УДК 004.056.55

Автаев Максим Сергеевич
студент
Российский технологический университет
Россия, г. Москва
e-mail: avtaev2max@gmail.com

АНАЛИЗ БЕЗОПАСНОСТИ МЕССЕНДЖЕРА TELEGRAM

Аннотация: *Telegram — это платформа для обмена мгновенными текстовыми сообщениями. Компания основана в 2013 году и имеет более 100 миллионов активных пользователей. Телеграмм был создан чтобы позволить пользователям иметь защищенную от слежки связь. В этой статье мы рассматриваем Telegram, обсуждаем его протокол и сравниваем его с похожими продуктами.*

Ключевые слова: Информационная безопасность, защита информации, утечка информации, угроза информационной безопасности, эксплойт.

Avtaev Maxim Sergeevich
student
Russian Technological University
Russia, Moscow

SECURITY ANALYSIS OF TELEGRAM

Abstract: *Telegram is an instant text messaging platform, with a secure messaging protocol called MTProto. The company was founded in 2013 and has more than 100 million active users. Telegram was created to allow users to have surveillance-proof communication. It claims to have the best security and privacy guarantees in the market. In this report we overview Telegram, discuss its protocol and compare it to similar products. We also exploit a leak on user availability and use it to predict when users are talking to each other.*

Keywords: Information security, information protection, information leakage, information security threat, exploit.

В последнее десятилетие, когда все больше и больше людей получали доступ к Интернету, службы обмена мгновенными сообщениями процветали. По состоянию на май 2020 года два из пяти крупнейших большинство загружаемых приложений на рынке Android — это службы обмена сообщениями. В последние годы пользователи коммуникационных средств, в том числе мессенджеров,

стали более осознанно относиться к конфиденциальности и безопасности. Чтобы лучше удовлетворить потребности пользователей, многие платформы начали предлагать сквозное шифрование. Среди множества мессенджеров — Telegram, основанный в 2013. Несмотря на то, что он новичок в этой области, он имеет более 100 миллионов пользователей в месяц, особенно в Восточной Европе. Telegram утверждает, что имеет лучшие гарантии безопасности и конфиденциальности среди аналогичных продуктов. Хотелось бы провести анализ безопасности Telegram, так как мессенджер вызвал шквал критики со стороны многих профессиональных криптографов.

Как и многие его конкуренты, Telegram придерживается традиционного подхода к использованию облачного хранилища для своих данных. Это означает, что если злоумышленник сможет получить контроль над серверной системой, у него будет доступ к (по крайней мере) незашифрованным сообщениям и, безусловно, все метаданные. Сообщения между пользователями и сервером передаются в соответствии с доморощенным Telegram протоколом обмена сообщениями MTProto. Все официальные клиенты Telegram имеют открытый исходный код. Telegram обеспечивает заметно более быстрый и плавный пользовательский интерфейс. Пользователи используют обмен ключами Диффи-Хеллмана для генерации общего ключа, который затем используется для передачи сообщений. Они взаимодействуют с сервером, используя открытый ключ RSA сервера, который жестко закодирован в клиентах Telegram и редко меняется. Telegram использует отечественный протокол MTProto, который обходит многие традиционные подходы к передаче сообщений. Telegram утверждает, что это сделано для его превосходной производительности, хотя многие эксперты по безопасности сомневаются в этих заявлениях.

На концептуальном уровне в Telegram есть некоторые нестандартные практики, которые, не должны быть частью защищенного протокола. А именно [1-4]:

• Функция сквозного шифрования Telegram по умолчанию не включена в приложении. По этой причине многие пользователи, у которых недостаточно

знаний в области безопасности / шифрования, в конечном итоге используют Telegram без функции «секретный чат», думая, что их сообщения зашифрованы.

• Telegram использует отечественный криптографический протокол под названием MTProto, решение, которое подверглось резкой критике; общая доктрина безопасности диктует, что разработчики никогда не должны «внедрять свою собственную» криптографию и должны оставить разработку криптографического протокола экспертам. Те, кто сам изучил протокол, также отнеслись к нему скептически; криптограф Мэтт Грин прокомментировал, что «Telegram - это десять миллионов движущихся частей Рубе Голдберга, и все они созданы для поддержки единого, неаутентифицированного обмена ключами Диффи-Хеллмана».

