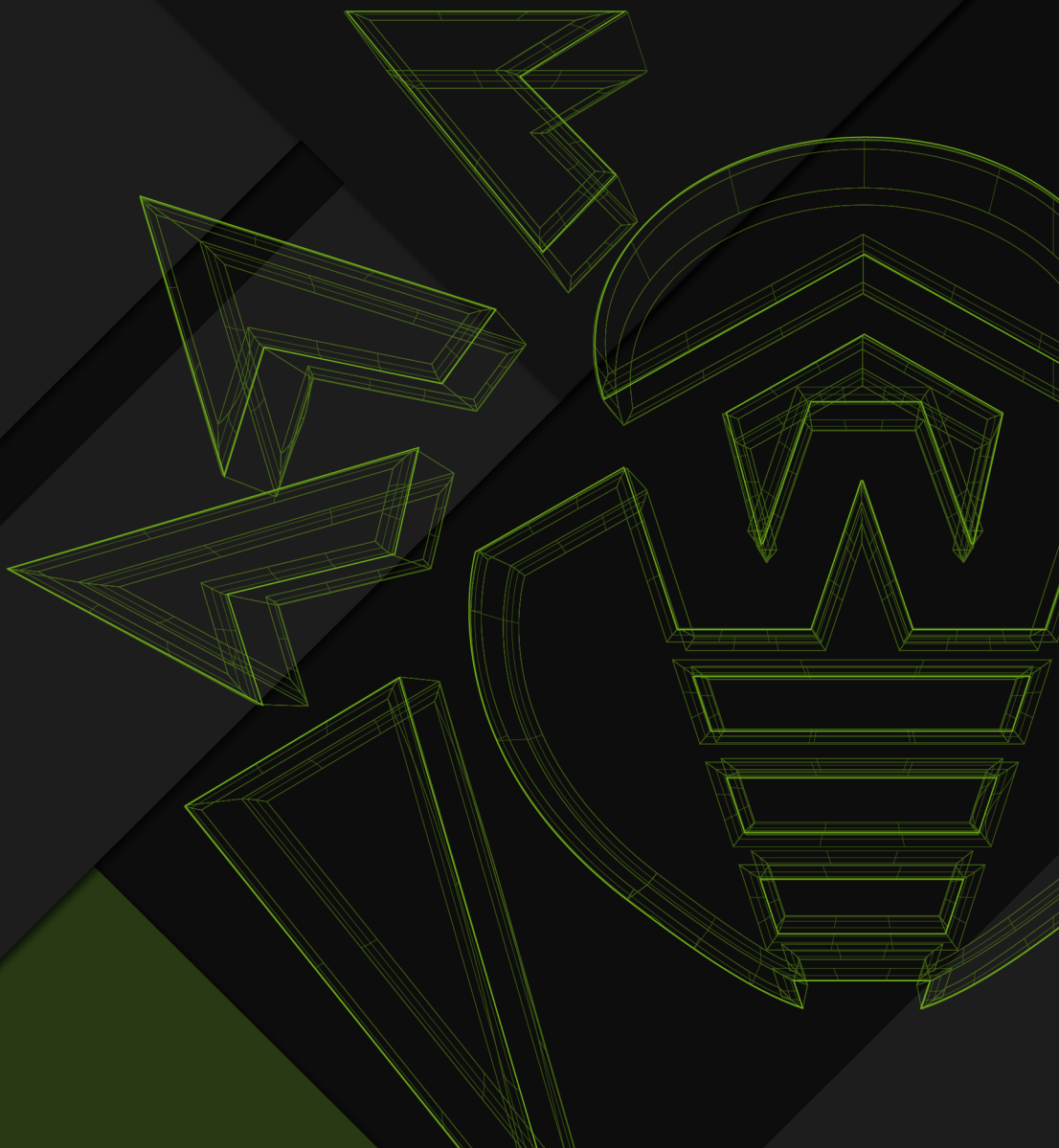
Dr.WEB

Исследование детских смарт-часов на предмет уязвимостей



«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности. Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Исследование детских смарт-часов на предмет уязвимостей
1.11.2021

«Доктор Веб», Центральный офис в России
125040
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: http://www.drweb.com/
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

Введение

Родители всегда стремятся позаботиться о своих детях. Благодаря развитию технологий все чаще в этом им помогают различные компактные носимые устройства — смарт-часы и GPS-трекеры. Все больше моделей таких устройств по функциональности приближаются к полноценным смартфонам. Многие из них позволяют отслеживать местоположение ребенка и маршрут его передвижения через спутниковую систему навигации, совершать и принимать телефонные звонки (в том числе — по видеосвязи), получать СМС, голосовую почту, по команде делать фотографии через встроенную камеру и даже прослушать окружение, а также обладают возможностью дистанционного управления.

Собираемые в процессе работы этих устройств данные обычно передаются на серверы производителей и доступны родителям через персональные учетные записи. При этом информация, которую можно получить с помощью «умных» часов, является очень чувствительной. Если она попадет в руки злоумышленников, детям может угрожать серьезная опасность.

