

Mamont вышел на охоту: разбираем новую версию Android-трояна

f6.ru/blog/mamont-rat

December 22, 2025

Как работает «Мамонт» с вредоносными

F6

Вредоносное Android-приложение **Mamont** в 2025 году стало одной из главных угроз для клиентов ведущих российских банков. По [данным](#) МВД России, во второй половине 2025-го на Mamont пришлось **38,7%** случаев заражений мобильных устройств, на «обратную» версию NFCGate – **52,4%**.

Аналитики департамента противодействия финансовому мошенничеству (Fraud Protection) компании **F6** отмечают, что по итогам 2025 года Mamont выходит на первое место в сравнении с NFCGate по количеству скомпрометированных устройств и ущербу для пользователей.

По данным F6, в третьем квартале 2025 года число устройств, на которые пользователи в России устанавливали Mamont под видом полезных приложений, увеличивалось в среднем на **60** в день. Средняя сумма списания в результате успешной мошеннической атаки за этот период составила около **30 тыс.** рублей. Общий ущерб от использования Mamont против клиентов российских банков только в ноябре 2025 года может превышать **150 млн.** рублей.

NFCGate и Mamont – представители разных путей эволюции. NFCGate создали как [легитимное приложение](#), на основе которого злоумышленники позже разработали семейство вредоносных версий. Mamont изначально разрабатывали как ПО с киберпреступными целями.

Первые экземпляры этого вируса специалисты нашей компании [обнаружили](#) в сентябре 2023 года. Одна из преступных групп, работавших по схеме «Мамонт», начала использовать в своих атаках Android-троян. Его замаскировали под приложение для оформления доставки товаров и распространялся через фейковый Google Play. Статистика атак с применением трояна говорила об эффективности мошеннической схемы: всего за десять дней сентября 2023-го с помощью этого ВПО злоумышленники похитили у пользователей почти **3 млн.** рублей, средняя сумма списания составляла примерно **67 тыс.** рублей.

За два года вредоносный функционал Mamont серьёзно изменился, а киберпреступники автоматизировали процессы эксплуатации атаки.

По сравнению с первой версией двухлетней давности Mamont образца декабря 2025 года по техническим возможностям ушёл далеко вперёд. В результате модернизации вредоносного приложения злоумышленники увеличили перечень атакуемых приложений пользователя, усовершенствовали функционал обработки перехваченных СМС и управления устройствами жертв, поставив атаки на пользователей Android-устройств на поток. Аналитики F6 разобрали последнюю версию ВПО, исследовали инфраструктуру злоумышленников и подготовили рекомендации по защите от Mamont для банков и пользователей.

Как распространяют Mamont

На момент появления ВПО схема атаки с использованием Android-трояна выглядела следующим образом.

Как работает «Мамонт» с вредоносными

F6

Рисунок 1. Схема атаки с использованием Mamont образца 2023 года

Позже мошенники упростили схему распространения ВПО и в 2025 году заражают устройство жертвы с использованием прямой фишинговой рассылки вредоносного файла без публикации в магазинах приложений. Атака чаще нацелена на открытые группы в популярных мессенджерах – такие как домовые чаты. Также для распространения фишинговых ссылок и вредоносных файлов через мессенджеры и СМС мошенники используют скомпрометированные устройства.

Изм.

Чаты



Поиск

Укажите свой день рождения! 🎂

Контакты будут знать, когда Вас поздравить.



✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

✓ 22:59

Привет, это не твой знакомый об фуру разбился?