• Telegram изначально запрашивает список контактов с телефона / рабочего стола и сохраняет их на своих серверах. Это обеспечивает огромную социальную сеть информация для них, которая либо подвергается атаке на их серверах, либо может быть продана различным органам власти без согласия пользователей. Это еще один случай, когда пользователи должны доверять Telegram свои данные.

Технические проблемы безопасности:

• Группа исследователей в 2015 году объявила об атаке «человек посередине» на Telegram. Атака включает в себя генерацию общих секретных ключей Диффи-Хеллмана для двух жертв, которые имеют один и тот же 128-битный визуальный отпечаток пальца, так что пользователи, которые сравнивают отпечатки пальцев, не смогут обнаружить атаку;

С тех пор Telegram значительно увеличил количество битов отпечатков пальцев, но тот факт, что эта уязвимость когда-либо присутствовала, по-прежнему вызывает беспокойство, поскольку это была ошибка, которую эксперты не должны допускать.

• До 2014 года MTProto Telegram использовал модифицированную версию Diffie-Hellman обмен ключами. Вместо использования ключа, сгенерированного обычным протоколом DH, сервер отправил бы пользователям ключ, зашифрованный с помощью одноразового номера. Это позволило бы злому

серверу использовать разные одноразовые переменные для двух пользователей. В результате пользователи по-прежнему будут иметь один и тот же ключ, но он также будет известен серверу. И снова пользователям пришлось доверять серверу Telegram. К их чести, Telegram решил эту проблему, но само его присутствие вызывает вопросы об их приверженность безопасности, потому что проблема очень проста.

• Telegram использует SHA-1 вместо SHA-256 для хэширования в некоторых частях своего протокола. Известно, что SHA-1 не является устойчивым к столкновениям.

Даже если Telegram, как он утверждает, использует SHA-1 в месте, где не требуется устойчивость к столкновениям, использование более сильной хэш-функции было бы более разумным.

• Даже при использовании «безопасного чата» для общения мобильное приложение Telegram позволяет третьим лицам наблюдать информацию о метаданных. Например, злоумышленники могут узнавать, когда пользователи выходят в Интернет или оффлайн, с точностью до секунды. Telegram не требует согласия обеих сторон для установления связи между ними. По этой причине злоумышленник может подключиться к пользователю, и он получит информацию о метаданных без того, чтобы пользователь что-либо знал об этом. По этой причине у злоумышленника может быть хороший шанс угадать, общаются ли 2 пользователя, подключившись к ним обоим и наблюдая за метаданными использования их приложения.

Как показывают предыдущие примеры, во многих случаях пользователи Telegram должны полностью доверять серверу, что является ироничным, поскольку основатели утверждают, что они хотели предоставить сервис, защищенный от слежки. Несмотря на то, что многие проблемы с безопасностью были исправлены, некоторых из них не должно было быть в первую очередь.

В этой статье мы исследовали мессенджер Telegram. Когда Telegram зародился как компания, он стал популярным из-за своих заявлений, доверия общественности к основателям, а также из-за сроков (утечки АНБ Сноуденом

произошли в том же году). Учитывая эти утверждения, можно было бы ожидать от Telegram очень высокого уровня безопасности. Однако наш опрос показывает, что у Telegram были серьезные и простые проблемы в протоколе (например, модифицированный обмен ключами Диффи-Хеллмана с ошибками), которые мог бы решить любой знающий специалист по безопасности.

Наконец, наш вывод заключается в том, что Telegram, как и любое другое приложение, имеет уязвимости. Пользователи должны знать об этом факте, но, к сожалению, заявления компаний заставляют пользователей, не разбирающихся в технологиях, полагать, что их сообщения нечитаемы третьими лицами.

Список литературы:

1. Сквозное шифрование. [Электронный ресурс] // Режим доступа: URL: https://www.whatsapp.com/faq/en/general/28030015 (дата обращения: 25.11.20222 г.)

2. Telegram. [Электронный ресурс] // Режим доступа: URL: https://web.telegram.org (дата обращения: 25.11.20222 г.)

3. Интерфейс командной строки мессенджера Telegram. [Электронный ресурс] // Режим доступа: URL: https://github.com/vysheng/tg (дата обращения: 25.11.20222 г.)

4. Является ли Телеграм безопасным [Электронный ресурс] URL https://habrahabr.ru/post/206900 (дата обращения: 25.11.20222 г.)