KELA REPORT

TELEGRAM

How a Messenger Turned Into a Cybercrime Ecosystem by 2023

Executive Summary

Telegram is a messaging app that is used by many people around the world for a variety of purposes. However, it has also become a hub for cybercrime activities, including the sale and leakage of stolen personal and corporate data, the organization of cybercrime gangs, the distribution of hacking tutorials, hacktivism and the sale of illegal physical products such as counterfeits and drugs.

There are several other messaging apps that are favored by cybercriminals, but Telegram is one of the most popular. This presents a significant challenge for security researchers trying to combat cybercrime on the platform.

One reason why Telegram is attractive to cybercriminals is its alleged built-in encryption and the ability to create channels and large, private groups. These features make it difficult for law enforcement and security researchers to monitor and track criminal activity on the platform. In addition, cybercriminals often use coded language and alternative spellings to communicate on Telegram, making it even more challenging to decipher their conversations.

This report, compiled by KELA, aims to provide an in-depth understanding of why Telegram has become a significant player in the cybercrime ecosystem. It covers various services, products and cybercrime activities that exist on the platform, as well as the threat actors involved. The report also includes showcases for each topic, highlighting specific examples of the types of activities that take place on Telegram. In addition, the report lists prominent groups and channels that are involved in these activities, providing a comprehensive overview of the scope and scale of cybercrime on the platform.

The following topics and actors are discussed in this report:

- Personal and corporate data being sold and leaked on Telegram
- Info-stealing hacking teams that use Telegram to sell and leak data harveste through infostealers, and to organize gangs and build bots to facilitate their activities
- Banking fraud actors that use Telegram to easily sell credit cards, checks and other financial instruments
- Ransomware and data extortion groups that adopt Telegram as an alternative or addition to their blogs and data leak sites, such as Lapsus$
- Hacktivists who use Telegram to publicize information about their attacks, such as Killnet and ALtahrea Team
- Illegal physical products being sold via Telegram, including counterfeits, guns, drugs and COVID-19 documents

While KELA chose to focus on items specific to each topic, it's important to remember that more information on each subject can be found on the platform, such as tutorials, services, etc.

Overall, Telegram has become a thriving ecosystem for cybercrime and will likely continue to be a major challenge for security researchers and law enforcement.

Table of Contents

Section #1

Overview

What is Telegram?

Telegram is a multi-platform messaging service launched by the Russian brothers Nikolai and Pavel Durov in 2013. They are also known to be founders of VK (formerly known as Vkontakte), a Russian online social media and social networking service. According to Telegram's privacy policy, Telegram Group Inc. is a parent company of Telegram Messenger Inc. and is located in the British Virgin Islands, and Telegram FZ-LLC is a group member located in Dubai.[1] Telegram mentions that the Telegram development team is based in Dubai. [2]

Telegram allows users to send messages, photos, videos and files of any type (doc, zip, mp3, etc.) up to 2GB in size, and to create groups and channels. The company claims that Telegram is unique because of its focus on privacy, encryption and an open-source API. It provides optional end-to-end encrypted chats, and sent messages can be deleted at any time on both sides. In addition, with the publicly available API, developers can create clients on other platforms, custom bots, themes, stickers and so on free of charge.[3]

However, there are some downsides to using Telegram. First, although Telegram offers APIs, the company doesn't disclose the code of the application itself. Therefore, there's no way to know if the encryption is truly secure. Second, Telegram has been known to cooperate with law enforcement in some cases, which means that messages are not as private as one might think.[4]

As shown in the following chart, the number of monthly active Telegram users worldwide has increased, and it had over 700 million monthly active users as of November 2022.[5]

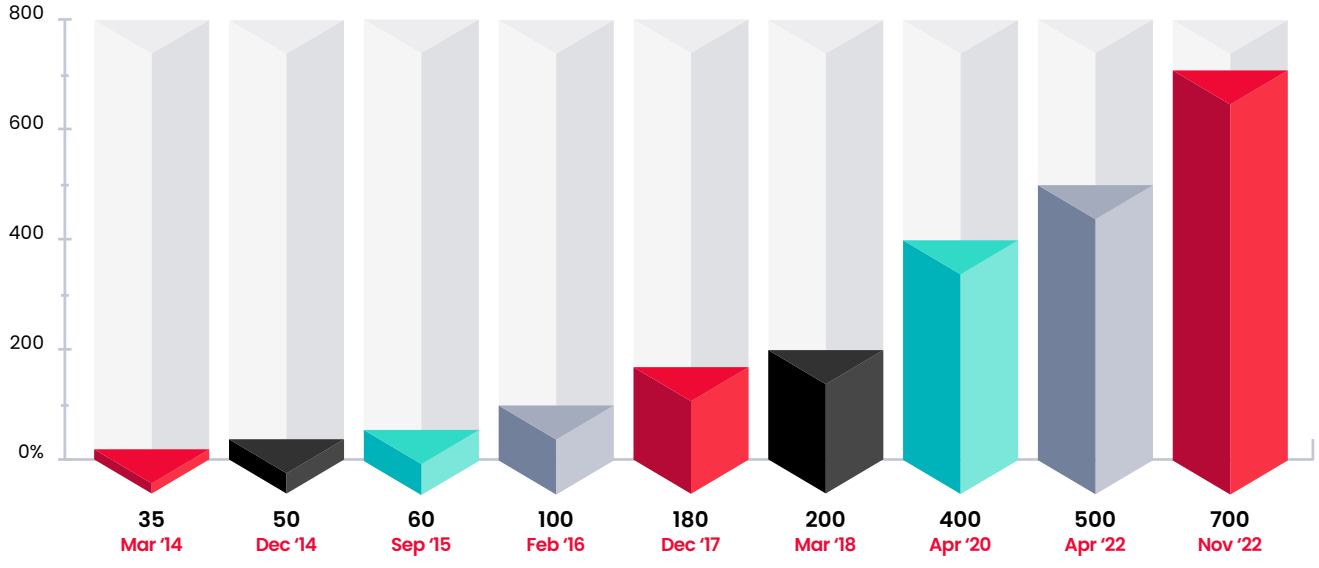


Figure: The number of monthly active Telegram users worldwide from March 2014 to November 2022 (in millions)

[1] Telegram Privacy Policy

[2] Telegram FAQ — Where is Telegram based?

[3] Telegram offers Telegram Premium, an optional subscription service that unlocks additional exclusive features. For example, all Telegram users can upload files up to 2GB; however, ***Premium users*** are allowed up to 4GB.

[4] Telegram Reportedly Handed User Data to German Authorities

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

How Telegram is Built

Telegram users have two key identifiers: "usernames" and "user IDs." Usernames are publicly facing and can be edited in the settings. Once Telegram users set their usernames, they can share their contact with others with a link, as a t.me/username or a username.t.me link (for example, the username of Pavel Durov, Telegram's CEO, is t.me/durov). User IDs, on the other hand, are assigned to users, groups and channels by Telegram, and users aren't able to change them.

Telegram has several features that allow users not only to use it as a messaging service but also to build a community on the platform. One of them is "channels" that Telegram users can create for broadcasting to unlimited audiences. Channels are one-way communication platforms on which only admins send messages, and channel subscribers can't reply. However, in 2020, Telegram updated the platform, allowing channel subscribers to comment under channel posts.[6] To let channel subscribers comment, a channel admin user creates a chat. The chat can be hidden from followers; however, the admin can also share it with channel subscribers who can join the chat and use it to comment on specific posts and communicate with others.

Another feature is "groups": chat groups where members can interact with each other and reply to messages, and members can see their contacts in the same group. There are open groups, and there are closed groups that can be accessed only by invitation. Users can add up to 200,000 people to one group. WhatsApp, a rival instant messaging platform, also allows users to create chat groups, but only up to 512 people can be added to a group.[8] A group conversation on Instagram can add even less - up to 250 participants.[9] Therefore, compared with other platforms, Telegram allows many more people to build a community.

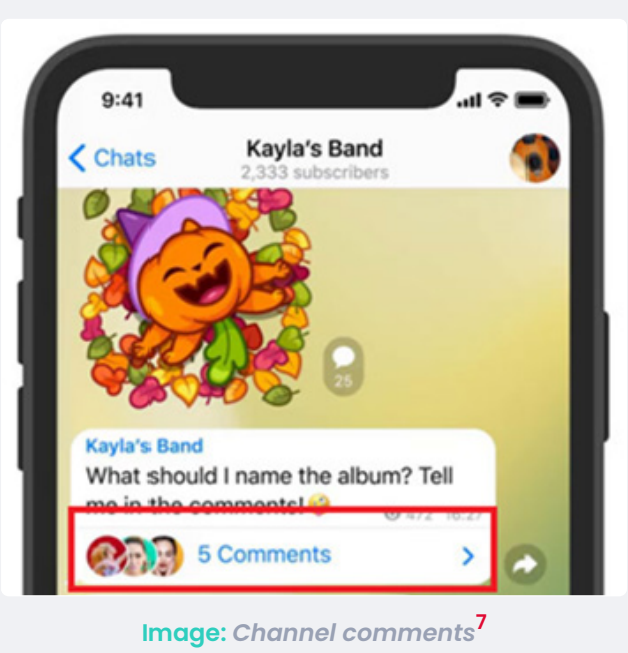


Image: *Channel comments*[7]

It's also possible to use and create bots, which are essentially automated Telegram accounts.[10] They are popular tools for a variety of purposes, including creating and managing group chats, acting as personal assistants and providing entertainment. The bots are also used to automate activity outside the app.

[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

Telegram also has its own cryptocurrency, Toncoin, formerly known as Gram, which is a token native to The Open Network, a blockchain-based technology developed by Telegram (TON, formerly Telegram Open Network). In April 2022, Telegram allowed its users to send Toncoin directly from chats within the app. In addition, Telegram now supports Toncoin transactions with no fees attached.[11]

Due to these features, Telegram became a tool that enables users and companies to build communities, promote their products and more. In fact, at the end of 2020, the sales volume on Telegram was reported to have reached $25 million. Goods from China had the highest sales volume in 2020, over $12 million. Products sold on Telegram included digital equipment, consumer loans, apparel and shoes.

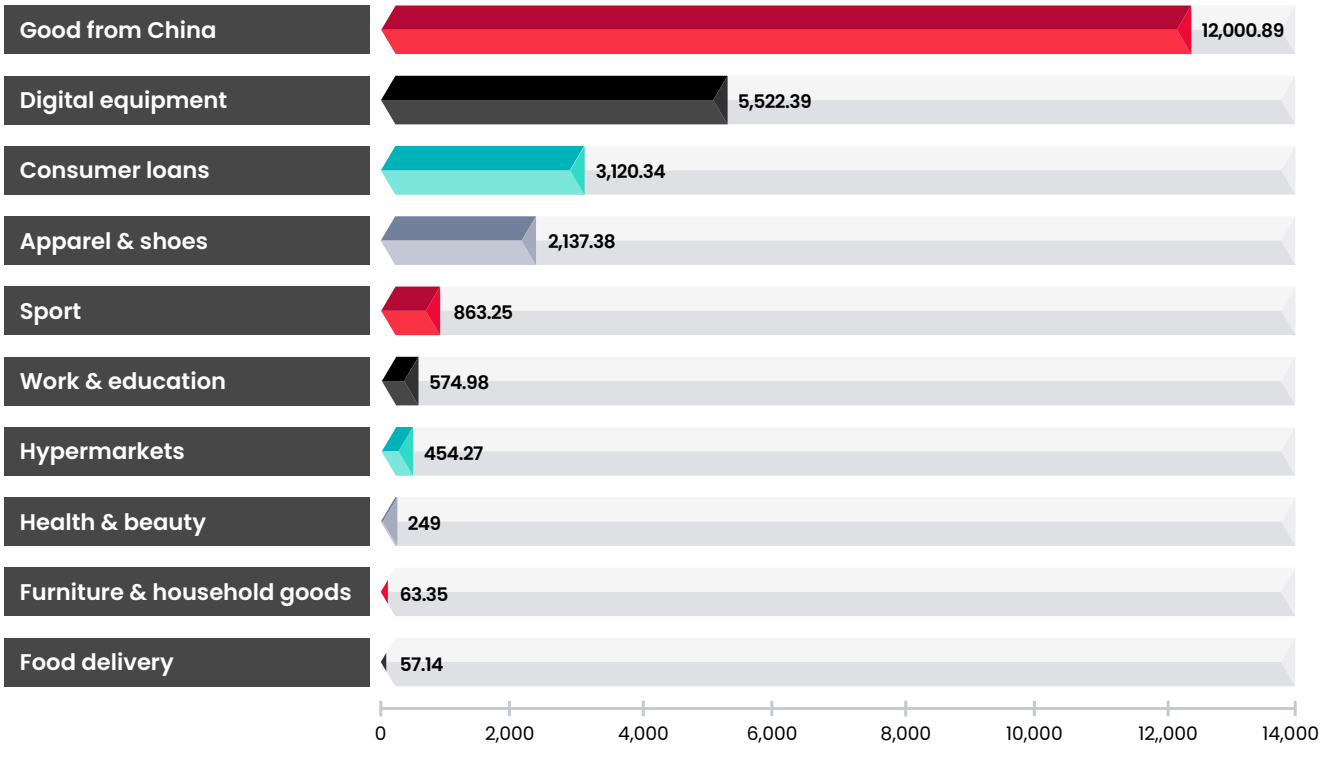


Figure: Sales volume on Telegram worldwide in 2020, by segment (in 1,000 U.S. dollars) [12]

[11] TON's Twitter

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

Why Telegram is Good for Cybercrime

Cybercriminals often use the popular platform to exchange information, share tips and tricks, and coordinate activities. User's accounts and channels are commonly advertised on cybercrime forums and other online communities that cater to cybercriminals. Through these forums, criminals can post links to Telegram groups and channels where they can further discuss and collaborate on criminal activities. Telegram can be used to share information about cybercrime techniques, as well as to distribute malicious tools such as password-stealing Trojans, keyloggers and ransomware. In addition, it's also used to facilitate the sale of stolen data and illicit goods and to recruit new members for criminal activities.

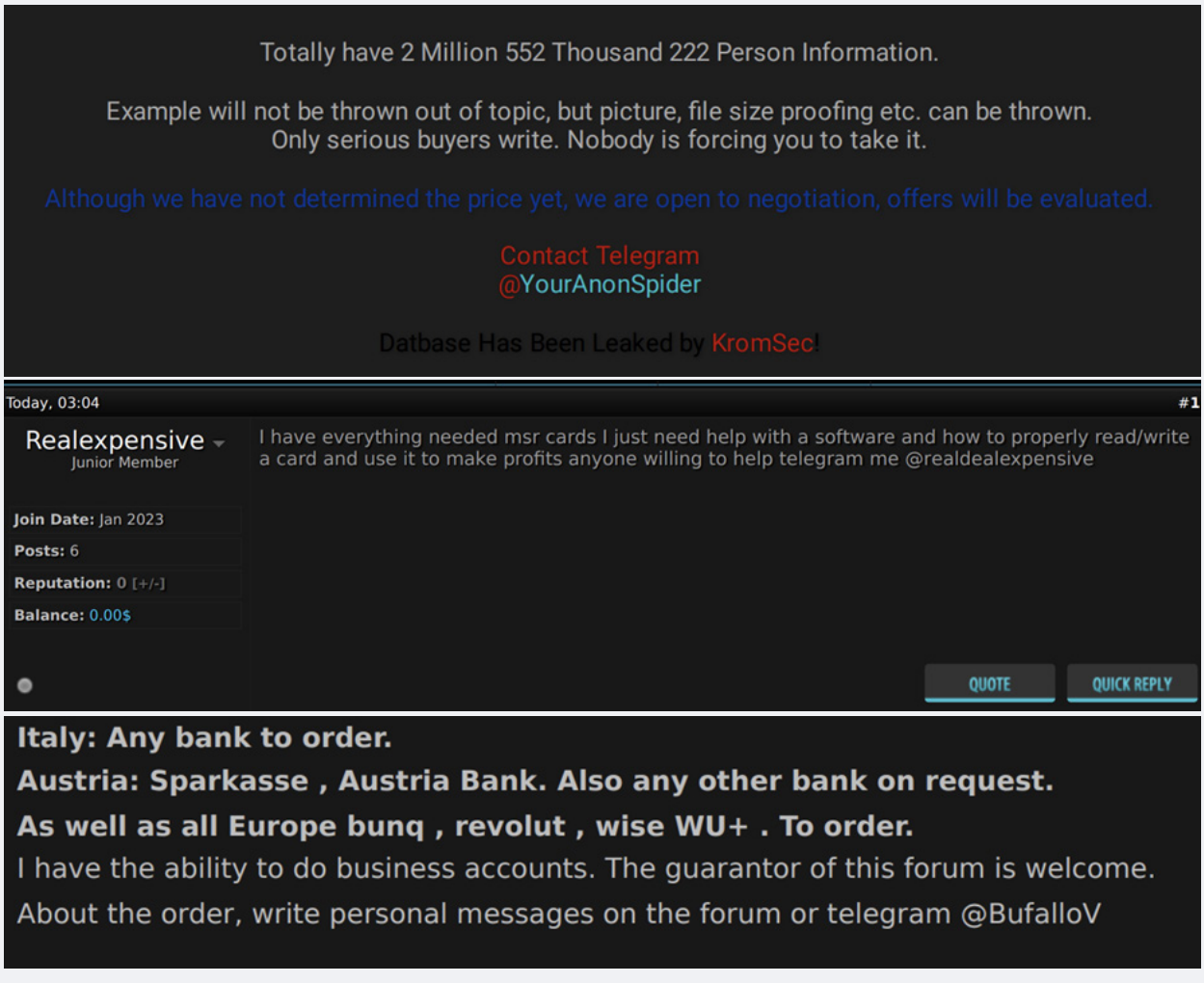


Image: *Different threat actors on various cybercrime forums advertising Telegram as their main point of contact*

Telegram is favored by hackers for a variety of reasons. One of the key reasons is that it prioritizes privacy and security. However, Telegram's standard chat is not fully encrypted – only the client/server is encrypted and kept in the Telegram cloud.[13] The Secret Chat feature provides end-to-end encryption so that only the sender and receiver can read the messages. This makes it difficult for anyone who isn't involved in the chat to intercept

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

and read the messages without being intercepted by third parties. This is a critical feature for consumers who value their privacy and wish to safeguard their personal information.

