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

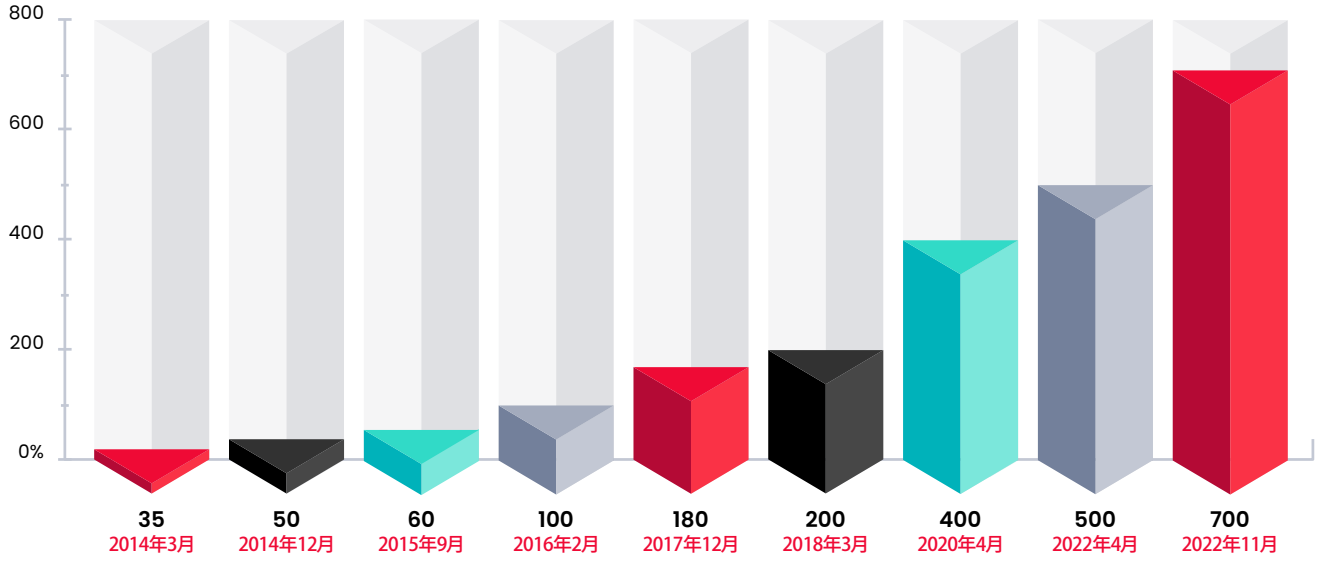
Telegramとは?

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

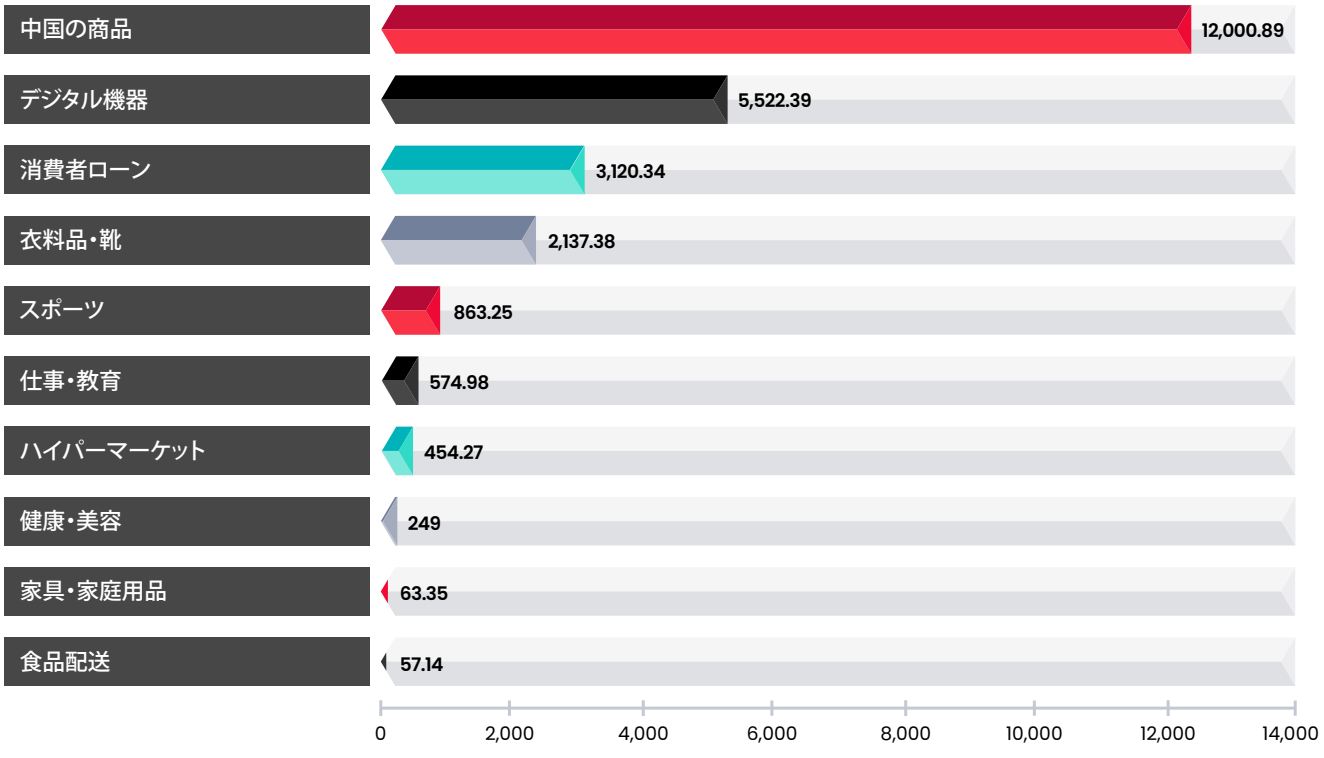
[8] WhatsApp Blog: Reactions, 2GB File Sharing, 512 Groups

[9] Instagram group chat size limits

[10] Bots: An introduction for developers

またTelegramには、独自の暗号資産「Toncoin（旧Gram）」があります。Toncoinは、Telegramが開発したブロックチェーンを基盤とする技術「The Open Network（略してTON、旧『Telegram Open Network』）」のネイティブトークンです。Telegramは、ユーザーが同アプリ内のチャットから直接Toncoinを送金できる機能を2022年4月に導入しており、現在、この機能を使って他のTelegramユーザーにToncoinを送金する際の手数料は無料となっています[11]。

これらの機能により、Telegramはユーザーや企業がコミュニティの構築や自社製品の宣伝・販売、その他様々な目的で活用できるツールとなりました。現在、同プラットフォームでは、デジタル機器や消費者向けローン、衣料品、靴などが商品として販売されています。また、Telegram上で行われた売買取引の売上高は、2020年末時点で2,500万米ドルに達したと報告されており、この時のデータによると、同年で最も高い売上高をみせたのは中国からの商品（1,200万米ドル超）となっています。



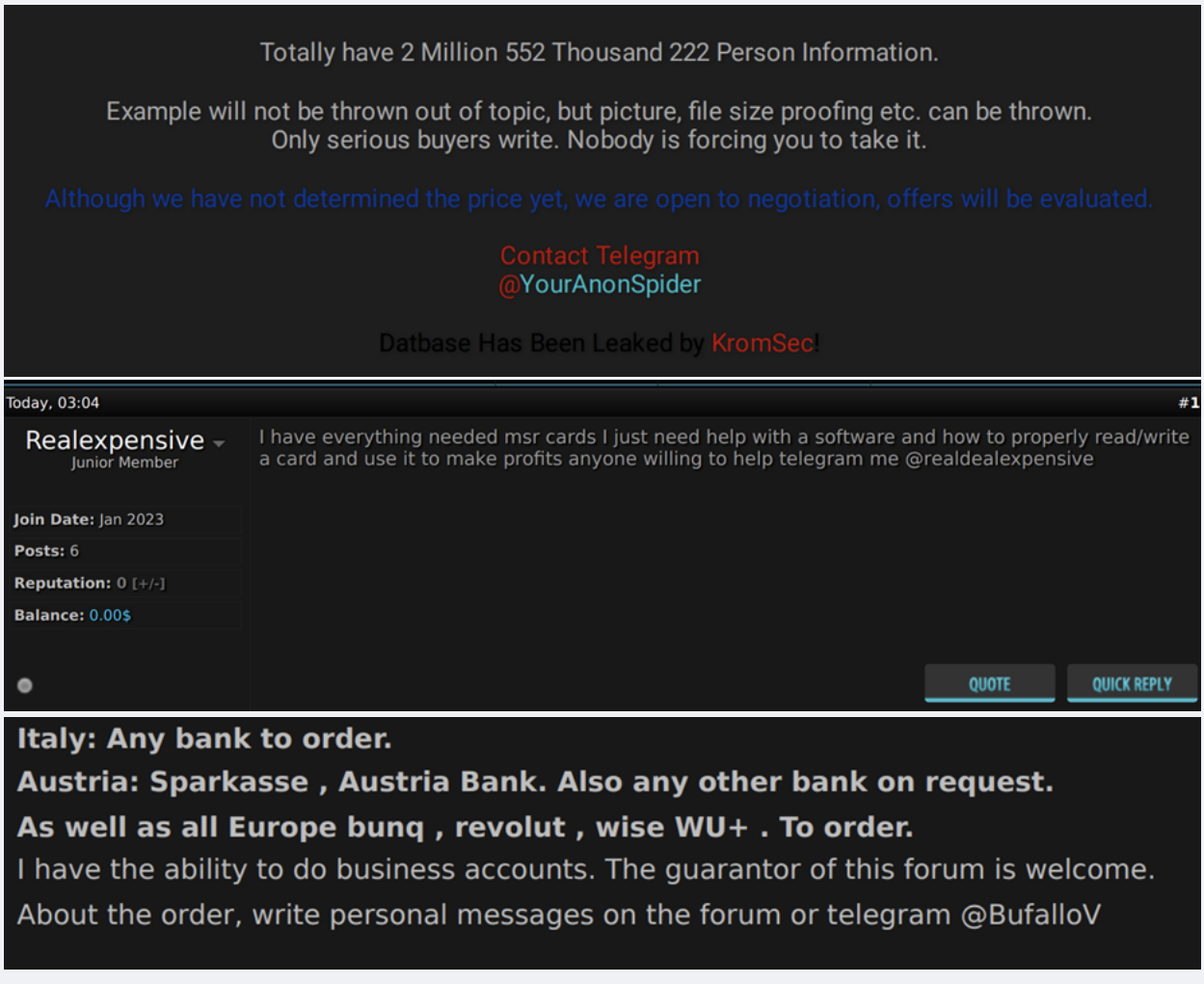
図：2020年にTelegram上で売買された商品のセグメント別売上高（単位：1,000米ドル）[12]

[11] TONのTwitter

[12] Statista: Sales volume on Telegram worldwide in 2020, by segment

Telegramがサイバー犯罪に適している理由

サイバー犯罪者は、様々な情報やヒント、コツなどを共有する他、活動を組織化する手段としてもTelegramを使用しています。彼らは、違法な活動について議論を深め、協力体制をとる場としてTelegramのグループやチャンネルを利用しており、それらグループのチャンネルやリンクをサイバー犯罪フォーラムやコミュニティに投稿しています。そのため、サイバー犯罪者の集うフォーラムやオンラインコミュニティには、Telegramのユーザーアカウントやチャンネルを掲載した広告が頻繁に投稿されています。またTelegramは、サイバー犯罪のテクニックに関する情報を共有したり、悪意あるツール（パスワードを窃取するトロイの木馬やキーロガー、ランサムウエアなど）を提供する他、窃取したデータや違法商品をスムーズに売買したり、犯罪活動に従事する新メンバーを募集する手段としても使用されています。



図：多数の脅威アクターが、様々なサイバー犯罪フォーラムで主要連絡先として
Telegramアカウントを掲載（上記はその一例）

ハッカーがTelegramを好む理由は多岐にわたりますが、同アプリがプライバシーとセキュリティに特化している点が大きな理由として挙げられます。ただし、Telegramが標準機能として提供しているチャットは完全には暗号化されておりません（標準機能で暗号化されるのはクライアント・サーバー間の通信のみであり、チャットのデータはTelegramのクラウドに保存されています[13]）。一方、「シークレットチャット」機能の場合は、エンドツーエンドで暗号化が行われるため、チャットのデータはTelegramのクラウドに保存されず、メッセージを閲覧できるのは送信者と受信者のみとなります。そのため、シークレットチャットは、第三者（チャットに参加

[13] Switched to Telegram? You need to know this about its encryption

していない人物）が当事者に気付かれることなく、メッセージを傍受・閲覧することが難しい仕組みとなっています。この機能は、プライバシーを重んじ、自らの個人情報を守りたいと願うユーザーにとって非常に重要なポイントとなります。

また、Telegramの匿名性もハッカーを引き付ける大きな要因となっています。Telegramでは個人情報を公開することなくアカウントを作成できるため、ユーザーが多数のアカウントを作成し、それらのアカウントを駆使して、自分の身元を明かすことなく他者とやり取りすることが容易になっています。そして法執行機関にとってはこの匿名性が、Telegramを違法行為に使用している個人を追跡・特定する妨げとなっています[14]。

Telegramでは、ユーザーが自分の身元と関係のない仮想電話番号や、海外の電話番号を使ってアカウントを作成することが可能となっています。また、自分の電話番号の代わりに1回限りのSMSサービスを使い、SMSサービスに送られたワンタイムパスワードを使用してアカウントを作成することもできます。さらに、最新のアップデート（バージョン9.2）ではブロックチェーンプラットフォーム「Fragment」が導入され、ユーザーが匿名番号をToncoinで購入して、SIMカードなしでアカウントを作成できるようになりました[15]。こういったアカウント作成の手軽さに加え、Telegramでは1人のユーザーが複数のアカウントを作成でき、またそれらアカウントを容易に切り替えられる仕組みになっていることから、セキュリティ研究者にとっては各ユーザーを追跡・特定することが困難となっています。そしてこういった状況は、Telegramを使用しているサイバー犯罪者に関する証拠を集め、立件する活動の妨げにもなっています。

Telegramのプライバシーポリシーには、「テロに関連する容疑で裁判所命令が提示された場合は、ユーザーのIPアドレスや電話番号を当局に開示することがある」と記載されていますが、Telegram社は、これまでそれら情報を開示したことはないと主張しています。しかし、同社がユーザーデータの安全性と機密性を約束しているにもかかわらず、最近ドイツで行われた捜査ではTelegramユーザーのデータが政府当局に公開され、コンテンツが検閲されていたことが明らかとなっています[16]。その報告によると、Telegram社は裁判所命令を受けてユーザーデータの開示を余儀なくされ、テロ活動や児童虐待の容疑者に関するデータをドイツ当局に引き渡したということです。Telegram社は、世界各地にある多数のデータセンターにデータを保存しており、異なる管轄区から複数の裁判所命令を受け取った場合に限っては、ドイツの事例のようにユーザーデータの提出・公開を余儀なくされることがあります。

またTelegramは、そのモデレーション機能（独自のルールを作成・実行して違法な投稿やコンテンツの内容をチェックし、不適切な場合は削除する機能）の緩さから、過激派やハクティビストにも好まれるプラットフォームとなっています。Telegramの場合は、モデレーション機能が独自のルールを作成・実行して違法コンテンツの削除リクエストを処理しており、マイノリティに該当する人々が平和的に表明している意見や、政治的動機に基づいたコンテンツなどは検閲していない一方で、テロリスト関連のコンテンツはブロックしています。またTelegramのユーザー数増加にともない、白人至上主義のコンテンツを含むチャンネルも削除しています。しかし、暴力の助長を禁止するというTelegramのルール順守状況にはむらがあり、同プラットフォームで交わされる情報を取り締まることが依然として困難な状況となっています。Telegramには現在も過激派のチャンネルが存在しており、その中には過去にTelegram社へ報告されたにもかかわらず、閉鎖されていないもの（イスラム教徒を殺害するとの声明や、個人情報のさらし投稿など）もあります[17]。Telegramがモデレーションの取り組みを強化する必要があるのか、そしてモデレーションを行う際には投稿そのもののみならず、投稿が掲載されていたチャンネルやグループの背景情報も考慮する必要があるのか（例えば、投稿そのものは平和的な表現で記述されているが、過激な投稿で知られるチャンネルに掲載されている場合は、チャンネルの特性も考慮して削除の要否を決定するなど）という点については、いまだ答えは出ていません。

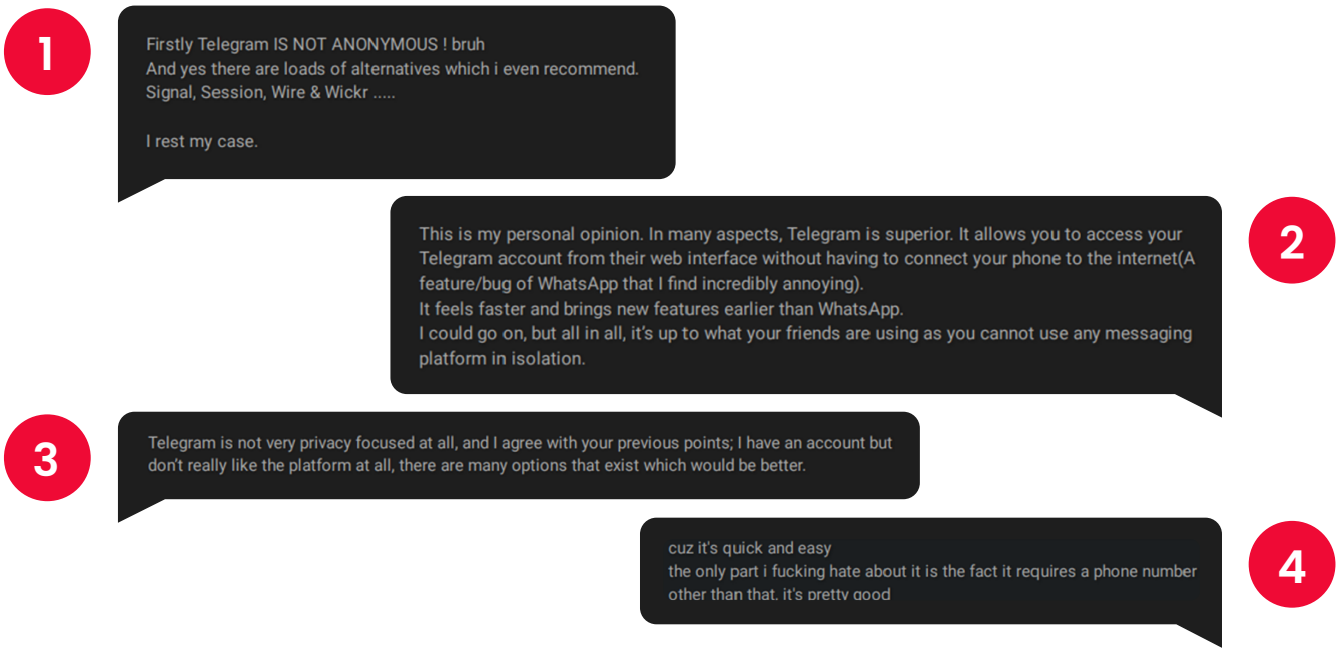
[14] How Criminals Are Tracked Down on Telegram

