heimdall

security research

A DIVISION OF ISH

Telegram, uma plataforma útil para o cibercrime.

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

Sumário

Lista de Figuras

1 SUMÁRIO

Podemos afirmar que o Telegram é um aplicativo de mensagens que está sendo utilizado por diversas pessoas ao todo o mundo, para as diversas utilidade, seja para atividade lícitas ou para ilícitas.

Para fins ilícitos, o Telegram é utilizado para a prática de crimes cibernéticos, seja para fins de venda de dados, vazamento de dados pessoais, hacktivismo, venda de produtos ilegais, como a venda de documentos falsos e entorpecentes e outros.

Um dos motivos do qual o Telegram é a escolha preferida para os cibercriminosos praticarem seus atos ilícitos é devido a criptografia integrada e a capacidade da criação de canais e grandes grupos privados.

Este relatório elaborado pela **Heimdall** é apresentar uma compreensão do porquê o Telegram se tornou um participante no âmbito do cibercrime. O relatório irá apresentar ainda exemplos de atividades identificadas e monitoradas pela equipe, visando exemplificar a possibilidade da ferramenta para prática de crimes.

2 TELEGRAM

O aplicativo Telegram é um tipo de serviço de mensagens "multiplataforma" lançado no ano de 2013 pelos russos Nikolai e Pavel, sendo estes irmãos. A plataforma permite que os usuários enviem mensagens, vídeos, fotos e arquivos de qualquer tipo, como .doc, .zip, .mp4 e outros de até 2 GB de tamanho e possibilita a criação de grupos e canais.

Segundo o Telegram, seria a única empresa focada em privacidade, criptografia e uma API de código aberto, fornecendo bate-papos criptografados de **"ponta a ponta"**[1] de forma opcional e todas as mensagens enviadas podem ser excluídas a qualquer momento, seja por quem está enviando ou por quem recebe.

Referente a API, esta pode ser utilizada para integração com outras plataformas, bots personalizados, temas, adesivos e para outras finalidades.

Um dos pontos que podemos mencionar é que o Telegram já realizou a cooperação com forças da lei para determinados casos, levando a questionar se realmente as mensagens são privadas o quanto todos imaginam que sejam.

Usuários no Telegram

Os usuários do Telegram possuem praticamente dois identificadores, sendo o "nomes de usuários" e "Ids de usuário", sendo que os nomes dos usuários não são públicos e podem ser editados nas configurações. Após a definição dos nomes, o usuário pode realizar o compartilhamento do seu perfil com outras pessoas por meio de um link, cujo link se forma da seguinte forma: **"t.me/username"**. Os Ids são atribuídos por usuários, grupos e canais pelo Telegram, e os usuários não podem alterá-los.

Canais no Telegram

Os canais que os usuários do Telegram podem criar

[1] Criptografia de Ponta a Ponta (End-to-End) de acordo com o Telegram: https://core.telegram.org/api/end-to-end

Os usuários podem utilizar os canais para construção de comunidades, havendo a possibilidade desta forma em compartilhar recursos ilimitados nestas comunidades. Os referidos canais são plataformas de comunicação unidirecional, ou seja, apenas os administradores podem enviar mensagens e os assinantes e participantes do canal não podem responder.

No ano de 2020, o Telegram atualizou a plataforma e permitiu que os assinantes dos canais comentassem nas postagens dos canais.

Grupos no Telegram

O recurso seguinte que mandamos são os grupos de bate-papos, onde os membros podem interagir uns com os outros e responder a mensagens. Para o caso de grupos, os demais usuários podem visualizar os demais contatos, existindo desta forma grupos fechados e grupos abertos.

Um dos pontos que o Telegram possui como diferença dos demais aplicativos é a possibilidade de adicionar até 200.000 pessoais a um único grupo.

Criação de Bots

O Telegram possibilita utilizar e criar bots que são essencialmente contas automatizadas no Telegram. São boas ferramentas para utilizar em uma variedade de objetivos, incluindo criar, gerenciar bate-papos em grupos, atuar como assistentes e outros. Além disso, os bots são automatizados para coletar dados de fora do aplicativo.