The anonymity of Telegram is one of the main reasons it appeals to hackers. Telegram allows users to register accounts without disclosing personal information, making it simple to set up many identities and use them to converse without revealing one's genuine identity. Because of this anonymity, law enforcement organizations have a tough time tracking down and identifying individuals who are using the program for illicit activities.[14]

Telegram users can sign up with virtual numbers or foreign phone numbers that are unrelated to their true identities. Users can also register for the service via a one-time SMS service, with the OTP number given to the one-time SMS service rather than their private phone. The latest update (version 9.2) introduced the Fragment blockchain platform, which allows users to buy anonymous numbers with Toncoins and sign up for Telegram without a SIM card.[15] Furthermore, Telegram allows users to create multiple accounts and switch between them easily, which makes it difficult for security researchers to track and identify individual users. This can make it challenging to gather evidence and build a case against cybercriminals using the platform.

While Telegram's privacy policy states that it may disclose a user's IP address and phone number to authorities if presented with a court order on terrorism-related charges, the company claims it hasn't done so yet. However, recent investigations in Germany have revealed that the platform is sharing user data with government agencies and censoring content, despite its promise to keep users' data secure and private.[16] Telegram has been forced to disclose user data by court order, and German authorities have received data on suspected terrorists and child abusers. Telegram stores its data worldwide in various data centers and can be forced to reveal or share user data only if it receives multiple court orders from different jurisdictions, like the case in Germany.

Telegram has also become the app of choice for extremists and hacktivists because of its loose moderation measures. It creates and enforces its own rules and processes requests to take down illegal public content. It won't censor content based on political motivations or peacefully expressed alternative opinions but will block terrorist-related content. Telegram is attempting to deal with the increase in users and removes channels that include white nationalist content. However, it has been erratic in following its rules against encouraging violence, and policing the service remains challenging. Extremist channels can still be found, and Telegram didn't close some cases that were reported to it in the past, such as a manifesto about killing Muslims and doxing information.[17] The questions of whether Telegram should boost its moderation efforts and whether context should be considered while engaging in moderation remain unanswered.
Many cybercriminals, as KELA observed from their chatter, value Telegram's user-friendly

[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

interfaces and that it provides new features before rival chat applications. Its simple interface enables users to access their accounts from the web without having to connect their phones to the internet. However, some people have expressed worries about its security and privacy, claiming that the encryption may not be safe enough for some users. Other cybercrime users have voiced concerns about the obligation to register with a phone number when using Telegram, but this has subsequently altered. Overall, it appears that users have differing ideas on the benefits of using Telegram, with some preferring to use alternative messaging apps such as Signal.

Image: *Chatter about Telegram on BreachForums, a prominent cybercrime forum*

Compared to cybercrime forums, Telegram channels and groups are easier to find: just typing a relevant word in the search bar would bring some communities of interest, for example, groups and channels that sell and share data. One will have to put in much more effort to find cybercrime forums and markets since many of them are not indexed by search engines and don't have indicative names. They also require users to create accounts and become members in order to view and acquire their content. For some, access is granted upon review by the forums' administrator, and for others, membership may be granted for a fee. Because Telegram is much easier to join, it's becoming increasingly popular with threat actors.

Cybercriminals' Language on Telegram

Cybercriminals frequently use English on Telegram because it's the most widely spoken language on the internet. However, many Telegram groups and channels are dedicated to certain areas or languages, allowing people who speak other languages to converse and exchange information in their native tongues, such as Chinese, Russian, and Arabic. The Translate tool was added to conversations in the November 2022 upgrade, making it simpler to interact across languages and giving. The ability to interact in different languages on Telegram gives cybercriminals a worldwide platform, where crimes can be carried out on a greater scale, making it more difficult for law enforcement authorities to hunt them down and shut them down.

In addition to several languages, cybercriminals (on Telegram and on cybercrime platforms in general) frequently use a combination of technical jargon, slang, and acronyms. They do it to illustrate their competence while describing their plans and techniques. Some of these users will also regularly converse using coded or encrypted messages (generated via third-party platforms) which can be decoded only by people who have the necessary decryption key.

Other Messengers Favored by Cybercriminals

Several additional chat applications are popular among cybercriminals, such as Discord, Jabber, Tox and Wickr, with new applications emerging once in a while. Each of these applications has its own set of features and characteristics, but they all provide some amount of secrecy and protection that cybercriminals find appealing.

Jabber is a protocol that uses a TCP connection to transmit data. It allows users to communicate through different clients in real time and it seems to be the most popular tool among Russian-speaking hackers. The infamous XSS and Exploit forums have semi-exclusive Jabber servers which allow approved members to use the messenger with no logging and strong privacy.

The Wickr Me app, owned by AWS, became popular among reporters and their sources due to its encrypted messaging capabilities. Criminals can communicate on the app and delete their conversations, leaving no evidence behind. The platform has become a popular place for sharing images of child sexual abuse, according to law enforcement.[18] Amazon has announced that it will be shutting down the app at the end of 2023

Tox is a decentralized, encrypted messaging service that doesn't require registration or the submission of personal information like a phone number or email address. Tox encrypts data using peer-to-peer technology and the NaCl library, and users are identifiable by a Tox ID. Voice messaging and screenshot capture are available in Tox clients. Contacts may be added by providing their Tox ID or QR code. One consequence of Tox's P2P architecture is that Tox contacts can see each other's IP addresses, but a non-friend user can't easily discover a Tox user's IP address using only their Tox ID.

Discord is a popular chat network that gamers regularly use to interact with one another. It has, however, become a popular platform for cybercriminals, who use it to communicate and organize actions like distributing malicious files and conducting illicit activities. Discord is geared more toward gaming and requires users to join a server in order to communicate with others. It allows up to 500,000 users to communicate with each other at once, making it a good choice for large groups.

For a cybercriminal, a combination of these chat applications is a natural state of operations. While Jabber, Wickr and Tox are used for personal conversations, Telegram and Discord are the only tools that allow the creation of communities, with Telegram being significantly more popular among cybercriminals.

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

Section #2

Types of Crimes

Focus

Personal & Corporate Data

- **Personal data** rrefers to information that relates to an identifiable individual. This can include a wide range of information, such as name, address, phone number, email address, date of birth and financial information. Personal data is often collected by organizations in the course of their business operations.

- **Corporate data** refers to information that is owned by a company or organization. This can include both personal data related to customers and employees, as well as financial information, and any other information that is relevant to the operation of the organization.

Telegram channels and groups are used as platforms to put up for sale and share all sorts of illicitly obtained data, such as information of regular users, corporate documents and accounts, source codes and more. In 2022, it became clear that the amount and diversity of data that can be found on Telegram is comparable to information seen on cybercrime forums and markets.

Selling Stolen Data

For example, usernames and passwords for online resources are readily available on a large number of Telegram channels and groups. The most popular account credentials include online streaming and food delivery services, gaming, retail, banking, mailing and social media. The following example highlights the Telegram channel "Netflix Account Cheap Seller Ott," which has over 100,000 subscribers and sells compromised accounts for Netflix, Spotify, YouTube and several other services. Potential buyers can select the accounts they wish to purchase according to their validity length (i.e., a month, three months, six months, etc.) and according to their country of interest (US, UK, India, etc.).

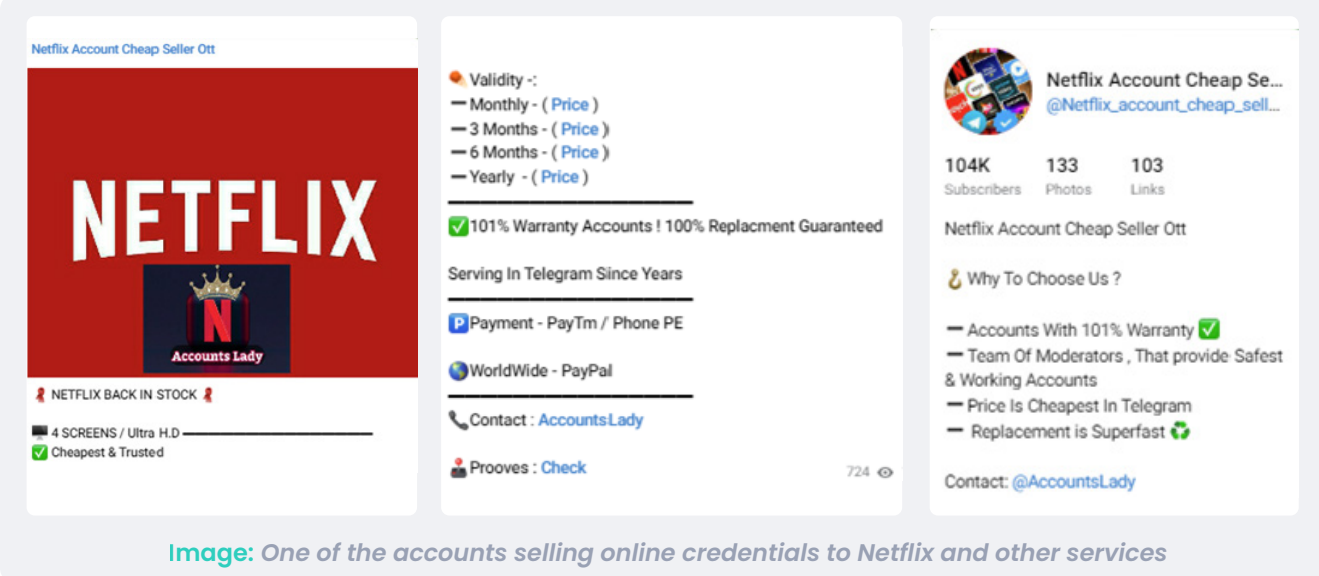
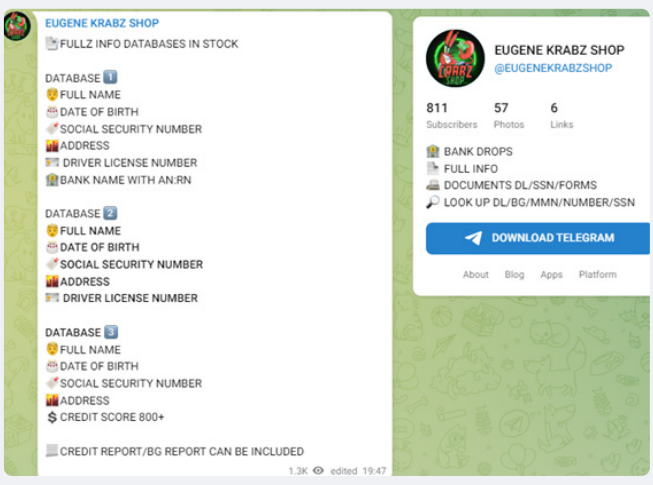


Image: *One of the accounts selling online credentials to Netflix and other services*

Similarly, many channels advertise the sale of online banking credentials, which are very sought after in hacking communities. Channels that are dedicated to the sale of such data can be found through a simple search using Telegram's search bar or through an open-source search engine.

Cybercriminals also use Telegram channels to sell and share a wide range of personal

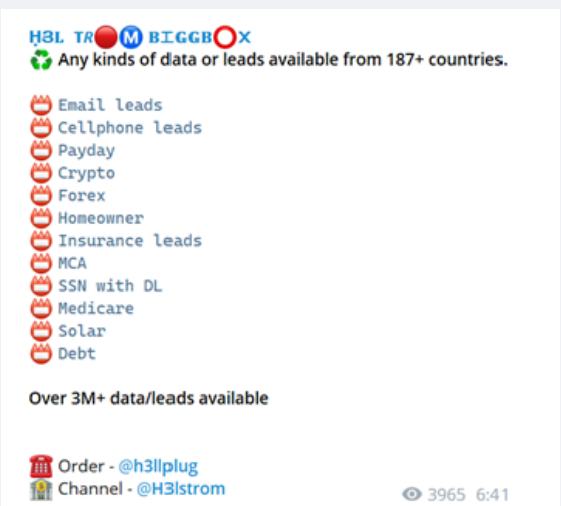
identifying information (PII), including Social Security numbers, driver's license numbers, passports, dates of birth, and physical and email addresses. Below is the channel "Eugene Krabz Shop" (@EUGENEKRABZSHOP), where information databases are offered for sale and can be purchased by messaging the channel's administrator:



The above post announces the availability of databases that consist of full name, date of birth, Social Security number, address and driver's license number, and that can include bank names and credit score data.

Other offerings include databases with different content types, such as "homeowner," "insurance leads" or "Medicare," but also from various countries as stated in the example below, which claims to have data from over 187 countries:

Image: *A Telegram post from the channel @h3lstrom*



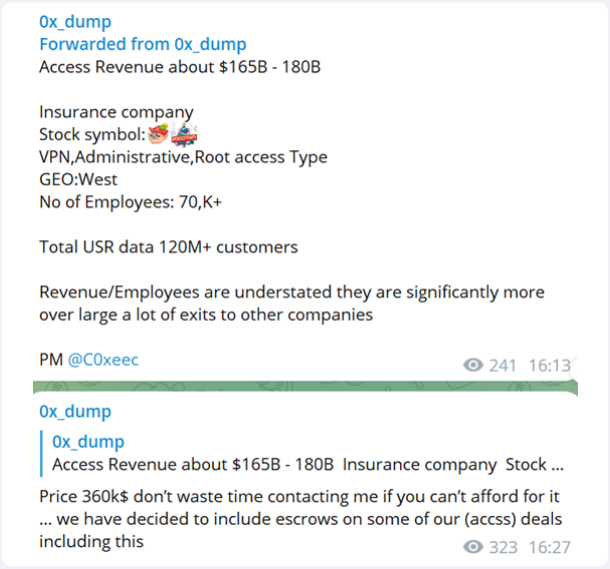
Threat actors may abuse such information to conduct various types of fraud involving the exploitation of stolen identities, including contracting bank loans and opening up bank accounts.

While some information mentioned above harms mostly end users (think of a Netflix or bank account owner), in Telegram there's plenty of data that poses high risk to companies.

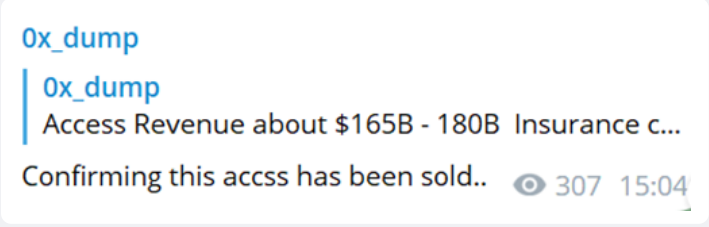
For example, a compromise can begin with initial access to organizations' internal resources (usually in form of credentials and the compromised URL) which can be found offered for sale in Telegram. An actor operating the private Telegram channel "0x_dump" constantly advertises such offers.[19]

[19] Register on KELA's platform and see a ***report about the 0x_dump channel***, including details on the threat actor behind the channel identified as a Kenya-based individual.

One of the recent examples is the alleged access to an insurance company with a revenue of "about $165B - 180B" which they claim has over 120 million customers. The threat actor set a price of $360,000 for the access.

