CHECK POINT

EXPOSURE MANAGEMENT

TELEGRAM'S CRACKDOWN AND CRIMINAL RESILIENCE IN 2026

March 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

Telegram was launched in August 2013 by Pavel and Nikolai Durov as a cloud-based messenger focused on speed, encryption, and resistance to censorship. Over the years it added groups, channels, bots, and monetization (like Telegram Premium), grew to hundreds of millions of users, and became a key platform for political activism, criminal and extremist communities and cybercriminal of any sort.

From 2022 the usage surged due to geopolitical conflicts and global events. Telegram surpassed 800+ million active users, becoming one of the world's largest messaging platforms. Since Pavel Durov's arrest in France in August 2024, Telegram has introduced new moderation policies and updated its enforcement processes, with most of these changes implemented throughout 2025.

Changes of Moderation in Telegram (2025)

For years, Telegram allowed threat actors to operate with little to no interference, until stricter moderation began in February 2025.

Over 43.5 million channels and groups were blocked throughout 2025. Our analysis indicates that many entities that were blocked between Feb-Apr 2025 were linked to carding, Fullz, and other hacking-related activities.

A Migration?

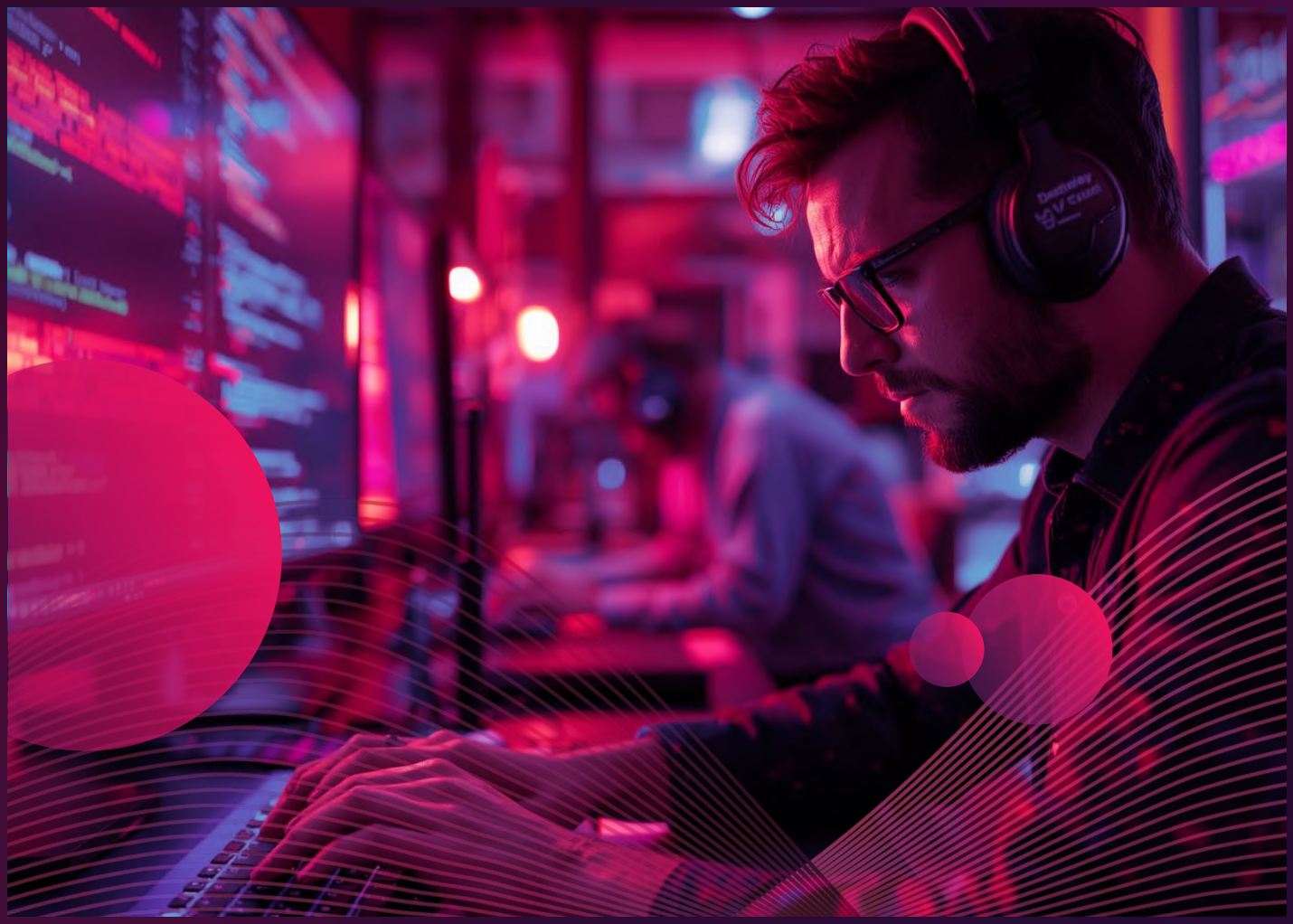
No significant migration has been observed from Telegram to alternative platforms. Some threat actors maintain a presence on other IM platforms for one-on-one communication while Telegram remains a primary channel of communication for most Threat Actors in the arena.

