Детали доставки: исследование новой версии Android-трояна DeliveryRAT

Описание угрозы

Впервые Android-троян DeliveryRAT мы упоминали в годовом отчете F6 за 2024 год. В апреле 2025 года нами была раскрыта обновленная версия трояна, дополненная различными функциональными возможностями, включая выполнение DDOS-атак, запуск различных визуальных активностей для кражи дополнительных данных или перенаправление пользователя на сторонние ресурсы через отображение QR-кодов .

Способы распространения данного ВПО были детально описаны в недавней публикации нашей компании — **F6 и RuStore заблокировали более 600 доменов, распространявших Android-троян DeliveryRAT**. В статье был разобран Telegram-бот «Bonvi Team», с помощью которого генерировались либо ссылки на фейковые страницы, мимикрирующие под сервис загрузки приложений с возможностью загрузить целевой сервис, либо генерировался непосредственно образец ВПО.

В этом блоге мы остановимся на описании обновленной версии ВПО DeliveryRAT, распространяемого злоумышленниками во второй половине 2025 года.

Приложение-загрузчик

В некоторых случаях злоумышленники использовали приложение-загрузчик при распространении DeliveryRAT. Все обнаруженные загрузчики имеют имя пакета com.harry.loader. DeliveryRAT расположен внутри секции ресурсов загрузчика в директории raw. После запуска отображается страница якобы с обновлением приложения сервиса для загрузки приложений и кнопкой «Обновить». (Рис. 1)

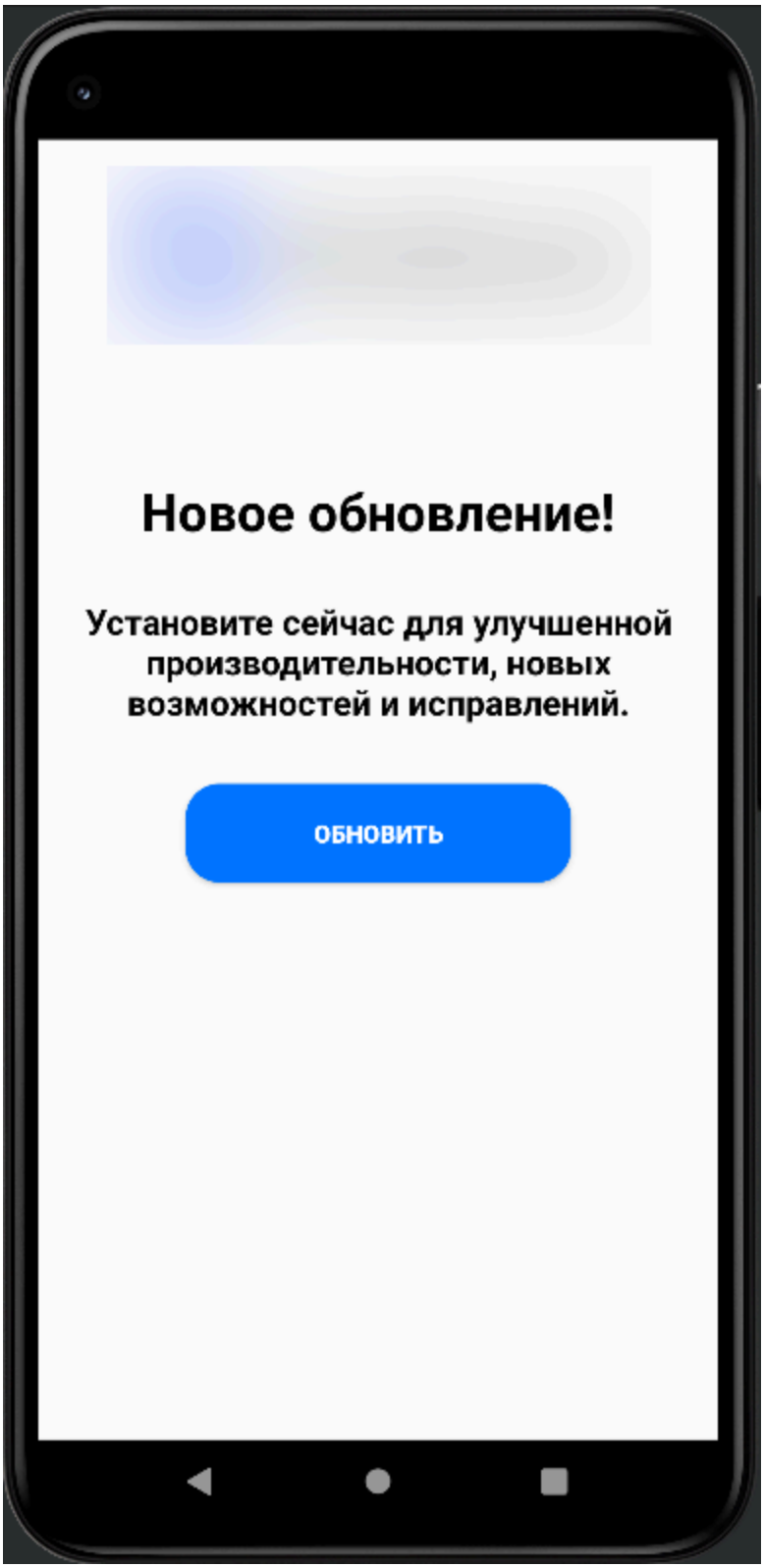

Рис. 1 Окно приложения-загрузчика

После того как пользователь нажмет на кнопку, приложение запросит права установки сторонних приложений на устройство. После выдачи пользователем запрашиваемых прав будет установлен DeliveryRAT. При следующих попытках запуска приложения загрузчика, когда целевое приложение установлено, загрузчик будет запускать это приложение по соответствию имени пакета.

Маскировка под доверенные приложения

В ходе нашего исследования было найдено множество образцов DeliveryRAT, мимикрирующих под различные сервисы, доступные в России. Среди которых:

- службы доставок;
- маркетплейсы;
- банки;
- нотариат (только названием и иконкой);
- мод для Telegram с функцией анонимности и управления переписками Oniongram (только названием и иконкой);
- сервис поиска специалистов;
- сервис для поиска попутчиков;
- сервисы размещения объявлений;
- сервис совместного просмотра видео и фильмов;
- сервис покупки автобусных билетов.

Также среди загрузчиков были найдены отдельные образцы, мимикрирующие своим названием и иконкой под государственный сервис.

Функциональные возможности DeliveryRAT

Перечислим функциональные возможности первой обнаруженной версии ВПО:

- эксфильтрация получаемых на устройство SMS-сообщений;
- эксфильтрация и сокрытие получаемых на устройство Push-уведомлений;
- выполнение произвольных USSD-запросов;
- сокрытие/отображение иконки приложения;
- отправка произвольных SMS-сообщений;
- отображение шаблонной активности с полем для ввода и модерируемым злоумышленниками текстовым полем.

В обновленную версию были добавлены следующие функциональные возможности:

- запуск по команде различных видов активностей для пользователя, в контексте которых присутствуют активности ввода информации о банковской карте, выбора фотографии, сканирование QR-кода и так далее;

- выполнение DDOS-атак путем осуществления одновременных запросов к переданной командой URL-ссылке;
- эксфильтрация списка контактов;
- рассылка SMS всем контактам;
- (в разработке/отключено билдером) возможность обмениваться сообщениями с жертвой под видом поддержки.