Чтобы понять, насколько уязвимы детские смарт-часы и каковы потенциальные риски их использования, специалисты компании «Доктор Веб» исследовали несколько популярных моделей: Elari Kidphone 4G, Wokka Lokka Q50, Elari FixiTime Lite, Smart Baby Watch Q19. Выбор моделей основывался на публичных рейтингах популярности смарт-часов в России, при этом целенаправленно выбирались устройства разной ценовой категории. Все смарт-часы были приобретены в крупном российском онлайн-магазине анонимно.

При исследовании выполнялся как статический, так и динамический анализ: поиск потенциальных закладок в ПО и возможного присутствия недокументированных функций, а также проверка передаваемых в интернет данных и их защищенность. Для анализа мобильного трафика использовалась программная реализация сети радиодоступа GSM/GPRS.

Выявленные в ходе исследования основные уязвимости смарт-часов представлены в сводной таблице:

	Стоимость часов (средняя) руб.	Расположение управляющего сервера	Протокол передачи данных	Использование стандартного пароля	Наличие скрытого вредоносного кода
Elari Kidphone 4G	5500	за пределами РФ	в зашифрованном виде	Нет	Android.DownLoader.3894 Android.DownLoader.812.origin Android.DownLoader.1049.origin
Wokka Lokka Q50	1300	в РФ	без шифрования	Да	Нет
Elari FixiTime Lite	3700	за пределами РФ	без шифрования	Нет	Нет
Smart Baby Watch Q19	1900	за пределами РФ	в зашифрованном виде	Да	Нет

Смарт-часы Elari Kidphone 4G

Существует несколько версий часов Elari Kidphone 4G, которые построены на базе различных аппаратных платформ, — процессорах MediaTek и Spreadtrum. При этом все они работают под управлением ОС Android и их прошивки отличаются незначительно.

Были рассмотрены прошивки, актуальные на момент проведения анализа:

- версия 1.17_20200529 — для часов с датой производства до ноября 2020 года (старая ревизия);
- версия 2.1.0_20210429_150350 — для часов с датой производства после ноября 2020 года (новая ревизия).

Основной управляющий сервер `dg3.wherecom.com`, куда часы передают собираемые при работе данные, а также вспомогательный сервер `wpush.wherecom.com`, который используется для регистрации устройства и отправки на него команд через протокол MQTT, расположены на хостинге Amazon за пределами России, что может представлять потенциальную опасность. Однако главная угроза этой модели исходит от установленного на ней ПО. В прошивку часов встроено приложение для автоматического обновления «по воздуху» (`/system/app/rsota.apk`), которое содержит троянские функции.

Во-первых, оно передает данные о местоположении ребенка на сторонний сервер `fota.redstone.net.cn`. Во-вторых, внутри него скрыт вредоносный код, детектируемый Dr.Web как **Android.DownLoader.3894**. При первом запуске устройства он расшифровывает и запускает два вредоносных модуля — **Android.DownLoader.812.origin** и **Android.DownLoader.1049.origin**, после чего при каждом последующем включении контролирует их целостность. Если при очередном включении устройства один из модулей будет отсутствовать, троян вновь расшифрует и активирует его.

В дальнейшем при каждом включении часов или изменении сетевого подключения эти модули запускаются автоматически. Они связываются с управляющими серверами для передачи на них различной информации, а также получения команд. По умолчанию модули подключаются к серверам каждые 8 часов. Таким образом, первое соединение они устанавливают с большой временной задержкой с момента первого включения устройства.

Модуль **Android.DownLoader.812.origin** отправляет на сервер `hxxp://mad[.]dwphonetest[.]com:58801/msg/pull` информацию о номере телефона пользователя, данные геолокации, а также сведения о SIM-карте и самом устройстве. В ответ он может получить команды на изменение частоты запросов на соединение с

сервером, обновление самого модуля, загрузку, установку, запуск и удаление приложений, а также загрузку заданных веб-страниц.

В свою очередь, модуль **Android.DownLoader.1049.origin** передает на сервер `hxxps://g[.]sinfoon[.]com:40081/data` информацию о SIM-карте и номере телефона, данные о местоположении, большой объем информации об устройстве и установленных на нем приложениях, а также о количестве СМС, телефонных звонков и контактов в адресной книге.

Таким образом, скрытые в этих часах трояны могут использоваться для кибершпионажа, показа рекламы и установки ненужных и даже опасных программ.

