Cyberint
A Check Point Company

Telegram Changes Shake Cyber Criminals

October 2024

TABLE OF CONTENTS

Timeline

EXECUTIVE SUMMARY

Telegram, with over 700 million users globally, is widely known for its privacy features, but its lack of strict moderation has made it a favored platform for cybercriminals.

Over recent years, the platform has been linked to illegal activities, including drug and weapons trafficking, child exploitation, and cybercrime operations like phishing, malware distribution, and stolen data trading.

In August 2024, Telegram CEO Pavel Durov was arrested by French authorities on charges related to enabling illegal activities and money laundering. Following his release, Durov announced changes to Telegram's policies, including disclosing user data, such as IP addresses and phone numbers, in response to legal requests for rule violations. Enhanced moderation measures were also introduced.

While some are exploring alternative platforms like Signal, Jabber, and SimpleX, the majority still favor Telegram. Many cybercriminals continue to use Telegram due to its large user base and community features.

The long-term impact of these changes is uncertain, but Telegram remains a key platform for both legitimate users and criminals, as it balances privacy with increasing legal scrutiny.

INTRODUCTION

Telegram, a cloud-based messaging app with over 700 million users globally, has emerged as a platform that prioritizes privacy and security. Known for its encrypted communication features, it allows users to send various types of content and supports large groups and channels. While widely popular for its commitment to privacy, this minimal moderation has also attracted cybercriminals and other bad actors.

In late August 2024, French authorities arrested Telegram CEO Pavel Durov as part of an investigation into alleged criminal activities on the platform. Charges included enabling illegal transactions, complicity in child exploitation, non-compliance with authorities, and money laundering.

Following his release, Durov announced policy changes, including disclosing user data, such as IP addresses and phone numbers for rules violations in response to legal requests.

CYBERCRIME ACTIVITY ON TELEGRAM

In the last years, Telegram has been implicated in facilitating various illegal activities:

1. Drug and weapons trafficking
2. Terrorism and extremism
3. Child exploitation
4. Cybercrime, including:
    a. Trading stolen data
    b. Selling malware
    c. Setting up illegal marketplaces
    d. Automating phishing attacks
    e. Coordinating cyberattacks

Cybercriminals are using Telegram's features like bots and channels to set up marketplaces, automate phishing, distribute malware, and manage command-and-control operations.

CEO'S DETENTION AND PRIVACY POLICY CHANGES

In August 2024, Telegram's CEO, Pavel Durov was arrested by French authorities at Le Bourget airport while traveling from Azerbaijan.

Durov, a Russian-born entrepreneur who founded Telegram in 2013, faced charges including enabling illegal transactions, complicity in disseminating child sexual abuse materials, non-compliance with authorities, and money laundering.
A few days later Durov was released on €5 million bail.

Interestingly, Russian officials expressed unexpected support for Durov, possibly indicating a reliance on Telegram for military communications due to its encryption. With Russia engaged in conflict with Ukraine, France's decision to arrest Durov may have had political undertones, as France has been a staunch supporter of Ukraine in its war efforts.

The effects of Durov's arrest

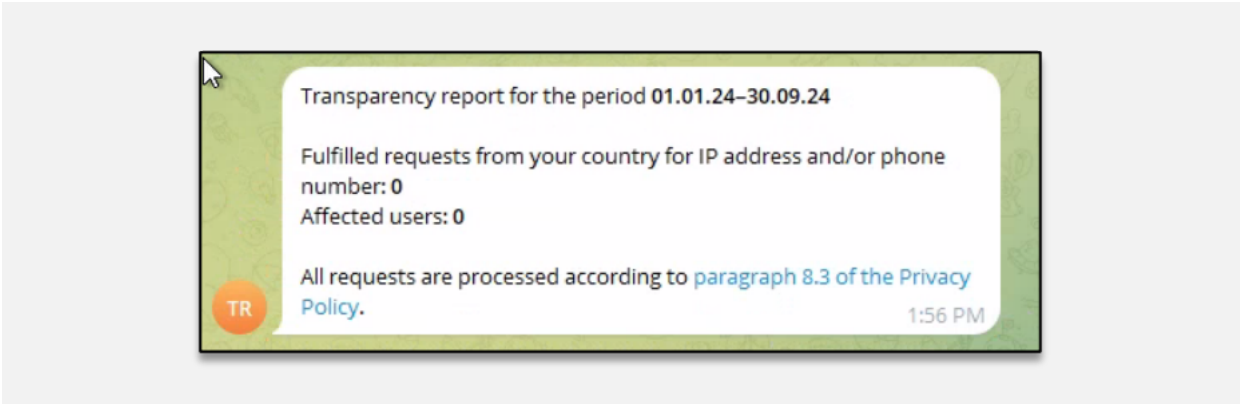
Following his release, Durov announced changes to Telegram's policies:

- Disclosure of user IP addresses and phone numbers for rule violations in response to legal requests.
- Removal of new media uploads to Telegram and the "People Nearby" feature.
- Strengthened moderation efforts and updated FAQs to reflect a more compliant stance on content moderation.