Toncoin, a moeda do Telegram

O aplicativo possui a própria criptomoeda, hoje conhecida como Toncoin, a qual é um token nativo da The Open Network, uma tecnologia baseada em blockchain desenvolvida pelo Telegram.

Podemos considerar que o Telegram é uma plataforma muito utilizada pelo cibercrime, visto que podem compartilhar informações, dados, coordenar atividades, bem como utilizar o Telegram como forma

de contato com outros atores maliciosos. Além disso, é constatado que o Telegram facilita a venda de dados roubados e mercadorias ilícitas ou, até mesmo para recrutar novos membros para as atividades.

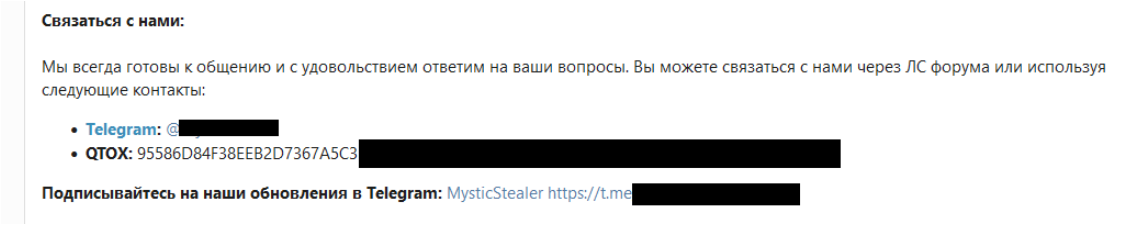

Figura 1 – Anuncio e divulgação do canal no Telegram.

A utilização do Telegram por cibercriminosos são devido aos motivos que garantem a privacidade e a segurança. A plataforma permite também que os usuários registrem contas sem divulgar informações pessoais, simplificando a configuração de várias identidades e poderá utilizar sem que seja relevado a identidade daquele usuário.

Outra opção para os cibercriminosos é que os usuários do Telegram podem se inscrever com números virtuais ou números de telefone estrangeiros que podem não estar relacionados às suas verdadeiras identidades, dificultando desta forma a identificação da identidade real do ator de ameaça.

Já para as organizações que atuam no combate a fraudes e atos maliciosos destes atores, é a possibilidade de realizar a pesquisa em canais e grupos do Telegram apenas digitando uma determinada palavra relevante na barra de pesquisa, bem como possibilitando realizar o acesso aos dados de determinados canais ou grupos e realizar a criação de bot para realizar a pesquisa e coleta de dados.

3 VENDA DE DADOS ROUBADOS

Contas de serviços populares de streaming e outros serviços são anunciados através de canais no Telegram, bem como as publicações realizadas podem ser disponibilizadas para os possíveis compradores escolherem e realizarem a negociação diretamente com o anunciante do tipo venda de contas.

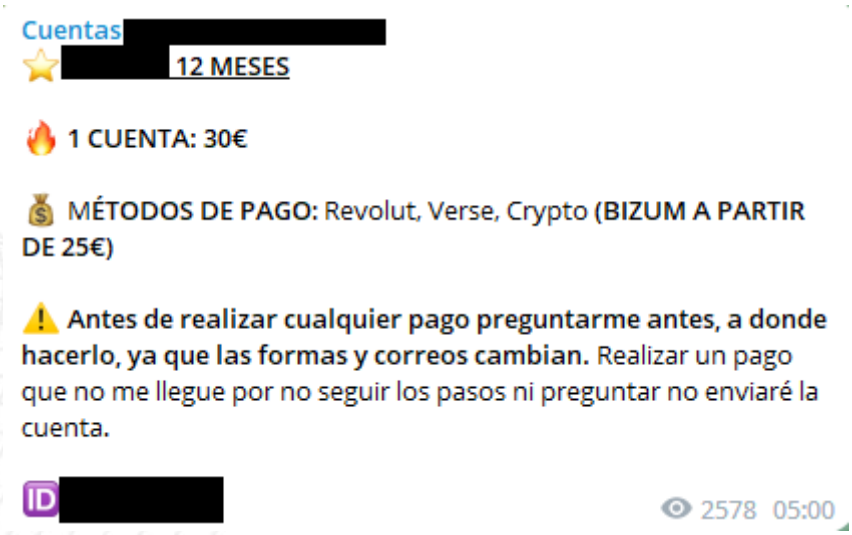

Figura 2 – Anúncio de contas de um serviço de stream.