[15] No-SIM Signup, Auto-Delete All Chats, Topics 2.0 and More

[16] Telegram Reportedly Handed User Data to German Authorities

[17] Why right-wing extremists' favorite new platform is so dangerous

我々がサイバー犯罪者のチャットを観察した結果、彼らの多くがTelegramのユーザーフレンドリーなインターフェースや、他の競合アプリよりもいち早く新機能を導入している点を高く評価していることが明らかとなっています。Telegramのインターフェースは操作性が容易であり、ユーザーは携帯端末をインターネットに接続することなく、PCのブラウザから直接アカウントにアクセスできる仕組みとなっています。しかしその一方で、Telegramの暗号化は一部のユーザーにとって安全性が不十分であるとして、同プラットフォームのセキュリティとプライバシーに懸念を示している者もいます。また以前は、Telegramでアカウントを作成する際に電話番号を登録しなければならない点に不安を示すサイバー犯罪者もいましたが、アカウント作成における電話番号の要否についてはその後変更されています。全体的に見て、Telegramを使用する利点についてはユーザー間で様々な見解があると思われ、また一部のサイバー犯罪者は「Signal」など別のメッセージアプリを好んでいると思われます。



図：有名なサイバー犯罪フォーラム「BreachForums」でTelegramについて交わされていた会話

サイバー犯罪フォーラムと比較して、Telegramではチャンネルやグループを簡単に検索することができるようになっており、プラットフォームの検索バーに特定の単語を入力すると、その単語と関連のあるコミュニティが表示されます（例えば、「sell data」、「share data」などを検索バーに入力すると、データを売買・公開しているグループが表示されます）。一方、サイバー犯罪者の集うフォーラムやマーケットの場合、そこで扱われているデータの大半は検索エンジンでインデックス化されておらず、またサイバー犯罪グループの名称にも活動内容を示唆するような単語は使用されていないため、興味のあるグループを探す際にはより手間を要します。また、フォーラムやマーケットでコンテンツを閲覧・入手するには、まずユーザーアカウントを作成してメンバーになる必要があります（例えばフォーラムであれば、管理者による審査を受けてユーザーになるパターンと、会員費を払ってユーザーになるパターンがあります）。それと比較して、Telegramの場合は簡単にユーザー登録できることから、脅威アクターの間でますます同プラットフォームの人気が高まっています。

サイバー犯罪者がTelegramで使用する言語

インターネット上で最も多くの人が使用している言語は英語であり、サイバー犯罪者も、Telegramでは高い頻度で英語を使用しています。しかしTelegramでは、多くのグループやチャンネルが特定の地域や言語に特化しており、そういったコミュニティは英語を母語としないユーザーが自分の母語（中国語やロシア語、アラビア語など）で会話し、情報を交換できる場となっています。また、2022年11月にTelegramがアップグレードされた際、チャットに翻訳ツールが追加され、言語の壁を越えたやり取りが簡単に行えるようになりました。しかしこの多言語間でやり取りできるという機能が、さらに大規模な犯罪を可能にする世界的規模のプラットフォームへとTelegramを進化させ、また法執行機関にとってはサイバー犯罪を取り締まり、その活動を停止させることが困難になる要因となりました。

一般的に、Telegramやその他のサイバー犯罪プラットフォームで活動するサイバー犯罪者は、複数の言語の他に、技術関連の専門用語やスラング、アクロニム（例えば「NATO」や「NASA」など、複数の単語で構成される言葉やフレーズの頭文字を取って1単語のように発音するもの）を多々組み合わせて使用しています。彼らは自らの計画やテクニックを説明する際に、あえてそういった言葉使いをすることで自身の能力を誇示しています。またそういったサイバー犯罪者の中には、普段から対応する復号キーを持っている人物のみが解読できるコード化（または暗号化）したメッセージを使っている者もいます（コード化または暗号化したメッセージそのものは別のプラットフォームで生成します）。

サイバー犯罪者が愛用しているその他のメッセージサービス

サイバー犯罪者の間で他に人気のあるチャットアプリとしては、「Discord」や「Jabber」、「Tox」、「Wickr」などが挙げられますが、新しいアプリも次々に登場しています。どのアプリも独自の機能と特長を備えていますが、サイバー犯罪者に人気のアプリは、いずれも犯罪者が魅力を感じるだけのセキュリティとプライバシー保護機能を備えています。

JabberはTCP接続を使用してデータを送信するプロトコルであり、ユーザーは様々なクライアントとリアルタイムにやり取りすることができます。このJabberは、ロシア語話者のハッカーの間で最も人気の高いツールになっているものと思われ、悪名高いフォーラム「XSS」や「Exploit」には専用のJabberサーバーが存在します（それらJabberサーバーの利用を承認されたメンバーは、フォーラムにログインせずともプライバシーを強固に保護してJabberを使用できる仕組みになっています）。

Wickr Meは、AWSが所有するアプリです。同アプリにはメッセージの暗号化機能があることから、報道記者やその情報源となる人々の間で人気が高まりました。Wickr Meではユーザーがアプリ上で交わした会話を削除することができるため、後に証拠が残ることはありません。しかし法執行機関によると、いまやWickr Meは児童の性的虐待画像を共有する場として人気のプラットフォームになっているということであり[18]、Amazon社は2023年末で同アプリを終了することを発表しました。

Toxは分散型の暗号化メッセージサービスであり、電話番号や電子メールアドレスなどの個人情報を登録したり、提出する必要はありません。Toxは、P2P技術とNaCIライブラリを使用してデータを暗号化しており、Tox IDでユーザーを識別しています。またToxのクライアントでは、ボイスメッセージやスクリーンショット撮影などの機能も使用することができます。他のユーザーを連絡先に追加する場合は、そのユーザーのTox IDかQRコードを使用します。ToxのP2Pアーキテクチャでは、友達として登録されているユーザー同士は互いのIPアドレスを見ることができますが、友達として登録されていないユーザーについては、Tox IDだけをもとにIPアドレスを特定することが困難な仕組みとなっています。

Discordは、主にゲームプレイヤーが他のプレイヤーと交流する際に使用している、人気の高いチャットネットワークです。しかしその一方で、他者と連絡を取り合って不正な活動（悪意あるファイルの配布や違法行為など）を組織化しようとするサイバー犯罪者の間でも人気の高いプラットフォームとなっています。Discordはゲームプレイヤー向けのプラットフォームであり、他のユーザーと連絡をとるためには、まず「サーバー（Discord上で作成されているコミュニティ）」に参加することが必要となります。Discordでは最大50万人まで同時に通信することが可能となっているため、大規模なグループの交流や活動に適しています。

サイバー犯罪者がこれらのチャットアプリを組み合わせて使用することは、もはや彼らの活動において常識となっています。なお、コミュニティを作成する機能があるのはTelegramとDiscordだけであり、JabberやWickr、Toxは個人的なやり取りに使用されています。また、TelegramとDiscordを比較した場合、サイバー犯罪者の間ではTelegramの方が圧倒的に大きな人気を集めています。

[18] Amazon's Encrypted Chat App Faces Charges Of Child Abuse

セクション #2

サイバー犯罪活動

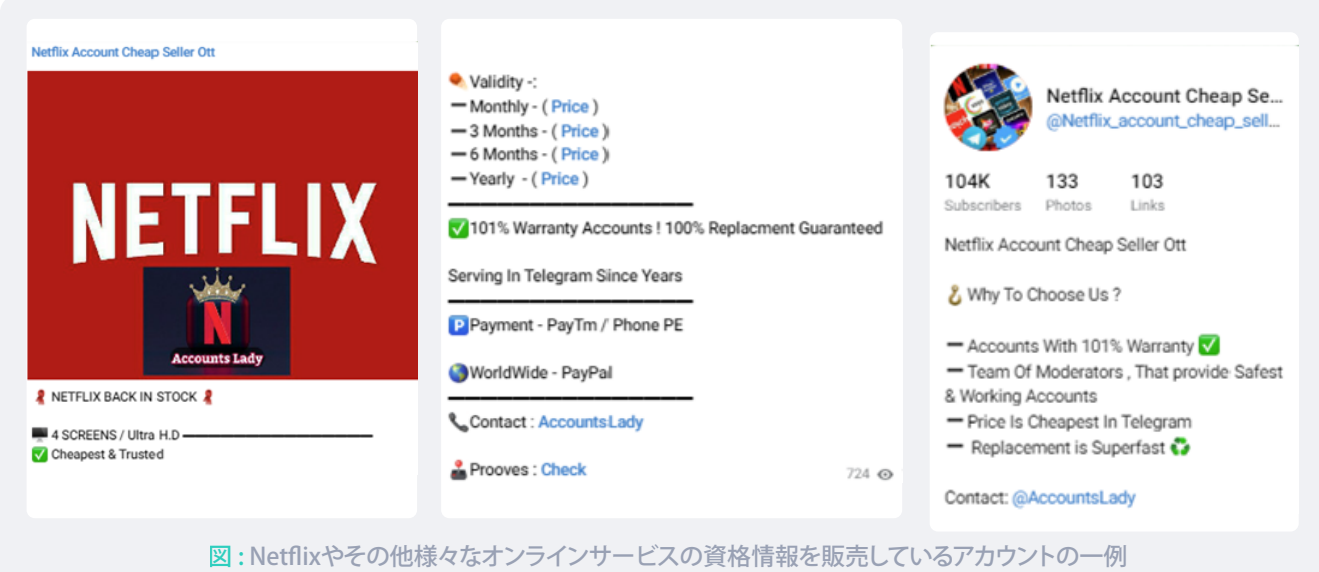
個人データと企業データ

- **個人データ**とは個人を特定することが可能となる情報を指し、氏名や住所、電話番号、電子メール、生年月日、財務情報など幅広い情報が含まれます。多くの場合、個人データは企業が事業活動を行う中で収集されています。
- **企業データ**とは企業や組織が所有する情報を指し、顧客や従業員の個人データの他、組織の財務情報や運営に関連する情報が含まれます。

Telegramのチャンネルやグループは、個人ユーザーの情報から企業の文書、ビジネス用アカウント、ソースコードにいたるまで、サイバー犯罪者が違法に入手した様々なデータを売り出し、公開するためのプラットフォームとして利用されています。2022年には、Telegramで確認できるデータがその量や多様性において、サイバー犯罪者の集うフォーラムやマーケットで見られる情報と同等であることが明らかとなりました。

窃取データの販売

Telegramでは、多数のチャンネルやグループが様々なオンラインサービスのユーザー名やパスワードを提供しています。最も出回っている資格情報としては、オンラインストリーミングや食品配送サービス、ゲーム、小売、銀行、郵便、ソーシャルメディアなどのアカウント情報が挙げられます。例えば、10万人を超える登録者を擁するチャンネル「Netflix Account Cheap Seller Ott」（下図）では、「Netflix」や「Spotify」、「YouTube」をはじめとするサービスのアカウントが売り出されており、購入希望者はアカウントの有効期間（1カ月、3カ月、6カ月など）や関心のある国（米国、英国、インドなど）などの条件をもとに、購入するアカウントを選択できる仕組みとなっています。

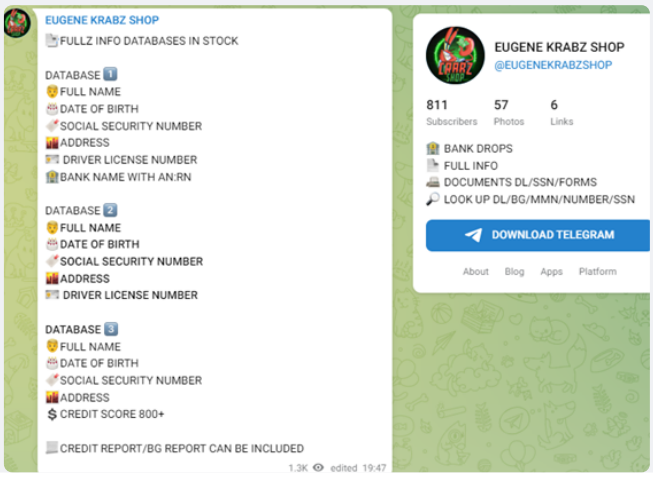


図：Netflixやその他様々なオンラインサービスの資格情報を販売しているアカウントの一例

ハッカーのコミュニティではオンラインバンキングの資格情報に大きな需要があり、Telegramでも多数のチャンネルがそういった資格情報の販売広告を掲載しています。オンラインバンキングの資格情報を専門に販売しているチャンネルについては、Telegramの検索バーやオープンソースの検索エンジンを使用して特定することができます。

サイバー犯罪者は、Telegramのチャンネルを使って様々な個人識別情報（社会保障番号や運転免許証番号、パスポート、生年月日、

住所、電子メールアドレスなど）も販売・公開しています。下図のチャンネル「Eugene Krabz Shop（@EUGENEKRABZSHOP）」ではそういった情報のデータベースが売り出されており、購入希望者は同チャンネルの管理者にメッセージを送ってデータベースを購入します。



左図の投稿では、個人の氏名や生年月日、社会保障番号、住所、運転免許証番号を含んだデータベースが複数売り出されており、その中には銀行名やクレジットカードの信用データを含んでいるものもあります。

右図の投稿では、「住宅所有者」や「保険の見込み顧客」、「高齢者向け医療保険」など様々なコンテンツのデータベースが売り出されています。また、それらデータの収集元となった国も多岐にわたっており、販売者（投稿主）は「187を超える国々から収集したデータを所有している」と主張しています。

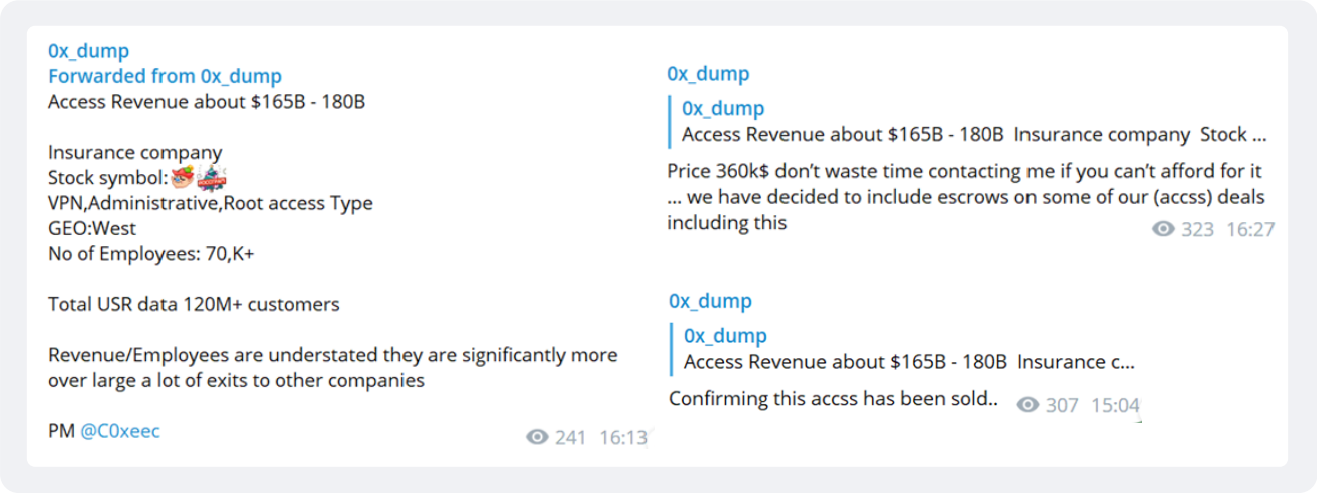
図：Telegramチャンネル「@h3lstrom」の投稿

脅威アクターは、銀行融資の契約や銀行口座の開設をはじめとする様々な詐欺行為を行う際に、第三者から窃取した資格情報を悪用することがあります。

上述した情報は、悪用されると各サービスのエンドユーザー（Netflixのユーザーや銀行口座主など）に被害をもたらすものが大半を占めています。しかしその一方で、Telegramには企業に大きなリスクをもたらすデータも大量に存在しています。例えば、Telegramで売り出されている社内リソースの初期アクセス（一般的には資格情報や侵害されたURLの形式）が社内ネットワークへの侵入経路として利用され、企業が侵害されるというパターンが考えられます。実際にTelegramでは、非公開チャンネル「0x_dump」を運営するアクターが、企業への不正アクセスに利用できる商品を定期的に宣伝しています[19]。

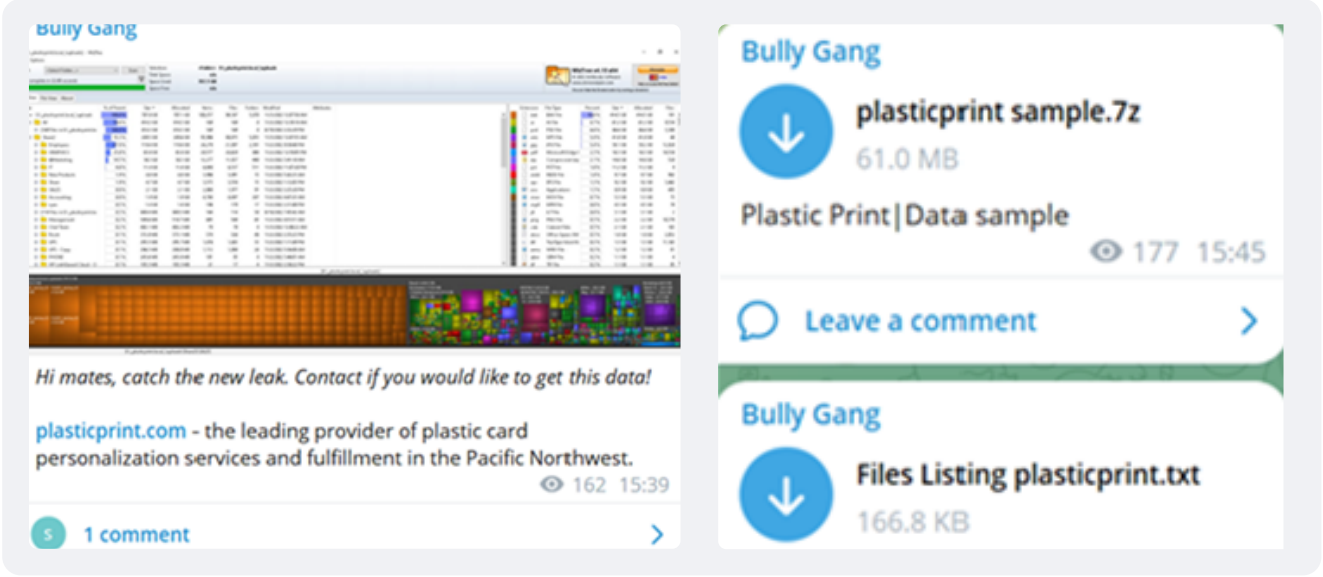
[19] チャンネル「0x_dump」の背後にいるアクターは、ケニア在住の人物であると思われ、弊社が**チャンネル「0x_dump」についてまとめたレポート**でも同アクターについて詳述しています。弊社のプラットフォームでアカウントを作成し、是非ご一読ください。

また最近同チャンネルでは、「約1,650億ドルから1,800億ドルの収益があり、1億2,000万人超の顧客を擁する保険会社のアクセス」と説明がついた商品が売り出されており、その希望販売価格は36万ドルとなっていました。
そしてこの広告が掲載された翌日、「0x_dump」はアクセスが買い取られたことを公表しました。



初期アクセスが何者かに買い取られた後は、大抵、そのアクセスを利用してネットワークや端末への不正侵入やデータの窃取が行われます。またそこで窃取されたデータは、その後売りに出されたり、リークされたりする可能性があります。

ランサムウエアグループを自称する「Bully Gang」の場合は、自らの被害組織をTelegramのチャンネル上で公表し、被害組織のものとされるデータを売りに出しています。また同グループは販売データのサンプルも掲載しています[20]（下図参照）。