Технические детали

За основу нашего исследования был взят образец DeliveryRAT, который распространялся через фишинговую ссылку, которая мимикрировала под сервис для загрузки приложений. Сам образец распространялся под видом приложения маркетплейса.

Исследуемый образец:

- MD5: 42ce4d0c3d373220d3a5c8c52579daa4
- SHA-1: a3261679ea0625be3ef7f8290984d35c3763fdf7
- SHA-256: c64eb9cc28335f000e61f5e2afa97b30e43dd8852e41edc30b4ec02684b81e5a

Конфигурация:

```
{
  "API": "akokakola[.]com",
  "APPLICATION_ID": "com.delviskesyty.{REDACTED}",
  "BUILD_TYPE": "debug",
  "DEBUG": false,
  "MODE": "standart",
  "Mail": "false",
  "Support": "false",
  "TEAM_ID": "5657606",
  "VERSION_CODE": 2,
  "VERSION_NAME": "2.0.4",
  "WORKER_ID": "7fc4bd09206efbb0"
}
```

После запуска приложение выполнит проверку наличия прав создания уведомлений на устройстве и игнорирования оптимизация батареи. Если такие права выданы (не первый запуск), то приложение перейдет к отображению окна для ввода трек номера. Если же приложение запущено впервые, то выполняется проверка интернет соединения, при его отсутствии отображает пользователю соответствующую информацию (Рис. 2).


Нет подключения к интернету
Проверьте подключения и перезапустите приложение

Рис. 2 Окно с информацией об отсутствии интернет соединения

Если устройство имеет подключение к интернету, то будет отображено окно предоставления прав приложению (Рис. 3).

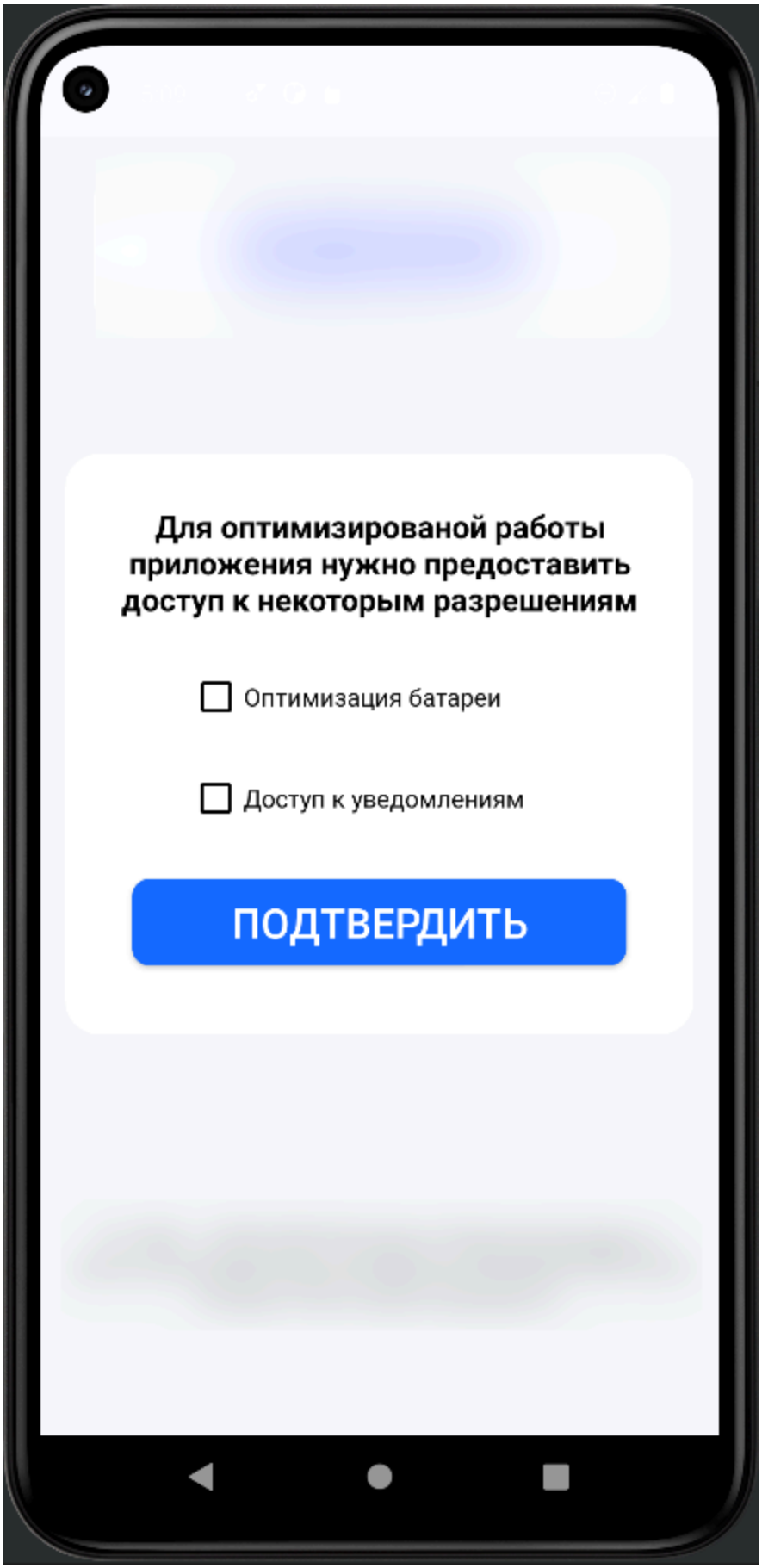
Для оптимизированой работы приложения нужно предоставить доступ к некоторым разрешениям
Оптимизация батареи
Доступ к уведомлениям
ПОДТВЕРДИТЬ

Рис. 3 Окно с запросом предоставления прав приложению

Затем приложение запускает сервис **WebSocketService**, который выполняет соединение по WebSocket с управляющим сервером (описан в соответствующем разделе ниже), и ожидает кликов на чек-боксы и выдачи прав приложению.

После того, как права были выданы, и пользователь нажал на кнопку подтвердить, приложение переходит к основной активности ввода трек номера.