It is worth mentioning that Durov recently clarified on his Telegram channel that no major changes were made to Telegram's policies. Since 2018, the platform has been authorized to disclose IP addresses and phone numbers of criminals to authorities based on legal requests.

Transparency and Trust

To enhance users' trust, Telegram launched the @transparency bot. This tool provides reports on Telegram's responses to law enforcement data requests, in line with section 8.3 of its Privacy Policy. Users can access these transparency reports directly through the bot.



Querying the bot yielded no results

TELEGRAM PLATFORM CHANGES

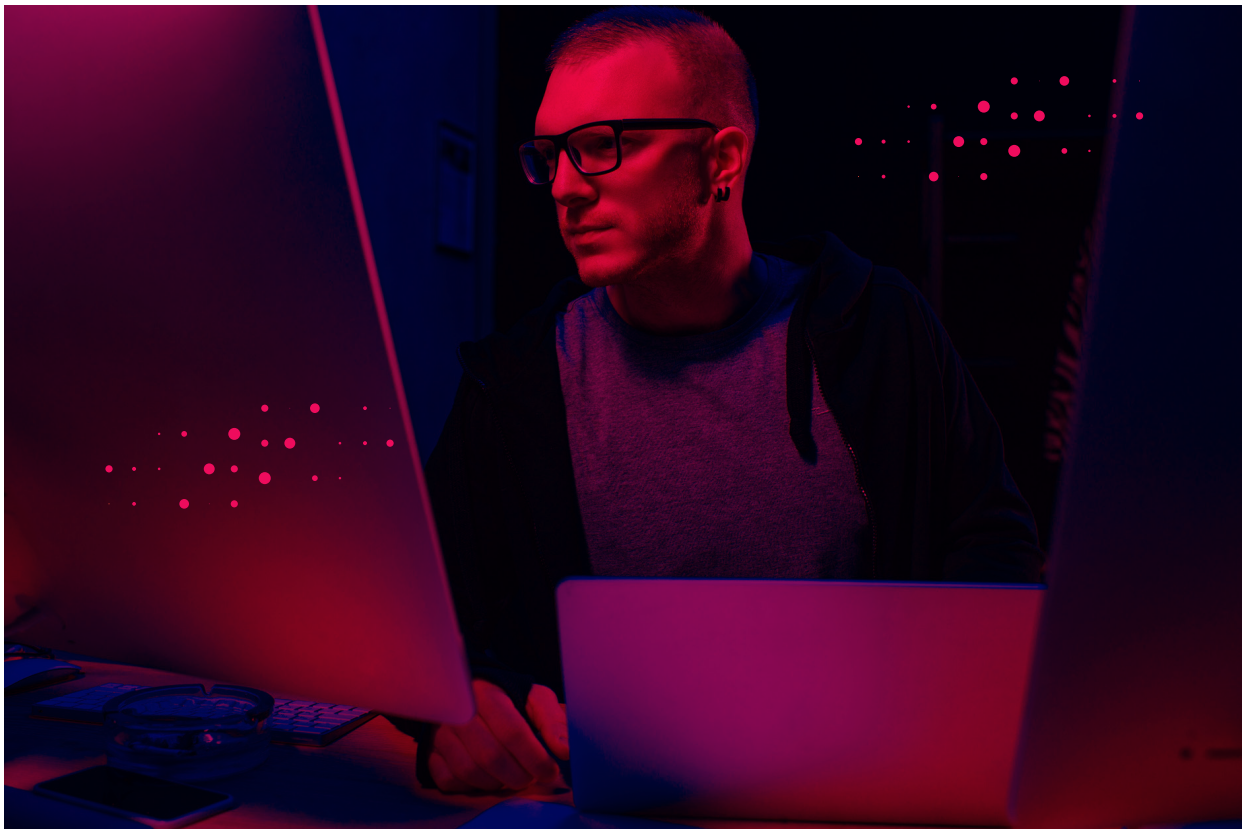
Besides the privacy policy changes, Telegram has made additional changes in the platform:

1. **New moderation measures introduced**, including the use of artificial intelligence to detect and remove problematic content from search results. This is part of a broader effort to address concerns about illegal activities facilitated through the app.

2. **New Business Nearby feature:** The "People Nearby" feature, which allowed users to connect with others in their area, has been disabled and replaced with a "Businesses Nearby" feature that focuses on verified businesses.

3. **Changes in FAQ section and Reporting Mechanisms:** Telegram has updated its FAQ section to clarify the process for reporting illegal content, shifting away from previous claims that private chats were entirely secure and not subject to legal requests.

