KELA REPORT

TELEGRAM

ひとつのメッセージアプリが 2023年にサイバー犯罪エコシステムへと 進化するまで

エグゼクティブサマリー

「Telegram」は、世界中で多くの人々が使用しているメッセージアプリであり、その使用目的も多岐にわたります。そしてその一方で、個人や企業から窃取したデータの売買・リークや、サイバー犯罪グループの組織化、ハッキング用チュートリアルの配信、ハクティビズム活動、違法な物品（コピー商品やドラッグなど）の売買をはじめとするサイバー犯罪活動の拠点にもなっています。

サイバー犯罪者が好んで使用しているメッセージアプリは複数ありますが、その中でもTelegramは最も人気の高いアプリです。そして、サイバー犯罪との戦いに挑むセキュリティ研究者にとっては、同アプリが大きな課題となっています。

サイバー犯罪者がTelegramに魅力を感じる理由として、同アプリに組み込まれているとされる暗号化機能や、チャンネルをはじめとする大規模な非公開グループを作成できる機能があることが挙げられます。しかし同時にこれらの機能は、法執行機関やセキュリティ研究者がTelegram上で行われるサイバー犯罪者の活動を監視・追跡する妨げとなっています。また、サイバー犯罪者はTelegramでやり取りを行う際、コード化したメッセージや同音異字を頻繁に使用しているため、他者が彼らの会話を解読することがさらに困難となっています。

今回KELAは、サイバー犯罪エコシステムの中でTelegramが重要な役割を果たしている理由を皆様に理解していただく一助として、本レポートを作成しました。本レポートでは、Telegram上に存在する様々なサービスや製品、サイバー犯罪活動、関与している脅威アクターに加え、各トピックに該当する具体的な事例（Telegram上で展開されている各種活動など）について解説します。また、Telegram上で展開されているサイバー犯罪の範囲と規模の概要を包括的に理解していただけるよう、各活動に関与している有名なグループやチャンネルの一覧も掲載しています。

本レポートで取り上げるトピックとアクター（グループ）は以下の通りです。

- Telegramで販売・リークされている個人や企業のデータ
- 情報窃取マルウエアを使って収集したデータを販売・リークしたり、活動の円滑化・拡大にむけたグループの組織化やボット構築を行う手段として、Telegramを使用している情報窃取グループ
- クレジットカードや小切手、その他の金融商品をTelegramで販売している銀行詐欺グループ
- 自らのブログやデータリークサイトの代用、または追加のサイトとしてTelegramを使用しているランサムウエアグループやデータリークグループ（Lapsus$など）
- 自らの攻撃に関する情報をTelegramで公開しているハクティビスト（KillnetやALtahrea Teamなど）
- コピー商品、銃、ドラッグ、新型コロナウイルス関連文書など、Telegramで販売されている違法な有形商品

今回KELAは、各トピックに該当する「商品」に焦点をあててレポートを作成しています。ただし、Telegramには各トピックに該当するコンテンツ（チュートリアルやサービス、その他）が、本レポートで取りあげたもの以外にも多数存在している点にご注意ください。

総合的に見て、いまやTelegramは活発なサイバー犯罪エコシステムを形成しており、今後もセキュリティ研究者や法執行機関の皆様にとって、大きな課題となる可能性が高いと考えられます。

目次

セクション #1

概要

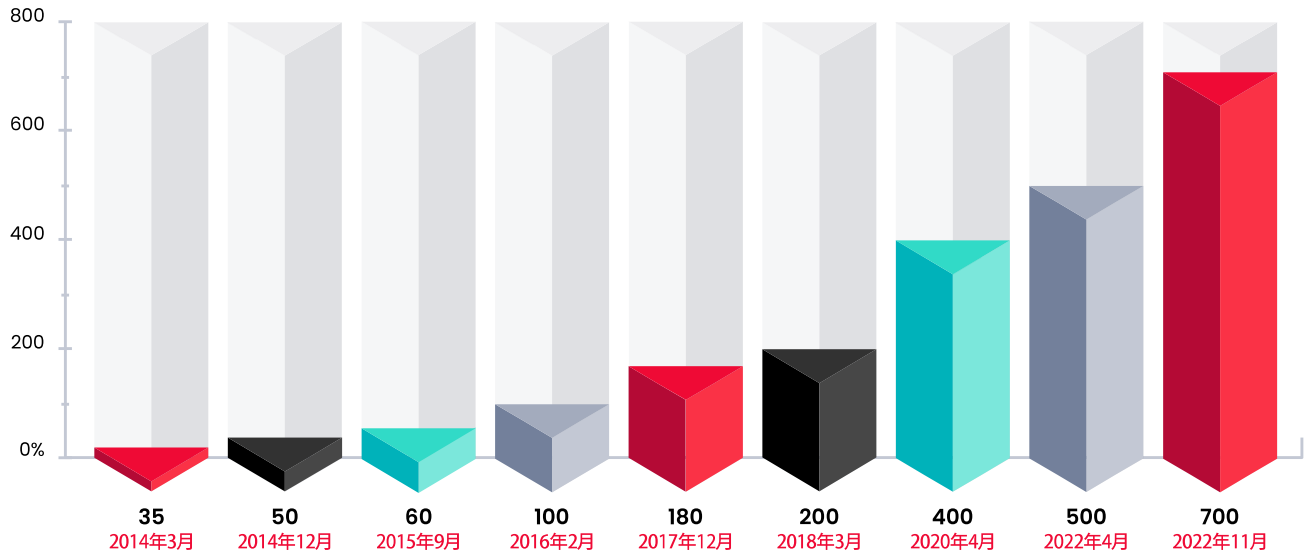
Telegramとは？

Telegramは、ロシア人兄弟であるNikolai Durov氏とPavel Durov氏が2013年に立ち上げた、マルチプラットフォーム型のメッセージサービスです。Durov兄弟は、ロシアのオンラインソーシャルメディア兼ネットワーキングサービスである「VK（旧Vkontakte）」の設立者でもあります。Telegramのプライバシーポリシーによると、「Telegram Messenger Inc.（以後Telegram社）」の親会社である「Telegram Group Inc.」は英国領バージニア諸島を拠点とし、グループ会社である「Telegram FZ-LLC」はドバイを拠点としています[1]。またTelegramのサイトにある説明によると、Telegramの開発チームもドバイを拠点としています[2]。