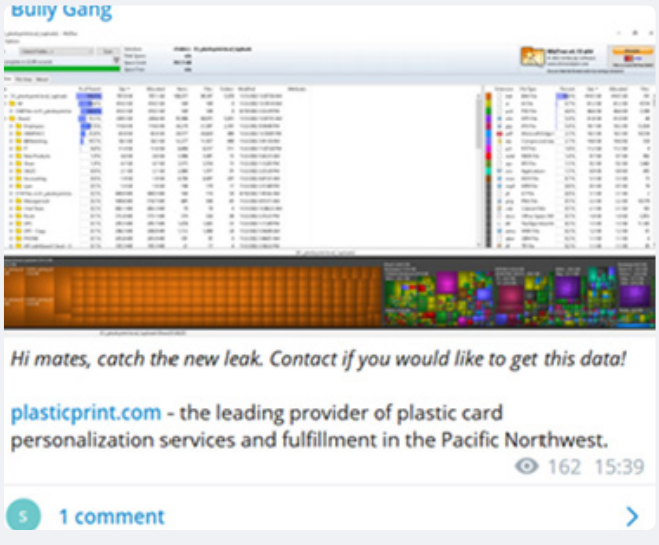


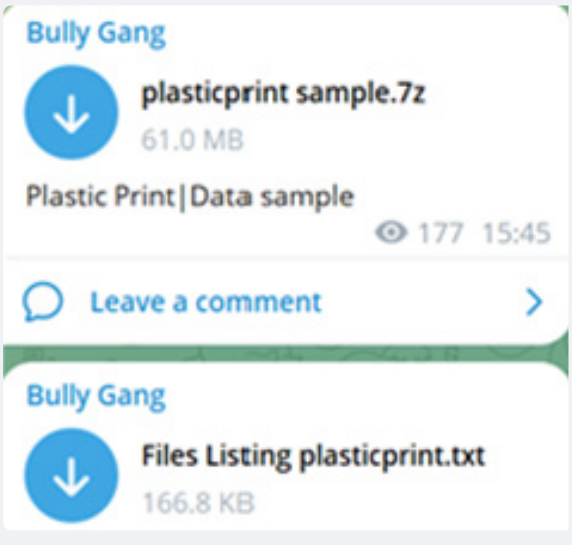
The following day 0x_dump announced that the access had been sold:



Once sold, initial access often leads to malicious intrusions and data exfiltration, with this data possibly being sold or leaked later.

The self-proclaimed ransomware group Bully Gang discloses its victims' names on its Telegram channel and offers the alleged victims' data (accompanied with samples) for sale, as can be seen in the example below:[20]

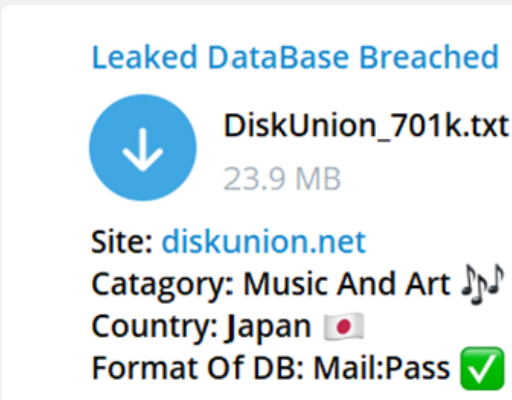




[20] Ransomware and data extortion actors operating via Telegram will be covered in more detail in a separate chapter: ***"Focus: Ransomware and data extortion groups."***

Corporate data exposed by such actors can include contracts, financial information, HR files, developer documentation, sensitive credentials to internal tools and services, intellectual property, trade secrets and proprietary information, and employee and customer data.

While both personal and corporate data are considered to be valued information, they're not only offered for sale but are leaked on an everyday basis. For instance, the threat actors operating the channel "Leaked DataBase Breached" were observed posting databases that their subscribers could download freely. The following example shows a data dump from the Japanese chain of music stores which includes over 700,000 records:



Some well-known cybercrime forums have their own Telegram channels, often used for general announcements (site going offline, new forums' guidelines/rules, etc.) but also to advertise the availability of new content, such as leaked databases. For instance, the popular English-speaking data leaking forum named BreachForums has an official Telegram channel such as previously described:

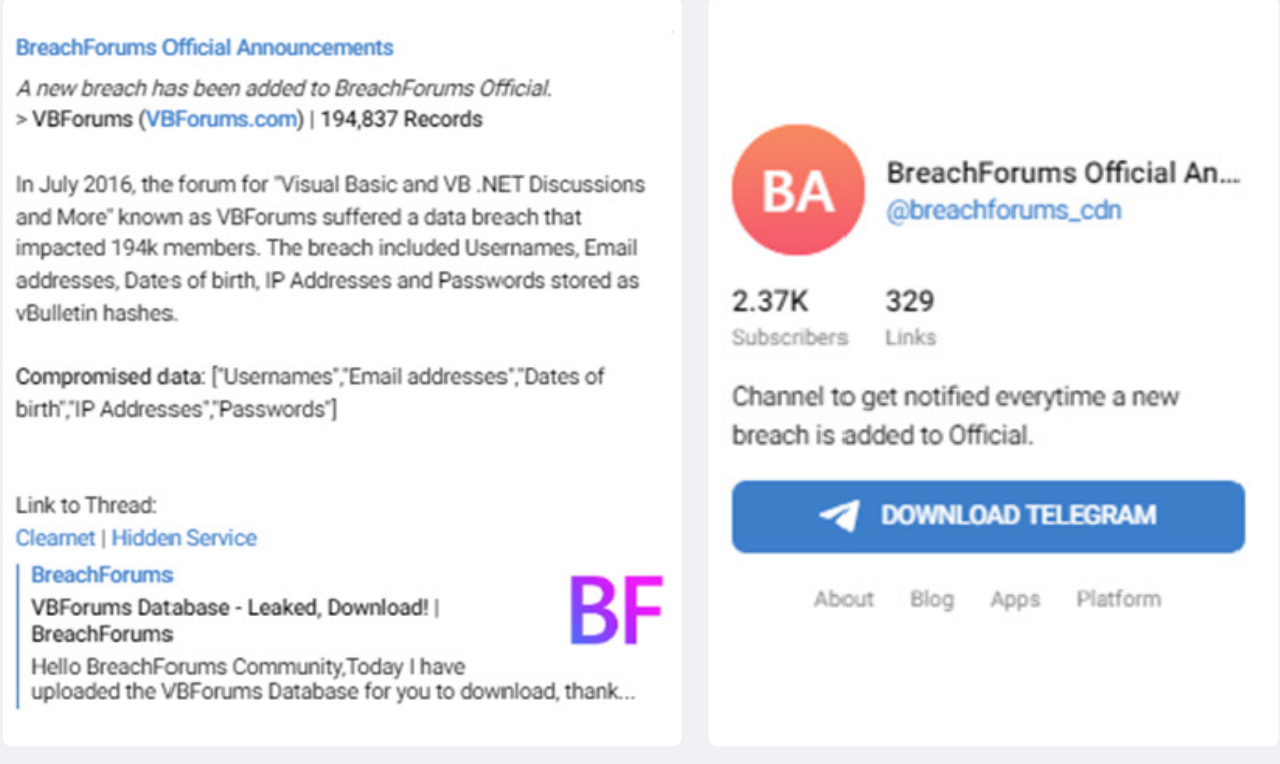


Image: *A screenshot from the Telegram channel @breachforums_cdn announcing the publication of a new database to its forum*

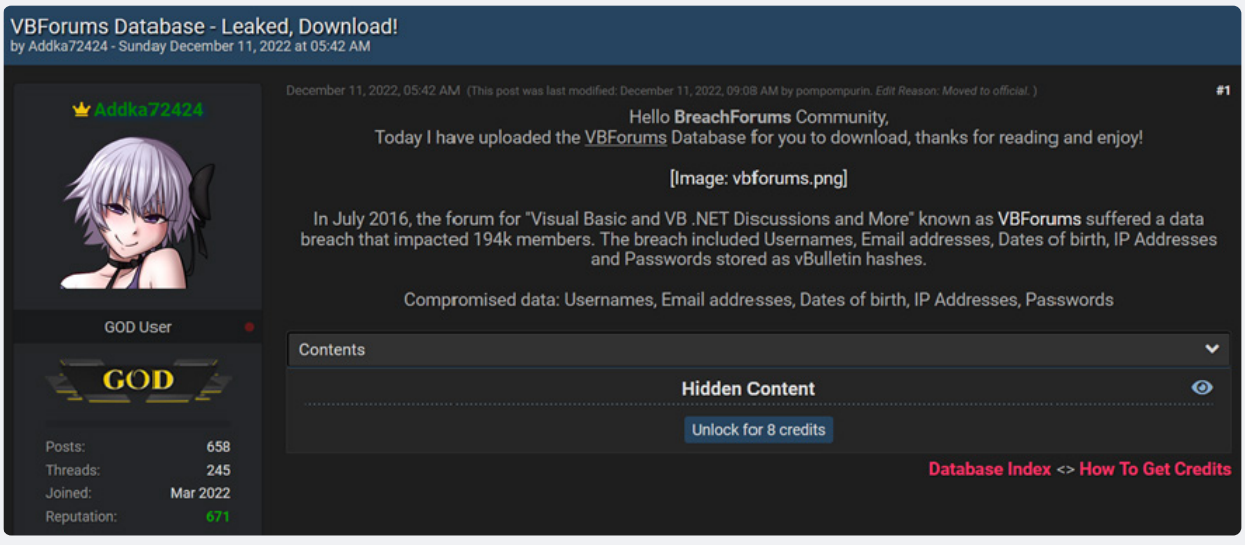


Image: *A screenshot of the post from BreachForums seen in the official Telegram channel*

Such leaks start a never-ending circulation of data among cybercriminals, and Telegram plays a vital role in this process.

Resharing Stolen Data

Once information is made public, it's common in cybercrime communities to reshare data. As a result, many corporate databases are posted numerous times on specialized Telegram groups and channels. Such channels and groups are easily available, and some have thousands of subscribers.

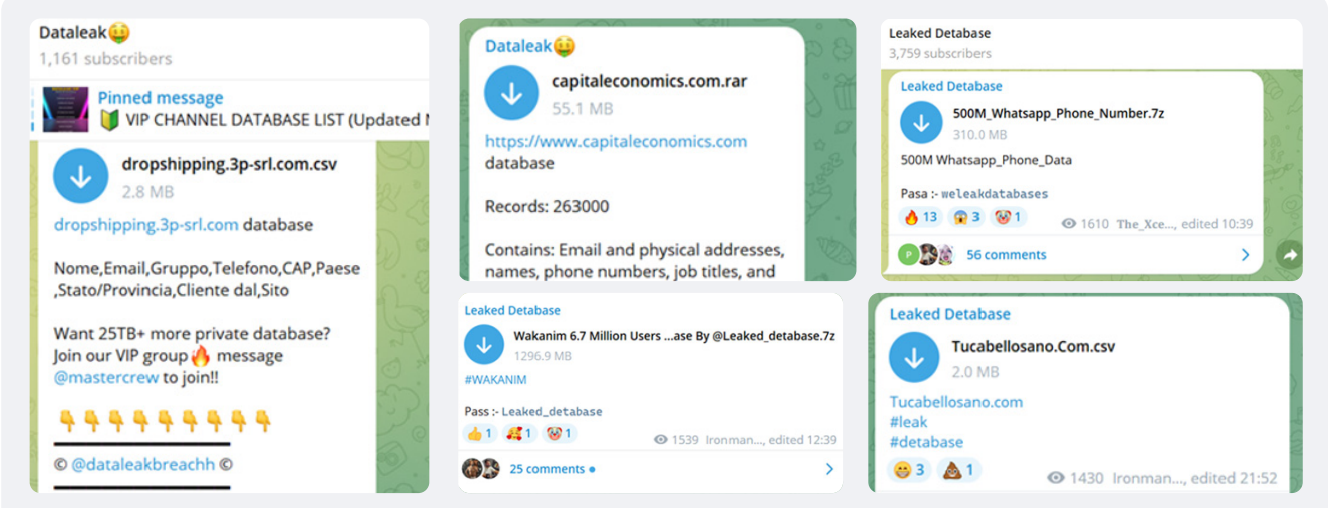
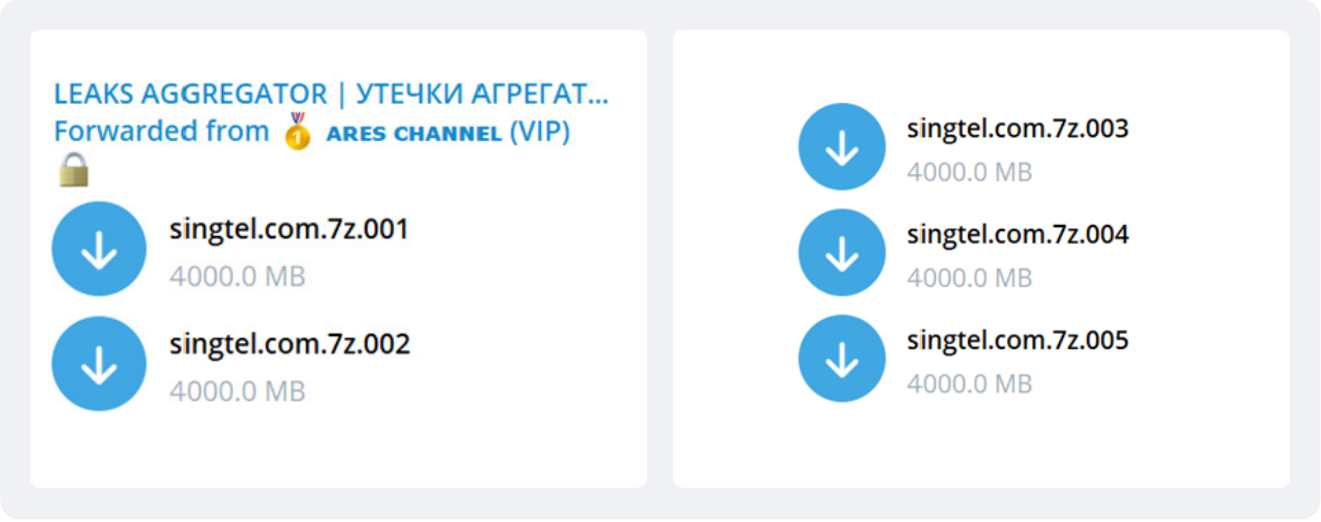


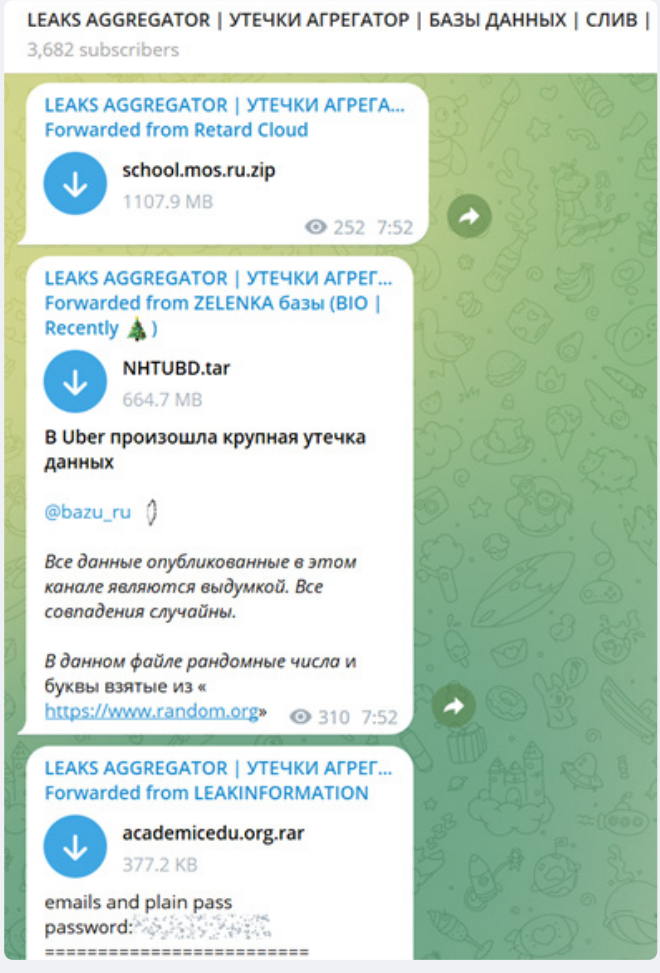
Image: *The "Dataleak" (left) and "Leaked Detabase" Telegram channels where corporate databases are shared*

Data leaked by ransomware and extortion gangs is often found on such Telegram channels. For example, Singapore Telecommunications Limited, also known as Singtel, was claimed as a victim of the Clop ransomware in February 2021; the company's data was posted on the ransomware public "shaming" website (blog). Soon KELA observed it reshared in the private channel "Ares Channel (VIP)," from there it was shared once more by "Leaks Aggregator," which is a public Telegram channel - and who knows how many more times?