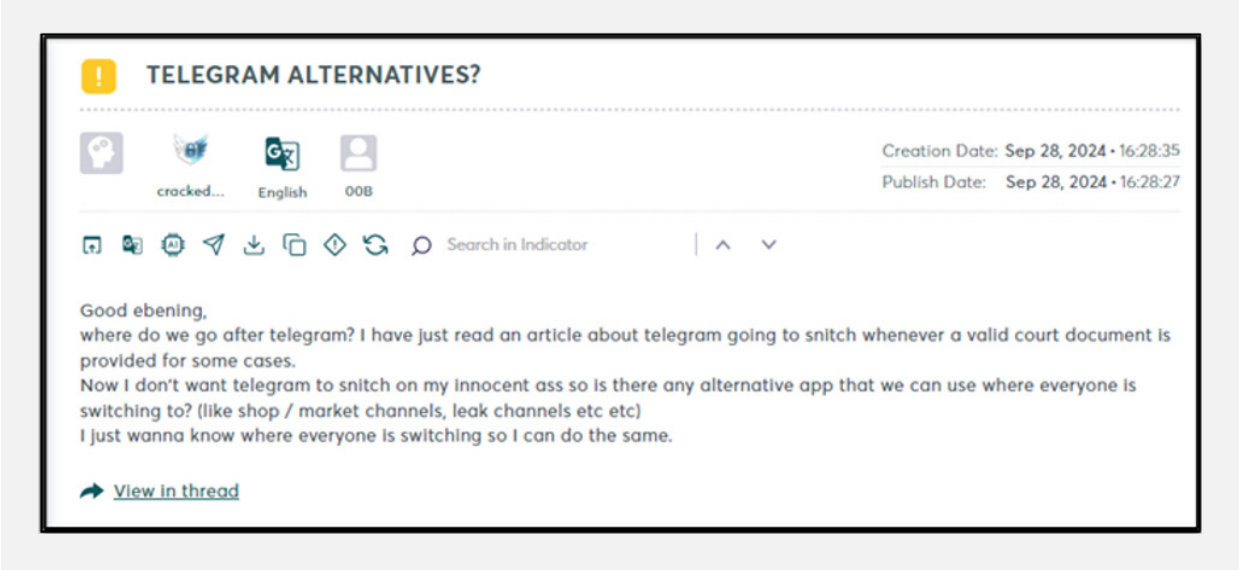
   On September 23 Durov announced in his Telegram channel that "...a dedicated team of moderators, leveraging AI, has made Telegram Search much safer. All the problematic content we identified in Search is no longer accessible..."



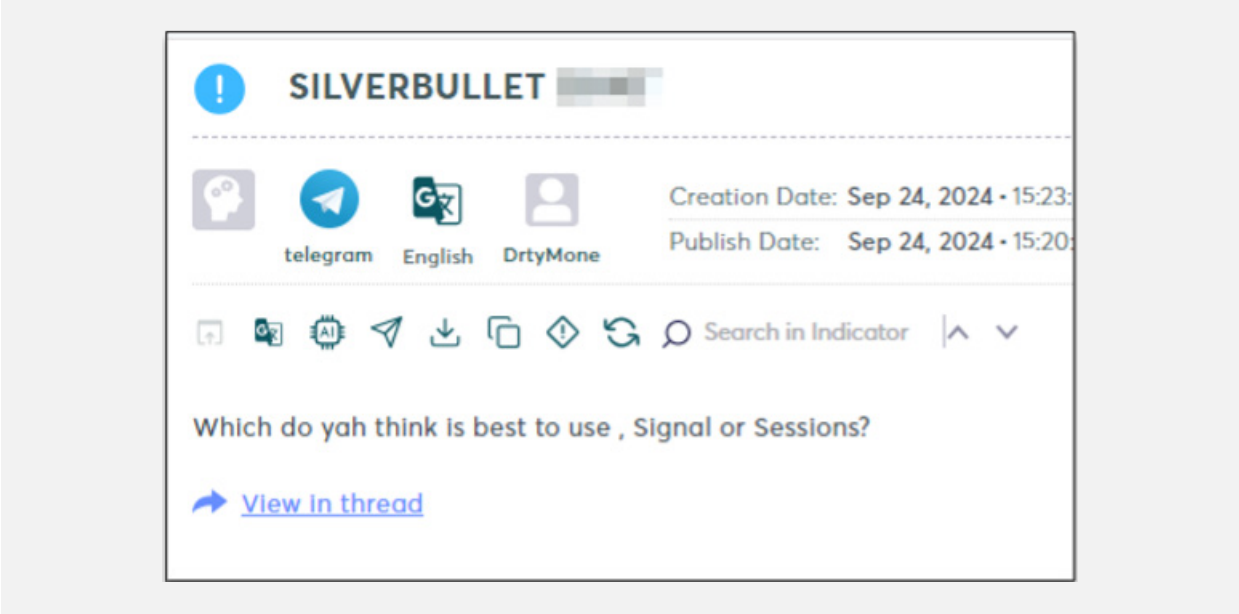
THREAT ACTORS ARE WORRIED

Following Telegram's policy changes, Cyberint observed discussions among threat actors on major underground forums about potential alternatives to Telegram.