1

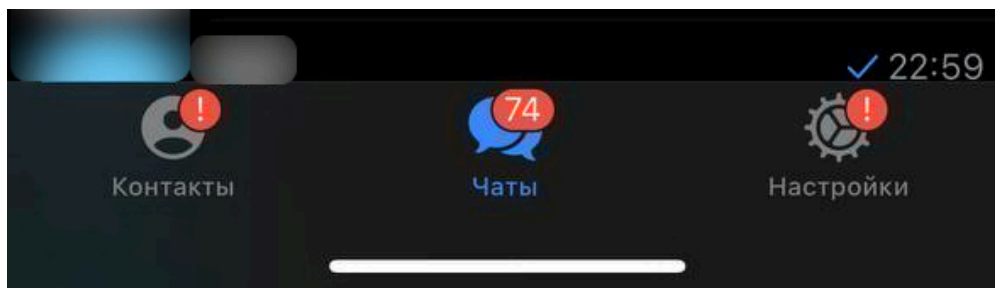


Рисунок 2. Массовая рассылка Mamont с зараженного устройства

Анализ каналов разработчиков вредоносного приложения показывает, что функционал Mamont активно дорабатывается и продолжит модернизироваться:

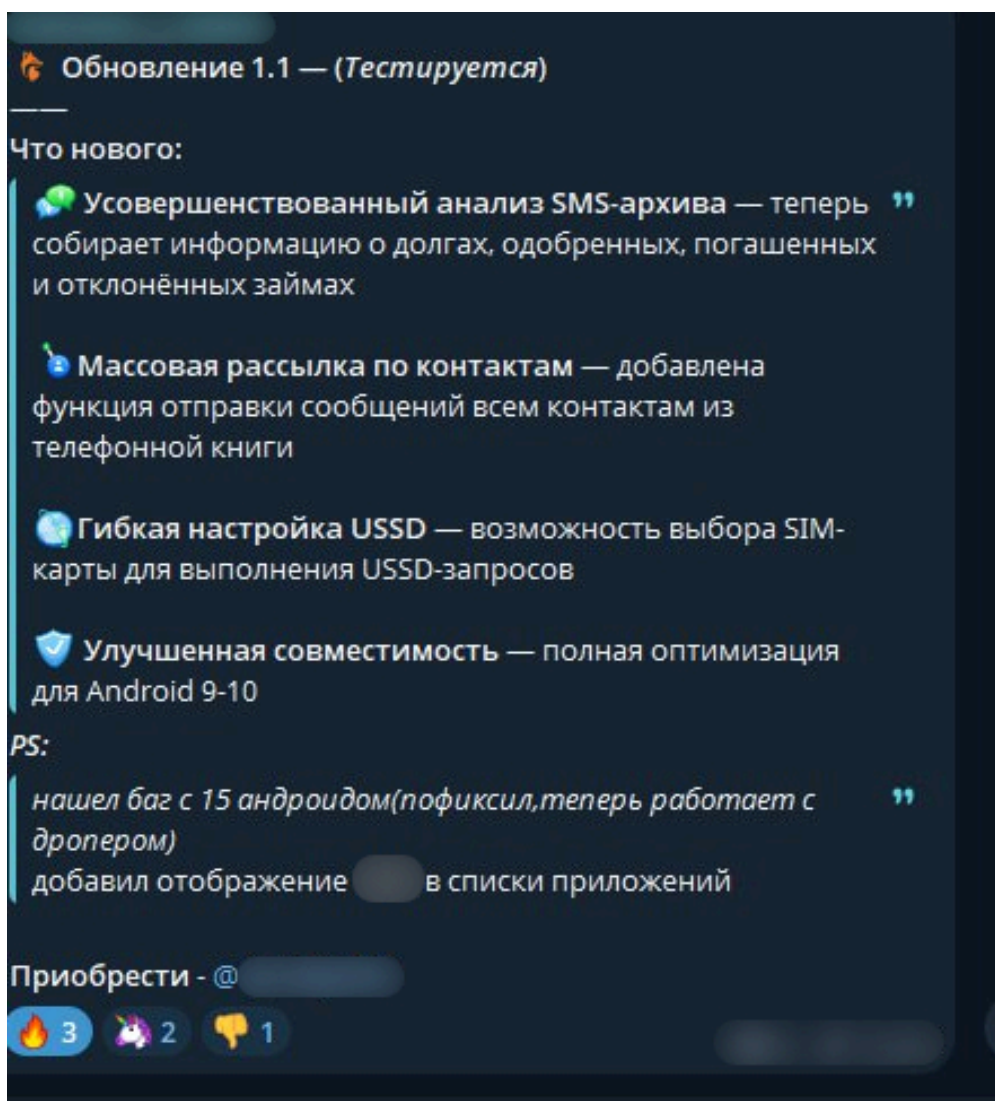


Рисунок 3. Сообщение из канала разработчиков Mamont

Сам вирус распространяется под видом папок фото и видео, списков погибших, раненых и пленных участников СВО, антивирусов и под другими масками. Например:

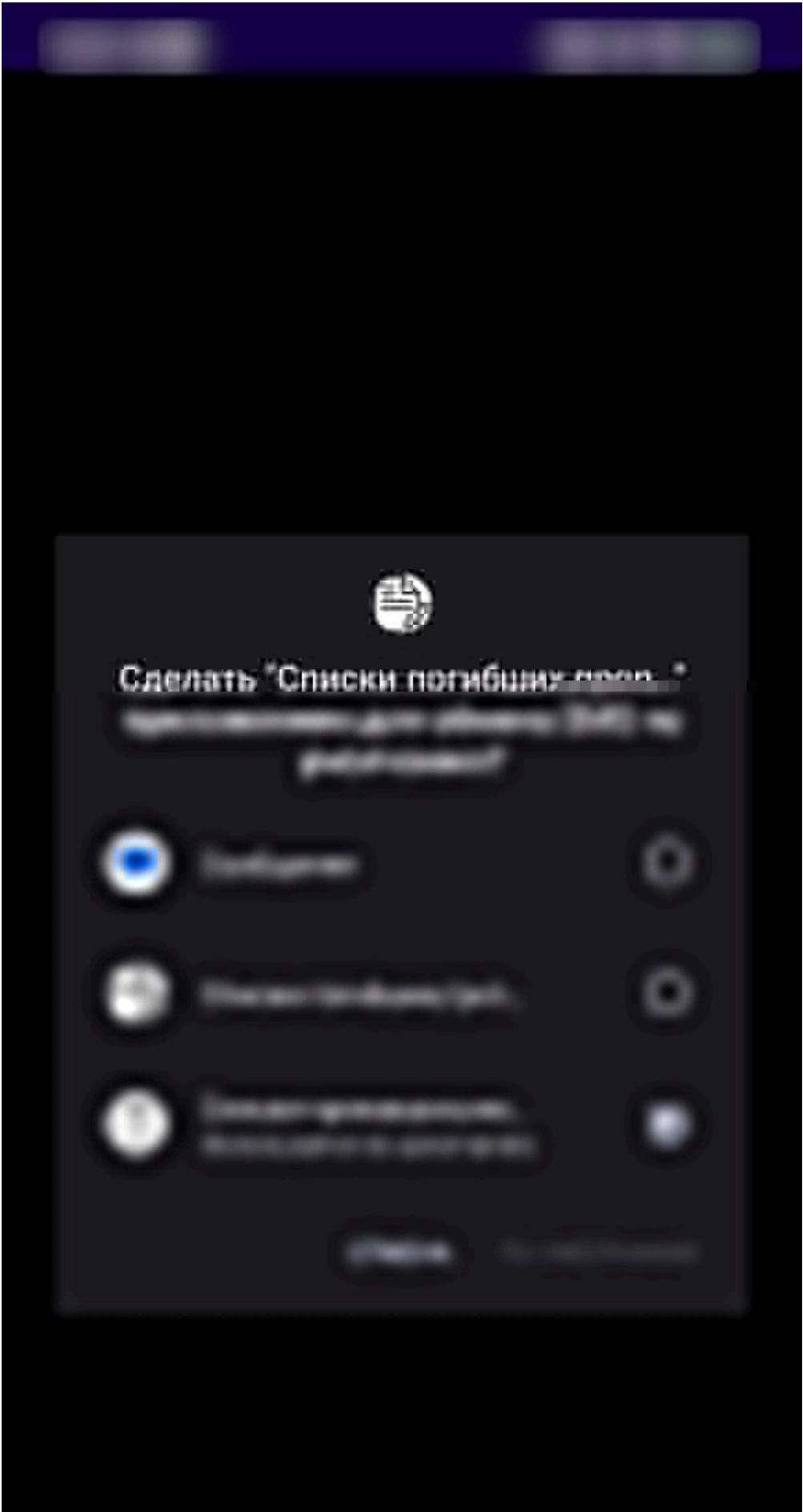
- [Название популярного поискового сервиса]Photo;
- ФОТО;

- Списки 200-300;
- Списки пропавших, пленных;
- Фото_СтРашной_аварии;
- [Название известного банка]-Антивирус;
- МоеВидео.