Other Telegram channels aggregate data from many different sources and provide all the leaked data in their channel, making it easier for users looking for such data to browse the available information. The channel titled "LEAKS AGGREGATOR | УТЕЧКИ АГРЕГАТОР | БАЗЫ ДАННЫХ | СЛИВ," as its name indicates, gathers public data leaks and aggregates them.

Image: *The screenshot above shows three leaks, which were first posted in three different Telegram-based sources and then forwarded to the Leaks Aggregator channel*



Such actors allow potential interested parties to acquire information more easily than cybercrime platforms do because they are more accessible; they don't require users to sign up and create an account. Therefore, when reviewing Telegram channels and groups, KELA often sees that the primary source of the leaked data is a cybercrime forum.

For example, a database from "axess.fr" was posted on Club Hydra Forum and shared on the "LEAKINFORMATION," "Leakbase.cc" and "Dataleak" Telegram channels:

Image: *"axess.fr" database shared on Club Hydra Forum*

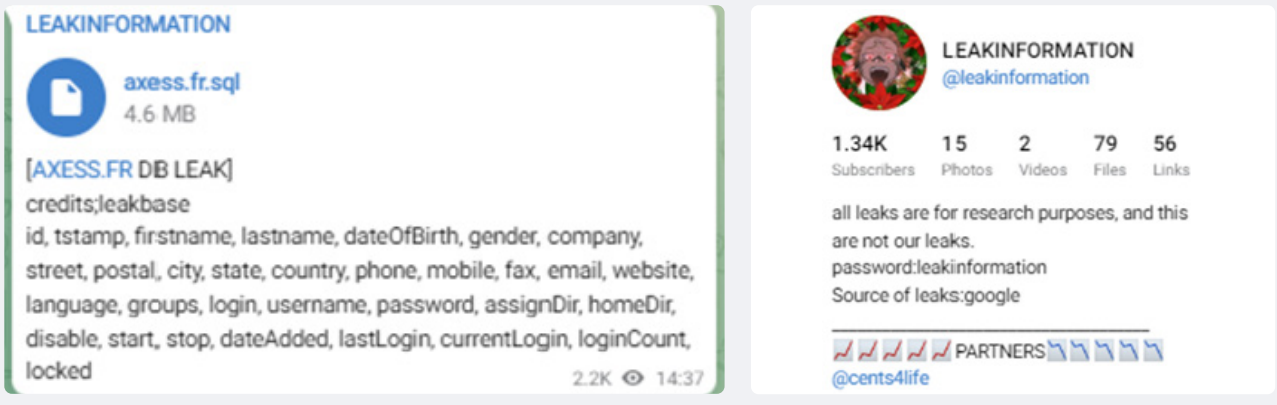


Image: *"axess.fr" database shared on LEAKINFORMATION*

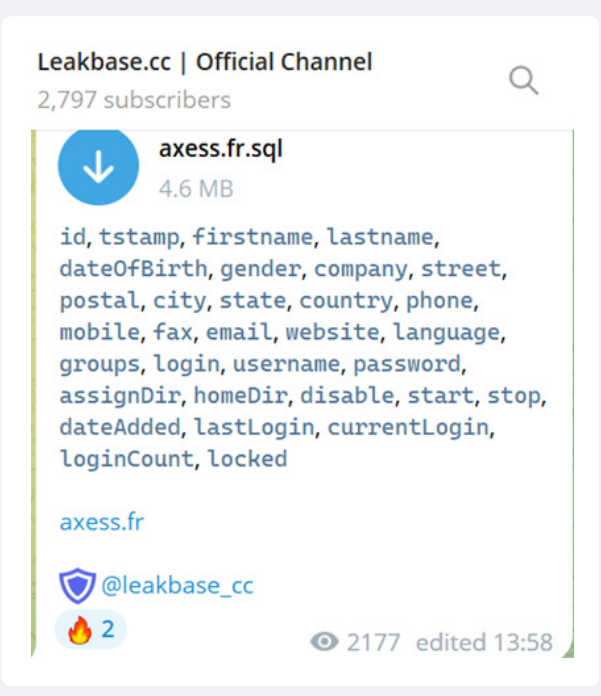


Image 3: *"axess.fr" database shared on Leakbase.cc*

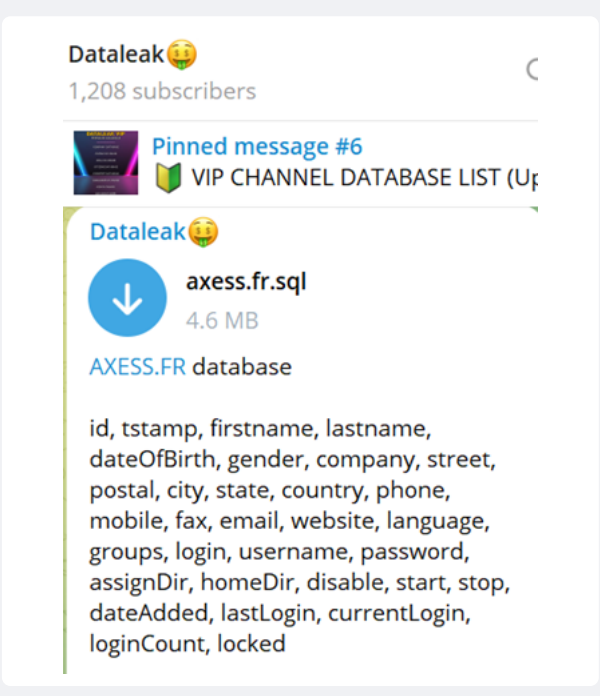


Image 4: *"axess.fr" database shared on Dataleak*

It is interesting to note that the data shared on forums is usually "conditionally free": it is often available against forum credits, which can be bought for a relatively cheap price but still cost money. The same databases are usually shared for free on Telegram, as once it has become public it is less valuable and may be distributed freely.

Case study for this chapter: SiegedSec

Why Telegram is Good for Cybercrime

Name	Description	Members or Followers	Language
Unsafe Internet	A database sharing channel	>1,900	English
Dataleak	A private channel that shares databases	>1,300	English
LEAKS AGGREGATOR | УТЕЧКИ АГРЕГАТОР | БАЗЫ ДАННЫХ | СЛИВ |	A data leaks aggregating channel	>3,700	Russian
0x_dump	A private channel that leaks its own databases	>900	English
Leakbase.cc	A database sharing channel	>3,200	English
A r e s ⚔️	A private channel where databases are shared and sold	>7,300	English
全球数据市场 Global Data Market	A channel that sells databases	>3,800	Chinese
Leaked Detabase	A database sharing channel	>3,700	English
MAKE 🏦THE💰BANDS 🇺🇸HERE🏧	A group that sells and shares banking data, PII and more	>7,000	English
Базы данных/ БД/ Утечки информации/Архив	A channel that shares databases and PII	>5,000	Russian
Hades Database	A channel that sells and shares databases	>1,600	English

Focus

Infomation Stealers

Clouds of Logs

- **Info-stealing malware** gathers information, usually credentials, from an infected machine. Stolen credentials "packages" are then referred to by cybercriminals as **"logs"** and the infected machines they came from - as **"bots"**. The information can be stolen through **commodity stealers** such as Redline, Raccoon, Meta and Vidar (working as malware-as-a-service), and **custom-made, private stealers.**

  The stolen information usually includes user login credentials, browsing history, cookies, authentication tokens and information about the user's machine. If purchased by threat actors, these credentials pose a significant risk to an organization, because they allow actors to access various resources that could result in data exfiltration, lateral movement and malware deployment.

  Logs can be sold on **automated botnet markets** such as RussianMarket, TwoEasy and Genesis, but they are also sold and leaked on cybercrime forums and across different platforms, with Telegram becoming one of the important channels to distribute logs. In recent years, a new type of product emerged: **"clouds of logs"**, meaning that threat actors are selling access to their collections of files via private cloud-based platforms for a subscription fee. These "clouds" can be hosted on file sharing platforms, such as MEGA or Yandex Disk, and Telegram is also becoming such a platform due to its ability to store big files, as observed by KELA.

Telegram became one of the popular platforms for cybercriminals to advertise, sell and leak logs harvested by information-stealing malware. Using the advantages of Telegram, actors created dedicated channels that allow access to credentials, helping cybercriminals to manage massive datasets and deliver large amounts of stolen data. When using legitimate file-sharing services for selling logs, cybercriminals have to deal with moderation that frequently deletes illegal information. Telegram's moderation is more lenient, attracting both sellers and buyers. Particularly interesting are actors who use Telegram to share their private logs collected by custom or commodity stealers. Traditionally they call them "clouds of logs" and offer to rent access to private Telegram channels collecting these logs. Some actors offer a small amount of logs for free as part of promoting their paid services.

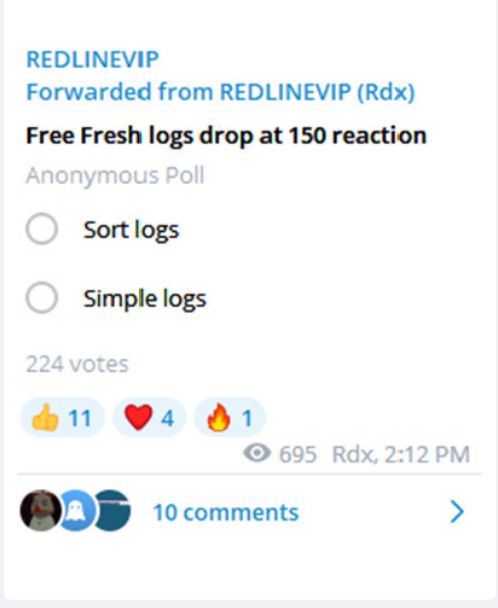


Image: *As part of promotion, some actors a number of reactions from users and then allow them to download free logs*

For "private" clouds, access is given usually via an administrator of a channel following the subscription payment. The prices vary among threat actors and are usually in a range of hundreds (for a month) to several thousand USD (for lifetime access). For example, in the channel "REDLINEVIP," the cheapest price is a weekly access for USD 200, while permanent access costs USD 2,200. In the channel "cBank [LOGS]", the premium logs channel costs USD 100 per week or USD 3,000 for lifetime access.[21]

[21] Register on KELA's platform and see a ***report on cBank [LOGS]***, containing information about the channel and identification of the threat actor behind the channel as a Russia-based individual.

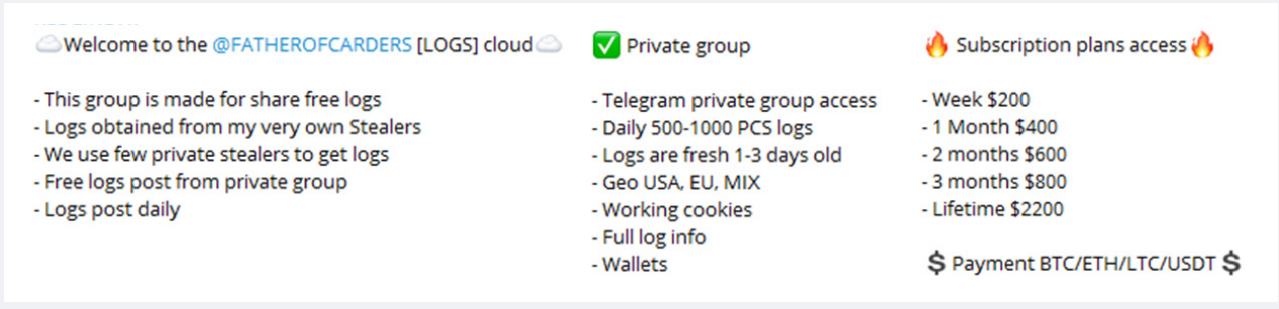


Image: *REDLINEVIP channel advertised the subscription plan*

The number of logs that could be accessed during the subscription varies. For instance, monthly subscribers on Snatch Premium Cloud would receive around 90,000 logs per month for USD 250. To provide more unique information, some actors limit the number of users who can access and buy logs: for example, "3 seats available in private cloud #1."

Image: *"ArtHouse Cloud limits the number of users accessing the cloud*

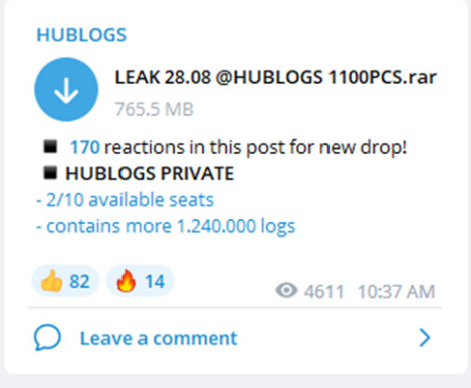


Image: *2 slots available of HubLogs Cloud*

Leaks of logs advertised for sale or for free sometimes include useful details regarding the leak, such as timeframe when the logs were stolen, geographies of the compromised machines, amount of logs, and source (information stealers).

When analyzing several most prominent Telegram clouds of logs, KELA found that the majority of the logs shared on these channels were obtained using the Redline stealer.

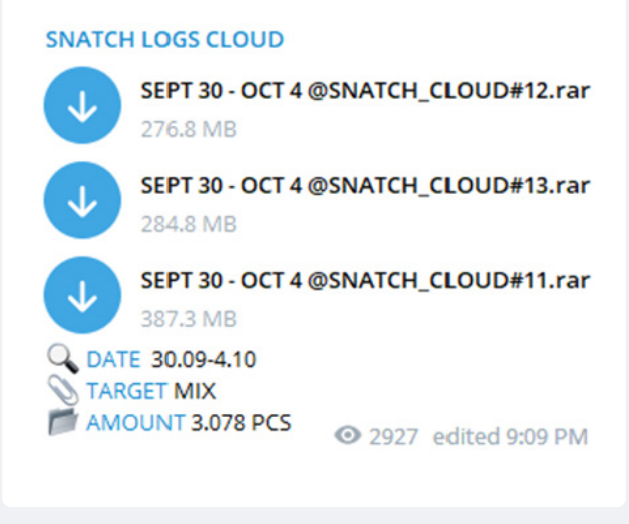


Image: *Post shared on Snatch Logs Cloud*

When analyzing several of the most prominent Telegram clouds of logs, KELA found that the majority of the logs shared on these channels were obtained using the Redline stealer.

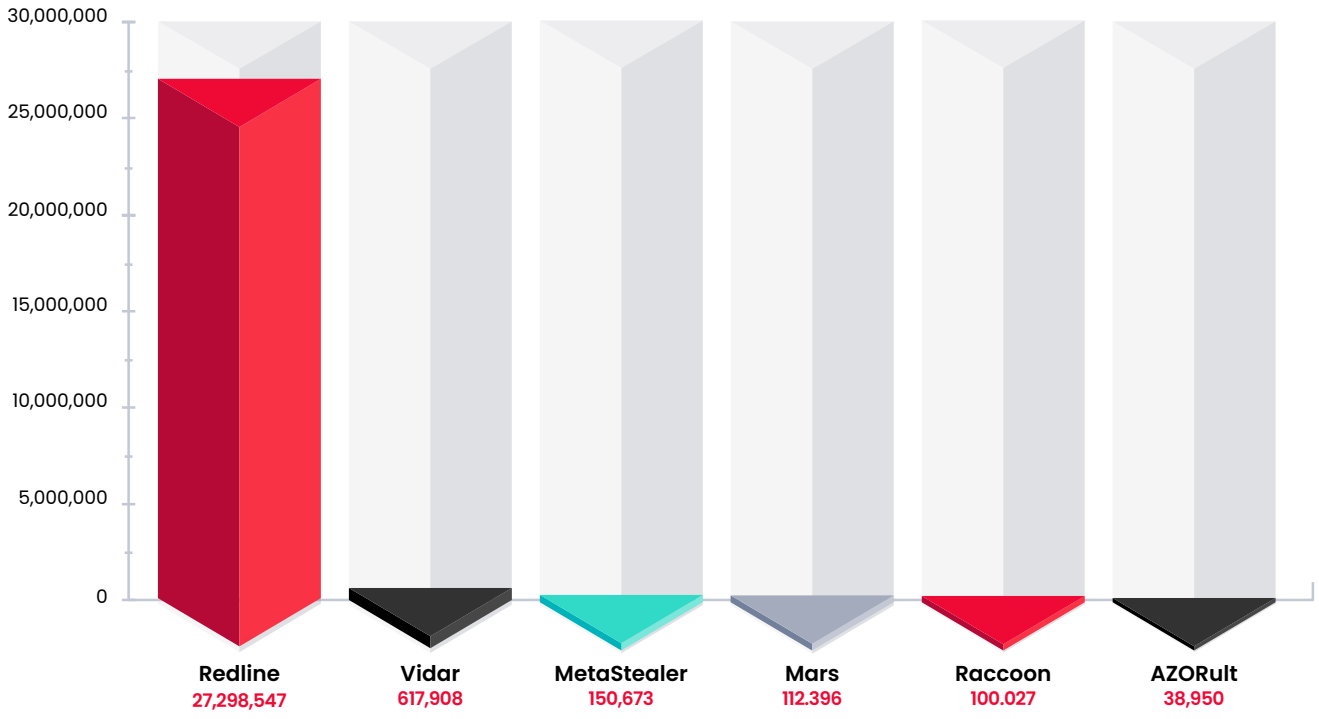


Figure: Distribution of bots offered for sale on Telegram channels called Snatch, Redlinevip and Cbank logs

As with all the data, once logs are leaked for free, they start to widely circulate across Telegram and other platforms, that are not necessarily focused on logs. For example, the threat actor named LeakBase (known for leaking databases on the BreachForums and operating their own site for the same purpose) is using a Telegram channel to share information coming both from their attacks and other threat actors. In addition to databases, the actor shares collections of logs, and the names of the files usually imply the logs were obtained via the aforementioned clouds, providing a glimpse into the most prominent log cloud services that exist in the cybercrime underground.