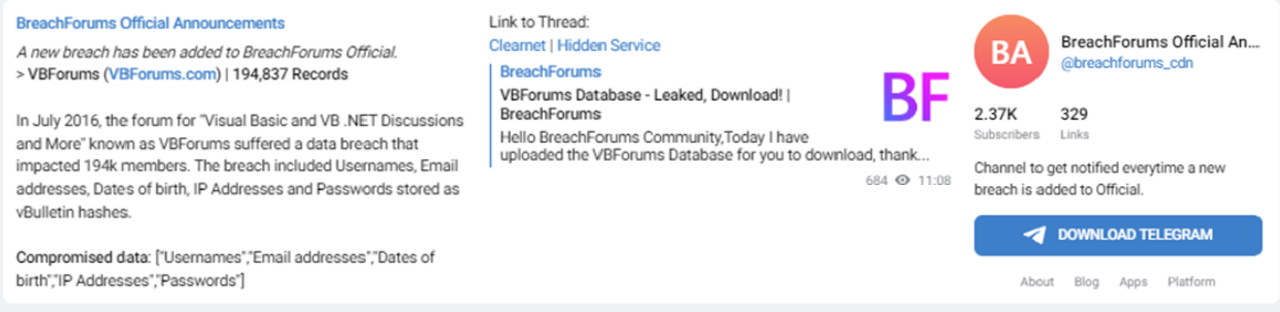


Bully Gangをはじめとするアクターが公開する企業データとしては、契約書や財務情報、人事ファイル、開発者用文書、社内用のツールやサービスの資格情報、知的財産、企業秘密、機密情報、従業員や顧客のデータなどが挙げられます。
個人データと企業データは、どちらもサイバー犯罪者から貴重な情報と見なされており、商品として売り出される他に日常的なリークの対象にもなっています。例えばTelegramのチャンネル「Leaked DataBase Breached」の場合は、運営者である脅威

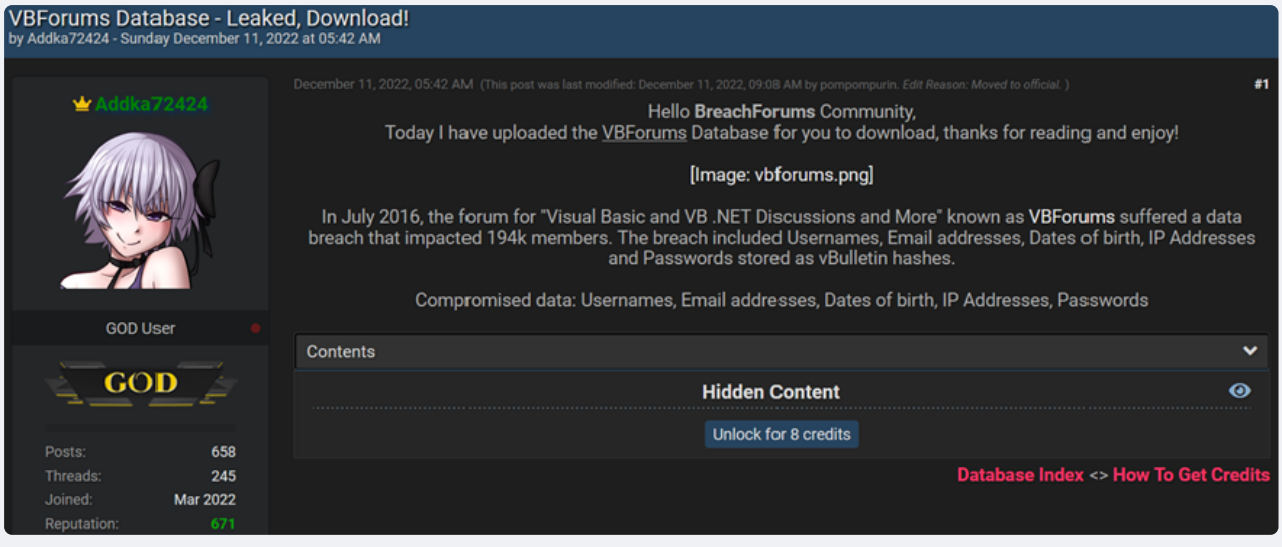
[20] Telegram上で活動しているランサムウエアグループやデータリークグループの詳細については、**「ランサムウエアグループ＆データリークグループ」の章**をご参照ください。

アクターがチャンネルにデータベースを投稿しており、チャンネル登録者はそのデータベースを無料でダウンロードできる仕組みになっています。右図は、同チャンネルに掲載されたメッセージの1つですが、そこには音楽ソフト・オーディオ機器小売業を手掛ける日本のチェーン企業のデータダンプが投稿されていること、そしてこのデータダンプには70万件を超えるデータが含まれていることが分かります。

また有名なサイバー犯罪フォーラムの中には、独自のTelegramチャンネルを作成しているところもあります。フォーラム系のチャンネルでは一般的な情報（サイトの停止や、フォーラムの新しいガイドライン、ルールの発表など）が度々発表されていますが、新たなリークデータなどのコンテンツが利用可能になった際には、その宣伝が行われています。例えば英語話者の間で人気の高いデータリークフォーラム「BreachForums」も、Telegramで公式チャンネルを作成して様々な情報を公開しています。



図：「@breachforums_cdn」が、自らのフォーラムで新たなデータベースを公開したとTelegramのチャンネルで周知している投稿



図：BreachForumsで公開された投稿のスクリーンショットが、Telegramの公開チャンネルに掲載されている様子

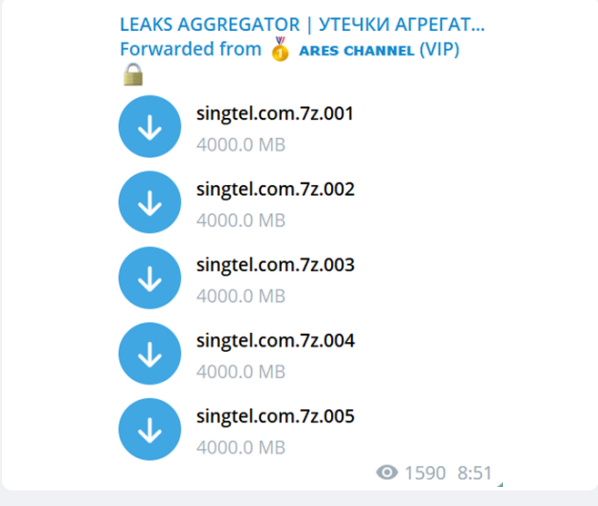
一度リークされたデータは、その後サイバー犯罪者の間で終わることなく流通・循環されます。そしてその流れの中で、Telegramが重要な役割を果たしています。

窃取データの再公開

窃取データが公開されると、大抵の場合はサイバー犯罪者の集うコミュニティで再度公開されます。その結果、窃取データを専門に扱うTelegramのグループやチャンネルで、多数の企業のデータベースが繰り返し投稿される事態となっています。Telegramでは、そういったグループやチャンネルを簡単に特定してアクセスすることが可能となっており、また該当するグループやチャンネルの中には数千人ものメンバーや登録者を擁するものも存在します。

図：企業のデータベースを公開しているTelegramチャンネル「Dataleak」と「Leaked Detabase」

また窃取データを専門とするTelegramチャンネルでは、ランサムウエアグループやデータリークグループが先に公開していたデータが頻繁に掲載されています。その一例として、ランサムウエアグループ「Clop」が攻撃を主張したシンガポールの電気通信企業「Singtel」社の事例が挙げられます。2021年2月、Singtel社のデータがClopの公式「シェイミング（さらし）」サイトで公開される事態となりましたが、我々は、その後間もなく同じデータがTelegramの非公開チャンネル「Ares Channel（VIP）」で公開され、追ってTelegramの公開チャンネル「LEAKS AGGREGATOR」でも公開されたことを確認しました。その後、何度Singtel社の情報が再公開されたのかは、もはや誰にも確認することはできません。



他にもTelegramには、多種多様なソースから収集したデータを集約して提供しているチャンネルが存在しており、窃取データを探しているユーザーが必要な情報を簡単に閲覧できる仕組みが整っています。例えば「LEAKS AGGREGATOR | УТЕЧКИ АГРЕГАТОР | БАЗЫ ДАННЫХ | СЛИВ」というチャンネルには、その名が示す通りリークされたデータが集約されています。

図：これら3件のリークデータは当初別々のTelegramソースに投稿されていたが、後に「LEAKS AGGREGATOR」に転送された。

こういったアクターの活動のおかげで、潜在的な利害関係者にとっては、サイバー犯罪プラットフォームにアクセスするよりも簡単に欲しい情報を入手することができるようになっています。サイバー犯罪フォーラムを利用する場合は、まずそのフォーラムでアカウントを作成したり、メンバー登録を行う必要がありますが、Telegramを利用する場合はTelegramのアカウントが1つあれば他に必要な登録作業はありません。そしてその結果、我々がTelegramのチャンネルやグループを調査し、そこでリークされているデータの主な出所を確認してみると、サイバー犯罪フォーラムにたどり着くという事例が多発しています。

その一例として、仏企業（axess.fr）が被ったデータリーク事件が挙げられます。同社のデータベースはサイバー犯罪フォーラム「Club Hydra Forum」に投稿された後、Telegramのチャンネル「LEAKINFORMATION」や「Leakbase.cc」、「Dataleak」でも公開されました。

図1：「Club Hydra Forum」で公開された仏企業（axess.fr）のデータベース

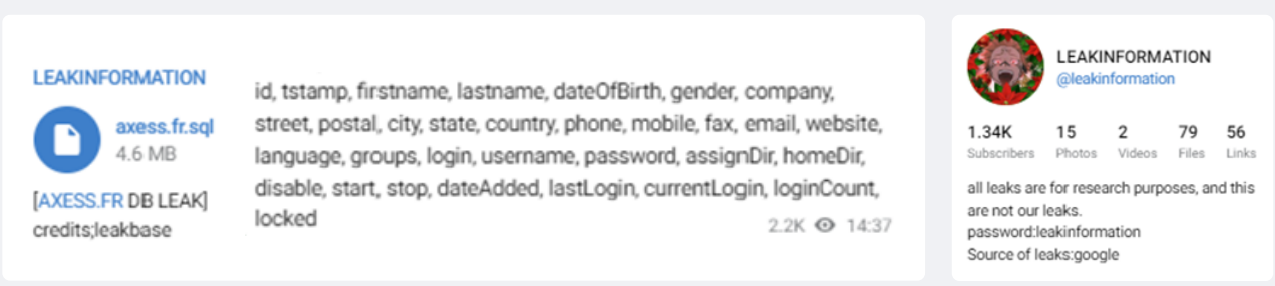


図2：「LEAKINFORMATION」で公開された仏企業（axess.fr）のデータベース

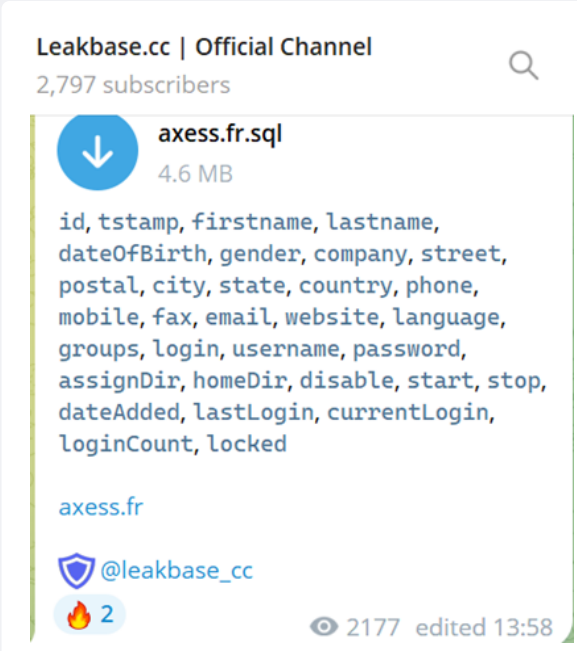


図3：「Leakbase.cc」で公開された仏企業（axess.fr）のデータベース

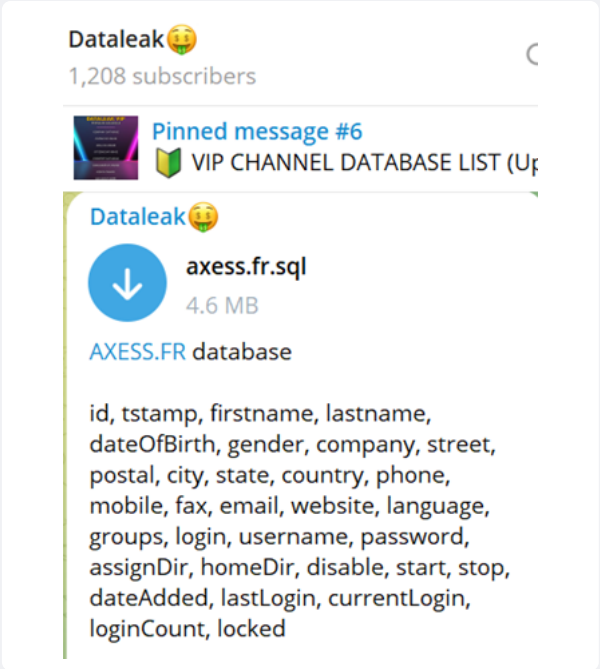


図4：「Dataleak」で公開された仏企業（axess.fr）のデータベース

特筆すべき点として、フォーラムで公開されているデータの場合、通常はデータを投稿したアクターが無料で公開すると決めた場合のみ無料で閲覧できるということが挙げられます。つまりフォーラムでデータを閲覧する場合、大抵はユーザーがフォーラムのクレジットで支払いを行う必要があり、クレジットそのものは比較的廉価であっても費用がかかることに変わりはありません。しかしTelegramであれば、大抵の場合は同じデータベースが無料で公開されています。Telegramでデータが無料公開される理由については、すでにそのデータがどこかで公開されて商品価値が下がっていること、そして初回の公開以降は他のアクターもデータを無料配信している可能性があることなどが考えられます。

本章のケーススタディについては、**ケーススタディ「SiegedSec」**をご参照ください。

有名なグループ＆チャンネルの一覧

名称	概要	メンバー・登録者	言語
Unsafe Internet	データベースを公開しているチャンネル	>1,900	英語
Dataleak	データベースを公開している非公開のチャンネル	>1,300	英語
LEAKS AGGREGATOR | УТЕЧКИ АГРЕГАТОР | БАЗЫ ДАННЫХ | СЛИВ |	データリークの集約チャンネル	>3,700	ロシア語
0x_dump	独自のデータベースをリークしている非公開のチャンネル	>900	英語
Leakbase.cc	データベースを公開しているチャンネル	>3,200	英語
A r e s ⚔️	データベースを公開・販売している非公開のチャンネル	>7,300	英語
全球数据市场 Global Data Market	データベースを販売しているチャンネル	>3,800	中国語
Leaked Detabase	データベースを公開しているチャンネル	>3,700	英語
MAKE 🏦THE💰BANDS 🇺🇸HERE🏧	銀行関連のデータや個人情報（PII）、その他を公開・販売しているグループ	>7,000	英語
Базы данных/ БД/ Утечки информации/Архив	データベースと個人情報（PII）を公開しているチャンネル	>5,000	ロシア語
Hades Database	データベースを公開・販売しているチャンネル	>1,600	英語

情報窃取マルウエア

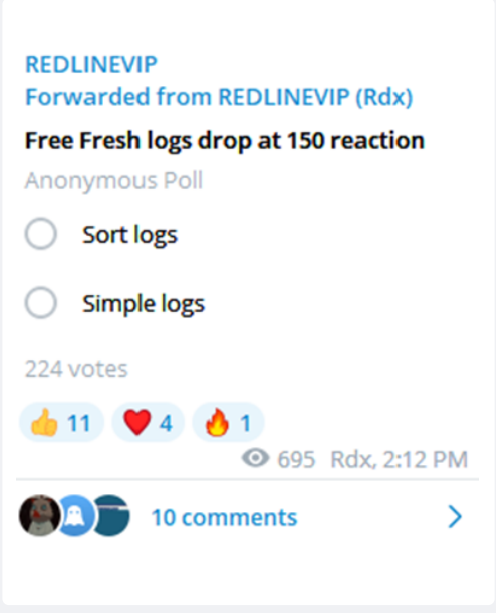
ログのクラウド（Clouds of logs）

- 一般的に**情報窃取マルウエア**は、感染した端末から資格情報を収集します。サイバー犯罪者の間では、窃取された資格情報の「パッケージ」を「**ログ**」、ログを収集した感染端末を「**ボット**」と読んでいます。ログの窃取には、**コモディティタイプ**（Redline、Raccoon、Meta、Vidar*）や**カスタムメイド、プライベートタイプ（非公開）の情報窃取マルウエア**が使われています。（*Vidarはマルウエア・アズ・ア・サービス）

- 通常、窃取される情報（ログ）としては、ユーザーのログイン資格情報や端末の情報、ブラウザの閲覧履歴、クッキー、認証トークンなどが挙げられます。脅威アクターはこれらの情報を購入することによって、感染端末ユーザーの使用している様々なリソースへ不正アクセスすることが可能となり、組織にとっては第三者にデータの窃取やネットワーク内での水平移動を行われたり、マルウエアを展開されうる重大なリスクとなります。

- ログは、ボットを自動売買するマーケット（Russian MarketやTwoEasy、Genesisなど）で売り出されている他、サイバー犯罪フォーラムをはじめとする様々なプラットフォームでも販売・リークされています。Telegramもそういったプラットフォームの1つであり、いまやログの流通において重要なチャンネルとなっています。また近年では、「ログのクラウド（clouds of logs）」という新しい種類の商品も登場しています。ログのクラウドは、脅威アクターが収集したデータのファイルに非公開のクラウドプラットフォーム経由でアクセスできるサブスクリプション形式の有料サービスです。この「クラウド型商品」の中には「MEGA」や「Yandex Disk」などのファイル共有プラットフォームでホストされているものもありますが、我々の監視活動では、サイズの大きいファイルを保存する機能のあるTelegramがこういった商品に悪用されるプラットフォームの1つとなりつつあることが観察されています。

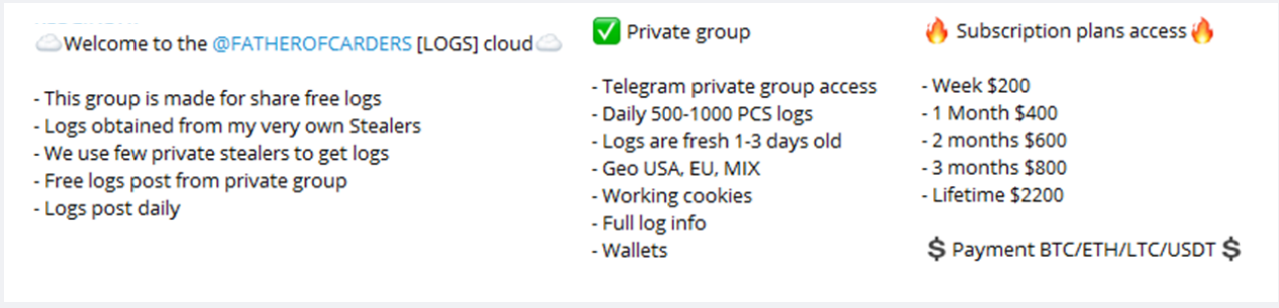
Telegramは、サイバー犯罪者が情報窃取マルウエアを使って収集したログを宣伝・販売したり、リークする場として人気のプラットフォームとなりました。いまや、様々なアクターがTelegramの機能を使って資格情報を閲覧できる専用チャンネルを作成しており、そこでは大規模なデータセットを管理したり、大量の窃取データを配信できるようになっています。合法的なファイル共有サービスを使ってログを販売する場合、サイバー犯罪者は違法な情報を速やかに削除する「モデレーション」に対処しなければなりません。しかし、Telegramはモデレーション機能が緩く、データの販売者と購入者の双方にとって魅力的なプラットフォームとなっています。また特筆すべき点として、カスタマイズした情報窃取マルウエアやコモディティタイプの情報窃取マルウエアを使って独自にログを収集し、収集したログをTelegram経由で提供しているアクターの存在が挙げられます。彼らは自らの商品を「ログのクラウド（clouds of logs）」と呼び、収集されたログを閲覧できる非公開のTelegramチャンネルへのアクセスを有料でレンタルしています。また一部のアクターは有料サービスのプロモーションの一環として、少量のログを無料で提供しています。