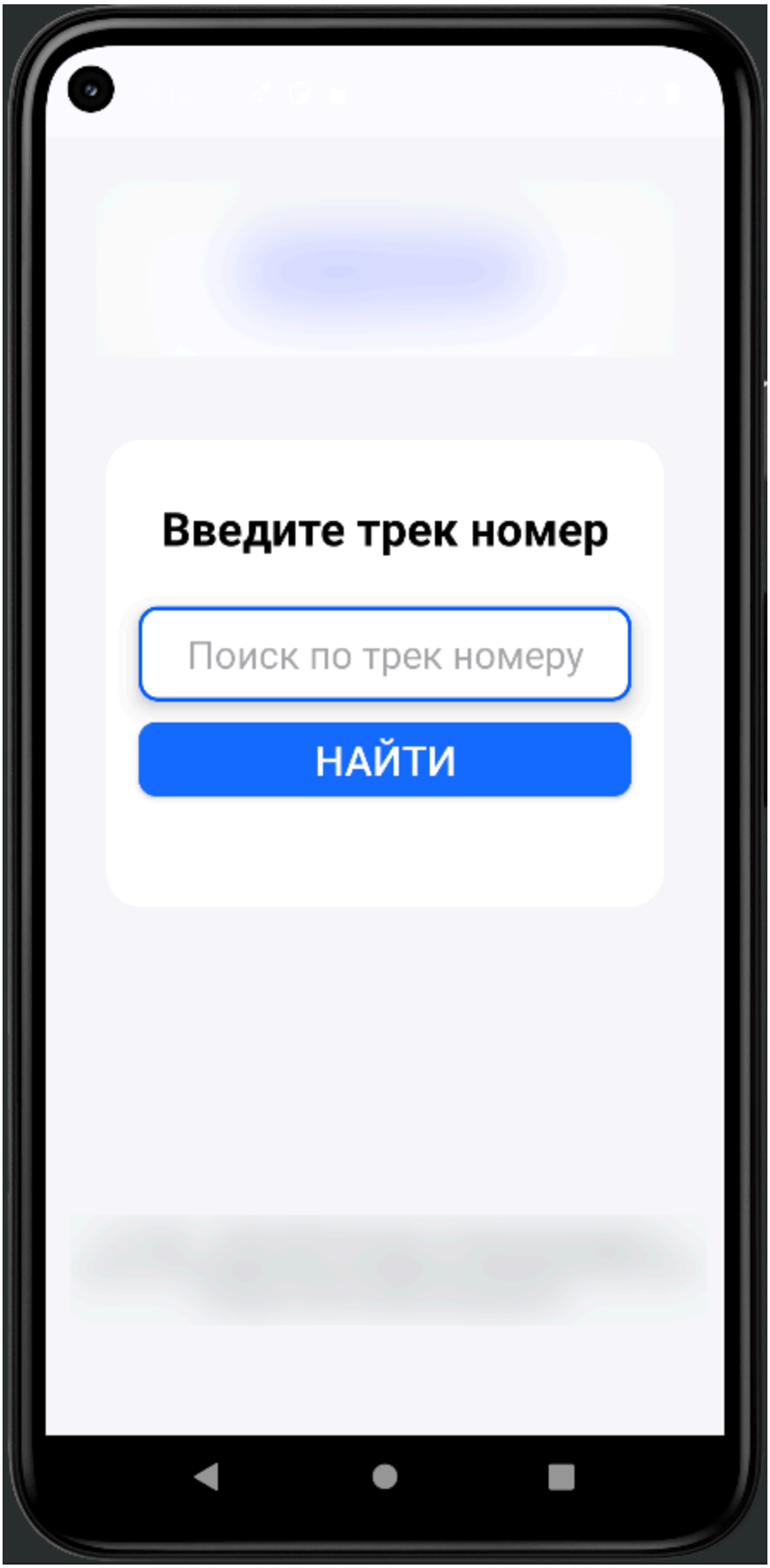
Введите трек номер
Поиск по трек номеру
НАЙТИ

Рис. 4 Основное окно с запросом ввода трек номера

После отображения данной активности будет выполнена проверка и запрос недостающих прав для чтения СМС и отслеживания звонков, среди которых: android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.READ_PHONE_STATE, android.permission.CALL_PHONE, android.permission.SEND_SMS.

Приложение создает задачу, выполняемую каждые 5 секунд, которая будет проверять наличие прав: android.permission.READ_PHONE_NUMBERS и android.permission.READ_PHONE_STATE, а также установку приложения в качестве обработчика. В контексте данной задачи, если права были выданы, поток исполнения переходит к сбору информации о SIM-картах и ее эксфильтрации на управляющий сервер через POST-запрос к URL: hxxps://akokakola[.]com/send-number (подробнее в разделе «HTTP-коммуникация»). Данная задача повторяется до момента первого прохождения проверок и отправки информации о SIM-картах на C2.

Далее приложение проверяет, запущен ли сервис WebSocketService, если нет – запускает его и ожидает от пользователя ввод трек номера и подтверждения путем клика по кнопке.

После ввода пользователем трек номера и нажатия на кнопку, трек номер будет записан в параметры SharedPreferences с именем globalTrackNumber. Далее будет выполнен POST-запрос к серверу по URL-ссылке hxxps://akokakola[.]com/track-nomer, содержащий информацию о трек номере, а также о SIM-картах (подробнее в разделе «HTTP-коммуникация»). В случае успешного ответа от сервера будет отображена активность с анимацией загрузки (Рис. 5).

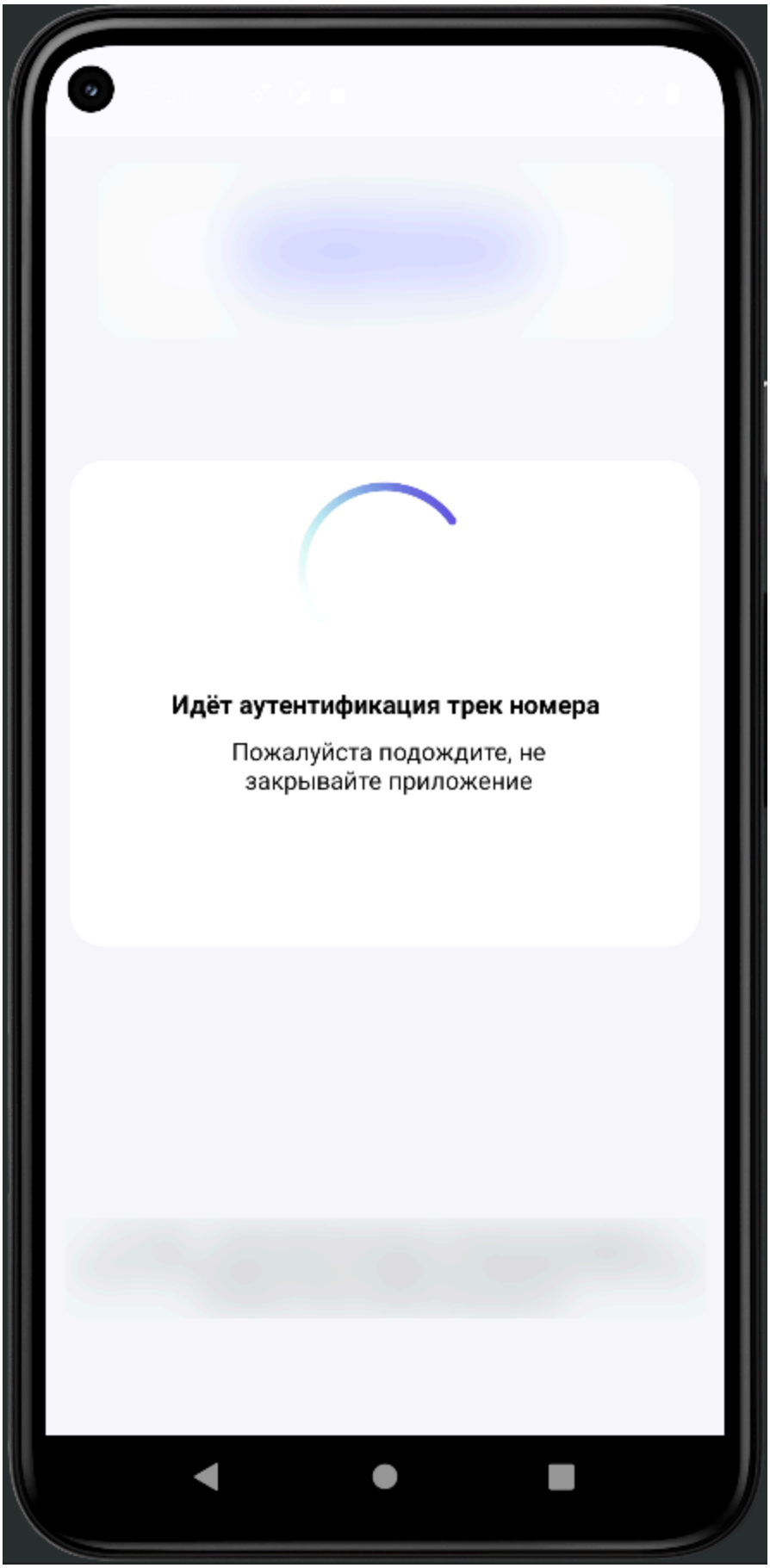
Идёт аутентификация трек номера
Пожалуйста подождите, не закрывайте приложение

