отправлять SMS-сообщения. С согласия пользователя запускается автоматическая процедура регистрации телефонного номера (8).

Устройство загружается с **Общее** server структура данных конфигурации для процедуры, которая включает адрес сервера, с которым будет осуществляться дальнейшая сетевая связь, номер телефона получателя SMS и другие параметры. Затем устройство генерирует SMS-сообщение и отправляет сообщение на номер телефона, указанный в структуре данных конфигурации (9). Отправленное сообщение немедленно удаляется из журнала отправленных сообщений.

При этом собранные данные SIM-карты хранятся во внутренней служебной базе данных (10). После отправки SMS-сообщения его содержимое шифруется и отправляется на сервер, адрес которого указан в структуре данных конфигурации, вместе с запросом на подтверждение регистрации.
(11).

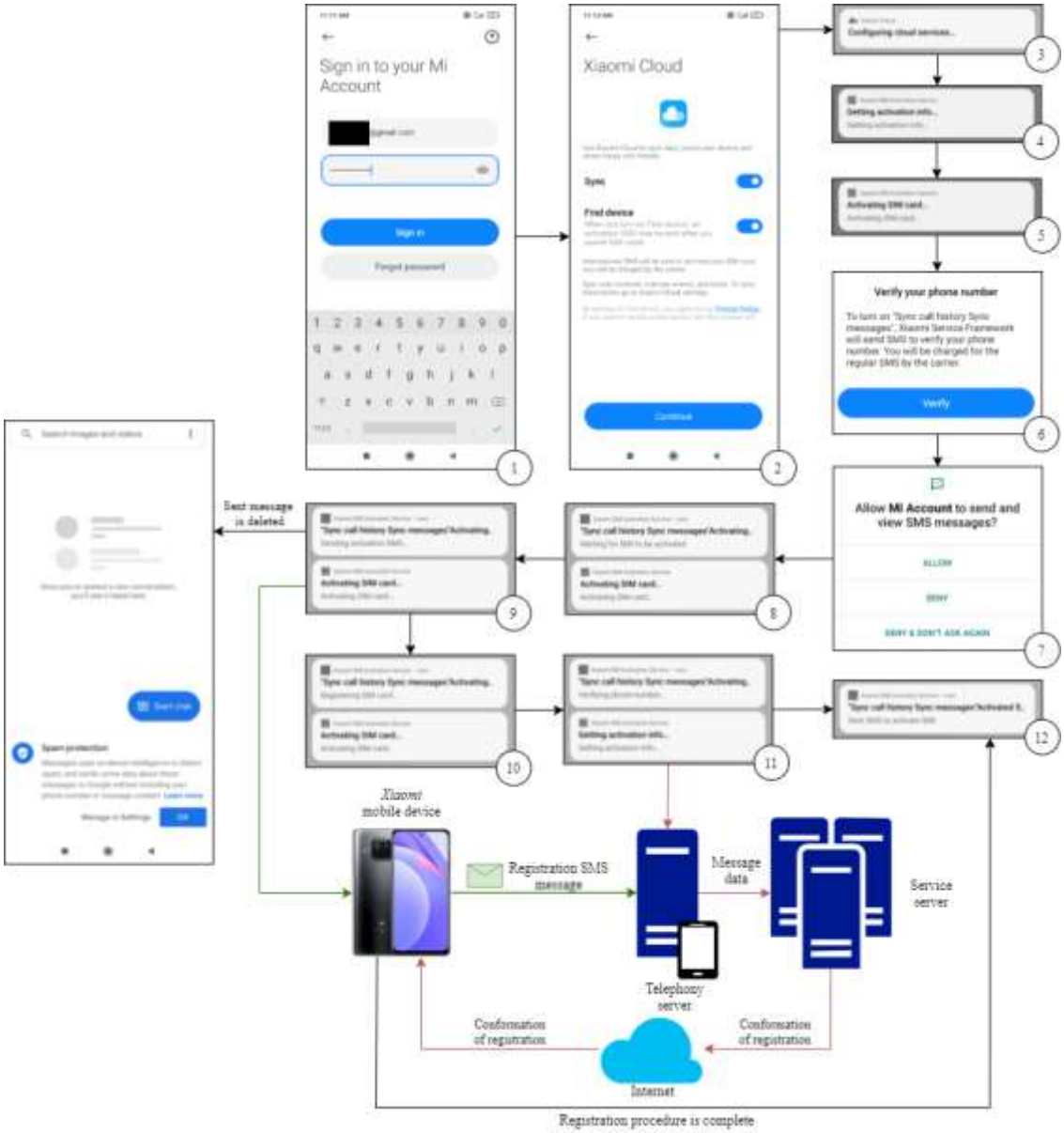


Рисунок 12. Процедура регистрации в облачных сервисах Xiaomi выполняется на телефоне путем отправки SMS сообщение

После отправки запроса на регистрацию на сервер устройство получает ответ на запрос, отображающий результат регистрации (положительный или отрицательный) (12).

Установлено, что регистрация телефонного номера осуществляется независимо от того, как пользователь выбирает аутентификацию: по номеру телефона или по адресу электронной почты. Важно отметить, что отправленное зашифрованное SMS-сообщение и его адресат не видны пользователю. На момент анализа после отключения функционала сервиса Xiaomi Cloud отправка сообщений не наблюдалась. Более подробная блок-схема сети представлена на рисунке 13.

