kaspersky

Analytical report
2025

Goodbye, dark Telegram: Blocks are pushing the underground out

Contents

Telegram, which launched just over ten years ago, has become one of the most popular messaging platforms not only among ordinary users but also among cybercriminals. For the latter, Telegram is much more than just a messaging app; with its built-in features it functions as a full-fledged dark web platform.

In this report, we examine Telegram through the eyes of cybercriminals, evaluate its technical capabilities for running underground operations, and analyze the lifecycle of Telegram resources, from creation to digital death.

?

Telegram as a shadow messenger

Telegram has won over users worldwide, and cybercriminals are no exception. While the average user chooses a messenger based on convenience, user experience and stability (and, perhaps, cool stickers), cybercriminals evaluate platforms through a different lens.

When it comes to anonymity, privacy and application independence — essential criteria for a shadow messenger — **Telegram is not as strong as its direct competitors.**

Evaluation criteria	Comparison parameters	Telegram	Discord	Signal	XMPP / TOX / Session
Anonymity and confidentiality	Availability of E2E encryption	Only available for Secret Chat [1]	–	+	+
	Ease of anonymous registration	SMS verification	Email verification	SMS verification	Only a username and password required
Autonomy and independence	Open-source code	Server code closed	–	+	+
	Decentralized infrastructure	–	–	–	+
	Lack of moderation	–	–	Limited due to E2E encryption of private chats	+

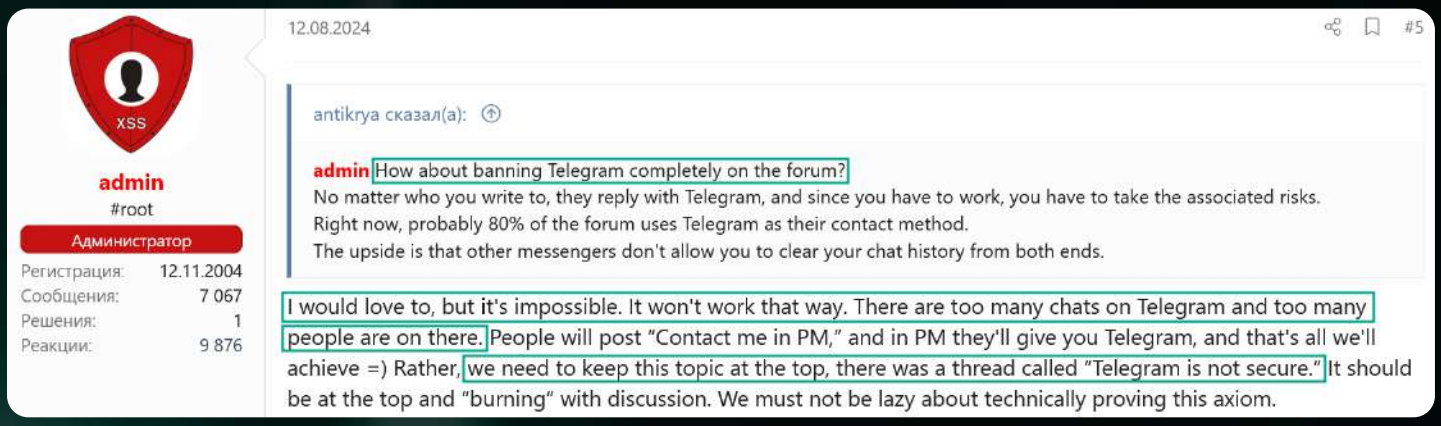
Full match · Partial match · Discrepancy

The disadvantages of Telegram for cybercriminals:

- Lack of default end-to-end (E2E) encryption for chats –
- Centralized infrastructure: users cannot use their own servers for communication –
- Closed server-side code: users cannot verify its functionality –
- Availability of moderation by technical support –

[1] Secret Chats differ from regular chats by using E2E encryption and allowing users to set a self-destruct timer for messages.