Процесс исполнения

Сразу после установки вредоносного ПО происходит запрос опасного разрешения на установку приложения в качестве основного приложения для обмена СМС по умолчанию. Это разрешение требуется вредоносу для дальнейшей работы с СМС на устройстве жертвы.

Рисунок 4. Запрос на установку приложения в качестве основного для обмена СМС



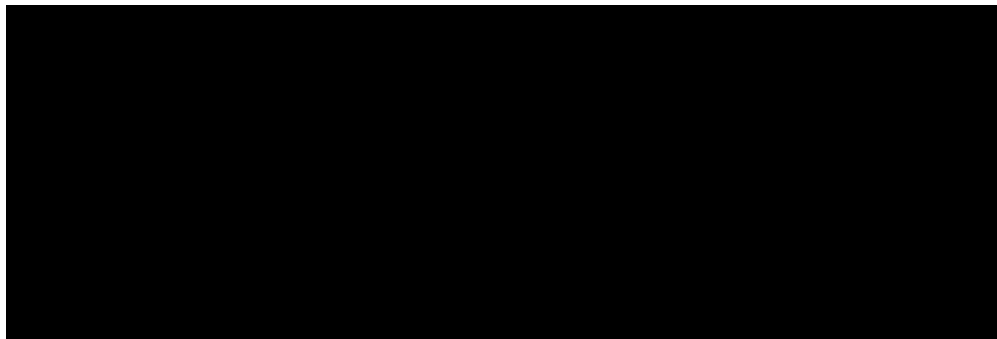


Рисунок 5. Окно получения разрешений SMS для ВПО, которое распространяется под видом приложения «Списки погибших, пропавших»

После получения запрашиваемых разрешений приложение закрывается, а в меню уведомлений появляется постоянное уведомление, оповещающее о наличии обновлений. Пользователь не может убрать оповещение, а при нажатии на него происходит переход на легитимную страницу известного веб-сервиса. Именно постоянное наличие этого оповещения позволяет вредоносному приложению постоянно работать в фоновом режиме и не завершать свою работу автоматически.

[REDACTED]

Рисунок 6. Уведомление, позволяющее вредоносному приложению работать в фоновом режиме

Функционал ВПО

В результате исследования представленного образца вредоносного приложения удалось обнаружить следующий функционал:

- перехват СМС;
- выгрузка архива СМС;
- поиск приложений банков и финансовых организаций на устройстве;
- сбор информации о SIM-картах;
- отправка USSD-запросов;
- рассылка СМС.

Алгоритм работы образца ВПО выстроен следующим образом.

Сразу после запуска исследуемый образец Mamont производит отправку сообщения злоумышленникам об успешном запуске и подключении устройства. В инициализационном сообщении присутствуют такие данные, как:

- ID (идентификатор устройства);
- воркер (злоумышленник-оператор ВПО);
- приложение (название приложения ВПО);
- версия Android;
- найденные на устройстве приложения;
- номера SIM-карт устройства.

Как можно заметить, исследуемый образец ВПО также умеет производить поиск приложений на устройстве. Оно перебирает все установленные приложения и ищет среди них приложения:

- мессенджеров;

- социальных сетей;
- банков;
- микрофинансовых организаций;
- маркетплейсов.

Из найденной информации формируется соответствующее сообщение для дальнейшей отправки злоумышленникам.