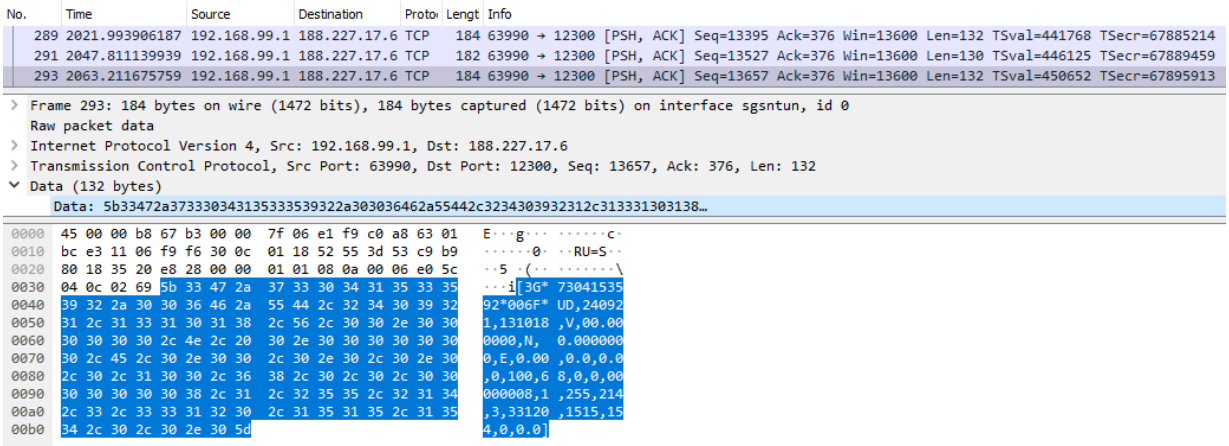
Смарт-часы Wokka Lokka Q50

Рассмотренная прошивка часов имела версию G36S_0.96_SHU_V1.1.

Анализ сетевой активности этой модели не выявил каких-либо подозрительных действий. Данные о местоположении ребенка, которые собираются в процессе работы часов, по умолчанию передаются на расположенный в России сервер `188.227.17.6`. При этом отправка чувствительной информации на сторонние серверы не наблюдалась.

Потенциальную опасность для пользователей Wokka Lokka Q50 может представлять то, что передача данных геолокации на сервер в них осуществляется в открытом виде, без шифрования. Теоретически злоумышленники могут перехватить незащищенные данные, выполнив атаку типа «человек посередине». Однако поскольку отправка информации происходит через мобильную сеть оператора, для успешного осуществления такой атаки потребуется специализированное оборудование и наличие у злоумышленников определенных навыков.

Пример запроса, в котором на сервер передаются незащищенные данные с информацией о местоположении на основе GPS и LBS:



Официально часы контролируются при помощи мобильного приложения, которое устанавливается на устройства родителей. Однако моделью Wokka Lokka Q50 можно также управлять и при помощи специальных СМС-команд. При этом в инструкции сведения о такой возможности отсутствуют. Сама же реализация СМС-управления несет в себе определенные риски.

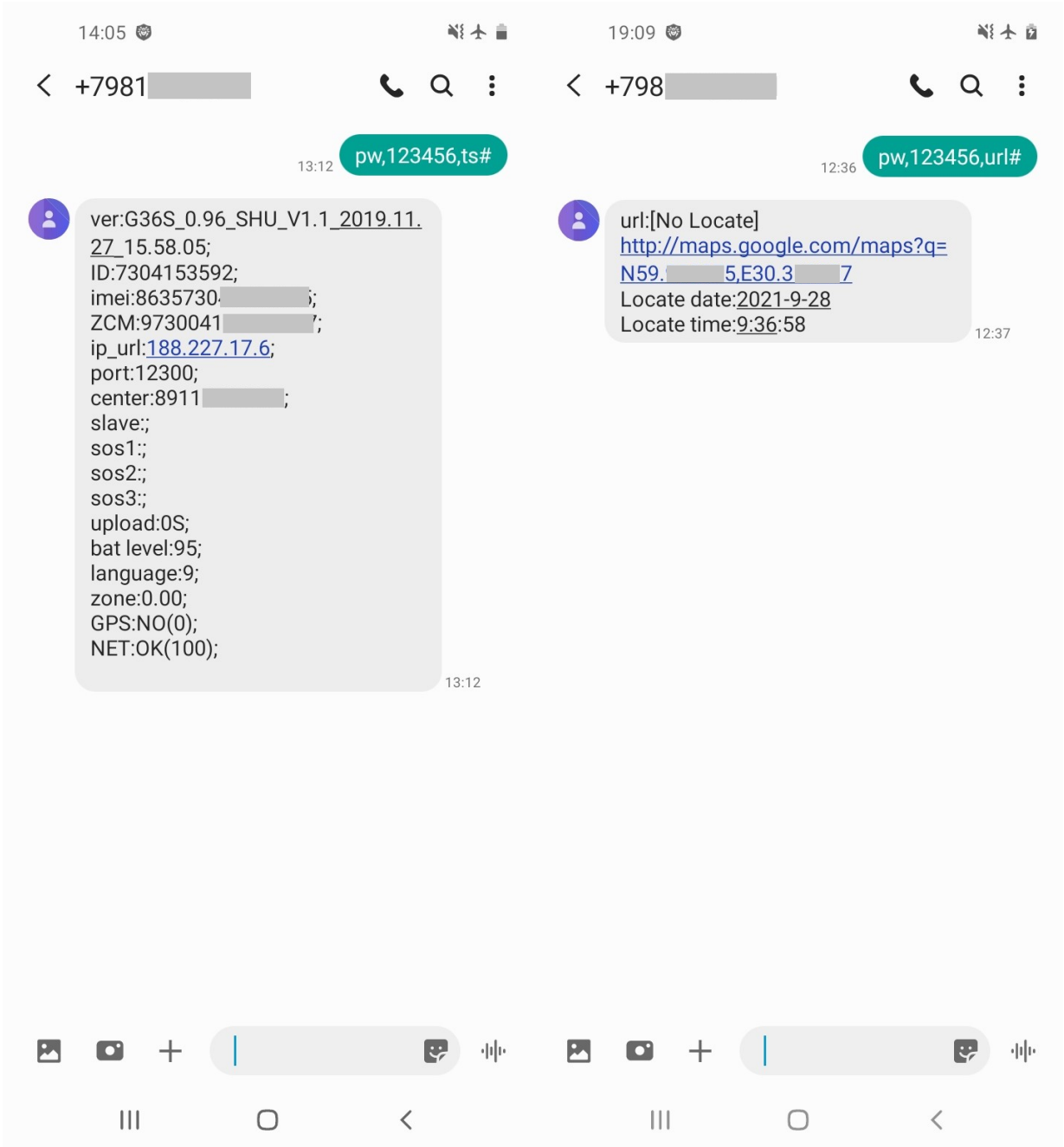
Главной уязвимостью Wokka Lokka Q50 в данном случае является использование стандартного для всех устройств линейки пароля `123456` для передачи СМС-команд (в некоторых версиях часов используется пароль `523681`). При этом в часах отсутствует функция его принудительной смены при первом включении. Нет рекомендации о его замене и в комплектной инструкции, сменить его через управляющее приложение тоже нельзя.