In early 2025 there was a temporary small exception: the AKULA group (likely Russian-speaking) moved to the SimpleX app along with its affiliated chat group "BF Repo" but they returned after SimpleX didn't seem to be popular enough among threat actors.

Evasion Techniques by Threat Actors

Threat Actors have adapted to the changes by using "Request to Join" buttons to prevent bots and by posting false disclaimers tagging Durov. They also have begun creating backup channels to maintain reach.

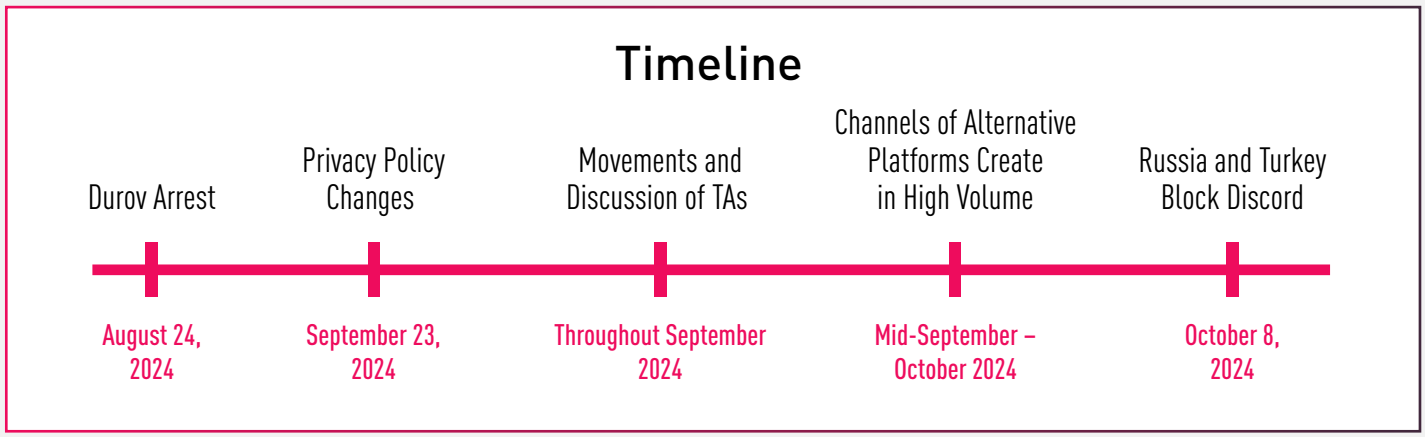
Check Point Exposure Management's conclusion is that despite the changes and the new moderation guidelines of Telegram shaking the arena and raising Threat Actors concerns (mainly around early 2025) they haven't succeeded in migrating them to another IM platform. The moderation keeps blocking channels and groups to some degree but they haven't rooted out threat actor activity.



TELEGRAM CHANGES

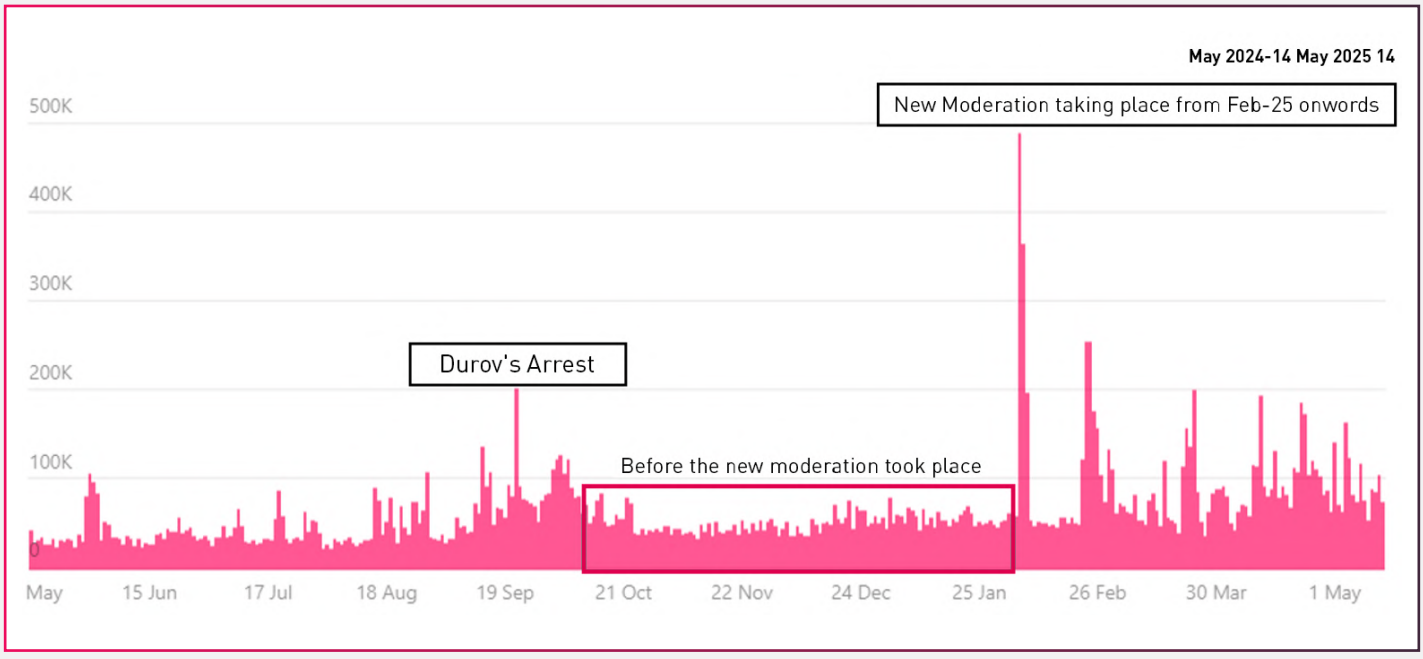
Over the past decade, Telegram has become a central platform for cybercriminal activity, with threat actors increasingly using it as their primary channel for communication and coordination. This is thanks to Telegram's relatively low level of moderation and content removal policies.

Following the arrest of CEO Pavel Durov in August–September 2024, moderation efforts were significantly intensified, particularly from February 2025 onward.



It was rumored in early 2026 that Russia and the Philippines sought to ban Telegram, but those rumours were quashed for the Philippines in March.

Telegram now publishes statistics that indicate that content moderation is at an all-time high. They have even disclosed that GenAI is being used to support these efforts.

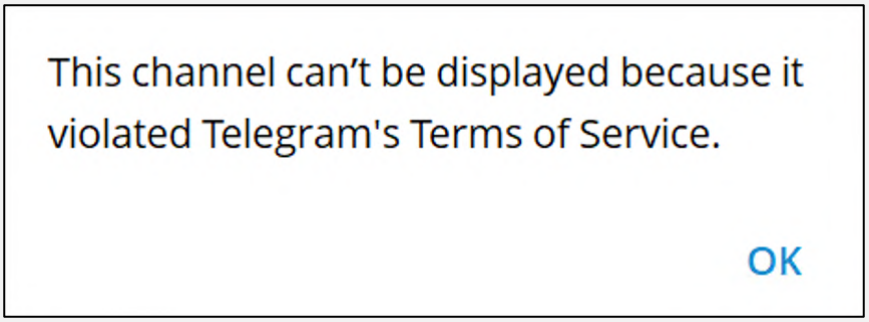


Statistics provided by Telegram moderation team about number of takedowns per day [1]

[1] https://telegram.org/moderation

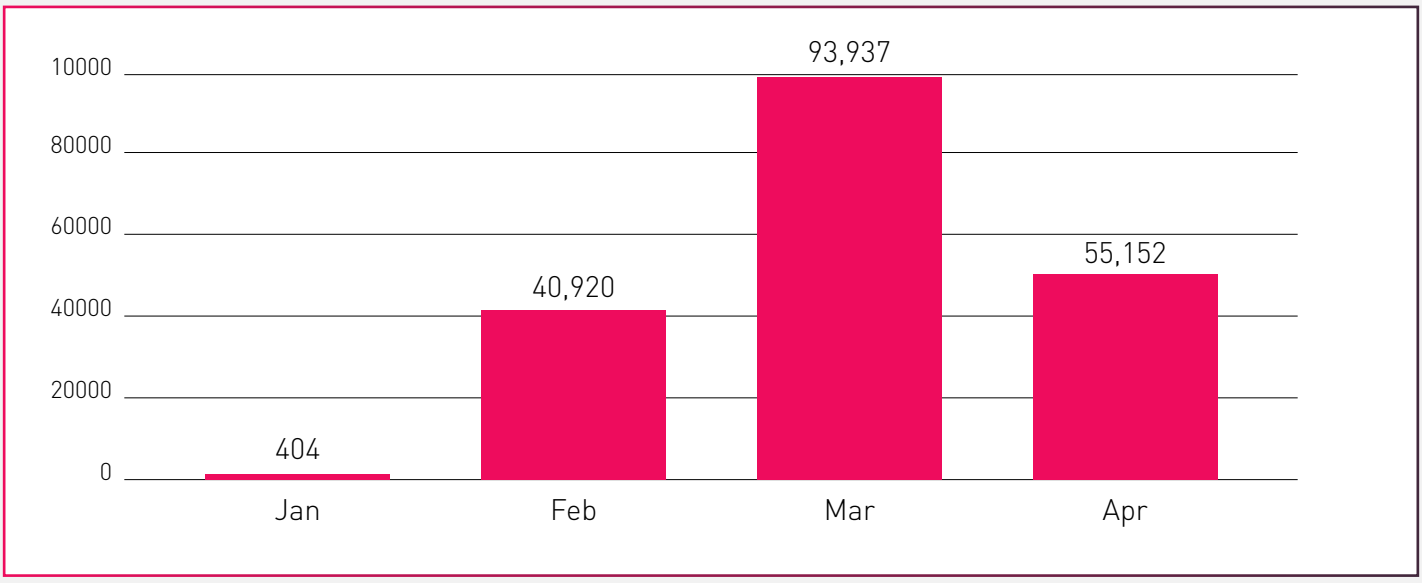
According to Telegram, over 43.5 million channels and groups were blocked throughout 2025. Of that total, only ~2% were related to CSAM (child sexual abuse material) and 0.8% to terrorism-related content. Research on the Check Point Exposure Management solution reveal thousands of mentions of blocked channels (mostly forwarded messages), especially from channels sharing exposed payment cards.

Besides carding channels, data from Check Point Exposure Management shows thousands of blocked messages from channels dealing with Fullz and hacking as well, notably throughout February, March and April 2025.



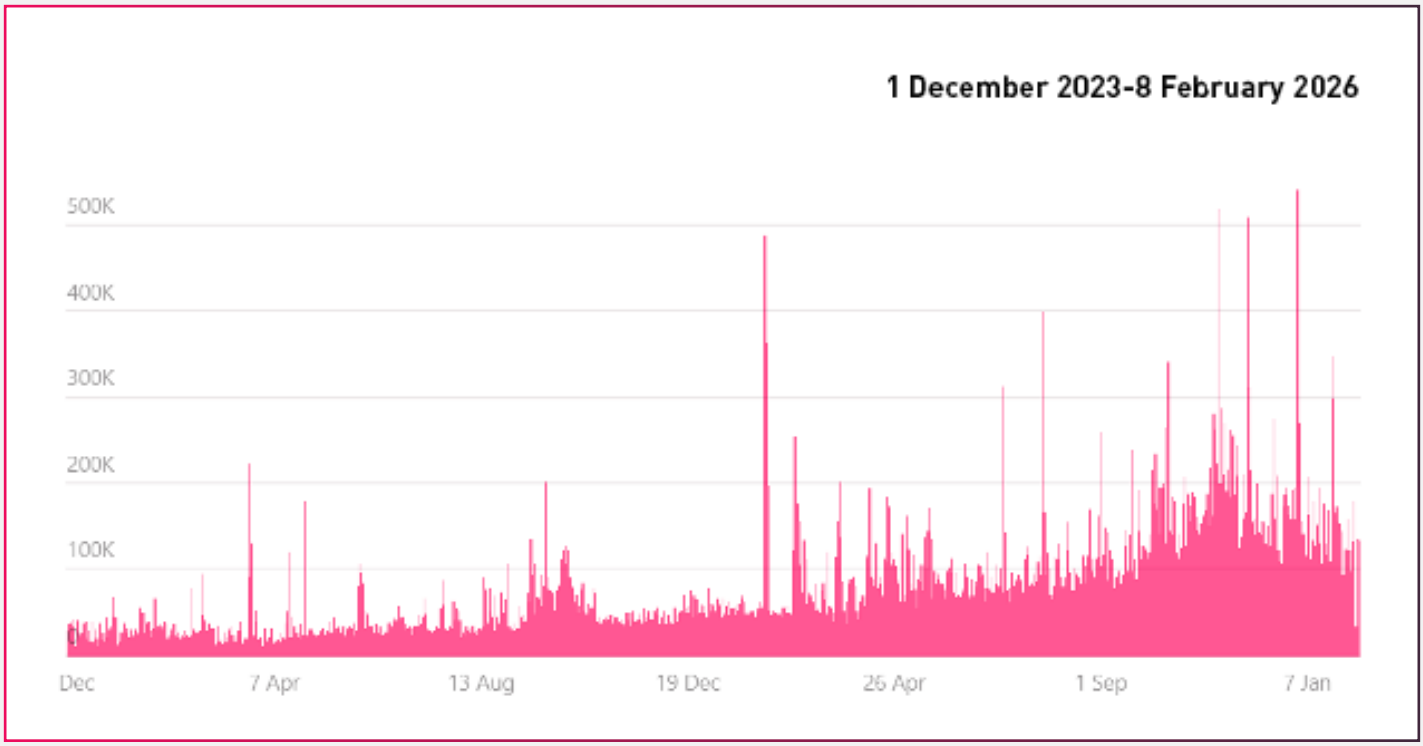
An example of the message displayed once a channel is blocked

Below is Check Point Exposure Management tracking on how often messages claiming a post came from a blocked source appeared. This data does include duplicates and forwards, but the peak in February and March and April is clear.



We determine that about 20% of the channels blocked on Telegram have some relation to criminal activity that relates to businesses and organizations and those are the ones reported on above.

And 2026 is not showing a slowdown. In fact, Telegram Moderation is booming, with the baseline climbing sharply over time. The "normal" level has risen from roughly ~10–30K takedowns earlier on to about ~80–140K in late 2025 - early 2026), indicating sustained growth rather than isolated events.



In fact the peaks have become much larger: the series reached a max of ~520K, with multiple additional late-period peaks around ~490–500K, plus an earlier standout around ~460–470K.

Big peaks become far more frequent: values >300K were rare early on but show up repeatedly in the final third of the timeline, suggesting a shift to a more extreme regime. At least 2–3 step-changes ("regime shifts") are visible. Firstly around mid 2024 a rise is evident. The second jump was around early 2025 as specified before, and since September there again was sharp increase. With each rise the baseline climbs and doesn't revert to prior levels. However volatility expands with growth: not only does the average rise, but the spread widens substantially. The late period shows dense, bursty clusters of spikes, consistent with increasingly event-driven surges.

IS THIS CAUSE FOR A MIGRATION?

As of now, we don't observe a noteworthy migration from Telegram to a specific alternative. We did see during Durov's arrest (Aug-Sep 2024) chatter on potential migration but since then, we haven't seen notable chatter in this regard.

Additionally, we don't see a considerable amount of Threat Actors sharing links to specific alternatives and leaving Telegram behind. Nevertheless, we're seeing Telegram groups and channels popping up at a faster rate than before. It is worth mentioning that some threat actors maintain a presence on other IM platforms for one-on-one communication, but Telegram remains a primary channel of communication for most Threat Actors in the arena.

SIMPLEX APP

One relatively very small movement we were able to observe was to the SimpleX app throughout early 2025 – where the AKULA group (who seem to be of Russian-speaking origin), moved its operation to SimpleX, together with its affiliated chatting group "BF Repo". The group was dissatisfied, as its followers did not follow its move to SimpleX as expected. Therefore, the groups returned to Telegram as SimpleX didn't seem to be popular enough among threat actors.

Another trend shows Telegram group admins sharing SimpleX links that lead to their personal profiles rather than actual groups or channels, emphasizing that groups aren't moving that quickly as of now.

On the left - a screenshot from a Threat Actor sharing (on Telegram) these are the only two groups they follow on SimpleX.
On the Right - AKULA expressed frustration that their followers have not migrated to SimpleX as expected, captured by Argos™.

TELEGRAM IS CLEARLY THE APP OF CHOICE

The Check Point Exposure Management team analsysed threat actor invite links over the last three months and the story is clear, threat actors clearly still prefer Telegram.

Invite Links over the past 3 months

Telegram	Discord	Signal	Element (Matrix)	SimpleX
3M	**153K**	**8K**	**6K**	**3K**

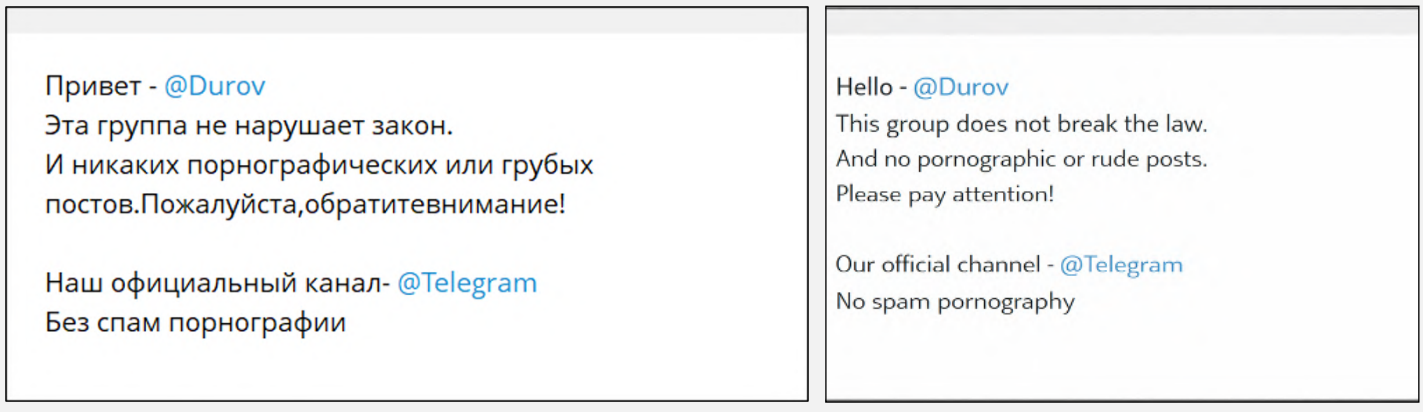
*the numbers above refer to mentions of links to social platforms across underground platforms of cybercriminals

None of the other channels come close, with the closest runner up having less than 6% (Discord) of the links posted when compared to Telegram.

EVASION TECHNIQUES: HOW THREAT ACTORS ADAPT TO INCREASED MODERATION

Threat actors have developed several techniques to avoid takedowns by moderation. They have begun to use the "Request to Join" feature to prevent automated bots and avatars from joining groups.

Not only this, but many have added a disclaimer in the channel bio, tagging Durov's profile and claiming the group/channel is legitimate and compliant with regulations, even when it isn't.



An example of a disclaimer in a bio and a translation

Finally, they have created backup channels and groups, which are often empty, to gather subscribers in advance. They also set up a Telegram community bundle that includes a backup channel.

THE FUTURE OF TELEGRAM AS A THREAT ACTOR HUB

Telegram's intensified moderation efforts throughout 2025 and into early 2026 represent a clear and sustained shift in the platform's enforcement posture. Following years of minimal intervention, the scale, frequency, and consistency of takedowns have increased dramatically, marking a structural change rather than a short lived reaction to external pressure. While these actions have disrupted a significant volume of malicious activity—particularly around carding, Fullz, and hacking-related communities—they have not fundamentally altered Telegram's role within the cybercriminal ecosystem.

Threat actors have demonstrated a high degree of adaptability. Rather than abandoning the platform, they have adjusted their operational behavior by introducing evasion techniques such as gated access, backup channels, disclaimers aimed at moderation teams, and selective use of alternative messaging platforms for limited, one to one communication. Importantly, no meaningful or sustained migration away from Telegram has been observed. Even groups that temporarily experimented with alternatives ultimately returned, reinforcing Telegram's continued dominance as the primary hub for threat actor communication and reach.

At the same time, moderation activity itself continues to accelerate. The rising baseline and increasingly frequent peaks suggest that Telegram is investing heavily in enforcement and automation, yet this escalation has so far resulted in containment rather than eradication. Criminal communities remain resilient, reconstituting quickly and leveraging Telegram's scale and network effects to maintain visibility and recruitment.

Telegram's moderation changes have reshaped the operational environment for threat actors but have not displaced them. Telegram remains the platform of choice, and its ecosystem continues to be a critical arena for monitoring cybercriminal trends, tactics, and infrastructure. As moderation pressure persists, ongoing tracking of adaptation patterns, platform abuse indicators, and cross platform signaling will remain essential to understanding how threat actors evolve, and how effective Telegram's enforcement efforts ultimately prove to be.

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: https://www.checkpoint.com/exposure-management/