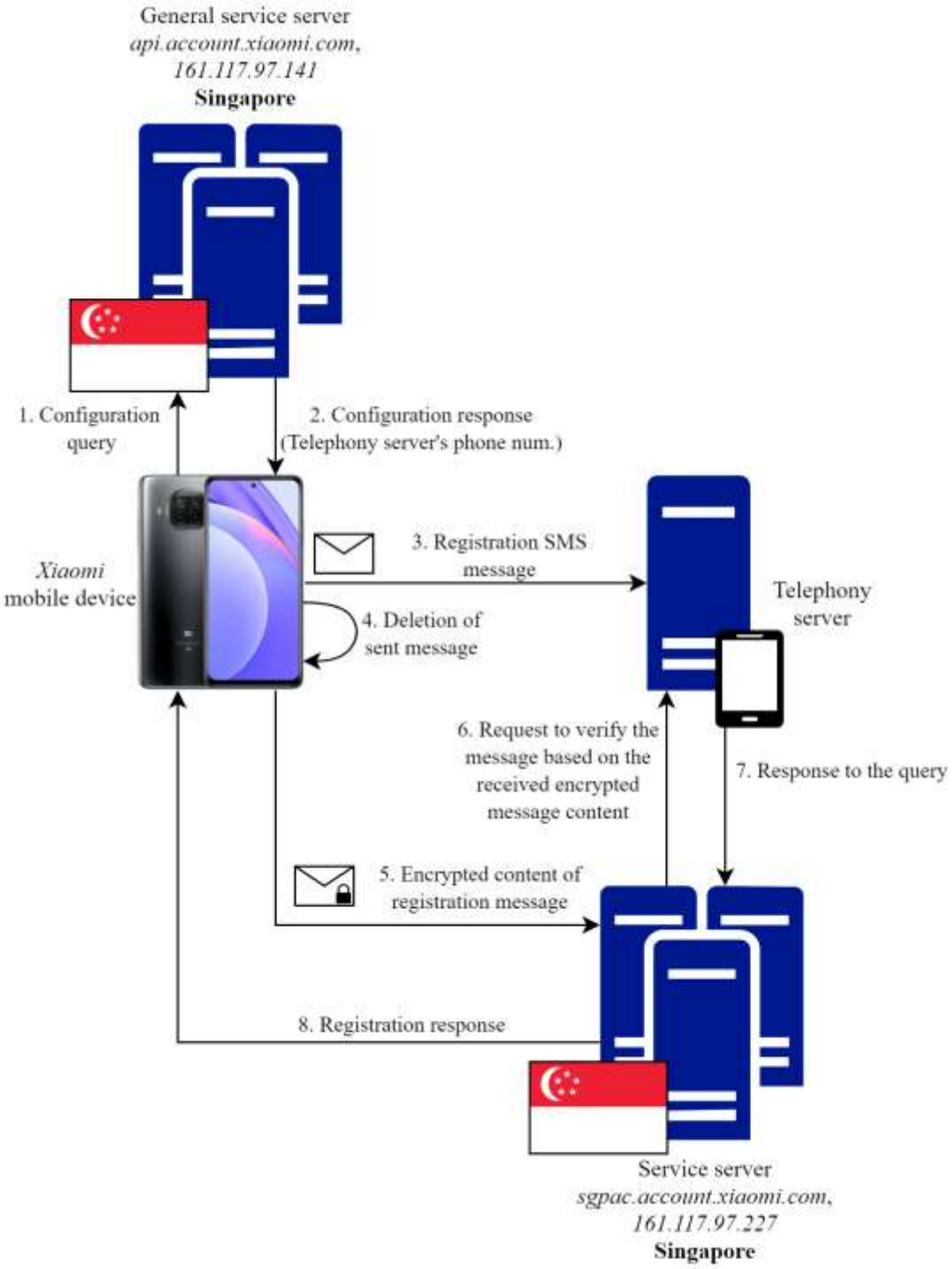


Рисунок 13. Схема регистрации в сети сервисов Xiaomi Cloud

После запуска процесса регистрации номера телефона устройство отправляет запрос на общий сервер, расположенный в Сингапуре (1), от которого в качестве ответа получает структуру данных. Эта структура данных включает адрес целевого сервера для этой услуги, номер сервера телефонии и другие параметры, используемые для процедуры регистрации (2). Затем устройство генерирует и отправляет SMS-сообщение на номер телефона, указанный в полученной структуре данных (3). Отправленное сообщение немедленно удаляется из журнала отправленных сообщений (4). После отправки сообщения устройство связывается с сервером, расположенным в Сингапуре, и отправляет на сервер телефонии зашифрованный контент отправленного сообщения.

сообщение (5). Сервер связывается с сервером телефонии, на который было отправлено SMS-сообщение (6, 7). Во время связи сообщение, отправленное по телефону, проверяется, и зашифрованное содержимое сообщения отправляется через мобильную интернет-сеть. После успешной проверки сообщений устройству выдается ответ на запрос, добавляющий результат регистрации (8).

Важно отметить, что если SIM-карта не установлена на устройстве во время регистрации, процесс регистрации прекращается и на устройстве отображается сообщение об ошибке.

Прежде чем устройство отправит SMS-сообщение о регистрации номера телефона, устройство связывается с общим сервером, расположенным в Сингапуре, адрес которого - api.account.xiaomi.com (IP-адрес: 161.117.97.141).