This architecture requires a high degree of trust in the developers, **but experienced cybercriminals prefer not to rely on third parties when it comes to protecting their operations and, more importantly, their personal safety.** The administrator of one of the major darkweb forums was even asked to ban Telegram using completely.



Proposal to ban the Telegram using on one of the shadow forums (translated from Russian)

That said, today **Telegram is widely viewed and used not only as a communication tool[2] (messenger)** but also as a full-fledged cybercriminal business platform, due to several features that underground communities actively exploit.

[2] This report does not cover cases involving terrorists, extremists, fraudsters, or dealers of weapons and drugs.

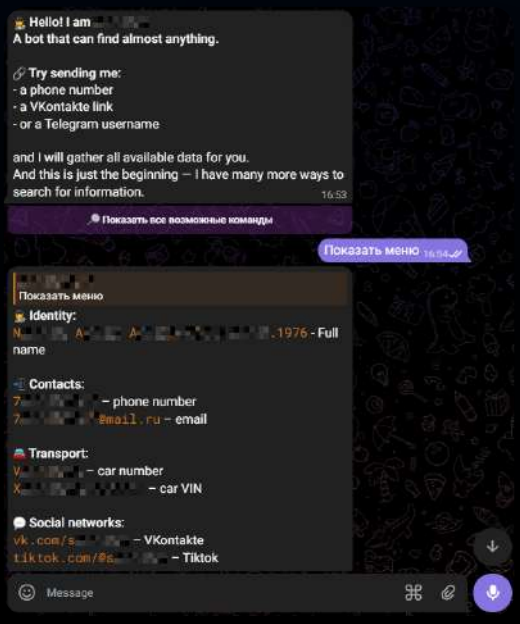
Telegram as a shadow business platform

As in any business, cybercriminals want to earn money quickly and conveniently. They exploit Telegram's built-in features to streamline those operations.

Many legitimate companies automate business processes through Telegram's bot system, and cybercriminals do too.

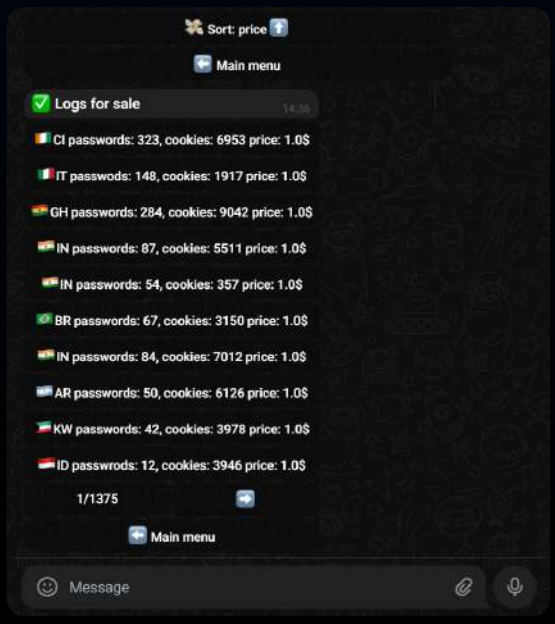
Ease of automation

For example, doxing[3] services typically use bots so an operator can run the service without direct involvement: the client simply sends a search query to the bot.



Built-in instructions for using a doxing bot (translated from Russian)

Cybercriminals have adapted Telegram bots not only to provide services but also to sell goods. For example, using bots to access malware log storefronts, as seen with MaaS[4] Lumma.



Info-stealer log storefront in a Telegram bot (translated from Russian)

This kind of **business process automation saves criminals time and money:** bots don't require salaries or sleep. Furthermore, **bots help scale the illicit business** by handling multiple transactions simultaneously without the owner's direct involvement.

[3] Doxing (slang) involves obtaining structured information about a person or organization from public databases or shadow resources. For example, a query might reveal the target's phone numbers, registered addresses, real estate, vehicles, etc.

[4] Malware-as-a-Service (MaaS) is a business model where cybercriminals sell their partners access to malware and the supporting infrastructure.