Единственная информация о возможности и способе изменения стандартного пароля имеется в онлайн-справке на официальном сайте бренда. Однако далеко не каждый пользователь целенаправленно посещает официальные сайты приобретаемой электроники в поисках дополнительной информации. Поэтому значительная доля покупателей данных часов не только не будет знать, что часами можно управлять через СМС, но и будет использовать устройства со стандартным паролем, не подозревая, что его можно и нужно сменить. В этом заключается серьезная угроза.

Так, зная номер телефона установленной в часы SIM-карты и используя известный пароль, потенциальный злоумышленник сможет без труда получить контроль над устройством. Например, запросить GPS-координаты командой `pw,123456,url#`, которые поступят в ответном СМС, дистанционно прослушать окружение через обратный звонок на указанный в команде номер и даже изменить адрес управляющего сервера на собственный, получая доступ ко всей информации, которую собирают эти часы.

При этом, даже если стандартный пароль будет изменен, это не решит проблему полностью. Для атакующего многие команды после смены пароля станут недоступны. Однако команда `pw,123456,ts#` для проверки параметров часов по-прежнему будет исполняться без ограничений, и вызвать ее будет возможно с любого номера. Поэтому, если злоумышленник задействует эту команду, часы среди прочих сведений об устройстве сообщат ему и текущий номер администратора. Узнав его, атакующий при помощи СМС-спуфинга (подмены номера) сможет от имени администратора (т. е. родителей) задать новый пароль и получить полный контроль над устройством.

На следующих изображениях продемонстрирован пример ответа часов Wokka Lokka Q50 на подобный запрос, а также данные о местоположении устройства после отправки соответствующей команды потенциального злоумышленника:

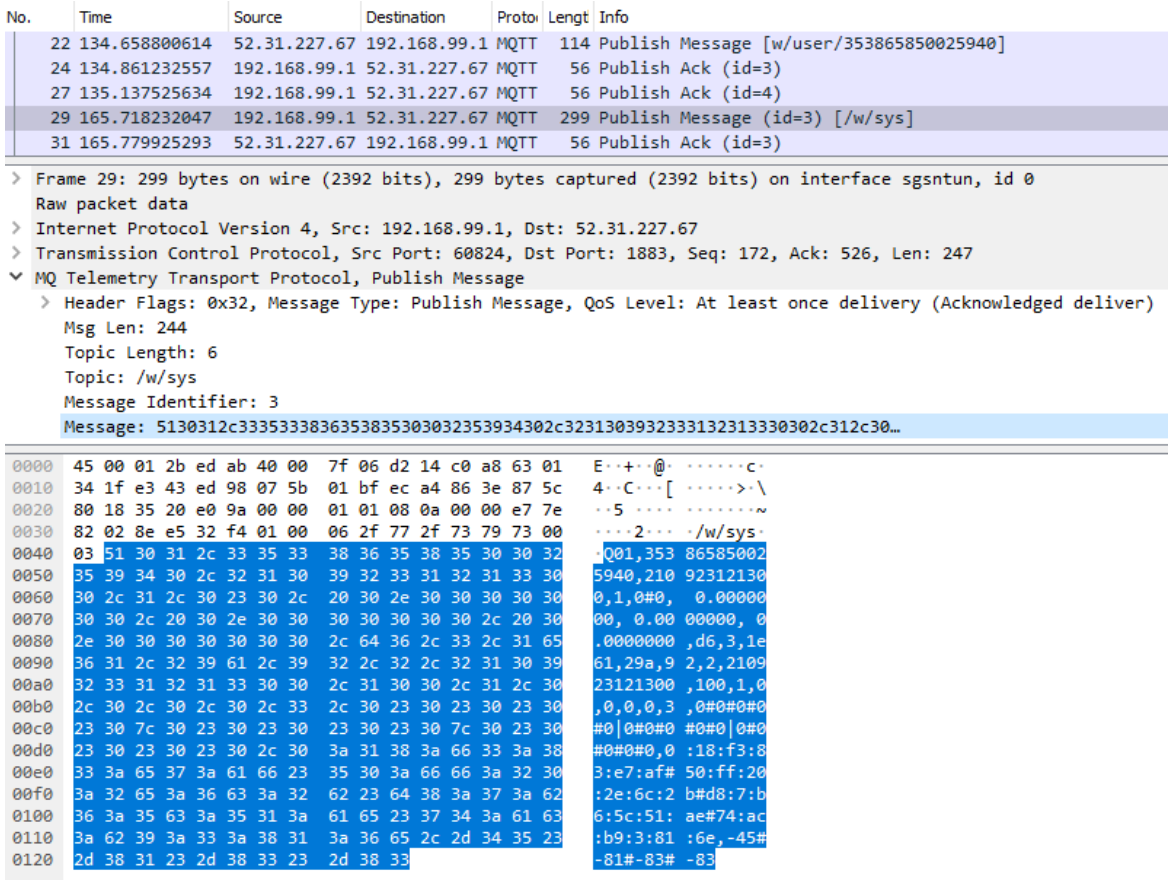


Смарт-часы Elari FixiTime Lite

Рассмотренная прошивка этой модели имела версию K16_2503D_FOREIGN_RU_H_V1.0.

При анализе сетевой активности часов Elari FixiTime Lite не было выявлено каких-либо подозрительных действий. Однако управляющий сервер `mqtt.wherecom.com` (`52.31.227.67`), на который пересылаются собираемые данные, находится за пределами России на хостинге Amazon. Кроме того, информация о GPS-координатах передается на сервер по протоколу MQTT в незашифрованном виде, как и в случае с часами Wokka Lokka Q50. Также через незащищенный протокол HTTP передаются и фотографии с голосовыми сообщениями. В случае успешной атаки «человек посередине» злоумышленники смогут перехватить эти данные.

Пример отправки незашифрованных данных о местоположении, в котором передаются данные GPS, LBS-позиционирования в шестнадцатеричном формате, а также данные об окружающих Wi-Fi-сетях:



Потенциальную опасность в этих смарт-часах представляет и то, что пароль для подключения к протоколу MQTT для передачи данных телеметрии жестко прописан в прошивке устройства. Если злоумышленнику будет известен IMEI часов и этот пароль, он сможет подключиться к серверу и «притвориться» атакованным устройством, передавая поддельные данные.

Смарт-часы Smart Baby Watch Q19

Рассмотренная прошивка этой модели имела версию R36CW_S12_v.1.0.

Анализ часов не выявил подозрительной активности, а также наличия управляющих команд, использование которых могло бы привести к утечке конфиденциальной информации. Собираемые часами данные передаются на управляющий сервер `52.28.132.157` в зашифрованном виде, поэтому для злоумышленников получить к ним доступ будет непросто. Потенциальную угрозу, однако, представляет то, что этот сервер находится не на территории России (хостинг Amazon). Кроме того, для отправки управляющих команд по СМС в них также используется стандартный пароль `123456`. Однако в данной модели часов список доступных команд значительно сокращен.

Выводы

Проведенный анализ показал, что в целом безопасность детских смарт-часов находится на весьма неудовлетворительном уровне. Наше исследование затронуло несколько моделей, однако проблема этих устройств заключается в том, что на разных моделях могут использоваться схожие прошивки и ПО. Например, прошивки, аналогичные той, что установлены в часах Wokka Lokka Q50, применяются в большом количестве других моделей смарт-часов различных брендов, а также во всевозможных GPS-трекерах. Кроме того, для них также задан стандартный пароль управления через СМС. Следовательно, их пользователи подвержены тем же рискам, что и владельцы часов Wokka Lokka Q50. При этом на рынке постоянно появляются новые модели, и нет гарантии, что и в них не будет каких-либо уязвимостей.

Кроме того, обнаружение предустановленного на смарт-часы Elari Kidphone 4G трояна наглядно демонстрирует, какая опасность может скрываться в устройствах такого типа, работающих под управлением ОС Android. Прошивки для них часто создаются сторонними фирмами, и производители редко проверяют их безопасность и целостность. Следовательно, велика вероятность того, что на одном из этапов производства Android-часов злоумышленники внедрят в них троянское или рекламное ПО.

Компания «Доктор Веб» уведомила производителей исследованных часов о выявленных уязвимостях.

Смарт-часы — удобное и относительно недорогое решение для защиты и наблюдения за ребенком. Но вместе с пользой такие устройства могут нести и определенные риски: без разрешения передавать конфиденциальную информацию сторонним сервисам, выполнять вредоносные функции и даже контролироваться злоумышленниками при взломе, подвергая опасности детей.

Родителям следует с осторожностью использовать такие устройства для контроля за детьми и взвешенно подходить к их покупке. Ведь может случиться так, что выбранная модель трекера принесет больше вреда, чем пользы.

Принцип действия найденных образцов вредоносных программ

Android.DownLoader.3894

Троянский код, встраиваемый в системные приложения для беспроводного обновления прошивок Android-устройств. Например, этот код был обнаружен в прошивке смарт-часов Elari Kidphone 4G, однако он может присутствовать и на других моделях и типах устройств. Его основная функциональность сосредоточена в отдельных модулях, которые он запускает в процессе своей работы.

Принцип действия

Троянские компоненты — `libcore64.jar` (**Android.DownLoader.812.origin**) и `libcore.jar` (**Android.DownLoader.1049.origin**) — хранятся внутри приложения в зашифрованном виде. При первом запуске устройства **Android.DownLoader.3894** расшифровывает и запускает их, после чего при каждом последующем включении контролирует их целостность. Если при очередном включении устройства один из модулей будет отсутствовать, троян вновь расшифрует и активирует его.