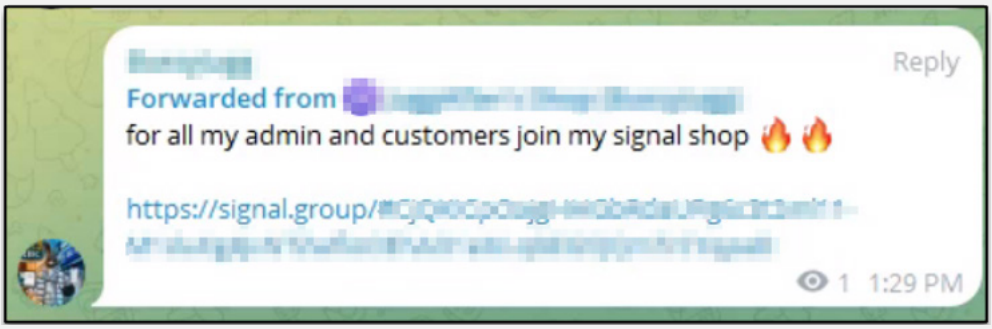
In some instances, **administrators have begun migrating their activities to other platforms** and informing their members about these new locations.



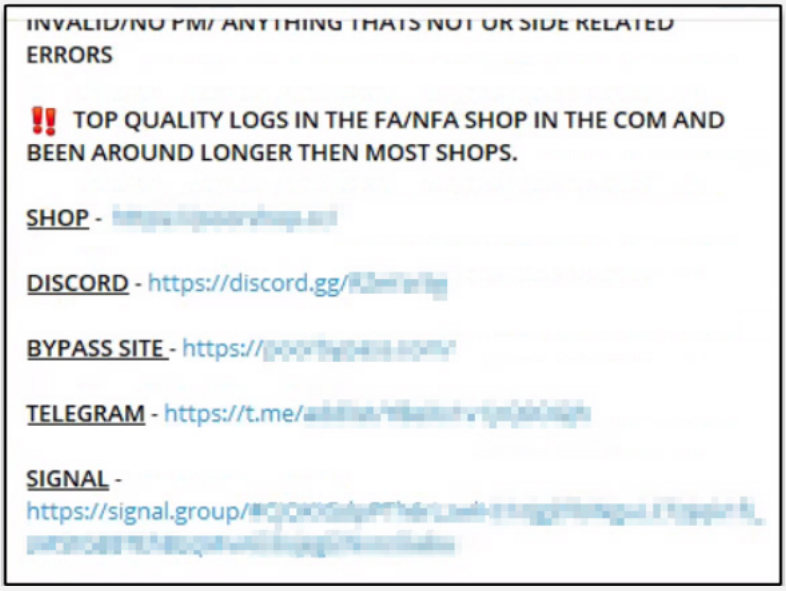
A threat actor posted a thread in Cracked, a major dark web forum, about concerns with Telegram.



