Aluno: Pedro Henrique Aquino Silva
Sistema avaliado: Telegram

Ativos

O Telegram é um serviço de mensagens fundado em 2013 pelos irmãos Nikolai e Pavel Durov. O serviço utiliza um modelo de segurança próprio, baseado no protocolo MTProto. Enquanto a empresa afirma que o Telegram não tem lucro como objetivo final, ela não é uma organização sem fins lucrativos. Desta forma, os principais ativos a serem protegidos são os dados e privacidade dos usuários e a confiança e integridade do serviço.

Adversários

Praticamente todos os componentes do Telegram são de código aberto e possuem builds reproduzíveis, o que permite a verificação da integridade e segurança do serviço por pesquisadores e usuários. Contudo, existem profissionais de segurança que contestam a verificabilidade do protocolo MTProto, uma vez que o código do servidor onde as mensagens são armazenadas e criptografadas é de código fechado, assim como há decisões de projeto no protocolo que não são necessariamente válidas, segundo algumas pesquisas em segurança e criptografia.

Os adversários da rede são, portanto, usuários e softwares maliciosos, que podem explorar tanto inseguranças no próprio código do servidor como problemas relatados pela comunidade.

Um aspecto interessante do Telegram é que a criptografia de ponta-a-ponta não é ativada por padrão nas conversas privadas, e não é disponível para grupos, o que faz com que hajam vazamentos de informações, principalmente relacionado ao uso incorreto por pessoas desinformadas sobre o modelo de segurança adotado pelo serviço. Este fato leva aos vazamentos de dados e conversas bastante comuns nas notícias relacionadas ao app, como o “Telegramgate” de Porto Rico, em 2019, ou o vazamento de conversas relacionadas à operação Lava Jato, no Brasil, também em 2019.

Gerenciamento de risco

Atualmente, o Telegram não oferece ferramentas para lidar com dados e transações financeiras, mas existem bots que podem armazenar informações sensíveis dos usuários e realizar operações deste tipo. É necessário, portanto, ter especial cuidado com os bancos de dados, o que é feito por meio dos algoritmos de criptografia desenvolvidos pela empresa.

Todas as mensagens, salvo quando os usuários optam pelos “chats secretos” são armazenados na nuvem, o que ressalta a importância de cuidar tanto com ocasionais falhas de hardware e software no armazenamento de informações privadas e registros pessoais que por ventura só estejam salvos na nuvem do Telegram, como com ataques e falhas nos servidores que cuidam dos dados.

Contramedidas

Por padrão, para acessar a conta do Telegram só é necessário o número do Telefone, sendo enviado um código de uso único para validar o acesso. Outros modos de login existem, incluindo autenticação de dois fatores (2FA).

O Telegram opta por não utilizar criptografia de ponto-a-ponto em todas as conversas para permitir uma série de recursos como edição de mensagens. É possível, como dito anteriormente, optar por "chats secretos" em conversas privadas, o que emprega criptografia ponto-a-ponto. Existe também uma grande quantidade de recursos de privacidade, como o uso de nomes de usuário anônimos como contatos, esconder número de telefone e última vez vista, etc. Ressalto que ainda é necessário que o usuário opte por utilizar estes recursos.

Todas as mensagens salvas na nuvem são armazenadas utilizando criptografia simétrica AES de 256 bits, criptografia RSA de 2048 bits ou troca de chave segura Diffie-Helman.

O Telegram também incentiva usuários avançados e especialistas em segurança a investigar falhas nos algoritmos de código aberto, sendo que já foram realizadas competições para tentar quebrar a criptografia do serviço, assim como premiações por encontrar bugs e falhas.

Custo/Benefício

O Telegram já foi alvo de várias críticas quanto à sua segurança, principalmente pelo fato de a rede social colocar-se como alternativa segura a outros chats como WhatsApp. É comum que dados de conversas sejam vazados, como nos casos citados anteriormente, mas comumente isto se dá por desinformação ou descuido do usuário, não tendo sido encontradas, até o momento, falhas de segurança relacionadas aos casos de vazamento.

A segurança oferecida pelo Telegram, no geral, é maior que de outros serviços, mas a falta de criptografia ponto-a-ponto por padrão leva a pontos fracos na segurança em chats de grupo ou individuais normais (não-secretos), com o benefício de habilitar outras funcionalidades para o usuário.

No geral, a segurança é o maior ponto de venda do Telegram, e deve-se investir em peso para garantir, ao máximo possível, que os algoritmos de criptografia abertos ou proprietários estejam de fato protegendo os usuários.