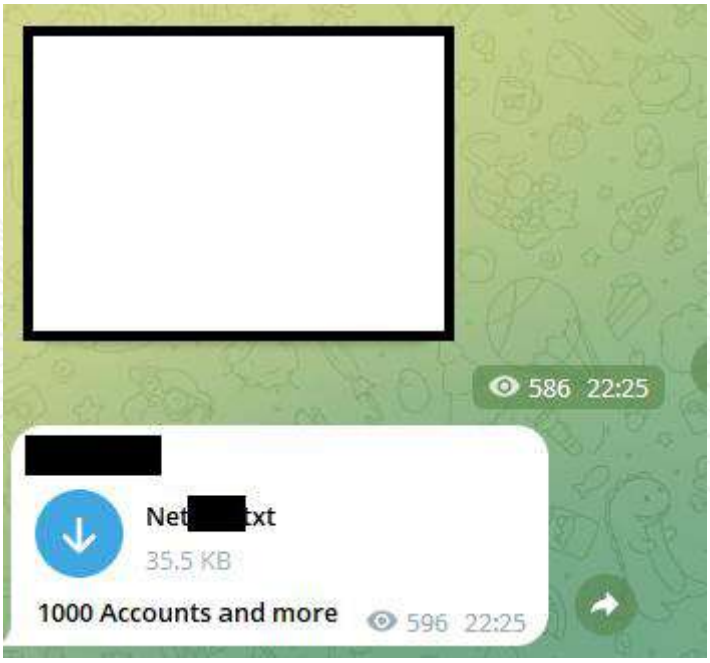

Figura 3 – Anúncio de contas da plataforma Netflix.

Vale salientar que alguns fóruns de crimes cibernéticos que se encontram hospedados na *deep* e *dark* web possuem canais exclusivos no Telegram, como por exemplo o canal no Telegram para o **Raid Forums.**

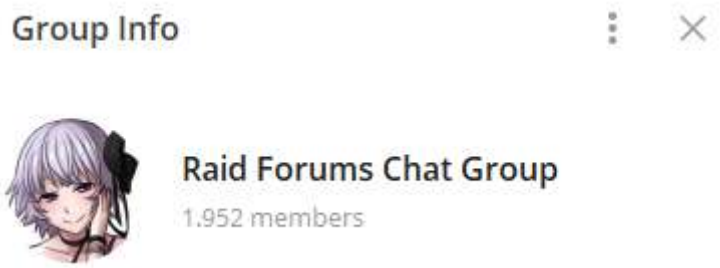

Figura 4 – Canal no Telegram do Raid Forums.