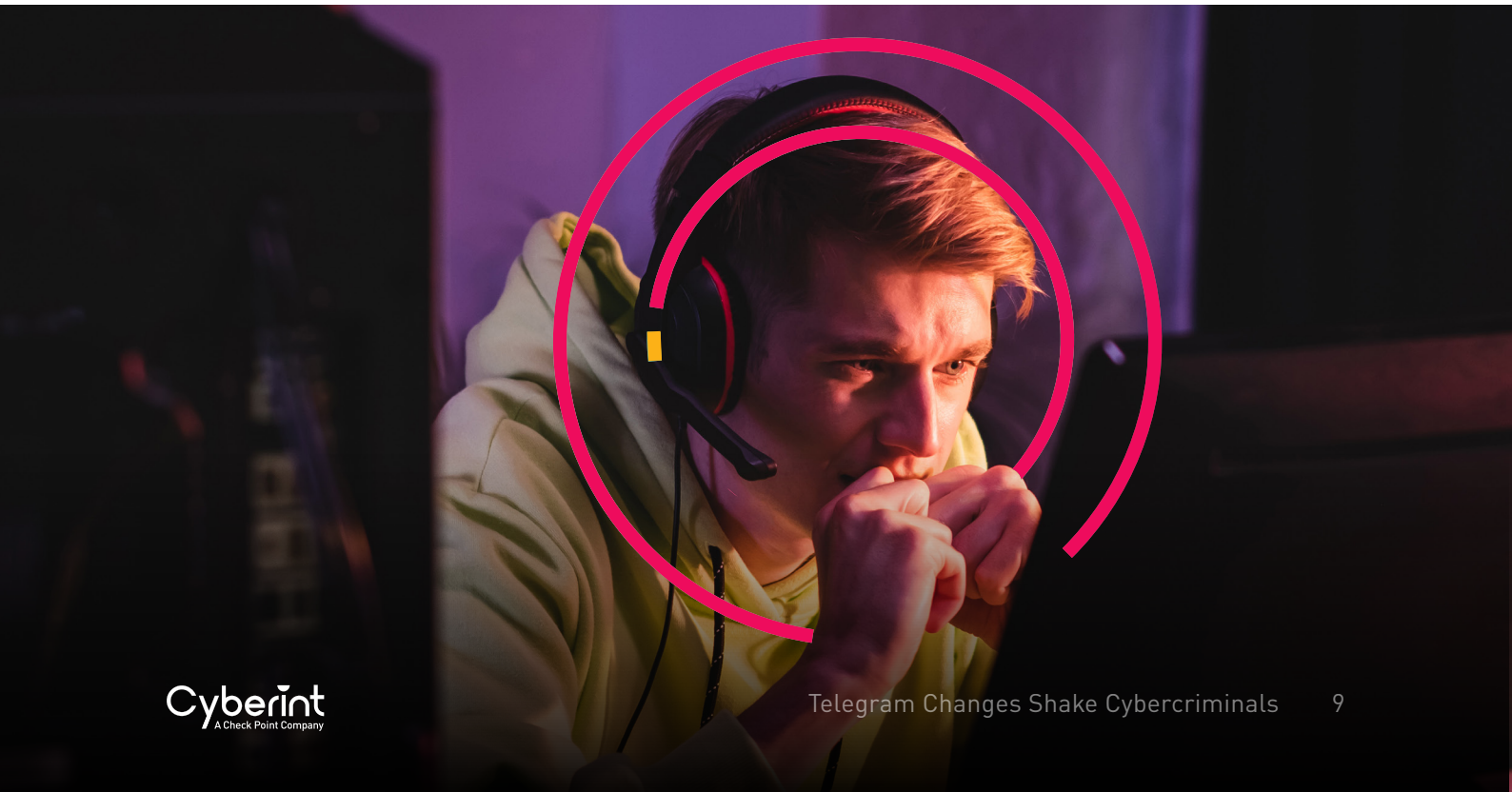
Cybercriminals are confused, as seen in this Telegram group that is focused on credential stuffing attacks.



An invitation link to a Signal group



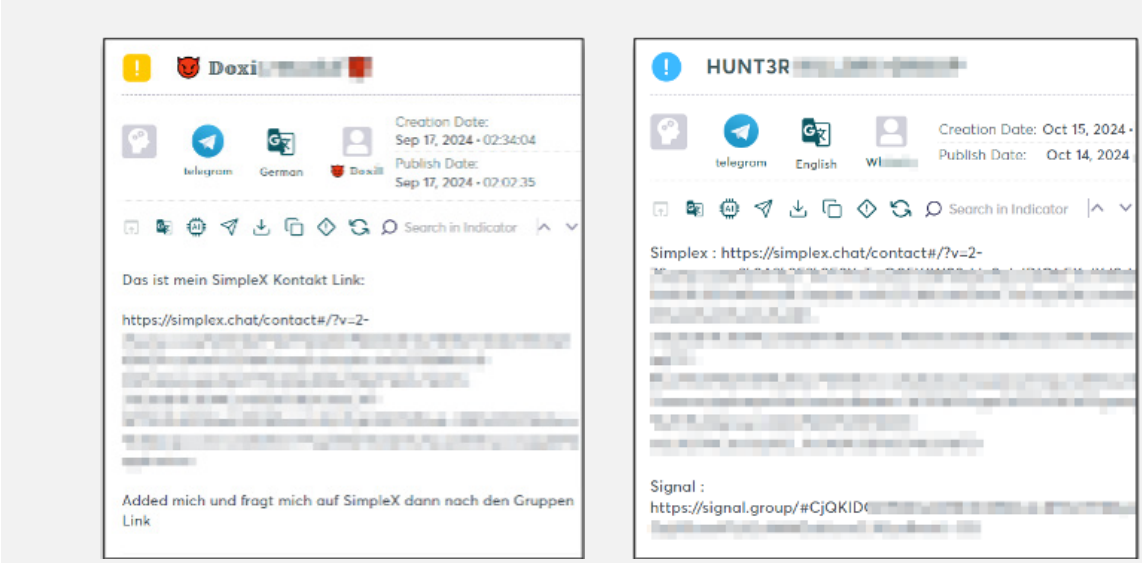
An invitation link to a Signal and Discord group