Рисунок 7. Формирование инициализационного сообщения злоумышленников

Зачастую злоумышленники выбирают отличные от классического взаимодействия по HTTP способы обмена данными между вредоносным приложением на устройстве жертвы и панелью управления. В нашем случае таким способом стало использование Telegram Bot и отправка данных боту через Telegram Bot API. Ниже представлен интерфейс взаимодействия с Telegram Bot API, реализованный в образце вредоносного ПО, где также можно заметить токен Telegram Bot.

Рисунок 8. Интерфейс взаимодействия с Telegram Bot API

При анализе работы образца вредоносного приложения с Telegram Bot API мы видим, что в образце присутствует возможность работы с такими API Telegram-бота, как:

- */getUpdates*
- */sendDocument*
- */sendMessage*

Рисунок 9. API Telegram-бота

Параллельно с запуском инициализационного сообщения ВПО производит запуск фонового сервиса, цель которого – поддержание соединения с Telegram-ботом для получения команд и их исполнение.

Получение команд через Telegram-бот производится с помощью метода Telegram Bot API “getUpdates”, который возвращает в качестве ответа команду пользователя.

Рисунок 10. Синхронизация с Telegram-ботом

В образце можно обнаружить перечень команд, обрабатываемых образцом Mamont:

- */online*
- */hidemsg*

- `/showmsg`
- `/getallsms`
- `/send`
- `/check`
- `/close`
- `/ussd`
- `/comment`
- `/spamallcontact` — отправить SMS всем контактам на устройстве.

Рассмотрим отдельно каждую из них.

Команда `/showmsg` выставляет вышеупомянутый флаг «*is_listen_sms*», тем самым позволяя сервису приложения читать СМС и ретранслировать их злоумышленникам. В результате выполнения команды злоумышленникам отправляется сообщение об успешном запуске этой функции.

Рисунок 11. Обработка команды `/showmsg`

Рисунок 12. Формирование сообщения о получении нового СМС

Команда `/hidemsg` совершает обратные действия, выставляя флаг в значение «*false*», тем самым останавливая перехват СМС в реальном времени.

Рисунок 13. Обработка команды `/hidemsg`

Команда `/getallsms` совершает отправку архива всех найденных на устройстве СМС с помощью выполнения метода `exportAllSMS`.

Рисунок 14. Метод экспорта СМС с устройства жертвы

Данный метод совершает перебор всех СМС на устройстве, объединяя их в одну строку, которая затем и возвращается в качестве результата выполнения.

В классе `SMSUtils`, частью которого является метод `exportAllSMS`, также присутствует функция для сохранения полученной строки в файл.

Рисунок 15. Сохранение СМС в файл

В дальнейшем, получившийся файл отправляется злоумышленниками в Telegram-бот с помощью метода Telegram API `sendDocument`.

Рисунок 16. Отправка файла с СМС в Telegram Bot

Команда */spamallcontact* производит рассылку всем контактам телефонной книги на устройстве жертвы. Таким образом, отправляя данную команду, злоумышленники могут, например, производить дальнейшее распространение ВПО.

Рисунки 17-18. Обработка команды */spamallcontact*

Рисунки 17-18. Обработка команды */spamallcontact*

Кроме возможности массовой рассылки сообщений, злоумышленники могут отправить СМС и точно, командой */send*, получив оповещение об ошибке, либо об успешной отправке сообщения.

Рисунок 19. Обработка команды */send*

Команда */ussd* производит отправку USSD-кода с устройства жертвы, а результат выполнения отправляет в Telegram-bot.

Рисунок 20. Обработка команды */ussd*

Также есть команды, завершающие работу приложения (*/close*), проверяющие статус устройств (*/online*) и состояние устройства (*/check*).

Таким образом, основной функционал вредоносных приложений Mamont заточен именно на работу с СМС для получения возможности чтения ОТР-кодов.

Инфраструктура злоумышленников

Инфраструктура злоумышленников представлена Telegram-ботом, в который ВПО отправляет сообщения, а также несколькими Telegram-чатами, из которых выполняется координация атак, отправка команд, получение сообщений от бота.