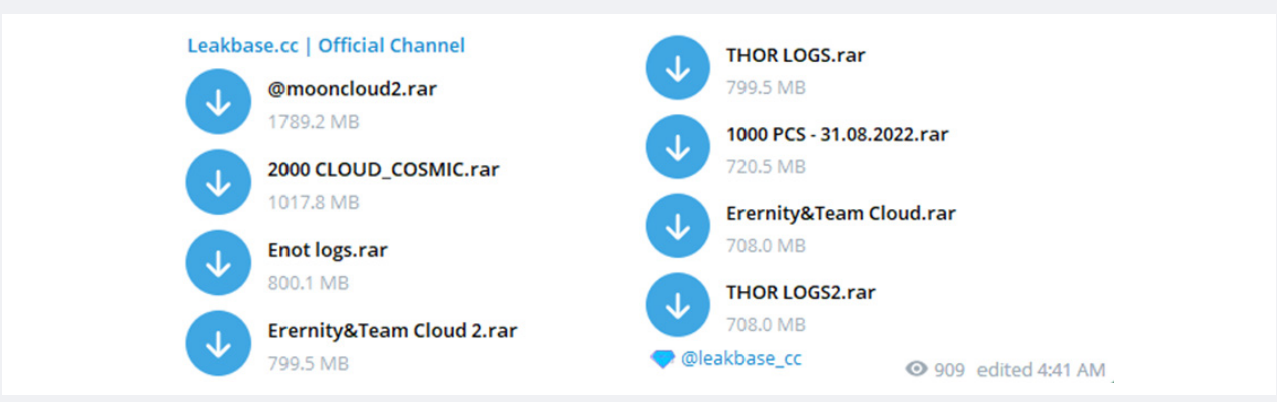


Image: LeakBase shares different logs files downloaded from different cloud services

Over the past years, cybercriminals have frequently used compromised credentials from logs as an entry vector, targeting high-profile companies such as Uber, T-Mobile and Electronic Arts.[22] Adoption of Telegram by actors using info-stealing malware increases the number of potential buyers and subsequently the number of victims.

[22] See KELA's blog: ***Defender-in-the-middle: How to reduce damage from info-stealing malware***

Info-stealing Malware Communities

- Commodity stealers operate as malware-as-a-service, providing access to their malware and admin panel for a fee. There are different threat actors involved in such operations, and they usually form **teams** to work with several stealers' operations. Teams' administrators acquire access to infostealers' malware by paying a subscription fee per month or for unlimited time. To spread the malware, they **hire traffers** — these actors are responsible for redirecting users' traffic to malicious content. A team's admin manages the traffers' team and provides them with **crypted builds** (a version of malware that has been created or compiled from its source code and obfuscated to evade detection). Traffers spread the malware, using the teams' delivery methods, and gain money based on the quantity and quality of logs generated by each infection. Admins employ stolen logs for further attacks or simply sell them.

Telegram is used by actors employing info-stealing malware not only to sell and share harvested data. Commodity infostealers provoked the emergence of cybercriminal gangs and teams working together to infect as many people as possible. To coordinate their activities, many use Telegram, creating all types of tools: channels for hiring new traffers and advertising the team, public and private chats for coordinating activities and discussions, and Telegram bots for automating tasks, payments and more (see the next section).

In their turn, administrators of commodity infostealers' affiliate programs use Telegram to promote their activities, announcing and releasing updated versions of infostealers on dedicated Telegram channels. Telegram has become a vital tool in the infostealers' landscape that has expanded this year, giving different threat actors the opportunity to take part in the infection chain and facilitating the process.[23]

Telegram Bots Used by Infostealers

When it comes to infostealers, Telegram is used not only to form communities and collaborate. Because this messenger allows the creation of bots that can interact with outside platforms, it has become a valuable tool to be used in infostealers' command and control (C&C) infrastructure. It's mostly used to save and share data harvested by malware.

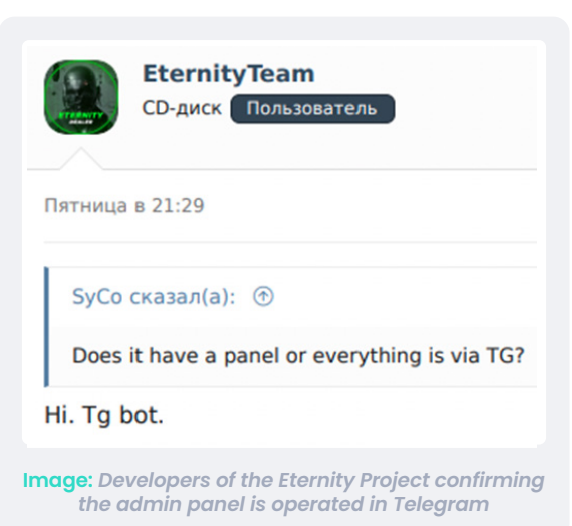


Image: *Developers of the Eternity Project confirming the admin panel is operated in Telegram*

For example, the Eternity Project, which is malware-as-a-service, uses Telegram bots to sell stolen information to actors who bought access to the service and to provide them with an opportunity to build the binary. The stealer doesn't have an administrator panel to manage the malware and attacks — everything is done via Telegram, as the project developers say.

[23] See KELA's report: ***The Next Generation of Info Stealers***

Some other projects that offer to send stolen logs through Telegram include Agrat, Ikarus and multiple unnamed stealers, all of which have relatively low prices (lifetime access for USD 100–300). Therefore, it seems that Telegram allows less skilled or less resourceful malware developers to easily build C&C infrastructure for their projects.

Telegram bots for infostealers are also offered as standalone projects that can be used with different malware-as-a-service. For example, developers of SantaresBot offer to administrators of teams manage their traffers via Telegram. The bot allows them to distribute builds to traffers, receive logs and check if they are valid, communicate with team members and more. The bot allows customization for each user and claims to work with Redline, Racoon, Meta, 000 and Aurora stealers, but the developers also mention they can implement any stealer that automatically saves stolen logs. Many other bots offer similar functionality and additional features, such as crypting infostealer builds through Telegram, incorporating builds into alleged benign files and more.

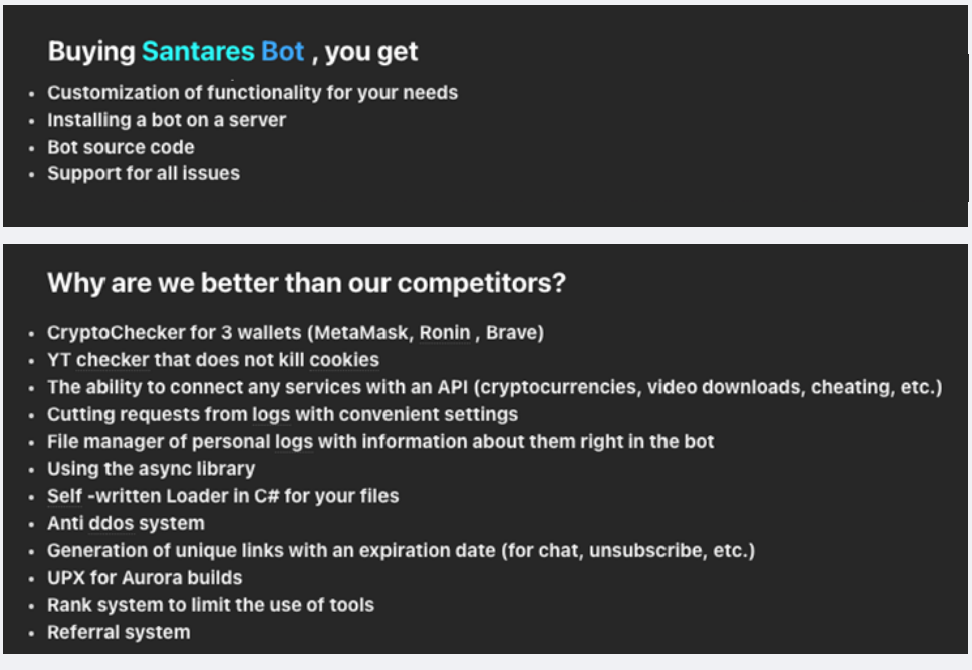


Image: *SantaresBot advertisement (auto-translated from Russian)*

Telegram bots are used in C&C infrastructure of different malware strains, but especially in the infostealers community they have become a valuable and popular tool.

Case study for this chapter: REDLINEVIP and Palm Team

List of Prominent Groups and Channels

Name	Description	Suscribers	Language	Created
REDLINEVIP	Free logs and access to private cloud	>6000	English	Sep 2021
Snatch logs cloud	Free logs and access to private cloud	>5800	English	Sep 2021
LOGS ARTHOUSE CLOUD	Free logs and access to private cloud	>5300	English	Sep 2021
Cosmic CLOUD	Free access to logs and private cloud	<5000	English	Aug 2021
HUBLOGS	Free logs and access to private cloud	>4850	English	Jan 2022
LeakBase	Free logs and dumps and access to private cloud	>3300	English & Russian	Jan 2022
SHARKCLOUD	Free distribution of logs	>3100	Russian	Sep 2022
DaisyCloud	Free logs and dumps and access to private cloud	<2500	English	July 2022
Total Cloud | Агрегатор логов	Free logs and access to private cloud	<2300	Russian	Dec 2020
Noxy Cloud	Free access to logs and private cloud	>1400	English	Aug 2022
METASTEALER OFFICIAL	META stealer	>7740	Russian	Aug 2022
AURORA BOTNET | STEALER	Aurora stealer	>3300	Russian & English	May 2022
Blackwalter	Blackwakter stealer	>1800	English	March 2020
Eternity	Eternity stealer	>1200	English & Russian	May 2022
Rhadamanthys	Rhadamanths	<1350	English	Oct 2022
REIMANN CHAT	Reimann chat	<1200	Russian	May 2021

РАЙ ТРАФЕРА	**Traffers Paradise**	**<240**	**Russian**	**Oct 2022**
Palm Team	**Palm Team**	**<200**	**Russian**	**July 2022**
OverDox Team	**OverDox services**	**170**	**Russian**	**March 2022**
Sky Team	**Sky SEO team**	**25**	**Russian**	**Aug 2022**

Focus

Banking Fraud

- **Banking fraud** refers to criminal activities that target the financial institutions, their employees and their customers. These crimes can take many forms, including common attacks, such as phishing, and industry-specific attacks, including:
  - **Credit card skimming**, which involves stealing credit card information by attaching a device to PoS terminals or ATM machines card reader
  - **Card cracking**, which refers to the use of stolen or compromised credit or debit card information to make unauthorized purchases or withdrawals
  - **Money muling**, which refers to the transfer of money obtained through illegal activities through a series of transactions in an attempt to conceal its origin

More slang terms that are commonly used in the context of banking cybercrime include **shimmer**, which is a type of device used to capture card information from the magnetic strip of a credit or debit card when it's inserted into an ATM or other card reader; and **fullz**, which refers to a package of personal identifying information used to commit fraud or other crimes. The term is often used in the context of identity theft, and may include information such as a person's name, address, date of birth, Social Security number and financial account numbers. Threat actors may use this information to open new accounts or make unauthorized purchases or withdrawals.

- **Credit card markets** refer to platforms selling various types of credit cards, such as Omerta, Brian's Club and Yale Lodge. One of the types that the underground credit card market consists of is compromised cards with CVV/CVV2 information, which includes a three- or four-digit security code used for online or phone purchases. This type is the most targeted one due to the anonymity of "card-not-present" purchases, the potential for additional personal information to be included with the cards and the ability to use it immediately.

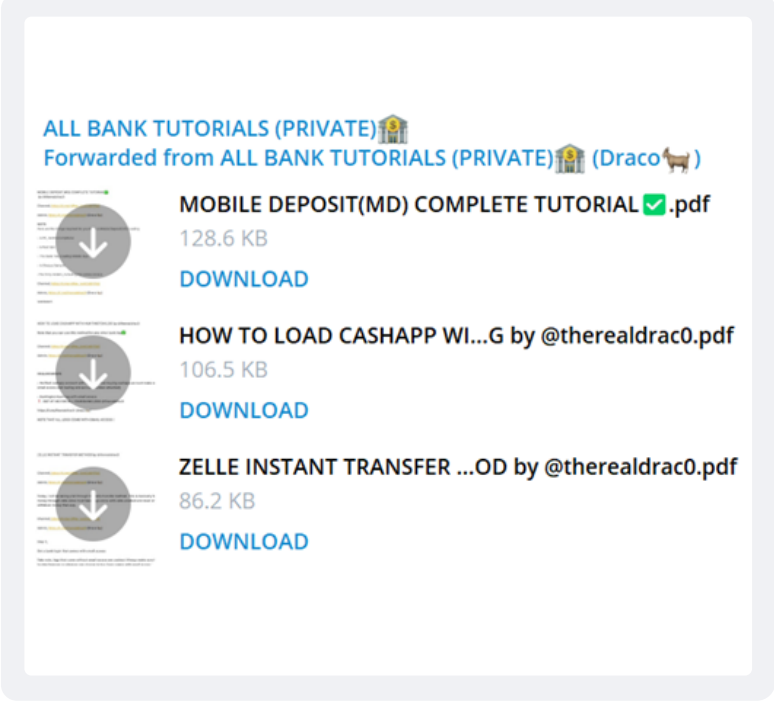
Another important aspect is checks that may be used in a variety of ways as threat actors may create and use **fake checks** to defraud individuals or businesses.

Cybercriminals also create **banking fraud tutorials** that include instructions on how to open and manage bank accounts, steal credit card information, fake checks and defraud individuals or businesses. These resources can be used by individuals who are new to banking fraud or who want to learn more about all this illegal activity.

- **Bank logs** refer to the details of an individual's account login information such as username, email, cookies, and account details. Cybercriminals use phishing techniques to obtain this information by creating fake login sites and sending them to targets. When a target enters their login information on these fake sites, the cybercriminals capture the information and use it for fraudulent activities.

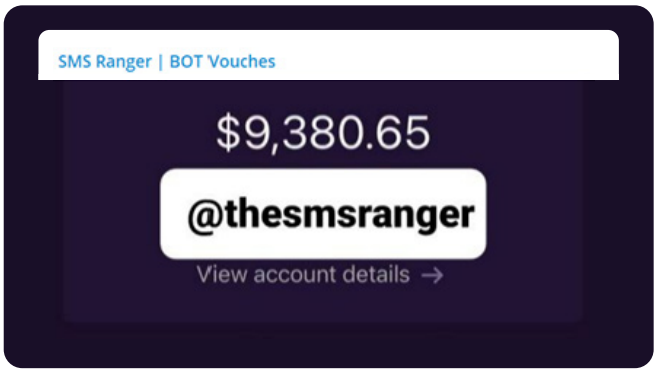
In the last few years, all activity mentioned above is happening in Telegram as well. It became a popular platform for banking fraud cybercriminals who created dedicated channels for advertising stolen credit card information and checks, fullz and financial accounts. Forged credit cards and banknotes are also a popular item for sale. For example, sellers claim that they provide a cloned ATM card with a PIN and add clear instructions:

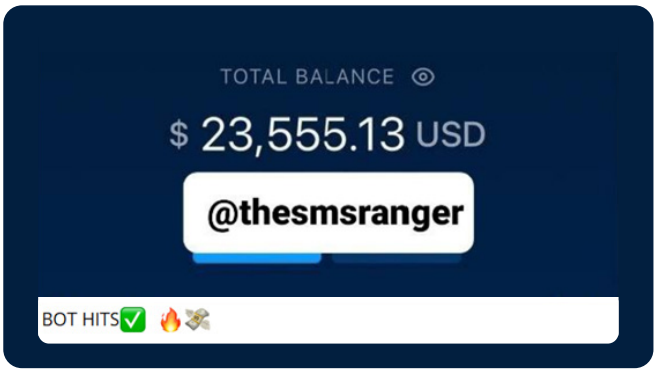
Counterfeit checks and stolen valid checks channels are common on Telegram. Fraudsters are sending those checks and money orders to other cybercriminals and to people as part of scam schemes, asking them to deposit the check into their bank account and return part of the money in cash or by wire transfer.