図：アクターによっては、プロモーションの一環で多数のリアクションを得ることと引き換えに、ログの無料ダウンロードを許可している。

一般的な「非公開のクラウド」の場合、ユーザーはチャンネル管理者に購読料を支払った後で、チャンネル（ログのクラウド）にアクセスできる仕組みとなっています。購読料はサービスを提供している脅威アクターによって異なりますが、大抵は数百米ドル（1カ月利用）から数千米ドル（終身利用）となっています。例えばチャンネル「REDLINEVIP」の場合、終身利用の価格は2,200米ドルですが、最も安い商品は200米ドル（1週間利用）となっています。その他にログを公開しているチャンネル「cBank [LOGS]」の場合は無料と有料のチャンネルを作成しており、有料チャンネルの購読料は1週間利用で100米ドル、終身利用で3,000米ドルとなっています[21]。

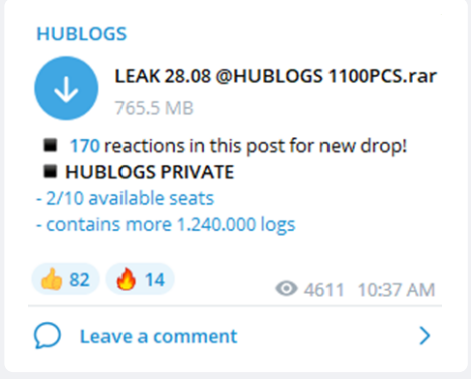
[21] チャンネル「cBank」の背後にいるアクターはロシア在住の人物であると思われ、弊社が作成したレポート**「cBank [LOGS]」**でも、同チャンネルおよび同アクターについて詳述しています。弊社のプラットフォームでアカウントを作成し、是非ご一読ください。



図：チャンネル「REDLINEVIP」で宣伝されている購読プラン

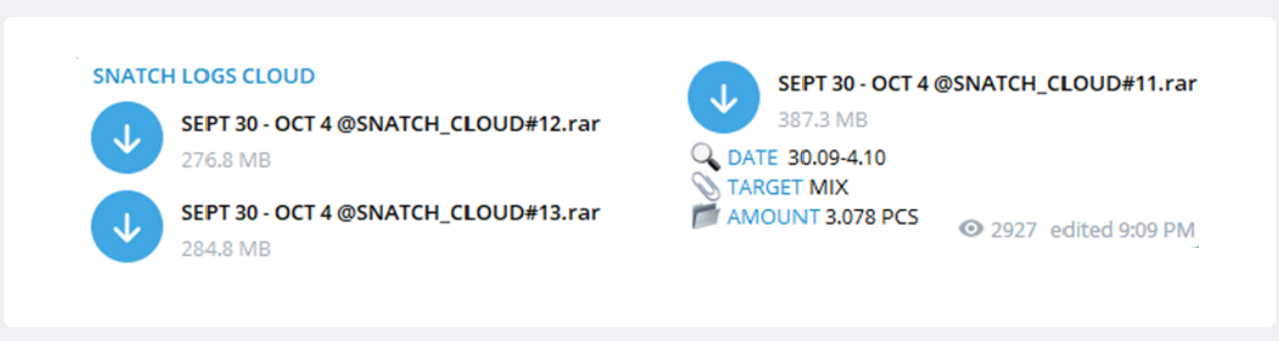
購読中に閲覧できるログの数も様々です。例えば「Snatch Premium Cloud」の場合、月額250米ドルで約9万件のログを閲覧することができます。また、より独自性の高い情報を提供するために「非公開のクラウド#1で3ユーザー利用可」などのメッセージを掲載して、ログを閲覧・購入できるユーザー数を限定しているアクターもいます。

図：「ArtHouse Cloud」では、クラウドを利用できるユーザー数を限定



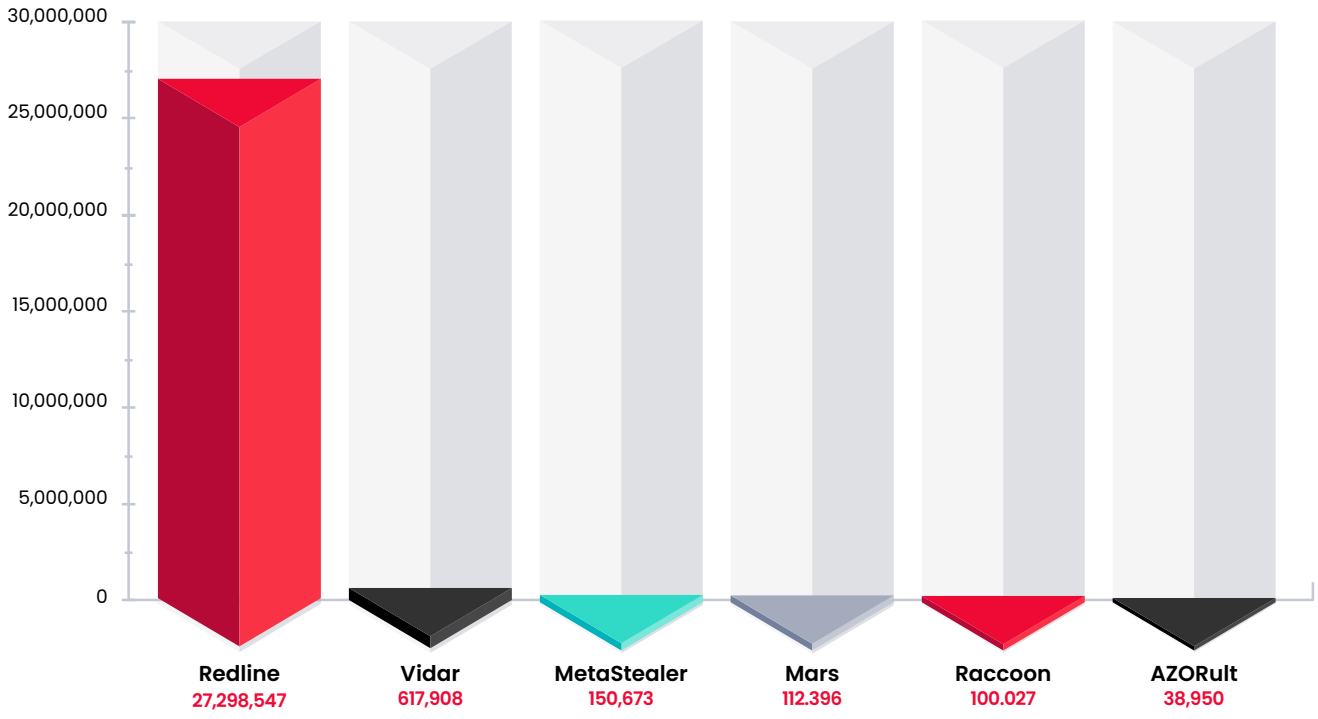
図：「HubLogsで2スロット利用可」と記載されたメッセージ

売り出されているログや無料で公開されているログの中には、ログが窃取された時間や、感染した端末の所在する地域、ログの数、ソース（情報窃取マルウエアの種類）など、リークされた経緯を知る上で役立つ情報が含まれていることがあります。



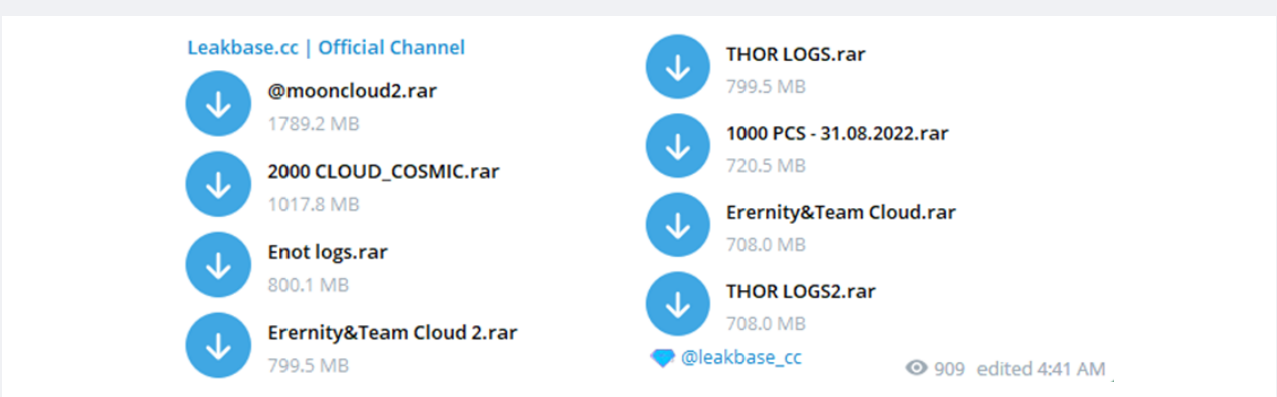
図：「Snatch Logs Cloud」で公開された投稿

我々は、Telegramで有名な「ログのクラウド」をいくつか分析する中で、調査対象となったチャンネルで公開されているログの大半は情報窃取マルウエア「Redline」を使って収集されたものであることを発見しました。



図：Telegramチャンネル「Snatch」、「REDLINEVIP」、「Cbank logs」で売り出されていたボットの分布（出典：KELA）

あらゆるデータと同じく、ログも一度無料で公開された後は、ログに特化していない他のTelegramチャンネルやグループ、その他のプラットフォームなどで広範に流通するようになります。例えば、独自のデータリークサイトを運営し、BreachForumsでもデータベースをリークしている脅威アクター「LeakBase」は、自らが攻撃を行って入手した情報や他の脅威アクターから入手した情報をTelegramのチャンネルで公開しています。LeakBaseは、データベースの他にログを集めたファイルも公開しており、大抵それらのファイルには、ログが前述の「ログのクラウド」経由で入手したものであることを示唆する名称が付けられています。つまり我々は、LeakBaseが公開している情報を確認することで、アンダーグラウンドのサイバー犯罪社会に存在する有名な「ログのクラウド」サービスを垣間見ることができるのです。



図：LeakBaseが様々なクラウドサービスからログファイルをダウンロードして公開している投稿

これまでの数年間、サイバー犯罪者は収集したログに含まれている資格情報を侵入ベクトルとして度々利用し、Uber社やT-Mobile社、Electronic Arts社などの有名企業を攻撃してきました[22]。情報窃取マルウエアを使用するアクターがTelegramを利用することによって、今後ログの購入者数がさらに増加し、その結果として被害者の数も増加の一途をたどるものと思われます。

[22] 弊社ブログ「**ディフェンダー・イン・ザ・ミドル**」をご参照ください。

情報窃取マルウエアのコミュニティ

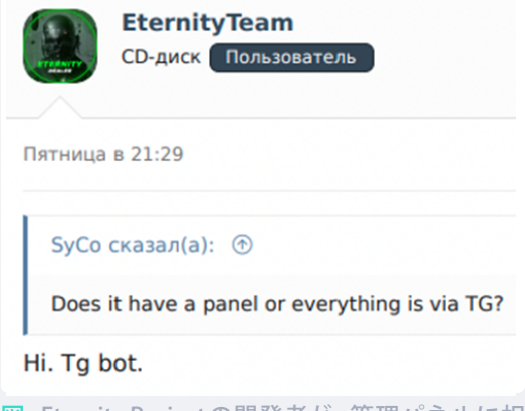
- コモディティタイプの情報窃取マルウエアは、マルウエア・アズ・ア・サービス（MaaS）形式で運営されており、ユーザーは料金を支払ってマルウエアを使用したり、管理パネルにアクセスします。そういったマルウエア・アズ・ア・サービスのオペレーションには様々な脅威アクターが関与しており、通常彼らはチームを作って複数の情報窃取マルウエアオペレーションに従事しています。まず、チームの管理者となるアクターは月額利用料（または終身利用料）を支払い、情報窃取マルウエアの使用権を入手します。その後管理者は、マルウエアを拡散するためにトラッファー（ユーザーのトラフィックを悪意あるコンテンツにリダイレクトするアクター）を雇い、トラッファーで構成したチームに「暗号化したビルド（ソースコードから作成・コンパイルされており、検知を回避するべく難読化されたマルウエア）」を提供します。ビルドを受け取ったトラッファーは、自身の所属するチームが採用している配信手法を使ってマルウエアを拡散し、感染した端末から窃取したログの質や量に応じて報酬を受け取ります。これらのログは、管理者がさらなる攻撃に使用する場合もあれば、単純に売りに出す場合もあります。

情報窃取マルウエアを操る脅威アクターがTelegramを利用する目的は、窃取したデータを販売したり、公開することに留まりません。コモディティタイプの情報窃取マルウエアが登場して以降、サイバー犯罪グループは、より多くの人々を感染させるべく他のグループと協力体制をとるようになっています。彼らの多くはTelegramのあらゆる機能を駆使して活動を組織化しており、チャンネルで新しいトラッファーの募集やチームの宣伝を行ったり、非公開のチャットやオープンチャットを活動の連携や議論を行うツールとして使用したり、ボットを使って支払いや様々なタスクを自動化しています（具体例については、次のセクションをご参照ください）。

また、コモディティタイプの情報窃取マルウエアを使ったアフィリエイトプログラムの管理者は、アフィリエイトプログラム専用のチャンネルを作成し、そこで情報窃取マルウエアの最新バージョンを発表・リリースするなど、自らの活動を宣伝するツールとしてTelegramを使用しています。2022年に情報窃取マルウエアを使った攻撃が拡大する中で、Telegramは様々な脅威アクターに感染チェーン関与の機会を与えるとともに、彼らの作業を容易にする存在となりました。マルウエアを操る攻撃者にとって、いまやTelegramは欠かせないツールとなっています[23]。

情報窃取マルウエアによるTelegramボットの悪用

情報窃取マルウエアを操る攻撃者がTelegramを利用する理由は、コミュニティを構築したり、協力体制をとるということに留まりません。Telegramでは、プラットフォーム外にある対象とやり取りを行うボットを作成することが可能となっており、このボットがいまや情報窃取マルウエアのC2（コマンド＆コントロール）インフラストラクチャにおいて重要なツールとなっています。C2インフラストラクチャの一部となっているボットは、主にマルウエアが収集したデータの保存や公開に使用されています。



図：Eternity Projectの開発者が、管理パネルに相当する機能はTelegramで対応していることを認めている投稿

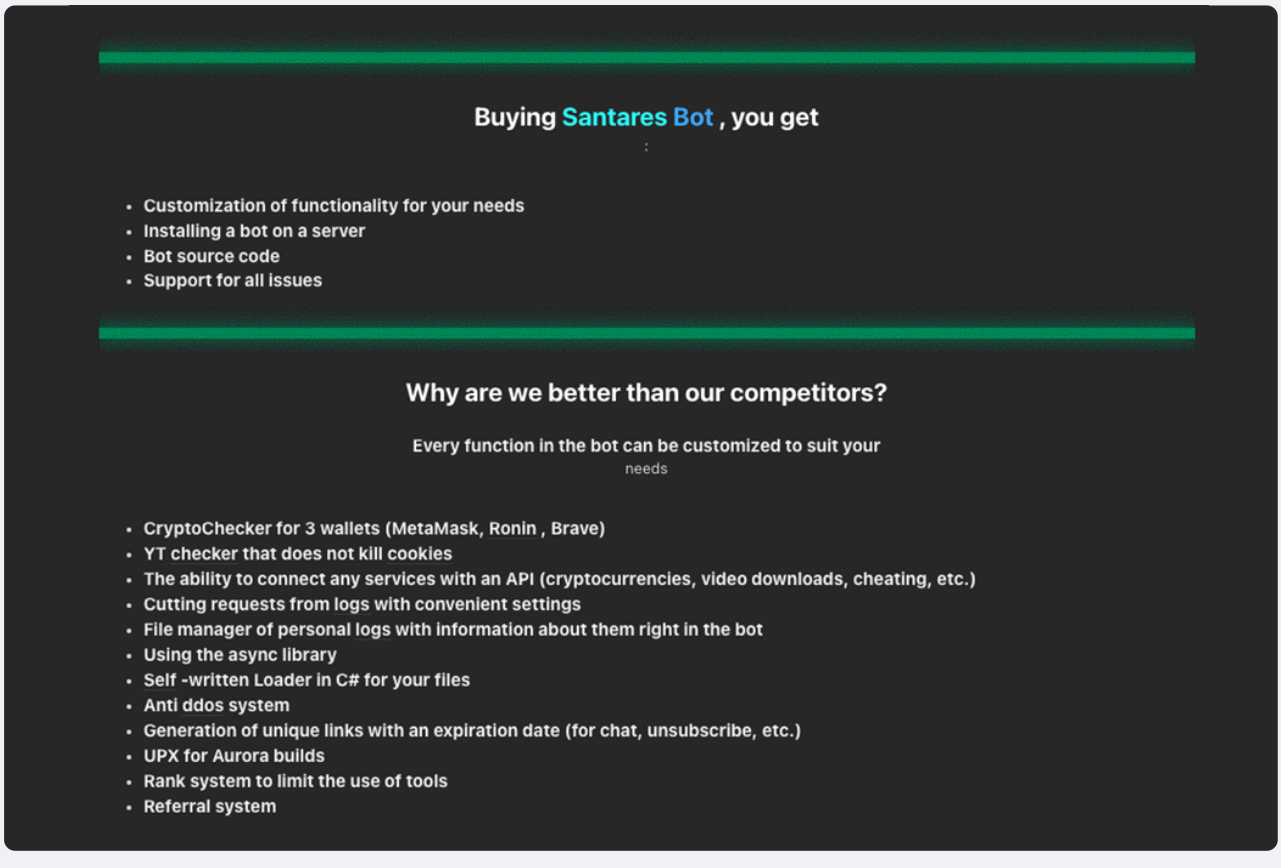
例えばマルウエア・アズ・ア・サービス「Eternity Project」では、サービスの使用料を支払ったユーザーに窃取データを販売したり、バイナリをビルドする機会を提供する手段としてTelegramのボットを使

[23] 弊社ブログ「**次世代の情報窃取マルウエア**」をご参照ください。

用しています。Eternity Projectの開発者の説明によると、彼らの情報窃取マルウエアにはマルウエアや攻撃を運用するための管理パネルが存在せず、全ての機能はTelegramを介して運用されているということです。

窃取したログをTelegram経由で提供しているプロジェクトは他にもあり、「Agrat」や「Ikarus」の他、マイナーな情報窃取マルウエアを使った多数のプロジェクトが存在します。その利用料はいずれも比較的廉価であり、終身利用で100 ～ 300米ドルとなっています。したがって、スキルが低いマルウエア開発者や活用できるリソースが少ないマルウエア開発者にとっては、Telegramを使うことでC2インフラストラクチャを手軽に構築できるようになっているものと思われます。