Functionality drives activity

On Telegram's shadow resources, the most common activities are those focused on high-volume, low-price sales (such as carding and DDoS services) and subscriptions (such as doxing and MaaS). **These are easy to automate, which makes Telegram an appealing platform for them.** Telegram also offers unlimited file storage, and unlike many anonymous hosting services [5], Telegram file links don't expire. Cybercriminals exploit this when distributing and selling stolen data through channels and chats.

We analyzed the activity in shadow communities and compiled comparative statistics on the messages and posts on topics [6] related to the specific cybercriminal activities on Telegram versus shadow forums, correlating them with the potential profit from a successful transaction.

The table below shows the percentage of posts by topic out of the total number from January 2024 to January 2025.

Post topic	Telegram	Shadow forums	Potential profit per transaction
Carding and other fraud	27.3 %	10.6 %	$ 15
Data leaks	4.4 %	2.5 %	$ 1,500 [7]
Malware sales	3.3 %	2.6 %	$ 200 for a monthly subscription
IAB (Initial access brokers)	<0.0001 %	0.08 %	$ 2,500
Exploit sales	<0.001 %	0.03 %	$ 60,000-250,000 for a zero-day exploit

It's worth noting that many posts on shadow resources are not related to specific activities. These include 'flood' posts, arbitrage discussions [8], gratitude or thank-you notes, etc. These posts make up the majority of content, which helps explain the relatively low percentages for criminal activities in the table.

The data in the table shows that exclusive goods and services — such as zero-day exploits and initial access to large companies — are much rarer on Telegram than on dark web forums. This is because forums typically have reputation systems, user deposits [9] to demonstrate serious intent, and guarantors. These mechanisms help ensure secure transactions, which is especially important when dealing with large sums.

[5] Anonymous file hosting services such as the once-popular anonfile are commonly used by cybercriminals to share large files on forums. Specific files are accessed via a link that eventually expires.

[6] Post topics were identified based on keywords.

[7] Many leaks also publish for free, but for clarity we have added a price if sold.

[8] Arbitration is a conflict-resolution procedure within a shadow community, mediated by a designated and trusted member known as an arbitrator.

[9] A "deposit" here refers to funds a user places in escrow with the forum. If they cause financial harm to another participant, the deposit is used to compensate the loss.

Telegram is no replacement for shadow forums

Lifespan of cybercriminal channels

Unlike the dark web, creating a resource on Telegram is remarkably easy. There's no need to develop and maintain a website — simply setting up a channel or group and share the invite link with potential participants is all it takes. However, while Telegram makes it simple to launch a resource, it lacks the resilience of dark web forums. These forums typically use the Tor network, which conceals the server's real IP address, and they can rotate domains, change addresses and maintain mirror sites, allowing them to survive for years. The shutdown of such a forum is therefore a major event.

