

Three Months After the Storm: Did Cybercriminals Move to Telegram Alternatives?

 kelacyber.com/blog/three-months-after-the-storm-did-cybercriminals-move-to-telegram-alternatives/

December 18, 2024

Introduction

Telegram, as previously reported by KELA, is a popular and legitimate messaging platform that has evolved in the past few years into a major platform for cybercriminal activities. Its lack of strict content moderation has made the platform cybercriminals' playground. They use the platform for distribution of stolen data and hacking tools, publicizing their campaigns, and other malicious activities.

The September 2024 Telegram policy change has caused cybercriminals to wonder if they can continue their operations on the platform: it included shifting from a privacy-first approach to sharing users' phone numbers and IP addresses with law enforcement for various criminal investigations, beyond just terrorism cases, and a commitment to cooperate with authorities in criminal investigations.

The policy change was made as a response to mounting legal pressures on the platform and its founder and CEO, Pavel Durov, following his arrest in France in September 2024, which also triggered an uproar among different threat actors using the platform.

The hackers saw the arrest and the policy change as a direct constraint to their freedom. Shortly after, KELA has observed discussions about moving to alternative platforms that will be their new home to keep their illegal activities alive.

After all of the strong reactions, and given the circumstances, it seemed that Telegram could lose its status as the go-to platform for cybercriminals, pushing them to find new spaces to continue their activities. But three months later, what has really changed?

BLUF (Bottom Line Up Front):

- **Exploration of Alternative Platforms:**
 - Cybercriminals explored alternatives such as Signal, Discord, Matrix, Tox, Session, Simplex, and Jabber, prioritizing encryption and confidentiality.
 - Discussions emphasized concerns about transparency and potential surveillance on new platforms.

- **Backup Channels on Telegram:**

Cybercriminals increasingly use backup Telegram channels to mitigate the risk of bans, maintaining strong activity on the platform.

- **Limited Migration to Alternatives:**

- Platforms like Signal and Discord showed slight increases in adoption but were used as supplementary options rather than replacements.
- Telegram continues to dominate, with an average of almost 247,000 shared links per month compared to around 700 links combined for Signal and Discord.

- **Groups' Declared Migration Outcomes:**

Multiple groups announced plans to leave Telegram but mostly retained active channels or created new ones. The examples include **AI Ahad**, **BI00dy Ransomware Gang**, **GlorySec**, **Moroccan Cyber Aliens**, **Team ARXU™**.

- **Telegram's Continued Dominance:**

Despite policy changes, Telegram remains the primary platform for cybercriminal activities due to its established user base and functionality. The cybercrime ecosystem remains dynamic, with evolving platforms and methods requiring continuous observation.

If not Telegram, what else is out there?

Threat actors have been discussing the alternatives since September 2024, when Telegram changed its policy. The potential substitutes included:

- **Discord** – instant messaging and VoIP platform that enables communication through voice and video calls, text messaging, and offers options for private conversations or open discussions within communities.
- **Jabber** – a platform enabling instant messaging, voice and video calls, voice messaging, desktop sharing, conferencing, and presence features, used mostly for direct messaging.
- **Matrix** – an open standard for interoperable, decentralised, real-time communication over IP. It is used for Instant Messaging, VoIP/WebRTC signalling.
- **Tox** – peer-to-peer messaging and video-calling protocol designed to provide secure, end-to-end encrypted communication, used for direct messaging.
- **Session** – a platform using end-to-end encryption, onion-routing for messages, allowing communication within small groups, used mostly for direct messaging.
- **Signal** – end-to-end encrypted texting, voice and video calls, and customizable disappearing messages, used both for private messaging and for groups and communities.
- **Simplex** – a decentralized messaging platform designed for privacy, without user identifiers such as phone numbers, or usernames, used mostly for direct messaging.

The most important parameter in most of the discussions was the confidentiality and high encryption of the messages, and one of the biggest concerns was the potential transparency of the new platform for authorities. Here are just a few examples:

Telegram alternatives??

 Publish date: **Oct 10, 2024**  Author: **poioii** in  Source: **ExploitIn**  ID: **330375583**

- 1) SimpleX chat - in terms of security, the most interesting solution at the moment and is developing, unlike the dead tox.
- 2) Sessions is not bad, but there will most likely be problems with spam, but there is an analogue like tor.
- 3) Tox - normal but dead.

Hackers discuss different alternatives on Exploit Forum

Will Telegram leak users to security forces?