Telegram-бот предоставляет полное описание команд для управления вредоносными приложениями:

/online — юзеры в сети;

/hidemsg — остановка прослушки;

/showmsg — старт перехвата СМС;

/getallsms — получить все СМС с устройства;

/send — отправить сообщение с одного телефона на другой;

/check — выполнить проверку состояния;

/close — завершить работу приложения / устройства;

/ussd — выполнить USSD-запрос с выбранной SIM;

/comment — добавить комментарий;

/spamallcontact — отправить SMS всем контактам на устройстве.

Рисунок 21: Команды Telegram-бота для работы с устройствами жертв

При вызове команды по получению всех СМС также проводится краткий контекстный анализ содержимого всех сообщений, позволяющий злоумышленникам оценить примерный баланс счетов жертвы, наличие кредитов, а также наличие паролей в СМС.

Рисунок 22-24. Примеры сообщений с выгрузками СМС с устройств жертв и их кратким контекстным анализом

Рисунок 22-24. Примеры сообщений с выгрузками СМС с устройств жертв и их кратким контекстным анализом

Рисунок 22-24. Примеры сообщений с выгрузками СМС с устройств жертв и их кратким контекстным анализом

В логах с устройств жертв достаточно большое количество номеров телефонов не было определено — на такой случай злоумышленники активно используют функционал отправки USSD.

Рисунок 25. Отправка команды */ussd* и получение результата

Команда */online* позволяет просмотреть подключенные в данный момент устройства, формат ответа выглядит следующим образом.

Пример ранее рассмотренного инициализационного сообщения выглядит следующим образом.

Рисунок 26. Отправка команды */online* и получение результата

Рисунок 27. Инициализационное сообщение

Получив номер телефона жертвы, злоумышленники проводят активное исследование ее личности, производят поиск персональных данных в открытых данных и утечках информации через специализированные сервисы.

Рисунок 28. Пример поиска персональных данных о жертве в утечках информации

Чаще всего, полученной информации (персональные данные из утечек информации, номер телефона, перехват СМС на устройстве) злоумышленникам достаточно для выполнения незаконных финансовых операций — входа в личный кабинет банков, микрокредитных

и микрофинансовых организаций, незаконных переводов средств, получения кредитов и займов.

С получением номера телефона пользователя и возможности отправки СМС с его устройства преступники производят дальнейшее распространение вредоносных файлов через встроенный функционал ВПО – рассылают сообщения с ВПО всем контактам жертвы.

Рисунки 29-30. Пример массовой рассылки сообщений

Рисунки 29-30. Пример массовой рассылки сообщений

Рисунок 31. Пример провокационного сообщения

Для большей вероятности запуска вредоносного файла получателями используются провокационные сообщения.

Рисунок 31. Пример провокационного сообщения

Перехваченные в реальном времени сообщения выглядят следующим образом.

В чате злоумышленников также обнаружено объявление о продаже / аренде панели управления (Telegram-бота), из которого известна цена ВПО:

Рисунок 32. Пример перехваченного в реальном времени сообщения

— **300 USD** – стоимость ежемесячной аренды;

— **250 USD + 15%** от прибыли злоумышленников – стоимость продажи + дальнейшей поддержки.

Рисунок 33. Объявление о продаже панели управления Mamont

Анализ чата злоумышленников позволил выяснить, как координируются действия внутри преступной команды: присутствуют внутренние правила, распределение обязанностей, приоритеты микрофинансовых организаций, где берутся займы на жертв.

Рисунки 34-35. Организация процесса работы группы злоумышленников

Рисунки 34-35. Организация процесса работы группы злоумышленников

Итоговые выплаты участникам преступной группы производятся на криптовалютные счета.

Рисунок 36. Сообщение о начислении средств участнику криминальной группы

Также из переписки можно сделать вывод о способе генерации вредоносных APK-файлов: они создаются автоматически с помощью билдера на основе еще одного Telegram-бота.

Рисунок 37. Фрагмент переписки из чата злоумышленников

Опасность Mamont, помимо широких возможностей приложения, заключается в относительно невысокой стоимости панели управления и сборки ВПО, простота его использования и отсутствия необходимости владения техническими навыками. Всё это в совокупности приводит к достаточно низкому порогу входа в мошеннические группы, что привлекает к использованию Mamont большое количество криминальных групп. Как следствие, Mamont на сегодня – одно из наиболее популярных на сегодня вредоносных Android-приложений.