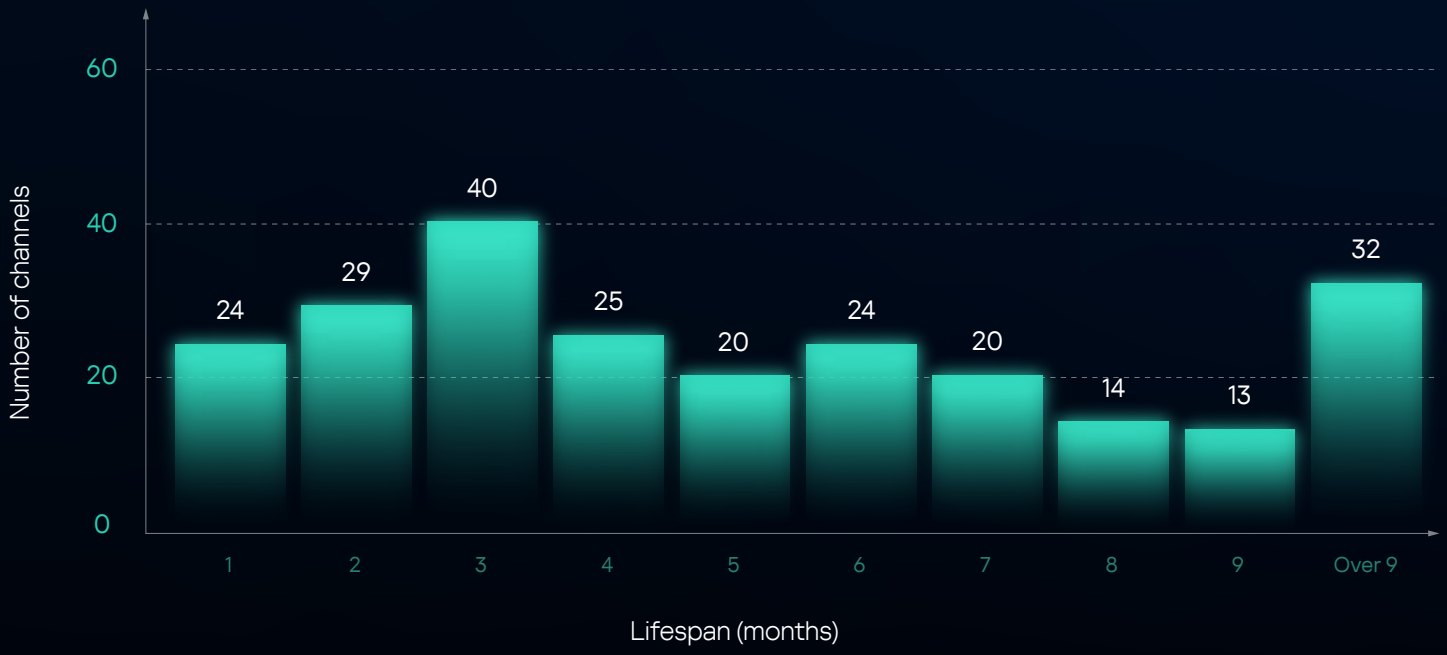
In contrast, Telegram channels offer no comparable fault tolerance and are subject to centralized moderation. So, how long do they last? To answer this question, we analyzed posting activity across various cybercriminal Telegram channels over the past four years.

Using data from more than 800 blocked channels under our observation, we categorized them by their lifespan — the time between the first publication and the last one before deletion.