 Publish date: **Oct 31, 2024**  Author: **poioii** in  Source: **ExploitIn**  ID: **332173205**

Quote

If you reject, offer. What solutions would you use for personal correspondence, for communication with an audience or commercial activities?

legal telegram, everything else simplex chat, sessions, tox, jabber

Discussion about the alternatives with focus on the safety

SimpleX replacing Telegram?

 Publish date: **Dec 7, 2024**  Author: **Trilex** in  Source: **BreachForumsReborn**  ID: **335673179**

With pressure from France due to the arrest of Pavel Durov, Telegram looks like it will start cracking down on groups that deal with illegal activities and work more closely with law enforcement.

SimpleX has many advantages over Telegram, such as encrypted-only messaging, IP address hiding, no phone number needed, and incognito mode. SimpleX currently has issues with bot functionality, limited group size, and being slow, but this will most likely improve over time.

Is SimpleX Chat a good replacement for Telegram? Let me know what you think.

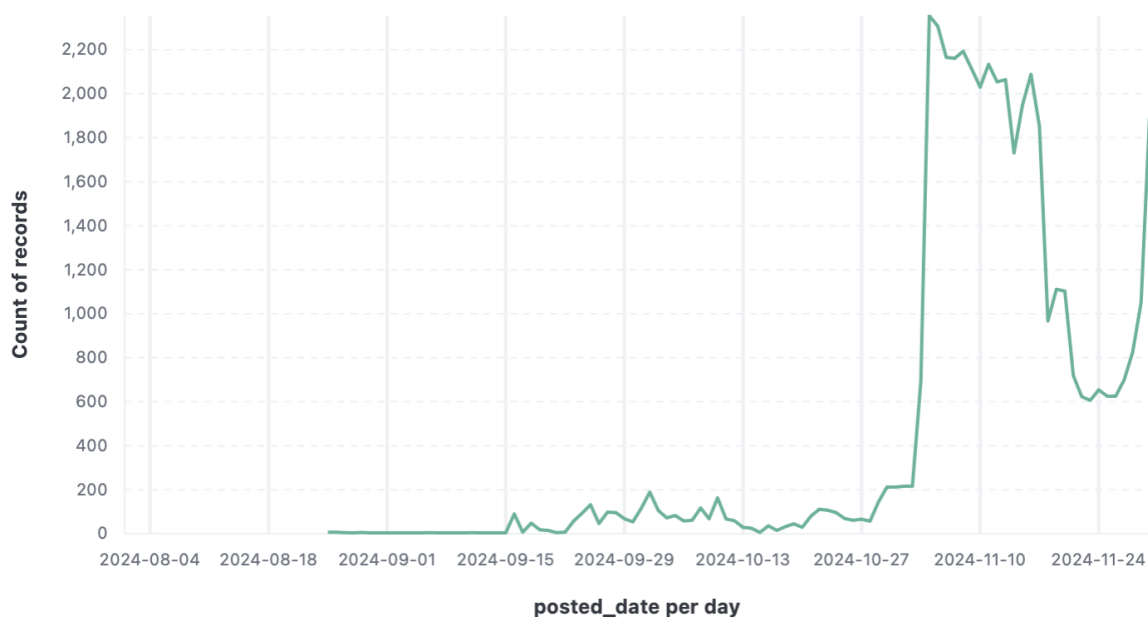
Three months after the topic is still discussed

Some cybercriminals have reported they witnessed the closing of Telegram channels and groups that are connected to illegal activities, which prompted more discussions. Indeed, the deactivation pace of Telegram channels was observed to increase. As a way to deal with this, cybercriminals have been maintaining backup Telegram channels, using these secondary channels when their primary one gets banned. These backups are typically pre-advertised to their audience in advance. However, there is a way to see if cybercriminals went further and really started using other platforms.

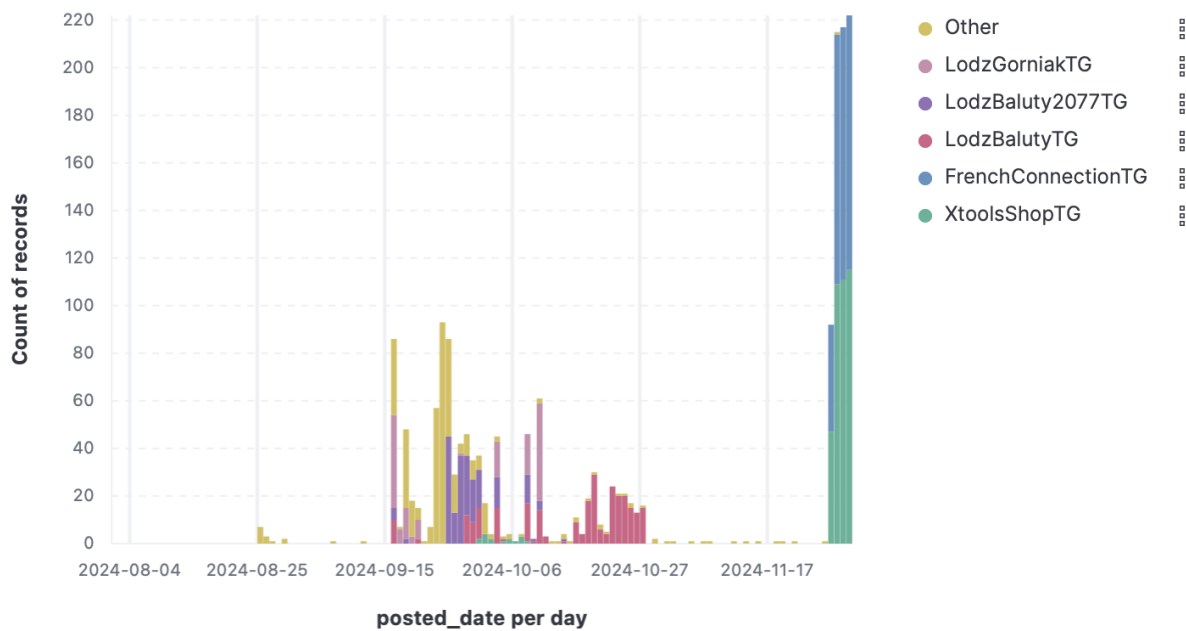
Telegram still more popular than Discord or Signal

To measure the popularity of Telegram versus other platforms, KELA has reviewed the number of links to the platforms shared by cybercriminals. These links are usually related to invitations to specific groups, as opposed to general discussions on the subject. Among the debated alternatives, two of them — Signal and Discord — have features that are similar to those that attracted users to Telegram in the first place, which is the ability to make groups and communities, as well as relatively easy registration.

When looking at a set of cybercrime-related Telegram channels, KELA has indeed observed an increase in the number of shared links to Signal groups since Pavel Durov was arrested on August 24, 2024. However, when looking closer, most of the mentions for the last 3 months came from primarily five groups, promoting the same links to their channels on Signal to promote their channel, in addition to their activity on Telegram.



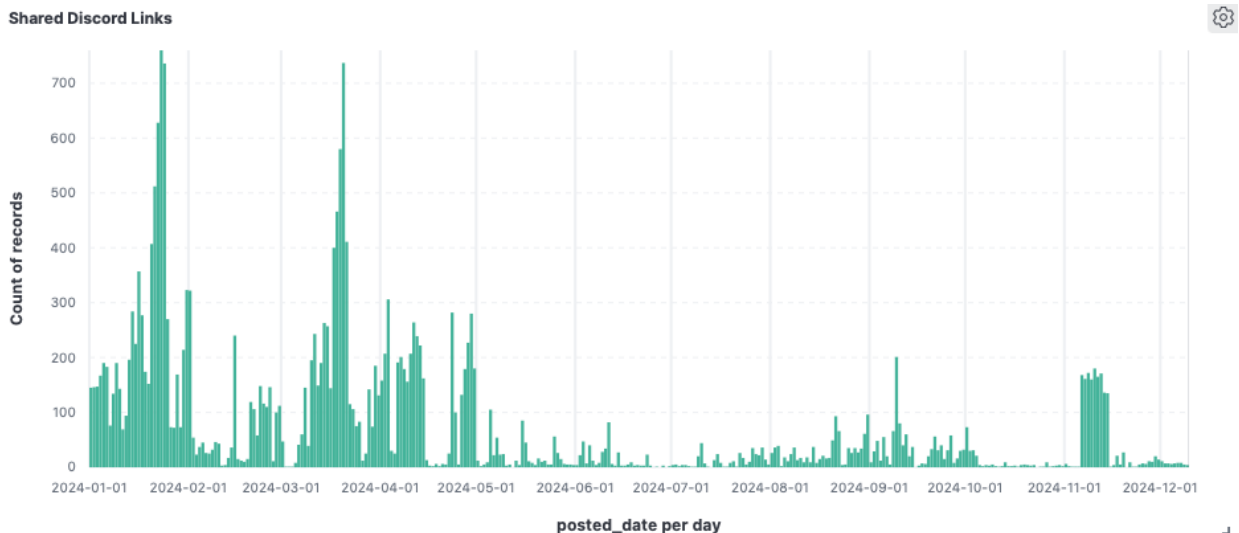
Amount of shared links of Signal since the arrest of Pavel Durov based on KELA's data lake (a set of cybercrime-related Telegram channels)



Amount of shared links of Signal since the arrest of Pavel Durov, broken down by the channel's name based on KELA's data lake (a set of cybercrime-related Telegram channels)

This way, while some actors have started to use Signal in parallel with Telegram, it doesn't seem its popularity significantly grew.

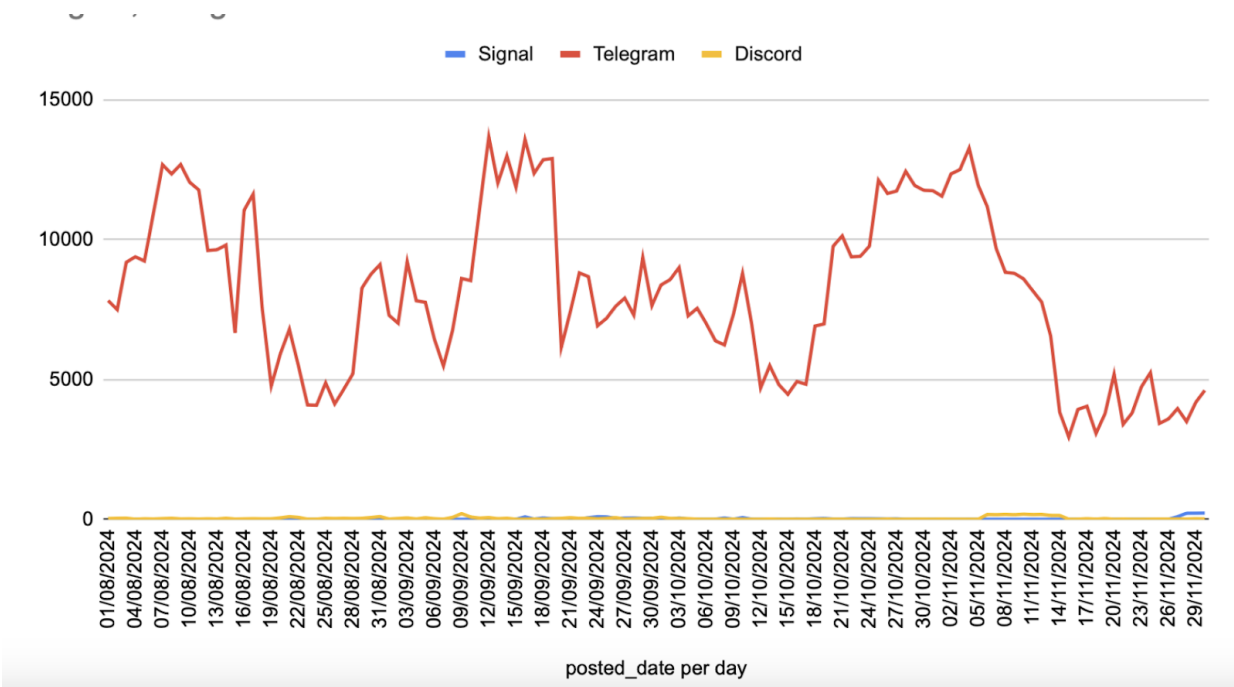
As for Discord, while the platform has frequently come up in various discussions, KELA as well did not observe an increase in the tendency of the shared links to redirect to Discord servers.



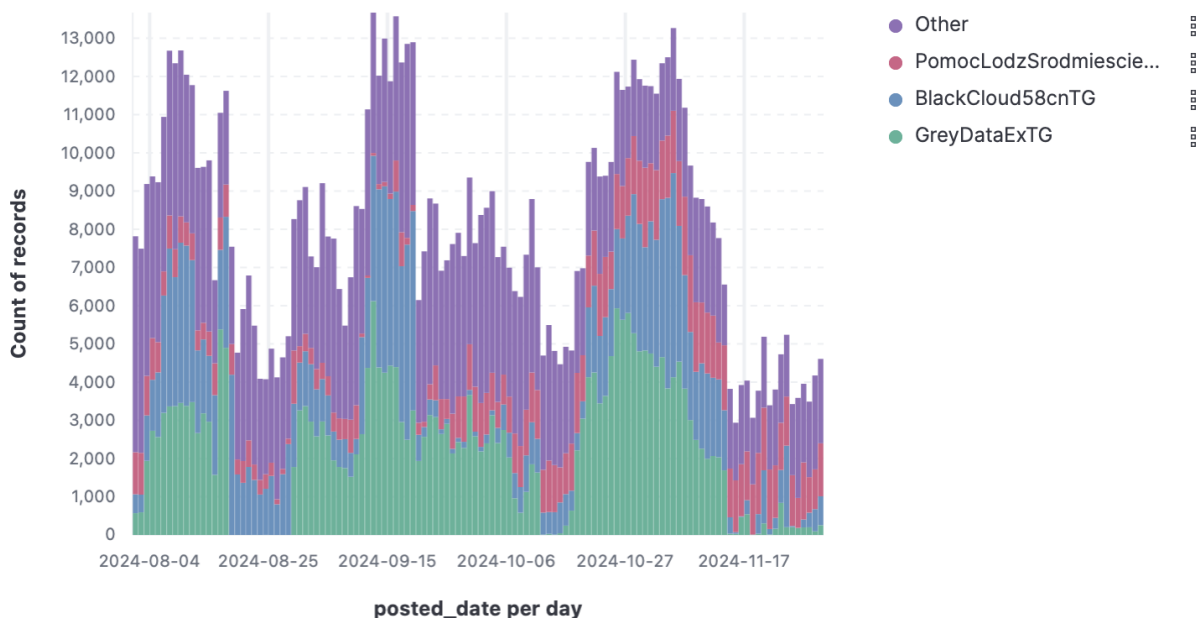
Amount of shared links of Discord since the beginning of 2024 based on KELA's data lake (a set of cybercrime-related Telegram channels)

With the increase of the shared links to Discord and Signal, it is also worth mentioning that the Telegram link sharing is still active and the most popular among the messaging platforms.

Signal and Discord collectively account for an average of 682 links shared per month between August and December. In stark contrast, Telegram leads significantly with an average of 246,903 links per month. While most of the mentions still come from several groups that include a link to their channel in each message, even removing these groups will not influence the Telegram's prevalence.



Amount of shared links of Signal, Telegram, and discord since August based on KELA's data lake (set of cybercrime-related Telegram channels)

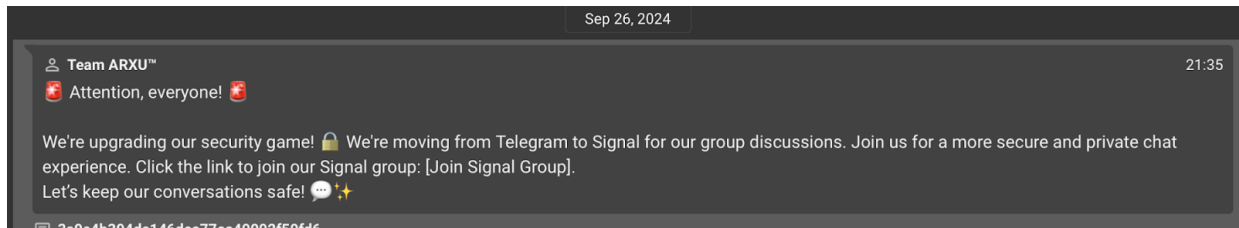


Amount of shared links of Telegram since the the arrest of Pavel Durov, broken down by the channel's name on KELA's data lake (a set of cybercrime-related Telegram channels)

Those who promised to leave Telegram and retreated

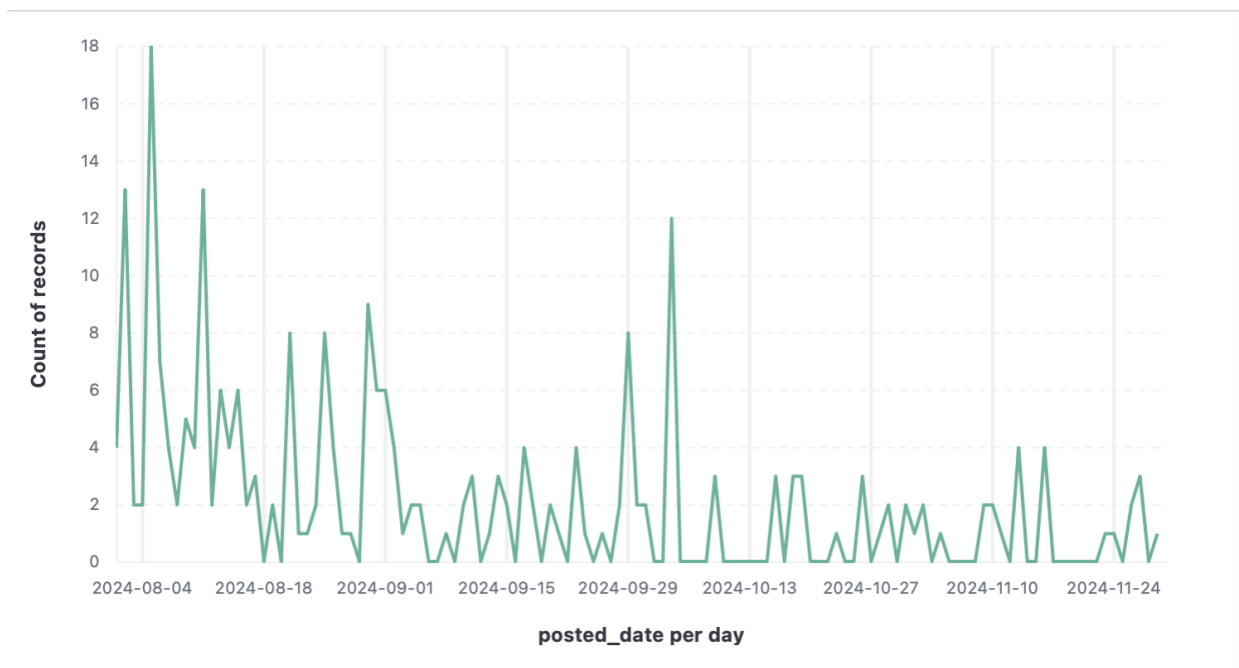
Right after Durov's arrest and the police change, some channel administrators stated their plans to migrate and create channels on other platforms. However, in many cases, these new channels became backup options rather than replacements for their primary Telegram channels.

For example, on September 26, 2024, the pro-Bangladeshi hacktivist group **Team ARXU™** announced their decision to transition from Telegram to Signal, citing enhanced security as their reason for the move. They encouraged their followers to join them for a “more secure and private chat experience” by sharing a link to their new Signal group.



Team ARXU™ posting their intentions to move from Telegram to Signal

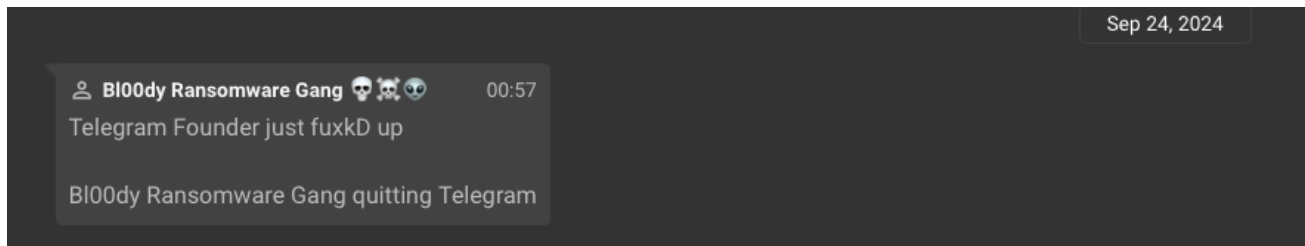
Three months later, their Telegram channel is still active and has a growing number of subscribers, now nearing 2,000. Despite claims about changes, Team ARXU™ continues to post new content regularly on Telegram. The provided Signal URL is not active as per the date of the report.



Amount of messages in a Telegram channel of Team ARXU™ in August-December 2024 (a set of cybercrime-related Telegram channels)

The ransomware group known as **BI00dy Ransomware Gang** has declared on September 24, 2024, that following the Telegram policy change, the group is leaving Telegram. Despite the claims and the sudden abruption of the activity on the channel after the quitting

,message, one month later, on October 24, 2024, they resumed their activity in a new Telegram channel, sharing on the channel their ransomware victims, as well as advertising the new Telegram channel on their X account.



The last message on the Telegram channel of the Bl00dy ransomware group

On September 24, 2024, the Iraqi anti-Israeli hacktivist group **Al Ahad** stated on their channel that they are shifting, along with their alliances and channels to Signal, following the new Telegram policy, and provided a link to their channel. Not only did they not quit their activity on their Telegram channels, but they also opened a channel in Hebrew, in addition to their main English channel, which was closed shortly after.

The group continued to operate on one of its groups under the new name — Al Ahad Security — and apparently fixed the group description where they mention Durov, claiming that this channel now “follows telegram rules. This channel is anti-terrorism and hack”, and that they don’t conduct illegal activities. This channel reposts information about attacks and criminal activities by pro-Palestinian groups. Before Al Ahad left their channel, Al Ahad Security forwarded messages about the group’s actions, mainly targeting Israeli entities.



Al Ahad Security | آل أَحَدُ

327 subscribers



t.me/WholssksghostLol

Link



ChatBot- [@alahad_chatbot](https://t.me/alahad_chatbot)

Hi [@durov](https://t.me/durov) this channel follows telegram rules
This channel is anti terrorism and hack

No Politics/ No Hate/ Follow All Terms And
Guidelines/ No Racist/ No Nudes/ No Spam/ No
Illegal Activities

Backup - <https://t.me/backupalahad>

Description

To illustrate further, here is a breakdown of 5 groups that promised to leave Telegram and the outcome:

Group name	Group Description	The group's plans following the arrest	Follow-up activity	Group's subscribers
Al Ahad	An Iraqi hacktivist group, mostly targeting Israel in the past	To move from Telegram to Signal	Continued their operation under the channel to "Al Ahad Security" and started to focus on reposting other cybercrime activity rather than posting their own attacks.	Al Ahad: closed the channel Al Ahad Security: 234 subscribers Signal: 120 subscribers
Bl00dy Ransomware gang	A ransomware group	To leave Telegram following the policy change, without specifying an alternative platform	The ransomware group opened a new Telegram channel, one month after saying they will leave Telegram.	New Telegram channel: 16 subscribers
GlorySec	A hacktivist group, which believes in "Avaritionism/Anarcho Capitalism"	"May or may not create a Facebook or Threads account soon"	The group did not take actions and remained active on the channel.	Telegram channel: 3867 subscribers No other channels of the group were found
Moroccan Cyber Aliens	Moroccan hacktivist group aiming at attacking Israel	To leave Telegram for safety reasons and to move to Signal	The hacktivist group opened a Signal channel yet remained active on their Telegram channel.	Telegram Channel: 852 subscribers Signal: 52 subscribers

Team Arxu	A pro-Bangladeshi hacktivist group	To move from Telegram to Signal	The group stayed active with their regular activities on the Telegram Channel. The provided Signal URL is not active as per the date of the report.	Telegram: 147 subscribers Signal: 59 subscribers
-----------	---------------------------------------	--	---	--

Thus, while the activity of some groups slightly changed and they may have adopted other platforms as backup, most of them did not stop using Telegram.

Conclusion

Telegram has long been perceived as a safe haven for criminals, providing them with freedom and a lack of oversight, allowing them to operate without adhering to any rules. The arrest of the CEO, followed by changes in the platform's policies, seemed to mark a turning point in the world of cybercrime. However, cybercriminals are slow to abandon a platform where an established audience has already been presented.

According to KELA's observations, there has been no decrease in the daily activities of threat actors active on Telegram, nor has there been a significant increase in the number of groups that announced their intention to move to different platforms. Although discussions about alternatives continue, there have been no proactive steps or trends indicating such migration. Among those who expressed intentions to move, none have completely transitioned to another platform. While Signal, Discord, and other alternative platforms are used by cybercriminals, it doesn't appear they will fully replace Telegram in the future, and rather serve as additional methods for threat actors to perform malicious activities.

These trends highlight the fact that the cybercrime ecosystem is always evolving and can often be less predictable than it initially appears. The various platforms and operating methods used by threat actors in this environment necessitate ongoing monitoring.

Try for Free

Discover the power of KELA's intelligence platform firsthand. Gain access to actionable insights, uncover critical risks, and explore the depths of the cybercrime underground—all tailored to help you stay ahead of threats. [Try for Free.](#)