Transparency and Trust

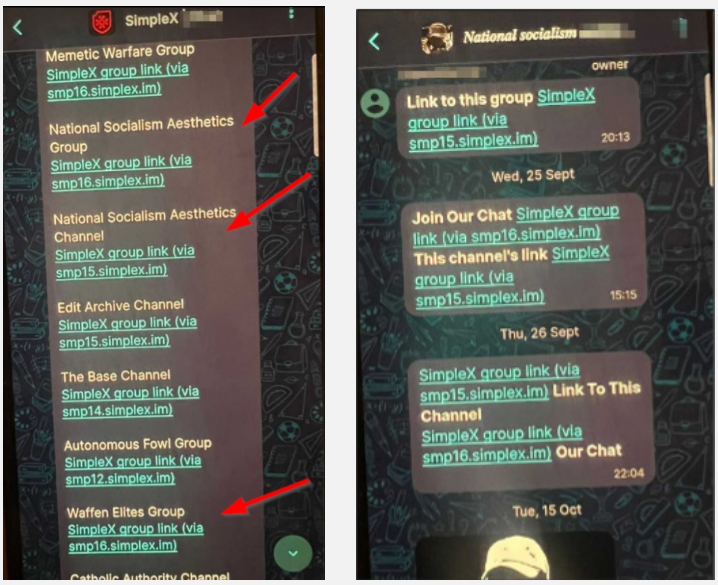
Based on data from the Infinity ERM solution and analysis of various forums and Telegram channels, Cyberint identified several potential alternatives to Telegram that cybercriminals are considering.

These include Signal, Jabber, Session, Discord, Matrix, and SimpleX, among others.



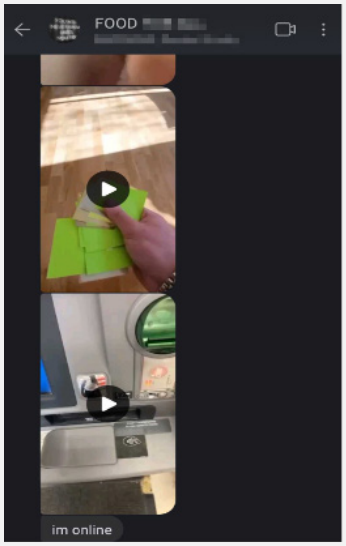
Check Point Infinity ERM showing Threat Actors sharing invite links to Signal and SimpleX.

Notably, SimpleX appears to be less popular among Chinese and Russian-speaking Threat Actors but more attractive among Europe and the US, as well as among far-right and neo-Nazi groups.



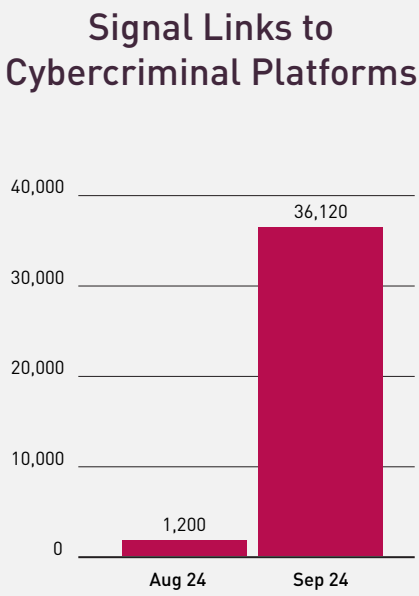
Screenshots from SimpleX, showing neo-Nazi underground groups

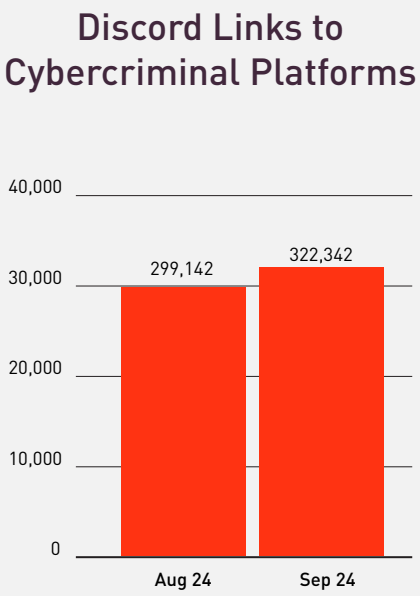
During our investigation of SimpleX links in underground Threat Actor forums, we identified over 6,000 mentions in September and early October—nearly double the volume recorded in August.



A Screenshot from Signal, showing a Threat Actor offering money laundering services and ATM scams

By examining invitation link mentions across different platforms collected by Infinity ERM, we compared the frequency of these alternatives before and after Telegram's recent announcements, providing insight into shifting preferences within cybercriminal communities.





As part of our investigative efforts, we tracked invite links shared by threat actor groups claiming to migrate to alternative platforms (e.g., SimpleX, Signal, Session). Our analysis led to the following conclusions:

- In most cases, the new alternative groups have only dozens or hundreds of members, compared to the thousands or tens of thousands still active on Telegram.

- Many of these newly-created groups on emerging platforms currently show little content or interaction, in contrast to the more active groups still on Telegram.

- It appears that many threat actors have established groups on alternative apps more for publicity purposes than for genuine migration or community building.

While not all alternatives to Telegram offer the same level of features, threat actors are still considering shifting to these platforms. However, it is worth mentioning, no one truly knows whether alternatives to Telegram provide a higher level of privacy.