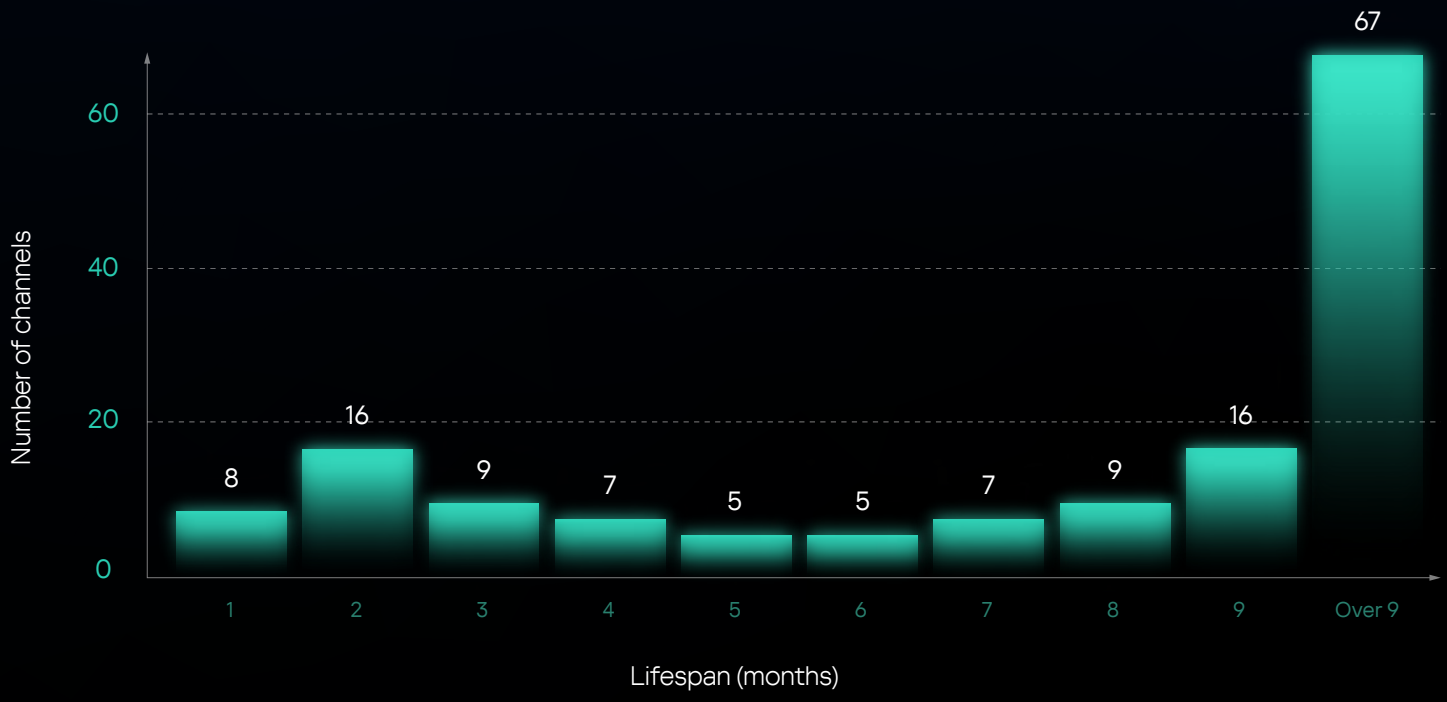
The findings showed that from 2021 to 2024, the average lifetime of a shadow Telegram channel was about seven months — significantly shorter than forums. However, this brevity is offset by how easy it is to create new channels.

?

We also examined how the lifespan of cybercriminal Telegram channels has changed over time. The compiled distributions are presented below.



Distribution of the number of shadow channels by their lifespan for the period 2021–2022



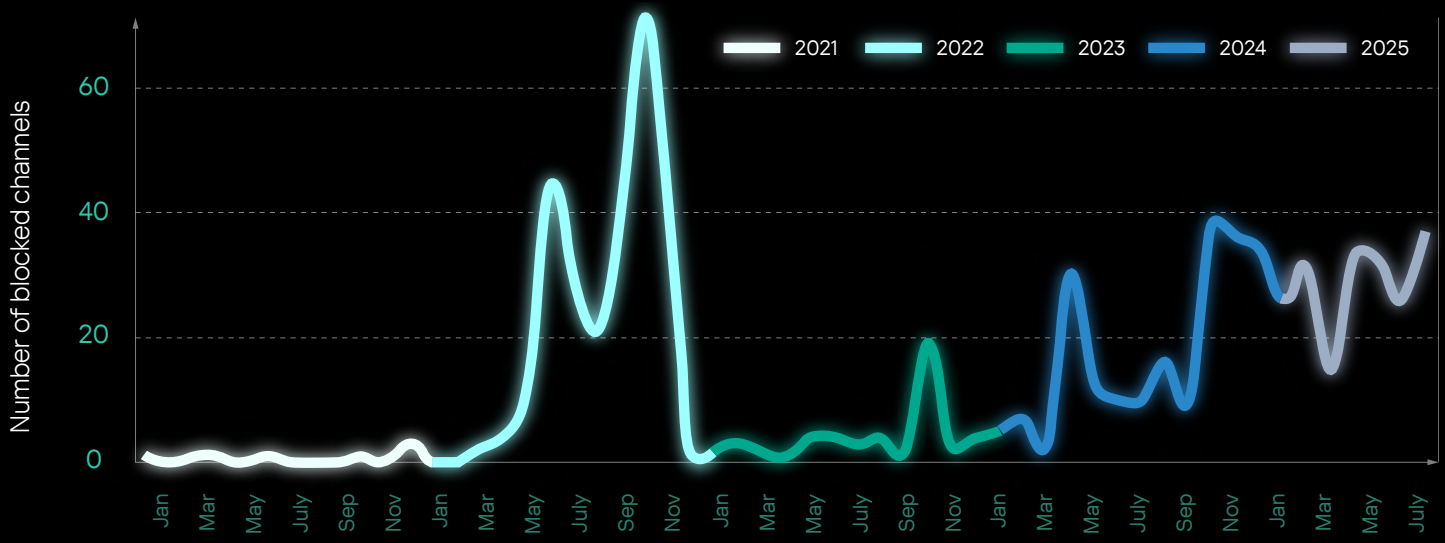
Distribution of the number of shadow channels by lifespan for the period 2023–2024