Для автоматического запуска модулей **Android.DownLoader.3894** устанавливает широковещательные приемники на следующие события:

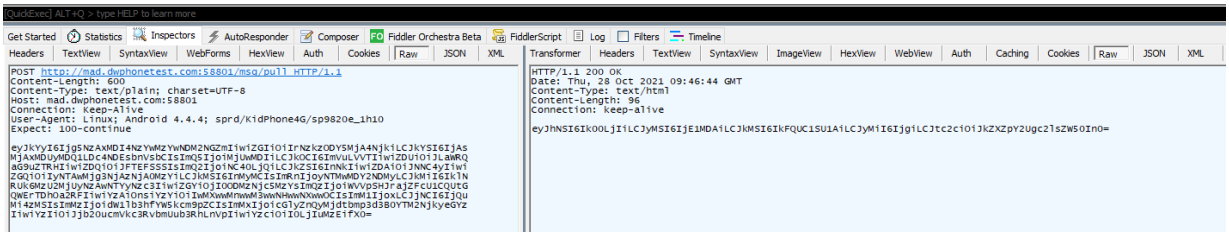
- `android.intent.action.BOOT_COMPLETED` — включение устройства;
- `android.net.conn.CONNECTIVITY_CHANGE` — изменение сетевого подключения.

Android.DownLoader.812.origin

Троянский модуль **Android.DownLoader.812.origin** представляет собой файл `libcore64.jar`, который в зашифрованном виде хранится в программном пакете приложения `rsota.apk`. При первом включении устройства встроенный в эту программу вредоносный код (**Android.DownLoader.3894**) расшифровывает и запускает его. При последующих включениях устройства, а также при изменении сетевого подключения модуль запускается автоматически.

Принцип действия

После запуска **Android.DownLoader.812.origin** с заданной периодичностью подключается к C&C-серверу по адресу `hxxp://mad[.]dwphonetest[.]com:58801/msg/pull` и отправляет на него запрос. Пример такого запроса:



В нем могут передаваться следующие данные, закодированные base64:

- `d0` — `version` — версия троянского модуля;
- `d1` — `session` — константа `APP-REQ`, заменяется значением `s20`;
- `d2` — `devid` — уникальный идентификатор устройства (IMEI-идентификатор для GSM-устройства, MEID- или ESN-идентификатор для CDMA-устройства);
- `d3` — `utdid` — уникальный идентификатор устройства UserTrack Device Identity;
- `d4` — `man` — наименование производителя устройства;
- `d5` — `mod` — наименование модели устройства;
- `d6` — `osv` — версия установленной на устройстве операционной системы;
- `d8` — `lang` — язык, установленный на устройстве по умолчанию;
- `d9` — `operator(mcc mnc)` — идентификатор мобильного оператора (MCC+MNC);
- `da` — `loc` — данные геолокации;
- `db` — `msisdn` — мобильный номер;
- `dc` — `iccid` — идентификатор SIM-карты;
- `dd` — `imsi` — уникальный идентификатор абонента мобильного оператора;

- de — dldir — расположение стандартной директории для загрузок файлов из интернета (для встроенной памяти присваивается значение data, для SD-карты — sd);
- df — avaisize — свободный объем встроенной памяти устройства;
- dg — totalsize — общий объем встроенной памяти устройства;
- c1 — appid — значение RSOTA_APP_ID из метаданных приложения;
- c2 — carrier_pkgname — имя пакета приложения, в которое встроен троян;
- c3 — channel — значение RSOTA_CHANNEL_ID из метаданных приложения;
- c4 — carrier_version — значение coreVersion;
- c5 — silent — параметр, указывающий на то, является ли приложение с троянским модулем системным или нет;
- c6 — capability — значение 01|02|03|04|05|08;
- c7 — stub_version — значение agentVersion.

В ответ троян может получать следующие команды:

- r2 — cycle — изменить частоту запросов к C&C-серверу;
- a0 — applist — получить параметры, необходимые для загрузки, запуска и установки приложений:
  - a3 — pkgname
  - a5 — appversion
  - a20 — versionCode
  - a4 — appname
  - a6 — brief
  - a7 — objecturi
  - a8 — objectsize
  - a9 — icon
  - a10 — start
    - a11 — type
    - a12 — action
    - a13 — class
    - a14 — extra
  - a1 — correlator
  - a2 — taskid
  - a15 — operation — выполнить действие в соответствии с указанным значением параметра:
    - 1 — загрузить и установить приложение;
    - 2 — загрузить, установить и запустить приложение;

    - 3 — запустить заданное приложение;
  - l0 — link — загрузить заданный URL;
- a21 — caplist — получить параметры, необходимые для удаления приложений, а также собственного обновления:
  - a3 — pkgname
  - a1 — correlator
  - a2 — taskid
  - a7 — objecturi
  - a8 — objectsize
  - a5 — appversion
  - a15 — operation — выполнить действие в соответствии с указанным значением параметра:
    - 4 — удалить заданное приложение;
    - 8 — обновить троянский модуль.

После успешного или неудачного выполнения задания троян связывается с C&C-сервером по адресу hxxp://mad[.]dwphonetest[.]com:58802/msg/post и отправляет на него запрос с номером и статусом задачи.