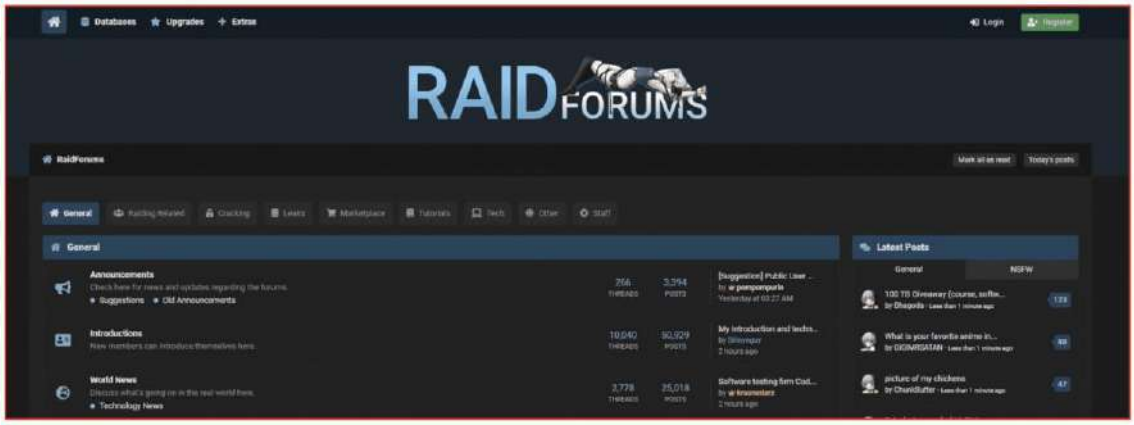

Figura 5 – Raid Forums público na Deep Web.

Outro fato que ocorre comumente nos chats do Telegram é a revenda de dados roubados e exfiltrados das empresas, sendo que após um determinado ator de ameaça tornar publicamente os dados, outros atores podem realizar o download e vende-los posteriormente alegando que seriam novos dados vazados.

Existem canais no Telegram que acabam por disponibilizar uma ampla fonte de recursos para identificar onde está sendo realizada a venda de determinados dados de organizações, como por exemplo as figuras abaixo.

Figura 6 – Venda de dados de uma organização brasileira.

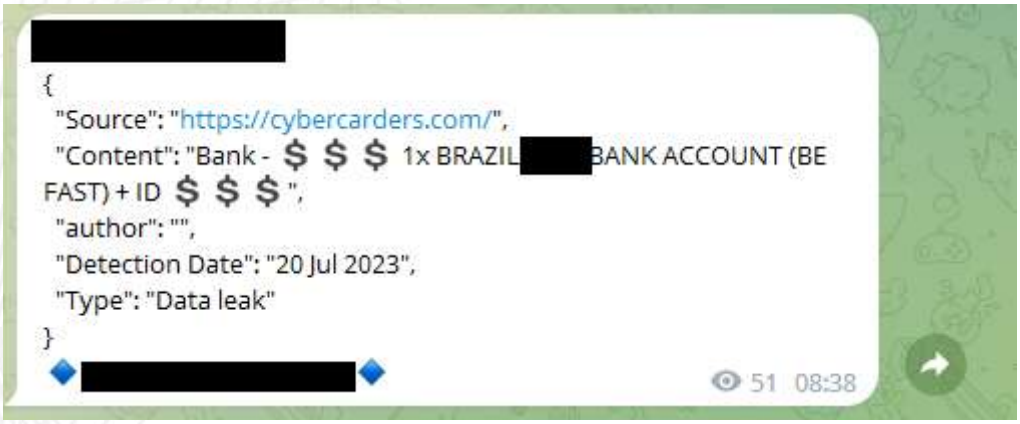

Figura 7 – Monitoramento de canais e sites de Fórum sobre organizações Brasileiras.

4 INFOSTEALERS

Os malwares do tipo stealers, são os malwares que possuem como foco realizar o roubo de informações e dados de um dispositivo que realizavam a infecção e, após a exfiltração dos dados, estes dados são vendidos como forma de "**logs**" de stealers, cujos logs contém toda a massa de dados que foram coletadas das vítimas.

A infecção por estes malwares está em avanço tendo em vista que a todo o momento novos programas de *malwares-as-a-service* são iniciados e divulgados, como por exemplo **Redline, Mysitc, Meduza, Vidar** e outros tipos de malwares.

Os logs vendidos contêm informações como credenciais de logins de usuários, históricos de navegações, cookies, tokens de autenticações e informações sobre o dispositivo do usuário. Caso algum ator de ameaça realize a compra destes logs, poderá resultar em outros tipos de ataques ou incidentes de seguranças, como exfiltração de dados, movimentações laterais, vendas de acessos e outros.