Median lifespan increased from 5 months in 2021–2022 up to 9 months in 2023–2024.
Shadow Telegram channels began to live longer. But why?

?

Resource blocking

A large surge in blocking of shadow Telegram resources was observed in 2022. We attribute it to the increased activity of hacktivist groups. Under conditions of strict moderation, shadow channels could not exist for long, which is why the median lifespan of a resource during this period is so low.



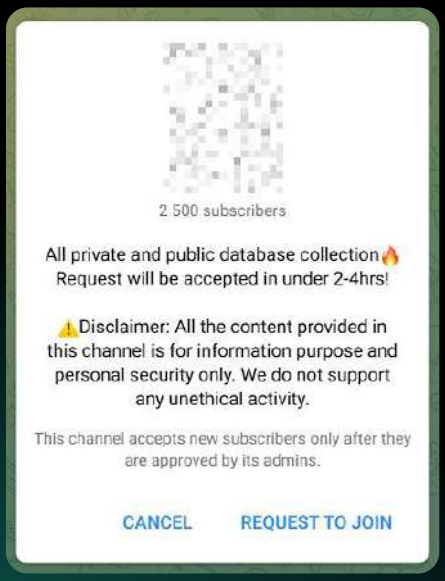
Statistics of shadow channel blocking between January 2021 and July 2025

Despite the longer lifespan of cybercriminal channels in recent years, **they are also being blocked more frequently.** The graph below illustrates the number of blocked resources. As seen in the data, even the lowest figures recorded since October 2024 are nearly equivalent to the peak values of 2023.

Cybercriminals use various tactics to prevent their communities being blocked:

01

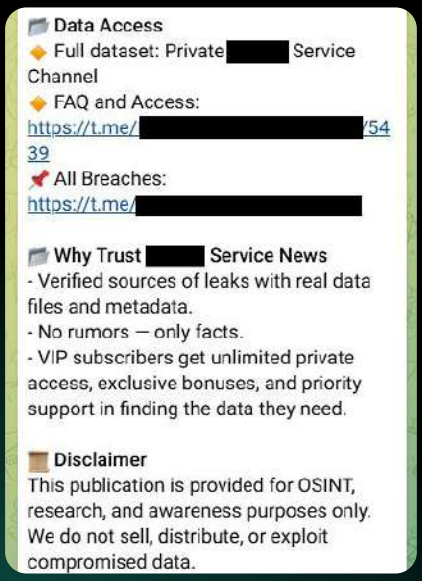
Request to join a shadow channel



Allowing new members only after owner approval, to help keep out outsiders and newbies[10] who might report the resource's content, and also avoid attracting unwanted attention.

02

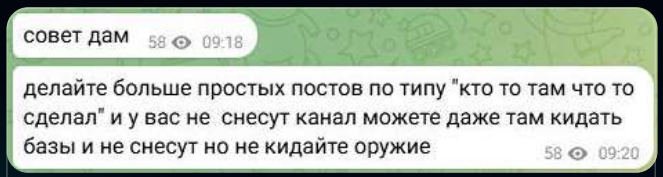
Disclaimer in a post about a database leak



Adding disclaimers about content legality or waivers of liability.