Рис. 5 Окно с анимацией загрузки

В ответ от сервера ожидается команда, в зависимости от которой будет отображена следующая активность.

Активности, отображаемые по команде от сервера

Всего существует пять типов отображаемых окон: Card, Custom, Photo, Qr, Text. Логика данных активностей описана далее.

Card

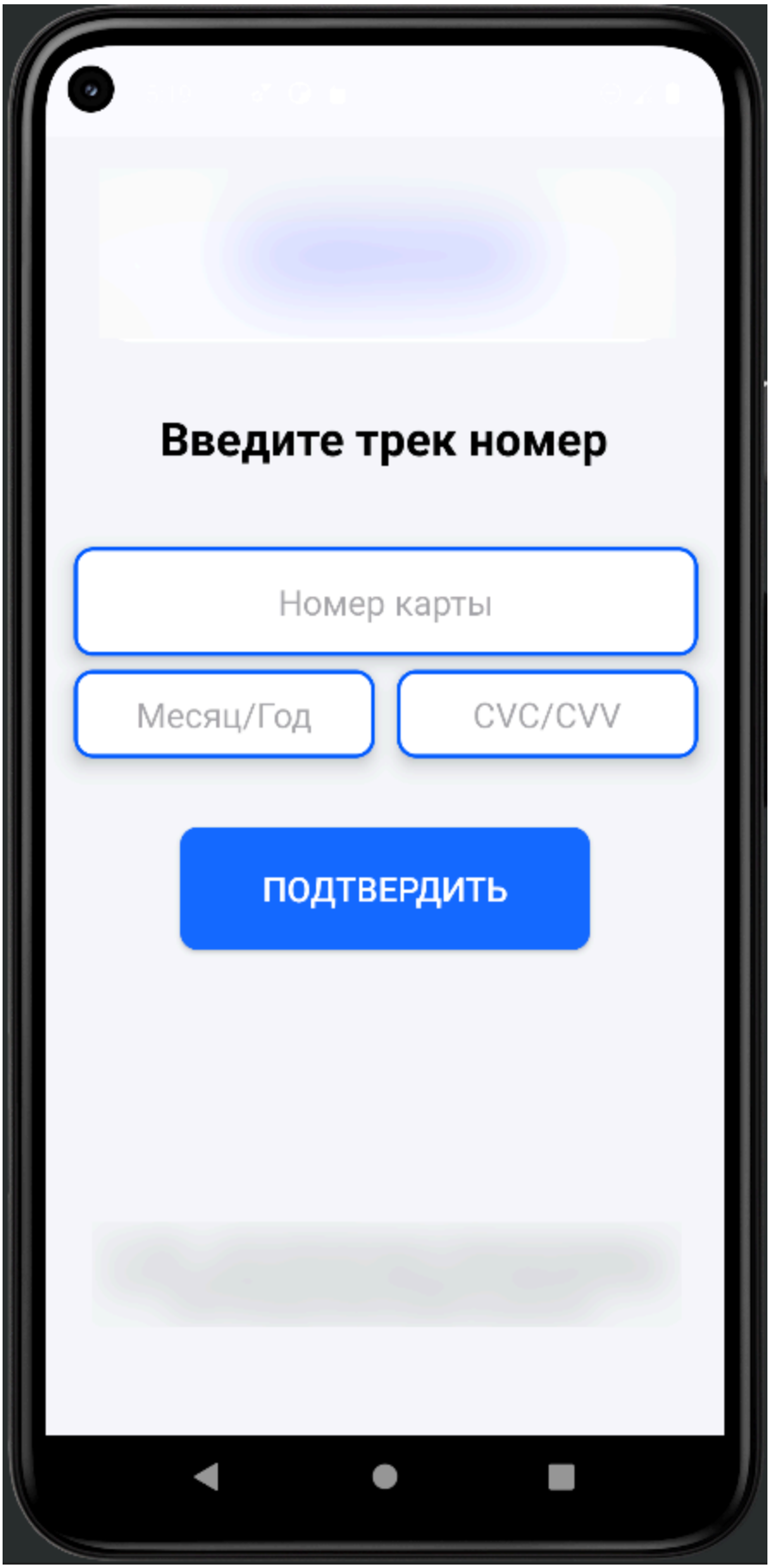
Введите трек номер
Номер карты
Месяц/Год
CVC/CVV
ПОДТВЕРДИТЬ

Рис. 6 Окно с формой ввода информации о банковской карте

Card-активность предназначена для ввода пользователем информации о банковской карте. В данном случае параметром из ответа от командного сервера модерируется текстовое поле, по умолчанию содержащее строку «Введите трек номер». Если пользователь введет данные банковской карты и нажмет кнопку «подтвердить», то ему будет отображена активность с анимацией загрузки, а также будет выполнен POST-запрос к URL-ссылке: hxxps://akokakola[.]com/send-card, содержащий информацию о введенных значениях банковской карты (подробнее в разделе «HTTP-коммуникация»).

Custom

В данном случае доступно три вариации окон в зависимости от количества передаваемых командой модерируемых текстовых полей.

Рис. 7-9 Модерируемые окна с полями ввода информации

Рис. 7-9 Модерируемые окна с полями ввода информации

Рис. 7-9 Модерируемые окна с полями ввода информации

В каждой из активностей модерируются текстовые поля, которые по умолчанию имеют значение «Введите трек номер». Также во всех случаях, после ввода пользователем данных в текстовые поля и клика по кнопке «подтвердить», пользователю будет отображена активность с анимацией загрузки, и будет выполнен POST-запрос к URL-ссылке: hxxps://akokakola[.]com/send-custom, содержащий информацию о введенных значениях в поля (подробнее в разделе «HTTP-коммуникация»).

Photo

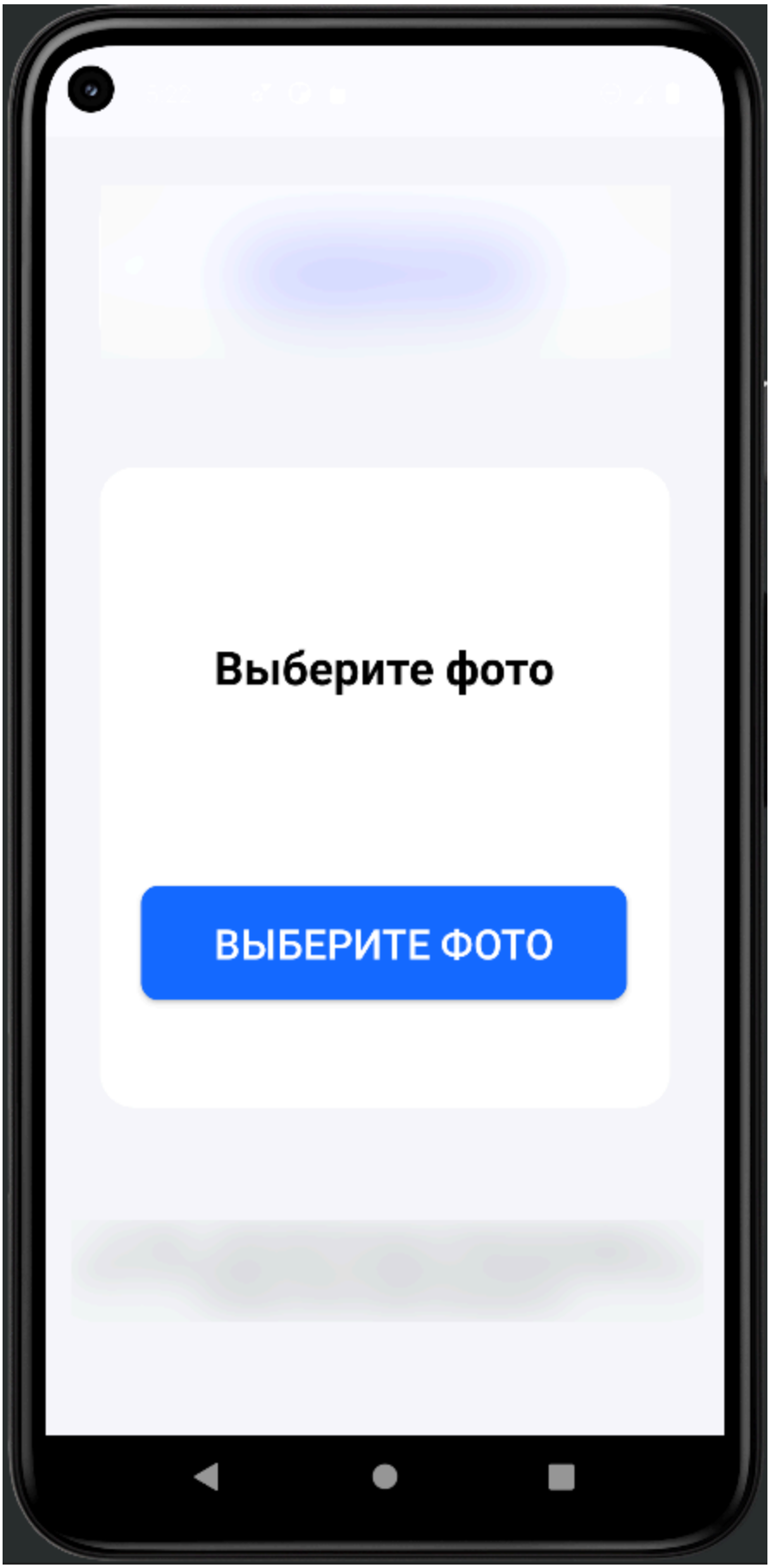
Выберите фото
ВЫБЕРИТЕ ФОТО

Рис. 10 Окно с формой отправки фото

Данная активность предназначена для отправки фотографии и содержит модерируемое текстовое поле параметром команды, которое по умолчанию имеет значение «Выберите фото». После того, как пользователь нажимает кнопку выбора фото, приложение проверяет наличие прав android.permission.READ_EXTERNAL_STORAGE или android.permission.READ_MEDIA_IMAGES, в зависимости от версии SDK, и запрашивает их в случае отсутствия. После выдачи прав и нажатия пользователем кнопки «выберите фото» отображается меню выбора фото из памяти устройства. Когда пользователь выберет фотографию, она будет отправлена на управляющий сервер путем выполнения POST-запроса к URL-ссылке: hxxps://akokakola[.]com/send-photo (подробнее в разделе «HTTP-коммуникация»).

QR

Данная активность предназначена для отображения пользователю QR-кода с двумя модерируемыми полями: текстовое поле, которое по умолчанию содержит значение «Введите трек номер» и путь к изображению QR-кода. Также активность содержит кнопку подтвердить, после нажатия которой будет запущена активность с анимацией загрузки.

Text

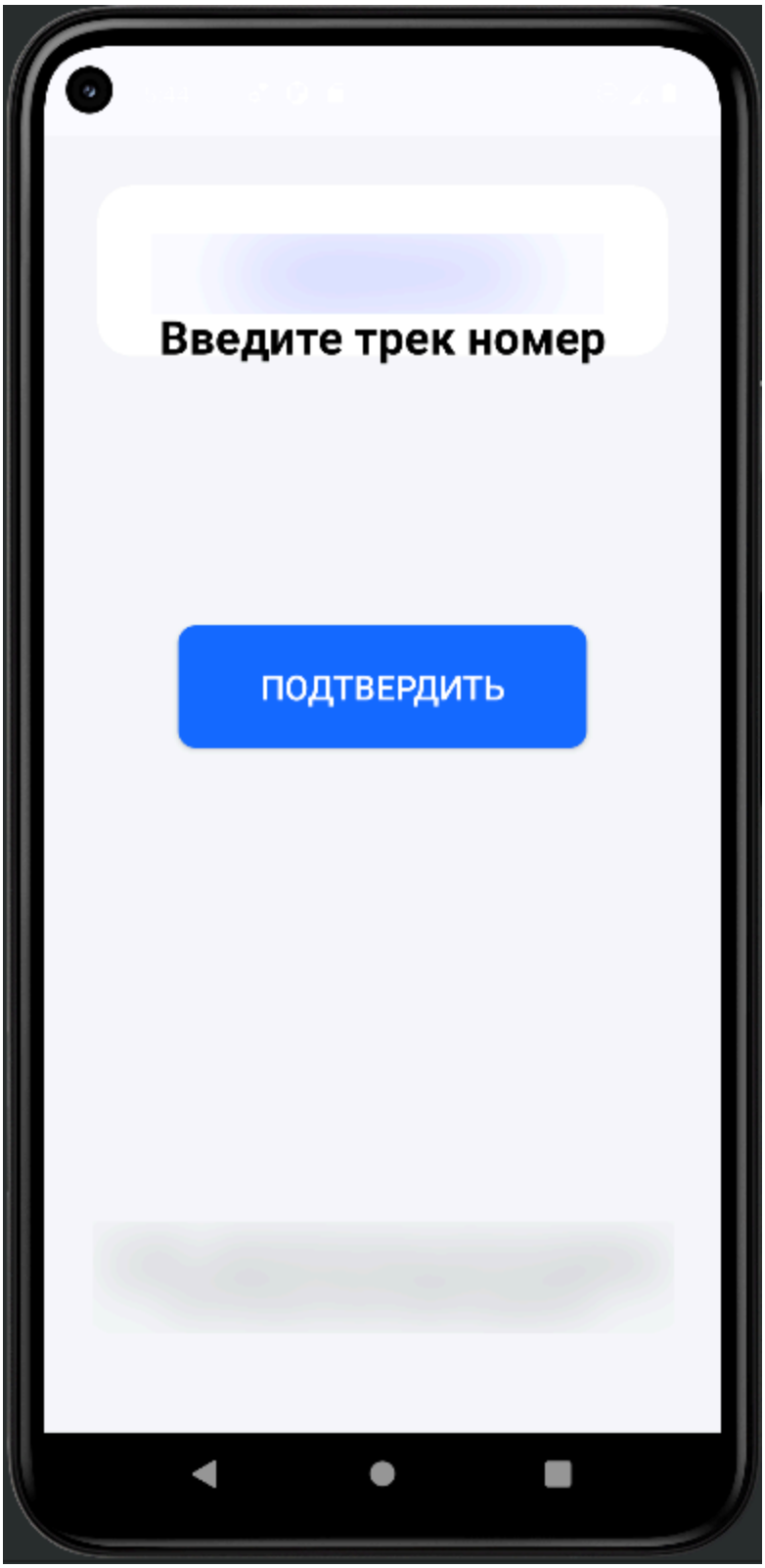

Рис. 11 Окно с отображением произвольного текста

Данная активность предназначена для отображения модерируемого командой от сервера текстового поля, которое по умолчанию имеет значение «Введите трек номер». После нажатия кнопки «подтвердить» отображается активность с анимацией загрузки.

Отслеживание состояния приложения

В большинстве активностей приложения реализованы функциональные возможности для выполнения запросов к серверу на определенных этапах жизненного цикла компонента. Это нужно для оповещения сервера о состоянии, в которое входит приложение. Всего реализовано три запроса:

- /open-app — был выполнен запуск приложения;
- /swap-app — приложение было свернуто;
- /close-app — приложение было выключено.

Подробнее о данных, передаваемых в запросе, в разделе «HTTP-коммуникация».

Режимы работы ВПО

DeliveryRAT v.2 имеет два возможных варианта работы приложения: standart и mini. Значение режима расположено в конфигурационном поле MODE. В случае standart режима будет получен полный набор необходимых прав для приложения, для полноценной поддержки всех функциональных возможностей. В режиме mini активность с предоставлением прав будет пропущена, и будут запрошены права только для установки текущего приложения как обработчика входящих SMS по умолчанию, что ограничивает часть функциональных возможностей ВПО.

NotificationListenerService

В данном ВПО реализован сервис, обрабатывающий полученные PUSH-уведомления. После того, как на устройство было получено уведомление, информация о нем будет отправлена на C2-сервер путем POST-запроса к URL-ссылке: hxxps://akokakola[.]com/send-notification (подробнее в разделе «HTTP-коммуникация»). Затем будет выполнена проверка возможности удаления уведомления, и, если такая возможность есть, уведомление будет скрыто от пользователя.

SmsReceiver

В данном ВПО реализован обработчик входящих SMS. В контексте данного сервиса выполняется сбор информации о полученном сообщении и последующая отправка данной информации путем создания внутреннего события ACTION_NEW_SMS. Обработчик данного события реализован в WebSocketService, и его целью является эксфильтрация полученных SMS через WebSocket-протокол.

BootReceiver

В исследуемом приложении реализован обработчик события загрузки системы, при сработки которого будет выполнен запуск сервиса WebSocketService, использующегося для создания и поддержания коммуникации с C2-сервером через WebSocket-протокол.

Взаимодействие с C2

WebSocketService

В контексте запуска данного сервиса приложение выполняет следующие действия:

- запускает Alarm с периодичностью сработки в 1 минуту для закрепления сервиса;
- создает периодическую задачу, выполняемую каждые 15 минут, для проверки работы сервиса и его запуска, если он отключен;
- инициализирует файл настроек SharedPreferences с именем «MyPrefs»;
- регистрирует обработчик широковещательных сообщений для обработки события «ACTION_NEW_SMS»;
- создает задачу, запускаемую каждые 5 секунд, в контексте которой выполняет сбор SMS, полученных после запуска сервиса, и эксфильтрацию информации о них на C2 сервер с использованием WebSocket-протокола.

Также при первой инициализации будут выполнены следующие действия:

- получает HWID параметра, который имеет значение android_id;
- регистрирует обработчик проверки сети, если сеть пропадает, то отключает подключение, а когда сеть появляется, то выполняет подключение к WebSocket;
- создает закрепленное уведомление с именем «Data Sync»;
- выполняет WebSocket-подключение к серверу.

Также при каждом получении сервисом действия «CHECK_WEBSOCKET», которое вызывается запланированными задачами и Alarm, запущенными при инициализации сервиса, будет выполнена проверка его работы. Если подключение не выполнено, то будет возобновлять его.

WebSocket-коммуникация

При первичном подключении выполняется проверка очереди запланированных сообщений с информацией о полученных SMS на устройство и их поочередная отправка. Шаблон JSON-объекта, отправляемого на сервер:

```
{
  "Data": {
    "message": "{sms_body}", // содержимое SMS
    "sender": "{sender_phone_number}", // номер телефона отправителя
    "messageId": "{sms_timestamp}", // временной слепок
    "dateString": "{sms_formatted_data}", // форматированная дата получения SMS
    "hwid": "{android_id}", // уникальное значение бота — android_id
    "service": "{app_name_service}", // имя приложения
    "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
    "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
    "trackNumber": "{track_number}", // трек номер, введенный пользователем
```

```
    "deviceModel": "{build_model}", // модель устройства
    "androidVersion": "{build_version_release}", // версия Android
    "type": "Новое смс",
    "serviceCenter": "{sms_service_center}", // номер телефона центра
обслуживания SIM
    "operator": "{sim_operator}", // название оператора SIM, на которое было
получено SMS
    "phoneNumber": "{phone_number}" // номер телефона, на который было получено
SMS
  }
}
```

При получении сообщений от сервера будет выполнена обработка команд с передаваемыми параметрами. Шаблон JSON-объекта, который содержит все возможные поля, обрабатываемые вредоносным приложением:

```
{
  "type": "{command_name}",
  "number": "{number}",
  "text": "{text_message}",
  "useAlternativeIcon": "{flag_hide_or_visible_icon}",
  "target": "{ddos_target}",
  "total": "{total_ddos_requests}",
  "concurrency": "{conrurrent_ddos_request}",
  "photo": "{base64_qrcode_bitmap}"
}
```

Ниже представлена таблица с перечнем команд, принимаемыми аргументами и описанием их возможностей.

Команда	**Параметры**	**Описание**
allSmsContact	text	Выполнить отправку сообщения, переданного в команде, на все уникальные номера в списке контактов.
call	number	Выполнить USSD-команду с отправкой информации о команде на C2-сервер POST-запросом к URL-ссылке hxxps://akokakola[.]com/send-ussd.
callTwo	number	Аналогично команде call, за исключением того, что вызов идет со второй SIM в устройстве.
card	text	Запуск активности Card, описанной в разделе «Активности, отображаемые по команде от сервера».
changeIcon	useAlternativeIcon	Смена иконки приложения (стандартная или полностью прозрачная).

contactPermission		Запуск активности, цель которой запрос прав доступа приложения к списку контактов устройства.
custom	text	Запуск активности Custom, описанной в разделе «Активности, отображаемые по команде от сервера».
hide		Скрывает иконку приложения.
oldsms		Выполняет сбор SMS-сообщений с устройства и записывает собранные данные в файл с именем sms_list.txt. Затем выполняет эксфильтрацию этого файла на сервер через POST-запрос к URL-ссылке: hxxps://akokakola[.]com/send-answer (подробнее в разделе «HTTP-коммуникация»).
photo	text	Запуск активности Photo, описанной в разделе «Активности, отображаемые по команде от сервера».
qr	text, photo	Запуск активности Qr, описанной в разделе «Активности, отображаемые по команде от сервера».
sendContactList		Выполняет сбор и эксфильтрацию списка контактов на сервер путем выполнения POST-запроса к URL-ссылке hxxps://akokakola[.]com/send-contact (подробнее в разделе «HTTP-коммуникация»).
show		Отображает иконку приложения.
sms	number, text	Выполняет отправку SMS с указанным содержимым и номером телефона получателя.
smsTwo	number, text	Аналогично команде sms, за исключением того, что SMS будет отправлено со второй SIM.
stress	target, total, concurrency	Выполняет указанное в total количество запросов к URL-адресу указанному в target. Они выполняются одновременно, но с ограничением по числу одновременных запросов, указанному в параметре concurrency. После выполнения команды, выполняет POST-запрос к URL-адресу: hxxps://akokakola[.]com/send-stress с информацией о выполнении задачи (подробнее в разделе «HTTP-коммуникация»).
text	text	Запуск активности Text, описанной в разделе «Активности, отображаемые по команде от сервера».

HTTP-коммуникация

В данном разделе представлены шаблоны данных, передаваемых по результату выполнения POST-запросов.

/send-number

```
{
  "hwid": "{android_id}", // уникальное значение бота — android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "phoneNumber": "{phone_number}", // номер телефона SIM 1
  "operator": "{sim_operator}", // название оператора SIM 1
  "simCount": "{sim_count}", // количество SIM в устройстве
  "phoneNumber2": "{phone_number_2}", // номер телефона SIM 2
  "operator2": "{sim_operator_2}" // название оператора SIM 2
}
```

/track-nomer

```
{
  "trackNomer": "{track_number}", // трек номер, введенный пользователем
  "hwid": "{android_id}", // уникальное значение бота — android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "phoneNumber": "{phone_number}", // номер телефона SIM 1
  "operator": "{sim_operator}", // название оператора SIM 1
  "simCount": "{sim_count}", // количество SIM в устройстве
  "phoneNumber2": "{phone_number_2}", // номер телефона SIM 2
  "operator2": "{sim_operator_2}" // название оператора SIM 2
}
```

В ответ от сервера ожидается объект:

```
{
  "message": "{status}", // ожидается "Track OK"
  "activity": "{activity_name}" // ожидается одна из команд: Card, Custom,
Photo, Qr, Text
}
```

/send-card

```
{
  "hwid": "{android_id}", // уникальное значение бота — android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "cardNumber": "{card_number}", // номер карты, введенный пользователем
```

```
  "expiryDate": "{expiry_date}", // дата истечения срока карты, введенная
пользователем
  "cvv": "{cvv_code}", // CVV-код, введенный пользователем
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "trackNomer": "{track_number}", // трек номер, введенный пользователем
  "customMessageText": "{custom_message_text}" // значение модерируемого
командой текстового поля
}
```

/send-custom

```
{
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "text": "{inputted_text}", // введенный пользователем текст в поля
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "trackNomer": "{track_number}", // трек номер, введенный пользователем
  "customMessageText": "{custom_message_text}" // значение модерируемого
командой текстового поля
}
```

/send-photo

В данном случае выполняется многокомпонентный запрос формы со следующими полями:

- hwid — {android_id} // уникальное значение бота – android_id
- teamId — {threat_actor_team_id} // ID команды операторов ВПО
- service — {app_name_service} // имя приложения
- workerId — {threat_actor_worker_id} // ID оператора ВПО
- trackNomer — {track_number} // трек номер, введенный пользователем
- customMessageText — {custom_message_text} // значение модерируемого командой текстового поля
- file — изображение с именем «photo.jpg»

/send-notification

```
{
  "title": "{notification_title}", // заголовок PUSH-уведомления
  "text": "{notification_text}", // текст PUSH-уведомления
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "packageName": "{notification_app_package_name}",
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
```

```
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "notTime": "{formatted_date}", // дата получения PUSH-уведомления
  "deviceModel": "{build_model}", // модель устройства
  "androidVersion": "{build_version_release}", // версия Android
  "notificationId": "{notification_id}", // ID PUSH-уведомления
  "trackNumber": "{track_number}" // трек номер, введенный пользователем
}
```

/send-ussd

```
{
  "hwid": "{android_id}", // уникальное значение бота — android_id
  "text": "{ussd_respones}", // ответ, полученный в результате выполнения USSD-
команды
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}" // ID оператора ВПО
}
```

/send-contact

```
{
  "hwid": "{android_id}", // уникальное значение бота — android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "trackNomer": "{track_number}", // трек номер, введенный пользователем
  "contacts": [{
    "name": "{contact_name}", // имя контакта
    "number": "{contact_namber}" // номер телефона контакта
  }, ...]
}
```

/send-stress

```
{
  "target": "{target_url}", // целевая URL-ссылка или домен
  "totalRequests": "{total_requests}", // общее количество выполняемых запросов
  "concurrency": "{concurrency_requests}", // количество одновременно
выполняемых запросов
  "success": "{success_requests_count}", // количество успешных запросов
  "failure": "{failure_requests_count}" // количество запросов, завершенных
```

```
с ошибкой
}
```

/send-answer

```
{
  "action": "{action_requests}", // категория события, по которой выполняется
отчетность
  "message": "{action_message}", // содержимое сообщения
  "status": "{action_status}", // success или error
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}" // ID оператора ВПО
}
```

Найденные сопоставления action и message:

- «sms» — «Отправлено {count} SMS»
- «sms» — «Произошла ошибка при массовой отправке SMS: {exception}»
- «changeIcon» — «Стандартная иконка восстановлена»
- «changeIcon» — «Прозрачная иконка активирована»
- «hide» — «Иконка приложения скрыта»
- «ussd» — «Разрешение CALL_PHONE не предоставлено. Не удалось выполнить USSD-код {ussd_code}»
- «ussd» — «Вторая SIM не найдена или не активна. Не удалось выполнить USSD-код {ussd_code}»
- «ussd» — «Не удалось выполнить USSD-код {ussd_code}. Код ошибки: {failure_code}»
- «ussd» — «USSD-код {ussd_code} успешно выполнен, ответ: {ussd_response}»
- «sms» — «SMS отправлено на номер {phone_number}»
- «sms» — «Не удалось отправить SMS на номер {phone_number}: {error}»
- «sms» — «Вторая SIM не найдена или не активна. Не удалось отправить SMS на номер {phone_number}»
- «sms» — «SMS отправлено на номер {phone_number} с использованием второй SIM»
- «sms» — «Разрешение SEND_SMS не предоставлено. Не удалось отправить SMS на номер {phone_number} с использованием второй SIM»
- «sms» — «Не удалось отправить SMS на номер {phone_number} с использованием второй SIM: {error}»
- «sendOld» — «Удалось получить файл с смс»
- «sendOld» — «Не удалось получить файл с смс «
- «show» — «Иконка приложения отображена»
- «custom» — «Пользовательская активность запущена с сообщением: {custom_message}»
- «custom» — «Запрос разрешения контактов доставлен»

/open-app

```
{
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "deviceModel": "{build_model}", // модель устройства
  "androidVersion": "{build_version_release}", // версия Android
  "sdkVersion": "{build_version_sdk_int}", // версия SDK устройства
  "versionName": "{app_version_name}", // версия приложения
  "installedApps": "{installed_apps}", // список установленных приложений
  "ipAddress": "{local_ip_address}", // IP-адрес устройства
  "mail": "{config_mail}", // false в анализируемом семпле
  "mod": "{config_mod}" // standart или mini в зависимости от режима работы
приложения
}
```

/swap-app и **/close-app**

```
{
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "service": "{app_name_service}", // имя приложения
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "workerId": "{threat_actor_worker_id}" // ID оператора ВПО
}
```

Дополнительная информация

Чат с поддержкой

В анализируемом приложении были найдены функциональные возможности для реализации чата, который имитирует чат с поддержкой. Вход в данный чат пользователю должен быть доступен по плавающей кнопке в каждой активности. Однако в анализируемом приложении данная кнопка скрыта от пользователя, что говорит либо о том, что это было выключено в сборщике ВПО, либо о том, что данные функциональные возможности на текущий момент находятся в разработке. После того, как пользователь нажмет на кнопку, будет отображен чат, где реализуется отправка и получение сообщений.

Если пользователь выполняет отправку сообщения, будет выполнен POST-запрос к URL-адресу hxxps://akokakola[.]com/sendMessage с передаваемым JSON-объектом. Шаблон JSON-объекта:

```
{
  "text": "{message_body}", // содержимое сообщения
```

```
  "hwid": "{android_id}", // уникальное значение бота – android_id
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "time": "{current time}", // время отправки сообщения
  "timezone": "{device_timezone}", // временная зона
  "track": "{track_number}", // трек номер, введенный пользователем
  "service": "{app_name_service}", // имя приложения
  "id": "{message_counter}", // ID сообщения
}
```

Для добавления сообщений со стороны сервера, ВПО выполняет GET-запросы к URL-адресу hxxps://akokakola[.]com/getMessages с передаваемыми GET-параметрами «hwid» и «teamId».

Конфигурационное поле Mail

Также в конфигурации приложения присутствует поле Mail, однако нами не было найдено применение данного флага для изменения поведения приложения или добавления каких-либо функциональных возможностей. Был только обнаружен факт отправки информации о состоянии данного поля на C2-сервер при выполнении запроса к /open-app. Предположительно, данное поле влияет на поведение со стороны сервера.

Измененный вариант

Нами была обнаружена измененная вариация данного трояна, мимикрирующая под несуществующий сервис возврата средств. В данном случае, вместо ввода трек номера у пользователя запрашивали ввести код возврата, после чего вместо окна загрузки, отображалась форма для ввода суммы возврата, номера телефона и банковской карты.

Рис. 12-13 Окна формы запроса номера телефона и банковской карты

Рис. 12-13 Окна формы запроса номера телефона и банковской карты

После того, как пользователь введет данные и нажмет на кнопку оформить возврат, будет отображена активность загрузки, а также выполнен POST-запрос на C2-сервер с gateway: /user-info и JSON-объектом вида:

```
{
  "summa": "{entered_sum_to_return}", // сумма возврата, введенная
пользователем
  "phoneNumber": "{phone_number}", // номер телефона, введенный пользователем
  "cardNumber": "{card_number}", // номер карты, введенный пользователем
  "hwid": "{android_id}", // уникальное значение бота – android_id
```

```
  "workerId": "{threat_actor_worker_id}", // ID оператора ВПО
  "teamId": "{threat_actor_team_id}", // ID команды операторов ВПО
  "service": "{app_name_service}" // имя приложения
}
```

Вывод

DeliveryRAT продолжает атаковать цели в России, активизировавшись с середины 2024 года. Данное вредоносное ПО обновляется и пополняет набор своих функциональных возможностей, несущих новые риски для пользователей Android-устройств в России. Так мы фиксируем, что стратегии по краже средств дополнились.

Помимо базовых функций, таких как кража содержания SMS и уведомлений, троян теперь может отображать заранее подготовленные варианты диалоговых окон с возможностью похищения фотографий, загружаемых пользователем, ввода данных банковской карты и так далее.

Кроме того, DeliveryRAT получил отличающиеся от стилера возможности для выполнения DDoS-атак, что позволяет использовать этот троян не только для финансовой выгоды, но и для проведения массовых атак на инфраструктуру организаций с целью нарушения их работы.

Индикаторы компрометации

Образцы ВПО DeliveryRAT

—

- 42ce4d0c3d373220d3a5c8c52579daa4
- a3261679ea0625be3ef7f8290984d35c3763fdf7
- c64eb9cc28335f000e61f5e2afa97b30e43dd8852e41edc30b4ec02684b81e5a

—

- 6ddf16c6893c30cd440403aaf416b632
- 744038673da11d2e52d32528503419d0de336d11
- 3a0284bef748a7d875d1ae3b3f53c8e8e63eecb485d5da6c60965a52ac69a1e8

Work.apk

- 88b2d2a02104ba370f12685738a42ab6
- 4e00aa31cc468ce4b66e73276d385af16f8b808a
- e26ad1588ba12005cfaf8d0ed006dc5ad2aefe92256e29a71a7abbb6636c4101

vozvrat.apk

- 0110b0a0cd20abe6e9c00829d1d92729

- affb560410fc3f08e77b6e0bc7ff1cb7dab2a575
- a7af4506f6adc3a7698df8b55056749ec2ba258761d3aee7a3aa735339a1d152

Загрузчики

domopult.apk

- f33ee079a1388b89b04fab6ce60198a5
- d1fb8ea2063e6d15e7d30384aeef43e7b7b5b1c6
- 2c897d0d43469381e4cab57a4ee33b862c16be4234524e013319a91224b5ef21

gosu.apk

- 19be4a6693579727a66439c45d9ce99e
- 0ac299edbe72a89a94787c3b379de803664d4f11
- a0e762f936312d7ac933c011e12fe2deb7f88ba63b6b80a188fa54178c6653f8

C2-сервер

- akokakola[.]com
- apiepi03[.]com
- apiepi01[.]com
- apiscoles[.]com
- apistorus[.]com
- apispawns[.]com
- apikosla[.]com
- kokospoki[.]com
- apiskasla[.]com
- keycardapi[.]com
- apistorus[.]com
- apitest[.]sbs
- i57038i[.]live
- shvuor[.]com

Gateway-пути

- /send-notification
- /close-app
- /notofication-app
- /open-app
- /send-card
- /send-custom
- /send-number
- /send-permission

- /send-photo
- /send-read
- /sms-app
- /socket
- /swap-app
- /track-nomer
- /getMessages
- /send-answer
- /send-contact
- /send-stress
- /send-ussd
- /sendMessage
- /user-info