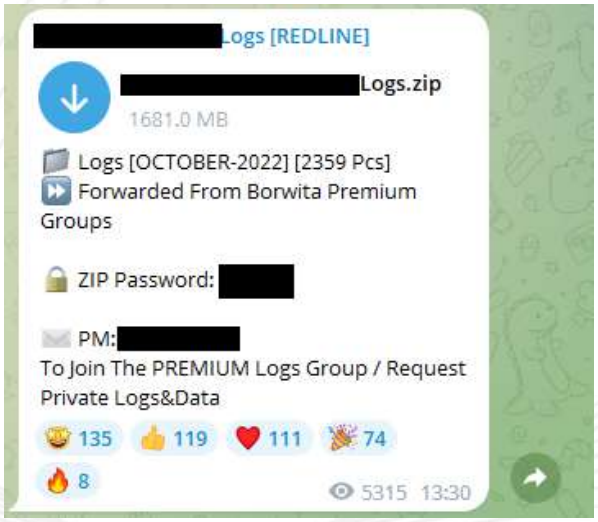

Figura 8 – Mensagem realizando a venda de logs do RedLine.

Figura 9 – Publicação do Mistyc Stealer (malware-as-a-service).

Alguns serviços de malwares realizam a integração com estes tipos de malwares que realizam a exfiltração de dados, como por exemplo, após uma infecção de uma vítima, o ator de ameaça poderá realizar a escolha de exfiltrar para um canal ou bot criado pelo ator malicioso.

O Telegram tornou para os agentes de ameaças uma das principais ferramentas para realizar a venda destes tipos de logs de *stealers*, podendo desta forma mencionar a importância de prevenção quanto a infecção de malwares do tipo *stealers*, adotando as melhores práticas para fins de não ser realizada a venda dos dados como em canais do tipo Telegram.

5 ATORES DE RANSOMWARE E OUTROS

Atores de ameaças que podemos classificar como grupos de Ransomwares também migraram para a utilização da plataforma do Telegram como meio de publicar e extorquir as organizações afetadas.

Outros atores de ameaças como **Lapsu$ e Stormous** realizaram e realizam a publicação de dados de organizações atacadas, criam chats para discussões entre os membros e criam até canais dedicados para vazamento de dados de uma vítima.