Telegramでは、ユーザーがメッセージや写真、ビデオをはじめ様々な種類のファイル（doc、zip、mp3など）を最大2GBまで送信したり、独自のグループやチャンネルを作成することが可能となっています。Telegram社は、同プラットフォームがプライバシーや暗号化、オープンソースのAPIに重点を置いている点を理由に挙げ、「Telegramは他に類のないプラットフォームである」と主張しています。Telegramには、エンドツーエンドでチャットを暗号化するオプション機能や、送信したメッセージを送受信者双方のデータから常時削除する機能があります。またTelegramのAPIも公開されており、開発者が他のプラットフォーム上で稼働するクライアントアプリを無料で作成したり、ボットやテーマ、ステッカーなどをカスタマイズすることが可能となっています[3]。

ただし、Telegramにもいくつかの欠点があります。まず、TelegramはAPIを公開しているものの、アプリのソースコードは公開していないため、本当にデータが安全に暗号化されていることを確認する術がないという点が挙げられます。また一部事例では、Telegramが法執行機関に協力していることも知られており、同アプリ上で取り交わされるメッセージは一般に思われているほど非公開な状態ではないと言えます[4]。

それでも、Telegramの月間アクティブユーザー数は世界中で増加しており、その数は2022年11月時点で7億人を超えています（下図参照）[5]。



図：全世界のTelegram月間アクティブユーザー数
（2014年3月～2022年11月、単位：100万人）

[1] Telegram Privacy Policy

[2] Telegram FAQ — Where is Telegram based?

[3] Telegramには有料サービス「Telegram Premium」があり、同サービスを使用するとプレミアムユーザー専用の機能を使用することができます（例：一般ユーザーの場合、アップロード可能なファイルサイズは最大2GBとなっていますが、**プレミアムユーザー**の場合は最大4GBとなっています）。

[4] Telegram Reportedly Handed User Data to German Authorities

[5] Telegram FAQ — What is Telegram? What do I do here?

Telegramの仕組み

Telegramのユーザー識別子は主に「ユーザー名」と「ユーザー ID」であり、ユーザー名が公開表示されます。ユーザーは、自分のユーザー名をアプリの「設定」で編集することができ、またユーザー名を設定した後は、自分の連絡先を「t.me/username」または「username.t.me link」という形式のリンクで他のユーザーに公開することができます（例えば、TelegramのCEOであるPavel Durov氏のユーザー名は「t.me/durov」となっています）。一方、ユーザーIDはTelegram側からユーザーやグループ、チャンネルへ割り当てられるものであり、ユーザー側で変更することはできません。

Telegramにはメッセージサービスの他、ユーザーがプラットフォーム上でコミュニティを作成できる機能があり、「チャンネル」や「グループ」がこれに該当します。「チャンネル」を作成した場合、チャンネル管理者となるユーザーは、送信先ユーザー数に上限なくメッセージを送信することができます。ただしチャンネルは一方向型のコミュニケーションプラットフォームであり、メッセージを発することができるのはチャンネル管理者のみとなります（チャンネル登録ユーザーは、チャンネルで公開された投稿に返信することができません）。ただし、2020年にTelegramがアップデートを行って以降は、チャンネル管理者が公開した投稿の下に、チャンネル登録者がコメントを入力できるようになりました[6]。チャンネル登録者がコメントを入力できるようにするためには、まずチャンネル管理者がチャットを作成する必要があり、作成したチャットをチャンネル登録者に公開すると、登録者が特定の投稿についてコメントしたり、他のユーザーとやり取りすることが可能となります（このチャットは、チャンネル登録者に対して非表示にすることも可能です）。

「グループ」はいわゆるチャットグループであり、グループ内のメンバーが互いにやり取りしたり、メッセージに返信することができる他、同じグループのメンバーの連絡先を見ることも可能となっています。なお、グループには「公開グループ」と「非公開グループ」があり、非公開グループに参加する場合は「招待状」が必要となります。また、1グループには最大20万人までユーザーを追加することが可能となっています。Telegramのライバル的存在であるインスタントメッセージプラットフォーム「WhatsApp」にも、ユーザーがチャットグループを作成できる機能がありますが、1グループに追加できる最大ユーザー数は512人となっており[8]、「Instagram」の場合はさらに少ない250人となっています[9]。つまり、他のプラットフォームと比較して、Telegramの方がより大勢の参加するコミュニティを構築することができるということになります。

図：チャンネルに掲載されたコメントの画像[7]

Telegramでは、ユーザーが「ボット」を作成することも可能となっています。基本的にボットとは、「自動化されたTelegramアカウント」を指し[10]、グループチャットの作成・管理やパーソナルアシスタントとしての機能、エンターテイメントの提供など、様々な目的で使用される人気のツールとなっています。そしてこのボットは、プラットフォーム外の活動を自動化する目的にも使用されています。

6 The Evolution of Telegram — September 2020

7 Search Filters, Anonymous Admins, Channel Comments and More

8 WhatsApp Blog: Reactions, 2GB File Sharing, 512 Groups

9 Instagram group chat size limits

10 Bots: An introduction for developers