03

Advice from a shadow channel on how to avoid Telegram blocking



Translation from Russian:

Here is a hint

Publish more simple posts like "someone do something" and your channel will not get banned, even you will post leakages. But don't publish qrm related info

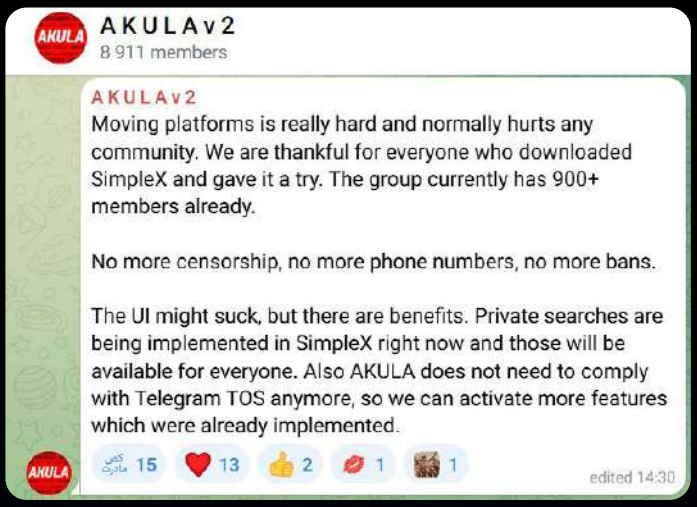
Frequently posting decoy content on unrelated topics to create the appearance of harmless activity.

To assess the effectiveness of these measures, we analyzed channels with a lifespan of nine months or longer. These precautionary tactics were found in only a handful of resources among hundreds. **Therefore, contrary to the criminals' belief, these attempts to bypass moderation and avoid blocking are ineffective.**

[10] Newbies are recently registered users. In shadow communities, they are typically viewed with suspicion as their background is unknown: they could be researchers, law enforcement officers, or other unwelcome observers.

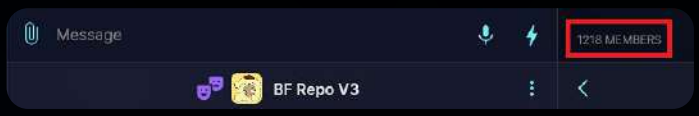
Migration

The first major community to migrate in 2025 was BFRepo, one of whose Telegram groups had reached nearly 9,000 subscribers. **BFRepo moved to SimpleX in May 2025 after repeated violations of Telegram's Terms of Service led to resource blocks.** The community's creator wrote about this in one of their groups, AKULA:



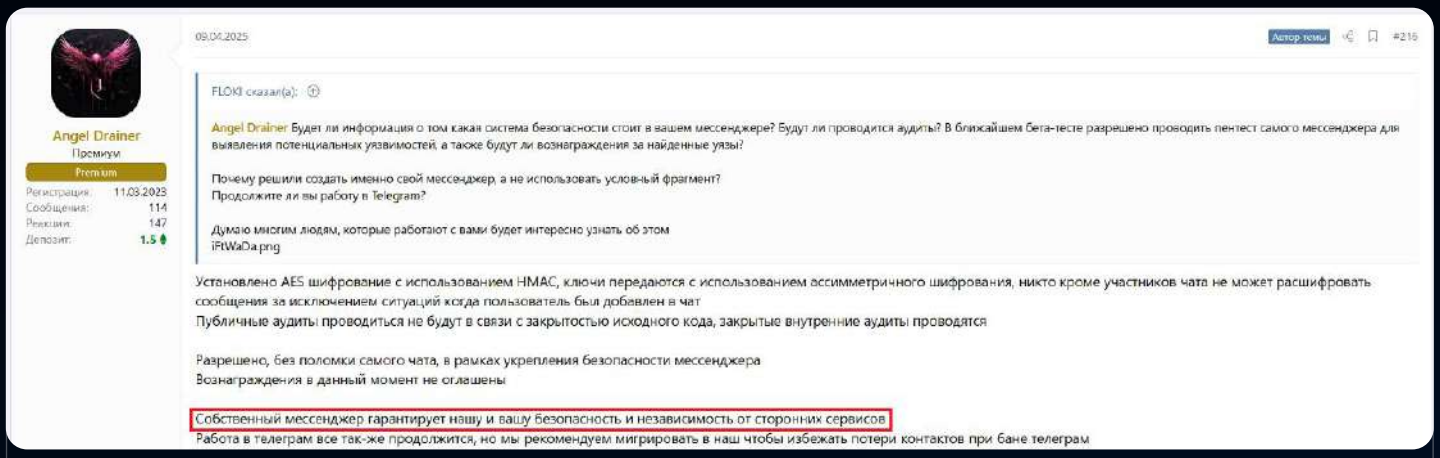
Message about the migration in one of the BFRepo groups