Как защититься от Mamont

Рекомендации специалистов F6 для пользователей

- Для защиты своего устройства от трояна Mamont важно знать: все известные образцы ВПО запрашивают роль приложения для обмена СМС по умолчанию. Если приложение при установке запросило такое разрешение, это может быть признаком вредоносной программы.
- **Не общайтесь** в мессенджерах с неизвестными, кем бы они ни представлялись: сотрудниками банков, операторов почтовой и сотовой связи, госсервисов или коммунальных служб.
- **Не переходите** по ссылкам из СМС и сообщений в мессенджерах, даже если внешне они похожи на сообщения от банков и других официальных структур.
- **Не устанавливайте** приложения по рекомендациям незнакомцев, по ссылкам из СМС, сообщений в мессенджерах, писем и подозрительных сайтов.
- Если вам предлагают установить или обновить приложение банка и присылают ссылку, позвоните на горячую линию, указанную на официальном сайте банка, и уточните, действительно ли полученное вами предложение исходит от банка.
- **Не сообщайте посторонним** CVV и ПИН-коды банковских карт, логины и пароли для входа в онлайн-банк. **Не вводите эти данные** на незнакомых, подозрительных сайтах и в приложениях, которые устанавливаете впервые.
- Если вы понимаете, что ваша банковская карта скомпрометирована, сразу же заблокируйте её, позвонив на горячую линию банка, или с использованием банковского приложения.
- **Не удаляйте** банковские приложения из телефона по запросу третьих лиц. Банковские приложения имеют встроенную защиту от мошеннических атак и могут защитить вас от действий преступников.

- Обращайте особое внимание на разрешения, которые запрашивают приложения. Не предоставляйте разрешения, если не понимаете, зачем оно требуется. *Например, если приложение для заказа пиццы просит дать ему разрешения для чтения контактов и отправки СМС – это сигнал тревоги.*

Рекомендации специалистов F6 для подразделений информационной безопасности банков

- Учитывать данные геолокации пользователей.
- При использовании СМС для отправки OTP-кода реализовать механизмы проверки приложения, принимающего СМС на устройстве пользователя.
- Реализовать дополнительные меры защиты на устройстве пользователя по выявлению сторонних вредоносных приложений.

Защититься от подобных операций банкам помогают антифрод-решения с анализом сессионных и поведенческих данных, а также новые технологии выявления подозрительной активности, способные анализировать как отправителя, так и получателя платежа.

Например, для оценки риска транзакции и проверки получателя (KYC – know your customer) модули решения [F6 Fraud Protection](#) могут реализовать сбор и обмен как кросс-канальными сессионными данными, в том числе идентификаторов устройств, параметров сетевого подключения, индикаторов компрометации, так и обезличенных персональных и транзакционных данных в режиме реального времени.

Индикаторы компрометации

Filename: Vid_182873092MP.apk

MD5: 4351a35613a06a10aa8c2f1b1e87edc2

SHA-1: 7d339584cf2ca20f86a273662158f87cd6e15488

SHA-256: 4a47f9c49216075c6e0c9d64b2ba110ca19816fa86cb43afe9ccb941f75305a0

Filename: YandexPhoto.apk

MD5: 794cec7f06fe67c71adc87df4c739570

SHA-1: 0a3f29dc2cb6d970f836b8fbda4b976a043f4099

SHA-256: 46da5fd63012361685563a919039444929bd0e6ad1f73e36b4a7ddf39625f71b

Filename: Фото_СтРашной_аварии.apk

MD5: 1fe7a3395c6e57bbef7ab8c663b0cebc

SHA-1: eca344e9a489eb7cd15ceb78568fcc69ced17e89

SHA-256: 775aa4a163ae291a8b83ed25c6ce079ec7d1797c9411f2de181e902ac7bc910d

© 2003 – 2025 F6 — российский разработчик технологий для борьбы с киберпреступлениями.