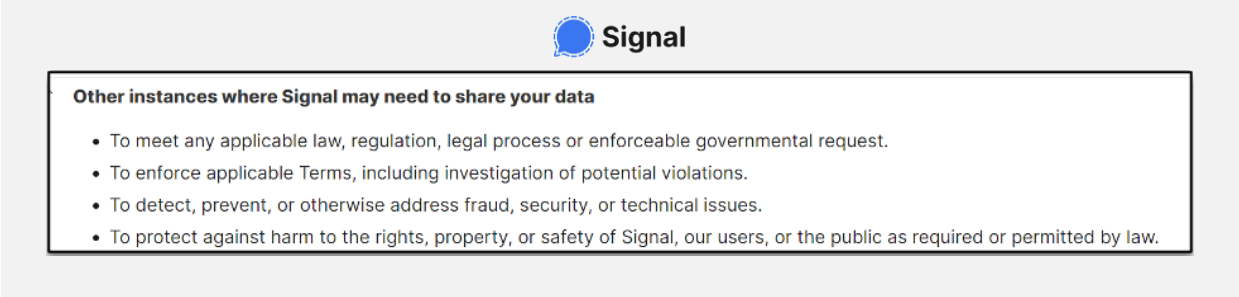
SECURITY MEASURES BY THREAT ACTORS

In general, cybercriminals are increasingly prioritizing security and identity protection on Telegram, as they are generally knowledgeable about security protocols. As Telegram enforces stricter privacy policies, we expect users to adopt enhanced security tools like encrypted communications and anonymity features. Consequently, any shift in user behavior may have a minimal overall impact on cybercriminal activities.

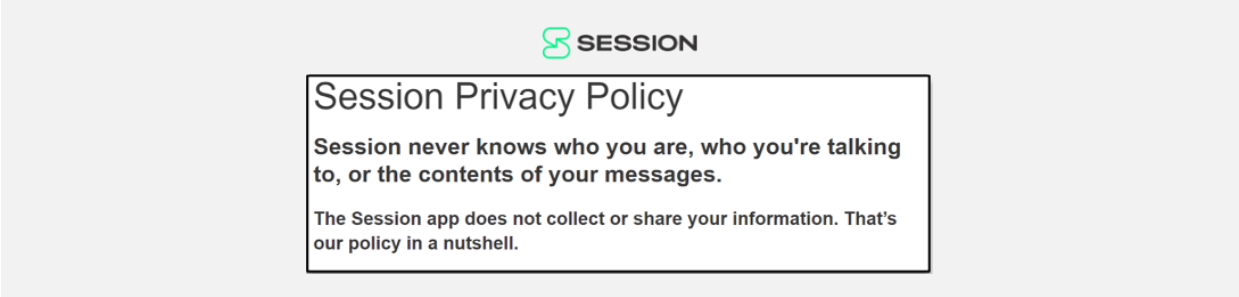
How safe are the alternatives?

While some might consider switching to alternative platforms for better privacy, the effectiveness of these options remains uncertain.

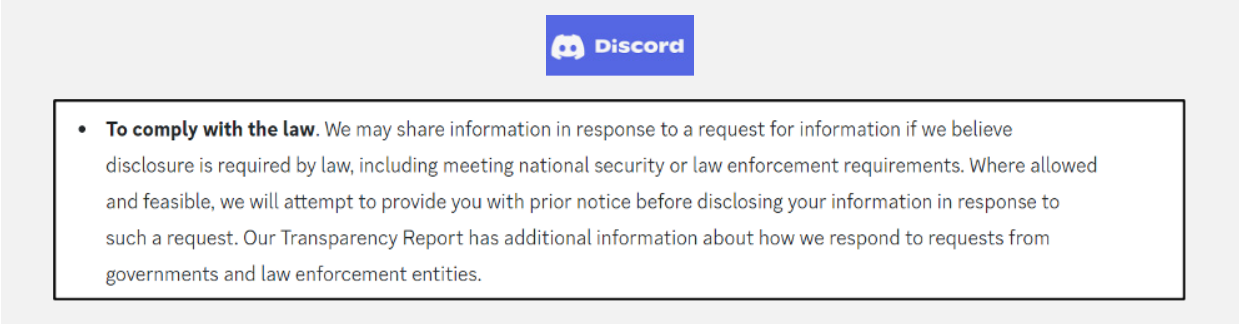
We have taken a deeper look at the alternatives privacy policy sections and compared them into Telegram.