Banking fraud tutorials are also found on Telegram as actors want to share their knowledge. For example, the owner of the channel "ALL BANK TUTORIALS (PRIVATE)" shares some tutorials they have:

The use of Telegram bots allows actors to automate various attacks, among them operations targeting banking users. By using automated bot services to send these messages, actors can potentially reach a larger number of victims more efficiently or delegate social engineering to other cybercriminals for a fee. For instance, SMSRanger is an OTP & SMS capture bot that is capable of getting OTP & SMS codes from victims by impersonating a company or bank. In the Telegram channel 'SMS Ranger | Updates' which has around 7700 subscribers, the admin advertised some examples as proof of the bot's success:





Based on the channel, it seems that the bot allows to contact a targeted person and receive OTP, credentials, or other information:

1. *"Use the OTP as you please"*
2. *"Call the victim from SMSranger"*
3. *"When prompted, send the OTP to the victim by using their card or logging account."*
4. *"Our bot will capture the OTP when the victim types it in"*

Service is available per USD 399/month, and lifetime access costs USD 1900.

Case study for this chapter: CHECKS GRUB SHOP

List of Prominent Groups and Channels

Name	Description	Members or Followers	Language
The Bank ®	A channel that sells stolen credit cards	>3,940	English
CHECKS GRUB SHOP	A channel that sells stolen credit cards	>8,180	English
WhiteList	A channel that sells stolen accounts	>6,700	English
FraudStars	A channel that sells stolen credit cards	>9,600	English
BioH4zard Market	A channel for selling credit cards	>3,800	English
CHECKS AND SAUCE	A channel for checks	>980	English
The Glass House	A channel for checks	>2,300	English
Glass Tank Grubs	A channel for checks	>2,160	English
FREE GUIDES	Bank tutorials channel	>680	English

Focus

Ransomware & Data Extortion Groups

- **Ransomware** and **data extortion** groups refer to cybercrime groups that exfiltrate confidential data from organizations and threaten to leak it, demanding from victims a ransom payment. Ransomware gangs encrypt data using ransomware, while data extortion groups don't operate this malware but only steal data. Some of these groups operate blogs where actors leak part of the data or sell it to third parties.

In addition to blogs maintained by ransomware and data extortion groups, Telegram became an attractive platform for the promotion of attacks and capabilities of specific gangs. The messaging platform attracts a broader audience that has access to the leaks, compared with blogs usually located on the TOR network (some gangs have clearweb versions, but those are easier for providers to block). In terms of leaking data, Telegram allows users to upload large sets of information, which is crucial for such actors.

Some groups, such as RansomHouse, maintain Telegram channels in addition to their blogs, posting there the same leaks. But this year, a few extortion groups leveraging Telegram exclusively have gained popularity following their alleged attacks against high-profile victims. Following the attacks, the threat actors published the data on their Telegram channels, attempting to force the victims to pay ransom.

The most notorious groups are Lapsus$ and Stormous, both emerging in 2021 and gaining attention in 2022. They widely used Telegram features to publicize information about their alleged attacks, creating chats for discussions, dedicated channels for leaking data of a specific victim, and polls for increasing members' activities. For example, in April, Stormous published a poll on its Telegram channel asking its subscribers to vote for the group's next target.

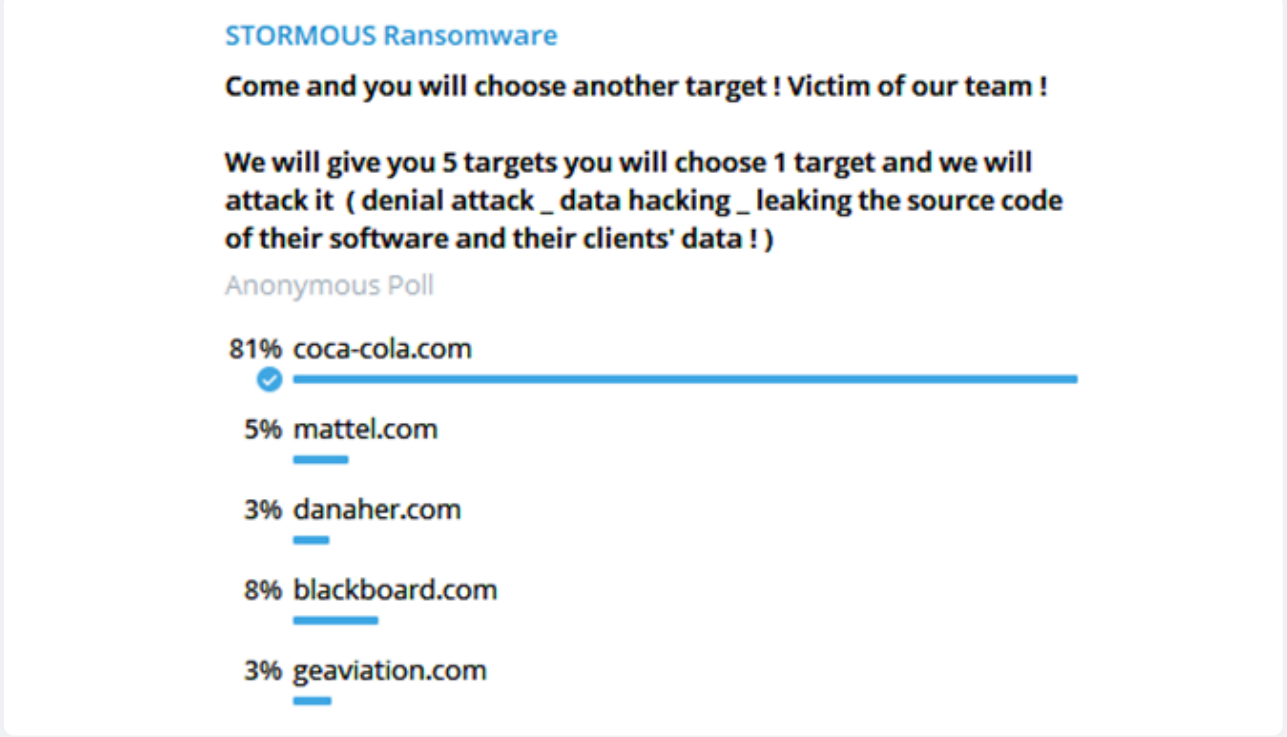


Image: *Stomous offering subscribers to vote for their next victim*

As opposed to one post about one victim on ransomware and data extortion blogs, such actors can send multiple messages, creating buzz around an attack. For instance, Lapsus$ used to share screenshots of one compromised victim day by day and urge their community to discuss the leaks.

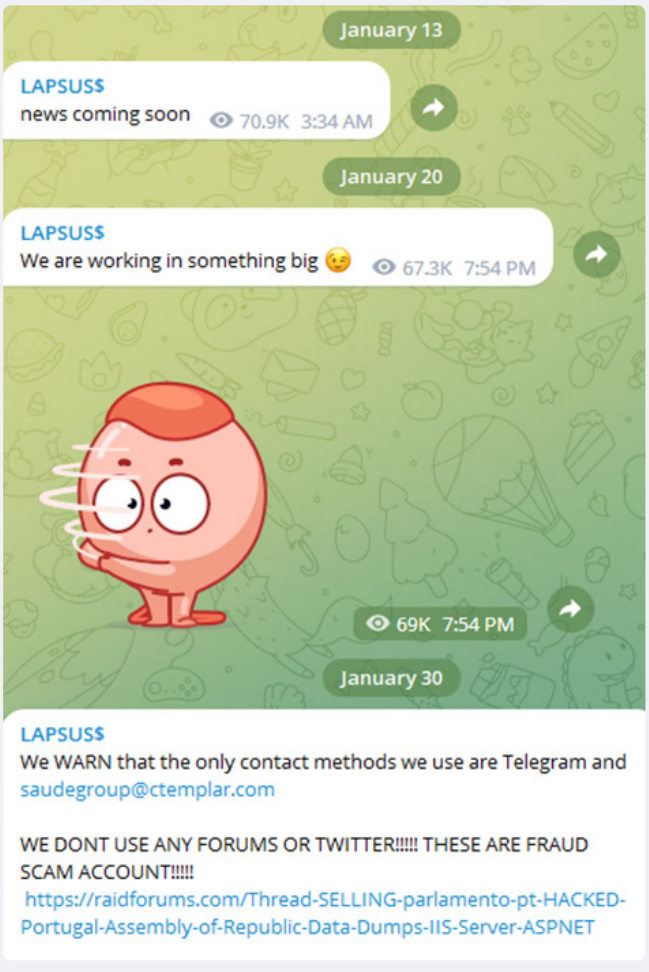


Image: *Lapsus$ creating tension around their activities*

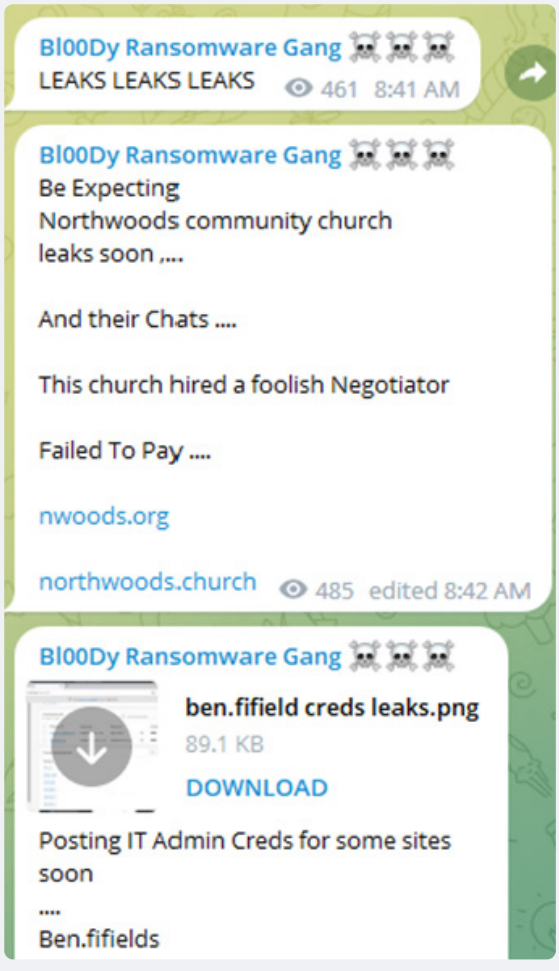


Image: *'Bl00dy Ransomware Gang', emerged in 2022, posted a few messages related to one victim*

It appears that less sophisticated actors mainly use Telegram. Most of them have the same rhetoric, drawing attention to themselves and communicating with followers on social media. Credibility of such groups is always questionable — for instance, for Stormous it is still largely unclear whether Stormous actually attacked most of its claimed victims. KELA observed data that was leaked on their channel being shared on cybercrime forums before.

Case study for this chapter: Lapsus$

List of Prominent Groups and Channels

Name	Description	Subscribers	Created
Lapsus$	Data extortion group	>55,800	December 2021
Stormous	Data extortion group	>2,900	April 2021
RansomHouse	Data extortion group	>2,000	March 2022
Bl00dy Ransomware Gang	Ransomware group	>1,300	July 2022
Bully	Ransomware group	>600	September 2022

Focus

Hacktivism

- The malicious use of computer technology by political or social activists to make a statement in support of their cause or ideology is referred to as **hacktivism**. Breaching a computer or a network is hacking, and defending or promoting an ideology or social view is activism; therefore, hacktivism is a combination of both. Hacktivists will oppose any entity that they believe to threaten their cause. They tend to target governments or institutions, but may also oppose corporations, religious groups, etc. Hacktivists also act to gain visibility for their cause or to send a message. Any organization may become a target, if their actions, or their government's actions, oppose the ideology of a certain hacktivist group.

Telegram became widely popular among hacktivists apparently due to the same features appreciated by the financially motivated cybercriminals: the ability to communicate with large groups of people via dedicated groups and channels, and the platform's lenient moderation policies. Therefore, for hacktivists, who need to draw the attention of the audience, share illegal actions and encourage others to follow their lead, Telegram seems to be a good match.

While many hacktivists have been using Telegram continually over the recent years, it seems that 2022 drove a large surge in the number of groups adopting the platform, mostly due to the Russia-Ukraine war. During the first 10 days of war, Check Point researchers noticed a sixfold increase in the number of groups concerning the conflict, with new groups created daily and some groups reaching over 250,000 users.[24] Ever since, both pro-Russian and pro-Ukrainian groups have been using Telegram abundantly to disclose their attacks and recruit supporters.

Toward the end of the year, another geopolitical event — Iranian protests — undoubtedly strengthened the use of Telegram by the hacktivists sympathizing with the resistance movement.

The most common type of posts in channels and groups managed by hacktivists, aside from general discussions and news, seems to be related to DDoS, defacement, doxing and information theft attacks that they performed.

All in all, the adoption of Telegram by hacktivism groups grew significantly in 2022, continuing the trend toward popularity of the platform among such attackers. With continuing geopolitical conflicts and the hacktivists' urge to receive support from the "ordinary" internet users (for example, through donating money or helping to perform DDoS attacks using their own computers), such a trend is expected to continue in the near future.

Case study for this chapter: Killnet and ALtahrea Team

[24] Telegram becomes a digital forefront in the Conflict

List of Prominent Groups and Channels

Name	Description	Members or Followers	Language
IT ARMY of Ukraine	A pro-Ukrainian volunteer movement	> 206 000	Ukrainian
Killnet	A pro-Russian movement performing mostly DDoS attacks	> 91 300	Russian
RaHDit	A pro-Russian group doxxing Ukrainian soldiers	> 69 000	Russian
Cyber Partisans	A Belarusian, pro-opposition movement mostly attacking Belarusian government	> 43 400	Belarusian, Russian
XakNet	An espionage team	> 36 500	Russian
Anonymous	International hacking collective	> 19 800	English
1877 Team	A pro-Kurdish group performing different attacks	>17 800	English, Arabic
Anonymous Russia	A pro-Rusian hacking group mostly performing DDoS attacks	> 12 500	Russian
Altahrea Team	A pro-Iranian group performing DDoS and defacement attacks	> 4900	English, Arabic
Phoenix	A pro-Russian group carrying out DDoS and defacement attacks	> 1300	Russian

Focus

Illegal Physical Products

Counterfeits of Luxury Goods

Different counterfeit products are sold through various Telegram channels, groups and users, with luxury goods being a perfect example. They are openly advertised counterfeits with notes that indicate the level of quality of the forgeries.[25] For instance, the Telegram channel "Outlet Luxury Brands Women's Room" sells counterfeit fashion items that copy a wide range of luxury brands, including Chanel, Dior, Balmain, Celine and Louis Vuitton. The fraudsters who operate this channel claim that their products are in "compliance of materials and other details 99.9%" compared with the original items.

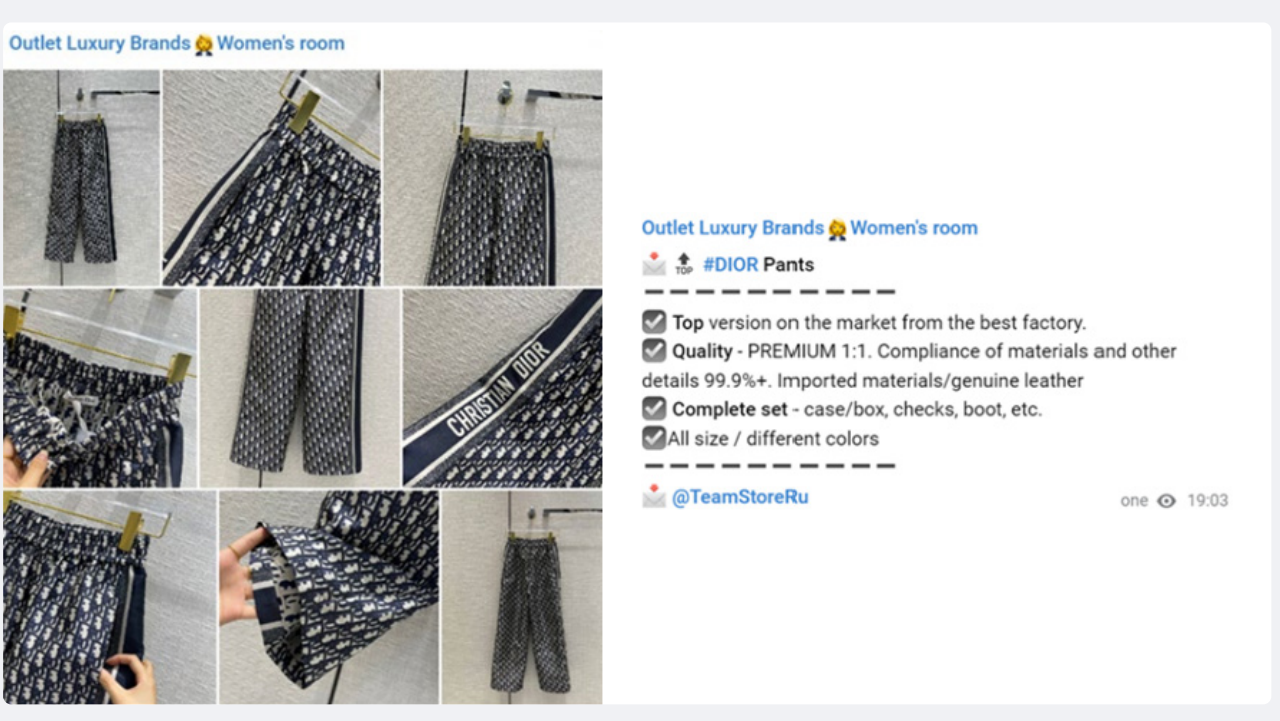


Image: *Telegram post advertising Dior counterfeits (automatically translated from Russian)*

COVID-19 Documents

During the pandemic, a surge in COVID-19 cases all over the world fueled a black market for counterfeit coronavirus tests and vaccination certificates (both fakes and valid certificates that were issued illegally), some of which were sold at prices ranging from USD 75 to USD 600. Many Telegram groups are still selling certificates and test results, making Telegram one of the largest selling platforms. The scam level in this area is huge: some certificates are of such poor quality that they're immediately recognized as fakes, and some sellers simply disappear once they receive payment.

Thousands of people join such groups and channels: for example, "Registered Digital COVID-19 Cert," who has more than 9,000 subscribers and was created only on July 28, 2022. The channel's admin @DrGeorgelowe also manages "UK NHS COVID-19 Vaccine Cert," and probably many actors in this area operate several groups dedicated to different types of products.

[25] See ***KELA's Top Luxury Brands in France: Threat Landscape Report***

The admins advertise their channels by scaring people to attract more subscribers:

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.

Drugs

Buying drugs online is a huge market, having several advantages as opposed to buying drugs in person:

- *Anonymity (drugs can be bought using a pseudonym and through a secure and encryptedconnection)*
- *Reduced risk of violence (as opposed to buying from a dealer, who might operate in a high-crime area)*
- *Quality control (drug sellers have a reputation and reviews of their products).*

Image: *Drug sellers posting proofs of delivered goods*

Generally, such services can be found on either dedicated cybercrime markets or marketplaces offering a wide range of physical goods. These platforms usually operate in the TOR network and can be hard for regular users to find and reach. Telegram, on the contrary, doesn't require any knowledge of the cybercrime ecosystem and allows users to perform the whole process in a few clicks. To search and locate relevant channels, buyers use a search bar or channels that aggregate information from sellers (for example, "Telegram Reviews"/@gangareviews). In the channel, a potential buyer selects the product that interests them, and pays for the service using cryptocurrency, contacting a support person or admin in direct messages. A downside of using Telegram for such activity is that information on sellers' reputation is scarce. The platform does not provide dedicated tools for customer reviews, and as such a buyer can only count on comments from other alleged buyers (if those are at all enabled in the channel).

It is possible to find popular channels that sell drugs and that have 15,000–30,000 followers in each. Such channels gain a lot of followers quickly. For example, the

"Mushrooms Doctor" channel was created only on October 28, 2022, but by the end of December it had rapidly reached more than 2,400 subscribers, most likely due to advertisements in other related channels. As for profits, a recent case involving the arrests of two drug dealers shows they made 3.7 million British pounds by selling different types of illegal drugs using Telegram.[26]

Guns

Cybercrime markets are used to sell a range of weapons from around the world, including automatic assault rifles, explosives, anti-tank missiles and rocket launchers. While guns seem to be harder to sell than other products, such offers still exist on Telegram. KELA observed numerous channels where sellers post pictures of the weapons with descriptions, prices and pick-up locations such as Syria and the US, while buyers can post requests or send direct messages to negotiate prices and meet-up locations. For example, the "GUNS AND ARMS SHOP" channel was created on July 31, 2022, and has over 100,000 subscribers. The shop is located in the US, and the channel admin is @gunssadmin1, who offers for sale "top quality brand new firearms" with anonymous packaging, shipping and worldwide deliveries and claims he sells the best pistols and rifles. The price range is USD 180 to USD 6,500.

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

Section #3

Recommendations for cybercrime researchers

In recent years, Telegram became a hub for various types of cybercrime activities. While there are other messaging apps favored by cybercriminals, Telegram is one of the most popular and presents a significant challenge for defenders trying to combat cybercrime on the platform. From ransomware and extortion actors to hacktivists, threat actors have widely adopted Telegram in their activities. Based on the current trend of increasing cybercrime activity on the platform, it's likely that Telegram will continue to be a popular choice for cybercriminals in 2023 and beyond. For security researchers, investigating crimes on Telegram may be difficult, because researching Telegram requires certain skills and knowledge.

The app's features and design make it tough for security experts to gather evidence and hunt down offenders. The app's use of anonymity, the ability for users to establish many identities and easily switch between them, the feature that allows users to delete conversation at both sides and to set a self-destruct timer for messages, as well as the use of non-personal phone numbers make researching criminality on Telegram a difficult process. Furthermore, Telegram's enormous and active user base makes monitoring and investigating all platform activities challenging.

One of the biggest difficulties for researchers in the application is that native search capabilities are limited. A search for content can only be performed within a specific community – if it is at all accessible to the user. Therefore, when researchers try to find a particular message or group, they will most likely not reach the desired result. There are various search engines created by platform users that aim to close this gap. These services crawl groups and channels and create their own databases to enable such search.

Private chats that can only be accessed if a user has an invite URL, and that aren't visible in the normal search, create an additional level of difficulty. For example, a hacker offered access to Medibank for sale in a private Telegram channel that could only be accessed using an invite link. A few weeks later, Medibank suffered a cyberattack and subsequent data leak, which might have been related to the sale of said access.

All of these factors make it challenging for researchers to study the behavior and activities of cybercriminals, and can hinder efforts to prevent and mitigate future cyberattacks. The difficulties of manually detecting cybercrime on Telegram emphasize the necessity for security researchers to adapt and develop new methodologies and tools for tracking and reducing cybercrime on the network. Working collaboratively with law enforcement agencies and using new technology to increase their capacity to obtain and evaluate evidence from encrypted conversations may be part of this.

There are several recommendations for defenders fighting against threats emerging on Telegram and organizations researching cybercrime:

- Using threat intelligence monitoring solutions to continuously monitor for potential threats on the platform and take proactive measures to prevent them
- Regularly training and educating employees on how to identify and respond to cyber threats on the platform

- Implementing technical controls, such as firewalls and intrusion prevention systems, to prevent cybercriminals from accessing sensitive data
- Increasing collaboration and information sharing with law enforcement agencies and other organizations to improve the ability to detect and disrupt cybercrime on the platform
- Conducting regular audits and assessments to identify any vulnerabilities or areas for improvement in the organization's defenses against cyber threats on the platform

Section #4

Apendix 1. Case Studies

Personal and Corporate Data: SiegedSec

For the showcase of this chapter, KELA chose an unusual channel that isn't financially motivated, as many of the aforementioned channels are. Nevertheless, the data it publishes seems to pose a serious risk.

The Telegram channel "SiegedSec" was created in April 2022. Its operators share corporate, education and government-related databases. The group also defaced a large number of sites and posted proofs on its Telegram channel. While the actors haven't stated their goal, it appears that they use their Telegram channel as a platform to promote their work and show off their hacking skills. The group operating this Telegram channel is linked to the actor behind the Twitter account @YourAnonWolf. Some of the attacks claimed by SiegedSec on their Telegram channel were also publicized by @YourAnonWolf on BreachForums:

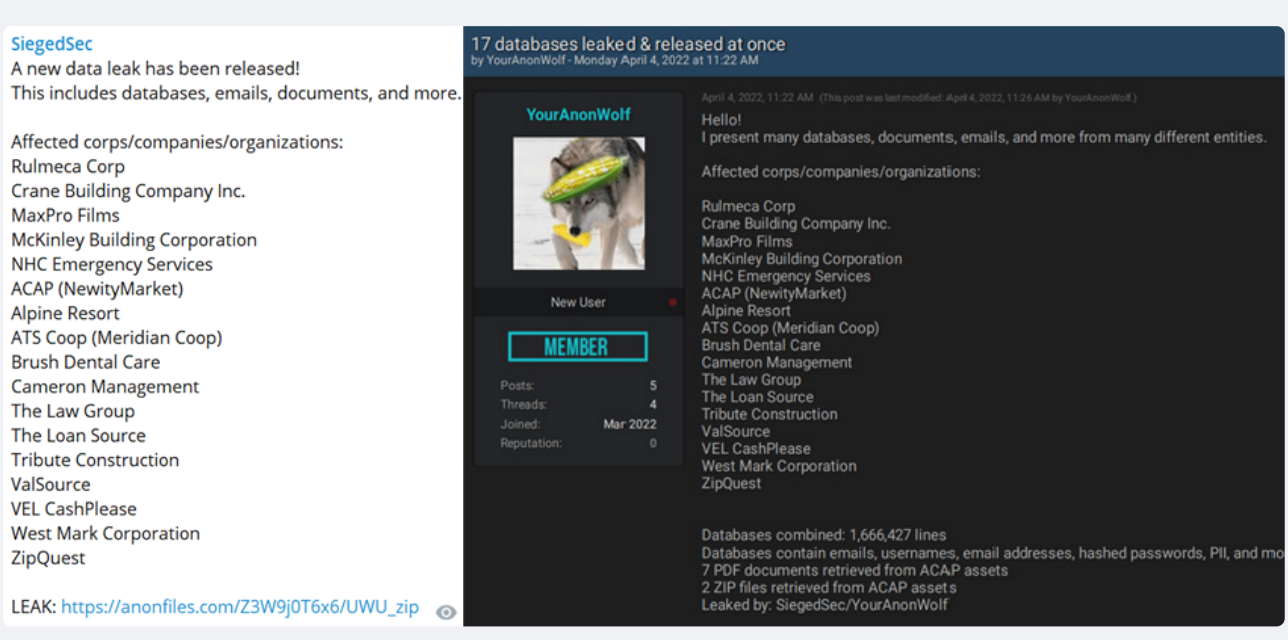


Image: *A post from SiegedSec's Telegram account about the leak of 17 companies (left) and a post from BreachForums by YourAnonWolf about a data leak of the same 17 companies*

In September 2022, the group members disclosed that YourAnonWolf had stepped back from its cybercriminal activities but stated that SiegedSec would go on. The group says that they are not involved in hacktivism, but in September, they announced that they would side with Ukraine in the cyber war opposing it to Russia.

Information Stealers: REDLINEVIP and Palm Team

REDLINEVIP

The REDLINEVIP channel has gained popularity among threat actors in the cybercrime underground since its creation in September 2021. The owner of the channel, Rdx (@Fatherofcarders), started sharing logs also on the carding forum CrdPro in October 2021, and a month later the channel was promoted on other cybercrime forums as RaidForums and BHF. The operators of the channel started posting free logs promoting their paid private clouds. The posts on the channel included polls to understand the buyers' preferences.

Image: *A poll showing the most popular targeted country*

It seems that the channel posted credentials harvested mainly from Redline infostealer malware and their private customized stealers. Over the year, the operators have increased the prices, almost doubling the price for permanent access to the private logs cloud service, from USD 2,200 to USD 4,000.

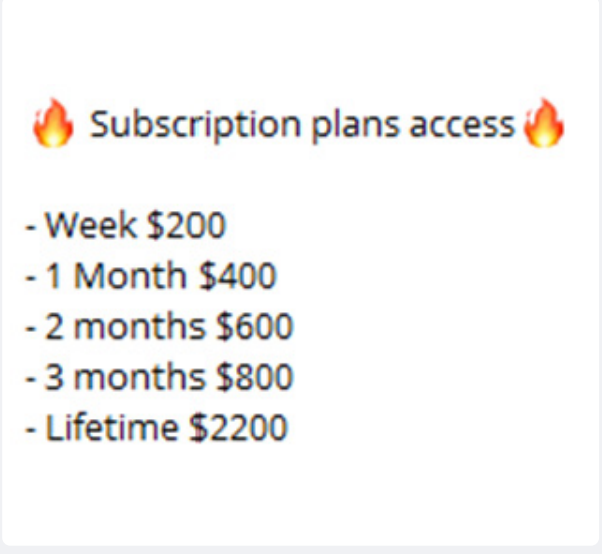


Image: *A subscription plan on Oct 2021*

Image: *A subscription plan on Dec 2022*

On December 7, 2022, the actor claimed that the private group allows access to 4 million logs. The actor detailed the benefits of being a subscriber to the private group:

1 *"All logs are private and not sent on the group channel"*

2 *"Daily logs sent privately to every member"*

3 *"Cookies method"*

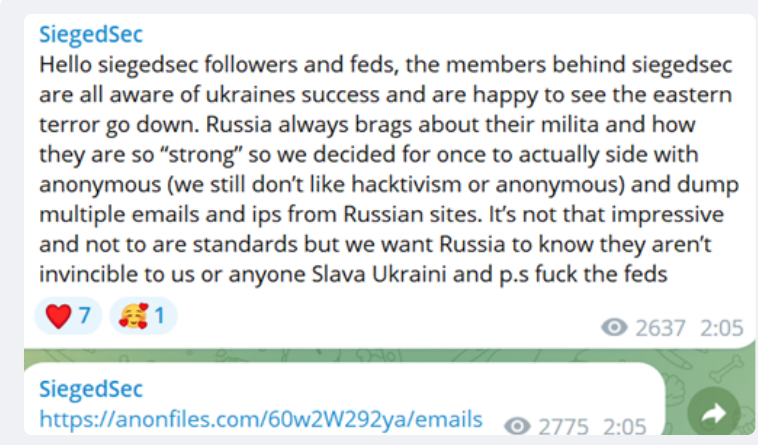
4 *"Wallet checking methods with videos"*

5 *"Ways to login to bank account"*

6 *"Limited slot only"*

The actor behind the REDLINEVIP Telegram channel was also operating under the moniker FATHER121 on several cybercrime forums, allowing the assessment of their credibility. There were some accusations of scamming against the actor; however, some of the accusers seem to be not reliable. The Telegram channel now has over 6,000 subscribers.

They posted a minor leak of emails and IP addresses from Russian sites, more as a symbolic contribution to the cause rather than a real hacktivist effort. In November 2022, following the social protests taking place in Iran, the group decided to collaborate with GhostSec on "Operation Iran," but they once again stated that they were not hacktivists and just wanted to join "for the fun of it."



At the end of November, the group announced its retirement from hacking and leaking and disclosed the nicknames of its members.

Palm Team

The main Telegram channel of Palm Team, a group of traffers, was created on July 1, 2022. Since then, Palm Team has also been advertised on the Russian cybercrime forum Lolz Guru. The team's admin "Luwyshka" operates on the forum under the moniker "LUWY".

Palm Team operates a few different Telegram tools:

1. *"Telegram bot for traffers' applications"*
2. *"A public Telegram group for experienced traffers from the team"*
3. *"Private groups for the team"*

The group also published a manual for traffic generation on the blogging platform Telegraph. Based on the owner's comments in Telegram and on Lolz Guru, their members use Raccoon and Redline stealers, but the options aren't limited to these stealers.

There are several members that are in charge of different projects and are responsible for stealing credentials from specific services like games, as well as social media platforms including Amazon, Twitter and Facebook. One member is responsible for providing support and answering traffers' questions.

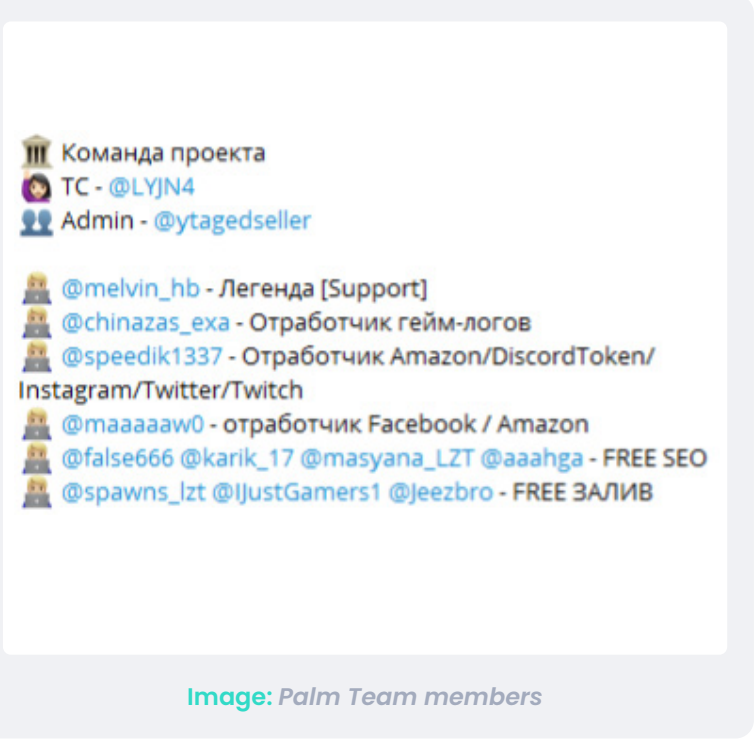
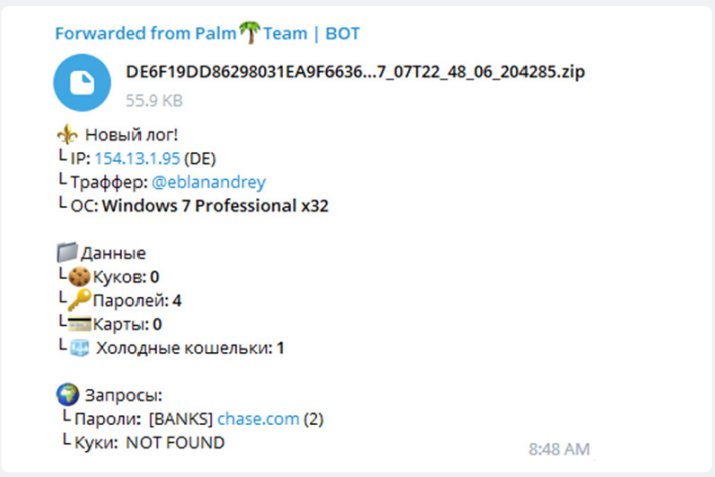


Image: *Palm Team members*

Traffers are paid with a percentage of profits on the logs that they generated and that were further exploited or sold by admins. Traffers can get 80% of the revenue, and on average, for 1,000 logs, traffers would earn 10,000 Russian rubles (around USD 140). The administrators usually publish challenges and competitions to encourage users to get more logs.



The owner of the group also advertised a VIP Telegram chat for Palm Team traffers. The threat actor invited experienced traffers to join the chat if they have at least 600 logs and constant traffic they can use to distribute malware.

Image: *Logs file collected by one of the traffers*

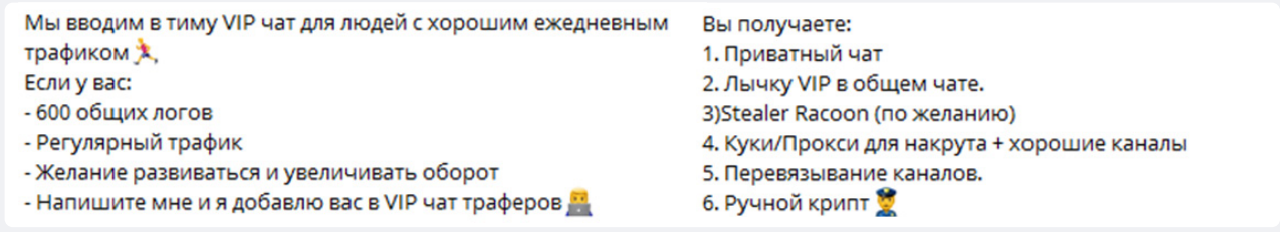
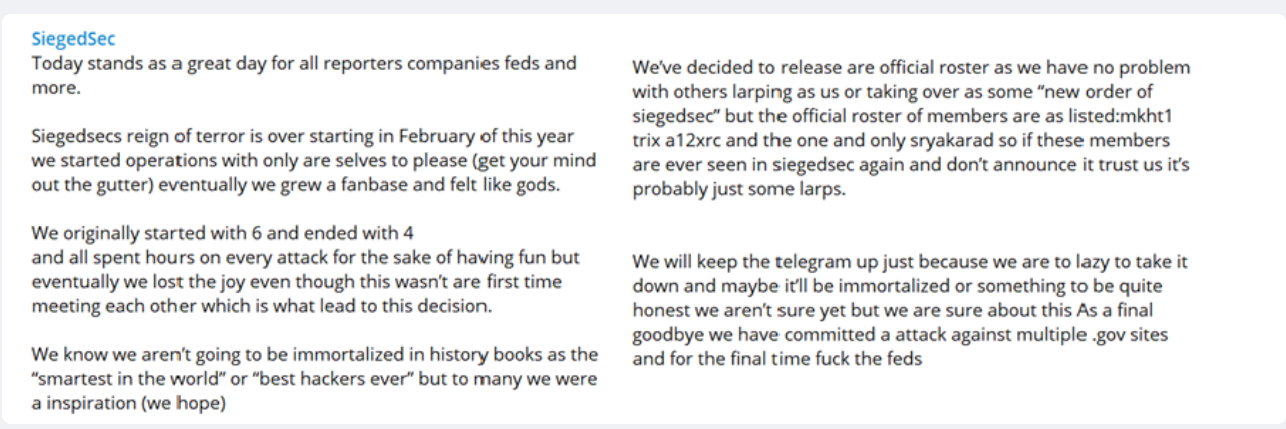


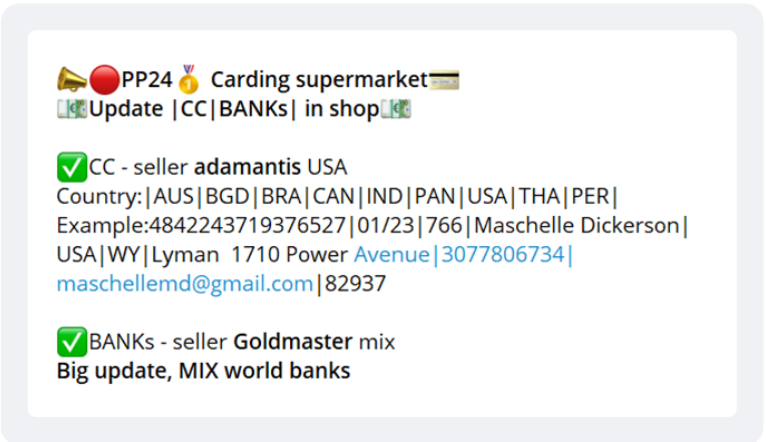
Image: *Conditions for joining VIP PalmTeam chat for traffers include having at least 600 logs and regular traffic. Members receive a private chat, access to Raccoon stealer, new distribution opportunities and customized manual encryption of builds*

Palm Team is one of dozens of teams that monetize the collected logs obtained by traffers. These teams use Telegram as an important pillar in the distribution of malware and process of collecting logs. The platform eases the communication process between the team members, allowing them to stay under the radar. Therefore, it's reasonable that cybercriminals will continue to leverage Telegram for their operations, spreading malware and stealing corporate and private credentials.



The group's activity spanned a short period of time, and Telegram seems to offer the ease of opening a channel and the freedom to "abandon" it once it isn't needed anymore, whereas opting for using a website to dump their data would have meant going through the trouble of creating and financing a site for just a few months' use.

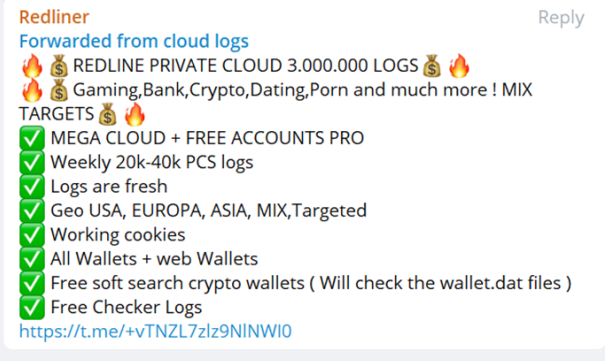
Bank Fraud: CHECKS GRUB SHOP



"CHECKS GRUB SHOP" is a popular group for selling credit card information, counterfeit and stolen valid checks, fullz and bank logs. The group was created on August 30, 2021, by the user called @TrippleeG. It was created as a group of the channel with the same name, allowing users to post comments in the channel and discuss posts from the channel in this group. First, only posts from the channel appeared in the group. In November 2021, other members started to join the group and offer their services. Currently the group has over 8,100 members, while the channel is inactive and has only around 300 members.

A typical member of the chat would be a user periodically offering credit cards for sale, including samples, targeted countries and banks, and relevant updates:

Channel members also advertise some items from other channels. For example, the member Redliner forwarded a message from a channel regarding a sale of logs:



The example illustrates how community features of Telegram helped to establish a dedicated group for banking fraudsters. First started as a discussion group meant to advertise offers of a single actor, the group attracted multiple members and eventually became more popular than the original channel.

Ransomware and Data Extortion: Lapsus$

Lapsus$ emerged in early December 2021 as a data extortion group mostly targeting entities from various sectors in Brazil and Portugal. The group posted the victims on its main Telegram channel, created on December 10, 2021; as of December 2022, it had over 55,800 subscribers. Lapsus$ also maintained a second channel; however, it only has posts starting from March 2022, and the majority were forwarded from the main channel. The group also created a chat, where they shared information from the channels regarding their victims and interacted with the chat's subscribers. Currently, the chat is not accessible, but it had over 14,000 subscribers.

The group has claimed dozens of victims in countries including Brazil, Portugal, the United States, South Korea and Argentina. The victims were from the telecommunications, media and entertainment, technology, and retail industries, as well as government-related organizations. In late February and March, Lapsus$ mostly focused on high-profile targets – Nvidia, Samsung, Microsoft and LG Electronics – and started publishing victims' data. Samsung and Nvidia reported cyberattacks around the same time the group announced them on the Telegram channel, and confirmed the content of the data leaked by Lapsus$.

Okta is one of the several big-name companies targeted by Lapsus$. On March 22, 2022, Lapsus$ posted screenshots on their Telegram channel claiming that they had acquired "superuser/admin" access to Okta.com. The group stated that they did not access any database and focused only on Okta's customers. One of the domains listed in the screenshots that the group uploaded was an account belonging to an engineer, who was employed at one of Okta's subcontractors. That gave Lapsus$ access to several high-privilege Okta portals and information about the Okta clients.

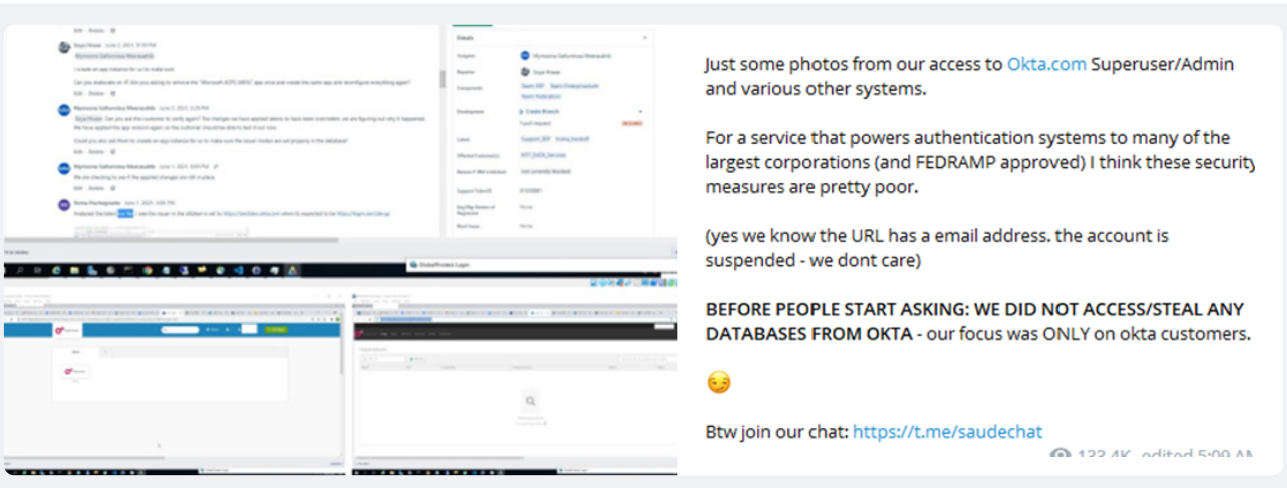


Image: *Lapsus$'s leaks regarding Okta attack*

In March, it was reported that City of London Police arrested seven teenagers in relation to the gang and allegedly one of them is a 16-year-old from Oxford, England. Another is suspected to be a teenager residing in Brazil, according to the investigators. As of December 29, 2022, the threat actors kept silent and haven't shared information on the channel since March 30, 2022, though KELA has seen some former members being active on cybercrime forums.

Hacktivism: Killnet and ALtahrea Team

Killnet

Killnet has become one of the most influential of the pro-Russian hacking groups that target states opposing the country in its invasion of Ukraine. Its main Telegram channel is followed by more than 90,000 users, and its campaigns are joined by many other influential hacking groups, including XakNet and NoName057(16). This group has been targeting governmental and private entities from Ukraine and its allies since March 2022.

The operation was originally founded by an actor under the moniker Killmilk in November 2021. They initially promoted their project as a botnet for DDoS attacks in January 2022, which they offered as a service for profit on cybercrime forums. In promotion posts, Killnet was described as "the first decentralized botnet" that could be used for DDoS attacks for a fee.

After the start of the Russia-Ukraine war, Killnet's activity shifted to hacktivism, and that's when the group joined Telegram and started to build their community. Their channel was created on February 26, 2022, two days after the Russian invasion. The group not only performed and promoted DDoS attacks against pro-Ukrainian entities and states (such as Poland, Lithuania, UK, Italy, and more) but also used Telegram as a means to create a hacktivist movement called Legion. Legion consists of cyber squads that operate under different hacking teams and launch DDoS, defacement and other attacks using a similar targets list. Some of these groups eventually separated (Anonymous Russia, Phoenix, Zarya) but continued to attack the same victims and repost Killnet's post in their own Telegram channels.

Killnet usually performs a wave of attacks against targets from one country, in parallel calling in their Telegram posts for Legion squads and other groups to join their efforts. In some cases, it doesn't only share the domain of an alleged victim, but also provides tools to perform the attack, aiming to attract as many hacktivists as possible. For example, Killnet distributed to Legion members a public script known as CC-Attack to automate the use of open proxy servers to relay attacks. These proxy servers help to preserve the anonymity of the attackers and increase the number of attacking IP addresses. The script is capable of generating three different Layer 7 attack types. The CC-Attack toolkit contains a few files and doesn't require a skilled actor to perform an attack.[27]

Between August and September 2022, Killmilk stepped back from Killnet activity, and a threat actor called BlackSide, who is said to be related to ransomware attacks, was named as a leader. However, per KELA's review, Killmilk is back as the leader since mid-September 2022. The group continues to be active and is using Telegram as its main channel of communication.

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

ALtahrea Team

ALtahrea Team is a pro-Iranian hacktivist group whose Telegram channel was created under the handle @ALtahrea on April 19, 2022. More specifically, the group was tied to "Sabreen News," an Iran-backed Iraqi militia outlet existing mainly as a Telegram channel (@sabreenS1) since 2020.[28]

Following its creation, the group immediately published on this channel a countdown signifying its first cyberattacks against several Israeli media websites. Since then, the group has claimed DDoS attacks and defacements on entities from several countries, including Israel, Turkey, Saudi Arabia, Iraq, the UAE, the UK and the US. Interestingly, the group also joined the Russia-Ukraine cyber war siding with Russia. The political motivations against Israel were clearly and repeatedly stated, and for most of the rest of the targets, the actors explained what victims' actions caused such a response.

It appears that ALtahrea Team has collaborated with Team 1877, a different politically motivated group based in Iraq, which is more actively involved in the cybercriminal underground at least since 2019. Said collaborations were claimed as responsible for at least two defacement attacks, as can be seen in the Telegram posts by both teams (with Team 1877 constantly using Telegram as well).

While the information regarding ALtahrea Team's reputation is limited, the fact that ALtahrea has collaborated with 1877 Team, a reputable actor in the underground forums, may contribute to its credibility. While ALtahrea Team was active most of the year, their Telegram channel went into silence mode on October 31, suggesting that the group may have stopped their activities, at least under this handle.

[28] Profile: Sabereen News