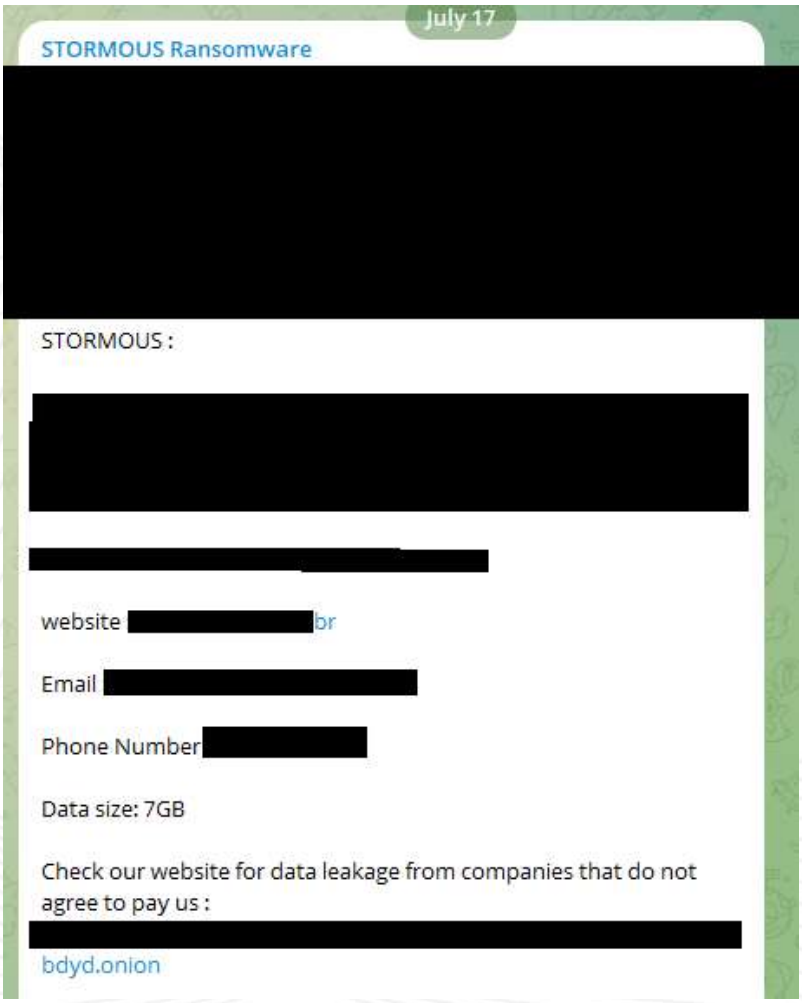

Figura 10 – Grupo de Ransomware Stormous divulgando empresa.

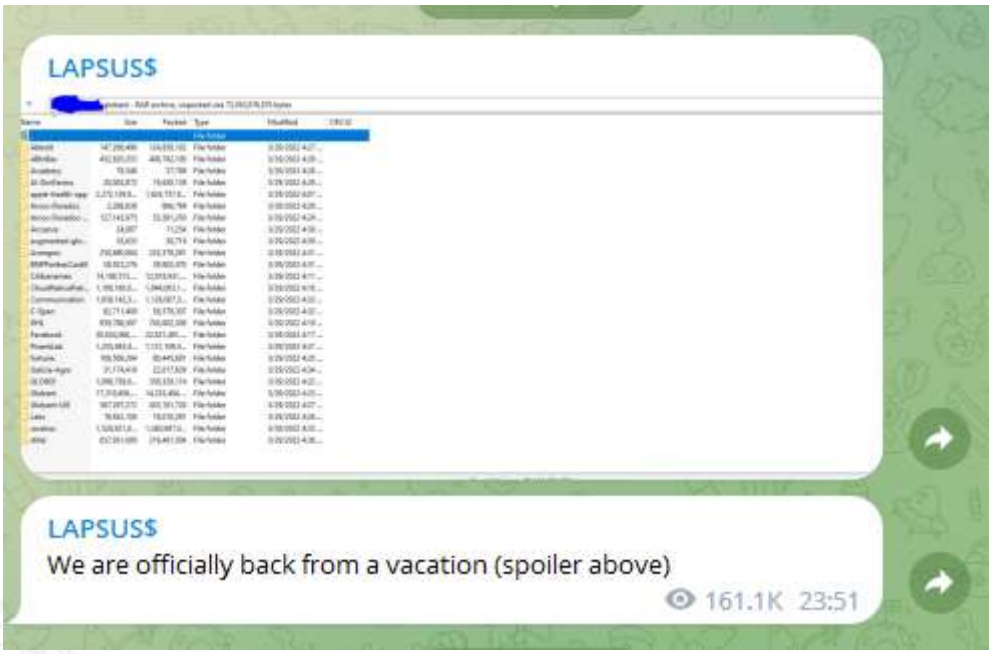

Figura 11 – Publicação realizada pela LAPSUS$.

Figura 12 – Canal do Bl00dy Ransomware.

6 Conclusão

O Telegram se tornou uma das maiores ferramentas que são utilizadas por atores de ameaças para fins de comunicação, venda, divulgações e para qualquer outro tipo de motivação que os atores de ameaças acharem interessantes e relevantes para as suas operações. Pode ser considerado como mais uma plataforma para ser monitorada, visto que é provável que o Telegram irá ser adotado e utilizado por atores de ameaças para prática destes atos ilícitos.

É evidente que se torna eficaz para os pesquisadores de segurança identificarem tais atores de ameaças, visto que o monitoramento poderá auxiliar para prevenir e mitigar ataques cibernéticos nas organizações e, poderá ser realizada a coleta de informações relevantes sobre estes atores, como táticas, técnicas e procedimentos, ferramentas utilizadas pelos atores e comportamentos destes.

heimdall
security research

A DIVISION OF ISH