Source: https://signal.org/legal/



Source: https://getsession.org/privacy-policy



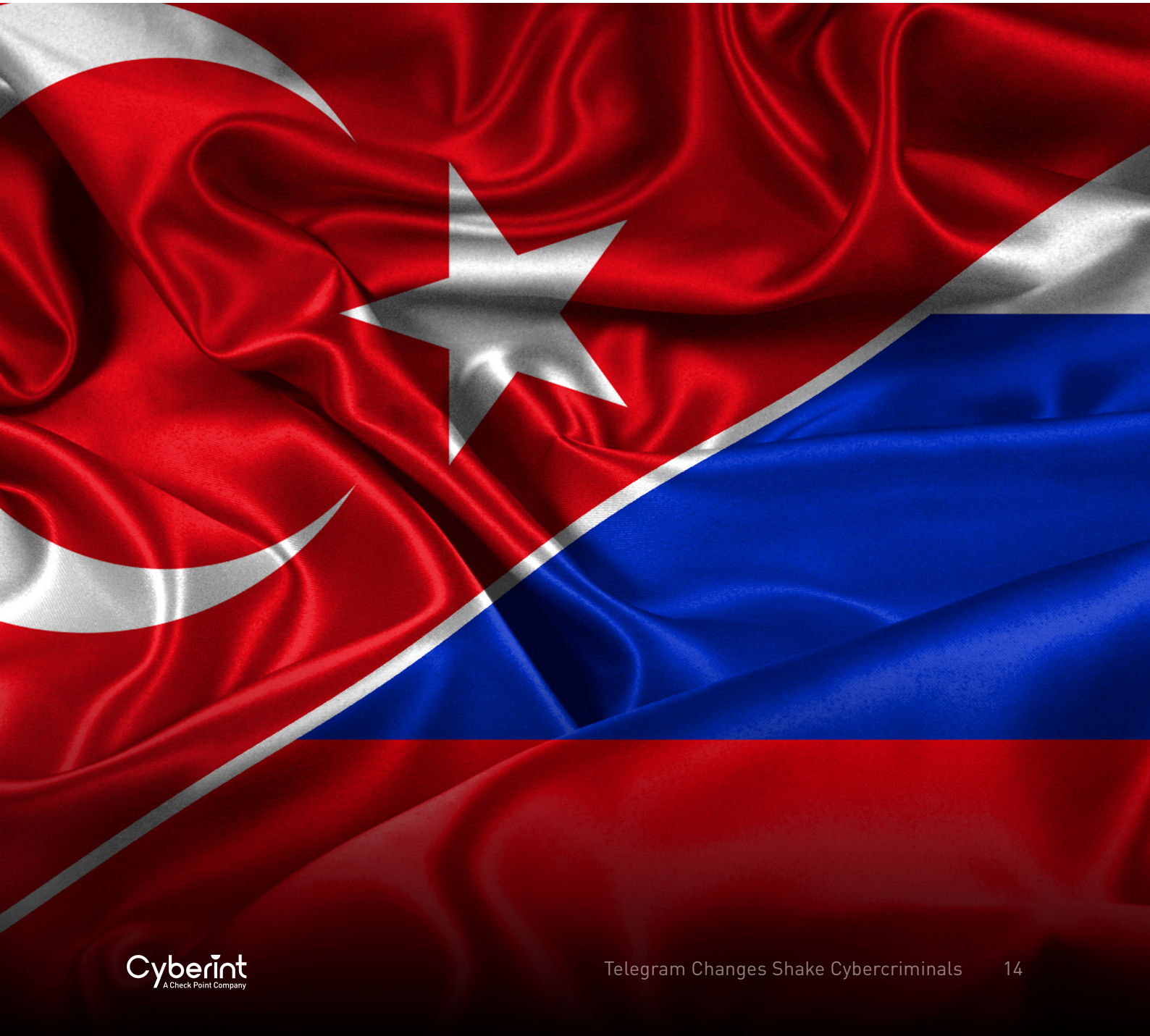
Source: https://discord.com/terms/privacy-policy-march-2022#5

RUSSIA AND TURKEY BAN DISCORD

Discord has been blocked in Russia and Turkey for violating local laws. In Russia, the ban was enacted on October 8, 2024, due to the platform's distribution of illegal materials and refusal to remove them.

In Turkey, the ban followed an Ankara court's ruling regarding child abuse and obscenity allegations, with authorities citing Discord's lack of cooperation.

Regardless of Telegram’s changes, or not, it is something that cannot be ignored when analyzing recent trends in the underground world.



CONCLUSIONS

The recent changes to the Telegram platform are substantial and have left many users feeling vulnerable to law enforcement scrutiny.

It is difficult to predict the impact of these changes and whether users will genuinely migrate to alternative platforms, especially since it remains uncertain if these alternatives offer improved privacy.

We anticipate a shift towards other platforms; however, we also expect users to pay greater attention to security measures and identity protection while using Telegram. Given that we are discussing cybercriminals, they are inherently aware of security protocols, so these regulatory changes are unlikely to significantly affect their activities.

The recent changes may influence our crawling and data collection efforts of cybersecurity enterprises, particularly due to the impact on threat actors' activities and availability. Building a channel takes time; it involves cultivating a community, attracting members, and establishing a solid reputation.

Cyberint will persist in monitoring these changes and will adapt our tools as needed.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-37-286-777
17 Ha-Mefalsim St Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House,
14-18 Great Titchfield Street,
London, W1W 8BD

USA TX

Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm