Aluno: Gustavo Emanuel Kundlatsch
Sistema Avaliado: Telegram

- **Ativos:** O Telegram é um serviço de troca de mensagens sem fins lucrativos, mantido até 2021 por um fundo criado por Pavel Durov. Portanto, o principal ativo a ser protegido é a segurança do próprio usuário e a integridade do serviço (tempo disponível online).
- **Adversários:** Os Apps do Telegram (Desktop, Mobile e Web) são de código aberto e possuem builds reproduzíveis, que garantem boa parte da integridade por meio da comunidade que contribui com o serviço. Segundo a própria empresa, este código permite que pesquisadores de segurança avaliem completamente a implementação da criptografia de ponta a ponta do serviço. Também é possível verificar de forma independente que os apps do Telegram na Google Play e na App Store são feitos usando o mesmo código que é publicado por eles no GitHub. Dito isso, podem existir ameaças internas no código do servidor, implantadas por membros da empresa, pessoas mal intencionadas de fora podem tentar usar os problemas de segurança relatados pela comunidade.
- **Gerenciamento de Risco:** Atualmente não existem transações financeiras dentro do Telegram, mas diversos bots possuem informações sensíveis dos usuários. Por conta disso, é preciso ter um grande cuidado ao manter o banco de dados bem protegido. Além disso, todas as mensagens são salvas na nuvem, portanto uma pane geral no servidor pode fazer com que usuários percam informações importantes ou registros pessoais que podem não estar disponíveis em nenhum outro lugar.
- **Contra Medidas:** Por padrão é apenas necessário o número de telefone para acessar sua conta do Telegram, mas é possível ativar senhas locais e autenticação de dois fatores (2FA). Dentre as opções de segurança do aplicativo, é possível configurar diversas informações particulares (como número de telefone e última vez visto online) para ser visto por todos, contatos ou ninguém. Além disso, é possível ver todas as sessões atualmente ativadas e desativar as desejadas. Todas as informações trocadas dentro do aplicativo possuem criptografia baseada em criptografia AES simétrica de 256 bits, criptografia RSA de 2048 bits ou troca de chave segura Diffie-Hellman.
- **Custo/Beneficio:** O Telegram surgiu para ser um chat livre e seguro, que possa ser usado em todo o tipo de situação ou país. Sua premissa é que possa ser usado dentro de ditaduras ou em situações onde o usuário está sendo caçado pelo estado, por exemplo. Portanto, é essencial que as tecnologias desenvolvidas para garantir isso sejam de ponta, caso contrário o aplicativo estará falhando com sua base de usuários. A maior parte disso é feito debaixo dos panos, pois o usuário final não vê o algoritmo de criptografia quando envia uma mensagem. Mas mesmo que seja necessário um pouco mais de burocracia (como no caso do 2FA), a segurança é um dos pilares do Telegram, portanto deve ser investida em peso.