Telegramでは、様々なマルウエア・アズ・ア・サービスで利用可能な「情報窃取マルウエア用ボット」が、単独のサービスとしても提供されています。例えば「SantaresBot」の開発者はトラッファーグループを管理するアクターに対し、Telegramを使ってメンバーを管理するよう提案しており、その内容によると、SantaresBotを使ってビルドの配信やログの受信、ログの有効性チェック、チームメンバーとのやり取りなどの作業を自動化できるということです。また開発者によると、SantaresBotは各ユーザーに合わせてカスタマイズしたり、RedlineやRacoon、Meta、000、Auroraなどの情報窃取マルウエアと連携することができ、他の情報窃取マルウエア（窃取した情報の自動保存機能があるもの）を実装することも可能であるということです。その他にも多数のボットが類似の機能や新たな機能（無害とされるファイルにビルドを組み込むことで情報窃取マルウエアのビルドを暗号化する機能など）を提供しています。



図：SantaresBotの広告（ロシア語からの自動翻訳）

Telegramのボットは様々なマルウエアのC2インフラストラクチャとして使用されていますが、特に情報窃取マルウエアを扱う脅威アクターのコミュニティにおいて、価値の高い人気のツールとなっています。

本章のケーススタディについては、ケーススタディ「REDLINEVIP、Palm Team」をご参照ください。

有名なグループ＆チャンネルの一覧

名称	概要	メンバー・登録者	言語
REDLINEVIP	ログの閲覧は無料、 非公開クラウドの利用は有料	>6,000	英語
Snatch logs cloud	ログの閲覧は無料、 非公開クラウドの利用は有料	>5,800	英語
LOGS ARTHOUSE CLOUD	ログの閲覧は無料、 非公開クラウドの利用は有料	>5,300	英語
Cosmic CLOUD	ログの閲覧は無料、 非公開クラウドの利用は有料	<5,000	英語
HUBLOGS	ログの閲覧は無料、 非公開クラウドの利用は有料	>4,850	英語
LeakBase	ログやデータダンプの閲覧は無料、 非公開クラウドの利用は有料	>3,300	英語、 ロシア語
SHARKCLOUD	ログの無料配信	>3,100	ロシア語
DaisyCloud	ログやデータダンプの閲覧は無料、 非公開クラウドの利用は有料	<2,500	英語
Total Cloud | Агрегатор логов	ログの閲覧は無料、 非公開クラウドの利用は有料	<2,300	ロシア語
Noxy Cloud	ログの閲覧は無料、 非公開クラウドの利用は有料	>1,400	英語
METASTEALER OFFICIAL	情報窃取マルウエア 「META」を使用	>7,740	ロシア語

AURORA BOTNET | STEALER	情報窃取マルウエア「Aurora」を使用	>3,300	ロシア語、英語
Blackwalter	情報窃取マルウエア「Blackwalter」を使用	>1,800	英語
Eternity	情報窃取マルウエア「Eternity」を使用	>1,200	ロシア語、英語
Rhadamanthys	情報窃取マルウエア「Rhadamanthys」を使用	<1,350	英語
REIMANN CHAT	REIMANNのチャット	<1,200	ロシア語
РАЙ ТРАФЕРА	Traffers Paradiseのチャット	<240	ロシア語
Palm Team	Palm Teamのチャット	<200	ロシア語
OverDox Team	OverDox Teamが提供しているサービス	170	ロシア語
Sky Team	Sky TeamでSEOを担当しているサブチーム	25	ロシア語

銀行詐欺

- **銀行詐欺とは、金融機関やその従業員、顧客を標的とした犯罪行為を指します。銀行詐欺はフィッシングなどの一般的な攻撃手法の他、以下に挙げる金融業界に特化した手口をはじめとする様々な手法で行われています。**
  - **クレジットカードのスキミング** — PoS端末やATMマシンのカードリーダーに専用の機器を接続し、クレジットカード情報を窃取します（ただし他の手法でカード情報を窃取する場合もあります）。
  - **カードのクラッキング** — 窃取した（または侵害した）クレジットカードやデビッドカードの情報を用いて、不正な購入や金銭の引出を行います。
  - **マネーミュール** — 複数の取引を介して、違法行為で得た金銭の出所を隠蔽し、送金します。

銀行を標的とするサイバー犯罪においては、上記以外のスラングも一般的に使われています。例えば「シマー（shimmer）」という用語は、被害者がクレジットカードやデビッドカードをATMやカードリーダーに挿入した時に、カードの磁気ストライプから情報を窃取する機器を指します。「フルズ（fullz）」は、個人情報窃取に関連する犯罪で頻繁に使われている用語であり、犯罪者が詐欺やその他の違法行為に使用する「個人情報のセット」を指します。フルズに含まれている可能性のある情報としては、個人の氏名や住所、誕生日、社会保障番号、金融機関の口座番号などが挙げられます。フルズは、脅威アクターが金融機関で口座を開設したり、不正な購入・金銭引出などを行う際に悪用される可能性があります。

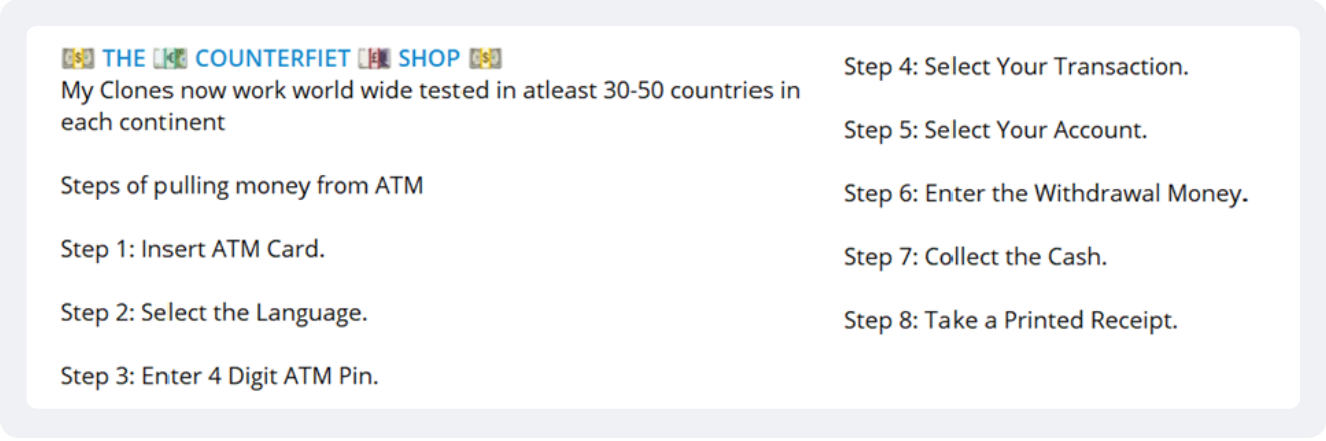
- **クレジットカードマーケットとは、様々な種類のクレジットカードを販売しているプラットフォームを指します。クレジットカードマーケットの具体例としては、「Omerta」や「Brian's Club」、「Yale Lodge」などが挙げられます。アンダーグラウンドのクレジットカードマーケットで販売されている「商品」の中には、侵害されたカード情報とそのCVV/CVV2情報（電話やオンラインで商品やサービスを購入する際に使用する、3桁または4桁のセキュリティコード）がセットになっているものがあります。こういった「セット商品」は、匿名性を保った「非対面取引」で即座に悪用できること、またカード情報以外の個人情報が含まれている可能性があることなどからサイバー犯罪者の間で最も人気があります。**

その他、様々な手口に悪用可能な小切手も重要な商品となっています。例えば脅威アクターが個人や企業に対して詐欺行為を働く際、小切手を偽造して使用することがあります。

またサイバー犯罪者は、銀行詐欺のチュートリアルも作成しています。それらのチュートリアルでは、銀行口座の開設・管理方法やクレジットカード情報の窃取方法の他、小切手を偽造して個人や企業を騙す方法などを解説しています。このようなチュートリアルは、銀行詐欺を始めたばかりのアクターや、銀行詐欺の全てについて詳しく知りたい個人が利用していると思われます。

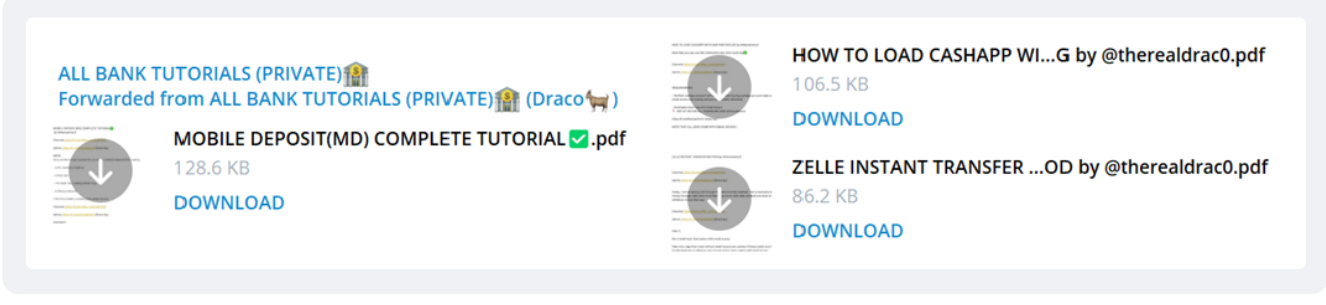
- **銀行のログとは、個人が銀行口座にログインする際に必要となる情報（ユーザー名や電子メールアドレス、クッキー、アカウントの詳細など）を指します。サイバー犯罪者は偽のログインサイトを作成し、その偽サイトの情報をフィッシングメールで被害者に送信します。被害者がこの偽サイトへアクセスしてログイン情報を入力すると、サイバー犯罪者が入力された情報を取得し、詐欺行為に利用します。**

そして上述した活動はいずれも、ここ数年の間にTelegramでも行われるようになってきました。Telegramは、銀行詐欺を行うサイバー犯罪者の間でいまや人気のプラットフォームとなっており、彼らは専用のチャンネルを作成して、(窃取した) クレジットカードや小切手、フルズ、金融機関のアカウントなどの商品を宣伝しています。また、偽造クレジットカードや偽造紙幣なども人気の商品となっており、ユーザーの中には「複製したATMカードとPIN番号」をセット商品にし、その使用方法を明記して販売している者もいます。

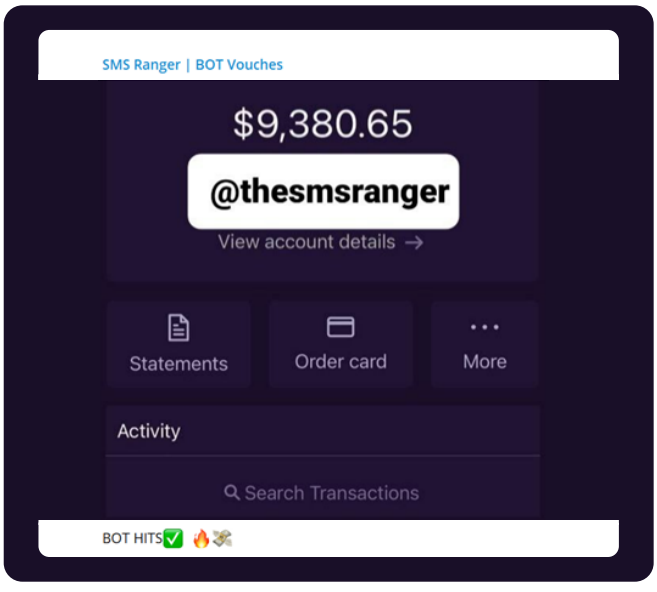


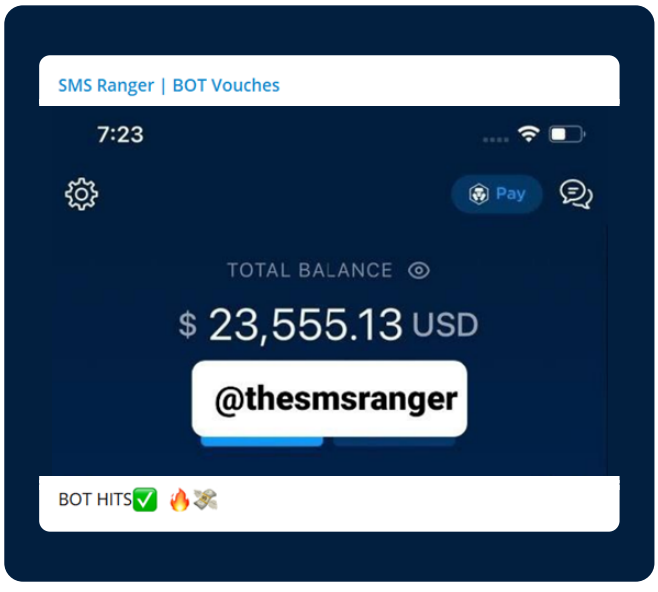
Telegramには、偽造小切手や窃取した有効な小切手を専門に扱うチャンネルも多数存在します。不正な小切手を扱う詐欺スキームの場合、詐欺師は他のサイバー犯罪者などに偽造 (または窃取した) 小切手や為替を送り、その小切手や為替を受取人の銀行口座に入金させます。その後、銀行口座に入金された金銭の一部を現金または電信送金で自分 (詐欺師) に送るよう指示します。

アクターは自らの知識を他者と共有することを好むため、Telegramでは銀行詐欺のチュートリアルも出回っています。例えば、チャンネル「ALL BANK TUTORIALS (PRIVATE)」の管理者は、自らが所有しているチュートリアルの一部を公開しています。



いまや脅威アクターは、Telegramのボットを使って様々な攻撃を自動化できるようになっており、銀行利用者を標的としたオペレーションもその1つとなっています。彼らは自動ボットを使用してメッセージを送信することで、多数の被害者とより効率的に連絡をとったり、他のサイバー犯罪者に「有償の仕事」としてソーシャルエンジニアリングを依頼することができるようになっています。例えば、約7,700人の登録者を擁するTelegramチャンネル「SMS Ranger | Updates」は、企業や銀行になりすまして被害者からワンタイムパスワード (OTP) やSMSコードを窃取するボット「SMSRanger」を提供しています。また同チャンネルの管理者は、彼らのボットの活動が成功した証拠となる事例を宣伝の一環としてチャンネルに掲載しています。





同チャンネルに記載されている説明によると、彼らのボット「SMSRanger」には、標的となる人物に連絡をとって様々な情報（ワンタイムパスワードや資格情報など）を窃取する機能があるようです。

1. ”自分好みにOTPを活用しよう”
2. ”SMSRangerから被害者に電話をかけよう”
3. “被害者のカード情報やログインアカウント情報を使用し、指示にしたがって被害者にOTPを送信しよう”
4. ”被害者がOTPを入力すると、我々のボットがOTPをゲット”

このボットは月額399米ドル、終身利用の場合は1,900米ドルで提供されています。

本章のケーススタディについては、「ケーススタディ「CHECKS GRUB SHOP」をご参照ください。

有名なグループ＆チャンネルの一覧

名称	概要	メンバー・登録者	言語
The Bank®	窃取したクレジットカード情報を販売しているチャンネル	>3,940	英語
CHECKS GRUB SHOP	窃取したクレジットカード情報を販売しているチャンネル	>8,180	英語
WhiteList	窃取したアカウント情報を販売しているチャンネル	>6,700	英語
FraudStars	窃取したクレジットカード情報を販売しているチャンネル	>9,600	英語
BioH4zard Market	窃取したクレジットカード情報を販売しているチャンネル	>3,800	英語
CHECKS AND SAUCE	小切手を販売しているチャンネル	>980	英語
The Glass House	小切手を販売しているチャンネル	>2,300	英語
Glass Tank Grubs	小切手を販売しているチャンネル	>2,160	英語
FREE GUIDES	銀行詐欺のチュートリアルを公開しているチャンネル	>680	英語

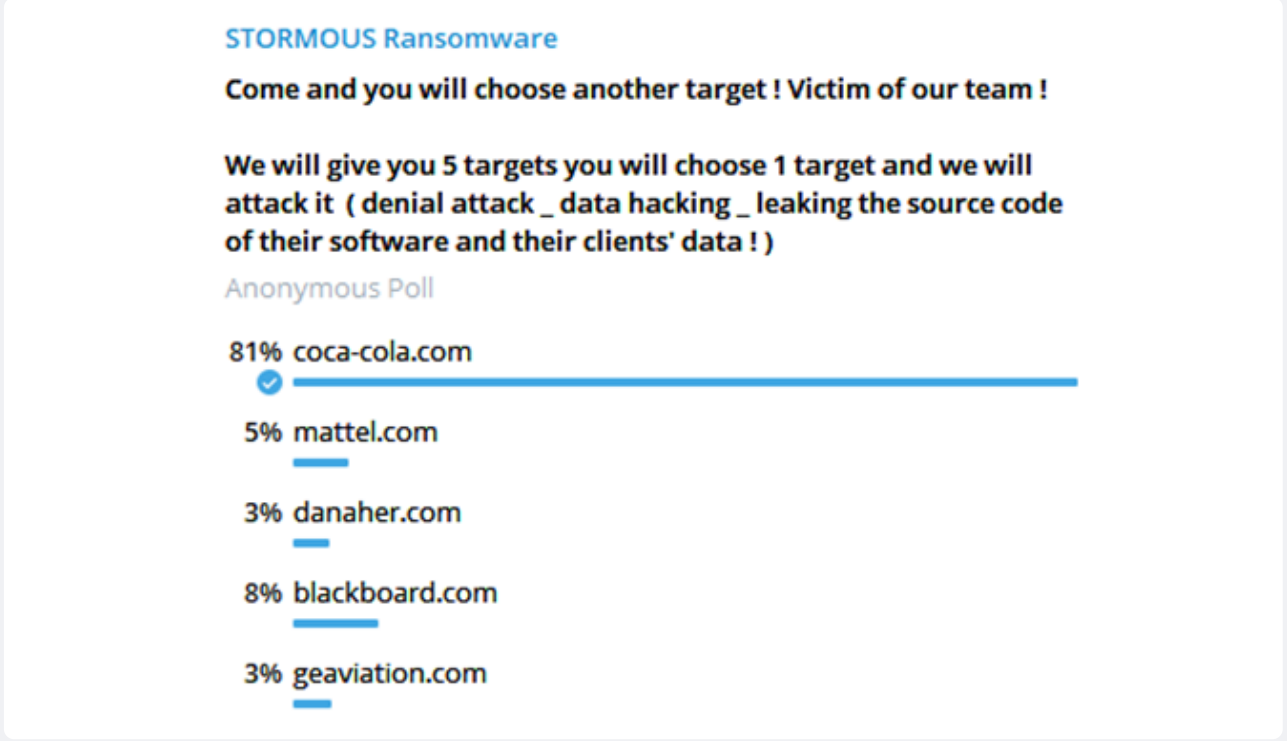
ランサムウエアグループ
&データリークグループ

- **ランサムウエアグループやデータリークグループ**とは、組織から機密データを窃取して身代金を要求し、「支払わなければデータをリークする」と恐喝行為を行うサイバー犯罪グループを指します。ただし、ランサムウエアグループはランサムウエアを使ってデータを暗号化しますが、データリークグループの場合はランサムウエアを使った暗号化は行わず、あくまでデータを窃取するのみに留まります。また一部のグループは、窃取データを部分的にリークしたり、第三者へ販売するためのブログを運営しています。

ランサムウエアグループやデータリークグループが運営するブログに加え、いまやTelegramも、彼らが自らの攻撃や能力を宣伝する場として利用できる魅力的なプラットフォームとなっています。その理由として、彼らが運営しているブログはそのほとんどがTOR上にあるため、Telegramでデータをリークしたほうがより多くの人にアクセスしてもらえるということが挙げられます（クリアウェブ版のブログを運営しているグループも存在しますが、この類のブログはプロバイダーから直ちにブロックされます）。またデータをリークするという作業そのものにおいても、Telegramではユーザーが大量のデータをアップロードすることが許可されており、これもランサムウエアグループやデータリークグループにとって重要なポイントとなっています。

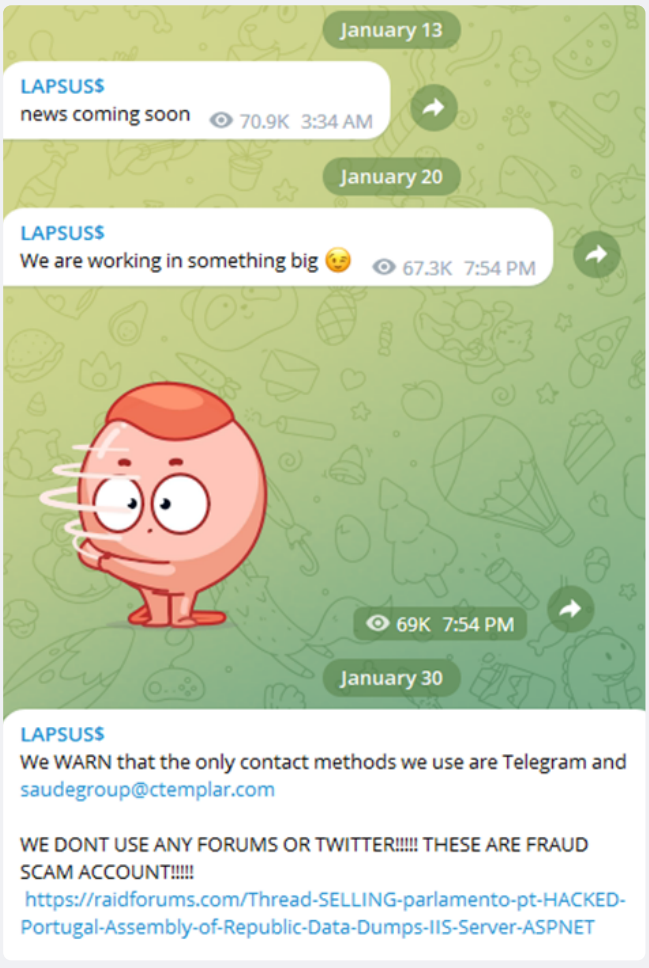
「RansomHouse」をはじめとする一部のグループは、独自のブログに加えてTelegramでチャンネルを運営し、両方で同じデータをリークしています。しかし2022年においては、ブログを運営せずTelegramだけを使用しているデータリークグループが、有名企業に対する攻撃を主張して人気を集めました。また彼らは、各攻撃の後にTelegramのチャンネルで被害組織のものとされるデータを公開し、被害組織に身代金を支払わせようと試みていました。

それらグループの中でも最も悪名高いとされているのが、「Lapsus$」と「Stormous」です。両グループは2021年に登場し、2022年に入って大きな注目を集めました。彼らはTelegramの機能を広範に利用して、自らが行ったとする攻撃の情報を公開し、特定の被害組織のデータをリークする専用チャンネルや議論用のチャットを作成しました。また、チャンネルに参加するTelegramユーザーの活動を活発化すべく「投票」も実施しており、例えば2022年4月にはStormousが自らのTelegramチャンネルで投票を開催し、次の標的とすべき組織を選ぶようチャンネル登録者に呼びかけていた様子が観察されています。

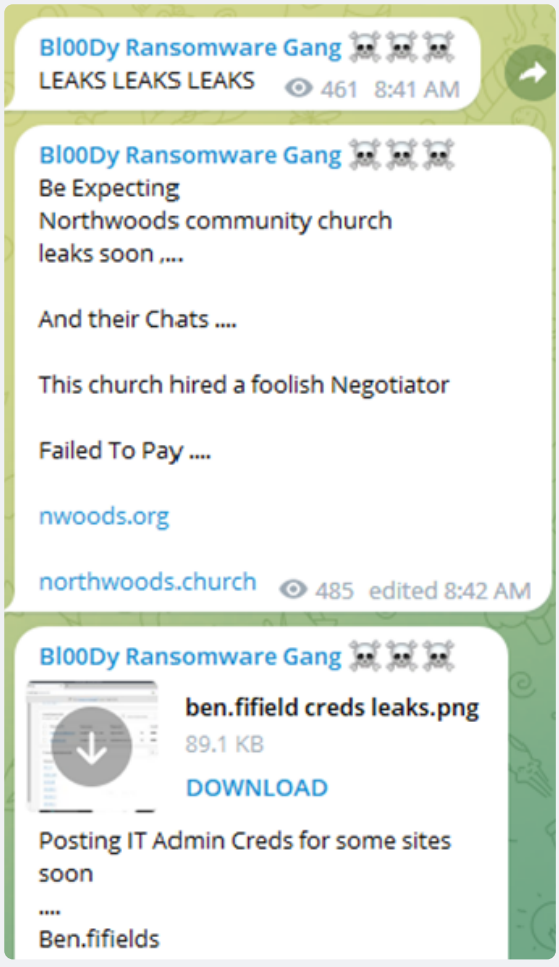


図：Stormousが、次の標的を選ぶようチャンネル登録者に呼びかけている投稿

ランサムウエアグループやデータリークグループのブログの場合は、1つの投稿に1つの被害組織が掲載されていますが、Telegramのチャンネルを利用していたLapsus$やStormousの場合は、1つの攻撃や被害組織について複数のメッセージを公開し、話題を呼ぶことに成功していました。例えばLapsus$の場合は、1つの被害組織のスクリーンショットをチャンネル上で日々公開し、自らのコミュニティのメンバーがその攻撃（リーク）について議論するよう扇動していました。



図：Lapsus$が自らの活動に話題を呼ぼうとしている投稿



図：2022年に登場したBl00dy Ransomware Gangが、1つの被害組織について複数のメッセージを投稿している様子

ランサムウエアグループやデータリークグループの場合、Telegramを主要ツールとして使用しているのはそれほど高度なスキルを有していないアクターであると思われます。また彼らのほとんどは、同じような言葉遣いで人々の注目を集め、ソーシャルメディアを使ってフォロワーと交流しています。こういったグループの信頼性については常に疑問の余地があり、例えばStormousについては、同グループが攻撃を主張した被害組織の大半を本当に彼ら自身で攻撃したのかがほぼ明らかになっていません。さらに我々の調査では、Stormousが自らのチャンネルでリークしたデータが、過去にサイバー犯罪フォーラムで公開されていたことを確認しています。

本章のケーススタディについては、ケーススタディ「Lapsus$」をご参照ください。

有名なグループ＆チャンネルの一覧

名称	概要	メンバー・登録者	言語
Lapsus$	データリークグループ	>55,800	英語
Stormous	データリークグループ	>2,900	英語
RansomHouse	データリークグループ	>2,000	英語
Bl00dy Ransomware Gang	ランサムウエアグループ	>1,300	英語
Bully	ランサムウエアグループ	>600	英語

ハクティビズム

- ハクティビズムとは、政治活動家や社会活動家がコンピューターを悪用して自らの理念やイデオロギーを支持し、声明を出す行為を指します。コンピューターやネットワークを侵害する行為はハッキングと呼ばれ、イデオロギーや社会的見解を擁護・推進する行為はアクティビズム（積極的行動主義）と呼ばれますが、ハクティビズムはこの2つを組み合わせた行為です。ハクティビストは、「自らの理念や信念を脅かす存在である」と彼らが信じる全ての人や組織を敵対視します。また、彼らは政府や機関を標的にする傾向がありますが、企業や宗教団体に対して敵対的な活動を行う場合もあります。その他、自らの理念に対する認知度を高めたり、メッセージを送るといった目的でも行動を起こします。いかなる組織も、組織として行う活動や、組織が属する国の政府が行う活動が特定のハクティビストグループのイデオロギーに反する場合は、彼らの標的となる可能性があります。

Telegramがハクティビストの間で広く普及した理由は、金銭的動機に基づいて活動するサイバー犯罪者と同じく、独自のグループやチャンネルを介して多数の人々とやり取りでき、なおかつプラットフォームのモデレーションポリシーが緩いところにあると思われます。言い換えると、Telegramは聴衆の注目を集め、違法行為を公開し、彼らの誘導に従って活動するよう他者を扇動するハクティビストにとってふさわしいプラットフォームであると考えられます。

ここ数年は多数のハクティビストが頻繁にTelegramを使用していますが、2022年は、主にロシア・ウクライナ間の戦争を理由に同プラットフォームを利用するグループの数が急増したようです。Check Point社の研究者からは、両国の戦争が始まった最初の10日間で、同戦争に関連するTelegramグループの数が6倍に増加したこと、そしてそれ以降も日々新たなグループが作成され、そのうちのいくつかは25万人を超えるユーザーを擁していることが報告されています[24]。この戦争が始まって以来、親ロシア派グループと親ウクライナ派グループの両方がTelegramを頻繁に利用して自らの攻撃を公表し、支援を募っています。

また2022年は、年末に向けてイランでも地政学的事件（反政府デモ）が発生しました。ロシア・ウクライナ間の戦争と同様にこの反政府デモも、事件に共感したハクティビストによるTelegramの使用率向上につながったことは間違いありません。

ハクティビストが運営するチャンネルやグループで最も頻繁に掲載されている投稿としては、一般的な議論やニュースの他、彼らが行ったDDoS攻撃やWebサイトの改ざん、ドキシング（個人情報などのさらし）、情報窃取に関するものが挙げられます。

結論として、Telegramを利用するハクティビストグループの数は2022年に急増しており、彼らの間では同プラットフォームに対する人気が現在も続いている傾向にあるといえます。また地政学的な紛争が続いていること、そしてハクティビストが一般のインターネットユーザーからの支援を切望していることを考えると、Telegramに対する人気は近い将来も続くと予想されます。

本章のケーススタディについては、ケーススタディ「Killnet、ALtahrea Team」をご参照ください。

24 Telegram becomes a digital forefront in the Conflict

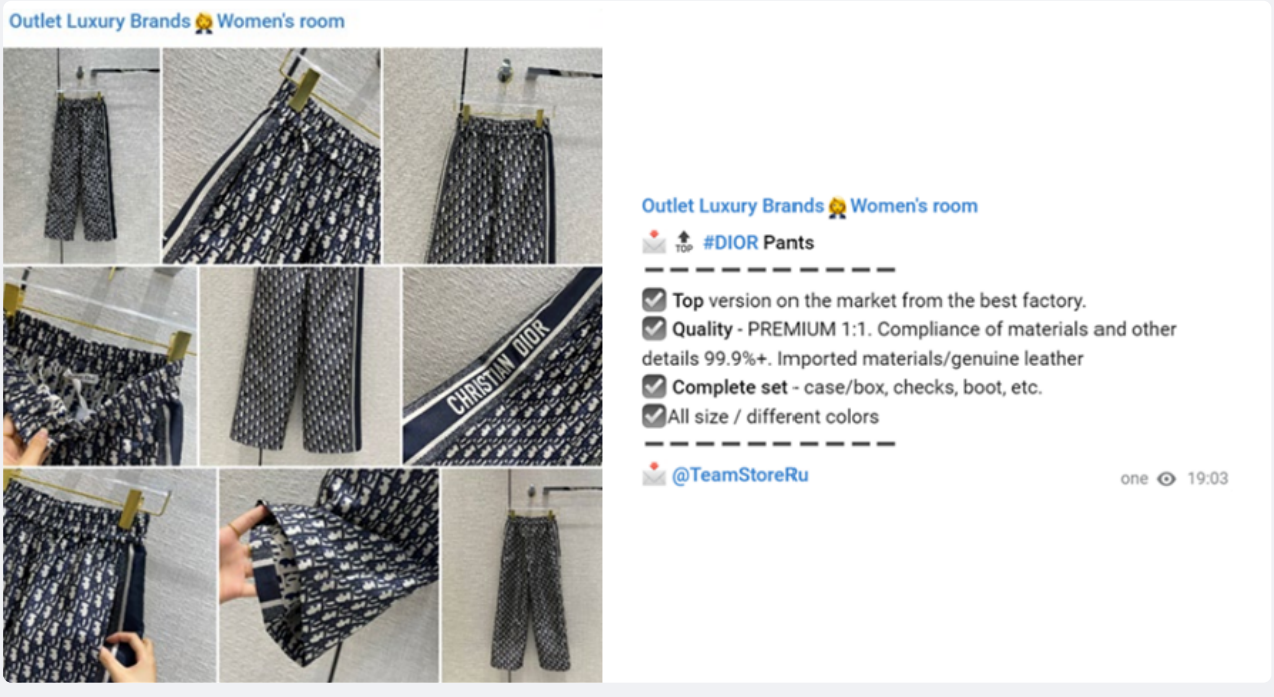
有名なグループ＆チャンネルの一覧

名称	概要	メンバー・登録者	言語
IT ARMY of Ukraine	親**ウクライナ**派の有志による運動	> 206,000	ウクライナ語
Killnet	親ロシア派による運動。 主にDDoS攻撃を実行	> 91,300	ロシア語
RaHDit	ウクライナ兵士の個人情報を 暴露している親ロシア派グループ	> 69,000	ロシア語
Cyber Partisans	ベラルーシの野党支持派による運動。 主にベラルーシ政府を攻撃	> 43,400	ベラルーシ語、 ロシア語
XakNet	偵察グループ	> 36,500	ロシア語
Anonymous	国際的ハッカー集団	> 19,800	英語
1877 Team	様々な攻撃を実行している 親クルド派グループ	>17,800	英語、 アラビア語
Anonymous Russia	主にDDoS攻撃を実行している 親ロシア派グループ	> 12,500	ロシア語
Altahrea Team	DDoS攻撃やウェブサイト改ざんを 行う親イラン派グループ	> 4,900	英語、 アラビア語
Phoenix	DDoS攻撃やウェブサイト改ざんを 行う親イラン派グループ	> 1,300	ロシア語

違法な有形商品

高級品のコピー商品

Telegramでは、多岐にわたるコピー商品が様々なチャンネルやグループ、ユーザーを介して販売されています。その中でも高級品のコピー商品は、本レポートで取り上げるのに最適な事例と言えるでしょう。Telegramではコピー商品が公然と宣伝されており、またそこには商品の品質レベルに関する説明も記載されています[25]。例えば、Telegramのチャンネル「Outlet Luxury Brands Women's Room」は、シャネルやクリスチャン・ディオール、バルマン、セリーヌ、ルイ・ヴィトンをはじめ、幅広い高級ブランドのコピー商品（衣料品）を販売しています。同チャンネルを運営している詐欺師の説明によると、彼らの商品は「素材やその他のディーテルはオリジナルの製品に99.9%準拠している」ということです。



図：クリスチャン・ディオールのコピー商品を宣伝しているTelegramの投稿（ロシア語からの自動翻訳）

新型コロナウイルス関連文書

パンデミックが続く中、新型コロナウイルス感染者数の世界的な増加を受けて、ブラックマーケットでは偽のウイルス検査キットやワクチン接種証明書（偽造した証明書や違法に発行された正式な証明書）の数が急増し、その一部は75～ 600米ドルで販売されていました。一方Telegramでは、現在もウイルス検査キットやワクチン接種証明書を販売しているグループが多数存在しており、いまや新型コロナウイルス関連の詐欺商品の販売において、最大規模を誇るプラットフォームの1つとなっています。この分野で行われている詐欺は非常に悪質であり、販売者の中には代金受領後に商品を発送することなく姿を消したり、即座に偽物と認識できるほど低品質な証明書を提供している者もいます。

このような新型コロナウイルス関連の詐欺商品を扱うグループやチャンネルには、何千人もの人々が参加しています。例えば、2022年7月28日に作成されたチャンネル「Registered Digital COVID-19 Cert」には、9,000人を超えるユーザーがチャンネル登録しています。同チャンネルの管理者である「@DrGeorgelowe」は、別のチャンネル「UK NHS COVID-19 Vaccine Cert」も運営しており、おそらくこの分野においては、1人のアクターが各商品を専門とするグループを複数運営するというパターンが数多く発生しているものと思われます。

25 弊社のブログ「Top Luxury Brands in France：Threat Landscape Report」をご参照ください。

新型コロナウイルス関連の詐欺商品を扱うチャンネルの管理者は、より多くのチャンネル登録者を獲得しようと人々の恐怖心をあおる広告を掲載しています（下図参照）。

UK NHS COVID-19 Vaccine Cert

It all started just one day after the biontech vaccination !!! terrible itching, sleepless nights ... the dermatologist diagnosed me with "psoriasis plantaris and lichen planus". Vaccination was on July 15th. , so far everything has gotten even worse ... so a catastrophe I reported side effects at the Paul Ehrlich Institute.

I will always be honest. Even though I'm a doctor, but I'm telling you the vaccine is no good. Contact us now and get your proof of vaccination without taking the vaccine.

ドラッグ

オンラインのドラッグ売買も、いまや巨大なマーケットとなっています。その理由として、購入者にとっては対面売買にはない以下のメリットがあることが挙げられます。

- 匿名性の保持（偽名を使用し、暗号化された安全な接続を介してドラッグを購入することができます）
- 暴力を受けるリスクの低減（犯罪多発地域で営業しているディーラーから対面で購入する場合は、暴力を受けるリスクが伴います）
- 品質の確認（ドラッグをオンライン販売しているユーザーについては、その商品に対する評判や評価を事前にチェックすることができます）

図：ドラッグの販売者が投稿した配送商品の証拠画像

オンラインでドラッグを購入できるサービスは、大抵の場合、サイバー犯罪を専門とするマーケットや有形商品を幅広く取り扱うマーケットなどで発見することができます。ただしそれらプラットフォームの大半はTOR上で運営されているため、一般のインターネットユーザーがマーケットを特定してアクセスするにはハードルが伴います。一方Telegram上でドラッグを購入する場合、購入者は数クリックで購買プロセスを完了することができ、サイバー犯罪のエコシステムに関する知識も必要ありません。またTelegramの場合、プラットフォームの検索バーやドラッグ販売者からの情報が集約されたチャンネルを使用して、ドラッグを購入できるチャンネルを特定することができます。

「@gangareviews」が運営する「Telegram Reviews」も、ドラッグ販売者からの情報を集約したチャンネルの1つです。Telegram Reviewsでは、購入希望者が欲しい商品を選択してサポート担当者（または管理者）にダイレクトメッセージで連絡をとり、暗号資産で代金を支払う仕組みとなっています。ただしTelegramでドラッグを購入する場合は、販売者の評価に関する情報が不足しているというデメリットがあります。Telegramには顧客からの評価やレビューに特化した機能が存在しないため、頼りにできる情報は商品を購入したと思われるユーザーのコメントのみとなります。またそのコメントの閲覧についても、ドラッグを販売しているチャンネルでコメント機能が有効になっている場合のみに限定されます。

そのようなデメリットはあっても、Telegramには人気の高いドラッグ販売チャンネルが複数存在します。いずれも短期間で多数のチャンネル登録者を獲得しており、それぞれ1万5,000人～ 3万人程度のチャンネル登録者を擁しています。例えばチャンネル「Mushrooms Doctor」は2022年10月28日に作成されましたが、チャンネル登録者数は同年12月末時点で2,400人を超えていました。Mushrooms Doctorが短期間で多数の登録者数を獲得した理由は、もっぱら同チャンネルが他の関連チャンネルに掲載していた広告が功を奏したことにあると思われます。Telegramでのドラッグ販売による利益については、最近逮捕されたドラッグの売人2人の場合、Telegramで様々な違法薬物を販売して370万英ポンドを稼いでいたことが報告されています[26]。

銃

サイバー犯罪マーケットでは、自動のアサルトライフルや爆発物、対戦車ミサイル、ロケット発射装置など、世界中の様々な武器も販売されています。銃は、他の製品よりも販売が難しいと思われますが、それでもTelegramでは商品として販売されています。我々は、販売者が武器の説明や値段、引渡し場所（シリアや米国など）を記載した写真を投稿しているチャンネルを多数観察しました。これらのチャンネルでは購入者がリクエストを投稿したり、ダイレクトメッセージを送信して価格や待ち合わせ場所を交渉できる仕組みになっています。そういったチャンネルの1つである「GUNS AND ARMS SHOP」は、2022年7月31日に作成されて以来、10万人を超えるチャンネル登録者を擁しています。GUNS AND ARMS SHOPは米国に拠点を置いており、チャンネル管理者である「@gunssadmin1」が「最高品質・新品の銃器」を世界中に匿名配送しています。@gunssadmin1は、最高品質のピストルやライフルを販売していると主張しており、商品の価格帯は180 ～ 6,500米ドルとなっています。

[26] WA Police target drug dealers using encrypted messaging apps

セクション #3

サイバー犯罪研究者への提言

近年、Telegramは様々なサイバー犯罪活動の拠点となっています。サイバー犯罪者が好むメッセージアプリは他にもありますが、その中でもTelegramは最も高い人気を誇っています。その一方で、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プラットフォームが大きな課題となっています。ランサムウエアグループからデータリークグループ、ハクティビストにいたるまで、脅威アクターはTelegramを自らの活動に幅広く取り入れています。Telegramでサイバー犯罪活動の件数が増加傾向にある現状を踏まえると、同プラットフォームは、2023年以降もサイバー犯罪者にとって人気の高い選択肢になるものと思われます。一方、Telegramで調査活動を行うには一定のスキルや知識が必要となるため、セキュリティ研究者にとっては同プラットフォームで犯罪を調査することがさらに困難になる可能性があります。

Telegramの機能と仕様は、セキュリティ研究者が証拠を集め、犯罪者を追跡して捕まえるうえでの障害にもなっています。Telegramではユーザーの匿名性が維持されているうえ、多数のアカウントを作成してそれらを簡単に切り替えることができ、送受信者の両方からメッセージを削除したり、メッセージの自己消滅タイマーを設定できる機能も備わっています。これらの機能に加え、いまや個人の電話番号を使用せずにアカウントを作成できるようになっていることから、Telegramでの犯罪調査がより困難になっています。また、Telegramのアクティブユーザー数が膨大な数にのぼることも、同プラットフォームで行われる全ての活動を監視・調査することが難しい要因となっています。

セキュリティ研究者にとっては、Telegramのネイティブ検索機能が制限されていることも調査の妨げとなっています。Telegramではユーザーがコンテンツを検索する場合、そのユーザーがアクセス可能なコミュニティ内でのみ、検索を実行することが可能となっています。つまり、セキュリティ研究者が特定のメッセージやグループを探そうとしても、まずそれらの情報が存在するコミュニティにアクセスすることが許可されていなければほぼ発見できないということになります。しかしその一方で、一部のTelegramユーザーはこの情報格差を埋めるべく多数の検索エンジンを開発し、サードパーティのサービスとして提供しています。こういった検索エンジンサービスは様々なグループやチャンネルをクローリングして独自のデータベースを作成し、ユーザーがデータベースを検索できる仕組みを提供しています。

またTelegramの非公開チャットは、招待状となるURLを持っているユーザーのみがアクセス可能となっており、通常の検索では表示されません。こういった仕組みも、同プラットフォームにおける調査の難易度をあげる要因となっています。例えば過去に、某ハッカーが非公開のTelegramチャンネルでMedibank社のアクセスを売りに出していたことがありましたが、このチャンネルも、招待状となるリンクを持っているユーザーのみがアクセス可能となっていました。このアクセスが売り出された数週間後にMedibank社がサイバー攻撃を受け、続いて同社のデータがリークされる事態となったことから、同社のインシデントは、非公開のチャンネルで販売されていたアクセスと関連している可能性が考えられます。このインシデントは、非公開のチャットの中に重要な情報が存在しうること、そして研究者がこういった非公開のチャットにアクセスできない場合は、調査がより困難になることを示唆する事例であると言えます。

これらの機能は全て、サイバー犯罪者の行動や活動を調査する研究者の作業を困難にし、また将来起こりうるサイバー攻撃の低減・阻止に向けた取り組みの妨げとなるものです。そして、Telegramで行われるサイバー犯罪を手動で検知することが難しいという現状は、セキュリティ研究者がTelegram上のサイバー犯罪を監視して抑制するという取り組みに、今や新たな手法やツールを開発・導入する必要があることを意味しています。法執行機関と連携したり、暗号化されたやり取りの中からサイバー犯罪の証拠を入手・検証する能力強化の一助として新たなテクノロジーを導入することも、そういった取り組みの一環と言えるでしょう。

KELAは、Telegramに出現する脅威との戦いに挑む防御者や、サイバー犯罪を研究する組織の皆様に向けて、以下の取り組みを提言します。

- *脅威インテリジェンス監視ソリューションを用いて、Telegram上の潜在的脅威を継続的に監視し、それら脅威の阻止に向けて事前の対策を講じる。*
- *従業員に対し、Telegram上のサイバー脅威を特定する方法や、それら脅威への対応について定期的なトレーニングや研修を実施する。*
- *制御ツール（ファイヤーウォールや侵入防止システムなど）を実装し、サイバー犯罪者による機密データへの不正アクセスを防止する。*
- *法執行機関やその他組織との協力体制・情報共有を強化し、Telegram上のサイバー犯罪検知・阻止能力を向上する。*
- *監査や評価を定期的に行い、Telegram上のサイバー脅威に対抗するにあたって、組織の防御において改善すべき領域や、修正すべき脆弱性を特定する。*

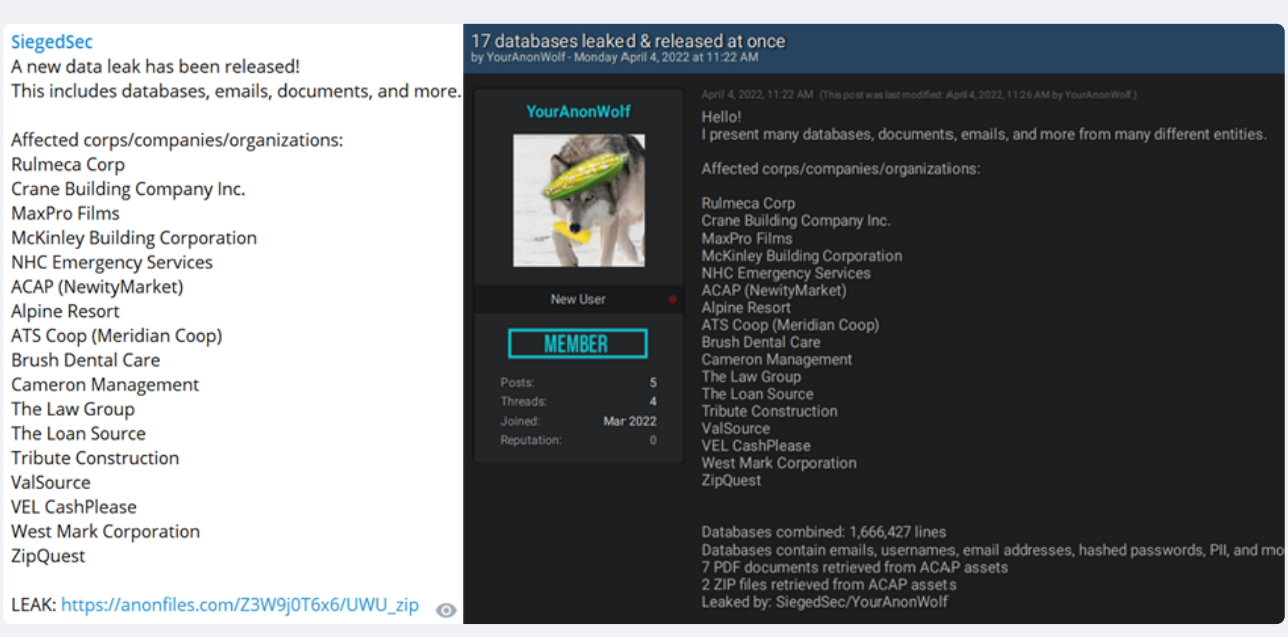
セクション #4

付録1
ケーススタディ

個人データ＆企業データ：SiegedSec

これまで取り上げてきたチャンネルの多くは金銭的動機に基づいて運営されていますが、本章の事例では、金銭目的以外の動機で活動している珍しいチャンネルを取り上げます（ただし金銭目的ではないにせよ、彼らが公開するデータは深刻なリスクをもたらすと思われます）。

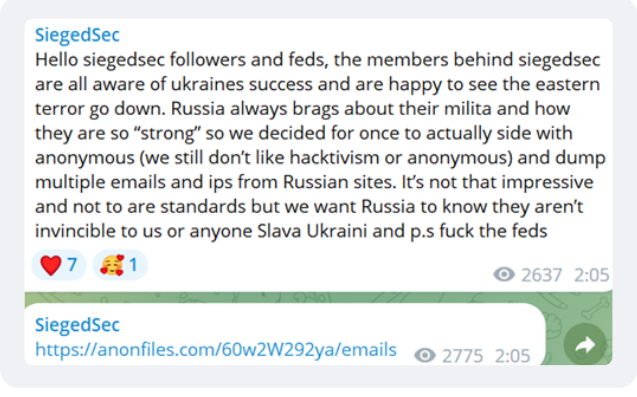
Telegramのチャンネル「SiegedSec」は、2022年4月に作成されました。同チャンネルの管理者は、企業や教育機関、政府関連のデータベースを公開しています。また同グループは多数のWebサイトを改ざんし、その証拠を自らのチャンネルに投稿しています。これまでSiegedSecが活動目的を明言したことはありませんが、おそらくは自らが行った攻撃を宣伝し、ハッキングスキルを誇示する目的でTelegramのチャンネルを利用していると思われます。同チャンネル（SiegedSec）を運営しているグループは、Twitterアカウント「@YourAnonWolf」を使用しているアクターとつながりがあり、@YourAnonWolfはSiegedSecがチャンネル上で犯行を主張した攻撃の一部をBreachForums上で公開していました。



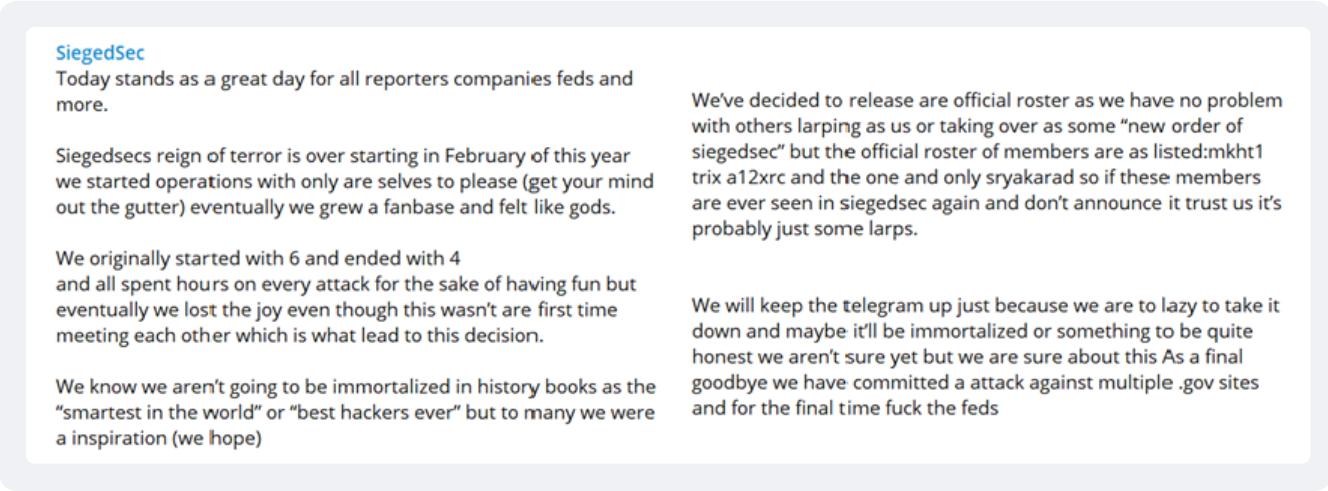
図：SiegedSecが17社のデータリークについて記載した投稿（左：Telegram）
YourAnonWolfが同じ17社のデータリークについて記載した投稿（右：BreachForums）

2022年9月、SiegedSecを運営するグループは、YourAnonWolfが同グループのサイバー犯罪活動から退いたこと、そして残りのメンバーは活動を続けることを公表しました。またSiegedSecはハクティビズムには関与しないと主張していますが、2022年9月、彼らはロシア・ウクライナ間のサイバー戦争でウクライナを支持する旨を表明していました。

SiegedSecは、ロシアのサイトから入手した電子メールアドレスやIPアドレスも多少リークしていましたが、その行為は真のハクティビスト活動というよりも、大義に対する貢献の象徴として行われていました。また、2022年11月にイランで反政府デモが行われた際、SiegedSecは「Operation Iran」の「GhostSec」と協力体制をとることを決定しましたが、それでも彼らは「自分達はハクティビストではなく、単なる『遊び』でOperation Iranに参加したいだけだ」と発言していました。



そして2022年11月末、SiegedSecはグループメンバーのニックネームを公表するとともに、ハッキング行為やリーク活動から引退することを発表しました。



SiegedSec

Today stands as a great day for all reporters companies feds and more.

Siegedsecs reign of terror is over starting in February of this year we started operations with only are selves to please (get your mind out the gutter) eventually we grew a fanbase and felt like gods.

We originally started with 6 and ended with 4
and all spent hours on every attack for the sake of having fun but eventually we lost the joy even though this wasn't are first time meeting each other which is what lead to this decision.

We know we aren't going to be immortalized in history books as the "smartest in the world" or "best hackers ever" but to many we were a inspiration (we hope)

We've decided to release are official roster as we have no problem with others larping as us or taking over as some "new order of siegedsec" but the official roster of members are as listed:mkht1 trix a12xrc and the one and only sryakarad so if these members are ever seen in siegedsec again and don't announce it trust us it's probably just some larps.

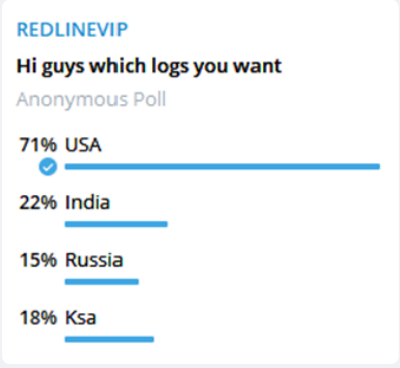
We will keep the telegram up just because we are to lazy to take it down and maybe it'll be immortalized or something to be quite honest we aren't sure yet but we are sure about this As a final goodbye we have committed a attack against multiple .gov sites and for the final time fuck the feds

彼らの活動期間は短いものでしたが、こういったグループが独自のウェブサイトを作成してデータを投稿しようとした場合、たとえ数カ月間使用するだけであったとしてもサイトの作成に労力を割き、かかる費用を調達する必要が生じます。一方Telegramにはユーザーが簡単にチャンネルを作成し、不要となれば「放置」できる仕組みが整っていると思われます。

情報窃取マルウエア：REDLINEVIP、Palm Team

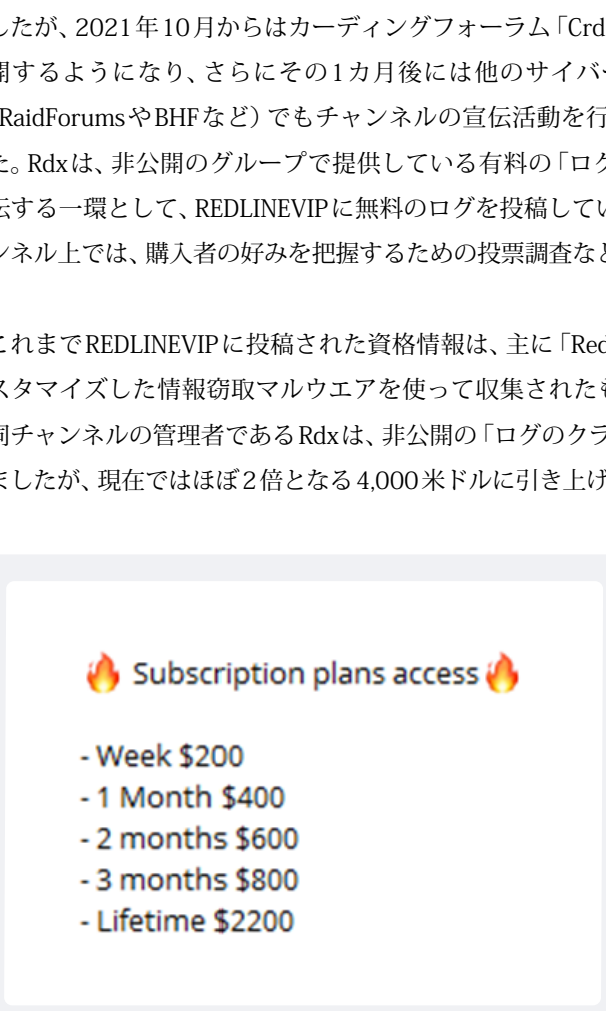
REDLINEVIP

Telegramのチャンネル「REDLINEVIP」は、2021年9月に作成されて以降、アンダーグラウンドのサイバー犯罪者の間で人気を博しています。REDLINEVIPの管理者「Rdx（@Fatherofcarders）」は同チャンネル上でログを公開していましたが、2021年10月からはカーディングフォーラム「CrdPro」でもログを公開するようになり、さらにその1カ月後には他のサイバー犯罪フォーラム（RaidForumsやBHFなど）でもチャンネルの宣伝活動を行うようになりました。Rdxは、非公開のグループで提供している有料の「ログのクラウド」を宣伝する一環として、REDLINEVIPに無料のログを投稿しています。また同チャンネル上では、購入者の好みを把握するための投票調査なども行っています。



図：どの国のログが欲しいかを質問している投票調査

これまでREDLINEVIPに投稿された資格情報は、主に「Redline」や、独自にカスタマイズした情報窃取マルウエアを使って収集されたものと思われます。同チャンネルの管理者であるRdxは、非公開の「ログのクラウド」サービスの終身使用料を1年前は2,200米ドルに設定していましたが、現在ではほぼ2倍となる4,000米ドルに引き上げています。



図：2021年10月のサービス使用料

図：2022年12月のサービス使用料

2022年12月7日、Rdxは「非公開の有料サービスを利用すれば、400万件のログにアクセスできる」と主張し、この有料サービスに登録するメリットとして以下を挙げていました。

1. “ログはいずれもチャンネル（REDLINEVIP）に掲載されていない非公開のもの”
2. “非公開のログを全メンバーに日次で送信”
3. “クッキー手法”
   （KELA注：「クッキーを含むログ」を指していると思われます）

4 “暗号資産ウォレットの確認方法に関するビデオ”

5 “銀行口座アカウントのログイン方法”

6 “サービス利用者数を限定”

REDLINEVIPの管理者であるアクターRdxは、複数のサイバー犯罪フォーラムで「FATHER121」とのユーザー名で活動しており、我々はその情報をもとに同アクターの信頼性を調査することができました。その結果、同アクターが詐欺を行ったとの告発がいくつか確認されましたが、それら告発の一部は告発者側の信頼性が疑われるものでした。現在、REDLINEVIPでは6,000人を超えるユーザーがチャンネルに登録しています。

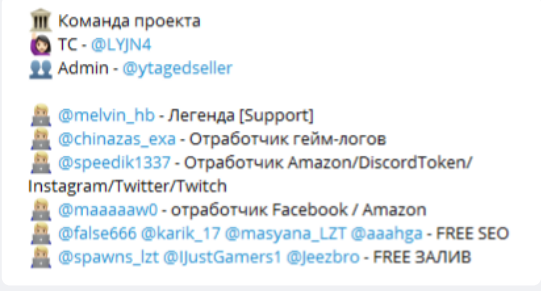
Palm Team

「Palm Team」は複数のチャンネルを運営しており、その中の主要なチャンネルがトラッファーの集まる場となっています。同チャンネルは2022年7月1日に作成されて以降、ロシア語話者の集うサイバー犯罪フォーラム「Lolz Guru」にも広告を掲載しています。同チャンネルの管理者「Luwyshka」は、Lolz Guruでは「LUWY」とのユーザー名で活動しています。

Palm Teamは、Telegramで以下の機能を使用しています。

1. “トラッファーのアプリケーションと通信するTelegramボット”
2. “Palm Teamの経験豊富なトラッファー用Telegram（公開）グループ”
3. “Palm Teamの非公開グループ”

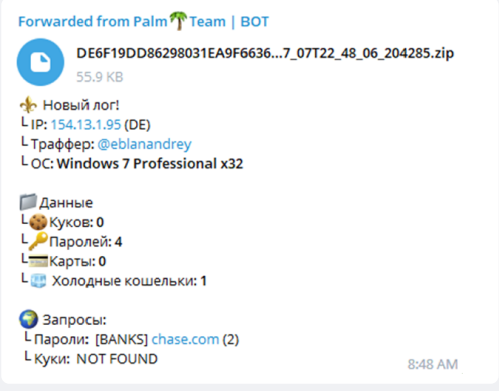
また、Palm Teamを運営しているアクター（グループ）は、ブログ投稿プラットフォーム「Telegraph」でトラフィック生成用のマニュアルを公開していました。Palm Teamのチャンネル管理者がTelegramやLolz Guruに投稿したコメントによると、彼らはRaccoonやRedline（情報窃取マルウエア）を使用しているということですが、その他の情報窃取マルウエアも使用している可能性があります。



図：Palm Teamのメンバー

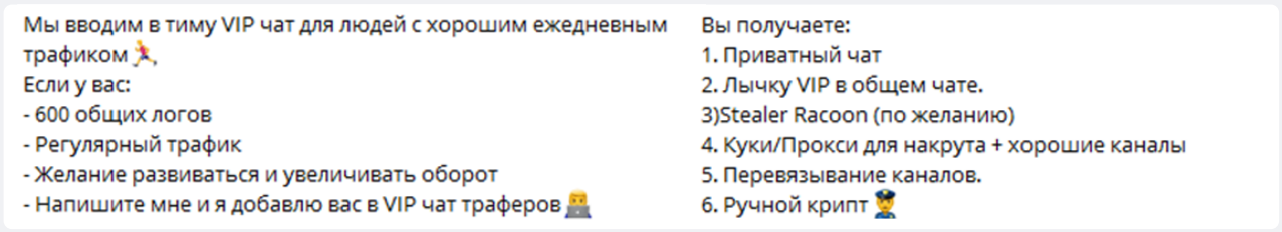
Palm Teamでは数人のメンバーが様々なプロジェクトを担当し、各サービス（ゲームやAmazon、Twitter、Facebookをはじめとするソーシャルメディアなど）の資格情報を窃取するプロセスを管理しています。そしてその他の1名がトラッファーからの質問に回答したり、サポートを提供しています。

トラッファーが収集したログは、さらなる悪事に利用される場合もあれば、管理者が商品として販売する場合もあります。トラッファーには、収集したログの対価が歩合（収益の約80％）で支払われており、トラッファーがログ1,000件を収集した場合、平均して1万ロシアルーブル（約140米ドル）が支払われているようです。またチャンネルの管理者は、トラッファーがさらに多くのログを収集するよう常時課題を提示したり、コンテストを開催しています。



同チャンネルの管理者は、Palm TeamのVIPトラッファーだけが参加できるTelegramチャットも宣伝しており、「最低600件のログを持っており、かつマルウエアの配信に利用できる安定したトラフィックを持っている」経験豊富なトラッファーに参加を呼びかけています。

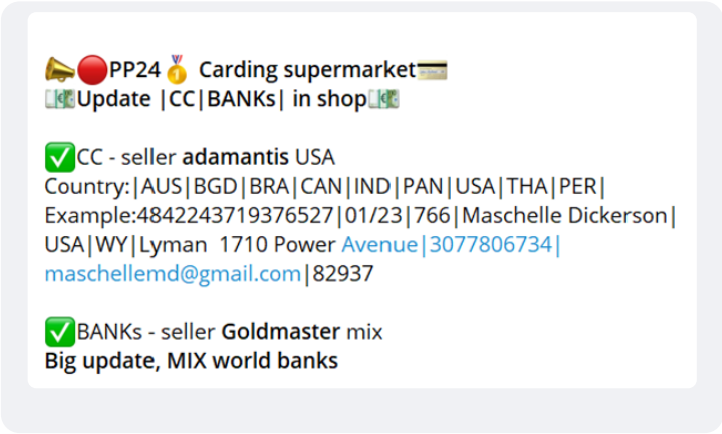
図：トラッファーの1人が収集したログのファイル



図：PalmTeam のVIPトラッファー用チャットに参加する条件として「少なくともログ600件と、常時使用できるトラフィックを持っていること」が記載されている投稿。VIPメンバーになると、非公開のチャットやRacoon（情報窃取マルウエア）が利用できる他、マルウエアを配信する機会や同グループがカスタマイズした手動の暗号化ツール（ビルド用）などが提供される。

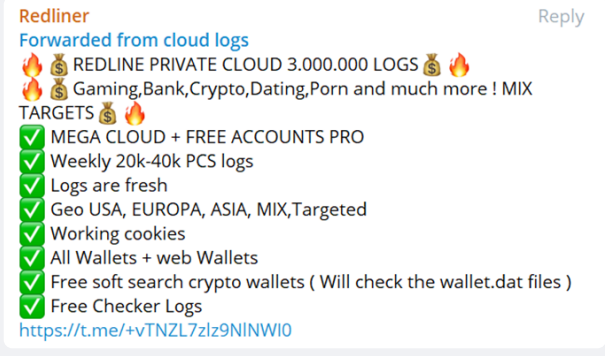
トラッファーが収集したログを収益化する集団は多数存在しており、Palm Teamはあくまでその1つです。彼らはマルウエアを配信し、ログを収集するプロセスの重要な拠点としてTelegramを使用しており、同プラットフォームの機能を利用することによって当局に気付かれることなく、スムーズに各メンバーと連携できるようになっています。したがって、サイバー犯罪者が今後もオペレーションの運営やマルウエアの拡散、企業や個人が使用する資格情報窃取などの活動においてTelegramを利用することは、理にかなっていると言えるでしょう。

銀行詐欺：CHECKS GRUB SHOP



「CHECKS GRUB SHOP」は、クレジットカード情報やコピー商品、有効な小切手（盗品）、フルズや銀行口座アカウントのログなどを販売するグループとして人気を集めています。同グループは2021年8月30日、ユーザー「@TrippleeG」によって作成されました。CHECKS GRUB SHOPにはチャンネルとグループ（いずれも同じ名称）があり、チャンネルでは彼らの投稿に対してチャンネル登録者がコメントを記入できるようになっており、グループではグループメンバーがチャンネルの投稿について議論できるようになっています。当初、CHECKS GRUB SHOPのグループで取りあげられていたコンテンツは同名のチャンネルに掲載されていた投稿のみでしたが、2021年11月に加入したユーザーが、同グループ内で自らのサービスを提供するようになりました。現在同グループは8,100人のメンバーを擁していますが、チャンネルの方は活動を停止しており、登録者数もわずか300人ほどとなっています。CHECKS GRUB SHOPのグループチャットに参加している典型的なメンバーの例としては、定期的にクレジットカード情報を販売しているユーザーが挙げられ、彼らは商品のサンプルやカード所有者の国名、銀行、その他最新の関連情報などをグループに投稿しています。

またCHECKS GRUB SHOPのグループメンバーの中には、他のチャンネルの商品を宣伝している者もいます。例えば「Redliner」と名乗るメンバーは、ログを販売している他のチャンネルのメッセージを同グループ（CHECKS GRUB SHOP）に転送していました。



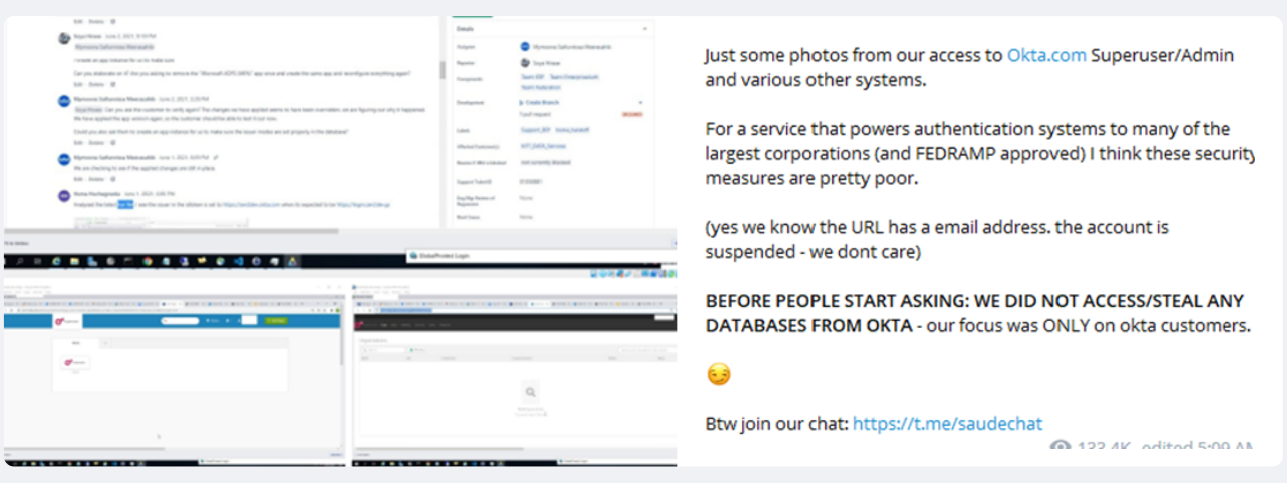
CHECKS GRUB SHOPのグループは、1人のアクターが同名のチャンネルで販売する商品を宣伝する場として作成しました。しかしその後、同グループは多数のユーザーを引き付け、最終的にチャンネルよりも人気を集めることとなりました。この事例は、Telegramでコミュニティを作成する機能が、銀行詐欺専用グループの確立にどのように貢献したかを物語っています。

ランサムウエア・データリーク：Lapsus$

Lapsus$は2021年12月初旬に登場したデータリークグループであり、活動当初は主にブラジルやポルトガルで様々な業界にわたる組織を攻撃していました。同グループは、2021年12月10日にTelegramで作成したチャンネルをメインチャンネルとして使用し、被害組織に関する情報を投稿していました。このメインチャンネルについては、2022年12月時点で登録者数が5万5,800人を超えていたことが確認されています。Lapsus$はメインチャンネルの他にもう1つチャンネルを作成していましたが、こちらのチャンネルに掲載されているのは2022年3月以降の投稿であり、またその大半はメインのチャンネルから転送されたもので構成されていました。さらにLapsus$はTelegramでチャット用のグループも作成し、チャンネルに掲載した被害組織に関する情報を再公開したり、グループメンバーと交流する場として利用していました。現在このグループはアクセス不可能となっていますが、以前は1万4,000人ものユーザーがグループメンバーに登録していました。

Lapsus$は、これまでブラジル、ポルトガル、米国、韓国、アルゼンチンをはじめとする国々の組織を多数攻撃したと主張しており、その業界も電気通信、メディア、娯楽、テクノロジー、小売、政府関連組織と多岐にわたっていました。しかし2022年2月後半から同年3月にかけて、同グループはNvidia社やSamsung社、Microsoft社、LG Electronics社など、主に有名企業のデータを公開するようになりました。Samsung社とNvidia社は、Lapsus$がTelegramのチャンネルで両社を被害組織として公表したのとほぼ同じ時期に、サイバー攻撃を受けた旨を報告するとともにリークされたデータが自社のものであることを認めていました。

Okta社もLapsus$に標的とされた有名企業の1社です。2022年3月22日、Lapsus$は自らのTelegramチャンネルで、「Okta.com」の「スーパーユーザー／管理者」権限を入手したと主張し、複数のスクリーンショットを投稿しました。同グループはこの投稿の中で、「Okta社のデータベースには不正アクセスせず、同社の顧客のみに標的を絞った」と説明していました。このとき投稿されたスクリーンショットには複数のドメインの他、Okta社が業務を委託している請負企業の従業員（エンジニア）のアカウントが表示されていました。Lapsus$はこのエンジニアのアカウントを悪用することで、高い権限が必要となる（Okta社の）社内ポータルや顧客情報にアクセスすることができたのです。



図：Lapsus$がOkta社への攻撃について説明している投稿

しかし同月、ロンドンの警察当局がLapsus$との関係が疑われる10代の容疑者7人を逮捕したことが報道されました。またそのうちの1人は、英オックスフォード出身の16歳の若者であったとされています。さらに同事件の捜査官によると、この7人の他に、ブラジルに住む10代と思われる人物も容疑者として浮かんでいるということでした。Lapsus$は、2022年3月30日以降現在（2022年12月29日）にいたるまで沈黙を守っており、Telegramのチャンネルでも情報を公開しておりません。しかし我々は、同グループで活動していた元メンバー数人（逮捕された上述の7人以外）がサイバー犯罪フォーラムで活動していることを確認しています。

ハクティビズム: Killnet、ALtahrea Team

Killnet

ウクライナ侵攻でロシアに反対する国々を標的とする親ロシア派ハッカーグループの中で、Killnetは最も強い影響力を持つグループの1つです。Killnetが主に使用しているTelegramのチャンネルには9万人を超えるユーザーが登録しており、また同グループのキャンペーンには「XakNet」や「NoName057（16）」をはじめ、影響力のあるハッキンググループが多数参加しています。2022年3月以降、Killnetは、ウクライナおよびその同盟国の政府機関や民間組織を標的にしています。

Killnetのオペレーションは、「Killmilk」と名乗るアクターによって2021年11月に立ち上げられました。そしてその後の2022年1月、KillnetはDDoS攻撃用のボットネットをプロジェクトとして宣伝し、サイバー犯罪フォーラムで営利目的のサービスとして提供していました。当時彼らがこのプロジェクトを宣伝していた投稿には、DDoS攻撃に使用可能な有料サービスで「初めての分散型ボットネット」との説明が記載されていました。

しかし、ロシア・ウクライナ間の戦争が始まって以降、Killnetの活動はハクティビズムへと移行しました。また同グループがTelegramに参加し、コミュニティを形成し始めたのもこの頃となっています。彼らは、ウクライナ侵攻が始まって2日後の2022年2月26日、Telegramで自らのチャンネルを作成しました。そして、親ウクライナ派の国々（ポーランドやリトアニア、英国、イタリア、その他多数の国々）や組織に対してDDoS攻撃を実行し、その活動を宣伝するとともに、Telegramを使って「Legion」と呼ばれるハクティビスト運動を立ち上げました。このLegionは、様々なハッキングチームの下で活動するサイバー「分隊（squad）」で構成されており、それらの分隊が同じ標的リストを使ってDDoS攻撃やウェブサイトの改ざん、その他の攻撃を実行しています。こういった「分隊」の一部（Anonymous Russia、Phoenix、Zarya）は後に独立したハッカーグループへと分離しましたが、彼らはその後もLegionと同じ標的を攻撃し、Killnetの投稿を自らのTelegramチャンネルに再投稿していました。

ほとんどの事例において、Killnetは一国の標的を連続的に攻撃しており、またそれと同時進行でLigeonの分隊や他のグループにも攻撃に参加するよう呼びかけています。またいくつかの事例では、できるかぎり多くのハクティビストの参加を促すため、標的とする組織のドメインを共有するのみならず、攻撃を実行するツールを提供していたことが観察されています。例えばKillnetは、オープンプロキシサーバーを使用した攻撃のリレープロセスを自動化するため、「CC-Attack（CC攻撃）」として知られている公開スクリプトを攻撃ツールキットとしてLegionのメンバーに配布していました（攻撃者はオープンプロキシサーバーを使用することで、自らの匿名性を維持しつつ、攻撃を仕掛ける側のIP数を増やすことが可能となります）。Killnetが配布したCC攻撃ツールキットは数本のファイルで構成されており、攻撃を実行するアクターに高度なスキルは必要ありません[27]。このツールキットに含まれているスクリプトの場合は、3種類のレイヤー7攻撃が生成できるようになっています。

KillnetのリーダーであったKillmilkは、2022年8月から同年9月の間にグループの活動から退き、ランサムウエア攻撃に関与しているとされているメンバー「BlackSide」が後任のリーダーに指名されました。しかし我々が調査したところ、Killmilkは2022年9月半ばに同グループのリーダーに復帰していました。同グループは現在も活動を続けており、Telegramを主要なコミュニケーションツールとして使用しています。

---

[27] KillNet Utilizes CC-Attack: A Quick & Dirty DDoS Method

ALtahrea Team

「ALtahrea Team」は親ロシア派のハクティビストグループであり、2022年4月19日にユーザー「@Altahrea」が同グループのTelegramチャンネルを作成しました。同グループは、「Sabreen News（イランの支援を受け、2020年からTelegramチャンネル『@sabreenS1』を中心に活動しているイラク民兵メディア）」とのつながりがあります[28]。

ALtahrea Teamは、Telegramでチャンネルを作成したその直後、イスラエルメディア数社のウェブサイトに対するサイバー攻撃のカウントダウンを公開しました。そしてこれ以降、ALtahrea Teamは同チャンネル上で、イスラエルやトルコ、サウジアラビア、イラク、アラブ首長国連邦、英国、米国をはじめとする国々の組織に対するDDoS攻撃やウェブサイト改ざんについて犯行声明を出しています。またALtahrea Teamはロシア・ウクライナ間のサイバー戦争にも参加し、ロシア側を支援していました。同グループは、自らがイスラエルを攻撃するに至った政治的動機を何度も明言しており、またイスラエル以外の組織に対する攻撃についても、大半は被害組織の活動が攻撃を誘発したと説明していました。

イラクには、政治的動機をもとに活動している別のグループ「1877 Team」が存在します。1877 Teamは、遅くとも2019年からアンダーグラウンドのサイバー犯罪に積極点に関与しており、ALtahrea Teamは同グループと協力体制をとっているものと思われます。その理由として、両グループが「合同でウェブサイトを改ざんした」との犯行声明をこれまでに少なくとも2件、Telegramに投稿していたことが挙げられます（1877 TeamもTelegramを頻繁に使用しています）。

ALtahrea Teamの評判について得られる情報は限られていますが、同グループが、アンダーグラウンドのフォーラムで高い評価を受けているサイバー犯罪グループ（1877 Team）と協力体制をとっているという事実は、ALtahrea Teamの信頼性に寄与しうるものと思われます。なおALtahrea Teamは、2022年の大半において活動している様子が観察されていましたが、同グループのTelegramチャンネルには2022年10月31日以降新たな動きが見られず、グループが活動を停止した、またはALtahrea Teamというハンドル名での活動を停止したという可能性が考えられます。

---

28 Profile: Sabereen News

真のインテリジェンスで
デジタル犯罪を
監視・調査・低減します。

利用を開始

KELA

サイバー犯罪防止における世界的リーダー