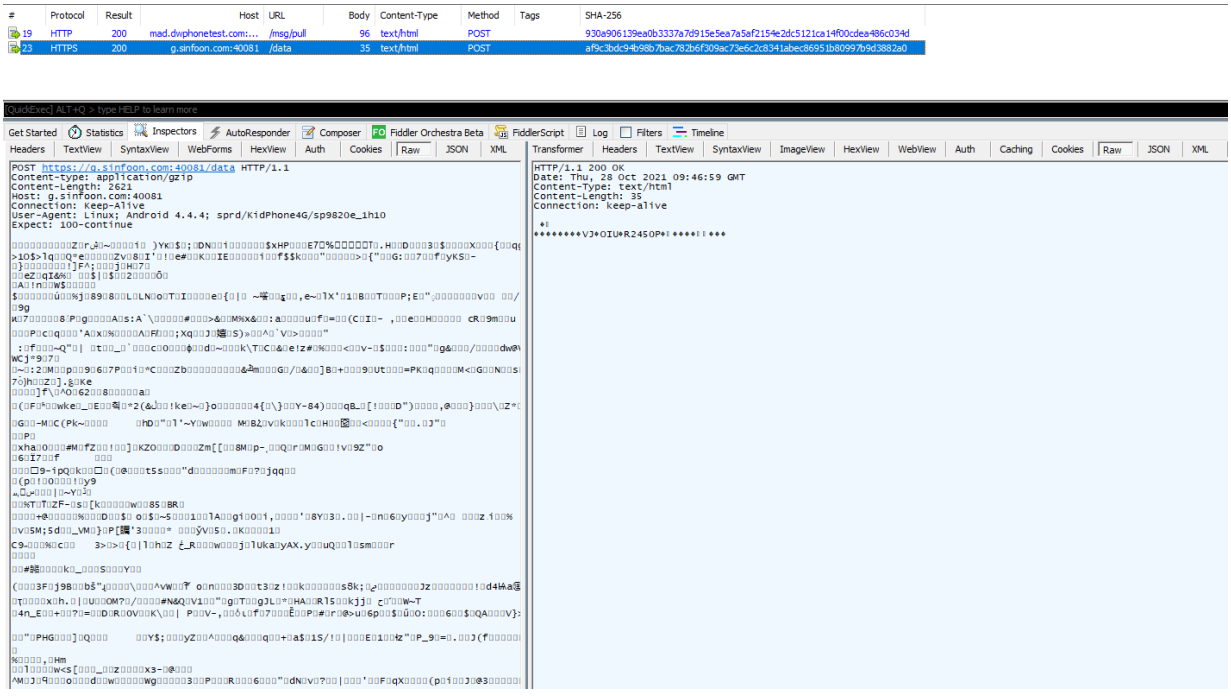
Как мы видим, **Android.DownLoader.812.origin** отправляет на сервер информацию о номере телефона пользователя, данные геолокации, а также сведения о SIM-карте и самом устройстве. В ответ он может получать команды на изменение частоты запросов на соединение с сервером, обновление самого модуля, загрузку, установку, запуск и удаление приложений, а также загрузку заданных веб-страниц.

Android.DownLoader.1049.origin

Троянский модуль **Android.DownLoader.1049.origin** представляет собой файл `libcore.jar`, который, как и первый модуль, в зашифрованном виде хранится в программном пакете основного приложения. Аналогично **Android.DownLoader.812.origin**, он расшифровывается и запускается вредоносным кодом **Android.DownLoader.3894** при первом включении устройства. При последующих включениях, а также при изменении сетевого подключения этот модуль запускается автоматически.

Принцип действия

После запуска **Android.DownLoader.1049.origin** с заданной периодичностью подключается к C&C-серверу, расположенному по адресу `hxxps://g[.]sinfoon[.]com:40081/pull`, и отправляет на него запрос, пример которого показан ниже:



В запросе передаются данные, сжатые GZIP:

- `version` — версия троянского модуля;
- `session` — константа `02`;
- `timestamp` — текущее время;
- `utdid` — уникальный идентификатор устройства UserTrack Device Identity;
- `appid` — значение `RSOTA_APP_ID` из метаданных приложения;
- `channel` — значение `RSOTA_CHANNEL_ID` из метаданных приложения;
- `man` — наименование производителя устройства;

- mod — наименование модели устройства;
- board — название печатной платы устройства;
- imei1 — IMEI-идентификатор для GSM-устройства;
- imei2 — IMEI-идентификатор для GSM-устройства;
- meid — MEID- или ESN-идентификатор для CDMA-устройства;
- osv — версия установленной на устройстве операционной системы;
- carrier1 — уникальный IMSI-идентификатор абонента мобильного оператора;
- carrier2 — уникальный IMSI-идентификатор абонента мобильного оператора;
- stubver — константа 1.0;
- implver — константа 2.

В ответ троян может получать следующие команды и параметры:

- profile — изменение общих настроек:
  - pulse — изменение частоты запросов к C&C-серверу;
  - enable — отключение троянского модуля.
- configlist — изменение параметров конфигурации:
  - configtype
  - typeenable
  - captureinterval
  - reportinterval
- updd — загрузить заданный файл. Возможные параметры:
  - taskid
  - version
  - objecturi
  - objectsize
  - icv

О результатах выполнения задания он информирует C&C-сервер по адресу hxxps://g[.]sinfoon[.]com:40081/result.

В процессе работы **Android.DownLoader.1049.origin** передает на C&C-сервер hxxps://g[.]sinfoon[.]com:40081/data большой объем информации:

- version — версия троянского модуля;
- session — константа 02;
- utdid — уникальный идентификатор устройства UserTrack Device Identity;
- appid — значение RSOTA_APP_ID из метаданных приложения;
- channel — значение RSOTA_CHANNEL_ID из метаданных приложения;
- man — наименование производителя устройства;

- `mod` — наименование модели устройства;
- `board` — название печатной платы устройства;
- `imei1` — IMEI-идентификатор для GSM-устройства;
- `imei2` — IMEI-идентификатор для GSM-устройства;
- `meid` — MEID- или ESN-идентификатор для CDMA-устройства;
- `os` — установленная на устройстве операционная система;
- `osv` — версия установленной на устройстве операционной системы;
- `carrier1` — уникальный IMSI-идентификатор абонента мобильного оператора;
- `carrier2` — уникальный IMSI-идентификатор абонента мобильного оператора.

А также:

- `app` — `appinfo` — сведения об установленных приложениях:
  - `pkg` — имя пакета;
  - `name` — название;
  - `apver` — версия;
  - `instts` — дата установки;
  - `usenum` — число запусков;
  - `usedur` — время использования;
  - `power` — использованный заряд аккумулятора;
  - `opents` — время последнего запуска приложения.
- `dev_id` — идентификаторы пользователя:
  - `dpid` — идентификатор Google Play Services Android ID;
  - `mac` — MAC-адрес;
  - `phoneno` — номер мобильного телефона;
  - `iccid1` — идентификатор SIM-карты;
  - `iccid2` — идентификатор SIM-карты;
  - `imsi1` — уникальный идентификатор абонента мобильного оператора;
  - `imsi2` — уникальный идентификатор абонента мобильного оператора.
- `dev_hw` — общие аппаратные характеристики устройства:
  - `devtype` — тип устройства;
  - `hwv` — название аппаратного обеспечения;
  - `resolution` — разрешение экрана;
  - `lang` — язык системы, используемый на устройстве по умолчанию.
- `dev_behavior` — статистика использования устройства:
  - `smsnum` — количество СМС;
  - `contactsnum` — количество контактов телефонной книги;

  - `callnum` — количество телефонных звонков;
  - `traffic` — информация о передаваемом на устройстве трафике:
    - `totalrx` — объем принятого сетевого трафика;
    - `totaltx` — объем переданного сетевого трафика;
- `dev_loc` — данные геолокации:
  - `gps` — местоположение на основе данных GPS;
  - `cell` — местоположение на основе данных сотовой сети.
- `dev_capa` — статистика использования аппаратных ресурсов устройства:
  - `romusage` — объем доступной внутренней памяти;
  - `ramusage` — объем доступной оперативной памяти;
  - `screenlight` — яркость подсветки экрана;
  - `conntype` — тип подключения к сети;
  - `batterylevel` — уровень заряда аккумулятора;
  - `chargecount` — счетчик циклов заряда аккумулятора;
  - `dischargecur` — ток разряда аккумулятора;
  - `fgu` — параметры аккумулятора (для устройств на базе процессоров Spreadtrum);
  - `runtime` — общее время работы устройства с момента последнего включения;
  - `process` — информация о процессах:
    - `psn` — имя процесса;
    - `bts` — время начала его работы;
    - `ets` — время завершения его работы.
  - `cputemper` — температура процессора;
  - `cpuusage` — статистика использования процессора:
    - `cupid` — индекс модели;
    - `rate` — уровень загруженности;
    - `freq` — частота.
  - `signal` — информация о мобильной сети:
    - `networktype` — тип подключения к сети;
    - `strength` — уровень мощности сигнала.
  - `sensor` — информация о датчиках устройства:
    - `sensortype` — тип датчика;
    - `sensorstatus` — включен ли датчик.
  - `wcn` — включены ли Bluetooth, Wi-Fi или GPS:
    - `wcntype` — тип передатчика;
    - `wcnstatus` — его статус.

- `timestamp` — текущее время;
- `boot` — время включения устройства.

Приложение №1. Индикаторы компрометации

SHA1-хеши

Android.DownLoader.3894

ac3dff8e8f58c9e1fc27e48f83819257d6553169 — rsota.apk (приложение Software Update, com.redstone.ota.ui)

00712a8154c7d399ff1905cdab34a73a1bdbde9d — rsota.odex

Android.DownLoader.1049.origin

7c7b9db22cb09f85371a41a2bce6f730b1fce5d9 — libcore.jar

Android.DownLoader.812.origin

1d5cb15e64612fcf35eaf8af5e5a3303a2a3258a — libcore64.jar

Домены

hxxp://mad[.]dwphonetest[.]com:58801/msg/pull

hxxp://mad[.]dwphonetest[.]com:58802/msg/post

hxxps://g[.]sinfoon[.]com:40081/pull

hxxps://g[.]sinfoon[.]com:40081/result

hxxps://g[.]sinfoon[.]com:40081/data