Malicious actors periodically attempt to restore the AKULA Telegram group, but it quickly gets blocked again. At the same time, one of the new BFRepo chats on the SimpleX messenger already has over 1000 participants.



One of the BFRepo groups on the SimpleX messenger

Another community that has retreated from Telegram as its primary communication channel is **the MaaS program. On April 2025, fraudsters recommended that clients use their own messenger** to avoid business downtime. The group has now ceased its activities.



Angel Drainer's announcement on a dark web forum about using their messenger

Translation from Russian:

AES encryption is set using HMAC, keys are transmitted using asymmetric encryption, no one other than chat participants can decrypt messages unless the user has been added to the chat.

Public audits will not be carried out due to the closed source code, closed internal audits are carried out.

(Answer about pentests of their own messanger) Allowed, without breaking the chat itself, as part of strengthening the security of the messenger.

Our own messenger guarantees our and your security and independence from third-party services.

Work in Telegram will still continue, but we recommend migrating to our messenger to avoid losing contacts if Telegram is banned.

The future of Telegram

In conclusion, let's answer the question: **Is Telegram truly a safe haven for cybercriminals?**

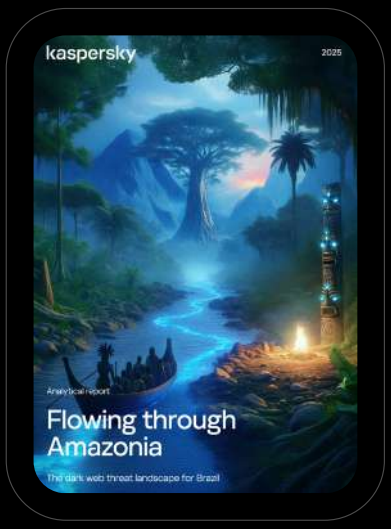
While the platform does offer functionality that attackers eagerly adapt to support their activities, it is actively countering this by strengthening moderation and increasingly blocking shadow resources. This is gradually pushing these communities off the platform. **Therefore, while Telegram may have once served as a safe haven for cybercriminals, it clearly no longer does.**

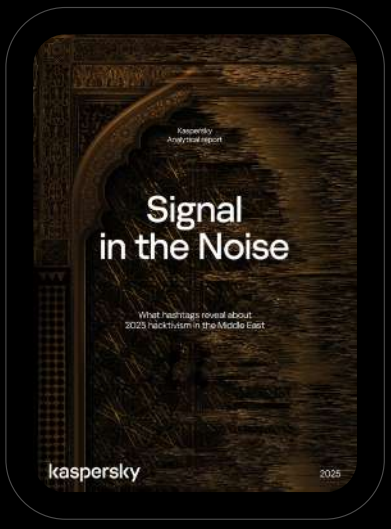
However, **Telegram is just one of many platforms** used by shadow communities. Whether malicious actors continue to use it or move to another service, they will always find a way to communicate. Cybersecurity specialists must therefore track these trends closely and respond promptly to the emergence of new criminal channels, maintaining comprehensive coverage of dark web resources.

Protect your business from hidden threats

Analytical report

Goodbye, dark Telegram: Blocks are pushing the underground out





The other reports are available on the website

Learn more

kaspersky.ru

#kaspersky
#activate_the_future