Во время связи устройство загружает структуру данных конфигурации, необходимую для процесса регистрации. Эта структура данных включает телефонный номер сервера телефонии, адрес сервера и другие данные. Выдержка данных сетевой связи от устройства к общему серверу показана в Таблице 18.

Таблица 18. Извлечение конфигурации загрузки сетевого трафика

```
Получить / передать / настроить HTTP / 1.1
Тип содержимого: application / x-www-form-urlencoded
Пользовательский агент: Dalvik / 2.1.0 (Linux; U; Android 10; M2007J3SY MI / V12.0.18.0.QJDEUXM) APP / unknown MK / TWkgMTBU
Cookie: sdkVersion = accountsdk-2020.01.09
Хост: api.account.xiaomi.com
Подключение: Keep-Alive
Принятие кодировки: gzip

HTTP / 1.1 200 OK
Дата: среда, 5 мая 2021 г., 09:48:42 GMT Content-Type:
application / json; charset = utf-8 Transfer-Encoding:
фрагментированный
Подключение: keep-Alive
Кодирование содержимого: gzip

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

Устройство отправляет SMS-сообщение на номер телефона, указанный в данных конфигурации.

состав.
В ходе анализа службы регистрации телефонных номеров Xiaomi SIM Activation Service было установлено, что устройство выполняет функцию автоматической отправки SMS-сообщения. Адресат SMS-сообщения и его содержание показаны на рисунке 14.

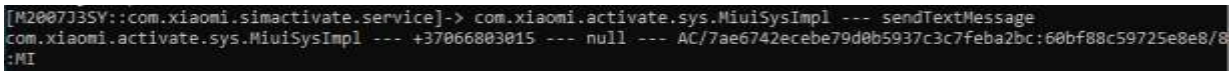


Рис 14. Содержание SMS-сообщения и процесс отправки

После анализа декомпилированной установленной на заводе системной службы Xiaomi SIM Activation Service было обнаружено, что приложение выполняет функцию автоматической отправки SMS-сообщения с использованием внешнего программного класса miui.telephony.SmsManager, которое не компилируется и заархивировано в установочный файл службы.

Фрагмент кода для отправки SMS-сообщения приведен в таблице 19.

Таблица 19. Фрагмент кода для отправки SMS-сообщения.

```
общественная пустота sendTextMessage(int i, String str2, String str3, PendingIntent pendingIntent, PendingIntent
pendingIntent2) {
пытаться {
класс <?> cls = Class.forName (miui.telephony.SmsManager)); Объектподнимать знак равно cls.getDeclaredMethod (
 getDefault, новый класс {Integer.TYPE}). Invoke ((Объект) нулевой, новый
Объект {Integer.valueOf (i)});
 CLS.getMethod (sendTextMessage, новый Класс {String. класс,Нить.класс,Нить.класс, PendingIntent. класс,
PendingIntent. класс}.invoke (invoke, новый объект {ул., ул2, str3, pendingIntent, pendingIntent2)); Log.d (
 MiuSysImpl, «успешно отправлено текстовое сообщение»); }ловить (NoSuchMethodException e) {Log.e (
 MiuSysImpl), «ошибка при отправке текстового сообщения: NoSuchMethodException., д);

 бросить новый RuntimeException (e); }ловить (IllegalAccessException e2) {Log.e (MiuSysImpl),
 «ошибка при отправке текстового сообщения: IllegalAccessException., e2);

 бросить новый RuntimeException (e2); }ловить (InvocationTargetException e3) {Log.e (MiuSysImpl),
 «ошибка при отправке текстового сообщения: InvocationTargetException., e3);

 бросить новый RuntimeException (e3); }ловить (ClassNotFoundException e4) {Log.e (MiuSysImpl),
 «ошибка при отправке текстового сообщения: ClassNotFoundException., e4);

 бросить новый RuntimeException
 (e4); }ловить (SecurityException e5
) {ActivateLog.m24w (MiSysImpl, sendTextMessage,e5); }

}
```

Стоит отметить, что в упомянутом выше внешнем программном классе miui.telephony.SmsManager реализован функционал, позволяющий удалять SMS-сообщения. Функции отправки и удаления SMS-сообщений, а также другие функции, реализованные во внешнем программном классе miui.telephony.SmsManager, показаны на рисунке 15.

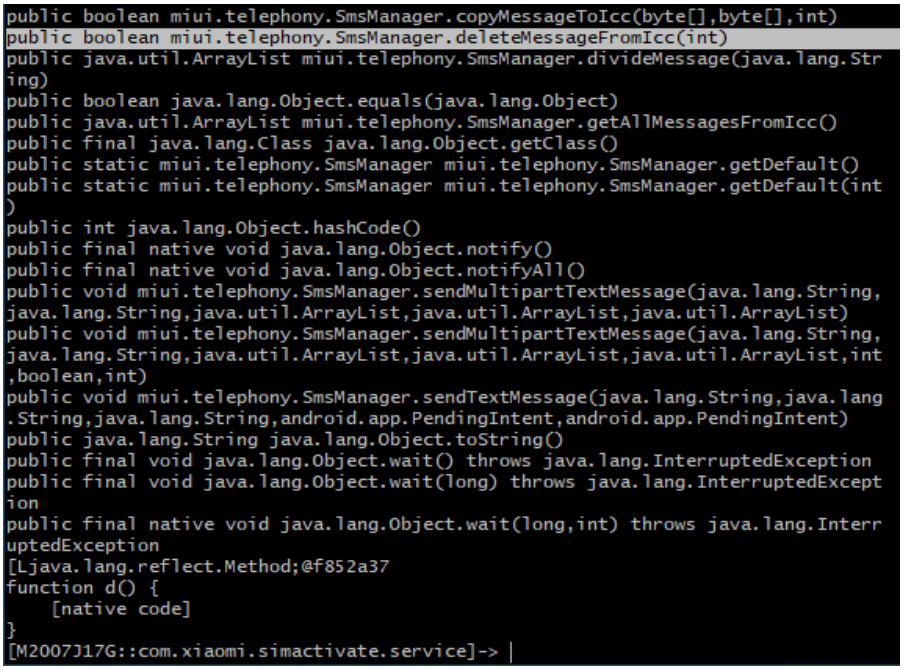


Рисунок 15. Функции отправки и удаления SMS-сообщений, а также другие функции, реализованные в внешний программный класс miui.telephony.SmsManager

Когда устройство отправляет SMS-сообщение на номер телефона, указанный в структуре данных конфигурации, устройство отправляет зашифрованное содержимое SMS-сообщения на адрес sgpac.account.xiaomi.com (Сингапур).

Сервер выполняет проверку содержимого по полученным зашифрованным данным с данными SMS-сообщения, полученными сервером телефонии, и отправляет результат активации на мобильное устройство. Выдержка сетевого трафика приведена в таблице 20.

Таблица 20. Связь с сервером, расположенным в Сингапуре

Опубликовать / пройти / активация / отчет HTTP / 1.1 Content-
Type: application / x-www-form-urlencoded
Пользовательский агент: Dalvik / 2.1.0 (Linux; U; Android 10; M2007J3SY MI / V12.0.18.0.QJDEUXM) APP / unknown MK / TWkgMTBU
Cookie: sdkVersion = accountsdk-2020.01.09
Хост: sgpac.account.xiaomi.com
Подключение: Keep-Alive
Принятие кодировки: gzip
Длина содержимого: 346
DevID = VqFuDPTDczp39bXc & features = CALL_LOG_SYNC ++ MMS_SYNC + & mnc = 24601 & activateMode = uplink & simId = F_9M83JIJb_VOKce &smsBodyEncrypted = fu_5ODSHBbJv5XO6wRTIUfNCEerj978hkm5RhLrK19IYsgPUeVQ oXbY9Di8-
B9WaMvgJeAVwudc_nYD9LWJww28gYA9A9V1kqzNCf8e1tfLftN_Y0UXpvy4cXlHISL5yiGj2sI77KFzS20PgKfocT xNcleEuLITEjTY_38% 3D& action = vkey% 3Aok% 2Cverify% 3A14% 2Cdone% 3A14HTTP / 1.1 200 OK Дата: среда, 5 мая 2021 г., 09:50:27 GMT
Content-Type: application / json Transfer-
Encoding: фрагментированное
соединение: keep-Alive
Кодирование содержимого: gzip
{«Результат»: «ок», «код»: 0, «дата»: {}, «описание»: «.....»}

В ходе анализа было установлено, что устройство взаимодействовало с серверами, расположенными в

Сингапур. Список идентифицированных коммуникаций приведен в Таблице 21.

Стол 21. Информация о связи с серверами, расположенными в Сингапуре.

Линия Нет.:	Домен	Адрес	Данные, Байты	Состояние	Цель
1	api.account.xiaomi.com	161.117.97.141	9200	Сингапур	**Общий сервер** *Конфигурация для аутентификация отправляется из сервер к телефону: СМС тел. номер, адрес сервера и т. д.*
2	sgpac.account.xiaomi.com	161.117.97.227	48990	Сингапур	**Сервер** *На основе SMS-сообщения получил с телефона, ответ на регистрацию генерируется и отправляется на телефон.*

IP-адреса, принадлежащие доменам api.account.xiaomi.com и sgpac.account.xiaomi.com, зарегистрированы в Alibaba.com Singapore E-Commerce Private Limited. Alibaba - компания информационных технологий, основанная в 1999 году в Китайской Народной Республике. Известно, что китайские ИТ-компании обязаны передавать любую форму информации, находящейся под контролем компаний, правительству Китая или его спецслужбам.[32].

Автоматическая отправка сообщений и их сокрытие с помощью программного обеспечения представляют потенциальную угрозу безопасности устройства и личных данных; Таким образом, без ведома пользователя данные устройства могут быть собраны и переданы на удаленные серверы.

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